Über die Bestimmung der ganzen Elemente in Radikalerweiterungen algebraischer Zahlkörper

vorgelegt von
Diplom–Mathematiker
Mario Daberkow
aus Dormagen

Vom Fachbereich 3 Mathematik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation.

Berlin 1995
D83

Promotionsausschuß

Vorsitzender:	*Professor Dr. Simon*
Berichter:	*Professor Dr. Pohst*
Berichter:	*Professor Dr. Jung*

Tag der wissenschaftlichen Aussprache: 2. März 1995

Inhaltsverzeichnis

KAPITEL 1

Einleitung

Das Bestreben, Algorithmen in der Zahlentheorie zu entwickeln, war schon zur Zeit der griechischen Antike weit verbreitet, was unter anderem die Schriften von Euklid und Diophant[1] belegen. Im Laufe der Zeit wurden Beispiele ein immer wichtigeres Hilfsmittel zur Erschließung der Theorie, so daß Algorithmen mehr und mehr an Bedeutung gewannen und heute in vielen Bereichen der Mathematik ein eigenständiges Forschungsgebiet sind.
Als Begründer der algebraischen Zahlentheorie kann wohl C. F. Gauß mit seinem berühmten Werk *Disquisitiones Arithmeticae* [Ga] bezeichnet werden. Auch er legte Wert auf die Berechenbarkeit theoretischer Ergebnisse. Nach Gauß haben sich viele große Mathematiker mit der algebraischen Zahlentheorie befaßt und wunderbare und tiefliegende Aussagen bewiesen. So bezeichnet Hilbert die „Theorie der Zahlkörper" als ein „Bauwerk von wunderbarer Schönheit und Harmonie" [Hi].
Zu Beginn dieses Jahrhunderts wurde der Berechenbarkeit von Invarianten algebraischer Zahlkörper durch die explizite Formulierung von Algorithmen mehr Aufmerksamkeit gewidmet. So hat G. F. Voronoi [Vo] schon um die Jahrhundertwende einen effizienten Algorithmus angegeben, mit dem für gewisse Zahlkörper die Einheitengruppe bestimmt werden kann. Eine der herausragenden Personen auf dem Gebiet der algorithmischen bzw. konstruktiven Zahlentheorie war H. Zassenhaus[2] [Po94], der sich intensiv mit den konstruktiven Problemen der algebraischen Zahlentheorie beschäftigte und zusammen mit anderen Mathematikern die ersten Algorithmen für die Bestimmung von Ganzheitsbasis [Za, Bo], Einheitengruppe [PoWeZa, PoZa77] und Klassenzahl [PoZa85] beliebiger algebraischer Zahlkörper formulierte.

[1] Diophant schrieb um 250 v. Chr. eine Serie von 13 Büchern, *Arithmetica*.
[2] H. Zassenhaus verstarb am 21.11.1991.

Die Kenntnis einer Ganzheitsbasis ist für die konstruktive algebraische Zahlentheorie von besonderer Bedeutung, denn im allgemeinen wird eine solche benötigt, um weitere Größen, wie die Klassenzahl oder die Einheitengruppe eines Zahlkörpers, zu bestimmen. Es existieren zwar Algorithmen, die eine solche Basis berechnen können [Za, Bo, Fo87, Fo92], sie sind aber aus mehreren Gründen für die Berechnung einer Ganzheitsbasis in Körpern höheren Grades (Grad > 50) nur sehr bedingt einsetzbar. In allen allgemeinen Methoden zur Ganzheitsbasenberechnung eines Zahlkörpers muß neben anderen Schwierigkeiten die Polynomdiskriminante eines den Körper erzeugenden Polynoms soweit faktorisiert werden, bis alle quadratischen Faktoren bekannt sind. Dies ist meist ein recht aufwendiges Problem.
Im Rahmen dieser Arbeit werden wir für die in der Klassenkörpertheorie wichtigen Kummererweiterungen, also für Relativerweiterungen der Form $\mathcal{E} = \mathcal{F}(\sqrt[n]{\mu})$, wobei $\mathcal{F}$ ein algebraischer Zahlkörper mit $\zeta_n \in \mathcal{F}$ ist, ein spezielles Verfahren zur Bestimmung der ganzen Elemente $o_{\mathcal{E}}$ von $\mathcal{E}$ vorstellen. Bei dieser Methode kann das Problem der Faktorisierung großer Zahlen weitestgehend vermieden werden. Es müssen nur vergleichsweise kleine Zahlen faktorisiert werden.
Wir werden einen Algorithmus angeben, der für eine gegebene Kummererweiterung $\mathcal{E}/\mathcal{F}$ zunächst ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ berechnet, und dann auch eine Ganzheitsbasis von $o_{\mathcal{E}}$ bestimmt. Anwendung findet das Verfahren bei verallgemeinerten Kummererweiterungen, womit alle abelschen Erweiterungen vom Grad n eines algebraischen Zahlkörpers $\mathcal{F}$ mit $\zeta_n \in \mathcal{F}$ behandelt werden können. Damit ist es dann möglich, für beliebige Radikalerweiterungen eine Ganzheitsbasis zu bestimmen.
Die Ergebnisse dieser Arbeit sind Verallgemeinerungen der entsprechenden Aussagen über relativquadratische Erweiterungen algebraischer Zahlkörper, die der Autor dieser Arbeit im Rahmen seiner Diplomarbeit [Da] behandelt hat. Die Verallgemeinerung baut auf der Theorie der Kummererweiterungen [Ha26, He] auf. Um die nötigen Aussagen beweisen zu können, wird das Hassesche „Lokal – Global“ Prinzip benutzt. Wir werden dazu gewisse Aussagen für die von Hensel eingeführten $\mathfrak{p}$–adischen Zahlen [Hen] beweisen und diese Ergebnisse dann auf den Zahlkörperfall übertragen. Dabei werden uns zunächst ausschließlich Kummererweiterungen von Primzahlgrad beschäftigen. Dieser Spezialfall wird es uns dann ermöglichen, den allgemeinen Fall einer Kummererweiterung und beliebige Radikalerweiterungen zu behandeln.

Eine große Anzahl von Beispielen zum Abschluß der Arbeit wird die Leistungsfähigkeit des Verfahrens unterstreichen. Es wurden mit diesem Algorithmus Ganzheitsbasen von Körpern $\mathcal{E}$ mit $[\mathcal{E} : \mathbb{Q}] > 1000$ bestimmt und Körperdiskriminanten mit mehreren 1000 Stellen berechnet.

KAPITEL 2

Grundlagen

In diesem Kapitel stellen wir einige theoretische Grundlagen für die weitere Arbeit bereit und definieren die wichtigsten Begriffe.

1. Kreisteilungskörper

Wir werden nun kurz die für diese Arbeit wichtigsten Ergebnisse aus der Theorie der Kreisteilungskörper zusammenfassen. Da die Ergebnisse einer mittlerweile stark vereinheitlichten Theorie entspringen, verzichten wir jeweils auf Literaturverweise. Alle aufgeführten Aussagen können in [CaFr, Ko, La65, La86, Na, Ne] nachgelesen werden.

Definition 2.1. *Sei n eine natürliche Zahl. Eine primitive n–te Einheitswurzel ζ_n ist eine Nullstelle des Polynoms*

$$t^n - 1 \in \mathbb{Z}[t],$$

für die $\zeta_n^k \neq 1$ $(0 < k < n)$ gilt. Der algebraische Zahlkörper $\mathbb{Q}(\zeta_n)$ heißt der n–te Kreisteilungskörper.

Der Ganzheitsring $o_{\mathcal{F}}$ eines Kreisteilungskörper $\mathcal{F}$ ist sehr einfach. Gilt $\mathcal{F} = \mathbb{Q}(\zeta_n)$ für $n \in \mathbb{N}$, so erhalten wir $o_{\mathcal{F}} = \mathbb{Z}[\zeta_n]$ mit Diskriminante

$$\mathfrak{d}_{\mathcal{F}} = n^{\varphi(n)} / \prod_{p|n} p^{\varphi(n)/(p-1)},$$

wobei φ die Eulersche φ–Funktion sei.
Wir werden im weiteren immer wieder auf Kreisteilungsköper der Form $\mathbb{Q}(\zeta_p)$ mit

$p \in \mathbb{P}$ zurückkommen. Wichtig bei diesen speziellen Kreisteilungskörpern ist für uns die Zerlegung von Primzahlen in Primideale.

SATZ 2.2. *Sei $p \in \mathbb{P}$ eine Primzahl und $\mathcal{F} = \mathbb{Q}(\zeta_p)$ bezeichne den p–ten Kreisteilungskörper.*

(i) *Es gilt $po_{\mathcal{F}} = \mathfrak{p}^{p-1}$ mit $\mathfrak{p} = (1-\zeta_p)o_{\mathcal{F}}$ und $\mathfrak{f}(\mathfrak{p}/p) = 1$.*
(ii) *Zu $q \in \mathbb{P} \setminus \{p\}$ sei $f \in \mathbb{N}$ die kleinste Lösung von $q^f \equiv 1 \mod p$. Dann gilt $qo_{\mathcal{F}} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$, wobei $r = \varphi(p)/f$ und $\mathfrak{f}(\mathfrak{p}_i/p) = f$ für $1 \leq i \leq r$ gelten.*

2. $\mathfrak{p}$–adische Körper

Die im folgenden wiedergegebenen Aussagen über $\mathfrak{p}$–adische Körper entnehmen wir [Ca, Ko, Na, Ne, PoZa89]. Ist $(\mathcal{K}, |\cdot|)$ ein bewerteter Körper, der eine endliche Erweiterung von $\mathbb{Q}_p$ für ein $p \in \mathbb{P}$ ist, so bezeichnen wir $\mathcal{K}$ als einen $\mathfrak{p}$–adischen Körper.
Für einen solchen Körper definieren wir

(i) $o_{\mathcal{K}} := \{x \in \mathcal{K} \mid |x| \leq 1\}$ als den Ring der ganzen Elemente in $\mathcal{K}$,
(ii) $\mathfrak{p}_{\mathcal{K}} := \{x \in o_{\mathcal{K}} \mid |x| < 1\}$ als das maximale Ideal in $o_{\mathcal{K}}$.

Ferner bezeichnen wir mit $\nu_{\mathcal{K}}(\cdot)$ die zu $\mathcal{K}$ gehörige exponentielle Bewertung. Als den Restklassenkörper von $\mathcal{K}$ bezeichnen wir dann den Faktor $o_{\mathcal{K}}/\mathfrak{p}_{\mathcal{K}}$, wobei wir die Charakteristik dieses Körpers als die Restklassencharakteristik von $\mathcal{K}$ bezeichnen, welche immer positiv ist.
Zwei wichtige Invarianten einer (endlichen) Erweiterung $\mathcal{L}/\mathcal{K}$ $\mathfrak{p}$–adischer Körper sind die Diskriminante $\mathfrak{d}_{\mathcal{L}/\mathcal{K}}$ und die Differente $\mathfrak{D}_{\mathcal{L}/\mathcal{K}}$. Die Differente ist das inverse Ideal der Codifferente

$$\mathfrak{D}^*_{\mathcal{L}/\mathcal{K}} := \{a \in \mathcal{L} \mid \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(ao_{\mathcal{L}}) \subseteq o_{\mathcal{K}}\}.$$

Die Norm $\mathrm{N}_{\mathcal{L}/\mathcal{K}}\left(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}\right)$ der Differente bezeichnet man als Diskriminante. Da $o_{\mathcal{L}}$ und $o_{\mathcal{K}}$ Hauptidealringe sind, ist es in der Literatur auch üblich, die Diskriminante einer Erweiterung $\mathcal{L}/\mathcal{K}$ über die Diskriminante einer $o_{\mathcal{K}}$–Basis von $o_{\mathcal{L}}$ zu definieren. Da die Diskriminante einer solchen Basis nur modulo dem Quadrat einer Einheit in $o_{\mathcal{K}}$ eindeutig ist, wird die Diskriminante der Erweiterung $\mathcal{L}/\mathcal{K}$ in diesem Fall als Element des (multiplikativen) Faktors $o_{\mathcal{K}}/U^2_{\mathcal{K}}$ definiert. Ist $d \cdot U^2_{\mathcal{K}}$ die so definierte Diskriminante, so gilt

$$do_{\mathcal{K}} = \mathfrak{d}_{\mathcal{L}/\mathcal{K}}.$$

Für unsere Zwecke ist die schwächere Idealdefinition $\mathrm{N}_{\mathcal{L}/\mathcal{K}}\left(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}\right)$ jedoch völlig ausreichend.

Ist $\alpha \in \mathcal{L}$ mit charakteristischem Polynom $f_\alpha(t) \in \mathcal{K}[t]$ gegeben, so bezeichnen wir $d_{\mathcal{L}/\mathcal{K}}(\alpha) := f'_\alpha(\alpha)$ als die Differente des Elements α.

SATZ 2.3. *Ist $\mathcal{L}/\mathcal{K}$ eine Erweiterung $\mathfrak{p}$–adischer Körper, so gilt*

$$\mathfrak{D}_{\mathcal{L}/\mathcal{K}} =< d_{\mathcal{L}/\mathcal{K}}(\alpha) \mid \alpha \in o_{\mathcal{L}} \text{ mit } \mathcal{L} = \mathcal{K}(\alpha) >_{o_{\mathcal{L}}},$$

d.h. die Differente der Erweiterung $\mathcal{L}/\mathcal{K}$ ist dasjenige Ideal in $o_{\mathcal{L}}$, das von allen Differenten $d_{\mathcal{L}/\mathcal{K}}(\alpha)$ mit $\mathcal{L} = \mathcal{K}(\alpha)$ erzeugt wird.

Die Bedeutung der Differente spiegelt sich in der folgenden Aussage wieder.

SATZ 2.4. *Sei $\mathcal{L}/\mathcal{K}$ eine Erweiterung $\mathfrak{p}$–adischer Körper. $\mathcal{L}/\mathcal{K}$ ist genau dann verzweigt, wenn $\nu_{\mathcal{L}}\left(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}\right) > 0$ gilt. Dies wiederum ist äquivalent zu $\nu_{\mathcal{K}}\left(\mathfrak{d}_{\mathcal{L}/\mathcal{K}}\right) > 0$.*

Für eine Erweiterung $\mathcal{L}/\mathcal{K}$ von $\mathfrak{p}$–adischen Körpern hat der Ring $o_{\mathcal{L}}$ eine relativ einfache $o_{\mathcal{K}}$–Basis. Ist nämlich $\pi_{\mathcal{L}} \in o_{\mathcal{L}}$ mit $|\pi_{\mathcal{L}}|_{\mathcal{L}} = \max\{|x|_{\mathcal{L}} \mid x \in \mathfrak{p}_{\mathcal{L}}\}$ gegeben, und ist $\{\beta_1, \ldots, \beta_{\mathfrak{f}(\mathcal{L}/\mathcal{K})}\} \subset o_{\mathcal{K}}$ ein vollständiges Restsystem von $(o_{\mathcal{L}}/\mathfrak{p}_{\mathcal{L}})/(o_{\mathcal{K}}/\mathfrak{p}_{\mathcal{K}})$, so gilt

$$o_{\mathcal{L}} = \left[\{\pi_{\mathcal{L}}^i \beta_j \mid 0 \le i < \mathfrak{e}(\mathcal{L}/\mathcal{K}) \text{ und } 1 \le j \le \mathfrak{f}(\mathcal{L}/\mathcal{K})\}\right]_{o_{\mathcal{K}}}, \tag{2.1}$$

wobei $\mathfrak{e}(\mathcal{L}/\mathcal{K})$ der Verzweigungsindex und $\mathfrak{f}(\mathcal{L}/\mathcal{K})$ der Trägheitsgrad der Erweiterung $\mathcal{L}/\mathcal{K}$ ist.

Man kann alle $\mathfrak{p}$–adischen Zahlkörper aus algebraischen Zahlkörpern $\mathcal{K}$ gewinnen, indem für ein passendes Primideal $\mathfrak{p} \in \mathbb{P}_{\mathcal{K}}$ die $\mathfrak{p}$–adische Vervollständigung $\mathcal{K}_{\mathfrak{p}}$ gebildet wird. Dieser Zusammenhang ist eine Anwendung von „Krasners Lemma“. Wir führen für einen so dargestellten $\mathfrak{p}$–adischen Zahlkörper die folgenden Bezeichnungen ein:

DEFINITION 2.5. *Seien $\mathcal{L}, \mathcal{K}$ algebraische Zahlkörper mit $\mathcal{K} \subseteq \mathcal{L}$ und $\mathfrak{p} \in \mathbb{P}_{\mathcal{K}}$ gegeben.*

(i) $o_{\mathcal{K}}(\mathfrak{p}) := \mathcal{K} \cap o_{\mathcal{K}_{\mathfrak{p}}}$ *heißt der Ring der $\mathfrak{p}$–ganzen Elemente in $\mathcal{K}$.*
(ii) $o_{\mathcal{L}}(\mathfrak{p}) := \bigcap_{\mathfrak{P} \in \mathbb{P}_{\mathcal{L}} : \mathfrak{P} \mid \mathfrak{p} o_{\mathcal{L}}} o_{\mathcal{L}}(\mathfrak{P})$ *bezeichnet man als den Ring der $\mathfrak{p}$–ganzen Elemente in $\mathcal{L}$. Hierbei sei $o_{\mathcal{L}}(\mathfrak{P})$ entsprechend Punkt (i) gegeben.*

Für den Ring der $\mathfrak{p}$–ganzen Elemente in $\mathcal{L}$ gilt eine zu (2.1) ähnliche Aussage.

Lemma 2.6. *Es sei $\mathcal{L}/\mathcal{K}$ eine Erweiterung algebraischer Zahlkörper und $\mathfrak{p}$ ein Primideal in $o_\mathcal{K}$ mit $\mathfrak{p}o_\mathcal{L} = \mathfrak{P}_1^{\mathfrak{e}_1} \cdot \ldots \cdot \mathfrak{P}_g^{\mathfrak{e}_g}$. Gilt $\mathcal{L} = \mathcal{K}(\delta)$ für eine Nullstelle δ eines normierten irreduziblen Polynoms $f(t) \in o_\mathcal{K}(\mathfrak{p})[t]$ mit*

$$|f'(\delta)|_{\mathfrak{P}_i} = 1 \qquad (1 \leq i \leq g),$$

so ist $1, \delta, \ldots, \delta^{[\mathcal{L}:\mathcal{K}]-1}$ eine $o_\mathcal{K}(\mathfrak{p})$–Basis von $o_\mathcal{L}(\mathfrak{p})$.

Da wir später auch Kummererweiterungen $\mathfrak{p}$–adischer Körper betrachten werden, gehen wir abschließend nochmals kurz auf Kreisteilungskörper im Zusammenhang mit $\mathfrak{p}$–adischen Körpern ein. Hierzu zitieren wir die folgenden beiden Aussagen.

Lemma 2.7. *Sei $p \in \mathbb{P} \setminus \{2\}$ eine Primzahl.*

(i) *$\mathbb{Q}_p$ enthält die $(p-1)$–ten Einheitswurzeln.*
(ii) *$\mathbb{Q}_p$ enthält keine p–te Einheitswurzel.*

Es stellt sich nun die Frage, wie der Körper $\mathbb{Q}_p(\zeta_p)$ aussieht, wenn ζ_p eine primitive p–te Einheitswurzel in $\bar{\mathbb{Q}}_p$ ist. Wir erhalten das folgende Lemma:

Lemma 2.8. *Sei $p \in \mathbb{P}$ beliebig gegeben. Gilt $\mathcal{F} = \mathbb{Q}(\zeta_p)$ und $\mathfrak{p} = (1-\zeta_p)o_\mathcal{F}$, so folgt*

$$\mathcal{F}_\mathfrak{p} = \mathbb{Q}_p(\zeta_p).$$

Die Erweiterung $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ ist total verzweigt mit Verzweigungsindex $p-1$ und Trägheitsgrad 1.

3. Hilbertsche Verzweigungstheorie

Wir wollen nun kurz auf die Hilbertsche Verzweigungstheorie in $\mathfrak{p}$–adischen Zahlkörpern eingehen. Hierfür sei $\mathcal{L}/\mathcal{K}$ eine galoissche Erweiterung $\mathfrak{p}$–adischer Körper mit Galoisgruppe $\mathrm{Gal}\,(\mathcal{L}/\mathcal{K})$.
Gewisse Untergruppen der Galoisgruppe sind von Bedeutung für die Differente. Um diesen Zusammenhang zu untersuchen, führen wir die folgende Definition ein.

Definition 2.9. (i) *Für $i \in \mathbb{N}_0$ definieren wir*

$$\mathfrak{G}_i\,(\mathcal{L}/\mathcal{K}) := \{g \in Gal(\mathcal{L}/\mathcal{K}) \mid g(x) - x \in \mathfrak{p}_\mathcal{L}^{i+1} \quad \forall\, x \in o_\mathcal{L}\}$$

als die i-te Verzweigungsgruppe von $\mathcal{L}/\mathcal{K}$.

(ii) *Wir bezeichnen $\mathfrak{G}_0\,(\mathcal{L}/\mathcal{K})$ als die Trägheitsgruppe von $\mathcal{L}/\mathcal{K}$.*

Die Verzweigungsgruppen bilden eine absteigende Kette von Untergruppen der Galoisgruppe $\mathrm{Gal}\,(\mathcal{L}/\mathcal{K})$:

$$\mathrm{Gal}\,(\mathcal{L}/\mathcal{K}) \supseteq \mathfrak{G}_0\,(\mathcal{L}/\mathcal{K}) \supseteq \ldots \supseteq \mathfrak{G}_n\,(\mathcal{L}/\mathcal{K}) \supseteq \ldots .$$

Hierbei sind nur endlich viele Verzweigungsgruppen nicht trivial und der Fixkörper der Trägheitsgruppe $\mathfrak{G}_0\,(\mathcal{L}/\mathcal{K})$ ist die maximal unverzweigte Erweiterung von $\mathcal{K}$ in $\mathcal{L}$. Das folgende Lemma stellt die Verzweigungsgruppen $\mathfrak{G}_i\,(\mathcal{L}/\mathcal{K})$ für $i \geq 1$ in den Kontext der sogenannten i–ten 1–Einheiten.

LEMMA 2.10. *Sei $i \in \mathbb{N}$. Definiert man die Menge $U_i(\mathcal{L})$ der i–ten 1–Einheiten in $\mathcal{L}$ durch $U_i(\mathcal{L}) := 1 + \mathfrak{p}_{\mathcal{L}}^i$, so gilt*

$$\mathfrak{G}_i\,(\mathcal{L}/\mathcal{K}) = \{g \in Gal\,(\mathcal{L}/\mathcal{K}) \mid g(x)x^{-1} \in \mathcal{U}_i(\mathcal{L}) \quad \forall\, x \in o_{\mathcal{L}} \setminus \{0\}\}.$$

Unsere lokalen Betrachtungen schließen wir mit dem folgenden wichtigen Ergebnis.

SATZ 2.11. *Für die Differente $\mathfrak{D}_{\mathcal{L}/\mathcal{K}}$ von $\mathcal{L}/\mathcal{K}$ gilt $\mathfrak{D}_{\mathcal{L}/\mathcal{K}} = \mathfrak{p}_{\mathcal{L}}^m$, wobei m durch*

$$m = \sum_{i=0}^{t}(|\mathfrak{G}_i\,(\mathcal{L}/\mathcal{K})| - 1) = \sum_{i=0}^{\infty}(|\mathfrak{G}_i\,(\mathcal{L}/\mathcal{K})| - 1)$$

gegeben ist. Hierbei sei t maximal mit $\mathfrak{G}_t\,(\mathcal{L}/\mathcal{K}) \neq \{id\}$ gewählt.

4. Relativerweiterungen

Da wir uns in dieser Arbeit mit Kummererweiterungen algebraischer Zahlkörper beschäftigen, wollen wir einige wichtige Aussagen über Relativerweiterungen im allgemeinen aufführen.
Analog zur lokalen Theorie ist die Differente $\mathfrak{D}_{\mathcal{L}/\mathcal{K}}$ einer Erweiterung $\mathcal{L}/\mathcal{K}$ eine wichtige Invariante. Auch hier ist sie definiert als das inverse Ideal der Codifferente

$$\mathfrak{D}^*_{\mathcal{L}/\mathcal{K}} := \{a \in \mathcal{L} \mid \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}\,(ao_{\mathcal{L}}) \subseteq o_{\mathcal{K}}\}.$$

Als Diskriminante $\mathfrak{d}_{\mathcal{L}/\mathcal{K}}$ der Erweiterung definieren wir dann die Norm der Differente

$$\mathfrak{d}_{\mathcal{L}/\mathcal{K}} = \mathrm{N}_{\mathcal{L}/\mathcal{K}}\left(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}\right).$$

Für Diskriminante und Differente von Relativerweiterungen gelten dann analog zu $\mathfrak{p}$–adischen Körpern die folgenden wichtigen Aussagen.

SATZ 2.12. *Seien $\mathcal{L}$ und $\mathcal{K}$ algebraische Zahlkörper mit $\mathcal{K} \subset \mathcal{L}$.*

(i) *Ein Primideal $\mathfrak{P} \in \mathbb{P}_{\mathcal{L}}$ ist genau dann in $\mathcal{L}/\mathcal{K}$ verzweigt, wenn $\nu_{\mathfrak{P}}\left(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}\right) > 0$ gilt.*

(ii) *Ein Primideal* $\mathfrak{p} \in \mathbb{P}_{\mathcal{K}}$ *ist genau dann in* $\mathcal{L}/\mathcal{K}$ *verzweigt, wenn* $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{L}/\mathcal{K}}\right) > 0$ *gilt.*

(iii) *Ist* $\alpha \in \mathcal{L}$ *mit charakteristischem Polynom* $f_\alpha(t) \in K[t]$ *gegeben, so definieren wir* $d_{\mathcal{L}/\mathcal{K}}(\alpha) := f'_\alpha(\alpha)$. *Dann gilt*

$$\mathfrak{D}_{\mathcal{L}/\mathcal{K}} =< d_{\mathcal{L}/\mathcal{K}}(\alpha) \mid \alpha \in o_{\mathcal{L}} \text{ mit } \mathcal{L} = \mathcal{K}(\alpha) >_{o_{\mathcal{L}}} .$$

(iv) *Für* $\mathfrak{P} \in \mathbb{P}_{\mathcal{L}}$ *ist*

$$\nu_{\mathfrak{P}}\left(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}\right) = \nu_{\mathfrak{P}}\left(\mathfrak{D}_{\mathcal{L}_{\mathfrak{P}}/\mathcal{K}_{\mathfrak{p}}}\right),$$

wobei $\mathfrak{p}$ *durch* $\mathfrak{p} = o_{\mathcal{K}} \cap \mathfrak{P}$ *gegeben ist.*

Da der Ganzheitsring eines algebraischen Zahlkörpers im allgemeinen kein Hauptidealring ist, können wir nicht garantieren, daß für eine Relativerweiterung $\mathcal{L}/\mathcal{K}$ der Ring $o_{\mathcal{L}}$ ein freier $o_{\mathcal{K}}$–Modul ist.

BEISPIEL 2.13. *Setzt man* $\mathcal{L} := \mathbb{Q}(\sqrt{5}, \sqrt{10})$ *und* $\mathcal{K} := \mathbb{Q}(\sqrt{10})$, *so ist* $o_{\mathcal{L}}$ *kein freier* $o_{\mathcal{K}}$*–Modul* [Ed]. *Weitere Beispiele für solche Erweiterungen sind in* [Da] *und* [DaPo94] *zu finden.*

Allgemeiner gilt nach H.B. Mann [Ma, MaHa] sogar der folgende Satz.

SATZ 2.14. *Sei* $\mathcal{K}$ *ein algebraischer Zahlkörper mit Klassenzahl* $h_{\mathcal{K}} \neq 1$. *Dann existiert eine quadratische Erweiterung* $\mathcal{L}$ *von* $\mathcal{K}$, *so daß* $o_{\mathcal{L}}$ *kein freier* $o_{\mathcal{K}}$*–Modul ist.*

Ein notwendiges und hinreichendes Kriterium, wann $o_{\mathcal{L}}$ ein freier $o_{\mathcal{K}}$–Modul ist, wurde von E. Artin in [Ar] gegeben:

SATZ 2.15. *Sei* $\mathcal{L} = \mathcal{K}(\rho)$ *für ein* $\rho \in o_{\mathcal{L}}$. *Für* $\mathcal{L}/\mathcal{K}$ *existiert genau dann eine Relativganzheitsbasis, wenn das Ideal*

$$\mathfrak{a} := \mathfrak{d}_{\mathcal{L}/\mathcal{K}}(\rho)\mathfrak{d}_{\mathcal{L}/\mathcal{K}}^{-1} \in \mathcal{I}_{\mathcal{F}}$$

das Quadrat eines Hauptideals ist.

Sollte die Erweiterung $\mathcal{L}/\mathcal{K}$ keine relative Ganzheitsbasis besitzen, so können wir dennoch eine Aussage über relative Erzeugendensysteme machen [Na].

Satz 2.16. *Sei $\mathcal{L}/\mathcal{K}$ eine Relativerweiterung algebraischer Zahlkörper. Mit $n = [\mathcal{L} : \mathcal{K}]$ existieren dann Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \in \mathcal{I}_\mathcal{K}$ und algebraische Zahlen $\xi_1, \ldots, \xi_n \in o_\mathcal{L}$ mit*

$$o_\mathcal{E} = \mathfrak{a}_1\xi_1 + \ldots + \mathfrak{a}_n\xi_n.$$

Bemerkung 2.17. *In* [BoPo] *wurde ein Algorithmus angegeben, der diese „Normalform“ berechnet.*

KAPITEL 3

Kummererweiterungen

In diesem Kapitel werden Kummererweiterungen algebraischer Zahlkörper untersucht, also Radikalerweiterungen $\mathcal{E}/\mathcal{F}$ vom Grad n mit $\mathbb{Q}(\zeta_n) \subseteq \mathcal{F}$. Unser Ziel ist es, für eine solche Erweiterung ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ zu bestimmen. Bevor wir dies im allgemeinen Fall tun, werden wir Erweiterungen von Primzahlgrad betrachten und das Problem für solche lösen. Hierauf aufbauend können wir dann die allgemeinen Kummererweiterungen behandeln. Wir werden also im weiteren folgender Konstellation unsere Aufmerksamkeit widmen:

$$\begin{tikzcd}
 & \mathcal{E} = \mathcal{F}(\sqrt[p]{\mu}) \arrow[d, dash] & \\
 & \mathcal{F} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathcal{K} \arrow[dr, dash] & & \mathbb{Q}(\zeta_p) \arrow[dl, dash] \\
 & \mathcal{M} = \mathcal{K} \cap \mathbb{Q}(\zeta_p) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Zunächst erwähnen wir jedoch einige interessante Aussagen über Kummererweiterungen. Der folgende Satz ist in [Ha67, La65, CaFr] zu finden.

SATZ 3.1. *Ist $\mathcal{F}$ ein algebraischer Zahlkörper mit $\zeta_n \in \mathcal{F}$, so ist jede zyklische Erweiterung $\mathcal{E}/\mathcal{F}$ vom Grad n von der Form*

$$\mathcal{E} = \mathcal{F}\,(\sqrt[n]{\mu})$$

für ein passendes $\mu \in o_{\mathcal{F}}$. Ist $\mathcal{E}$ eine abelsche Erweiterung vom Grad n über $\mathcal{F}$, so existieren $n_1, \dots, n_k \in \mathbb{N}$ mit $n_1 \cdot \ldots \cdot n_k = n$ und $\mu_1, \dots, \mu_k \in o_{\mathcal{F}}$ mit

$$\mathcal{E} = \mathcal{F}\,(\sqrt[n_1]{\mu_1}, \dots, \sqrt[n_k]{\mu_k})\,.$$

Wir bezeichnen dann $\mathcal{E}/\mathcal{F}$ als verallgemeinerte Kummererweiterung.

Es wird später wichtig sein, den Erzeuger einer Kummererweiterung mit gewissen Bedingungen zu wählen. Dabei wird uns das folgende einfache Lemma leider Schranken setzen [Ko].

Lemma 3.2. *Es sei $\mathcal{F}$ ein algebraischer Zahlkörper mit $\zeta_n \in \mathcal{F}$. Für $\mu, \eta \in \mathcal{F}$ mit $t^n - \mu$ und $t^n - \eta$ irreduzibel in $\mathcal{F}[t]$ gilt:*

$$\mathcal{F}(\sqrt[n]{\mu}) = \mathcal{F}(\sqrt[n]{\eta}) \Longleftrightarrow \exists \alpha \in \mathcal{F}, r \in \mathbb{Z} \text{ mit } \mathrm{ggT}(r,n) = 1 \text{ und } \mu = \eta^r \alpha^n.$$

Im weiteren werden wir spezielle Ergebnisse über das Zerlegungsverhalten von Primidealen in Kummererweiterungen von Primzahlgrad benötigen. Das hier zitierte Ergebnis ist [He] entnommen, aber auch in [Ha26, Ha67] zu finden.

Satz 3.3. *Es seien $p \in \mathbb{P}$ sowie $\mathcal{F}, \mathcal{E}$ algebraische Zahlkörper mit $\zeta_p \in \mathcal{F}$ und*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

für ein $\mu \in o_{\mathcal{F}}$. Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ folgt dann $\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}^p$, falls $\mathrm{ggT}(\nu_{\mathfrak{p}}(\mu), p) = 1$ gilt. Im Fall $\mathrm{ggT}(\nu_{\mathfrak{p}}(\mu), p) = p$ erhalten wir:

(i) *Gilt $\mathfrak{p} \nmid p$, so folgt $\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_p$ falls die Kongruenz $x^p \equiv \mu \mod \mathfrak{p}$ eine Lösung hat, oder $\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}$, falls sie keine Lösung hat.*
(ii) *Gilt $\mathfrak{p} | p$, so folgen mit $\mathfrak{e}_0 := \nu_{\mathfrak{p}}(p) / (p-1)$:*
    (a) *$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_p$, falls die Kongruenz $x^p \equiv \mu \mod \mathfrak{p}^{\mathfrak{e}_0 p+1}$ lösbar ist.*
    (b) *$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}$, falls die Kongruenz $x^p \equiv \mu \mod \mathfrak{p}^m$ für $m = \mathfrak{e}_0 p$, aber nicht für $m = \mathfrak{e}_0 p + 1$ lösbar ist.*
    (c) *$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}^p$, falls die Kongruenz $x^p \equiv \mu \mod \mathfrak{p}^{\mathfrak{e}_0 p}$ nicht lösbar ist.*

Abschließend führen wir noch eine für uns nützliche Sprechweise ein.

Definition 3.4. *Für $n \in \mathbb{N}$ und einen algebraischen Zahlkörper $\mathcal{K}$ bezeichnen wir mit*

$$\mathcal{P}_n(\mathcal{K}) := \{x \in \mathcal{K} \mid \exists y \in \mathcal{K} : y^n = x\}$$

die Menge der n–ten Potenzen in $\mathcal{K}$.

Diese Sprechweise wird deshalb von Vorteil sein, weil wir für einen algebraischen Zahlkörper $\mathcal{K}$ und ein $p \in \mathbb{P}$ durch Wahl eines Elementes μ aus $o_{\mathcal{K}} \setminus \mathcal{P}_p(\mathcal{K})$ eine Körpererweiterung $\mathcal{L} = \mathcal{K}(\sqrt[p]{\mu})$ mit $[\mathcal{L} : \mathcal{K}] = p$ erhalten, ohne dann jedesmal darauf hinweisen zu müssen, daß μ mit $[\mathcal{L} : \mathcal{K}] = p$ gewählt sei.

1. Lokale Kummererweiterungen

Wir werden nun den Ganzheitsring einer $\mathfrak{p}$–adischen Kummererweiterung $\mathcal{E}/\mathcal{F}$ von Primzahlgrad p untersuchen. Für diese Betrachtung ist es notwendig, den Trägheitsgrad $\mathfrak{f}(\mathcal{E}/\mathcal{F})$ und den Verzweigungsindex $\mathfrak{e}(\mathcal{E}/\mathcal{F})$ zu berücksichtigen. Dabei können in unserem speziellen Fall nur die beiden folgenden Fälle auftreten:

(a) Die Erweiterung $\mathcal{E}/\mathcal{F}$ ist verzweigt, d.h. es gelten

$$\mathfrak{e}(\mathcal{E}/\mathcal{F}) = p \text{ und } \mathfrak{f}(\mathcal{E}/\mathcal{F}) = 1.$$

(b) Die Erweiterung $\mathcal{E}/\mathcal{F}$ ist unverzweigt, d.h. es gelten

$$\mathfrak{e}(\mathcal{E}/\mathcal{F}) = 1 \text{ und } \mathfrak{f}(\mathcal{E}/\mathcal{F}) = p.$$

Das Ergebnis dieses Abschnitts wird darin bestehen, daß wir für diese beiden Typen von Erweiterungen eine $o_{\mathcal{F}}$–Basis der ganzen Elemente in $\mathcal{E}$ angeben können. Dazu benötigen wir jedoch noch ein Kriterium, mit dem wir die verzweigten und unverzweigten Erweiterungen voneinander unterscheiden können. Der nächste Satz, den der Leser in [Ha67] findet, wird bei dieser Unterscheidung von Bedeutung sein.

Satz 3.5. *Es sei $\mathcal{F}$ ein $\mathfrak{p}$–adischer Körper mit Restklassencharakteristik p und maximalem Ideal $\mathfrak{p}_{\mathcal{F}}$. Ist $n \in \mathbb{N}$ gegeben, so existiert eine nur von $\mathcal{F}$ und n abhängige Zahl $k \in \mathbb{N}$, so daß für alle $\alpha \in \mathcal{F}$ gilt:*

$$\exists \beta \in \mathcal{F} \,:\, \nu_{\mathfrak{p}_{\mathcal{F}}}(\alpha - \beta^n) \geq k \Longrightarrow \exists \alpha_0 \in \mathcal{F} \,:\, \alpha = \alpha_0^n.$$

Es genügt hierbei

$$k \geq \lfloor \frac{\nu_{\mathfrak{p}_{\mathcal{F}}}(p)}{p-1} \rfloor + 1 + \nu_p(n)\, \nu_{\mathfrak{p}_{\mathcal{F}}}(p)$$

zu wählen.

Wir sind nun in der Lage, für lokale Kummererweiterungen ein notwendiges und hinreichendes Kriterium zu beweisen, das verzweigte von unverzweigten Erweiterungen unterscheidet. Die Aussage dieses Satzes ist an Hecke [He] angelehnt.

Satz 3.6. *Es seien $\mathcal{F}$ und $\mathcal{E}$ $\mathfrak{p}$–adische Körper mit Restklassencharakteristik p und maximalen Idealen $\mathfrak{p}_{\mathcal{F}}$ bzw. $\mathfrak{p}_{\mathcal{E}}$. Ferner enthalte $\mathcal{F}$ die p–ten Einheitswurzeln, und es gelte $[\mathcal{E} : \mathcal{F}] = p$ sowie*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

für ein $\mu \in U_{\mathcal{F}}$. Ist $\mathfrak{e}_0$ der Verzweigungsindex von $\mathcal{F}$ über $\mathbb{Q}_p(\zeta_p)$, so gelten:

(a) *$\mathcal{E}/\mathcal{F}$ ist genau dann unverzweigt, wenn die Kongruenz*

$$\gamma^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{\mathfrak{e}_0 p}$$

lösbar ist.

(b) *$\mathcal{E}/\mathcal{F}$ ist genau dann (total) verzweigt, wenn die Kongruenz*

$$\gamma^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{\mathfrak{e}_0 p}$$

nicht lösbar ist. Ist $\kappa = \max\{0 \leq k < \mathfrak{e}_0 p \mid \exists \gamma \in o_{\mathcal{F}} : \gamma^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^k\}$, so gilt

$$\mathrm{ggT}(p, \kappa) = 1.$$

Beweis. Zunächst bemerken wir, daß die Kongruenz

$$\gamma^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^m \tag{3.1}$$

keine Lösung für $m > \mathfrak{e}_0 p$ haben kann, denn es gilt $\nu_{\mathfrak{p}_{\mathcal{F}}}(p) = \mathfrak{e}_0(p-1)$ und somit

$$\begin{aligned} \lfloor \frac{\nu_{\mathfrak{p}_{\mathcal{F}}}(p)}{p-1} \rfloor + 1 + \nu_p(p)\,\nu_{\mathfrak{p}_{\mathcal{F}}}(p) &= \lfloor \frac{\mathfrak{e}_0(p-1)}{p-1} \rfloor + 1 + \mathfrak{e}_0(p-1) \\ &= \mathfrak{e}_0 + 1 + \mathfrak{e}_0(p-1) \\ &= \mathfrak{e}_0 p + 1. \end{aligned}$$

Daher besitzt (3.1) keine Lösung für $m > \mathfrak{e}_0 p$, da sonst nach Satz 3.5 ein $\mu_0 \in \mathcal{F}$ mit

$$\mu = \mu_0^p$$

existiert. Dies steht im Widerspruch zu $[\mathcal{E} : \mathcal{F}] = p$.
Um die Aussage des Satz zu beweisen, werden wir im weiteren zeigen:

(a) Hat die Kongruenz (3.1) für $m = \mathfrak{e}_0 p$ eine Lösung, so folgt die Unverzweigtheit von $\mathcal{E}/\mathcal{F}$.
(b) Hat die Kongruenz (3.1) für $m = \mathfrak{e}_0 p$ keine Lösung, so ist die Erweiterung verzweigt.

Daraus folgen die behaupteten Äquivalenzen.
Zu (a): Wir zeigen, daß ein primitives Element $\rho \in o_{\mathcal{E}}$ mit $\nu_{\mathfrak{p}_{\mathcal{E}}}\left(d_{\mathcal{E}/\mathcal{F}}(\rho)\right) = 0$ existiert. Dann teilt $\mathfrak{p}_{\mathcal{E}}$ nach Satz 2.3 nicht die Differente $\mathfrak{D}_{\mathcal{E}/\mathcal{F}}$, und es gilt folglich (a).
Es sei $\pi_{\mathcal{F}} \in \mathfrak{p}_{\mathcal{F}} \setminus \mathfrak{p}_{\mathcal{F}}^2$ ein Primelement. Definieren wir

$$\rho := \frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}} \left(\sqrt[p]{\mu} - \gamma \right),$$

so ist ρ eine Nullstelle von $f(t) = \left(t + \frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\gamma\right)^p - \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\right)^p \mu$, denn es gilt

$$\begin{aligned} f(\rho) &= \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\left(\sqrt[p]{\mu} - \gamma\right) + \frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\gamma\right)^p - \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\right)^p \mu \\ &= \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\sqrt[p]{\mu}\right)^p - \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\right)^p \mu = 0. \end{aligned}$$

Da das Polynom $f(t)$ die Darstellung

$$\begin{aligned} f(t) &= \sum_{i=1}^{p} \binom{p}{i} \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\gamma\right)^{p-i} t^i + \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\gamma\right)^p - \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\right)^p \mu \\ &= \sum_{i=1}^{p} \binom{p}{i} \left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\gamma\right)^{p-i} t^i + \frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0 p}}\left(\gamma^p - \mu\right) \end{aligned}$$

besitzt, erhalten wir wegen $\nu_{\mathfrak{p}_{\mathcal{F}}}(p) = \mathfrak{e}_0(p-1)$ nun

$$\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\binom{p}{i}\left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\right)^{p-i}\right) = \nu_{\mathfrak{p}_{\mathcal{F}}}(p) - (p-i)\mathfrak{e}_0 \geq 0$$

für $1 \leq i < p$. Daraus folgt

$$f(t) \in o_{\mathcal{F}}[t],$$

denn nach Voraussetzung ist auch der Absolutkoeffizient von $f(t)$ ganz in $\mathcal{F}$. Weil per Definition $\mathcal{E} = \mathcal{F}(\rho)$ gilt, erhalten wir

$$\begin{aligned} d_{\mathcal{E}/\mathcal{F}}(\rho) &= m_\rho'(\rho) = f'(\rho) = p\left(\rho + \frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\gamma\right)^{p-1} \\ &= p\left(\frac{1}{\pi_{\mathcal{F}}^{\mathfrak{e}_0}}\sqrt[p]{\mu}\right)^{p-1} = \frac{p}{\pi_{\mathcal{F}}^{\mathfrak{e}_0(p-1)}}\sqrt[p]{\mu} \in U_{\mathcal{F}} \end{aligned}$$

für die Differente von ρ. Damit ist $\mathcal{E}/\mathcal{F}$ unverzweigt.

Zu (b): Sei $\kappa = \max\{0 \leq k < \mathfrak{e}_0 p \mid \exists \gamma \in o_{\mathcal{F}} : \gamma^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^k\}$. Dann gilt zunächst $\kappa \geq 1$, denn die Frobeniusabbildung

$$F : o_{\mathcal{F}}/\mathfrak{p}_{\mathcal{F}} \longrightarrow o_{\mathcal{F}}/\mathfrak{p}_{\mathcal{F}} : x \mapsto x^p \tag{3.2}$$

ist ein Automorphismus auf dem endlichen Körper $o_{\mathcal{F}}/\mathfrak{p}_{\mathcal{F}}$. Bevor wir beweisen, daß $\mathcal{E}/\mathcal{F}$ verzweigt ist, wenn (3.1) für $m = \mathfrak{e}_0 p$ nicht lösbar ist, benötigen wir

$$\mathrm{ggT}(\kappa, p) = 1.$$

Dazu beweisen wir: Ist die Kongruenz $x^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{fp}$ für ein $0 < f < \mathfrak{e}_0$ lösbar, so auch die Kongruenz $x^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{fp+1}$. Sei dazu η eine Lösung der Kongruenz

$$x^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{fp}$$

mit $0 < f < \mathfrak{e}_0$. Für $\tilde{\omega} \in o_{\mathcal{F}}$ gilt dann

$$(\eta + \pi_{\mathcal{F}}^f \tilde{\omega})^p \equiv \eta^p + \pi_{\mathcal{F}}^{fp} \tilde{\omega}^p \mod \mathfrak{p}_{\mathcal{F}}^{fp+1}, \tag{3.3}$$

denn aus

$$(\eta + \pi_{\mathcal{F}}^f \tilde{\omega})^p = \sum_{k=0}^{p} \binom{p}{k} \eta^{p-k} \pi_{\mathcal{F}}^{fk} \tilde{\omega}^k$$

erhalten wir wegen

$$\begin{aligned}
\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\binom{p}{k}\eta^{p-k}\pi_{\mathcal{F}}^{fk}\tilde{\omega}^k\right) &= \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\binom{p}{k}\right) + \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\eta^{p-k}\right) + \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\pi_{\mathcal{F}}^{fk}\right) + \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\tilde{\omega}^k\right) \\
&\geq \nu_{\mathfrak{p}_{\mathcal{F}}}(p) + 0 + fk + 0 \\
&= (p-1)\mathfrak{e}_0 + fk \\
&\geq (p-1)(f+1) + fk \geq pf + (p-1)
\end{aligned}$$

für $1 \leq k < p$ die Kongruenz (3.3). Da ferner die Kongruenz $\eta^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{pf}$ die Existenz eines $\alpha \in o_{\mathcal{F}}$ mit

$$\eta^p - \mu = \alpha \pi_{\mathcal{F}}^{pf}$$

impliziert und die Frobeniusabbildung (3.2) ein Automorphismus ist, existieren $\beta, \omega \in o_{\mathcal{F}}$ mit $\alpha + \omega^p = \beta \pi_{\mathcal{F}} \in \mathfrak{p}_{\mathcal{F}}$. Damit erhalten wir

$$\begin{aligned}
(\eta + \pi_{\mathcal{F}}^f \omega)^p - \mu &\equiv \eta^p - \mu + \pi_{\mathcal{F}}^{fp}\omega^p \\
&\equiv \alpha\pi_{\mathcal{F}}^{pf} + \pi_{\mathcal{F}}^{pf}\omega^p \\
&\equiv \pi_{\mathcal{F}}^{pf}(\alpha + \omega^p) \\
&\equiv \pi_{\mathcal{F}}^{pf+1}\beta \equiv 0 \mod \mathfrak{p}_{\mathcal{F}}^{pf+1}.
\end{aligned}$$

Wir haben also $\mathrm{ggT}(\kappa, p) = 1$ gezeigt.
Es bleibt somit $\mathfrak{e}(\mathcal{E}/\mathcal{F}) = p$ zu zeigen. Dazu sei $\kappa = fp + r$ mit $0 \leq f < \mathfrak{e}_0$ und $0 < r < p$. Definieren wir

$$\rho := \frac{1}{\pi_{\mathcal{F}}^f}\left(\sqrt[p]{\mu} - \gamma\right),$$

so teilt $\pi_{\mathcal{F}}$ nicht ρ, denn aus $\pi_{\mathcal{F}} \mid \rho$ folgt $\rho/\pi_{\mathcal{F}} \in o_{\mathcal{E}}$. Somit würde $|\rho/\pi_{\mathcal{F}}|_{\mathcal{E}} \leq 1$ gelten. Aber mit $|\pi_{\mathcal{F}}|_{\mathcal{F}} = \alpha^{-1}$ $(\alpha > 1)$ erhalten wir:

$$\begin{aligned}\left|\frac{\rho}{\pi_{\mathcal{F}}}\right|_{\mathcal{E}} &= \left|\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\frac{\rho}{\pi_{\mathcal{F}}}\right)\right|_{\mathcal{F}}^{1/p} = \left|\frac{\mu-\gamma^p}{\pi_{\mathcal{F}}^{(f+1)p}}\right|_{\mathcal{F}}^{1/p} = \left(\frac{1}{\alpha}\right)^{\frac{1}{p}\left(\nu_{\mathfrak{p}_{\mathcal{F}}}(\mu-\gamma^p)-\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\pi_{\mathcal{F}}^{(f+1)p}\right)\right)} \\ &= \left(\frac{1}{\alpha}\right)^{\frac{1}{p}(fp+r-fp-p)} = \left(\frac{1}{\alpha}\right)^{\frac{1}{p}(r-p)} = \alpha^{\frac{1}{p}(p-r)} > 1.\end{aligned}$$

Daher gilt $\rho/\pi_{\mathcal{F}} \notin o_{\mathcal{E}}$. Ferner gilt $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\rho) = \frac{1}{\pi_{\mathcal{F}}^{fp}}(\mu-\gamma^p)$ und somit $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\rho)\right) = r$. Ist nun $\mathfrak{a}$ das von ρ und $\pi_{\mathcal{F}}$ erzeugte Ideal in $o_{\mathcal{E}}$, so erhalten wir

$$\pi_{\mathcal{F}} o_{\mathcal{E}} \subsetneq \mathfrak{a} \subsetneq o_{\mathcal{E}}, \tag{3.4}$$

denn offenbar gelten $\pi_{\mathcal{F}} o_{\mathcal{E}} \subseteq \mathfrak{a}$ und $\pi_{\mathcal{F}} \nmid \rho$. Damit haben wir $\pi_{\mathcal{F}} o_{\mathcal{E}} \subsetneq \mathfrak{a}$ gezeigt. Andererseits folgt aus $\rho, \pi_{\mathcal{F}} \in o_{\mathcal{E}}$ natürlich $\mathfrak{a} \subseteq o_{\mathcal{E}}$. Da $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\rho)\right) = r > 0$ und $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\pi_{\mathcal{F}})\right) > 0$ gelten, erhalten wir

$$\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha)\right) > 0 \quad \forall \alpha \in \mathfrak{a}.$$

Also gilt $U_{\mathcal{F}} \nsubseteq \mathfrak{a}$, und wir haben $\mathfrak{a} \neq o_{\mathcal{E}}$ bewiesen.
Wir haben damit gezeigt, daß $\pi_{\mathcal{F}} o_{\mathcal{E}}$ kein Primideal in $o_{\mathcal{E}}$ sein kann, denn es gilt (3.4). Damit ist die Erweiterung $\mathcal{E}/\mathcal{F}$ verzweigt. □

Lemma 3.7. *Es seien $\mathcal{F}, \mathcal{E}$ $\mathfrak{p}$–adische Körper mit maximalen Idealen $\mathfrak{p}_{\mathcal{F}}$ bzw. $\mathfrak{p}_{\mathcal{E}}$. Ferner enthalte $\mathcal{F}$ die p–ten Einheitswurzeln, und es gelte $[\mathcal{E}:\mathcal{F}] = p$ sowie*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

für ein $\mu \in \mathfrak{p}_{\mathcal{F}} \setminus \mathfrak{p}_{\mathcal{F}}^2$. Dann ist die Erweiterung $\mathcal{E}/\mathcal{F}$ verzweigt.

Beweis. Aus $\nu_{\mathfrak{p}_{\mathcal{F}}}(\mu) = 1$ folgt $\mathfrak{e}(\mathcal{E}/\mathcal{F}) = \nu_{\mathfrak{p}_{\mathcal{E}}}(\mu) = p\nu_{\mathfrak{p}_{\mathcal{E}}}\left(\sqrt[p]{\mu}\right) \geq p > 1$. □

Lemma 3.8. *Es seien $\mathcal{F} \subseteq \mathcal{E}$ $\mathfrak{p}$–adische Zahlkörper mit $[\mathcal{E}:\mathcal{F}] = n$ und Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$. Ist dann $\{\omega_1, \ldots, \omega_n\} \subseteq o_{\mathcal{E}}$ eine Basis von $\mathcal{E}/\mathcal{F}$ mit*

$$\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n)\right) = \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right),$$

so wird durch $\omega_1, \ldots, \omega_n$ eine $o_{\mathcal{F}}$–Basis von $o_{\mathcal{E}}$ gegeben.

Beweis. Sei $\eta_1, \ldots, \eta_n$ eine Ganzheitsbasis von $\mathcal{E}/\mathcal{F}$. Dann existiert wegen $\{\omega_1, \ldots, \omega_n\} \subset o_{\mathcal{E}}$ eine Matrix $M \in o_{\mathcal{F}}^{n\times n}$ mit

$$(\omega_1, \ldots, \omega_n) = (\eta_1, \ldots, \eta_n)M.$$

Für die Diskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ ergibt sich damit

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\eta_1, \dots, \eta_n) = \det(M)^2 \mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\omega_1, \dots, \omega_n).$$

Da nach Voraussetzung $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\omega_1, \dots, \omega_n)\right) = \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\eta_1, \dots, \eta_n)\right)$ gilt, folgt

$$\det(M)^2 \in U_{\mathcal{F}}$$

und somit $\det(M) \in U_{\mathcal{F}}$. Also ist $M \in GL(n, o_{\mathcal{F}})$, und $\omega_1, \dots, \omega_n$ ist eine Ganzheitsbasis von $\mathcal{E}/\mathcal{F}$. □

BEMERKUNG 3.9. *Wenn wir eine Erweiterung $\mathcal{E}/\mathcal{F}$ mit $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ betrachten, so können wir immer annehmen, daß $\mu \in o_{\mathcal{F}} \setminus \mathfrak{p}_{\mathcal{F}}^2$ gilt, wenn $\mathfrak{p}_{\mathcal{F}}$ das maximale Ideal von $o_{\mathcal{F}}$ ist.*
Es sei $\mu = \alpha\pi_{\mathcal{F}}^n$ mit $\alpha \in U_{\mathcal{F}}$ und $n \in \mathbb{Z}$. Sei nun $k \in \mathbb{Z}$ so gewählt, daß $0 \leq m < p$ für $m := n + kp$ gilt. Dann gilt

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\eta})$$

mit $\eta = \mu\pi_{\mathcal{F}}^{kp}$.
Für $\nu_{\mathfrak{p}_{\mathcal{F}}}(\eta) = m = 0$ ist nichts weiter zu zeigen. Sonst gilt $\mathrm{ggT}(p, m) = 1$, und es seien daher $a, b \in \mathbb{Z}$ mit $am + bp = 1$ gegeben. Setzen wir $\tilde{\mu} := \eta^a\pi_{\mathcal{F}}^{bp}$, so gelten $\nu_{\mathfrak{p}_{\mathcal{F}}}(\tilde{\mu}) = am + bp = 1$ und $\mathcal{F}(\sqrt[p]{\tilde{\mu}}) = \mathcal{E}$.

SATZ 3.10. *Es seien $\mathcal{F}, \mathcal{E}$ $\mathfrak{p}$–adische Körper mit maximalen Idealen $\mathfrak{p}_{\mathcal{F}}$ bzw. $\mathfrak{p}_{\mathcal{E}}$. Ferner enthalte $\mathcal{F}$ die p–ten Einheitswurzeln, und es gelten*

(a) $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ *für ein* $\mu \in o_{\mathcal{F}} \setminus \mathfrak{p}_{\mathcal{F}}^2$,
(b) $\mathfrak{e}(\mathcal{E}/\mathcal{F}) = p$,
(c) $[\mathcal{E} : \mathcal{F}] = p$.

Dann erhalten wir mit $\pi_{\mathcal{F}} \in \mathfrak{p}_{\mathcal{F}} \setminus \mathfrak{p}_{\mathcal{F}}^2$:

(i) $\pi_{\mathcal{F}} \nmid p\mu$ *ist nicht möglich.*
(ii) *Gilt* $\pi_{\mathcal{F}} \mid \mu$, *so folgt*

$$o_{\mathcal{E}} = \left[1, \sqrt[p]{\mu}, \dots, \sqrt[p]{\mu}^{p-1}\right]_{o_{\mathcal{F}}}.$$

Für die Diskriminante gilt $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = (p-1) + p\nu_{\mathfrak{p}_{\mathcal{F}}}(p)$.

(iii) *Gelten* $\pi_{\mathcal{F}} \mid p$ *und* $\pi_{\mathcal{F}} \nmid \mu$, *so sei*

$$\kappa = \max\{0 \leq k < \mathfrak{e}_0 p \mid \exists \gamma \in o_{\mathcal{F}} : \gamma^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^k\}.$$

Dann gilt (vgl. Satz 3.6) $\mathrm{ggT}(\kappa, p) = 1$, *und es existieren* $r, s \in \mathbb{Z}^{\geq 0}$ *mit* $r\kappa - sp = 1$. *Ist* γ *eine Lösung der Kongruenz* $x^p \equiv \mu \mod \mathfrak{p}_{\mathcal{F}}^{\kappa}$, *so gilt mit*

$$\rho := \frac{\left(\gamma - \sqrt[p]{\mu}\right)^r}{\pi_{\mathcal{F}}^s}$$

dann

$$o_{\mathcal{E}} = \left[1, \rho, \dots, \rho^{p-1}\right]_{o_{\mathcal{F}}}.$$

Ist $\mathfrak{e}_0$ *der Verzweigungsindex von* $\mathcal{F}$ *über* $\mathbb{Q}_p(\zeta_p)$, *so gilt für die Diskriminante* $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = (p-1)(\mathfrak{e}_0 p - \kappa + 1)$.

Beweis. Zu (i): Es existiert ein $\alpha \in o_{\mathcal{F}}$ mit $\alpha^2 \mathfrak{d}_{\mathcal{E}/\mathcal{F}} = \mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\sqrt[p]{\mu})$. Aus $\pi_{\mathcal{F}} \nmid p\mu$ und $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\sqrt[p]{\mu}) = p^p \mu^{p-1} \in U_{\mathcal{F}}$ folgt $\alpha \in U_{\mathcal{F}}$, und wir erhalten

$$0 \leq \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) \leq \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\sqrt[p]{\mu})\right) = 0.$$

Aus Satz 2.4 folgt nun die Behauptung.
Zu(ii): Gilt $\pi_{\mathcal{F}} \mid \mu$, so folgt aus den Voraussetzungen des Satzes $\nu_{\mathfrak{p}_{\mathcal{F}}}(\mu) = 1$. Daher gilt $\left|\sqrt[p]{\mu}\right|_{\mathcal{E}} = \max\{|x|_{\mathcal{E}} \mid x \in \mathfrak{p}_{\mathcal{E}}\}$, was

$$\sqrt[p]{\mu} \in \mathfrak{p}_{\mathcal{E}} \setminus \mathfrak{p}_{\mathcal{E}}^2.$$

impiziert. Aus der lokalen Theorie folgt jetzt, daß $1, \sqrt[p]{\mu}, \dots, \sqrt[p]{\mu}^{p-1}$ eine $o_{\mathcal{F}}$–Basis von $o_{\mathcal{E}}$ ist. Der Zusatz über die Bewertung der Diskriminante ist evident.
Zu (iii): Es gelten $\pi_{\mathcal{F}} \mid p$ und $\pi_{\mathcal{F}} \nmid \mu$. Ferner seien $\kappa, r, s, \gamma, \rho$ wie in der Satzaussage gegeben. Wegen $\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\gamma - \sqrt[p]{\mu}\right) = \gamma^p - \mu$ gilt dann

$$\begin{aligned} \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\rho) &= \mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\pi_{\mathcal{F}}^{-s}\right) \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\gamma - \sqrt[p]{\mu})^r \\ &= \pi_{\mathcal{F}}^{-sp}(\gamma^p - \mu)^r. \end{aligned}$$

Mit $|\pi_{\mathcal{E}}|_{\mathcal{E}} = \beta^{-1}$ impliziert dies

$$\begin{aligned} |\rho|_{\mathcal{E}} &= \left|\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\rho)\right|_{\mathcal{F}}^{1/p} = \left|\pi_{\mathcal{F}}^{-sp}(\gamma^p - \mu)^r\right|_{\mathcal{F}}^{1/p} \\ &= \left(\left(\frac{1}{\beta^p}\right)^{\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\pi_{\mathcal{F}}^{-sp}(\gamma^p-\mu)^r\right)}\right)^{1/p} = \left(\left(\frac{1}{\beta^p}\right)^{-sp+r\kappa}\right)^{1/p} = \frac{1}{\beta}. \end{aligned}$$

Somit folgt $\rho \in \mathfrak{p}_{\mathcal{E}} \setminus \mathfrak{p}_{\mathcal{E}}^2$, und $1, \rho, \dots, \rho^{p-1}$ ist eine $o_{\mathcal{F}}$–Basis von $o_{\mathcal{E}}$. Um den Zusatz über die Bewertung der Diskriminante zu beweisen, benötigen wir Resultate der Hilbertschen Verzweigungstheorie für lokale Körper. Aus Satz 2.11 folgt

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}} = \mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\mathfrak{D}_{\mathcal{E}/\mathcal{F}}\right) = \mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\mathfrak{p}_{\mathcal{E}}^a\right) = \mathfrak{p}_{\mathcal{F}}^a,$$

wobei a durch

$$a = \sum_{i=0}^{\infty} \left(\left| \mathfrak{G}_i \left(\mathcal{E}/\mathcal{F} \right) \right| - 1 \right)$$

gegeben ist. Da wir eine zyklische Erweiterung von Primzahlgrad betrachten, gilt $\mathfrak{G}_i\left(\mathcal{E}/\mathcal{F}\right) \in \{\{id\}, \mathrm{Gal}\left(\mathcal{E}/\mathcal{F}\right)\}$ für alle $i \in \mathbb{N}_0$. Wir werden nun $a = (p\mathfrak{e}_0 - \kappa + 1)(p-1)$ zeigen, indem wir $\mathfrak{G}_i\left(\mathcal{E}/\mathcal{F}\right) = \{id\}$ für $i \geq (p\mathfrak{e}_0 - \kappa + 1)$ und $\mathfrak{G}_{p\mathfrak{e}_0 - \kappa}\left(\mathcal{E}/\mathcal{F}\right) \neq \{id\}$ nachweisen.
Zunächst gilt wegen $\mathfrak{e}(\mathcal{E}/\mathcal{F}) = p$ und $\mathfrak{f}(\mathcal{E}/\mathcal{F}) = 1$ natürlich

$$\nu_{\mathfrak{p}_{\mathcal{E}}}\left(\eta\right) = \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\eta\right)\right) \quad \forall \eta \in \mathcal{E}.$$

Mit $< \sigma >= \mathrm{Gal}\left(\mathcal{E}/\mathcal{F}\right)$ ergibt sich daraus

$$\begin{aligned} \frac{\sigma(\rho)}{\rho} &= \frac{\left(\gamma - \zeta_p \sqrt[p]{\mu}\right)^r}{\pi_{\mathcal{F}}^s} \frac{\pi_{\mathcal{F}}^s}{\left(\gamma - \sqrt[p]{\mu}\right)^r} \\ &= \left(\frac{\gamma - \zeta_p \sqrt[p]{\mu}}{\gamma - \sqrt[p]{\mu}}\right)^r = \left(1 + \frac{(1-\zeta_p)}{\gamma - \sqrt[p]{\mu}} \sqrt[p]{\mu}\right)^r. \end{aligned}$$

Wir untersuchen nun $\eta := \frac{(1-\zeta_p)}{\gamma - \sqrt[p]{\mu}} \sqrt[p]{\mu}$ näher. Es gilt $\nu_{\mathfrak{p}_{\mathcal{E}}}\left(1 - \zeta_p\right) = \mathfrak{e}_0 p$, denn $1 - \zeta_p$ ist in $\mathbb{Q}_p(\zeta_p)$ ein Primelement, und

$$\begin{aligned} \nu_{\mathfrak{p}_{\mathcal{E}}}\left(\gamma - \sqrt[p]{\mu}\right) &= \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\gamma - \sqrt[p]{\mu}\right)\right) \\ &= \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\gamma^p - \mu\right) = \kappa. \end{aligned}$$

Da nach Voraussetzung schließlich $\nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mu\right) = 0$ gilt, erhalten wir

$$\nu_{\mathfrak{p}_{\mathcal{E}}}\left(\eta\right) = \mathfrak{e}_0 p - \kappa.$$

Wegen

$$(1+\eta)^r = 1 + \sum_{k=1}^{r} \binom{r}{k} \eta^k = 1 + r\eta + \eta'$$

gilt zunächst $(1+\eta)^r = 1 + \tilde{\eta}$ mit $\tilde{\eta} \in \mathfrak{p}_{\mathcal{E}}^{\mathfrak{e}_0 p - \kappa}$. Aus $\mathrm{ggT}(r,p) = 1$ folgt aber sogar $\tilde{\eta} \notin \mathfrak{p}_{\mathcal{E}}^{\mathfrak{e}_0 p - \kappa + 1}$. Also gelten nach Lemma 2.10

(1) $\mathfrak{G}_{\mathfrak{e}_0 p - \kappa}\left(\mathcal{E}/\mathcal{F}\right) = \mathrm{Gal}\left(\mathcal{E}/\mathcal{F}\right)$,
(2) $\mathfrak{G}_{\mathfrak{e}_0 p - \kappa + 1}\left(\mathcal{E}/\mathcal{F}\right) = \{id\}$.

Wir erhalten somit $\mathfrak{D}_{\mathcal{E}/\mathcal{F}} = \mathfrak{p}_{\mathcal{E}}^a$, wobei a durch

$$a = \sum_{i=0}^{\mathfrak{e}_0 p - \kappa} \left(\left| \mathfrak{G}_i\left(\mathcal{E}/\mathcal{F}\right) \right| - 1 \right) = (\mathfrak{e}_0 p - \kappa + 1)(p-1)$$

gegeben ist. Daraus folgt

$$\begin{aligned}\nu_{\mathfrak{p}_\mathcal{F}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) &= \nu_{\mathfrak{p}_\mathcal{F}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\mathfrak{D}_{\mathcal{E}/\mathcal{F}}\right)\right) = \nu_{\mathfrak{p}_\mathcal{F}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\mathfrak{p}_\mathcal{E}\right)^a\right)\\ &= \nu_{\mathfrak{p}_\mathcal{F}}\left(\mathfrak{p}_\mathcal{F}^a\right) = a = (\mathfrak{e}_0 p - \kappa + 1)(p-1),\end{aligned}$$

und der Satz ist vollständig bewiesen. □

Zum Abschluß dieses Kapitels werden wir eine zu dem letzten Satz analoge Aussage für total unverzweigte lokale Erweiterungen beweisen.

Satz 3.11. *Es seien $\mathcal{F}, \mathcal{E}$ $\mathfrak{p}$–adische Körper mit maximalen Idealen $\mathfrak{p}_\mathcal{F}$ bzw. $\mathfrak{p}_\mathcal{E}$. Ferner enthalte $\mathcal{F}$ die p–ten Einheitswurzeln und es gelten $[\mathcal{E} : \mathcal{F}] = p$ sowie*

(a) *$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ für ein $\mu \in o_\mathcal{F} \setminus \mathfrak{p}_\mathcal{F}^2$,*
(b) *$\mathfrak{f}(\mathcal{E}/\mathcal{F}) = p$.*

Dann erhalten wir mit $\pi_\mathcal{F} \in \mathfrak{p}_\mathcal{F} \setminus \mathfrak{p}_\mathcal{F}^2$:

(i) *$\pi_\mathcal{F} \mid \mu$ ist nicht möglich.*
(ii) *Gilt $\pi_\mathcal{F} \nmid p\mu$, so folgt*

$$o_\mathcal{E} = \left[1, \sqrt[p]{\mu}, \ldots, \sqrt[p]{\mu}^{p-1}\right]_{o_\mathcal{F}}.$$

(iii) *Gelten $\pi_\mathcal{F} \mid p$ und $\pi_\mathcal{F} \nmid \mu$, so sei $\gamma \in o_\mathcal{F}$ mit $\gamma^p \equiv \mu \mod \mathfrak{p}_\mathcal{F}^{p\mathfrak{e}_0}$ gegeben. Hierbei sei $\mathfrak{e}_0$ der Verzweigungsindex von $\mathcal{F}$ in $\mathbb{Q}_p(\zeta_p)$. Definiert man*

$$\rho := \frac{\gamma - \sqrt[p]{\mu}}{\pi_\mathcal{F}^{\mathfrak{e}_0}},$$

so gilt

$$o_\mathcal{E} = \left[1, \rho, \ldots, \rho^{p-1}\right]_{o_\mathcal{F}}.$$

Beweis. In jedem Fall gilt für die Erweiterung $\mathcal{E}/\mathcal{F}$ unter den Voraussetzungen dieses Satzes $\mathfrak{d}_{\mathcal{E}/\mathcal{F}} = o_\mathcal{F}$, denn $\mathcal{E}/\mathcal{F}$ ist unverzweigt.
Zu (i): Gilt $\pi_\mathcal{F} \mid \mu$, so folgt aus den Voraussetzungen $\nu_{\mathfrak{p}_\mathcal{F}}(\mu) = 1$. Dann ist die Erweiterung aber nach Lemma 3.7 verzweigt.
Zu (ii): Wegen $\pi_\mathcal{F} \nmid p\mu$ gilt $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\sqrt[p]{\mu}) = p^p\mu^{p-1}o_\mathcal{F} = o_\mathcal{F}$. Daher folgt aus 3.8 die Behauptung.
Zu (iii): Da $\mathcal{E}/\mathcal{F}$ unverzweigt ist, folgt die Existenz von γ aus Satz 3.6. Aus

$$\nu_{\mathfrak{p}_\mathcal{E}}(\rho) = p\mathfrak{e}_0 - \mathfrak{e}_0\nu_{\mathfrak{p}_\mathcal{E}}(\pi_\mathcal{F}) = (p-1)\mathfrak{e}_0 > 0$$

folgt daher $\rho \in o_{\mathcal{E}}$. Für die Diskriminante von $1, \rho, \dots, \rho^{p-1}$ gilt

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\rho) = p^p \mu^{p-1} \det(M_\rho)^2 o_{\mathcal{F}}$$

mit $(1, \rho, \dots, \rho^{p-1}) = \left(1, \sqrt[p]{\mu}, \dots, \sqrt[p]{\mu}^{p-1}\right) M_\rho$ $(M_\rho \in \mathcal{F}^{p\times p})$. Für $\det(M_\rho)$ ergibt sich aus

$$M_\rho = \begin{pmatrix} 1 & \gamma/\pi_{\mathcal{F}}^{\mathfrak{e}_0} & \gamma^2/\pi_{\mathcal{F}}^{2\mathfrak{e}_0} & \cdots & * \\ & -1/\pi_{\mathcal{F}}^{\mathfrak{e}_0} & -2\gamma/\pi_{\mathcal{F}}^{2\mathfrak{e}_0} & \cdots & * \\ & & 1/\pi_{\mathcal{F}}^{2\mathfrak{e}_0} & \cdots & * \\ & & & \ddots & * \\ & & & & * \\ & & & & \pm 1/\pi_{\mathcal{F}}^{(p-1)\mathfrak{e}_0} \end{pmatrix}$$

offenbar

$$\det(M_\rho) = (-1)^{\lfloor \frac{p}{2} \rfloor} \pi_{\mathcal{F}}^{-(\sum_{i=1}^{p-1} i) e_0} = (-1)^{\lfloor \frac{p}{2} \rfloor} \pi_{\mathcal{F}}^{-\frac{\mathfrak{e}_0(p-1)p}{2}}.$$

Für die Diskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\rho)$ impliziert dies

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\rho) = p^p \mu^{p-1} \left(\pi_{\mathcal{F}}^{-\frac{\mathfrak{e}_0(p-1)p}{2}}\right)^2 o_{\mathcal{F}} = p^p \pi_{\mathcal{F}}^{-\mathfrak{e}_0(p-1)p} o_{\mathcal{F}},$$

und wir erhalten

$$\begin{aligned} \nu_{\mathfrak{p}_{\mathcal{F}}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\rho)\right) &= p\nu_{\mathfrak{p}_{\mathcal{F}}}(p) - \mathfrak{e}_0(p-1)p \\ &= \mathfrak{e}_0(p-1)p - \mathfrak{e}_0(p-1)p = 0. \end{aligned}$$

Also ist $1, \rho, \dots, \rho^{p-1}$ nach Lemma 3.8 eine $o_{\mathcal{F}}$–Basis von $o_{\mathcal{E}}$. □

BEMERKUNG 3.12. *Die Sätze* 3.10 *und* 3.11 *sind eine Verallgemeinerung eines Ergebnisses von Fröhlich* [Fr, Na]*, der das entsprechende Problem einer Ganzheitsbasis für quadratische Erweiterungen $\mathfrak{p}$–adischer Zahlkörper gelöst hat.*

2. Semilokale Ganzheitsringe

Nachdem wir im letzten Abschnitt die lokalen Kummererweiterungen untersucht und für solche den Ring der ganzen Elemente vollständig beschrieben haben, wenden wir uns nun den $\mathfrak{p}$–ganzen Elementen in Kummererweiterungen zu.
Hierbei werden wir zum einen die letzten Ergebnisse aufgreifen und zeigen, daß diese auch für den semilokalen Fall von Nutzen sind. Zum anderen werden wir für total zerlegte Primideale die $\mathfrak{p}$-ganzen Elemente gesondert untersuchen.
Da wir uns im weiteren mit Kummererweiterungen algebraischer Zahlkörper beschäftigen, wird es von Bedeutung sein, für eine Erweiterung $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ an den Erzeuger gewisse Bedingungen zu stellen. Wie wir sehen werden, können diese Bedingungen immer erfüllt werden. Die folgende Bemerkung liefert hierfür die Grundlage.

Bemerkung 3.13. *Seien $\mathcal{E}, \mathcal{F}$ algebraische Zahlkörper mit $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ für ein $\mu \in o_{\mathcal{F}} \setminus \mathcal{P}_p(\mathcal{F})$ und ein $p \in \mathbb{P}$. Ist $\Pi \subseteq \mathbb{P}_{\mathcal{F}}$ endlich, so existiert ein $\mu^* \in o_{\mathcal{F}}$ mit*

(i) $\mathcal{F}\left(\sqrt[p]{\mu}\right) = \mathcal{F}\left(\sqrt[p]{\mu^*}\right)$,
(ii) $\nu_{\mathfrak{p}}(\mu^*) \in \{0, \ldots, p-1\}$ *für alle* $\mathfrak{p} \in \Pi$.

Die Existenz eines solchen Elementes weisen wir konstruktiv nach. Dazu seien für $\mathfrak{p} \in \Pi$ ein $\pi_{\mathfrak{p}} \in o_{\mathcal{F}}$ mit

(iii) $\pi_{\mathfrak{p}} \in \mathfrak{p} \setminus \mathfrak{p}^2$,
(iv) $\pi_{\mathfrak{p}} \notin \mathfrak{q}$ *für alle* $\mathfrak{q} \in \Pi \setminus \{\mathfrak{p}\}$

und $\alpha_{\mathfrak{p}} \in o_{\mathcal{F}}$ mit

(v) $\alpha_{\mathfrak{p}} \notin \mathfrak{p}$,
(vi) $\nu_{\mathfrak{q}}(\alpha_{\mathfrak{p}}) = \nu_{\mathfrak{q}}(\pi_{\mathfrak{p}})$ *für alle* $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}} \setminus \{\mathfrak{p}\}$ *mit* $\nu_{\mathfrak{q}}(\pi_{\mathfrak{p}}) > 0$

gegeben. Ist außerdem für $\mathfrak{p} \in \Pi$ ein $a_{\mathfrak{p}} \in \mathbb{Z}^{\geq 0}$ mit $\nu_{\mathfrak{p}}(\mu) - a_{\mathfrak{p}} p \in \{0, \ldots, p-1\}$ gegeben, so folgt die Behauptung mit

$$\mu^* := \mu \prod_{\mathfrak{p} \in \Pi} \left(\frac{\alpha_{\mathfrak{p}}}{\pi_{\mathfrak{p}}}\right)^{a_{\mathfrak{p}} p}.$$

Dies ist das bestmögliche Ergebnis, das wir im allgemeinen für den Erzeuger einer Kummererweiterung erzielen können, wenn wir für eine endliche Menge von Primidealen die Bewertungen des Erzeugers gleichmäßig beschränken wollen. Speziell können wir

$$\nu_{\mathfrak{p}}(\mu) \in \{0,1\} \qquad \forall \mathfrak{p} \in \Pi \tag{3.5}$$

nicht sicherstellen. Um dies einzusehen, betrachten wir o.B.d.A. den Fall $\Pi = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ und $\nu_{\mathfrak{p}_i}(\mu) = r_i$ $(i = 1,2)$ mit $0 < r_1 < r_2 < p$.
Angenommen, es gäbe einen Erzeuger $\mu^* \in \mathcal{F}$ von $\mathcal{E}$, der (3.5) erfüllt. Nach Lemma 3.2 gilt dann

$$\mu^* = \mu^n \alpha^p$$

für ein passendes $\alpha \in \mathcal{F}$ und ein $n \in \mathbb{Z} \setminus p\mathbb{Z}$. Wegen $0 < r_1, r_2 < p$ gilt $\nu_{\mathfrak{p}_i}(\mu^*) = 1$ $(i = 1,2)$, und wir erhalten somit

$$1 = \nu_{\mathfrak{p}_i}(\mu^*) = r_i n + p\nu_{\mathfrak{p}_i}(\alpha) \qquad (i = 1,2).$$

Diese beiden Gleichungen sind aber wegen $0 < r_1 < r_2 < p$ für ein festes $n \in \mathbb{Z}$, welches zu p teilerfremd ist, nicht lösbar.
Wir können also für eine endliche Menge $\Pi \in \mathbb{P}_{\mathcal{F}}$ von Primidealen genau dann

$$\nu_{\mathfrak{p}}(\mu) \in \{0,1\} \qquad \forall \mathfrak{p} \in \Pi$$

sicherstellen, wenn ein $r \in \{0, \ldots, p-1\}$ existiert, so daß für $\mathfrak{p} \in \Pi$ entweder $\nu_{\mathfrak{p}}(\mu) \equiv 0 \mod p$ oder $\nu_{\mathfrak{p}}(\mu) \equiv r \mod p$ gilt.

Untersuchen wir also im weiteren eine Kummererweiterung $\mathcal{E}/\mathcal{F}$ von Primzahlgrad p mit $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$, so setzen wir

$$\nu_{\mathfrak{p}}(\mu) \in \{0, \ldots, p-1\} \qquad \forall \mathfrak{p} \in \{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid \nu_{\mathfrak{p}}(p) > 0\}$$

für den Erzeuger μ voraus, ohne dies nochmals explizit zu erwähnen.

Betrachten wir nun die $\mathfrak{p}$-ganzen Elemente für total zerlegte Primideale $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$.

Lemma 3.14. *Es seien $p \in \mathbb{P}$ sowie $\mathcal{E}, \mathcal{F}$ algebraische Zahlkörper mit $\zeta_p \in \mathcal{F}$ und*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

für ein $\mu \in o_{\mathcal{F}} \setminus \mathcal{P}_p(\mathcal{F})$. Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ gelte $\mathfrak{p}o_{\mathcal{E}} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_p$, und für $\pi \in o_{\mathcal{F}}$ gelte $\nu_{\mathfrak{p}}(\pi) = 1$. Dann erhalten wir

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \rho, \ldots, \rho^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})},$$

wobei ρ wie folgt gewählt werden kann:

(i) *Gelten* $\mathfrak{p} \mid \mu$ *und* $\mathfrak{p} \nmid p$, *so leistet*

$$\rho = \frac{1}{\pi^\kappa}\sqrt[p]{\mu}$$

mit $\kappa := \frac{\nu_\mathfrak{p}(\mu)}{p} \in \mathbb{N}$ *das Gewünschte.*

(ii) *Gelten* $\mathfrak{p} \nmid \mu$ *und* $\mathfrak{p} \mid p$, *so sei* $\mathfrak{e}_0$ *durch* $\nu_\mathfrak{p}(p) = \mathfrak{e}_0(p-1)$ *definiert. Dann existiert ein* $\gamma \in o_\mathcal{F}$ *mit*

$$\gamma^p \equiv \mu \mod \mathfrak{p}^{p\mathfrak{e}_0}.$$

Die Aussage folgt mit

$$\rho = \frac{\gamma - \sqrt[p]{\mu}}{\pi^{\mathfrak{e}_0}}.$$

(iii) *Gilt* $\mathfrak{p} \nmid p\mu$, *so folgt mit* $\rho = \sqrt[p]{\mu}$ *die Behauptung.*

Beweis. Zunächst gilt wegen $\mathfrak{p}o_\mathcal{E} \neq \mathfrak{P}^p$ nach Satz 3.10 $\mathrm{ggT}(\nu_\mathfrak{p}(\mu), p) \neq 1$. Daher kann der Fall $\mathfrak{p} \mid \mu$ und $\mathfrak{p} \mid p$ nicht eintreten, denn dann gilt $\nu_\mathfrak{p}(\mu) \in \{1, \dots, p-1\}$ und somit $\mathrm{ggT}(\nu_\mathfrak{p}(\mu), p) = 1$. Nach Satz 3.3 folgt daraus $\mathfrak{p}o_\mathcal{E} = \mathfrak{P}^p$. Aus $\mathfrak{p}o_\mathcal{E} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_p$ und der Definition der Norm folgen ferner:

(a) Gilt $\nu_{\mathfrak{P}_i}(\alpha) = c$ $(1 \le i \le p)$ für $\alpha \in \mathcal{E}$, so folgt $\nu_{\mathfrak{P}_i}(\alpha) = \frac{1}{p}\nu_\mathfrak{p}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha)\right)$ $(1 \le i \le p)$.

(b) Gilt $\nu_{\mathfrak{P}_i}(\alpha) \neq 0$ für ein i und $\nu_{\mathfrak{P}_j}(\alpha) = 0$ $(1 \le j \le p, j \neq i)$ für $\alpha \in \mathcal{E}$, so folgt $\nu_{\mathfrak{P}_i}(\alpha) = \nu_\mathfrak{p}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha)\right)$.

Mittels 2.6 beweisen wir jetzt die Behauptungen.
Zu (i): Nach Satz 3.10 gilt $\kappa \in \mathbb{N}$. Für das Minimalpolynom von ρ folgt daher

$$m_\rho(t) = t^p - \frac{1}{\pi^{p\kappa}}\mu = t^p - \frac{1}{\pi^{\nu_\mathfrak{p}(\mu)}}\mu \in o_\mathcal{F}(\mathfrak{p})[t].$$

Für $1 \le i \le p$ gilt

$$\begin{aligned}
\nu_{\mathfrak{P}_i}\left(m'_\rho(\rho)\right) &= \nu_{\mathfrak{P}_i}\left(p\rho^{p-1}\right) = \nu_{\mathfrak{P}_i}(p) + (p-1)\nu_{\mathfrak{P}_i}(\sqrt[p]{\mu}/\pi^\kappa) \\
&= 0 + (p-1)\left(\nu_\mathfrak{p}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\sqrt[p]{\mu})\right) - \nu_\mathfrak{p}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\pi^\kappa)\right)\right) \\
&= (p-1)\left(\nu_\mathfrak{p}(\mu) - \kappa\nu_\mathfrak{p}(\mu^p)\right) \\
&= (p-1)\left(\nu_\mathfrak{p}(\mu) - \kappa p\right) = 0.
\end{aligned}$$

Also folgt die Behauptung aus 2.6 wegen $\mathcal{E} = \mathcal{F}(\sqrt[p]{\rho})$.
Zu(ii): Zunächst müssen wir $\rho \in o_\mathcal{E}(\mathfrak{p})$ und damit $m_\rho(t) \in o_\mathcal{F}(\mathfrak{p})[t]$ zeigen. Dies

ist äquivalent zu

$$\nu_{\mathfrak{P}_i}\left(\gamma - \sqrt[p]{\mu}\right) \geq \mathfrak{e}_0 \qquad (1 \leq i \leq p). \tag{3.6}$$

Für diesen Schritt beachten wir, daß nach Voraussetzung $\nu_{\mathfrak{p}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\gamma - \sqrt[p]{\mu}\right)\right) = \nu_{\mathfrak{p}}\left(\gamma^p - \mu\right) \geq \mathfrak{e}_0 p$ gilt und demnach wegen $\gamma - \sqrt[p]{\mu} \in o_{\mathcal{E}}$ ein $i \in \{1, \ldots, p\}$ mit

$$\nu_{\mathfrak{P}_i}\left(\gamma - \sqrt[p]{\mu}\right) \geq 1$$

existiert. Ist nun $j \in \{1, \ldots, p\} \setminus \{i\}$ gegeben, so gibt es ein $\sigma \in \mathrm{Gal}\left(\mathcal{E}/\mathcal{F}\right) \setminus \{id\}$ mit $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, und es gilt

$$\sigma(\gamma - \sqrt[p]{\mu}) = \gamma - \zeta_p^l \sqrt[p]{\mu} \in \mathfrak{P}_j,$$

wobei $l \in \mathbb{N}_0$ passend gewählt sei. Da ζ_p eine primitive p–te Einheitswurzel ist, erzeugt $(1 - \zeta_p^l)$ das eindeutig bestimmte Primideal über p in $\mathbb{Q}(\zeta_p)$, und es gilt $\nu_{\mathfrak{P}_k}\left(1 - \zeta_p^l\right) = \mathfrak{e}_0$ für $1 \leq k \leq p$. Daraus folgt

$$\begin{aligned}
\nu_{\mathfrak{P}_j}\left(\gamma - \sqrt[p]{\mu}\right) &= \nu_{\mathfrak{P}_j}\left(\sigma(\gamma - \sqrt[p]{\mu}) + (\gamma - \sqrt[p]{\mu}) - \sigma(\gamma - \sqrt[p]{\mu})\right) \\
&\geq \min\{\nu_{\mathfrak{P}_j}\left(\sigma(\gamma - \sqrt[p]{\mu}) - (\gamma - \sqrt[p]{\mu})\right), \nu_{\mathfrak{P}_j}\left(\sigma(\gamma - \sqrt[p]{\mu})\right)\} \\
&= \min\{\nu_{\mathfrak{P}_j}\left((1 - \zeta_p^l)\sqrt[p]{\mu}\right), 1\} \\
&= \min\{\mathfrak{e}_0, 1\} = 1
\end{aligned}$$

für $j \in \{1, \ldots, p\} \setminus \{i\}$. Gilt nun $1 \leq \nu_{\mathfrak{P}_k}\left(\gamma - \sqrt[p]{\mu}\right) = c$ für ein $k \in \{1, \ldots, p\}$, so folgt analog

$$\nu_{\mathfrak{P}_j}\left(\gamma - \sqrt[p]{\mu}\right) \geq \min\{c, \mathfrak{e}_0\} \quad (1 \leq j \leq p).$$

Falls wir $\nu_{\mathfrak{P}_i}\left(\gamma - \sqrt[p]{\mu}\right) \geq \mathfrak{e}_0$ für ein Primideal $\mathfrak{P}_i$ zeigen können, gilt also $\nu_{\mathfrak{P}_j}\left(\gamma - \sqrt[p]{\mu}\right) \geq \mathfrak{e}_0$ für $1 \leq j \leq p$. Ist $i \in \{1, \ldots, p\}$ mit $\nu_{\mathfrak{P}_i}\left(\gamma - \sqrt[p]{\mu}\right) = \max\{\nu_{\mathfrak{P}_j}\left(\gamma - \sqrt[p]{\mu}\right) \mid 1 \leq j \leq p\}$ gegeben, so erhalten wir

$$\begin{aligned}
\nu_{\mathfrak{P}_i}\left(\gamma - \sqrt[p]{\mu}\right) &\geq \frac{1}{p}\nu_{\mathfrak{p}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}\left(\gamma - \sqrt[p]{\mu}\right)\right) = \frac{1}{p}\nu_{\mathfrak{p}}\left(\gamma^p - \mu\right) \\
&\geq \frac{1}{p}\mathfrak{e}_0 p = \mathfrak{e}_0.
\end{aligned}$$

Also ist (3.6) bewiesen, und es folgt

$$\begin{aligned}
\nu_{\mathfrak{P}_j}\left(\rho\right) &= \nu_{\mathfrak{P}_j}\left(\frac{\gamma - \sqrt[p]{\mu}}{\pi^{\mathfrak{e}_0}}\right) = \nu_{\mathfrak{P}_j}\left(\gamma - \sqrt[p]{\mu}\right) - \mathfrak{e}_0 \\
&\overset{(3.6)}{\geq} \mathfrak{e}_0 - \mathfrak{e}_0 = 0 \qquad (1 \leq j \leq p).
\end{aligned}$$

Somit gelten $\rho \in o_{\mathcal{E}}(\mathfrak{p})$ und $m_\rho(t) \in o_{\mathcal{F}}(\mathfrak{p})[t]$. Wir untersuchen nun $\left|m'_\rho(\rho)\right|_{\mathfrak{P}_i}$ für $1 \leq i \leq p$. Für das Minimalpolynom von ρ erhalten wir $m_\rho(t) = \prod_{i=1}^{p}(t - \rho^{(i)}) \in \mathcal{F}[t]$ und es folgt

$$m'_\rho(t) = \sum_{i=1}^{p} \prod_{\substack{j=1\\ j\neq i}}^{p} (t - \rho^{(j)}).$$

Wegen $\rho = \rho^{(p)}$ ergibt sich $m'_\rho(\rho) = \prod_{j=1}^{p-1}(\rho - \rho^{(j)})$ mit $\rho - \rho^{(j)} = -\frac{1}{\pi^{\mathfrak{e}_0}}\left(1 - \zeta_p^j\right)\sqrt[p]{\mu}$. Da ζ_p^j für $1 \leq j < p$ eine primitive p–te Einheitswurzel ist, erhalten wir

$$\nu_{\mathfrak{P}_k}\left(1 - \zeta_p^j\right) = \mathfrak{e}_0 \qquad (1 \leq k \leq p).$$

Für $1 \leq k \leq p$ folgt daher $\left|m'_\rho(\rho)\right|_{\mathfrak{P}_i} = 1$ aus

$$\begin{aligned}\nu_{\mathfrak{P}_k}\left(m'_\rho(\rho)\right) &= \sum_{j=1}^{p-1} \nu_{\mathfrak{P}_k}\left(\rho - \rho^{(j)}\right) = \sum_{j=1}^{p-1}\left(\nu_{\mathfrak{P}_k}\left((1-\zeta_p^j)\sqrt[p]{\mu}\right) - \mathfrak{e}_0\right)\\ &= \sum_{j=1}^{p-1}(\mathfrak{e}_0 + 0 - \mathfrak{e}_0) = 0.\end{aligned}$$

Mit Lemma 2.6 folgt die Behauptung.
Zu (iii): Dies ist eine offensichtliche Konsequenz aus 2.6. □

LEMMA 3.15. *Es seien $p \in \mathbb{P}$ sowie $\mathcal{E}, \mathcal{F}$ algebraische Zahlkörper mit $\zeta_p \in \mathcal{F}$ und*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

für ein $\mu \in o_{\mathcal{F}} \backslash \mathcal{P}_p(\mathcal{F})$. Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ gelte $\mathfrak{p}o_{\mathcal{E}} = \mathfrak{P}$, und für $\pi \in o_{\mathcal{F}}$ gelte $\nu_{\mathfrak{p}}(\pi) = 1$. Dann erhalten wir

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \rho, \dots, \rho^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})},$$

wobei ρ wie folgt gewählt werden kann:

(i) *Gelten $\mathfrak{p} \mid \mu$ und $\mathfrak{p} \nmid p$, so leistet*

$$\rho = \frac{1}{\pi^\kappa}\sqrt[p]{\mu}$$

mit $\kappa := \frac{\nu_{\mathfrak{p}}(\mu)}{p} \in \mathbb{N}$ das Gewünschte.

(ii) *Gelten $\mathfrak{p} \nmid \mu$ und $\mathfrak{p} \mid p$, so sei $\mathfrak{e}_0$ durch $\nu_{\mathfrak{p}}(p) = \mathfrak{e}_0(p-1)$ definiert. Dann existiert ein $\gamma \in o_{\mathcal{F}}$ mit*

$$\gamma^p \equiv \mu \mod \mathfrak{p}^{p\mathfrak{e}_0}.$$

Die Aussage folgt mit

$$\rho = \frac{\gamma - \sqrt[p]{\mu}}{\pi^{\mathfrak{e}_0}}.$$

(iii) *Gilt* $\mathfrak{p} \nmid p\mu$, *so folgt mit* $\rho = \sqrt[p]{\mu}$ *die Behauptung.*

Beweis. Ebenso wie in Lemma 3.14 kann der Fall $\mathfrak{p} \mid \mu$ und $\mathfrak{p} \mid p$ ausgeschlossen werden. Daher genügt es, die aufgeführten Fälle zu betrachten.
Zu (i): Man beachte, daß mit $a := \nu_{\mathfrak{p}}(\mu)$ wegen $p \mid a$ für $\tilde{\mu} := \frac{1}{\pi^a}\mu$

$$\mathcal{E} = \mathcal{F}\left(\sqrt[p]{\tilde{\mu}}\right)$$

nach Satz 3.3 gilt. Somit folgt

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \sqrt[p]{\tilde{\mu}}, \ldots, \sqrt[p]{\tilde{\mu}}^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})}.$$

aus $\nu_{\mathfrak{p}}(\tilde{\mu}) = 0$ und Satz 3.11.
Zu (ii),(iii): Diese Fälle sind direkte Folgerungen der lokalen Theorie. Der Satz 3.11 ist unmittelbar anwendbar. □

Bemerkung 3.16. *Die Aussagen der Lemmata* 3.14 *und* 3.15 *sind bei verschiedenen Voraussetzungen identisch. Da die Beweise jedoch sehr unterschiedlich sind, haben wir diese beiden Lemmata getrennt notiert.*

Lemma 3.17. *Es seien* $p \in \mathbb{P}$ *sowie* $\mathcal{E}, \mathcal{F}$ *algebraische Zahlkörper mit* $\zeta_p \in \mathcal{F}$ *und*

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$$

für ein $\mu \in o_{\mathcal{F}} \setminus \mathcal{P}_p(\mathcal{F})$. *Ferner gelte* $\mathfrak{p}o_{\mathcal{E}} = \mathfrak{P}^p$ *für* $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, *und es sei* $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ *gegeben. Dann erhalten wir*

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \rho, \ldots, \rho^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})},$$

wobei ρ *wie folgt gewählt werden kann:*

(i) *Gelten* $\mathfrak{p} \mid \mu$ *und* $\mathfrak{p} \mid p$, *so gilt* $\operatorname{ggT}(\nu_{\mathfrak{p}}(\mu), p) = 1$. *Sind* $a, b \in \mathbb{Z}^{\geq 0}$ *mit* $a\nu_{\mathfrak{p}}(\mu) - bp = 1$ *gegeben, so leistet*

$$\rho = \frac{1}{\pi^b}\sqrt[p]{\mu}^a$$

das Gewünschte. Ferner gilt

$$\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = p - 1 + p\nu_{\mathfrak{p}}(p).$$

(ii) *Gelten* $\mathfrak{p} \nmid \mu$ *und* $\mathfrak{p} \mid p$, *so seien* $\mathfrak{e}_0 := \frac{\nu_{\mathfrak{p}}(p)}{p-1}$ *und*

$$\kappa := \max\left\{1 \leq k < p\mathfrak{e}_0 \mid \exists \gamma \in o_{\mathcal{F}} \,:\, \gamma^p \equiv \mu \mod \mathfrak{p}^k\right\}.$$

Dann existieren $r, s \in \mathbb{Z}^{\geq 0}$ *mit* $r\kappa - sp = 1$. *Gilt für* $\gamma \in o_{\mathcal{F}}$ *die Kongruenz* $\gamma^p \equiv \mu \mod \mathfrak{p}^\kappa$, *so folgt die Aussage mit*

$$\rho = \frac{\left(\gamma - \sqrt[p]{\mu}\right)^r}{\pi^s}.$$

Für die Diskriminante ergibt sich $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = (p-1)(\mathfrak{e}_0 p - \kappa + 1)$.

(iii) *Gelten* $\pi|\mu$ *und* $\pi \nmid p$, *so gilt* $\mathrm{ggT}(\nu_{\mathfrak{p}}(\mu), p) = 1$. *Ist nun* $\nu_{\mathfrak{p}}(\mu) = k = sp+r$, *so seien* $a \in \mathbb{Z}^{\geq 0}$ *und* $b \in \mathbb{Z}^{\leq 0}$ *mit* $ar - bp = 1$ *gegeben. Dann folgt die Behauptung mit*

$$\rho = \frac{1}{\pi^{b+as}} \sqrt[p]{\mu}^a.$$

Für die Diskriminante gilt $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = p - 1$.

Beweis. Gelten $\mathfrak{p} \nmid \mu$ und $\mathfrak{p} \nmid p$, so folgt $\mathfrak{p} \nmid \mathfrak{d}(\mu)$ und somit $\mathfrak{p} \nmid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}$. Dann gilt aber $\mathfrak{p}o_{\mathcal{E}} \neq \mathfrak{P}^p$ für ein $\mathfrak{P} \in \mathbb{P}_{\mathcal{E}}$ im Widerspruch zur Voraussetzung. Also kann der Fall $\mathfrak{p} \nmid \mu$ und $\mathfrak{p} \nmid p$ nicht eintreten.
Zu (i): Wegen $\nu_{\mathfrak{p}}\left(\frac{1}{\pi^{pb}}\mu^a\right) = -pb + a\nu_{\mathfrak{p}}(\mu) = 1$ folgt die Behauptung aus Satz 3.10.
Zu (ii): Die Aussage ist eine direkte Konsequenz aus Satz 3.10.
Zu (iii): Es gilt

$$\begin{aligned}
\nu_{\mathfrak{p}}\left(\frac{1}{\pi^{p(b+as)}}\mu^a\right) &= -p(b+as) + a\nu_{\mathfrak{p}}(\mu) \\
&= -p(b+as) + a(sp+r) \\
&= -pb - pas + asp + ar \\
&= ar - bp = 1.
\end{aligned}$$

Also ergibt sich auch hier die Aussage wiederum aus Satz 3.10. □

3. Globale Ganzheitsringe

In diesem Abschnitt werden wir die lokalen und semilokalen Ergebnisse verwerten, um für eine Kummererweiterung $\mathcal{E}/\mathcal{F}$ von Primzahlgrad ein $o_{\mathcal{F}}$–Erzeugendensystem für den Ring $o_{\mathcal{E}}$ zu bestimmen.
Im weiteren seien $p \in \mathbb{P}$ und $\mathcal{F}$ ein algebraischer Zahlkörper mit $\zeta_p \in \mathcal{F}$. Ferner sei $\mathcal{E}$ eine Kummererweiterung von $\mathcal{F}$, d.h. es gelte $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ mit $\mu \in o_{\mathcal{F}} \setminus \mathcal{P}_p(\mathcal{F})$. Wie gesehen können wir nach Bemerkung 3.13

$$\nu_{\mathfrak{p}}(\mu) \in \{0, \dots, p-1\} \qquad \forall \mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \text{ mit } \nu_{\mathfrak{p}}(p) > 0 \tag{3.7}$$

annehmen.

Bemerkung 3.18. *Da der Erzeuger der Erweiterung $\mathcal{E}/\mathcal{F}$ die Bedingung* (3.7) *erfüllt, gilt nach Satz* 3.3 *für ein Primideal $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ die Implikation*

$$\mathfrak{p} \mid \mu \textit{ und } \mathfrak{p} \mid p \Longrightarrow \mathfrak{p} \mid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}.$$

Wir führen die folgenden Bezeichnungen ein:

Definition 3.19. *Für $\mathcal{E}/\mathcal{F}$ bezeichnen wir mit*

$$\Delta_{\mathcal{E}/\mathcal{F}} := \{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid \nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) > 0\}$$

die Menge der Diskriminantenteiler. Ferner definieren wir die Ideale Φ und $\Phi_{\Delta_{\mathcal{E}/\mathcal{F}}}$ mittels der Zerlegung

$$\mathfrak{d}(\sqrt[p]{\mu}) = \Phi^2 \Phi^2_{\Delta_{\mathcal{E}/\mathcal{F}}} \mathfrak{d}_{\mathcal{E}/\mathcal{F}},$$

wobei $\mathrm{ggT}(\Phi, \Phi_{\Delta_{\mathcal{E}/\mathcal{F}}}) = o_{\mathcal{F}}$ *und die Implikation „$\mathfrak{p} \mid \Phi_{\Delta_{\mathcal{E}/\mathcal{F}}} \Rightarrow \mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$" gelten. Dann heißt $\Phi_{\Delta_{\mathcal{E}/\mathcal{F}}}$ der Diskriminantenindex von $\mathcal{E}/\mathcal{F}$. Das Ideal $\left(\Phi\Phi_{\Delta_{\mathcal{E}/\mathcal{F}}}\right)^2$ bezeichnen wir als den Index von $\mathcal{E}/\mathcal{F}$, und für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ definieren wir abschließend*

$$\kappa_{\mathfrak{p}} := \nu_{\mathfrak{p}}(\Phi) \frac{2}{p(p-1)}.$$

Desweiteren definieren wir die folgenden Abbildungen.

Definition 3.20. *Für ein Primideal $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ setzen wir*

$$l(\mathfrak{p}) := \begin{cases} \max\{0 < k < pe_{\mathfrak{p}} \mid \exists c \in o_{\mathcal{F}} : c^p \equiv \mu \mod \mathfrak{p}^k\} & ; \mathfrak{p} \nmid \mu \text{ und } \nu_{\mathfrak{p}}(p) = e_{\mathfrak{p}}(p-1) > 0, \\ \nu_{\mathfrak{p}}(\mu) & ; \mathfrak{p} \mid \mu \text{ und } \mathfrak{p} \mid p, \\ r & ; \mathfrak{p} \nmid p \text{ und } \nu_{\mathfrak{p}}(\mu) = kp + r > 0. \end{cases}$$

Hierbei sei r im letzten Fall minimal gewählt.
Es existieren dann $r(\mathfrak{p}), s(\mathfrak{p}) \in \mathbb{Z}^{\geq 0}$ mit

$$r(\mathfrak{p})l(\mathfrak{p}) - s(\mathfrak{p})p = 1.$$

3.1. Einige Lemmata. Um die bereits erzielten lokalen und semilokalen Ergebnisse verwerten zu können, benötigen wir noch einige vorbereitende Lemmata, die wir nun formulieren und beweisen werden. Ein entscheidender Punkt bei der Behandlung von Kummererweiterungen ist die Existenz von p–ten Potenzen modulo gewisser Primidealpotenzen. Für die Verwertung der lokalen Ergebnisse im globalen Fall, d.h. für den Fall, daß wir algebraische Zahlkörper betrachten, ist es notwendig, die oben angesprochenen Kongruenzen simultan zu lösen. Das folgende Lemma beleuchtet diesen Punkt.

LEMMA 3.21. *Seien $\mathcal{L}$ ein algebraischer Zahlkörper und $\mathfrak{a}_1, \dots, \mathfrak{a}_k \subset o_{\mathcal{L}}$ paarweise komaximale Ideale. Gelten für $p \in \mathbb{P}$ und $\alpha, \alpha_1, \dots, \alpha_k \in o_{\mathcal{L}}$ die Kongruenzen*

$$\alpha \equiv \alpha_i^p \mod \mathfrak{a}_i \quad (1 \leq i \leq k),$$

so existiert ein $\beta \in o_{\mathcal{L}}$ mit

$$\alpha \equiv \beta^p \mod \prod_{i=1}^{k} \mathfrak{a}_i.$$

BEWEIS. Nach dem Chinesischen Restsatz existiert ein $\beta \in o_{\mathcal{F}}$ mit

$$\beta \equiv \alpha_i \mod \mathfrak{a}_i \quad (1 \leq i \leq k).$$

Für dieses β gilt dann

$$\alpha \equiv \beta^p \mod \prod_{i=1}^{k} \mathfrak{a}_i$$

wegen $\beta^p \equiv \alpha_i^p \equiv \alpha \mod \mathfrak{a}_i$ für $1 \leq i \leq k$. $\square$

Wir können nun ein wichtiges Lemma beweisen.

LEMMA 3.22. *Es existiert ein $\gamma \in o_{\mathcal{F}}$ mit*

(i) $\gamma^p \equiv \mu \mod \mathfrak{p}^{l(\mathfrak{p})}$ *für alle* $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ *mit* $\mathfrak{p} \nmid \mu$,
(ii) $\gamma^p \equiv \mu \mod \mathfrak{p}^{\mathfrak{e}_0 p}$ *für alle* $\mathfrak{p} \notin \Delta_{\mathcal{E}/\mathcal{F}}$ *und* $\nu_{\mathfrak{p}}(p) = \mathfrak{e}_0(p-1) > 0$,
(iii) $\gamma \in \mathfrak{p}^{\frac{1}{p}\nu_{\mathfrak{p}}(\mu)}$ *für alle* $\mathfrak{p} \notin \Delta_{\mathcal{E}/\mathcal{F}}$ *mit* $\mathfrak{p} \mid \mu$.

BEWEIS. Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ ist eine Kongruenz der Form

$$x^p \equiv \mu \mod \mathfrak{p}^k$$

genau dann in $\mathcal{F}$ lösbar, wenn die entsprechende Kongruenz in der $\mathfrak{p}$–adischen Vervollständigung $\mathcal{F}_{\mathfrak{p}}$ von $\mathcal{F}$ lösbar ist. Daher folgt aus den Lemmata 3.15 und 3.17 zusammen mit dem gerade gezeigten Lemma die Existenz eines $\tilde{\gamma} \in o_{\mathcal{F}}$, welches die Aussagen (i) und (ii) der Behauptung erfüllt. Nach dem Chinesischen Restsatz existiert dann ein $\gamma \in o_{\mathcal{F}}$ mit den geforderten Eigenschaften. □

Es sei hier noch kurz bemerkt, daß für die Primideale $\mathfrak{p}$, die in Punkt (iii) von Lemma 3.22 auftreten, stets $\mathfrak{p} \nmid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ und $\mathfrak{p} \nmid p$ gelten. Sei γ ab jetzt eine ganz algebraische Zahl aus $\mathcal{F}$, welche die Aussagen (i)–(iii) des letzten Lemmatas erfüllt. Dann gilt das folgende Korollar (vgl. Definition 3.19).

KOROLLAR 3.23. *Sei ein Primideal $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ gegeben. Dann gelten:*

(i) $\kappa_{\mathfrak{p}} \in \mathbb{N}_0$.
(ii) *Definiert man*

$$\rho_{\mathfrak{p}} := \frac{\gamma - \sqrt[p]{\mu}}{\pi^{\kappa_{\mathfrak{p}}}}$$

mit $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, so gilt

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})}.$$

Darüberhinaus gilt $\sharp\{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid \kappa_{\mathfrak{p}} > 0\} < \infty$.

BEWEIS. Wir beweisen dieses Lemma, indem wir alle möglichen Fälle für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ getrennt betrachten.
(a): $\mathfrak{p} \mid \mu$ und $\mathfrak{p} \nmid p$
Nach Voraussetzung gilt $\mathfrak{p} \nmid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ und daher $\mathrm{ggT}(\nu_p(\mu), p) = p$. Wegen

$$\begin{aligned} \nu_{\mathfrak{p}}(\Phi) &= \frac{1}{2}\nu_{\mathfrak{p}}(\mathfrak{d}(\sqrt[p]{\mu})) \\ &= \frac{1}{2}((p-1)\nu_{\mathfrak{p}}(\mu) + 0) \\ &= \frac{1}{2}(p-1)\nu_{\mathfrak{p}}(\mu) \end{aligned}$$

folgt $\kappa_{\mathfrak{p}} = \nu_{\mathfrak{p}}(\Phi)\frac{2}{p(p-1)} = \frac{1}{2}(p-1)\nu_{\mathfrak{p}}(\mu)\frac{2}{p(p-1)} = \nu_{\mathfrak{p}}(\mu)\frac{1}{p} \in \mathbb{N}_0$. Damit ist Teil (i) der Behauptung für diesen Fall bewiesen. Teil (ii) ist eine direkte Anwendung von Lemma 3.14 und Lemma 3.15.
(b): $\mathfrak{p} \nmid \mu$ und $\mathfrak{p} \mid p$

Wieder gilt wegen $\mathfrak{p} \nmid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ die Relation $p \mid \nu_{\mathfrak{p}}(\mu)$. Setzen wir $\mathfrak{e}_0 := \frac{\nu_{\mathfrak{p}}(p)}{p-1}$ als den Verzweigungsindex von $\mathbb{Q}_p(\zeta_p)$ über $\mathcal{F}_{\mathfrak{p}}$, so erhalten wir $\nu_{\mathfrak{p}}(\Phi) = \frac{p(p-1)\mathfrak{e}_0}{2}$. Daraus folgt

$$\kappa_{\mathfrak{p}} = \nu_{\mathfrak{p}}(\Phi)\frac{2}{p(p-1)} \in \mathbb{N}_0,$$

und mit den Lemmata 3.14 und 3.15 folgt die Behauptung.
(c): $\mathfrak{p} \nmid \mu$ und $\mathfrak{p} \nmid p$
Aus der Voraussetzung folgt $\mathfrak{p} \nmid \mathfrak{d}(\sqrt[p]{\mu})$. Daher gilt $\mathfrak{p} \nmid \Phi$ und deshalb $\kappa_{\mathfrak{p}} = 0 \in \mathbb{N}_0$. Damit folgt die Aussage aus 3.14 und 3.15.
Es bleibt noch der Zusatz $\sharp\{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid \kappa_{\mathfrak{p}} > 0\} < \infty$ zu zeigen. Dieser folgt jedoch direkt aus

$$\kappa_{\mathfrak{p}} > 0 \Rightarrow \mathfrak{p} \mid p\mu \qquad \forall \mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}.$$

□

Aufgrund dieses Korollars ist die folgende Definition sinnvoll.

Definition 3.24. *Für die Erweiterung $\mathcal{E}/\mathcal{F}$ definieren wir*

$$\mathfrak{a}_{\mathcal{E}/\mathcal{F}} := \prod_{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}} \mathfrak{p}^{\kappa_{\mathfrak{p}}}$$

als den Hauptindex von $\mathcal{E}/\mathcal{F}$.

Hiermit sind die Vorbereitungen abgeschlossen.

3.2. Relative Erzeugendensysteme. Wir können nun unser Ziel in Angriff nehmen ein relatives $o_{\mathcal{F}}$–Erzeugendensystem für $o_{\mathcal{E}}$ anzugeben. Dabei werden wir im weiteren eine Anzahl von Elementen bestimmen, die ganz algebraisch und jeweils für gewisse Primideale maximal sind.

Lemma 3.25. *Sei $\mathfrak{a}_{\mathcal{E}/\mathcal{F}}$ der Hauptindex von $\mathcal{E}/\mathcal{F}$. Ferner seien ein ganzes Ideal $\mathfrak{b} = \beta_1 o_{\mathcal{F}} + \beta_2 o_{\mathcal{F}}$ und $\delta \in o_{\mathcal{F}}$ mit*

$$\delta o_{\mathcal{F}} = \mathfrak{b}\mathfrak{a}_{\mathcal{E}/\mathcal{F}}$$

gegeben. Definiert man dann

$$\rho_i := \beta_i \frac{\gamma - \sqrt[p]{\mu}}{\delta} \qquad (i = 1, 2),$$

so gelten:

(i) $\rho_i \in o_{\mathcal{E}}$ *für* $i = 1, 2$.

(ii) *Für alle* $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ *existieren* $a(\mathfrak{p})$, $b(\mathfrak{p}) \in o_{\mathcal{F}}(\mathfrak{p})$, *so daß mit* $\rho_{\mathfrak{p}} := a(\mathfrak{p})\rho_1 + b(\mathfrak{p})\rho_2$

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})}$$

gilt.

BEWEIS. Wir zeigen zunächst $\rho_1, \rho_2 \in o_{\mathcal{E}}$. Sei dazu $\mathfrak{P} \in \mathbb{P}_{\mathcal{E}}$ beliebig und $\mathfrak{p} = o_{\mathcal{F}} \cap \mathfrak{P}$.
Gilt $\mathfrak{p} \nmid \mathfrak{a}_{\mathcal{E}/\mathcal{F}}$, so folgt wegen $\beta_i \in \mathfrak{b}$ sofort $\nu_{\mathfrak{p}}(\beta_i) \geq \nu_{\mathfrak{p}}(\mathfrak{b}) = \nu_{\mathfrak{p}}(\delta)$, und wir erhalten

$$\begin{aligned} \nu_{\mathfrak{P}}(\rho_i) &= \nu_{\mathfrak{P}}(\beta_i) - \nu_{\mathfrak{P}}(\delta) + \nu_{\mathfrak{P}}(\gamma - \sqrt[p]{\mu}) \\ &\geq \nu_{\mathfrak{P}}(\beta_i) - \nu_{\mathfrak{P}}(\delta) \geq 0 \qquad (i = 1, 2). \end{aligned}$$

Gilt $\mathfrak{p} \mid \mathfrak{a}_{\mathcal{E}/\mathcal{F}}$, so seien $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ und $\lambda_i := \nu_{\mathfrak{p}}(\beta_i) - \nu_{\mathfrak{p}}(\mathfrak{b}) \geq 0$ $(i = 1, 2)$. Dann existiert eine Einheit $\alpha_i \in o_{\mathcal{F}}(\mathfrak{p})$ mit

$$\rho_i = \alpha_i \pi^{\lambda_i} \frac{\gamma - \sqrt[p]{\mu}}{\pi^{\kappa_{\mathfrak{p}}}} \qquad (i = 1, 2).$$

Aus Korollar 3.23 erhalten wir dann $\rho_i \in o_{\mathcal{F}}(\mathfrak{p})$, denn es gilt $\lambda_i \geq 0$ und $\alpha_i \in o_{\mathcal{F}}(\mathfrak{p})^*$ $(i = 1, 2)$. Daraus folgt $\nu_{\mathfrak{P}}(\rho_i) \geq 0$ $(i = 1, 2)$.
Wir haben also $\nu_{\mathfrak{P}}(\rho_i) \geq 0$ für alle $\mathfrak{P} \in \mathbb{P}_{\mathcal{E}}$ und somit $\rho_i \in o_{\mathcal{E}}$ $(i = 1, 2)$ gezeigt.
Um den Teil (ii) der Behauptung zu zeigen, seien $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ und $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Es reicht gemäß Korollar 3.23 nachzuweisen, daß

$$\frac{\gamma - \sqrt[p]{\mu}}{\pi^{\kappa_{\mathfrak{p}}}}$$

mittels ρ_1 und ρ_2 darstellbar ist. Dazu unterscheiden wir die beiden Fälle $\kappa_{\mathfrak{p}} = 0$ und $\kappa_{\mathfrak{p}} > 0$.
Untersuchen wir zuerst den Fall $\kappa_{\mathfrak{p}} = 0$. Wegen $\delta \in \mathfrak{b}$ existieren $a, b \in o_{\mathcal{F}}$ mit $\delta = a\beta_1 + b\beta_2$. Es gilt in $o_{\mathcal{F}}(\mathfrak{p})$:

$$\begin{aligned} a\rho_1 + b\rho_2 &= (a\beta_1 + b\beta_2)\frac{\gamma - \sqrt[p]{\mu}}{\delta} \\ &= \gamma - \sqrt[p]{\mu} \\ &= \frac{\gamma - \sqrt[p]{\mu}}{\pi^{\kappa_{\mathfrak{p}}}}. \end{aligned}$$

Für den Fall $\kappa_{\mathfrak{p}} > 0$ setzen wir

$$\phi := \frac{\gamma - \sqrt[p]{\mu}}{\pi^{\kappa_{\mathfrak{p}}}}$$

und erhalten $o_{\mathcal{E}}(\mathfrak{p}) = [1, \phi, \dots, \phi^{p-1}]_{o_{\mathcal{F}}(\mathfrak{p})}$. In $o_{\mathcal{F}}$ impliziert die Definition von δ eine Darstellung

$$\delta = \sum_{i=1}^{m} \pi_i^{(1)} \cdot \ldots \cdot \pi_i^{(\kappa_{\mathfrak{p}})} b_i$$

mit $m \in \mathbb{N}, \pi_i^{(1)}, \dots, \pi_i^{(\kappa_{\mathfrak{p}})} \in \mathfrak{p}$ sowie $b_i \in \mathfrak{b}$ für $1 \leq i \leq m$. Es sei nun $b_i = b_i^{(1)}\beta_1 + b_i^{(2)}\beta_2$ mit $b_i^{(1)}, b_i^{(2)} \in o_{\mathcal{F}}$ $(1 \leq i \leq m)$ und $\pi_i^{(1)} \cdot \ldots \cdot \pi_i^{(\kappa_{\mathfrak{p}})} = u_i \pi^{\kappa_{\mathfrak{p}}}$ für gewisse $u_i \in o_{\mathcal{F}}(\mathfrak{p})$ $(1 \leq i \leq m)$. Dann folgt

$$\begin{aligned} \delta &= \sum_{i=1}^{m} \pi_i^{(1)} \cdot \ldots \cdot \pi_i^{(\kappa_{\mathfrak{p}})} b_i \\ &= \sum_{i=1}^{m} \pi_i^{(1)} \cdot \ldots \cdot \pi_i^{(\kappa_{\mathfrak{p}})} b_i^{(1)} \beta_1 + \sum_{i=1}^{m} \pi_i^{(1)} \cdot \ldots \cdot \pi_i^{(\kappa_{\mathfrak{p}})} b_i^{(1)} \beta_1 \\ &= \left(\beta_1 \sum_{i=1}^{m} u_i b_i^{(1)} + \beta_2 \sum_{i=1}^{m} u_i b_i^{(2)} \right) \pi_i^{(\kappa_{\mathfrak{p}})}. \end{aligned}$$

Setzen wir $a(\mathfrak{p}) = \sum_{i=1}^{m} u_i b_i^{(1)}$ und $b(\mathfrak{p}) = \sum_{i=1}^{m} u_i b_i^{(2)}$, so erhalten wir offenbar $a(\mathfrak{p})$, $b(\mathfrak{p}) \in o_{\mathcal{F}}(\mathfrak{p})$ und weiter

$$\phi = a(\mathfrak{p})\rho_1 + b(\mathfrak{p})\rho_2.$$

□

BEMERKUNG 3.26. *Seien ρ_1 und ρ_2 wie im letzten Lemma gegeben. Dann wird für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ durch*

$$\left\{1, \rho_1, \dots, \rho_1^{p-1}, \rho_2, \dots, \rho_2^{p-1}\right\}$$

ein $o_{\mathcal{F}}(\mathfrak{p})$–Erzeugendensystem von $o_{\mathcal{E}}(\mathfrak{p})$ gegeben.

Als nächstes behandeln wir die Diskriminantenteiler.

LEMMA 3.27. *Sei $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ mit $\mathfrak{p} \nmid \mu$ und $\mathfrak{p} \mid p$. Ferner sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, und es gelte*

$$\pi o_{\mathcal{F}} = \mathfrak{p}\mathfrak{b}_{\mathfrak{p}}$$

mit einem ganzen Ideal $\mathfrak{b}_{\mathfrak{p}} \subseteq o_{\mathcal{F}}$. Ist $\beta_{\mathfrak{p}} \in \mathfrak{b}_{\mathfrak{p}}$ mit $\nu_{\mathfrak{p}}(\beta_{\mathfrak{p}}) = 0$, so wird durch

$$\rho_{\mathfrak{p}} := \beta_{\mathfrak{p}}^{s(\mathfrak{p})} \frac{\left(\gamma - \sqrt[p]{\mu}\right)^{r(\mathfrak{p})}}{\pi^{s(\mathfrak{p})}}$$

eine ganz algebraische Zahl definiert, mit der durch

$$\left\{1, \rho_{\mathfrak{p}}, \dots, \rho_{\mathfrak{p}}^{p-1}\right\}$$

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

Beweis. Wir werden neben der Aussage über die $o_{\mathcal{F}}(\mathfrak{p})$–Basis von $o_{\mathcal{E}}(\mathfrak{p})$ zeigen, daß $\nu_{\mathfrak{P}}(\rho_{\mathfrak{p}}) \geq 0$ für alle $\mathfrak{P} \in \mathbb{P}_{\mathcal{E}}$ gilt. Daraus ergibt sich dann $\rho_{\mathfrak{p}} \in o_{\mathcal{E}}$.
Seien $\mathfrak{P} \in \mathbb{P}_{\mathcal{E}}$ beliebig und $\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}}$ durch $\mathfrak{p}' := o_{\mathcal{F}} \cap \mathfrak{P}$ gegeben. Gilt $\mathfrak{p}' \neq \mathfrak{p}$, so erhalten wir

$$\begin{aligned} \nu_{\mathfrak{P}}(\rho_{\mathfrak{p}}) &= s(\mathfrak{p})\nu_{\mathfrak{P}}(\beta_{\mathfrak{p}}) - s(\mathfrak{p})\nu_{\mathfrak{P}}(\pi) + r(\mathfrak{p})\nu_{\mathfrak{P}}(\gamma - \sqrt[p]{\mu}) \\ &\geq s(\mathfrak{p})\left(\nu_{\mathfrak{P}}(\beta_{\mathfrak{p}}) - \nu_{\mathfrak{P}}(\pi)\right) \geq 0 \end{aligned}$$

wegen $\nu_{\mathfrak{p}'}(\beta_{\mathfrak{p}}) \geq \nu_{\mathfrak{p}'}(\pi)$.
Gilt $\mathfrak{p}' = \mathfrak{p}$, so folgt $\nu_{\mathfrak{p}'}(\beta_{\mathfrak{p}}) = 0$. Dies impliziert $\beta_{\mathfrak{p}} \in o_{\mathcal{F}}(\mathfrak{p})^*$, und wir erhalten wegen $\mathfrak{p}o_{\mathcal{E}} = \mathfrak{P}^p$ nach Lemma 3.17 einerseits $\nu_{\mathfrak{P}}(\rho_{\mathfrak{p}}) \geq 0$ und andererseits die Behauptung bzgl. der $o_{\mathcal{F}}(\mathfrak{p})$–Basis von $o_{\mathcal{E}}(\mathfrak{p})$. □

Lemma 3.28. *Es sei $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ mit $\mathfrak{p} \mid \mu$ gegeben. Ferner sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ und es gelte*

$$\pi o_{\mathcal{F}} = \mathfrak{p}\mathfrak{b}_{\mathfrak{p}}.$$

Setzen wir

$$k := \begin{cases} s(\mathfrak{p}) + r(\mathfrak{p})\frac{\nu_{\mathfrak{p}}(\mu) - l(\mathfrak{p})}{p} & \text{falls } \mathfrak{p} \nmid p \\ s(\mathfrak{p}) & \text{falls } \mathfrak{p} \mid p \end{cases}$$

und ist $\beta_{\mathfrak{p}} \in \mathfrak{b}$ mit $\nu_{\mathfrak{p}}(\beta_{\mathfrak{p}}) = 0$ gegeben, so wird durch

$$\rho_{\mathfrak{p}} := \frac{\beta_{\mathfrak{p}}^k}{\pi^k} \sqrt[p]{\mu}^{r(\mathfrak{p})}$$

eine ganz algebraische Zahl in $\mathcal{E}$ definiert. Schließlich bilden die Elemente

$$1, \rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1}$$

eine $o_{\mathcal{F}}(\mathfrak{p})$–Basis von $o_{\mathcal{E}}(\mathfrak{p})$.

Beweis. Analog zu dem Beweis von Lemma 3.27. □

Wir sind nun in der Lage, die Hauptaussage dieses Kapitels zu formulieren und zu beweisen.

Satz 3.29. *Seien ρ_1, ρ_2 wie in Lemma 3.25, und für $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ sei $\rho_{\mathfrak{p}}$ wie in den Lemmata 3.27 und 3.28 gegeben. Definiert man dann*

$$\Omega := \left\{1, \rho_1, \ldots, \rho_1^{p-1}, \rho_2, \ldots, \rho_2^{p-1}\right\} \cup \left\{\rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1} \;\middle|\; \mathfrak{p} \mid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right\},$$

so wird durch Ω ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ gegeben.

Beweis. Es sei $1 = \eta_1, \dots, \eta_n$ eine Ganzheitsbasis von $o_{\mathcal{F}}$. Betrachten wir die Menge

$$\tilde{\Omega} := \{\eta_i \omega \mid 1 \le i \le n,\ \omega \in \Omega\},$$

so wird durch $\tilde{\Omega}$ ein freier $\mathbb{Z}$–Modul von vollem Rang in $\mathcal{E}$ gegeben. Daher existieren $\omega_1, \dots, \omega_{np} \in o_{\mathcal{E}}$ mit

$$\left[\tilde{\Omega}\right]_{\mathbb{Z}} = \omega_1 \mathbb{Z} + \ldots + \omega_{np}\mathbb{Z}.$$

Also gibt es gewisse $\gamma_j(\tau) \in \mathbb{Z}$ $(1 \le j \le np$ und $\tau \in \tilde{\Omega})$ mit

$$\tau = \sum_{j=1}^{np} \gamma_j(\tau)\omega_j. \tag{3.8}$$

Ist nun $\alpha \in o_{\mathcal{E}}$ beliebig gegeben, so existieren für $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}}$ und $\omega \in \Omega$ Elemente $\alpha(\mathfrak{q}, \omega) \in o_{\mathcal{F}}(\mathfrak{q})$ mit

$$\alpha = \sum_{\omega \in \Omega} \alpha(\mathfrak{q}, \omega)\omega. \tag{3.9}$$

Da ferner $\eta_1, \dots, \eta_n$ eine Ganzheitsbasis von $o_{\mathcal{F}}$ ist, können wir zu $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}}$ und $\omega \in \Omega$ mit $q = \mathbb{Z} \cap \mathfrak{q}$ Zahlen $\alpha_i(\mathfrak{q}, \omega) \in \mathbb{Z}(q)$ $(1 \le i \le n)$ wählen, mit denen

$$\alpha(\mathfrak{q}, \omega) = \sum_{i=1}^{n} \alpha_i(\mathfrak{q}, \omega)\eta_i \tag{3.10}$$

gilt. Beachtet man abschließend, daß $\{\eta_1, \dots, \eta_n\} \subset \tilde{\Omega}$ wegen $1 \in \Omega$ gilt, so erhalten wir für $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}}$ die Gleichheit

$$\begin{aligned}
\alpha &\overset{3.9}{=} \sum_{\omega \in \Omega} \alpha(\mathfrak{q}, \omega)\omega \\
&\overset{3.8}{=} \sum_{\omega \in \Omega} \left(\sum_{j=1}^{np} \alpha(\mathfrak{q}, \omega)\gamma_j(\omega)\omega_j \right) \\
&\overset{3.10}{=} \sum_{\omega \in \Omega} \left(\sum_{j=1}^{np} \sum_{l=1}^{n} \left(\alpha_l(\mathfrak{q}, \omega)\eta_l \gamma_j(\omega)\omega_j\right) \right) \\
&\overset{3.8}{=} \sum_{\omega \in \Omega} \left(\sum_{j=1}^{np} \sum_{l=1}^{n} \sum_{k=1}^{np} \alpha_l(\mathfrak{q}, \omega)\eta_l \gamma_j(\omega)\omega_j \gamma_k(\eta_l)\omega_k \right) \\
&=: \sum_{\omega \in \Omega} \left(\sum_{j=1}^{np} \beta_j(\mathfrak{q}, \omega)\omega_j \right) = \sum_{j=1}^{np} \left(\sum_{\omega \in \Omega} \beta_j(\mathfrak{q}, \omega) \right) \omega_j =: \sum_{j=1}^{np} \beta_j(\mathfrak{q})\omega_j.
\end{aligned}$$

Aufgrund der Wahl von $\alpha_l(\mathfrak{q}, \omega)$ und $\gamma_k(\omega)$ gilt $\beta_j(\mathfrak{q}) \in \mathbb{Z}(q) \subset \mathbb{Q}$ $(1 \le j \le np)$ mit $q := \mathbb{Z} \cap \mathfrak{q}$. Da $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}}$ beliebig gewählt war, trifft dies für alle Primideale aus

$o_{\mathcal{F}}$ zu.
Weil die Elemente $\omega_1, \dots, \omega_{np}$ eine $\mathbb{Q}$–Basis von $\mathcal{E}$ bilden, sind die Koeffizienten $\beta_1(\mathfrak{q}), \dots, \beta_{np}(\mathfrak{q})$ eindeutig und daher unabhänig von der Wahl von $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}}$. Es sei daher $\beta_i := \beta_i(\mathfrak{q})$ für $1 \leq i \leq np$. Damit erhalten wir wegen der Unabhängigkeit von $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}}$

$$\beta_1, \dots, \beta_{np} \in \bigcap_{q \in \mathbb{P}} \mathbb{Z}(q) = \mathbb{Z}.$$

Da $\alpha \in o_{\mathcal{E}}$ beliebig war, ist $\omega_1, \dots, \omega_{np}$ somit eine Ganzheitsbasis von $o_{\mathcal{E}}$. Also ist $\tilde{\Omega}$ ein $\mathbb{Z}$–Erzeugendensystem von $o_{\mathcal{E}}$, und mithin wird durch Ω ein $o_{\mathcal{F}}$–Erzeugendensystem gegeben. □

BEMERKUNG 3.30. (i) *Wie im letzten Beweis schon angedeutet, ist es mittels des relativen Erzeugendensystems sehr einfach, eine Ganzheitsbasis von $o_{\mathcal{E}}$ zu bestimmen. Für eine Ganzheitsbasis $\eta_1, \dots, \eta_n$ von $o_{\mathcal{F}}$ und ein $o_{\mathcal{F}}$–Erzeugendensystem $\Omega \subset o_{\mathcal{E}}$ von $o_{\mathcal{E}}$ wird durch*

$$\tilde{\Omega} := \{\eta_i \omega \mid 1 \leq i \leq n,\ \omega \in \Omega\}$$

ein $\mathbb{Z}$–Erzeugendensystem von $o_{\mathcal{E}}$ gegeben. Daraus kann man dann mit Standardmethoden eine Ganzheitsbasis von $o_{\mathcal{E}}$ bestimmen.

(ii) *Man benötigt für alle Berechnungen lediglich eine Ganzheitsbasis von $o_{\mathcal{E}}$.*

(iii) *Bei den im Rahmen dieser Arbeit durchgeführten praktischen Untersuchungen waren die berechneten Erzeugendensysteme immer relativ klein. Durch während der Berechnungen durchgeführte Vereinfachungen erhielten wir als Ergebnis stets ein Erzeugendensystem Ω mit $p \leq |\Omega| < 3p$. Bei der überwiegenden Anzahl der Beispiele war $|\Omega| < 2p$ erfüllt.*

(iv) *Mittels eines in* [BoPo] *beschriebenen Verfahrens lassen sich mit Ω ganze Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_p \subseteq \mathcal{I}_{\mathcal{F}}$ und algebraische Zahlen $\xi_1, \dots, \xi_p \in \mathcal{E}$ bestimmen, so daß*

$$o_{\mathcal{E}} = \mathfrak{a}_1 \xi_1 + \ldots + \mathfrak{a}_p \xi_p$$

gilt. Wir werden später noch auf diesen Algorithmus eingehen.

Zum Abschluß wollen wir noch ein kleines Beispiel für eine Kummererweiterung vom gerade behandelten Typ angeben:

BEISPIEL 3.31. *Wir betrachten eine Kummererweiterung des Körpers $\mathcal{F} = \mathbb{Q}(\rho, \zeta_3)$, wobei ρ eine Nullstelle des Polynoms*

$$\tilde{f}(t) = t^3 - 2t^2 + 4t + 1$$

sei. Ist δ eine passende Nullstelle des Polynoms

$$f(t) = t^6 + 5t^5 + 18t^4 + 43t^3 + 63t^2 + 50t + 28,$$

so wird durch δ ein primitives Element von $\mathcal{F}$ gegeben, und wir erhalten $\mathfrak{d}_{\mathcal{F}} = -2958147$ für die Diskriminante und $h_{\mathcal{F}} = 4$ für die Klassenzahl von $\mathcal{F}$. Eine Ganzheitsbasis von $o_{\mathcal{F}}$ wird durch

$$\begin{aligned}
\omega_1, \dots, \omega_4 &= 1, \delta, \delta^2, \delta^3, \\
\omega_5 &= \frac{1}{2}(-\delta + \delta^4), \\
\omega_6 &= \frac{1}{128}(12 - 54\delta - 73\delta^2 - 68\delta^3 - 46\delta^4 + \delta^5)
\end{aligned}$$

gegeben. Setzen wir nun

$$\mu = \sqrt[3]{123 + 445\omega_2 + 23\omega_3 + 12\omega_4 + 23\omega_5 + 2\omega_6},$$

und untersuchen $\mathcal{E} = \mathcal{F}(\mu)$, so ergibt sich aus

$$\begin{aligned}
3o_{\mathcal{F}} &= (3o_{\mathcal{F}} + (1 + \omega_2)o_{\mathcal{F}})^2 \cdot (3o_{\mathcal{F}} + (1 + \omega_3)o_{\mathcal{F}})^2 \\
&=: \mathfrak{q}_1^2\mathfrak{q}_2^2, \\
\mu o_{\mathcal{F}} &= (2o_{\mathcal{F}} + (\omega_4 - \omega_5 - \omega_6)o_{\mathcal{F}}) \\
&\quad \cdot(37o_{\mathcal{F}} + (16\omega_1 + \omega_2)o_{\mathcal{F}}) \\
&\quad \cdot(2053o_{\mathcal{F}} + (1076\omega_1 + \omega_2)o_{\mathcal{F}}) \\
&\quad \cdot(398368903213o_{\mathcal{F}} + (138280672974\omega_1 + \omega_2)o_{\mathcal{F}}) \\
&=: \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4
\end{aligned}$$

die Relativdiskriminante

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}} = \mathfrak{q}_2^6\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_4^2.$$

Ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ wird dann durch

$$\begin{aligned}
\alpha_1 &= 1, \\
\alpha_2 &= \mu, \\
\alpha_3 &= \mu^2, \\
\alpha_4 &= \frac{1}{3}(2 + 2\omega_4 + 2\omega_5 + \omega_6)(1 + \mu), \\
\alpha_5 &= \frac{1}{3}((2 + 2\omega_2 + \omega_3 + \omega_5) \\
&\quad +(2 + \omega_2 + 2\omega_3 + \omega_4 + \omega_6)\mu \\
&\quad +(2\omega_2 + \omega_3 + \omega_4 + 2\omega_5 + 2\omega_6)\mu^2)
\end{aligned}$$

gegeben. Als Absolutdiskriminante von $\mathcal{E}$ ergibt sich schließlich

$$\mathfrak{d}_{\mathcal{E}} = -201551716505357141773100256933962151918850846184734522577712.$$

4. Der allgemeine Fall

Wir gehen nun auf allgemeine Kummererweiterungen ein, d.h. wir untersuchen bei gegebenem $n \in \mathbb{N}$ für einen Zahlkörper $\mathcal{F}$ mit $\zeta_n \in \mathcal{F}$ eine Erweiterung $\mathcal{E}$ von $\mathcal{F}$, für die

$$\mathcal{E} = \mathcal{F}(\sqrt[n]{\mu})$$

gilt. Hierbei sei $\mu \in o_{\mathcal{F}}$ so gewählt, daß $t^n - \mu$ in $\mathcal{F}[t]$ irreduzibel ist.
Gilt $n = p_1 \cdots p_k$ mit $p_i \in \mathbb{P}$ $(1 \leq i \leq k)$, so erhalten wir den folgenden Körperturm:

$$\begin{tikzcd}[column sep=small]
& & & \mathcal{E} = \mathcal{F}(\sqrt[n]{\mu}) \arrow[d, phantom, "\vdots"] \\
& & & \mathcal{F}(\sqrt[p_1 p_2]{\mu}) \arrow[dl, dash] \\
& & \mathcal{F}(\sqrt[p_1]{\mu}) \arrow[dl, dash] & \\
& \mathcal{F} & &
\end{tikzcd}$$

Wir können für einen solchen Körperturm ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ bestimmen, indem wir für jede Stufe ein relatives Erzeugendensystem bestimmen und dann die Einzelergebnisse zusammenfassen. Jede Stufe ist mit der vorgestellten Methode lösbar, denn bei den einzelnen Erweiterungen handelt es sich jeweils um Erweiterungen von Primzahlgrad.

Bemerkung 3.32. *Eine solche Unterteilung in Teilerweiterungen kann auch bei verallgemeinerten Kummererweiterungen (vgl.* 3.1*) benutzt werden.*

Beispiel 3.33. *Wir werden nun eine Kummererweiterung vom Grad* $6 = 2 \cdot 3$ *des Körpers* $\mathcal{F} = \mathbb{Q}(\rho)$ *untersuchen, wobei* ρ *eine Nullstelle des Polynoms*

$$f(t) = t^6 + 5t^5 + 18t^4 + 43t^3 + 63t^2 + 50t + 28$$

sei. Da dies der gleiche Körper wie schon in Beispiel 3.31 *ist, wählen wir als Ganzheitsbasis* $\omega_1, \ldots, \omega_6$ *die dort angegebene Basis.*
Wir definieren nun $\mathcal{E}_1 = \mathcal{F}(\sqrt{5})$ *und* $\mathcal{E}_2 = \mathcal{E}_1(\sqrt[3]{5})$ *und wollen ein* $o_{\mathcal{F}}$*–Erzeugendensystem von* $o_{\mathcal{E}_2}$ *berechnen. Aus Gründen der Übersichtlichkeit beschränken wir uns*

auf die Angabe eines $o_{\mathcal{F}}$–Erzeugendensystems von $o_{\mathcal{E}_1}$ und eines $o_{\mathcal{E}_1}$–Erzeugendensystems von $o_{\mathcal{E}_2}$. Für die Diskriminante des Körpers $\mathcal{E}_1$ erhalten wir dann

$$|\mathfrak{d}_{\mathcal{E}_1}| = 136728651150140625$$

und mit

$$\alpha_1 = 1, \qquad \alpha_2 = \frac{1+\sqrt{5}}{2}$$

gilt $o_{\mathcal{E}_1} = [\alpha_1, \alpha_2]_{o_{\mathcal{F}}}$. Für die Erweiterung $\mathcal{E}_2/\mathcal{E}_1$ erhalten wir dann das folgende $o_{\mathcal{E}_1}$–Erzeugendensystem von $o_{\mathcal{E}_2}$:

$$\begin{aligned}
\beta_1 &= 1,\\
\beta_2 &= \sqrt[3]{5},\\
\beta_3 &= \sqrt[3]{5}^2,\\
\beta_4 &= \frac{1}{3}(((\omega_3+\omega_4+\omega_6)+(1+\omega_2+2\omega_3+\omega_5+2\omega_6)\sqrt{5})\\
&\quad +(\omega_5+(2\omega_2+\omega_4+\omega_6)\sqrt{5})\sqrt[3]{5}\\
&\quad +((2\omega_2+\omega_4+2\omega_5)+(2\omega_2+2\omega_4+2\omega_5+\omega_6)\sqrt{5})\sqrt[3]{5}^2),\\
\beta_5 &= \frac{1}{3}(((2+2\omega_3+\omega_4+\omega_6)+(2+2\omega_2+2\omega_3+\omega_5+\omega_6)\sqrt{5})\\
&\quad +((\omega_2+\omega_3+\omega_4+2\omega_5+2\omega_6)+(2\omega_2+2\omega_5+\omega_6)\sqrt{5})\sqrt[3]{5}\\
&\quad +((1+2\omega_4+2\omega_5+2\omega_6)+(\omega_2+2\omega_4+2\omega_5+2\omega_6)\sqrt{5})\sqrt[3]{5}^2),\\
\beta_6 &= \frac{1}{3}(((1+\omega_2+2\omega_4)+(2+\omega_3+\omega_4+\omega_5)\sqrt{5})\\
&\quad +((2+\omega_2+2\omega_3)+(1+\omega_2+\omega_3+2\omega_4)\sqrt{5})\sqrt[3]{5}\\
&\quad +((2\omega_2+2\omega_3+\omega_5+2\omega_6)+(2+\omega_2+\omega_5)\sqrt{5})\sqrt[3]{5}^2),\\
\beta_7 &= \frac{1}{3}(((2+2\omega_2+\omega_3+2\omega_4+\omega_5+2\omega_6)+(2+2\omega_2+\omega_3+2\omega_4+\omega_5+\omega_6)\sqrt{5})\\
&\quad +((2\omega_2+\omega_4+2\omega_5+2\omega_6)+(2+2\omega_2+\omega_4)\sqrt{5})\sqrt[3]{5}\\
&\quad +((2+2\omega_2+2\omega_3+\omega_4+2\omega_5)+(2+\omega_3+\omega_5+\omega_6)\sqrt{5})\sqrt[3]{5}^2),\\
\beta_8 &= \frac{1}{3}(((\omega_2+2\omega_3+2\omega_4+\omega_6)+(1+2\omega_2+2\omega_3+2\omega_5)\sqrt{5})\\
&\quad +((\omega_2+2\omega_3+2\omega_4+\omega_5)+(2+2\omega_2+2\omega_3+2\omega_4+\omega_5+\omega_6)\sqrt{5})\sqrt[3]{5}\\
&\quad +((\omega_3+\omega_4+2\omega_5+2\omega_6)+(2+\omega_2+2\omega_3+\omega_4+\omega_5)\sqrt{5})\sqrt[3]{5}^2),\\
\beta_9 &= \frac{1}{3}(((1+\omega_3+\omega_4)+(\omega_3+2\omega_4)\sqrt{5})\\
&\quad +((\omega_2+2\omega_3+\omega_5+2\omega_6)+(\omega_2+\omega_3+\omega_4+\omega_5)\sqrt{5})\sqrt[3]{5}\\
&\quad +((1+\omega_2+\omega_3+\omega_4+2\omega_5+2\omega_6)\sqrt{5})\sqrt[3]{5}^2).
\end{aligned}$$

Damit ergibt sich für $\mathcal{E}_2$ die Absolutdiskriminante

$$\begin{aligned} |\mathfrak{d}_{\mathcal{E}_2}| &= 1762498490114207271017532000509650015135467 \\ &\, 16238790191709995269775390625. \end{aligned}$$

KAPITEL 4

Algorithmen

Wir werden in diesem Kapitel die Algorithmen formulieren, die wir zur Bestimmung einer Ganzheitsbasis bzw. eines relativen Erzeugendensystems für Kummererweiterungen $\mathcal{E}/\mathcal{F}$ benötigen. Als Anwendung dieser Algorithmen werden wir zum Abschluß des Kapitels ein Verfahren zur Bestimmung einer Ganzheitsbasis einer Radikalerweiterung angeben.

1. p–te Potenzen

Bei der Bestimmung eines $o_{\mathcal{F}}$–Erzeugendensystems von $o_{\mathcal{E}}$ für eine Kummererweiterung $\mathcal{E}/\mathcal{F}$ von Primzahlgrad p spielt die Bestimmung p–ter Potenzen modulo gewisser Primidealpotenzen eine entscheidende Rolle (vgl. Lemma 3.21). Da wir die theoretischen Ergebnisse praktisch verwerten wollen, ist es für diese Arbeit von vitalem Interesse, dieses Problem effizient zu lösen. Wir beschäftigen uns daher mit dieser Fragestellung näher.
Falls nichts anderes gesagt wird, seien $p \in \mathbb{P}$ und $\mathcal{F}$ ein algebraischer Zahlkörper mit $\zeta_p \in \mathcal{F}$. Ferner sei $\mu \in o_{\mathcal{F}}$ eine algebraische Zahl, für die das Polynom $t^p - \mu$ in $\mathcal{F}[t]$ irreduzibel ist. Schließlich seien $\mathfrak{p}$ ein Primideal in $o_{\mathcal{F}}$ mit $\nu_{\mathfrak{p}}(\mu) = 0$ und $\mathfrak{e}_{\mathfrak{p}} > 0$ durch

$$\nu_{\mathfrak{p}}(p) = \mathfrak{e}_{\mathfrak{p}}(p-1)$$

definiert. Wir müssen für ein solches Primideal die folgenden Werte bestimmen:

(a) $\kappa_{\mathfrak{p}} \in \mathbb{N}$ mit $\kappa_{\mathfrak{p}} := \max\{0 < k \leq p\mathfrak{e}_{\mathfrak{p}} \mid \exists c \in o_{\mathcal{F}} : c^p \equiv \mu \mod \mathfrak{p}^k\}$,
(b) $\gamma \in o_{\mathcal{F}}$ mit $\gamma^p \equiv \mu \mod \mathfrak{p}^{\kappa_{\mathfrak{p}}}$.

Diese Probleme werden wir in zwei Stufen behandeln. Zunächst untersuchen wir, wie wir entscheiden können, für welche $k \in \{1, \ldots, \mathfrak{e}_\mathfrak{p}(p-1)\}$ die Kongruenz

$$x^p \equiv \mu \mod \mathfrak{p}^k \tag{4.1}$$

eine Lösung hat und wie wir eine solche gegebenenfalls bestimmen können. Anschließend betrachten wir die Kongruenz (4.1) für Exponenten $k \in \{\mathfrak{e}_\mathfrak{p}(p-1)+1, \ldots, \mathfrak{e}_\mathfrak{p}p\}$ unter der gleichen Fragestellung.

Lemma 4.1. *Es sei $\mathcal{K}$ ein algebraischer Zahlkörper, und es sei $\mathfrak{p} \in \mathbb{P}_\mathcal{K}$ mit $\mathfrak{p} \mid p$ gegeben. Dann ist für $1 \leq n \leq \nu_\mathfrak{p}(p)$ die Abbildung*

$$\phi : o_\mathcal{K}/\mathfrak{p}^n \longrightarrow o_\mathcal{K}/\mathfrak{p}^n : x \mapsto x^p$$

ein Ringhomomorphismus.

Beweis. Wir zeigen zuerst die Wohldefiniertheit der Abbildung ϕ. Seien dazu $a, b \in o_\mathcal{K}$ mit $a \equiv b \mod \mathfrak{p}^n$ gegeben. Dann folgt aus

$$a^p - b^p = (a-b)\sum_{i=0}^{p-1} a^i b^{p-1-i}$$

$a^p - b^p \in \mathfrak{p}^n$, denn nach Voraussetzung gilt $a - b \in \mathfrak{p}^n$ und $\mathfrak{p}^n$ ist ein Ideal. Wir beweisen nun, daß ϕ ein Ringhomomorphismus ist:

(i) $\phi(x+y) = \phi(x) + \phi(y)$
Seien $a, b \in o_\mathcal{K}$ gegeben. Dann gilt

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p.$$

Aus $\nu_\mathfrak{p}(p) \geq n$ und $p \mid \binom{p}{i}$ $(1 \leq i \leq p-1)$ folgt

$$\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} \in \mathfrak{p}^n.$$

Dies bedeutet aber $\phi((a+\mathfrak{p}^n) + (b+\mathfrak{p}^n)) = \phi(a+\mathfrak{p}^n) + \phi(b+\mathfrak{p}^n)$.

(ii) $\phi(xy) = \phi(x)\phi(y)$
Dies gilt offenbar.

Damit ist $\phi \in \mathrm{End}(o_\mathcal{K}/\mathfrak{p}^n)$ gezeigt. □

Wir setzen dieses Lemma nun konstruktiv um, indem wir im nächsten Satz einen Algorithmus andeuten, der für den eben behandelten Fall untersucht, ob eine p–te Potenz existiert und diese dann gegebenenfalls bestimmt.

Satz 4.2. *Es seien ein algebraischer Zahlkörper $\mathcal{K}$, $\mathfrak{p} \in \mathbb{P}_{\mathcal{K}}$ mit $\mathfrak{p} \mid p$ und $n \in \mathbb{N}$ mit $0 < n \leq \nu_{\mathfrak{p}}(p)$ gegeben. Ferner seien $o_{\mathcal{K}} = \omega_1\mathbb{Z} + \ldots + \omega_m\mathbb{Z}$, $\mathfrak{p}^n = \pi_1\mathbb{Z} + \ldots + \pi_m\mathbb{Z}$ sowie $(\omega_1^p, \ldots, \omega_m^p) = (\omega_1, \ldots, \omega_m)H_1$ und $(\pi_1, \ldots, \pi_m) = (\omega_1, \ldots, \omega_m)H_2$. Definieren wir nun*

$$\tilde{H} := (H_1|H_2),$$

so gilt mit der zugehörigen Hermite Normalform $H := HNF(\tilde{H}) = \tilde{H}T$ ($T \in GL(2m, \mathbb{Z})$):
Zu $\beta = \sum_{i=1}^m b_i\omega_i$ existiert genau dann ein $\gamma \in o_{\mathcal{K}}$ mit

$$\gamma^p \equiv \beta \mod \mathfrak{p}^n, \tag{4.2}$$

wenn ein $\underline{x} \in \mathbb{Z}^{2m}$ existiert mit $(\omega_1, \ldots, \omega_m)H\underline{x} = \beta$. Eine Lösung der Kongruenz (4.2) wird dann durch $\gamma := \sum_{i=1}^m (T\underline{x})_i\omega_i$ gegeben.

Beweis. Betrachten wir die Abbildung

$$\phi : o_{\mathcal{K}}/\mathfrak{p}^n \longrightarrow o_{\mathcal{K}}/\mathfrak{p}^n : x \mapsto x^p,$$

so ist ϕ nach Lemma 4.1 ein Ringhomomorphismus. Für $\alpha = \sum_{i=1}^m a_i\omega_i \in o_{\mathcal{K}}$ mit $a_i \in \mathbb{Z}$ $(1 \leq i \leq m)$ gilt daher

$$\phi(\alpha + \mathfrak{p}^n) = a_1\omega_1^p + \ldots + a_m\omega_m^p + \mathfrak{p}^n. \tag{4.3}$$

Wir beweisen nun die behauptete Äquivalenz.
Dazu sei $\gamma = \sum_{i=1}^m c_i\omega_i \in o_{\mathcal{K}}$ mit $c_i \in \mathbb{Z}$ $(1 \leq i \leq m)$ und $\gamma^p \equiv \beta \mod \mathfrak{p}^n$ gegeben. Dann gilt einerseits

$$\phi(\gamma + \mathfrak{p}^n) = \beta + \mathfrak{p}^n,$$

andererseits gilt nach (4.3) aber auch $\phi(\gamma + \mathfrak{p}^n) = \sum_{i=1}^m c_i\omega_i^p + \mathfrak{p}^n$. Daher existieren $p_1, \ldots, p_m \in \mathbb{Z}$ mit

$$\sum_{i=1}^m c_i\omega_i^p + \sum_{i=1}^m p_i\pi_i = \beta. \tag{4.4}$$

Sei $\underline{\beta} = (b_1, \ldots, b_m)^{\mathrm{tr}} \in \mathbb{Z}^m$ mit $\beta = \sum_{i=1}^m b_i\omega_i$ gegeben. (4.2) impliziert dann

$$\tilde{H}\begin{pmatrix} c_1 \\ \vdots \\ c_m \\ p_1 \\ \vdots \\ p_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Für $\underline{x} := T^{-1}(c_1, \ldots, c_m, p_1, \ldots, p_m)^{\mathrm{tr}}$ erhalten wir somit

$$H\underline{x} = \tilde{H}TT^{-1}\begin{pmatrix} c_1 \\ \vdots \\ c_m \\ p_1 \\ \vdots \\ p_m \end{pmatrix} = \tilde{H}\begin{pmatrix} c_1 \\ \vdots \\ c_m \\ p_1 \\ \vdots \\ p_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Also erfüllt $\underline{x}$ die Bedingung $H\underline{x} = \underline{\beta}$.
Es bleibt zu zeigen, daß

$$\tilde{\gamma} := \sum_{i=1}^{m} (T\underline{x})_i \omega_i$$

eine Lösung von (4.2) ist. Es gilt $\tilde{H}T\underline{x} = \underline{\beta}$ und somit

$$\sum_{i=1}^{m} (T\underline{x})_i \omega_i^p + \sum_{i=m+1}^{2m} (T\underline{x})_i \pi_i = \beta. \tag{4.5}$$

Ferner erhalten wir $\phi(\tilde{\gamma} + \mathfrak{p}^n) = \sum_{i=1}^{m} (T\underline{x})_i \omega_i^p + \mathfrak{p}^p$ aus (4.3). Aus (4.5) folgt mit $\pi := \sum_{i=m+1}^{2m} (T\underline{x})_i \pi_i$ daher

$$\phi(\tilde{\gamma} + \mathfrak{p}^n) = \beta - \pi + \mathfrak{p}^n = \beta + \mathfrak{p}^n.$$

Wir haben also $\tilde{\gamma}^p + \mathfrak{p}^n = \beta + \mathfrak{p}^n$ und somit

$$\tilde{\gamma}^p \equiv \beta \mod \mathfrak{p}^n$$

gezeigt. Um aus der Existenz von $\underline{x}$ auf die Existenz von γ zu schließen betrachten wir den 2.Teil des gerade geführten Beweises. Wir stellen fest, daß wir ausschließlich $H\underline{x} = \underline{\beta}$ verwendet haben. Somit ist der Satz bewiesen. □

Bemerkung 4.3. *Die Aussagen von* 4.1 *und* 4.2 *sind für beliebige algebraische Zahlkörper* $\mathcal{K}$ *richtig. Sie gelten unabhängig von der Bedingung* $\zeta_p \in \mathcal{K}$.

Mit den letzten beiden Aussagen kann die Kongruenz (4.1) für Primidealpotenzen bis $\nu_{\mathfrak{p}}(p)$ gelöst werden. Höhere Potenzen werden durch die folgenden Aussagen behandelt. Für diese werden wir jedoch die zu Beginn dieses Kapitels gemachten Einschränkungen benötigen.

Satz 4.4. *Es sei* $n \in \{\nu_{\mathfrak{p}}(p) + 1, \ldots, \nu_{\mathfrak{p}}(p) + \mathfrak{e}_{\mathfrak{p}} = p\mathfrak{e}_{\mathfrak{p}}\}$, *und für* $m \in o_{\mathcal{F}}$ *gelte*

$$m \equiv 1 \mod \mathfrak{p}^{n-1}.$$

Dann erhalten wir:

(i) *Gilt* $\mathfrak{e}_\mathfrak{p} < p$, *so folgt*

$$\exists c \in o_\mathcal{F} : c^p \equiv m \mod \mathfrak{p}^n \Longleftrightarrow m \equiv 1 \mod \mathfrak{p}^n.$$

(ii) *Gilt* $\mathfrak{e}_\mathfrak{p} \geq p$, *so folgt*

$$\begin{array}{rl} & \exists c \in o_\mathcal{F} : c^p \equiv m \mod \mathfrak{p}^n \\ \Longleftrightarrow & \exists (x + \mathfrak{p}^{\mathfrak{e}_\mathfrak{p}}) \in \mathfrak{p}^{\lceil \mathfrak{e}_\mathfrak{p} - \frac{\mathfrak{e}_\mathfrak{p}}{p} \rceil} / \mathfrak{p}^{\mathfrak{e}_\mathfrak{p}} : (1+x)^p \equiv m \mod \mathfrak{p}^n. \end{array}$$

Beweis. In beiden Fällen ist die Rückrichtung trivial. Es bleiben also lediglich die Hinrichtungen zu zeigen. Sei dazu o.B.d.A. $m \not\equiv 1 \mod \mathfrak{p}^n$ und $c \in o_\mathcal{F}$ mit

$$c^p \equiv m \mod \mathfrak{p}^n$$

gegeben. Dann gilt wegen $m \equiv 1 \mod \mathfrak{p}$ die Beziehung $c^p \equiv 1 \mod \mathfrak{p}$ und daher weiter $c \equiv 1 \mod \mathfrak{p}$, weil die Frobenius Abbildung

$$F : o_\mathcal{F}/\mathfrak{p}_\mathcal{F} \longrightarrow o_\mathcal{F}/\mathfrak{p}_\mathcal{F} : x \mapsto x^p$$

ein Automorphismus ist. Damit hat c die Form $c = 1+x$ mit $x \in \mathfrak{p}$ bzw. $\nu_\mathfrak{p}(x) \geq 1$. Somit erhalten wir

$$c^p = (1+x)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} x^i + x^p,$$

wobei für die einzelnen Summanden

(i) $\nu_\mathfrak{p}\left(\binom{p}{i} x^i\right) = \nu_\mathfrak{p}(p) + i\nu_\mathfrak{p}(x)$ für $1 \leq i < p$,
(ii) $\nu_\mathfrak{p}(x^p) = p\nu_\mathfrak{p}(x)$

gelten. Aus $\nu_\mathfrak{p}(x) \geq 1$ folgt $\nu_\mathfrak{p}\left(\binom{p}{k} x^k\right) \neq \nu_\mathfrak{p}\left(\binom{p}{l} x^l\right)$ für $1 \leq k < l < p$, wodurch

$$\begin{aligned} \nu_\mathfrak{p}\left(\sum_{i=1}^{p-1} \binom{p}{i} x^i\right) &= \min\left\{\nu_\mathfrak{p}\left(\binom{p}{i} x^i\right) \middle| 1 \leq i < p\right\} \\ &= \nu_\mathfrak{p}(p) + \nu_\mathfrak{p}(x) \end{aligned} \tag{4.6}$$

impliziert wird. Ferner gilt $\nu_\mathfrak{p}(x) < \mathfrak{e}_\mathfrak{p}$, denn wegen $\nu_\mathfrak{p}(x) \geq \mathfrak{e}_\mathfrak{p}$ folgt

$$\begin{aligned} \nu_\mathfrak{p}\left(\sum_{i=1}^{p} \binom{p}{i} x^i\right) &\geq \min\{\nu_\mathfrak{p}(p) + \nu_\mathfrak{p}(x), p\nu_\mathfrak{p}(x)\} \\ &\geq \min\{\nu_\mathfrak{p}(p) + \mathfrak{e}_\mathfrak{p}, p\mathfrak{e}_\mathfrak{p}\} \\ &= \min\{\mathfrak{e}_\mathfrak{p}(p-1) + \mathfrak{e}_\mathfrak{p}, p\mathfrak{e}_\mathfrak{p}\} = p\mathfrak{e}_\mathfrak{p} \geq n, \end{aligned}$$

und wir erhalten aus

$$c^p \equiv (1+x)^p \equiv 1 + \sum_{i=1}^{p} \binom{p}{i} x^i \equiv 1 \mod \mathfrak{p}^n$$

die Kongruenz $m \equiv 1 \mod \mathfrak{p}^n$. Dies aber steht im Widerspruch zu unserer Annahme. Also erfüllt $\nu_{\mathfrak{p}}(x)$ stets $\nu_{\mathfrak{p}}(x) < \mathfrak{e}_{\mathfrak{p}}$. Die Äquivalenz „$\nu_{\mathfrak{p}}(p) + \nu_{\mathfrak{p}}(x) = p\nu_{\mathfrak{p}}(x) \Longleftrightarrow \nu_{\mathfrak{p}}(x) = \mathfrak{e}_{\mathfrak{p}}$“ bedeutet speziell $\nu_{\mathfrak{p}}(p) + \nu_{\mathfrak{p}}(x) \neq p\nu_{\mathfrak{p}}(x)$. Daraus folgt

$$\begin{aligned} \nu_{\mathfrak{p}}\left(\sum_{i=1}^{p} \binom{p}{i} x^i\right) &= \min\{\nu_{\mathfrak{p}}(p) + \nu_{\mathfrak{p}}(x), p\nu_{\mathfrak{p}}(x)\} \\ &= p\nu_{\mathfrak{p}}(x). \end{aligned}$$

Aus $m \equiv 1 \mod \mathfrak{p}^{n-1}$ und $m \equiv c^p \mod \mathfrak{p}^n$ erhalten wir $c^p \equiv 1 \mod \mathfrak{p}^{n-1}$. Dies impliziert $\sum_{i=1}^{p} \binom{p}{i} x^i \equiv 0 \mod \mathfrak{p}^{n-1}$, welches zu

$$\nu_{\mathfrak{p}}\left(\sum_{i=1}^{p} \binom{p}{i} x^i\right) \geq n-1$$

äquivalent ist. Wir erhalten schließlich aus

$$\begin{aligned} p\nu_{\mathfrak{p}}(x) &= \nu_{\mathfrak{p}}\left(\sum_{i=1}^{p} \binom{p}{i} x^i\right) \geq n-1 \\ \Leftrightarrow \quad \nu_{\mathfrak{p}}(x) &\geq \frac{n-1}{p} \end{aligned}$$

die Abschätzung

$$\nu_{\mathfrak{p}}(x) \geq \frac{n-1}{p} \geq \frac{\mathfrak{e}_{\mathfrak{p}}(p-1)}{p} = \mathfrak{e}_{\mathfrak{p}} - \frac{\mathfrak{e}_{\mathfrak{p}}}{p}.$$

Gilt nun $\mathfrak{e}_{\mathfrak{p}} < p$, so folgt wegen $\nu_{\mathfrak{p}}(x) \in \mathbb{N}$

$$\nu_{\mathfrak{p}}(x) \geq \mathfrak{e}_{\mathfrak{p}},$$

was nicht möglich ist, da stets $\nu_{\mathfrak{p}}(x) < \mathfrak{e}_{\mathfrak{p}}$ gilt. Also kann für $\mathfrak{e}_{\mathfrak{p}} < p$ der Fall $m \not\equiv 1 \mod \mathfrak{p}^n$ nicht eintreten.

Gilt andererseits $\mathfrak{e}_{\mathfrak{p}} \geq p$, so folgt

$$\mathfrak{e}_{\mathfrak{p}} > \nu_{\mathfrak{p}}(x) \geq \lceil \mathfrak{e}_{\mathfrak{p}} - \frac{\mathfrak{e}_{\mathfrak{p}}}{p} \rceil.$$

Dies bedeutet aber

$$(x + \mathfrak{p}^{\mathfrak{e}_{\mathfrak{p}}}) \in \left(\mathfrak{p}^{\lceil \mathfrak{e}_{\mathfrak{p}} - \frac{\mathfrak{e}_{\mathfrak{p}}}{p} \rceil} / \mathfrak{p}^{\mathfrak{e}_{\mathfrak{p}}}\right) \setminus \{0 + \mathfrak{p}^{\mathfrak{e}_{\mathfrak{p}}}\},$$

wobei wegen $x \notin \mathfrak{p}^{\mathfrak{e}_\mathfrak{p}}$ das Element $0 + \mathfrak{p}^{\mathfrak{e}_\mathfrak{p}}$ ausgeschlossen werden kann.
Insgesamt impliziert dies (unter Berücksichtigung des Falles $m \equiv 1 \mod \mathfrak{p}$, also $x = 0$)

$$(x + \mathfrak{p}^{\mathfrak{e}_\mathfrak{p}}) \in \left(\mathfrak{p}^{\lceil \mathfrak{e}_\mathfrak{p} - \frac{\mathfrak{e}_\mathfrak{p}}{p} \rceil} / \mathfrak{p}^{\mathfrak{e}_\mathfrak{p}}\right).$$

Damit ist der Satz bewiesen. □

Lemma 4.5. *Es seien* $n \in \{\nu_\mathfrak{p}(p) + 1, \ldots, \nu_\mathfrak{p}(p) + \mathfrak{e}_\mathfrak{p} = p\mathfrak{e}_\mathfrak{p}\}$ *sowie* $c \in o_\mathcal{F}$ *mit*

$$c^p \equiv \mu \mod \mathfrak{p}^{n-1}$$

gegeben und für $m \in o_\mathcal{F}$ *gelte* $mc^p \equiv \mu \mod \mathfrak{p}^n$. *Es existiert genau dann ein* $\alpha \in o_\mathcal{F}$ *mit*

$$\alpha^p \equiv \mu \mod \mathfrak{p}^n,$$

wenn ein $\beta \in o_\mathcal{F}$ *mit*

$$\beta^p \equiv m \mod \mathfrak{p}^n$$

existiert. Es kann dann α *als* $c\beta$ *gewählt werden.*

Beweis. „$\Longrightarrow$“: Wir beachten $\nu_\mathfrak{p}(\mu) = 0$. Daraus folgt wegen

$$c^p \not\equiv 0 \mod \mathfrak{p} \text{ und } c \not\equiv 0 \mod \mathfrak{p},$$

daß c eine Einheit in $o_\mathcal{F}(\mathfrak{p})$ ist, und wir erhalten $\frac{\alpha}{c} \in o_\mathcal{F}(\mathfrak{p})$. Setzen wir

$$\tilde{\beta} = \frac{\alpha}{c},$$

so folgt $\nu_\mathfrak{p}\left(\tilde{\beta}^p - m\right) \geq n$, denn es gilt nach Voraussetzung

$$\begin{aligned} n &\leq \nu_\mathfrak{p}(\mu - \alpha^p) = \nu_\mathfrak{p}\left(c^p\left(\left(\frac{\alpha}{c}\right)^p - m\right)\right) \\ &= p\nu_\mathfrak{p}(c) + \nu_\mathfrak{p}\left(\tilde{\beta} - m\right) = \nu_\mathfrak{p}\left(\tilde{\beta}^p - m\right). \end{aligned}$$

Also ist m eine p–te Potenz modulo $\mathfrak{p}^n$ in der $\mathfrak{p}$–adischen Vervollständigung $\mathcal{F}_\mathfrak{p}$ von $\mathcal{F}$. Dann ist m aber auch in $o_\mathcal{F}$ eine p–te Potenz modulo $\mathfrak{p}^n$.
„$\Longleftarrow$“: trivial. □

Lemma 4.6. *Es sei* $\mathcal{K}$ *ein algebraischer Zahlkörper und* $\alpha, c \in o_\mathcal{K}$, $\mathfrak{p} \in \mathbb{P}_\mathcal{K}$ *sowie* $n \in \mathbb{N}$ *gegeben. Gelten dann*

(i) $\alpha \equiv c \mod \mathfrak{p}^n$,
(ii) $c \not\equiv 0 \mod \mathfrak{p}^n$,

so existiert ein $m \in o_{\mathcal{F}}$ *mit*

$$mc \equiv \alpha \mod \mathfrak{p}^{n+1}.$$

BEWEIS. Sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ und $k = \nu_{\mathfrak{p}}(c)$. Dann existiert ein $\tilde{c} \in o_{\mathcal{K}} \setminus \mathfrak{p}$ mit

$$c \equiv \tilde{c}\pi^k \mod \mathfrak{p}^{n+1}.$$

Dann gilt $k < n$ wegen $c \not\equiv 0 \mod \mathfrak{p}^n$ und aus $\tilde{c} \in o_{\mathcal{K}} \setminus \mathfrak{p}$ folgt $\tilde{c} + \mathfrak{p}^{n+1} \in (o_{\mathcal{K}}/\mathfrak{p}^{n+1})^*$. Ist $a \in o_{\mathcal{K}}$ mit $a\pi^n \equiv \alpha - c \mod \mathfrak{p}^{n+1}$ gegeben, so definieren wir $m + \mathfrak{p}^{n+1} \in o_{\mathcal{K}}/\mathfrak{p}^{n+1}$ durch

$$m \equiv 1 + \frac{a}{\tilde{c}}\pi^{n-k} \mod \mathfrak{p}^{n+1}.$$

Dann gilt

$$\begin{aligned} mc &\equiv \left(1 + \frac{a}{\tilde{c}}\pi^{n-k}\right) c \equiv c + \frac{a}{\tilde{c}}\pi^{n-k}\tilde{c}\pi^k \\ &\equiv c + a\pi^n \equiv c + \alpha - c \equiv \alpha \mod \mathfrak{p}^{n+1}, \end{aligned}$$

womit die Behauptung bewiesen ist. □

BEMERKUNG 4.7. (i) *Für ein gegebenes* $k \in \{1, \dots, \mathfrak{e}_{\mathfrak{p}}(p-1)\}$ *liefert der Satz 4.2 unmittelbar einen Algorithmus, der entscheiden kann, ob die Kongruenz (4.1) für k lösbar ist, und gegebenenfalls eine solche Lösung bestimmt.*
(ii) *Für ein* $k \in \{\mathfrak{e}_{\mathfrak{p}}(p-1)+1, \dots, \mathfrak{e}_{\mathfrak{p}}p\}$ *können wir nach Satz 4.4 unser Problem der p–ten Potenzen relativ einfach lösen. Wir formulieren hierzu einen Algorithmus.*

ALGORITHMUS 1. (Entscheidet für $l \in \{\mathfrak{e}_{\mathfrak{p}}(p-1)+1, \dots, \mathfrak{e}_{\mathfrak{p}}p\}$, ob die Kongruenz (4.1) für $k = l$ lösbar ist.)
Eingabe: $l \in \{\mathfrak{e}_{\mathfrak{p}}(p-1)+1, \dots, \mathfrak{e}_{\mathfrak{p}}p\}$ *und eine Lösung* $c \in o_{\mathcal{F}}$ *der Kongruenz (4.1) für* $k = l - 1$
Ausgabe: *„Unlösbar“ oder „Lösbar“ und ein* $\gamma \in o_{\mathcal{F}}$, *daß die Kongruenz (4.1) löst.*

Schritt 1: *Finde gemäß Lemma 4.6 ein* $m \in o_{\mathcal{F}}$ *mit* $mc^p \equiv \mu \mod \mathfrak{p}^l$.

Schritt 2: *Prüfe, ob für m die Kongruenz* $x^p \equiv m \mod \mathfrak{p}^l$ *lösbar ist.*

Schritt 3: *Falls die Kongruenz* $x^p \equiv m \mod \mathfrak{p}^l$ *nicht lösbar ist, terminiere mit „Unlösbar“.*

Schritt 4: *Bestimme* $\tilde{\gamma} \in o_{\mathcal{F}}$ *als Lösung von* $x^p \equiv m \mod \mathfrak{p}^l$.

Schritt 5: *Setze* $\gamma = \tilde{\gamma} c$ *und terminiere mit „Lösbar“.*

BEMERKUNG 4.8. (i) *Da die Abbildung* $\Phi : o_{\mathcal{F}}/\mathfrak{p}^l \longrightarrow o_{\mathcal{F}}/\mathfrak{p}^l \; : \; x \mapsto x(c^p + \mathfrak{p}^l)$ *eine* $\mathbb{Z}$*–lineare Abbildung ist, können wir* m *sehr einfach bestimmen.*

(ii) *Da die Voraussetzungen von Satz* 4.4 *erfüllt sind, kann Schritt 2 mit einem einfachen Test* ($\mathfrak{e}_\mathfrak{p} < p$) *oder durch einige wenige Tests* ($\mathfrak{e}_\mathfrak{p} \geq p$) *gelöst werden.*
Im Fall $\mathfrak{e}_\mathfrak{p} < p$ *ist die Anwendung von Satz* 4.4 *evident. Sonst lasse man* x *ein Restsystem von* $\mathfrak{p}^{\lceil \mathfrak{e}_\mathfrak{p} - \frac{\mathfrak{e}_\mathfrak{p}}{p} \rceil}/\mathfrak{p}^{\mathfrak{e}_\mathfrak{p}}$ *durchlaufen und prüfe für jedes Element des Restsystems, ob* $1 + x$ *die Kongruenz erfüllt. In der Praxis ist dieses Restsystem extrem klein und ohne Probleme zu bewältigen.*

(iii) *Lemma* 4.5 *garantiert die Korrektheit des Algorithmus.*

2. Kummererweiterungen

Wir sind nun in der Lage, Algorithmen anzugeben, die für eine gegebene Kummererweiterung $\mathcal{E}/\mathcal{F}$ von Primzahlgrad die Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ und ein $o_{\mathcal{F}}$–Erzeugendensystem $\xi_1, \dots, \xi_m$ von $o_{\mathcal{E}}$ bestimmen.
Wir benutzen dazu die folgenden Bezeichnungen: Es seien $p \in \mathbb{P}$ und $\mathcal{F}$ ein algebraischer Zahlkörper mit $\zeta_p \in \mathcal{F}$ sowie $\mathcal{E}$ eine Erweiterung von $\mathcal{F}$ mit $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ für ein $\mu \in o_{\mathcal{F}} \setminus \mathcal{P}_p(\mathcal{K})$. Wie schon früher setzen wir

$$\nu_{\mathfrak{p}}(\mu) \in \{0, \dots, p-1\} \quad \forall \mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \text{ mit } \nu_{\mathfrak{p}}(p) > 0$$

für den Erzeuger voraus. Unser Vorgehen ist an den Beweis von Satz 3.29 angelehnt. Wir werden also in einem ersten Schritt die Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ bestimmen und dann für die Primideale, die nicht die Diskriminante teilen, Erzeuger $\rho_1, \rho_2 \in o_{\mathcal{E}}$ ermitteln, so daß

$$o_{\mathcal{E}}(\mathfrak{p}) = \left[1, \rho_1, \dots, \rho_1^{p-1}, \rho_2, \dots, \rho_2^{p-1}\right]_{o_{\mathcal{F}}(\mathfrak{p})}$$

für alle $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}}$ gilt. Dann werden wir für Primideale $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ ein ähnliches System berechnen.
Bei allen angegebenen Algorithmen benötigen wir Standardverfahren der konstruktiven algebraischen Zahlentheorie. Falls wir nicht ausdrücklich auf eine Literaturstelle verweisen, ist der entsprechende Algorithmus in einem der drei Standardwerke [Co, Po93, PoZa89] zu finden.

2.1. Die Diskriminante. Wir werden zunächst einen Algorithmus angeben, der für eine gegebene Kummererweiterung $\mathcal{E}/\mathcal{F}$ die Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ bestimmt. Dies wird in zwei Schritten geschehen. Zuerst werden wir für Primideale $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, für die $\nu_{\mathfrak{p}}(p) > 0$ gilt, die Bewertung $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)$ bestimmen. Analog verfahren wir mit den Primidealen $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid \nu_{\mathfrak{p}}(p) > 0\}$, für die $\nu_{\mathfrak{p}}(\mu) > 0$ gilt. Damit haben wir für alle Primideale $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ die entsprechende Bewertung für die Relativdiskriminante bestimmt, denn es gilt

$$\mathfrak{p} \mid \mathfrak{d}_{\mathcal{E}/\mathcal{F}} \Longrightarrow \mathfrak{p} \mid p\mu.$$

ALGORITHMUS 2. (Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ mit $\nu_{\mathfrak{p}}(p) > 0$ wird $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)$ bestimmt.)
Eingabe: $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ *mit* $\nu_{\mathfrak{p}}(p) > 0$.
Ausgabe: $k_{\mathfrak{p}} \in \mathbb{N}_0$ *mit* $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = k_{\mathfrak{p}}$. *Falls* $\nu_{\mathfrak{p}}(\mu) = 0$ *gilt, wird außerdem ein* $\kappa_{\mathfrak{p}} \in \mathbb{N}$ *und* $\gamma_{\mathfrak{p}} \in o_{\mathcal{F}}$ *mit*

$$\gamma^p \equiv \mu \mod \mathfrak{p}^{\kappa_{\mathfrak{p}}}$$

zurückgegeben. Hierbei ist $\kappa_{\mathfrak{p}}$ maximal mit der Eigenschaft, daß eine solche Kongruenz lösbar ist.

Verzweigung: *Bestimme $\mathfrak{e}_{\mathfrak{p}}$ als Verzweigungsindex von $\mathcal{F}_{\mathfrak{p}}$ über $\mathbb{Q}_p(\zeta_p)$ mit*

$$\nu_{\mathfrak{p}}(p) = \mathfrak{e}_{\mathfrak{p}}(p-1).$$

Test: *Gilt $\nu_{\mathfrak{p}}(\mu) = 0$, so gehe zu „Potenz".*

Direkt: *Setze $k_{\mathfrak{p}} := p\nu_{\mathfrak{p}}(p) + (p-1)$ und terminiere.*

Potenz: *Mittels der Methoden des letzten Abschnitts bestimme:*
(a) $\kappa_{\mathfrak{p}} \in \mathbb{N}$ *mit* $\kappa_{\mathfrak{p}} = \max\{0 < l \leq p\mathfrak{e}_{\mathfrak{p}} \mid \exists c \in o_{\mathcal{F}} : c^p \equiv \mu \mod \mathfrak{p}^l\}$,
(b) $\gamma_{\mathfrak{p}} \in o_{\mathcal{F}} \,:\, \gamma_{\mathfrak{p}}^p \equiv \mu \mod \mathfrak{p}^{\kappa_{\mathfrak{p}}}$.

Bewertung: *Gilt $\kappa_{\mathfrak{p}} = p\mathfrak{e}_{\mathfrak{p}}$, so setze $k_{\mathfrak{p}} = 0$ und terminiere.*
Sonst setze $k_{\mathfrak{p}} = (p-1)(p\mathfrak{e}_{\mathfrak{p}} - \kappa_{\mathfrak{p}} + 1)$ und terminiere.

Wir kommen nun zu den Primidealen, die nicht im letzten Algorithmus behandelt wurden. Diese Ideale sind erheblich einfacher zu behandeln.

ALGORITHMUS 3. (Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ mit $\nu_{\mathfrak{p}}(p) = 0$ und $\nu_{\mathfrak{p}}(\mu) > 0$ wird $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)$ bestimmt.)
Eingabe: $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ *mit* $\nu_{\mathfrak{p}}(p) = 0$ *und* $\nu_{\mathfrak{p}}(\mu) > 0$.
Ausgabe: $k_{\mathfrak{p}} \in \mathbb{N}_0$ *mit* $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = k_{\mathfrak{p}}$.

Test: *Bestimme $l \in \{0, \ldots, p-1\}$ mit $l \equiv \nu_{\mathfrak{p}}(\mu) \mod p$. Gilt $l = 0$, so gehe zu „Index".*

Diskriminante: *Setze $k_{\mathfrak{p}} := p-1$ und terminiere.*

Index: *Setze $k_{\mathfrak{p}} := 0$ und terminiere.*

Damit können wir nun für alle Primideale $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ mit $\nu_{\mathfrak{p}}(p\mu) > 0$ die Bewertung $\nu_{\mathfrak{p}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)$ der Diskriminante bestimmen. Wir sind also in der Lage, für die Kummererweiterung $\mathcal{E}/\mathcal{F}$ die Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ vollständig zu berechnen.

ALGORITHMUS 4. (Die Relativdiskriminante von $\mathcal{E}/\mathcal{F}$.)
Eingabe: *$\mathcal{F}, p$ und μ wie zu Beginn des Abschnitts angegeben.*
Ausgabe: *Die Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}} = \prod_{i=1}^m \mathfrak{p}_i^{k_{\mathfrak{p}_i}}$. Für $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ mit $\nu_{\mathfrak{p}}(p) > 0$ ferner $\kappa_{\mathfrak{p}} \in \mathbb{N}$ und $\gamma_{\mathfrak{p}} \in o_{\mathcal{F}}$ wie in Algorithmus 2.*

Init: *Berechne* $p o_{\mathcal{F}} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ *und* $\mu o_{\mathcal{F}} = \prod_{i=1}^{s} \mathfrak{q}_i^{b_i}$.

Diskriminante p: *Für* $1 \leq i \leq r$ *bestimme* $k_{\mathfrak{p}_i}, \kappa_{\mathfrak{p}_i}$ *und* $\gamma_{\mathfrak{p}_i}$ *gemäß Algorithmus* 2.

Diskriminante μ: *Für* $1 \leq i \leq s$ *bestimme* $k_{\mathfrak{q}_i}$ *für* $\mathfrak{q}_i$ *mit* $\nu_{\mathfrak{q}_i}(p) = 0$ *gemäß Algorithmus* 3 *und setze* $k_{\mathfrak{q}_i} = 0$ *für nicht behandelte* $\mathfrak{q}_i$.

Ende: *Berechne* $\mathfrak{d}_{\mathcal{E}/\mathcal{F}} = \prod_{i=1}^{r} \mathfrak{p}_i^{k_{\mathfrak{p}_i}} \prod_{i=1}^{s} \mathfrak{q}_i^{k_{\mathfrak{q}_i}}$ *und terminiere.*

2.2. Das Erzeugendensystem. Nachdem wir die Diskriminante der Erweiterung bestimmt haben, wenden wir uns der Berechnung der $o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$ zu. Diese Aufgabe werden wir in mehreren Schritten lösen:

(i) Berechne ein $\gamma \in o_{\mathcal{F}}$, das die in Lemma 3.22 angegebenen Eigenschaften hat.
(ii) Bestimme gemäß Lemma 3.25 ein $\delta \in o_{\mathcal{F}}$ sowie ein $\mathfrak{b} \subseteq o_{\mathcal{F}}$ mit
$$\delta o_{\mathcal{F}} = \mathfrak{b}\mathfrak{a}_{\mathcal{E}/\mathcal{F}}.$$
(iii) Für $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ bestimme $\pi_{\mathfrak{p}} \in \mathfrak{p} \setminus \mathfrak{p}^2$ und $\beta_{\mathfrak{p}} \in (\pi_{\mathfrak{p}} o_{\mathcal{F}})\mathfrak{p}^{-1}$ mit $\nu_{\mathfrak{p}}(\beta_{\mathfrak{p}}) = 0$.
(iv) Als letzten Schritt bestimme die in den Lemmata 3.25, 3.27 und 3.28 angegebenen Erzeuger.

Die Berechnung von γ führen wir analog zu den Beweisen von 3.21 und 3.22 durch. Bei der Bestimmung der Diskriminante haben wir für die Primideale $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ mit $\nu_{\mathfrak{p}}(p) > 0$ bereits die beiden Werte $\kappa_{\mathfrak{p}}$ und $\gamma_{\mathfrak{p}}$ bestimmt. Für diese gelten:

(a) $\kappa_{\mathfrak{p}} = \max\{0 < l \leq p\mathfrak{e}_{\mathfrak{p}} \mid \exists c \in o_{\mathcal{F}} : c^p \equiv \mu \mod \mathfrak{p}^l\}$,
(b) $\gamma_{\mathfrak{p}}^p \equiv \mu \mod \mathfrak{p}^{\kappa_{\mathfrak{p}}}$.

Mittels dieser $\gamma_{\mathfrak{p}}$ formulieren wir einen Algorithmus, der ein $\gamma \in o_{\mathcal{F}}$, das den Anforderungen von Lemma 3.22 genügt, berechnet. Dieses Verfahren benutzt den Chinesischen Restsatz konstruktiv. Ein entsprechender Algorithmus hierzu ist in [Da] zu finden.

Algorithmus 5. (Berechnung von γ gemäß Lemma 3.22)
Eingabe: $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid \nu_{\mathfrak{p}}(p) > 0\}$ *und die Werte* $\kappa_{\mathfrak{p}_i}$ *sowie* $\gamma_{\mathfrak{p}_i}$ *mit den obigen Eigenschaften* $(1 \leq i \leq r)$. *Ferner Primideale* $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\} = \{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \setminus \Delta_{\mathcal{E}/\mathcal{F}} \mid \nu_{\mathfrak{q}_j}(\mu) > 0\}$.
Ausgabe: *Ein* $\gamma \in o_{\mathcal{F}}$, *das die Aussage von Lemma 3.22 erfüllt.*

Init: *Berechne* $\mathfrak{a}_1 := \prod_{i=1}^{r} \mathfrak{p}_i^{\kappa_{\mathfrak{p}_i}}$ *und* $\mathfrak{a}_2 := \left(\prod_{j=1}^{s} \mathfrak{q}_j^{\nu_{\mathfrak{q}_j}(\mu)}\right)^{\frac{1}{p}}$.

Teiler von p: *Mittels des Chinesischen Restsatzes bestimme* $\tilde{\gamma} \in o_{\mathcal{F}}$ *mit*

$$\tilde{\gamma} \equiv \gamma_{\mathfrak{p}_i} \mod \mathfrak{a}_1 \quad (1 \leq i \leq r).$$

Teiler von μ: *Bestimme mittels des Chinesischen Restsatzes* $\gamma \in o_{\mathcal{F}}$ *mit*

$$\begin{aligned} \gamma &\equiv \tilde{\gamma} \mod \mathfrak{a}_1, \\ \gamma &\equiv 0 \mod \mathfrak{a}_2 \end{aligned}$$

und terminiere.

Wir schließen diese Serie von Algorithmen, mit der Berechnung eines kompletten $o_{\mathcal{F}}$–Erzeugendensystems von $o_{\mathcal{E}}$.

ALGORITHMUS 6. (Berechnung eines $o_{\mathcal{F}}$–Erzeugendensystems von $o_{\mathcal{E}}$.)
Eingabe: $\mathcal{F}, p$ *und* μ *wie zu Beginn des Abschnitts angegeben.*
Ausgabe: $\Omega \subset o_{\mathcal{E}}$ *mit* $|\Omega| < \infty$ *und* $[\Omega]_{o_{\mathcal{F}}} = o_{\mathcal{E}}$.

Diskriminante: *Bestimme die Diskriminante* $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ *von* $\mathcal{E}/\mathcal{F}$.

Gamma: *Berechne* γ *gemäß Algorithmus* 5.

Index: *Berechne den Hauptindex* $\mathfrak{a}_{\mathcal{E}/\mathcal{F}}$ *von* $\mathcal{E}/\mathcal{F}$. *Dies ist mittels der Faktorisierung der Diskriminante* $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ *möglich.*

Delta: *Wähle* $\delta \in \mathfrak{a}_{\mathcal{E}/\mathcal{F}}$ *und berechne* $\mathfrak{b} = \beta_1 o_{\mathcal{F}} + \beta_2 o_{\mathcal{F}}$ *mit* $\delta o_{\mathcal{F}} = \mathfrak{b}\mathfrak{a}_{\mathcal{E}/\mathcal{F}}$.

Beta: *Für* $\mathfrak{p} \in \Delta_{\mathcal{E}/\mathcal{F}}$ *bestimme* $\pi_{\mathfrak{p}} \in \mathfrak{p} \setminus \mathfrak{p}^2$ *und* $\beta_{\mathfrak{p}} \in (\pi_{\mathfrak{p}} o_{\mathcal{F}})\mathfrak{p}^{-1}$ *mit* $\nu_{\mathfrak{p}}(\beta_{\mathfrak{p}}) = 0$.

Erzeuger 1.1: *Berechne* $\rho_i := \beta_i \frac{\gamma - \sqrt[p]{\mu}}{\delta}$ $(i = 1, 2)$.

Erzeuger 1.2: *Definiere* $\Omega_1 := \{1, \rho_1, \ldots, \rho_1^{p-1}, \rho_2, \ldots, \rho_2^{p-1}\}$.

Erzeuger 2: *Setze* $\Omega_2 := \emptyset$, $P := \Delta_{\mathcal{E}/\mathcal{F}}$.

Anfang While: *Solange* $P \neq \emptyset$:

Auswahl: *Wähle* $\mathfrak{p} \in P$ *und setze* $P := P \setminus \{\mathfrak{p}\}$.

Falls $\nu_{\mathfrak{p}}(\mu) = 0$: *Berechne* $r, s \in Z^{\geq 0}$ *mit* $r\kappa_{\mathfrak{p}} - sp = 1$ *und definiere*

$$\rho_{\mathfrak{p}} = \beta_{\mathfrak{p}}^s \frac{\left(\gamma - \sqrt[p]{\mu}\right)^r}{\pi_{\mathfrak{p}}^s}.$$

Setze $\Omega_2 := \Omega_2 \cup \{\rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1}\}$.

Falls $\nu_{\mathfrak{p}}(p) = 0$: *Sei* $l \in \{1, \ldots, p-1\}$ *so gegeben, daß* $\nu_{\mathfrak{p}}(\mu) \equiv l \mod p$ *gilt. Berechne dann* $r, s \in Z^{\geq 0}$ *mit* $rl - sp = 1$ *und setze* $k := s + r\frac{\nu_{\mathfrak{p}}(\mu)-l}{p}$. *Definiere*

$$\rho_{\mathfrak{p}} = \frac{\beta_{\mathfrak{p}}^k}{\pi_{\mathfrak{p}}^k} \sqrt[p]{\mu}^r.$$

Setze $\Omega_2 := \Omega_2 \cup \{\rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1}\}$.

Sonst: *Finde* $r, s \in Z^{\geq 0}$ *mit* $r\nu_{\mathfrak{p}}(\mu) - sp = 1$ *und definiere*

$$\rho_{\mathfrak{p}} = \frac{\beta_{\mathfrak{p}}^s}{\pi_{\mathfrak{p}}^s} \sqrt[p]{\mu}^r.$$

Setze $\Omega_2 := \Omega_2 \cup \{\rho_{\mathfrak{p}}, \ldots, \rho_{\mathfrak{p}}^{p-1}\}$.

Ende While:

Ende: *Setze* $\Omega := \Omega_1 \cup \Omega_2$ *und terminiere.*

Bemerkung 4.9. (i) *Der hier angegebene Algorithmus ist eine Version, die kaum optimiert ist. Man kann die Berechnung des Erzeugendensystems verbessern. Da dies jedoch nur zu Lasten der Übersichtlichkeit der Darstellung möglich ist, verzichten wir an dieser Stelle auf die Präsentation einer optimierten Fassung. Die wesentlichen Reduktionsideen sind in (ii) aufgeführt.*

(ii) *Man kann schon durch die Wahl des Primelementes* $\pi_{\mathfrak{p}}$ *den für einen Erzeuger* $\rho_{\mathfrak{p}}$ *auftretenden Nenner beeinflussen. Wählt man ein einziges Primelement* π *für alle Primideale, so erhält man Erzeuger, die eng miteinander verbunden sind. Man kann dann einen neuen Erzeuger modulo schon berechneter reduzieren, denn es lassen sich relativ einfach Abhängigkeiten für die so bestimmten Elemente überprüfen. Im allgemeinen sind die Mengen* Ω_1 *und* Ω_2 *dann so gegeben, daß man durch einfache Tests viele Elemente schon bei der Berechnung weglassen oder vereinfachen kann. Ein wichtiger Punkt hierbei ist auch, daß wir* $\sqrt[p]{\mu} \in [\Omega_1]_{o_{\mathcal{F}}}$ *berücksichtigen können.*

(iii) *Durch die in Punkt (ii) angesprochenen Vereinfachungen des Erzeugendensystems bestimmt der Algorithmus in der Praxis bis auf wenige Ausnahmen Systeme von* $o_{\mathcal{F}}$*–Erzeugern von* $o_{\mathcal{E}}$*, die höchstens* $2p$ *Elemente enthalten.*

Wie schon in Bemerkung 3.30 angesprochen, ist es sehr einfach, mittels des Erzeugendensystems Ω eine Ganzheitsbasis von $o_{\mathcal{E}}$ zu bestimmen.

Sei dazu $1 = \eta_1, \ldots, \eta_n$ eine Ganzheitsbasis von $o_{\mathcal{F}}$. Dann wird durch

$$\tilde{\Omega} := \{\eta_i \omega \mid 1 \leq i \leq n,\ \omega \in \Omega\} = \{\tau_1, \ldots, \tau_m\}$$

ein $\mathbb{Z}$–Erzeugendensystem von $o_{\mathcal{E}}$ gegeben. Da

$$\eta_1, \ldots, \eta_n, \eta_1 \sqrt[p]{\mu}, \ldots, \eta_n \sqrt[p]{\mu}, \eta_1 \sqrt[p]{\mu}^{p-1}, \ldots, \eta_n \sqrt[p]{\mu}^{p-1}$$

eine $\mathbb{Q}$–Basis von $\mathcal{E}$ ist, existieren $d \in \mathbb{Z}$ und $\alpha_{i,j} \in \mathbb{Z}$ $(1 \leq i \leq np, 1 \leq j \leq m)$ mit

$$\tau_j = \frac{1}{d} \sum_{k=1}^{n} \sum_{l=0}^{p-1} \alpha_{ln+k,j} \eta_k \sqrt[p]{\mu}^l$$

für $1 \leq j \leq m$. Wir haben also ein Matrix $A = (\alpha_{i,j})_{\substack{1 \leq i \leq pn \\ 1 \leq j \leq m}} \in \mathbb{Z}^{pn \times m}$ erhalten, durch die wir mittels einer Hermite–Normalform eine Ganzheitsbasis von $o_{\mathcal{E}}$ berechnen können. Da sogar $\eta_1, \ldots, \eta_n \sqrt[p]{\mu}^{p-1} \in [\tau_1, \ldots, \tau_m]_{\mathbb{Z}}$ gilt, können wir die Basis auch mittels einer d–modularen Hermite–Normalform berechnen. Dies führt zu einer erheblichen Beschleunigung des Verfahrens [Br].

Neben der Berechnung einer Ganzheitsbasis bietet sich auch eine andere Art der Normalisierung für das Erzeugendensystem Ω an. Hierbei handelt es sich um eine Verallgemeinerung der Hermite–Normalform auf beliebige Dedekindringe. Mittels des Erzeugendensystems Ω bestimmt man Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_p$ und algebraische Zahlen $\xi_1, \ldots, \xi_p$, für die

$$[\Omega]_{o_{\mathcal{F}}} = \mathfrak{a}_1 \xi_1 + \ldots + \mathfrak{a}_p \xi_p$$

gilt. Im Gegensatz zur Hermite - Normalform ist diese Normalform jedoch nicht eindeutig. Ein Algorithmus hierzu ist in [BoPo] zu finden. Eine Implementierung des Verfahrens für algebraische Zahlkörper hat gezeigt, daß die in Zwischenrechnungen auftretenden Zahlen explosionsartig an Größe zunehmen. Dies ist ein ähnliches Phänomen, wie es auch bei der Berechnung einer Hermite–Normalform bekannt ist.
Das folgende Beispiel macht deutlich, wie die Koeffizienten schon bei einer relativ einfachen Rechnung explodieren:

Beispiel 4.10. *Betrachten wir den Körper $\mathcal{F} = \mathbb{Q}(\rho)$, wobei ρ eine Nullstelle von*

$$f(t) = t^6 + 5t^5 - 6t^4 - 53t^3 + 3t^2 + 206t + 244$$

sei, so hat $\mathcal{F}$ die Körperdiskriminante -182099043 und eine Ganzheitsbasis wird durch

$$\omega_1, \ldots, \omega_6 = 1, \rho, \rho^2, \rho^3, \frac{1}{2}(\rho + \rho^4), \frac{1256 + 120\rho + 487\rho^2 + 140\rho^3 + 596\rho^4 + \rho^5}{2740}$$

gegeben. Untersuchen wir die Erweiterung $\mathcal{E} = \mathcal{F}(\sqrt[3]{\mu})$ *mit* $\mu = \omega_1 + \ldots + \omega_6$*, so wird* $o_{\mathcal{E}}$ *als* $o_{\mathcal{F}}$*–Modul von den Elementen*

$$
\begin{aligned}
\tau_1 &= 1,\\
\tau_2 &= \sqrt[3]{\mu},\\
\tau_3 &= \sqrt[3]{\mu}^2,\\
\tau_4 &= \frac{1}{3}\left((\omega_1+\omega_2+2\omega_3+2\omega_5+2\omega_6)+(\omega_1+\omega_2+2\omega_3+2\omega_5+2\omega_6)\sqrt[3]{\mu}\right),\\
\tau_5 &= \frac{1}{3}\left((2\omega_2+2\omega_6)+(2\omega_1+\omega_3+\omega_5+2\omega_6)\sqrt[3]{\mu}+(2\omega_1+\omega_2+\omega_3+\omega_5)\sqrt[3]{\mu}^2\right),\\
\tau_6 &= \frac{1}{2}\left((\omega_1+\omega_5)\sqrt[3]{\mu}^2\right),\\
\tau_7 &= \frac{1}{2}\left((\omega_2+\omega_4)\sqrt[3]{\mu}^2\right)
\end{aligned}
$$

erzeugt. Berechnet man eine „Normalform“ dieses Erzeugendensystems, so treten Zwischenergebnisse mit bis zu 50 Stellen auf. Als Ergebnis erhält man

$$o_{\mathcal{E}} = \mathfrak{a}_1\xi_1 + \mathfrak{a}_2\xi_2 + \mathfrak{a}_3\xi_3$$

mit

$$
\begin{aligned}
\xi_1 = {}& \frac{1}{6}(\omega_1 - (2060274517369288\omega_1 - 912854687610440\omega_2 + 1156993464445939\omega_3\\
&+279964773427774\omega_4 + 2371281121332741\omega_5 - 4914930015962230\omega_6)\sqrt[3]{\mu}\\
&-(151777746902012\omega_1 + 28998299161880\omega_2 + 76537039291445\omega_3\\
&+6784635624828\omega_4 + 105979160114635\omega_5 - 123703110092175\omega_6)\sqrt[3]{\mu}^2),\\
\xi_2 = {}& \frac{1}{6}(\omega_1\sqrt[3]{\mu} + (6122175302073640609480975588028\omega_1 - 2640319035966486185180773436244\omega_2\\
&+2514113625548012304659486327334\omega_3 + 7740959948705185157685708728848\omega_4\\
&+6090495748491686725541438608474\omega_5 - 1400840142689692655384215188436 0\omega_6)\sqrt[3]{\mu}^2),\\
\xi_3 = {}& \frac{1}{2}\omega_1\sqrt[3]{\mu}^2
\end{aligned}
$$

und

$$
\begin{aligned}
\mathfrak{a}_1 &= 6o_{\mathcal{F}} + (30\omega_1+28\omega_2+36\omega_3+36\omega_4+36\omega_5+34\omega_6)o_{\mathcal{F}},\\
\mathfrak{a}_2 &= 6o_{\mathcal{F}} + (28\omega_1+34\omega_2+32\omega_3+36\omega_4+32\omega_5+26\omega_6)o_{\mathcal{F}},\\
\mathfrak{a}_3 &= 2o_{\mathcal{F}} + (2\omega_1+2\omega_2+2\omega_3+\omega_4+3\omega_5+4\omega_6)o_{\mathcal{F}}.
\end{aligned}
$$

Durch einfache technische Modifikationen [DaPo95] *kann man bei der Berechnung der* ξ_i *eine Explosion der Koeffizienten weitestgehend vermeiden. Bei dem obigen Beispiel haben dann alle Zwischenergebnisse weniger als 10 Stellen und im Endergebnis sind alle Koeffizienten der* ξ_i $(1 \le i \le 3)$ *bei gleichen Idealen* $\mathfrak{a}_i$ $(1 \le i \le 3)$

einstellig:

$$\begin{aligned}
\xi_1 &= \frac{1}{6}(\omega_1 + (2\omega_1 + 2\omega_2 + 5\omega_3 + 2\omega_4 + 3\omega_5 + 4\omega_6)\sqrt[3]{\mu} + (4\omega_1 + 4\omega_2 + \omega_3 + 5\omega_5 + 3\omega_6)\sqrt[3]{\mu}^2),\\
\xi_2 &= \frac{1}{6}(\omega_1\sqrt[3]{\mu} + (2\omega_1 + 2\omega_4 + 4\omega_5 + 2\omega_6)\sqrt[3]{\mu}^2),\\
\xi_3 &= \frac{1}{2}\omega_1\sqrt[3]{\mu}^2.
\end{aligned}$$

2.3. Allgemeine Kummererweiterungen. Wir untersuchen nun beliebige Kummererweiterungen $\mathcal{E}/\mathcal{F}$, und wollen einen Algorithmus angeben, der für eine solche Erweiterung eine Ganzheitsbasis und ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ bestimmt.
Im weiteren sei $n = p_1 \cdot \ldots \cdot p_m \in \mathbb{N}$ mit $p_i \in \mathbb{P}$ $(1 \leq i \leq m)$, und $\mathcal{F}$ sei ein algebraischer Zahlkörper mit $\zeta_n \in \mathcal{F}$. Wir untersuchen eine Erweiterung $\mathcal{E}$ von Grad n über $\mathcal{F}$, für die

$$\mathcal{E} = \mathcal{F}(\sqrt[n]{\mu})$$

mit $\mu \in o_{\mathcal{F}}$ gilt.
Es wird extrem wichtig sein, für die gegebene Relativerweiterung $\mathcal{E}/\mathcal{F}$ zunächst ein irreduzibles und normiertes Polynom $f(t) \in \mathbb{Z}[t]$ zu finden, so daß für eine Nullstelle ρ dieses Polynoms

$$\mathbb{Q}(\rho) =: \tilde{\mathcal{E}} \simeq \mathcal{E}$$

gilt. Weiter benötigen wir auch einen Isomorphismus $\phi : \mathcal{E} \longrightarrow \tilde{\mathcal{E}}$. Sowohl $f(t)$ als auch ϕ lassen sich durch einen von B. Trager in [Tr] veröffentlichten Algorithmus berechnen. Da wir diesen Algorithmus später nochmals anwenden werden, sei schon hier angemerkt, daß das Verfahren auf beliebige Relativerweiterungen angewendet werden kann.

Algorithmus 7. (Berechnung einer Ganzheitsbasis und eines $o_{\mathcal{F}}$–Erzeugendensystems für $o_{\mathcal{E}}$.)
Eingabe: *$\mathcal{F}, n$ und μ wie oben angegeben.*
Ausgabe: *$\Omega_1, \Omega_2 \subset o_{\mathcal{E}}$, so daß Ω_1 eine Ganzheitsbasis und Ω_2 ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ ist.*

Init 1: $\Omega_2 := \{1\}$.

Init 2: $\mathcal{K} := \mathcal{F}, \eta := \mu$.

Primzahlen: *Berechne $p_1, \ldots, p_m \in \mathbb{P}$ mit $n = p_1 \cdot \ldots \cdot p_m$.*

Anfang Schleife: *Für $1 \leq i \leq m$:*

S 1: $\mathcal{L} := \mathcal{K}(\sqrt[p_i]{\eta})$.

S 2: *Bestimme für* $o_{\mathcal{L}}$ *eine Ganzheitsbasis* $\tilde{\Upsilon}_1$ *und ein* $o_{\mathcal{K}}$*–Erzeugendensystem* $\tilde{\Upsilon}_2$.

S 3: *Berechne ein irreduzibles und normiertes Polynom* $f(t) \in \mathbb{Z}[t]$, *so daß* $\mathbb{Q}(\rho) =: \tilde{\mathcal{L}} \simeq \mathcal{L}$ *für eine Nullstelle* ρ *von* $f(t)$ *gilt. Berechne ferner einen Isomorphismus* $\phi : \mathcal{L} \longrightarrow \tilde{\mathcal{L}}$.

S 4: $\Upsilon_j := \phi(\tilde{\Upsilon}_j)$ *für* $j = 1, 2$.

S 5: $\Omega_1 := \Upsilon_1$.

S 6: $\Omega_2 := \{\omega v \mid \omega \in \Omega_2$ *und* $v \in \Upsilon_2\}$.

S 7: $\mathcal{K} := \tilde{\mathcal{L}}$, $\eta := \phi(\sqrt[p_i]{\eta})$.

Ende Schleife:

Ende: *Terminiere.*

Bemerkung 4.11. *Mit dem gerade angegebenen Algorithmus kann man auch für Kummererweiterungen vom allgemeinen Typ (vgl. Satz* 3.1*) eine Ganzheitsbasis und ein relatives Erzeugendensystem bestimmen.*

3. Radikalerweiterungen

Eine interessante Anwendung von Kummererweiterungen sind Radikalrweiterungen. Wir sind in der Lage, einen Algorithmus anzugeben, der eine Ganzheitsbasis für eine beliebige Radikalerweiterung bestimmen kann, wenn eine solche Basis für eine passende Kummererweiterung bekannt ist. Hierbei verstehen wir unter einer Radikalerweiterung eines algebraischen Zahlkörpers $\mathcal{K}$ einen Zahlkörper $\mathcal{L}$, für den $\mathcal{L} = \mathcal{K}(\sqrt[n]{\eta})$ mit passendem $\eta \in o_{\mathcal{K}}$ und minimalem $n \in \mathbb{N}$ gilt. Das folgende Diagramm zeigt das zugehörige Teilkörpergitter.

$$\begin{tikzcd}[arrows=dash]
 & & & \mathcal{E} = \mathcal{F}(\sqrt[n]{\eta}) \arrow[dl] \arrow[dd] & \\
 & & \mathcal{L} = \mathcal{K}(\sqrt[n]{\eta}) \arrow[dd] & & \\
 & & & \mathcal{F} \arrow[dl] \arrow[dr] & \\
r & s & \mathcal{K} \arrow[dr] & & \mathbb{Q}(\zeta_n) \arrow[dl] \\
 & & & \mathcal{M} = \mathcal{K} \cap \mathbb{Q}(\zeta_n) \arrow[d] & \\
 & & & \mathbb{Q} &
\end{tikzcd}$$

In Übereinstimmung mit diesem Diagramm vereinbaren wir die folgenden Bezeichnungen für diesen Paragraphen:
Es sei $\mathcal{K}$ ein algebraischer Zahlkörper, und es gelte $\mathcal{L} = \mathcal{K}(\sqrt[n]{\eta})$ mit $[\mathcal{L} : \mathcal{K}] = n$ für ein $\eta \in o_{\mathcal{K}}$. Ferner seien $\mathcal{F} = \mathcal{K}\mathbb{Q}(\zeta_n)$ und $\mathcal{E} = \mathcal{F}(\sqrt[n]{\eta})$. Desweiteren bezeichnen wir mit $\omega_1, \dots, \omega_r$ eine Ganzheitsbasis von $\mathcal{E}$ und mit $\delta_1, \dots, \delta_l$ eine Ganzheitsbasis von $\mathcal{K}$. Außerdem definieren wir die $\mathbb{Q}$–Basis $\alpha_1, \dots, \alpha_r$ von $\mathcal{E}$ durch

$$\gamma_1, \dots, \gamma_k, \sqrt[n]{\eta}\gamma_1, \dots, \sqrt[n]{\eta}\gamma_k, \dots, \sqrt[n]{\eta}^{n-1}\gamma_1, \dots, \sqrt[n]{\eta}^{n-1}\gamma_k$$

und mit $\beta_1, \dots, \beta_s$ die $\mathbb{Q}$–Basis

$$\delta_1, \dots, \delta_l, \sqrt[n]{\eta}\delta_1, \dots, \sqrt[n]{\eta}\delta_l, \dots, \sqrt[n]{\eta}^{n-1}\delta_1, \dots, \sqrt[n]{\eta}^{n-1}\delta_l$$

von $\mathcal{L}$.
Wegen $\mathcal{L} \subseteq \mathcal{E}$ existiert eine Matrix $D \in \mathbb{Z}^{r\times s}$ mit

$$(\beta_1, \ldots, \beta_s) = (\alpha_1, \ldots, \alpha_r)D. \tag{4.7}$$

Um diese Matrix explizit zu berechnen, reicht es, eine Einbettung von $\mathcal{K}$ in $\mathcal{F}$ zu finden. Wie man eine solche Einbettung bestimmt, wurde schon im Abschnitt über Kummererweiterungen in diesem Kapitel diskutiert.
Wir führen von jetzt an alle Berechnungen in $\mathcal{E}$ bzw. in $\mathcal{L}$ in der Basis $\alpha_1, \ldots, \alpha_r$ von $\mathcal{E}$ bzw. $\beta_1, \ldots, \beta_s$ von $\mathcal{F}$ durch. Um $o_{\mathcal{L}} = \mathcal{L} \cap o_{\mathcal{E}}$ zu bestimmen, seien Elemente $\tilde{b}_i, b_i$ und a_j $(1 \leq i \leq s, 1 \leq j \leq r)$ (in den Basen $\alpha_1, \ldots, \alpha_r$ bzw. $\beta_1, \ldots, \beta_s$) mit den folgenden Eigenschaften gegeben:

(1) $b_1, \ldots, b_s \in \mathcal{L}$ mit $o_{\mathcal{L}} \subseteq b_1\mathbb{Z} + \ldots + b_s\mathbb{Z}$,
(2) $\tilde{b}_1, \ldots, \tilde{b}_s \in \mathcal{E}$ mit $\tilde{b}_i = b_i$ (in $\mathcal{E}$) für $1 \leq i \leq s$,
(3) $a_1, \ldots, a_r \in \mathcal{E}$ mit $o_{\mathcal{E}} + \tilde{b}_1\mathbb{Z} + \ldots + \tilde{b}_s\mathbb{Z} \subseteq a_1\mathbb{Z} + \ldots + a_r\mathbb{Z}$.

Wir werden nun klären, wie wir die Elemente $\tilde{b}_i, b_i$ und a_j $(1 \leq i \leq s, 1 \leq j \leq r)$ wählen können.

(1) Wir können $b_1, \ldots, b_s \in \mathcal{L}$ als
$$\delta_1, \ldots, \delta_l, \frac{1}{n^n\eta^{n-1}}\sqrt[n]{\eta}\delta_1, \ldots, \frac{1}{n^n\eta^{n-1}}\sqrt[n]{\eta}\delta_l, \ldots, \frac{1}{n^n\eta^{n-1}}\sqrt[n]{\eta}^{n-1}\delta_1, \ldots, \frac{1}{n^n\eta^{n-1}}\sqrt[n]{\eta}^{n-1}\delta_l$$
wählen, denn es gilt [Ne]
$$(n^n\eta^{n-1})o_{\mathcal{L}} \subseteq \sqrt[n]{\eta}o_{\mathcal{F}} + \ldots + \sqrt[n]{\eta}^{n-1}o_{\mathcal{F}}.$$
(2) Gilt $b_i = \sum_{j=1}^{s} \gamma_{j,i}\beta_j$ mit $\gamma_{j,i} \in \mathbb{Z}$ $(1 \leq j \leq s)$, so erhalten wir $\tilde{b}_i = \sum_{j=1}^{r} \tilde{\gamma}_{j,i}\alpha_j$ mittels
$$\begin{pmatrix} \tilde{\gamma}_{1,i} \\ \vdots \\ \tilde{\gamma}_{r,i} \end{pmatrix} = D \begin{pmatrix} \gamma_{1,i} \\ \vdots \\ \gamma_{s,i} \end{pmatrix}$$
für $1 \leq i \leq s$.
(3) Da $o_{\mathcal{E}} + \tilde{b}_1\mathbb{Z} + \ldots + \tilde{b}_s\mathbb{Z}$ ein freier $\mathbb{Z}$–Modul von vollem Rang in $\mathcal{E}$ ist, finden wir mittels einer Hermite–Normalform Elemente $a_1, \ldots, a_r \in \mathcal{E}$.

Wir erhalten dann Matrizen $M \in \mathbb{Z}^{r\times r}$ und $N \in \mathbb{Z}^{r\times s}$ mit
$$\begin{aligned}(\omega_1, \ldots, \omega_r) &= (a_1, \ldots, a_r)M,\\ (\tilde{b}_1, \ldots, \tilde{b}_s) &= (a_1, \ldots, a_r)N.\end{aligned}$$

Der nächste Satz liefert uns einen Algorithmus zur Bestimmung von $o_{\mathcal{L}} = \mathcal{L} \cap o_{\mathcal{E}}$.

SATZ 4.12. *Es gilt* $x = \sum_{i=1}^{s} x_i \tilde{b}_i \in o_{\mathcal{L}} = \mathcal{L} \cap o_{\mathcal{E}}$ *genau dann, wenn* $y_1, \ldots, y_r \in \mathbb{Z}$ *existieren mit*

$$\underline{0} = (N| - M)(x_1, \ldots, x_s, y_1, \ldots, y_r)^{tr}.$$

Es gilt dann

$$o_{\mathcal{L}} = \{x = \sum_{i=1}^{s} x_i b_i \mid \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} \in \mathbb{Z}^s : \exists y_1, \ldots, y_r \in \mathbb{Z}^r : \begin{pmatrix} x_1 \\ \vdots \\ x_s \\ y_1 \\ \vdots \\ y_r \end{pmatrix} \in Ker(N| - M)\}.$$

BEWEIS. „$\Longrightarrow$“: Es sei $x = \sum_{i=1}^{s} x_i \tilde{b}_i \in \mathcal{L} \cap o_{\mathcal{E}}$ gegeben. Wegen $x \in o_{\mathcal{E}}$ existieren $y_1, \ldots, y_r \in \mathbb{Z}$ mit

$$x = \sum_{i=1}^{r} y_i \omega_i,$$

und mit der Definition von N und M erhalten wir

$$\text{(i)}\ x = (\tilde{b}_1, \ldots, \tilde{b}_s) \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = (a_1, \ldots, a_r) N \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix},$$
$$\text{(ii)}\ x = (\omega_1, \ldots, \omega_r) \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = (a_1, \ldots, a_r) M \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}.$$

Aus (i) und (ii) ergibt sich nun wegen

$$\begin{aligned} 0 = x - x &= (a_1, \ldots, a_r) N \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} - (a_1, \ldots, a_r) M \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} \\ &= (a_1, \ldots, a_r) \left(N \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} - M \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} \right) \end{aligned}$$

die Behauptung.
„$\Longleftarrow$“: Aus der Voraussetzung folgt

$$N \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = M \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}.$$

Daher gilt $x = (\tilde{b}_1, \dots, \tilde{b}_s)(x_1, \dots, x_s)^{\mathrm{tr}} = (a_1, \dots, r)M(y_1, \dots, y_r)^{\mathrm{tr}} \in o_{\mathcal{E}}$. Hieraus folgt wegen $x \in \mathcal{L}$ die Behauptung.
Da $\tilde{b}_i = b_i$ für $1 \le i \le s$ gilt, ist die Aussage über $o_{\mathcal{L}}$ evident. $\square$

BEMERKUNG 4.13. *Die Ausführungen dieses Kapitels führen direkt zu einem Algorithmus. Wir verzichten hier deshalb auf eine schematische Darstellung der Vorgehensweise.*

Zum Abschluß des Abschnitts geben wir noch ein kurzes Beispiel.

BEISPIEL 4.14. *Es sei $\mathcal{K} = \mathbb{Q}(\rho)$ durch eine Nullstelle ρ des Polynoms*

$$f(t) = t^4 + 65$$

definiert. Dieser Körper hat die Diskriminante $\mathfrak{d}_{\mathcal{K}} = 70304000$, eine Ganzheitsbasis von $\mathcal{F}$ wird durch $1, \rho, \rho^2, \rho^3$ gegeben und für die Klassenzahl von $\mathcal{K}$ gilt

$$h_{\mathcal{K}} = 128.$$

Wir wollen nun eine Ganzheitsbasis des Körpers $\mathcal{L} = \mathcal{K}(\mu)$ mit $\mu = \sqrt[3]{10}$ berechnen. Dazu bestimmen wir den Körper $\mathcal{F} = \mathcal{K}(\zeta_3)$ und für die Kummererweiterung $\mathcal{E} = \mathcal{F}(\mu)$ eine Ganzheitsbasis. Ein primitives Element von $\mathcal{F}$ ist z.B. eine Nullstelle δ des Polynoms

$$g(t) = t^8 + 4t^7 + 10t^6 + 16t^5 + 149t^4 + 276t^3 - 380t^2 - 516t + 4161.$$

Damit ergibt sich für $o_{\mathcal{F}}$ die Ganzheitsbasis:

$$\begin{aligned} \omega_1, \dots, \omega_6 &= 1, \delta, \dots, \delta^5, \\ \omega_7 &= \frac{1}{d}(222388 + 2108494\delta + 83920\delta^2 + 104904\delta^3 \\ &\quad +1395174\delta^4 + 3147\delta^5 + 1049\delta^6), \\ \omega_8 &= \frac{1}{d}(197142 + 150164\delta + 130051\delta^2 + 181030\delta^3 \\ &\quad +179522\delta^4 + 150802\delta^5 + 528\delta^6 + \delta^7) \end{aligned}$$

mit $d = 263299$. *Als Diskriminante dieses Körpers erhalten wir dann* $\mathfrak{d}_{\mathcal{F}} = 400354845696000000$ *und für* $o_{\mathcal{E}}$ *wurde das folgende* $o_{\mathcal{F}}$*–Erzeugendensystem aus* 9 *Elementen berechnet:*

$$\begin{aligned}
\xi_1, \xi_2, \xi_3 &= 1, \mu, \mu^2, \\
\xi_4 &= \frac{1}{3}((2\omega_2 + 2\omega_4 + \omega_5) + (\omega_2 + \omega_4 + \omega_5)\mu), \\
\xi_5 &= \frac{1}{3}((2\omega_1 + 2\omega_3 + \omega_4 + \omega_5 + \omega_8) + (\omega_1 + \omega_2 + \omega_4 + 2\omega_6 + \omega_7 + \omega_8)\mu \\
&\quad + (2\omega_2 + \omega_3 + \omega_4 + 2\omega_5 + \omega_6 + 2\omega_7 + \omega_8)\mu^2), \\
\xi_6 &= \frac{1}{2}(\omega_1 + \omega_4 + \omega_5 + \omega_7)\mu, \\
\xi_7 &= \frac{1}{2}(\omega_1 + \omega_3 + \omega_5)\mu^2, \\
\xi_8 &= \frac{1}{5}(2\omega_1 + \omega_2 + 3\omega_3 + \omega_4 + 4\omega_5 + 3\omega_7)\mu, \\
\xi_9 &= \frac{1}{5}(3\omega_2 + 3\omega_3 + 3\omega_4 + 3\omega_5 + 2\omega_7)\mu^2.
\end{aligned}$$

Mittels der gerade beschriebenen Vorgehensweise erhält man dann die folgende Ganzheitsbasis $\alpha_1, \dots, \alpha_{12}$ *für* $o_{\mathcal{L}}$*:*

$$\begin{aligned}
\alpha_1, \dots, \alpha_4 &= 1, \dots, \rho^3, \\
\alpha_5, \alpha_6, \alpha_7 &= \mu, \rho\mu, \rho^2\mu, \\
\alpha_8 &= \frac{1}{10}(5 + 5\rho + 5\rho^2 + \rho^3)\mu, \\
\alpha_9 &= \frac{1}{3}(1 + \mu + \mu^2), \\
\alpha_{10} &= \frac{1}{3}(\rho + \rho\mu + \rho\mu^2), \\
\alpha_{11} &= \frac{1}{30}((20 + 10\rho^2) + (20 + 10\rho^2)\mu + (5 + \rho^2)\mu^2), \\
\alpha_{12} &= \frac{1}{30}((20\rho + 10\rho^3) + (15 + 5\rho + 15\rho^2 + \rho^3)\mu + (5\rho + \rho^3)\mu^2).
\end{aligned}$$

Daraus ergibt sich für $\mathcal{L}$ *die Diskriminante*

$$\mathfrak{d}_{\mathcal{L}} = 281465470718115840000000000.$$

KAPITEL 5

Anwendung

Wir werden nun eine größere Anzahl von Beispielen präsentieren. Da die berechneten Datenmengen extrem umfangreich sind, können wir nur wenige ausführlich diskutieren. Dies werden wir im ersten Abschnitt tun. Im zweiten Abschnitt dieses Kapitels werden wir einige Tabellen aufführen, in denen statistische Informationen zu den gemachten Rechnungen wiedergegeben werden.
Alle Algorithmen wurden in dem Computeralgebrasystem **KANT V4** [Ka] implementiert und alle Rechnungen wurden auf einer HP9000/735 mit 96MB RAM unter HPUX 9.01 durchgeführt.

1. Beispiele

Wir wollen in diesem Abschnitt einige Kummererweiterungen von Primzahlgrad ausführlicher untersuchen.
Dazu betrachten wir zunächst den von einer Nullstelle ρ des Polynoms

$$f(t) = t^{12} + 2t^{11} + 15t^{10} + 24t^9 + 87t^8 + 102t^7 + 223t^6 + 138t^5 + 167t^4 + 4t^3 + 179t^2 + 66t + 43$$

erzeugten Körper $\mathcal{F}$, welcher zu $\mathbb{Q}(\zeta_7, \sqrt{2})$ isomorph ist. Eine Ganzheitsbasis dieses Körpers wird durch

$$\begin{aligned}
\omega_1, \dots, \omega_{11} &= 1, \dots, \rho^{10}, \\
\omega_{12} &= \frac{1}{d}(5890278886148 + 4276397788932\rho + 8748874411789\rho^2 \\
&\quad +6405183876073\rho^3 + 5683481457604\rho^4 + 7140919061033\rho^5 \\
&\quad +6283701086835\rho^6 + 2111895174273\rho^7 + 6548924083001\rho^8 \\
&\quad +14605458356344\rho^9 + 11942118405614\rho^{10} + \rho^{11})
\end{aligned}$$

mit $d = 15329045383457$ gegeben, woraus sich

$$\mathfrak{d}_{\mathcal{F}} = 74049191673856$$

für die Diskriminante von $\mathcal{F}$ ergibt.
Wir gehen nun auf die Erweiterung $\mathcal{E} = \mathcal{F}(\mu)$ mit $\mu = \sqrt[7]{10}$ näher ein. Dies ist ein Körper vom Grad 84 und wegen $\mathrm{ggT}(\mathfrak{d}_{\mathcal{F}}, \mathfrak{d}(\mathbb{Q}(\sqrt[7]{10}))) = 2^6 7^7 \neq 1$ kann weder die Diskriminante noch eine Ganzheitsbasis unmittelbar angegeben werden.
Zunächst bestimmen wir eine Zerlegung der Ideale $7o_{\mathcal{F}}$ und $\mu o_{\mathcal{F}}$ in Primideale. Es gelten:

$$\begin{aligned}
7o_{\mathcal{F}} &= (7o_{\mathcal{F}} + (\omega_1 + 5\omega_2 + \omega_3)o_{\mathcal{F}})^6 \\
&=: \mathfrak{q}^6, \\
\mu o_{\mathcal{F}} &= (2o_{\mathcal{F}} + (\omega_1 + \omega_2 + \omega_4)o_{\mathcal{F}})^2 \\
&\quad \cdot (2o_{\mathcal{F}} + (\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}})^2 \\
&\quad \cdot (5o_{\mathcal{F}} + (3\omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_6 + \omega_7)o_{\mathcal{F}}) \\
&\quad \cdot (5o_{\mathcal{F}} + (\omega_1 + \omega_3 + 4\omega_4 + 4\omega_5 + \omega_6 + \omega_7)o_{\mathcal{F}}) \\
&=: \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_4.
\end{aligned}$$

Der Verzweigungsindex von $\mathbb{Q}_7(\zeta_7)$ in $\mathcal{F}_{\mathfrak{q}}$ ist damit 1, und da $\sqrt[7]{10}$ in $o_{\mathcal{F}}/\mathfrak{q}^6$ aber nicht mehr in $o_{\mathcal{F}}/\mathfrak{q}^7$ eine 7–te Potenz ist, erhalten wir

$$\nu_{\mathfrak{q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = (7-1)(1\cdot 7 - 6 + 1) = 12.$$

Für die Primideale $\mathfrak{p}_i$ $(i = 1, 2, 3, 4)$ gilt ferner

$$\nu_{\mathfrak{p}_i}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) = 6,$$

woraus sich schließlich

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}} = \mathfrak{q}^{12}\mathfrak{p}_1^6\mathfrak{p}_2^6\mathfrak{p}_3^6\mathfrak{p}_4^6 = 612500o_{\mathcal{F}}$$

für die Relativdiskriminante ergibt. Für die Absolutdiskriminante folgt somit

$$\begin{aligned}
|\mathfrak{d}_{\mathcal{E}}| &= |\mathfrak{d}_{\mathcal{F}}|^7 \,\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right) \\
&= 340341862437633348234343528311961823957354971174452410 8 \\
&\quad 3080290701801649984310660300106725718143410347442176 \cdot 10^{73}.
\end{aligned}$$

Das Verfahren bestimmt dann 19 Elemente $\alpha_1, \ldots, \alpha_{19} \in o_{\mathcal{E}}$, für die

$$o_{\mathcal{E}} = [\alpha_1, \ldots, \alpha_{19}]_{o_{\mathcal{F}}}$$

gilt. Diese Erzeuger führen auf die Normalform ([BoPo]):

$$o_{\mathcal{E}} = \mathfrak{a}_1\xi_1 + \ldots \mathfrak{a}_7\xi_7,$$

wobei die Elemente $\xi_1, \dots, \xi_7 \in o_{\mathcal{E}}$ und die Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_7 \in \mathcal{I}_{\mathcal{F}}$ wie folgt gegeben sind:

$$
\begin{aligned}
\xi_1 &= \frac{1}{14}(1+\\
&\quad (2+5\omega_2+8\omega_3+2\omega_4+11\omega_5+\omega_6+2\omega_7+10\omega_8+2\omega_9+5\omega_{10}+2\omega_{11}+9\omega_{12})\mu\\
&\quad +(5+11\omega_2+3\omega_3+6\omega_4+8\omega_5+5\omega_6+2\omega_7+11\omega_8+3\omega_{10}+12\omega_{11}+8\omega_{12})\mu^2\\
&\quad +(1+11\omega_2+12\omega_3+12\omega_4+7\omega_5+4\omega_6+12\omega_7+2\omega_8+\omega_9+12\omega_{10}+\omega_{11}+10\omega_{12})\mu^3\\
&\quad +(6+8\omega_2+4\omega_3+\omega_4+\omega_5+5\omega_6+13\omega_7+10\omega_8+5\omega_{10}+\omega_{11}+9\omega_{12})\mu^4\\
&\quad +(2+8\omega_2+\omega_3+9\omega_4+3\omega_5+9\omega_6+2\omega_7+11\omega_8+3\omega_{10}+5\omega_{11}+13\omega_{12})\mu^5\\
&\quad +(2+11\omega_2+12\omega_3+13\omega_4+4\omega_5+13\omega_6+13\omega_7+8\omega_8+6\omega_{10}+6\omega_{12})\mu^6),\\
\xi_2 &= \frac{1}{14}(\mu+\\
&\quad +(3+2\omega_2+\omega_3+10\omega_4+5\omega_5+12\omega_6+8\omega_7+3\omega_8+12\omega_9+5\omega_{10}+11\omega_{11}+5\omega_{12})\mu^2\\
&\quad +(13+10\omega_2+10\omega_3+\omega_4+10\omega_5+3\omega_6+10\omega_7+3\omega_8+3\omega_9+10\omega_{10}+4\omega_{11}+4\omega_{12})\mu^3\\
&\quad +(7+10\omega_2+6\omega_3+8\omega_4+13\omega_5+4\omega_6+13\omega_7+\omega_8+4\omega_9+13\omega_{11})\mu^4\\
&\quad +(1+\omega_2+3\omega_3+13\omega_5+3\omega_6+4\omega_7+5\omega_8+8\omega_9+\omega_{10}+6\omega_{11}+5\omega_{12})\mu^5\\
&\quad +(8+7\omega_2+7\omega_4+12\omega_5+6\omega_6+5\omega_7+10\omega_8+8\omega_9+5\omega_{10}+9\omega_{11}+11\omega_{12})\mu^6),\\
\xi_3 &= \frac{1}{14}(\mu^2+\\
&\quad +(12+\omega_2+3\omega_3+7\omega_4+11\omega_5+7\omega_7+4\omega_8+5\omega_9+3\omega_{10}+10\omega_{11}+4\omega_{12})\mu^3\\
&\quad +(6+6\omega_2+8\omega_3+11\omega_4+3\omega_5+8\omega_6+11\omega_7+2\omega_8+8\omega_9+10\omega_{11}+9\omega_{12})\mu^4\\
&\quad +(2+11\omega_2+3\omega_3+5\omega_4+4\omega_5+8\omega_6+4\omega_7+11\omega_8+4\omega_9+\omega_{10}+10\omega_{11}+11\omega_{12})\mu^5\\
&\quad +(1+12\omega_2+11\omega_3+11\omega_5+11\omega_6+11\omega_7+2\omega_8+3\omega_9+4\omega_{10}+7\omega_{11}+8\omega_{12})\mu^6),\\
\xi_4 &= \frac{1}{14}(\mu^3+\\
&\quad +(11+2\omega_2+2\omega_3+10\omega_4+9\omega_5+13\omega_6+7\omega_7+6\omega_8+5\omega_9+\omega_{10}+9\omega_{11}+7\omega_{12})\mu^4\\
&\quad +(5+\omega_2+13\omega_3+13\omega_4+7\omega_5+10\omega_6+12\omega_7+6\omega_8+7\omega_9+2\omega_{10}+6\omega_{11}+13\omega_{12})\mu^5\\
&\quad +(12+2\omega_2+9\omega_3+7\omega_4+9\omega_5+10\omega_6+8\omega_8+7\omega_9+10\omega_{10}+\omega_{11}+3\omega_{12})\mu^6),\\
\xi_5 &= \frac{1}{14}(\mu^4+\\
&\quad +(11+4\omega_3+5\omega_4+11\omega_5+5\omega_6+11\omega_7+7\omega_9+9\omega_{10}+6\omega_{11}+2\omega_{12})\mu^5\\
&\quad +(5+6\omega_2+\omega_3+\omega_4+6\omega_5+2\omega_6+8\omega_7+5\omega_8+2\omega_9+3\omega_{10}+13\omega_{11}+9\omega_{12})\mu^6),\\
\xi_6 &= \frac{1}{2}\mu^5,\\
\xi_7 &= \frac{1}{2}\mu^6,\\
\mathfrak{a}_1 &= 14o_{\mathcal{F}},\\
\mathfrak{a}_2 &= 14o_{\mathcal{F}}+(2\omega_9-6\omega_{10}-4\omega_{11}-10\omega_{12})o_{\mathcal{F}},\\
\mathfrak{a}_3 &= 14o_{\mathcal{F}}+(91\omega_1+91\omega_2+91\omega_3+91\omega_4+91\omega_5+90\omega_6+92\omega_7+95\omega_8+92\omega_9\\
&\quad +95\omega_{10}+93\omega_{11}+97\omega_{12})o_{\mathcal{F}},
\end{aligned}
$$

$$\begin{aligned}
\mathfrak{a}_4 &= 14o_{\mathcal{F}} + (2\omega_4 - 4\omega_5 - 8\omega_6 - 2\omega_7 - 10\omega_8 - 8\omega_9 - 12\omega_{10} - 12\omega_{11} - 8\omega_{12})o_{\mathcal{F}}, \\
\mathfrak{a}_5 &= 14o_{\mathcal{F}} + (\omega_2 - 3\omega_3 - 2\omega_4 + 6\omega_5 - 10\omega_6 - 14\omega_7 - 14\omega_8 - 7\omega_9 - 19\omega_{10} - 20\omega_{11} - 2\omega_{12})o_{\mathcal{F}}, \\
\mathfrak{a}_6 &= 2o_{\mathcal{F}} + (\omega_5 - \omega_6 - \omega_7 - \omega_8 - \omega_9 - \omega_{10} - \omega_{11} - \omega_{12})o_{\mathcal{F}}, \\
\mathfrak{a}_7 &= 2o_{\mathcal{F}} + (\omega_5 - \omega_6 - \omega_7 - \omega_8 - \omega_9 - \omega_{10} - \omega_{11} - \omega_{12})o_{\mathcal{F}}.
\end{aligned}$$

Für die Berechnung des $o_{\mathcal{F}}$–Erzeugendensystems waren 82 Sekunden nötig, wovon 15 Sekunden auf die Bestimmung der Diskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ entfielen. Für die Berechnung der oben angegebenen Normalform wurden weitere 1756 Sekunden Rechenzeit beansprucht, so daß sich eine Gesamtrechenzeit von 1838 Sekunden ergibt. Im Vergleich hierzu benötigt die Berechnung einer Ganzheitsbasis mittels des $o_{\mathcal{F}}$–Erzeugendensystems insgesamt nur 95 Sekunden.

Bei unserem nächsten Grundkörper handelt es sich um den 37–ten Kreisteilungskörper $\mathbb{Q}(\zeta_{37})$. Die Klassenzahl dieses Körpers ist 37 [Wa] und die Diskriminante von $\mathbb{Q}(\zeta_{37})$ beträgt

$$\mathfrak{d}_{\mathbb{Q}(\zeta_{37})} = 37^{35}.$$

Wir wollen nun für $\mathcal{E} = \mathbb{Q}(\zeta_{37})(\sqrt[37]{10})$ ein relatives Erzeugendensystem und eine Ganzheitsbasis bestimmen. Da der Absolutgrad dieses Körpers 1332 ist, verzichten wir jedoch auf die genaue Angabe des vollständigen Ergebnisses.
Es konnte ein Erzeugendensystem aus 73 Elementen in 46859 Sekunden berechnet werden, wobei 439 Sekunden für die Bestimmung der Relativdiskriminante nötig waren. Dabei ergab sich für die Absolutdiskriminante:

$$\begin{aligned}
|\mathfrak{d}_{\mathcal{E}}| = {} & 5392085867231775301615665603434809501157497168761540760968077902150789224 \\
& 7874457539208586723177530161566560343480950115749716876154076096807790215 \\
& 0789224787445751345677671131555793271722850362965242698873019264426937221 \\
& 5878842304038007474410972630386807317550945573645724159688760716497941261 \\
& 2090500729678160275487913324996810506810469462936076552582985657579296000 \\
& 8158439436106396589184155776025640101264786491585901542565691464927994114 \\
& 0557944253505162679377423955459596647379737388620182832549144616797843635 \\
& 4703237338939008786810096599715345194636054954881408039853470130882414116 \\
& 6535110380106474641029962810125846371389311087700337020315146831597739134 \\
& 5752013538179363726723631634713228261858731442514415491204918909264899690 \\
& 3248733790462974696940275964476631121417730610070894668507147943955336702 \\
& 8503517642418823193633601587237942488281844062869024964514234201126349035 \\
& 6890223862346770013005969173132346466275587643481291673766633128377239549 \\
& 3759931406019138400533656411297124080228775594672487309077107305862517957 \\
& 9904452234041793459057511548706617014559459042132459346129215593510081416 \\
& 5764902546581211778556518279964190775271922936497985805231401591040975702
\end{aligned}$$

$$
\begin{aligned}
&4866971841106009386272697285477706129592026359580883912116550615253015845\\
&3861155272718932519295321772317258802402645822010983543333331390965842500\\
&7348413195250179033012396450899965951532273220945524660184938445695200227\\
&7640144964105033459220323418411384186249572365097162449041295284040433167\\
&9139936832526448943067821184325481969527586719641099816296040478625986400\\
&4226828602162610898704046122711679933730389452476622130389290049631277109\\
&7217985468957164491732873793857990791833591424331646943019532711127890691\\
&0206125257687478365375677327036462881689552167359871968160822076564376485\\
&6432351973643063241536870402046826345129880431743350779560254455686746643\\
&1988655597931160330286212254850430616562210235701413063075615027600857056\\
&6778212139069140363334298377925801181568332981472842642255205200719149964\\
&5423223919498128705116104062418246280694829962253769565441581460335024909\\
&8548230728063137686006060366447214340153384576250173700013550596325591878\\
&6174990789031708016800601456827761452868830262445527497677483103927995923\\
&4353695885334893306633507830256333 \cdot 10^{1296},
\end{aligned}
$$

wobei diese Diskriminante 3440 Stellen hat. Für die Berechnung einer Ganzheitsbasis von $\mathcal{E}$ waren dann weitere 79154 Sekunden nötig.

2. Tabellen

In diesem Abschnitt werden wir einige Tabellen zu verschiedenen Folgen ähnlich erzeugter Relativerweiterungen angeben. Vor jeder Tabelle wird der entsprechende Grundkörper $\mathcal{F}$ und der Grad p der betrachteten Erweiterung angegeben. Die Tabellen umfassen dann die folgenden Daten:

(1) Den Erzeuger μ der Relativerweiterung. Wir untersuchen den Körper $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$.
(2) Die Diskriminante $\mathfrak{d}_{\mathcal{E}}$. Da dieser Wert in fast allen Beispielen extrem groß ist, geben wir aus Gründen der Übersichtlichkeit nur $\log_{10}(|\mathfrak{d}_{\mathcal{E}}|)$ (auf 6 Stellen gerundet) an.
(3) Ebenso geben wir den Logarithmus

$$\log_{10}\left[\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)\right]$$

der Norm der Relativdiskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ an.
(4) Wir bestimmen für die Erweiterung $\mathcal{E}/\mathcal{F}$ ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$. Die Größe dieses Erzeugendensystems wird in der Spalte „♯ Erzeuger“ angegeben. Ist die Anzahl der Erzeuger mit einem „(P)“ versehen, so besitzt die entsprechende Erweiterung eine relative Potenzganzheitsbasis.

(5) t_1 : Die komplette Rechenzeit zur Bestimmung eines relativen Erzeugendensystems. Diese Zeit beinhaltet nicht die Berechnung der angegebenen Ganzheitsbasis von $\mathcal{F}$.
(6) t_2 : Die komplette Rechenzeit zur Bestimmung einer Ganzheitsbasis. (Die Zeit t_2 beinhaltet also auch die Rechenzeit t_1 zur Bestimmung eines $o_{\mathcal{F}}$–Erzeugendensystems).

Wir beginnen mit dem Grundkörper $\mathcal{F} = \mathbb{Q}(\rho)$, der von einer Nullstelle ρ des Polynoms

$$f(t) = t^4 - 14t^2 + 169$$

erzeugt wird. Es gilt $\mathcal{F} = \mathbb{Q}(\zeta_3, \sqrt{10})$. Eine Ganzheitsbasis des Körpers wird durch

$$\begin{aligned}
\omega_1 &= 1, \\
\omega_2 &= \rho, \\
\omega_3 &= \frac{1}{52}\left(39 + 26\rho + 13\rho^2\right), \\
\omega_4 &= \frac{1}{52}\left(26 + 51\rho + \rho^3\right)
\end{aligned}$$

gegeben. Die Körperdiskriminante $\mathfrak{d}_{\mathcal{F}}$ beträgt somit 14400 und für die Klassenzahl $h_{\mathcal{F}}$ erhalten wir 4. Die folgende Tabelle gibt einen Überblick über Erweiterungen von $\mathcal{F}$, die in der Form

$$\mathcal{E} = \mathcal{F}(\sqrt[3]{2 + p\omega_2 + \omega_3 + \omega_4})$$

mit $p \in \mathbb{P}$ parametrisiert sind.

Erzeuger	$\log_{10}(\lvert\mathfrak{d}_{\mathcal{E}}\rvert)$	$\log_{10}\left[\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)\right]$	$\sharp$ Erzeuger	t_1	t_2
$2+503\omega_2+\omega_3+\omega_4$	41.417256	28.942168	5	1.400sec	1.470sec
$2+509\omega_2+\omega_3+\omega_4$	43.366808	30.891721	4	3.089sec	3.139sec
$2+521\omega_2+\omega_3+\omega_4$	41.539030	29.063943	5	3.130sec	3.189sec
$2+523\omega_2+\omega_3+\omega_4$	44.415029	31.939941	3(P)	2.160sec	2.199sec
$2+541\omega_2+\omega_3+\omega_4$	44.532238	32.057151	3(P)	2.660sec	2.689sec
$2+547\omega_2+\omega_3+\omega_4$	44.570446	32.095358	3(P)	2.780sec	2.809sec
$2+557\omega_2+\omega_3+\omega_4$	41.770478	29.295390	5	3.259sec	3.309sec
$2+563\omega_2+\omega_3+\omega_4$	43.716082	31.240994	4	2.260sec	2.300sec
$2+569\omega_2+\omega_3+\omega_4$	43.752808	31.277721	4	1.379sec	1.420sec
$2+571\omega_2+\omega_3+\omega_4$	44.719207	32.244120	3(P)	1.519sec	1.550sec
$2+577\omega_2+\omega_3+\omega_4$	42.527536	30.052449	4	2.450sec	2.490sec
$2+587\omega_2+\omega_3+\omega_4$	43.860714	31.385627	4	2.859sec	2.909sec
$2+593\omega_2+\omega_3+\omega_4$	41.987465	29.512378	5	1.960sec	2.030sec
$2+599\omega_2+\omega_3+\omega_4$	43.930833	31.455746	4	2.649sec	2.709sec
$2+601\omega_2+\omega_3+\omega_4$	44.896626	32.421538	3(P)	1.649sec	1.679sec
$2+607\omega_2+\omega_3+\omega_4$	44.931048	32.455960	3(P)	1.510sec	1.539sec
$2+613\omega_2+\omega_3+\omega_4$	44.965132	32.490045	3(P)	0.660sec	0.690sec
$2+617\omega_2+\omega_3+\omega_4$	44.033428	31.558341	4	2.419sec	2.489sec
$2+619\omega_2+\omega_3+\omega_4$	44.998885	32.523798	3(P)	1.500sec	1.539sec
$2+631\omega_2+\omega_3+\omega_4$	45.065423	32.590336	3(P)	2.120sec	2.140sec
$2+641\omega_2+\omega_3+\omega_4$	44.165672	31.690585	4	2.460sec	2.500sec
$2+643\omega_2+\omega_3+\omega_4$	45.130711	32.655624	3(P)	1.490sec	1.530sec
$2+647\omega_2+\omega_3+\omega_4$	42.289476	29.814389	5	3.079sec	3.149sec
$2+653\omega_2+\omega_3+\omega_4$	44.229953	31.754866	4	2.060sec	2.100sec
$2+659\omega_2+\omega_3+\omega_4$	44.261653	31.786566	4	2.100sec	2.159sec
$2+661\omega_2+\omega_3+\omega_4$	45.226398	32.751311	3(P)	2.380sec	2.429sec
$2+673\omega_2+\omega_3+\omega_4$	45.288756	32.813669	3(P)	1.509sec	1.539sec
$2+677\omega_2+\omega_3+\omega_4$	44.355054	31.879966	4	2.190sec	2.240sec
$2+683\omega_2+\omega_3+\omega_4$	42.477153	30.002065	5	1.950sec	2.020sec
$2+691\omega_2+\omega_3+\omega_4$	45.380244	32.905157	3(P)	0.980sec	1.010sec
$2+701\omega_2+\omega_3+\omega_4$	42.567321	30.092234	5	1.679sec	1.739sec
$2+709\omega_2+\omega_3+\omega_4$	45.469384	32.994297	3(P)	1.849sec	1.879sec
$2+719\omega_2+\omega_3+\omega_4$	42.655208	30.180121	5	3.189sec	3.250sec
$2+727\omega_2+\omega_3+\omega_4$	45.556295	33.081207	3(P)	1.540sec	1.579sec
$2+733\omega_2+\omega_3+\omega_4$	45.584788	33.109701	3(P)	1.370sec	1.390sec
$2+739\omega_2+\omega_3+\omega_4$	45.613050	33.137963	3(P)	2.940sec	2.980sec
$2+743\omega_2+\omega_3+\omega_4$	44.677522	32.202434	4	4.290sec	4.349sec
$2+751\omega_2+\omega_3+\omega_4$	45.668893	33.193806	3(P)	2.420sec	2.449sec
$2+757\omega_2+\omega_3+\omega_4$	45.696482	33.221394	3(P)	1.450sec	1.480sec
$2+761\omega_2+\omega_3+\omega_4$	44.760511	32.285423	4	3.009sec	3.069sec
$2+769\omega_2+\omega_3+\omega_4$	45.751010	33.275923	3(P)	1.299sec	1.329sec

Erzeuger	$\log_{10}(\lvert\mathfrak{d}_{\mathcal{E}}\rvert)$	$\log_{10}\left[\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)\right]$	$\sharp$ Erzeuger	t_1	t_2
$2+773\omega_2+\omega_3+\omega_4$	42.906270	30.431183	5	1.940sec	2.000sec
$2+787\omega_2+\omega_3+\omega_4$	45.831231	33.356144	3(P)	1.710sec	1.740sec
$2+797\omega_2+\omega_3+\omega_4$	44.920768	32.445681	4	2.509sec	2.559sec
$2+809\omega_2+\omega_3+\omega_4$	43.064101	30.589013	5	3.310sec	3.370sec
$2+811\omega_2+\omega_3+\omega_4$	45.935390	33.460302	3(P)	1.859sec	1.889sec
$2+821\omega_2+\omega_3+\omega_4$	45.023642	32.548554	4	2.150sec	2.200sec
$2+823\omega_2+\omega_3+\omega_4$	45.986321	33.511234	3(P)	2.150sec	2.180sec
$2+827\omega_2+\omega_3+\omega_4$	43.140406	30.665319	5	1.410sec	1.480sec
$2+829\omega_2+\omega_3+\omega_4$	46.011510	33.536422	3(P)	2.030sec	2.060sec
$2+839\omega_2+\omega_3+\omega_4$	45.098846	32.623759	4	2.619sec	2.689sec
$2+853\omega_2+\omega_3+\omega_4$	46.110476	33.635388	3(P)	2.700sec	2.730sec
$2+857\omega_2+\omega_3+\omega_4$	45.172457	32.697369	4	2.180sec	2.229sec
$2+859\omega_2+\omega_3+\omega_4$	46.134783	33.659696	3(P)	1.689sec	1.719sec
$2+863\omega_2+\omega_3+\omega_4$	43.288166	30.813079	5	2.090sec	2.159sec
$2+877\omega_2+\omega_3+\omega_4$	46.206701	33.731613	3(P)	1.129sec	1.159sec
$2+881\omega_2+\omega_3+\omega_4$	43.359755	30.884667	5	2.310sec	2.379sec
$2+883\omega_2+\omega_3+\omega_4$	46.230346	33.755259	3(P)	2.329sec	2.359sec
$2+887\omega_2+\omega_3+\omega_4$	45.291779	32.816691	4	2.979sec	3.030sec
$2+907\omega_2+\omega_3+\omega_4$	46.323351	33.848264	3(P)	2.030sec	2.060sec
$2+911\omega_2+\omega_3+\omega_4$	45.384371	32.909283	4	2.549sec	2.609sec
$2+919\omega_2+\omega_3+\omega_4$	46.368937	33.893849	3(P)	0.830sec	0.870sec
$2+929\omega_2+\omega_3+\omega_4$	45.452230	32.977143	4	3.469sec	3.520sec
$2+937\omega_2+\omega_3+\omega_4$	46.436212	33.961125	3(P)	1.560sec	1.590sec
$2+941\omega_2+\omega_3+\omega_4$	45.496745	33.021657	4	3.269sec	3.329sec
$2+947\omega_2+\omega_3+\omega_4$	43.290903	30.815816	5	3.190sec	3.260sec
$2+953\omega_2+\omega_3+\omega_4$	43.632211	31.157124	5	2.639sec	2.750sec
$2+967\omega_2+\omega_3+\omega_4$	46.545522	34.070435	3(P)	2.290sec	2.300sec
$2+971\omega_2+\omega_3+\omega_4$	43.697113	31.222026	5	2.969sec	3.039sec
$2+977\omega_2+\omega_3+\omega_4$	45.626965	33.151878	4	2.659sec	2.719sec
$2+983\omega_2+\omega_3+\omega_4$	45.648202	33.173114	4	1.930sec	1.979sec
$2+991\omega_2+\omega_3+\omega_4$	46.630560	34.155472	3(P)	1.550sec	1.580sec
$2+997\omega_2+\omega_3+\omega_4$	46.651498	34.176410	3(P)	1.760sec	1.789sec

Aus Platzgründen geben wir für zusätzlich berechnete Erweiterungen des Körpers $\mathcal{F}$ nur noch eine Statistik über die Anzahl der erhaltenen Erzeuger.

Erzeuger	Parameter $p \in \mathbb{P} \cap P$	Anzahl Körper	Anzahl Erzeuger 3	4	5	6
$2+p\omega_2+\omega_3+\omega_4$	$P=[0,\dots,1500]$	239	111	87	41	0
$2+2\omega_2+p\omega_3+\omega_4$	$P=[0,\dots,1500]$	239	116	117	5	1
$2+2\omega_2+2\omega_3+p\omega_4$	$P=[0,\dots,1500]$	239	235	3	1	0
$4987+124387\omega_2+p\omega_3+232\omega_4$	$P=[0,\dots,400]$	78	38	39	1	0

Als nächstes betrachten wir einen Körper $\mathcal{F}$ vom Grad 8, der durch Adjunktion von ζ_5 an $\mathbb{Q}(\delta)$ definiert ist. Hierbei ist δ eine Nullstelle des Polynoms

$$\tilde{f}(t) = t^4 - 2t^3 - 93t^2 + 94t + 2129.$$

Der Körper $\mathcal{F}$ kann durch eine Nullstelle ρ von

$$f(t) = t^8 + 14t^7 - 102t^6 - 1710t^5 + 4901t^4 + 76040t^3 - 173153t^2 - 1222667t + 3470531$$

erzeugt werden. Für die Diskriminante von $\mathcal{F}$ gilt

$$\mathfrak{d}_{\mathcal{F}} = 18534101265625$$

und eine Ganzheitsbasis ist durch

$$\begin{aligned} \omega_1, \ldots, \omega_7 &= 1, \rho, \ldots, \rho^6, \\ \omega_8 &= \frac{1}{d}(28195785118845 + 8910153667115\rho + 22941493323808\rho^2 \\ &\quad +23934646815337\rho^3 + 21259953214218\rho^4 + 26507464821450\rho^5 \\ &\quad +915838371932\rho^6 + \rho^7) \end{aligned}$$

mit $d = 34768395319361$ gegeben. Wir untersuchen Erweiterungen $\mathcal{E}$ vom Grad 5 über $\mathcal{F}$, die mittels

$$\tilde{\mu} = 2 + \omega_2 + \omega_3 + \omega_4 + \omega_5 + \omega_6 + \omega_7$$

durch

$$\mathcal{E} = \mathcal{F}\left(\sqrt[5]{\tilde{\mu} + p\omega_8}\right)$$

mit $p \in \mathbb{P}$ parametrisiert sind.

Erzeuger	$\log_{10}(\lvert\mathfrak{d}_{\mathcal{E}}\rvert)$	$\log_{10}\left[\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)\right]$	$\sharp$ Erzeuger	t_1	t_2
$\tilde{\mu} + 2\omega_8$	250.433277	184.093419	8	2037sec	2039sec
$\tilde{\mu} + 3\omega_8$	247.968124	181.628266	13	105sec	108sec
$\tilde{\mu} + 5\omega_8$	251.059460	184.719603	8	786sec	787sec
$\tilde{\mu} + 7\omega_8$	250.914881	184.575023	8	126sec	128sec
$\tilde{\mu} + 11\omega_8$	302.982473	236.642616	9	589sec	591sec
$\tilde{\mu} + 13\omega_8$	156.459579	90.119722	13	162sec	165sec
$\tilde{\mu} + 17\omega_8$	283.276658	216.936800	8	481sec	483sec
$\tilde{\mu} + 19\omega_8$	283.276658	216.936800	7	489sec	490sec
$\tilde{\mu} + 23\omega_8$	251.801304	185.461446	13	321sec	324sec
$\tilde{\mu} + 29\omega_8$	254.597184	188.257326	7	409sec	410sec
$\tilde{\mu} + 31\omega_8$	258.616004	192.276146	9	1194sec	1196sec
$\tilde{\mu} + 37\omega_8$	264.780813	198.440955	8	1733sec	1735sec
$\tilde{\mu} + 41\omega_8$	186.900718	120.560861	9	322sec	324sec
$\tilde{\mu} + 43\omega_8$	353.305158	286.965300	13	1070sec	1073sec
$\tilde{\mu} + 47\omega_8$	268.938218	202.598361	8	1077sec	1078sec
$\tilde{\mu} + 53\omega_8$	320.832679	254.492821	13	1255sec	1258sec

Erzeuger	$\log_{10}(\lvert\mathfrak{d}_{\mathcal{E}}\rvert)$	$\log_{10}\left[\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)\right]$	$\sharp$ Erzeuger	t_1	t_2
$\tilde{\mu}+59\omega_8$	251.498747	185.158889	7	409sec	409sec
$\tilde{\mu}+61\omega_8$	270.363832	204.023974	9	1170sec	1172sec
$\tilde{\mu}+67\omega_8$	274.626750	208.286892	8	1162sec	1163sec
$\tilde{\mu}+71\omega_8$	272.727062	206.387204	9	709sec	711sec
$\tilde{\mu}+73\omega_8$	273.153829	206.813971	13	6875sec	6878sec
$\tilde{\mu}+79\omega_8$	279.839783	213.499925	7	453sec	453sec
$\tilde{\mu}+83\omega_8$	277.043903	210.704045	13	481sec	484sec
$\tilde{\mu}+89\omega_8$	385.511322	319.171464	7	2269sec	2270sec
$\tilde{\mu}+97\omega_8$	175.479805	109.139947	8	219sec	220sec

Ähnlich wie schon für das letzte Beispiel, geben wir auch hier noch einige statistische Informationen über weitere Kummererweiterungen des Grundkörpers.

Erzeuger	Parameter $p \in \mathbb{P} \cap P$	Anzahl Körper	Anzahl Erzeuger 5	7	8	9	12	13
$2+\omega_2+\omega_3+\omega_4+\omega_5+\omega_6+\omega_7+p\omega_8$	$P=[0,\dots,100]$	25	0	5	8	5	0	7
$2+\omega_2+\omega_3+\omega_4+\omega_5+\omega_6+\omega_7+p\omega_8$	$P=[200,\dots,300]$	16	15	1	0	0	0	0
$1+p\omega_4$	$P=[200,\dots,300]$	16	15	0	1	0	0	0
$2+2\omega_3+2\omega_5+p\omega_7$	$P=[100,\dots,250]$	28	15	2	5	5	1	0

In unserem letzten Beispiel benutzen wir als Grundkörper $\mathcal{F}$ den 23–ten Kreisteilungskörper $\mathbb{Q}(\zeta_{23})$. Dieser Körper hat die Klassenzahl $h_{\mathcal{F}}=2$ und es gilt

$$\mathfrak{d}_{\mathcal{F}} = -39471584120695485887249589623.$$

Wir untersuchen nun einige Kummererweiterungen $\mathcal{E}=\mathcal{F}(\sqrt[23]{p})$, die durch $p \in \mathbb{P}$ parametrisiert sind. Die folgende Tabelle gibt einen Überblick über solche Erweiterungen.

Erzeuger	$\log_{10}(\mathfrak{d}_{\mathcal{E}})$	$\log_{10}\left[\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}\right)\right]$	$\sharp$ Erzeuger	t_1	t_2
53	1552.180090	894.465546	45	1844sec	5309sec
59	1574.722943	917.008398	45	1931sec	5405sec
61	1581.730210	924.015665	45	1869sec	5320sec
67	1601.450774	943.736229	45	1861sec	5330sec
71	1613.639610	955.925066	45	1905sec	5388sec
73	1619.478834	961.764289	45	1910sec	5401sec
79	1636.082082	978.367537	45	1873sec	5367sec
83	1646.464366	988.749821	45	1865sec	5361sec
89	1661.135333	1003.420788	45	1868sec	5368sec
97	1679.228089	1021.513544	45	1849sec	5345sec

Bezeichnungen

$\mathbb{N}$	Menge der natürlichen Zahlen $\{1, 2, \dots\}$
$\mathbb{P}$	Menge der Primzahlen
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
R^*	Die Einheiten des Ringes R
$\lvert M\rvert$ bzw. $\sharp M$	Anzahl der Elemente in der Menge M
HNF(H)	Hermite Normalform der Matrix $H \in \mathbb{Z}^{n\times m}$
$[a_1, \dots, a_k]_R$	$a_1R + \dots + a_kR$
p, q	Primzahlen
$\nu_p(a)$	Exponent von p in der Primfaktorzerlegung von $a \in \mathbb{Z} \setminus \{0\}$
$\mathbb{Z}(p)$	Menge der p–ganzen Elemente in $\mathbb{Q}$ $(= \{a \in \mathbb{Q} \mid \nu_p(a) \geq 0\})$
a_{ij} bzw. $A(i, j)$	Element der Matrix A an der Stelle (i, j)
$\mathcal{F}, \mathcal{E}, \mathcal{K}, \mathcal{L}, \mathcal{M}$	algebraische oder lokale Zahlkörper
$o_{\mathcal{F}}, o_{\mathcal{E}}$, etc.	Ganzheitsringe der entsprechenden Körper
$U_{\mathcal{F}}, U_{\mathcal{E}}$, etc.	Einheitengruppen von $o_{\mathcal{F}}, o_{\mathcal{E}}$, etc.
$\mathbb{P}_{\mathcal{F}}, \mathbb{P}_{\mathcal{E}}$, etc.	Mengen der Primideale der entsprechenden Körper
$o_{\mathcal{F}}(\mathfrak{p})$	für ein $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$: Menge der $\mathfrak{p}$–ganzen Elemente in $\mathcal{F}$ $(= \{\alpha \in \mathcal{F} \mid \nu_{\mathfrak{p}}(\alpha) \geq 0\})$
$o_{\mathcal{E}}(\mathfrak{p})$	für ein $\mathfrak{p} \notin \mathbb{P}_{\mathcal{E}}$: Menge der $\mathfrak{p}$–ganzen Elemente in $\mathcal{E}$ $(= \{\alpha \in \mathcal{E} \mid \nu_{\mathfrak{P}}(\alpha) \geq 0\ \forall \mathfrak{P} \in \mathbb{P}_{\mathcal{E}}\ :\ \mathfrak{p}o_{\mathcal{E}} \subseteq \mathfrak{P}\})$
α, β	(ganz) algebraische Zahlen
ζ_n	eine primitive n–te Einheitswurzel
$m_\alpha(t)$	Minimalpolynom zu α

$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$	Ideale
$\mathfrak{p}, \mathfrak{P}, \mathfrak{q}$	Primideale
$\mathfrak{p}_{\mathcal{F}}, \mathfrak{p}_{\mathcal{E}}$	Primideale in Bewertungsringen $\mathfrak{p}$ – adischer Körper $\mathcal{F}$, $\mathcal{E}$.
$\mathfrak{e}(\mathfrak{P}/\mathfrak{p})$	Verzweigungsindex von $\mathfrak{P}$ über $\mathfrak{p}$
$\mathfrak{e}(\mathcal{L}/\mathcal{K})$	Verzweigungsindex der $\mathfrak{p}$ – adischen Körpererweiterung $\mathcal{L}/\mathcal{K}$.
$\mathfrak{f}(\mathfrak{P}/\mathfrak{p})$	Trägheitsgrad von $\mathfrak{P}$ über $\mathfrak{p}$
$\mathfrak{f}(\mathcal{L}/\mathcal{K})$	Trägheitsgrad der $\mathfrak{p}$ – adischen Körpererweiterung $\mathcal{L}/\mathcal{K}$.
$\nu_{\mathfrak{p}}(\mathfrak{a})$ bzw. $\nu_{\mathfrak{p}}(\alpha)$	Exponent von $\mathfrak{p}$ in der Primidealzerlegung von $\mathfrak{a}$ bzw. $\alpha o_{\mathcal{F}}$
$\nu_{\mathcal{F}}(\alpha)$	exponentielle Bewertung von α im $\mathfrak{p}$ – adischen Körper $\mathcal{F}$
$\lvert\alpha\rvert_{\mathfrak{p}}$	$\mathfrak{p}$–adische Bewertung von α
$\mathfrak{D}^*_{\mathcal{E}/\mathcal{F}}$	Codifferente der Erweiterung $\mathcal{E}/\mathcal{F}$
$\mathfrak{D}_{\mathcal{E}/\mathcal{F}}$	Differente der Erweiterung $\mathcal{E}/\mathcal{F}$
$d_{\mathcal{E}/\mathcal{F}}(\alpha)$	Differente des Elementes $\alpha \in \mathcal{E}$
$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$	Diskriminante der Erweiterung $\mathcal{E}/\mathcal{F}$ (Relativdiskriminante)
$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\alpha)$	Diskriminante des $o_{\mathcal{F}}$–Moduls $\left[1, \alpha, \dots, \alpha^{[\mathcal{E}:\mathcal{F}]-1}\right]_{o_{\mathcal{F}}}$
$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\beta_1, \dots, \beta_{[\mathcal{E}:\mathcal{F}]})$	Diskriminante des $o_{\mathcal{F}}$–Moduls $\left[\beta_1, \dots, \beta_{[\mathcal{E}:\mathcal{F}]}\right]_{o_{\mathcal{F}}}$
$\mathfrak{G}_i(\mathcal{E}/\mathcal{F})$	i–te Hilbertsche Verzweigungsgruppe der galoisschen Erweiterung $\mathcal{E}/\mathcal{F}$
$\mathfrak{a}_{\mathcal{E}/\mathcal{F}}$	„Hauptindex“ der Erweiterung $\mathcal{E}/\mathcal{F}$
$\Delta_{\mathcal{E}/\mathcal{F}}$	Menge der Teiler der Diskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$

Literaturverzeichnis

[Ar] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, The collected papers of Emil Artin, Addison–Wesley 1965, 229 – 231.

[BoPo] W. Bosma und M. Pohst, *Computations with finitely generated modules over Dedekind rings*, Proc. ISSAC'91 (1991), 151–156.

[Bo] W. Böffgen, *Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren*, Ann. Univ. Saarbrücken, Ser. Math., **1**, 3 (1987).

[Br] R. J. Bradford, *On the Computation of Integral Bases and Defects of Integrity*, Dissertation, Universität von Bath 1988.

[Co] H. Cohen, *A Course in Computational Algebraic Number Theory*, 1. Aufl., Springer Verlag 1993.

[Ca] J. W. S. Cassels, *Local Fields*, Cambridge University Press 1986.

[CaFr] J. W. S. Cassels und A. Fröhlich, *Algebraic number theory*, Proceedings, Academic Press 1967.

[Da] M. Daberkow, *Bestimmung relativer Ganzheitsbasen in relativquadratischen Zahlkörpern*, Diplomarbeit, Heinrich–Heine–Universität Düsseldorf 1993.

[DaPo94] M. Daberkow und M. Pohst, *On Integral Bases in Relative Quadratic Extensions*, erscheint in Math. Comp.

[DaPo95] M. Daberkow und M. Pohst, *Computations with relative extensions of number fields with an application to the construction of Hilbert class fields* , eingereicht bei ISSAC'95.

[Ed] H. M. Edgar, *A number field without an integral basis*, Math. Mag., **52** (1979), 248 – 251.

[Fo87] D. Ford, *The Construction of Maximal Orders over a Dedekind Domain*, J. Symbolic Computation, **4** (1987), 69 – 75.

[Fo92] D. Ford, *Implementing the Round Four Maximal Order Algorithm*, Preprint.

[Fr] A. Fröhlich, *Discriminants of algebraic number fields*, Math. Zeitschrift **74** (1960), 18 – 28.

[Ga] C. F. Gauß, *Disquisitiones Arithmeticae*, Göttingen 1801.

[Ha26] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresbericht DMV, **35** (1926).

[Ha67] H. Hasse, *Vorlesung über Klassenkörpertheorie*, Physica–Verlag 1967.

[He] E. Hecke, *Vorlesung über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft Geest & Portig K.–G. 1954.

[Hen] K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresbericht DMV, **6** (1897), 83–88.

[Hi] D. Hilbert, *Gesammelte Abhandlungen*, Volume I, Chelsea, New York 1932.

[Ka56] Immanuel Kant, *Beantwortung der Frage: Was is Aufklärung*, Werke in 6 Bdn., hrsg. von W. Weischedel, Bd. 6, Insel Verlag (1956).

[Ka] Fachgruppe Computeralgebra der GI, *Computeralgebra in Deutschland*, Fachgruppe Computeralgebra der GI (1993), 212 – 218.

[Ko] H. Koch, *Number Theory II*, Encyclopaedia of Mathematical Sciences, Springer Verlag 1992.

[Kob] N. Koblitz, *A course in Number Theory and Cryptography*, Graduate Texts in Mathematics 114, Springer Verlag 1987.

[La65] S. Lang, *Algebra*, 6. Aufl. (1974), Addison–Wesley Verlag 1965.

[La86] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics 110, Springer Verlag 1986.

[Ma] H. B. Mann, *On integral bases*, Proceedings of the American Mathematical Society, **9** (1958), 167 – 172.

[MaHa] H. B. Mann und V. Hanley, *A note to the paper "On integral bases" by H. B. Mann*, Proceedings of the American Mathematical Society, **9** (1958), 173 – 174.

[Ne] J. Neukirch, *Algebraische Zahlentheorie*, 1. Aufl., Springer Verlag 1992.

[Na] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2. Aufl., Springer Verlag 1990.

[PoWeZa] M. Pohst, M. Weiler und H. Zassenhaus, *On effective computation of fundamental units I,II*, Math. Comp., **38** (1982), 275 – 329.

[PoZa77] M. Pohst und H. Zassenhaus, *An effective number geometric method of computing the fundamental units of an algebraic number field*, Math. Comp., **31** (1977), 754 – 770.

[PoZa85] M. Pohst und H. Zassenhaus, *Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper*, J. Reine Angew. Math., **361** (1985), 50 – 72.

[PoZa89] M. Pohst und H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press 1989.

[Po93] M. Pohst, *Computational algebraic number theory*, DMV Seminar Bd. 21, Birkhäuser Verlag 1993.

[Po94] M. Pohst, *In Memoriam: Hans Zassenhaus (1912 – 1991)*, J. Number Theory, **47** (1994), 1–19.

[Tr] B. M. Trager, *Algebraic Factoring and Rational Function Integration*, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, 219 – 226.

[Vo] G. Voronoi, *Über eine Verallgemeinerung des Kettenbruchalgorithmus*, Dissertation, Universität von Warschau, 1896, [russisch].

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 1. Aufl., Springer Verlag 1982.

[Za] H. Zassenhaus, *Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung*, Funktionalanalysis, Approx. Th., Numer. Math., Oberwolfach 1965, 90 – 103.

Zusammenfassung

Es seien $n \in \mathbb{N}$ und $\mathcal{F}$ ein algebraischer Zahlkörper, der eine primitive n–te Einheitswurzel ζ_n enthält, gegeben. Wir untersuchen in dieser Arbeit den Ganzheitsring $o_\mathcal{E}$ einer Kummererweiterung $\mathcal{E}$ von $\mathcal{F}$. Für eine solche Erweiterung wird erstmalig ein Verfahren angeben, das ein $o_\mathcal{F}$–Erzeugendensystem von $o_\mathcal{E}$ mit relativen Methoden berechnen kann. Daran schließt sich dann die Bestimmung einer Ganzheitsbasis von $o_\mathcal{E}$ an. Anwendung finden die Methoden bei verallgemeinerten Kummererweiterungen $\mathcal{L}/\mathcal{F}$ und bei Radikalerweiterungen beliebiger Zahlkörper $\mathcal{K}$.

Um die oben angegebenen Ergebnisse zu erhalten, werden zunächst nur Kummererweiterungen von Primzahlgrad $p \in \mathbb{P}$ betrachtet. Es sei daher zunächst $\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu})$ für ein $\mu \in o_\mathcal{F}$. Dieser Spezialfall wird mittels des Hasseschen „Lokal – Global“ Prinzips behandelt. Für eine gegebene $\mathfrak{p}$–adische Kummererweiterung $\mathcal{E}_\mathfrak{P}/\mathcal{F}_\mathfrak{p}$ von Primzahlgrad wird einerseits die Diskriminante $\mathfrak{d}_{\mathcal{E}_\mathfrak{P}/\mathcal{F}_\mathfrak{p}}$ und andererseits eine $o_{\mathcal{F}_\mathfrak{p}}$–Basis für den Ring der ganzen Elemente $o_{\mathcal{E}_\mathfrak{P}}$ von $\mathcal{E}_\mathfrak{P}$ bestimmt. Diese Ergebnisse werden bei den sich anschließenden semilokalen Untersuchungen aufgegriffen und dienen für ein $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$ zur Beschreibung des Ringes $o_\mathcal{E}(\mathfrak{p})$ der $\mathfrak{p}$–ganzen Elemente von $\mathcal{E}$ als freier $o_\mathcal{F}(\mathfrak{p})$–Modul. Wegen

$$o_\mathcal{E} = \bigcap_{\mathfrak{p} \in \mathbb{P}_\mathcal{F}} o_\mathcal{E}(\mathfrak{p})$$

können wir dann mit den semilokalen Aussagen ein $o_\mathcal{F}$–Erzeugendensystem von $o_\mathcal{E}$ angeben.
Diesen theoretischen Überlegungen schließen sich algorithmische Untersuchungen an. Dabei ist es besonders wichtig, Gleichungen der Form

$$x^p \equiv \mu \mod \mathfrak{p}^k$$

mit $\mathfrak{p} \in \{\mathfrak{q} \in \mathbb{P}_\mathcal{F} \mid \nu_\mathfrak{q}(p) > 0\}$ effizient zu lösen. Es wird ein entsprechendes, neues Verfahren vorgestellt.
Kummererweiterungen von beliebigem Grad und verallgemeinerte Kummererweiterungen $\mathcal{E}/\mathcal{F}$ werden nun durch Betrachtung eines entsprechenden Körperturms

$$\mathcal{F} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \ldots \subseteq \mathcal{F}_k = \mathcal{E}$$

auf den Fall einer Kummererweiterung von Primzahlgrad zurückgeführt. Für eine Radikalerweiterung $\mathcal{L}/\mathcal{K}$ vom Grad n wird über die Kummererweiterung $(\mathcal{L}\mathcal{K}(\zeta_n))/\mathcal{K}(\zeta_n)$ eine Ganzheitsbasis von $o_\mathcal{L}$ bestimmt. Zum Abschluß der Arbeit wird eine große Anzahl illustrativer Beispiele präsentiert. So können mit dieser Methode Ganzheitsbasen von algebraischen Zahlkörpern $\mathcal{E}$ mit $[\mathcal{E} : \mathbb{Q}] > 1000$ bestimmt werden.

Beantwortung der Frage: Was ist Aufklärung?
Aufklärung ist der Ausgang des Menschen aus seiner selbstverschuldeten Unmündigkeit. Unmündigkeit ist das Unvermögen, sich seines Verstandes ohne Leitung eines anderen zu bedienen. Selbstverschuldet ist diese Unmündigkeit, wenn die Ursache derselben nicht am Mangel des Verstandes, sondern der Entschließung und des Mutes liegt, sich seiner ohne Leitung eines anderen zu bedienen. Sapere aude! Habe Mut, dich deines eigenen Verstandes zu bedienen! ist also der Wahlspruch der Aufklärung.

Immanuel Kant ([Ka56])

Ich danke Herrn Professor Pohst für die Betreuung dieser Arbeit. Ich habe in ihm stets einen interessierten Zuhörer gefunden.
Mein besonderer Dank gilt jedoch meinen Eltern sowie Tim und Caroline für viele schöne Stunden. Ihnen ist diese Arbeit gewidmet.

Lebenslauf

Name:	Mario Hermann Daberkow
geboren am	25.06.1969 in Neuss
Vater:	Hermann Daberkow, Statiker
Mutter:	Ingrid Daberkow, geb. Spalteholz, Hausfrau
Schulbesuch:	1975 – 1979: Grundschule An der Weyhe, Nievenheim 1979 – 1988: Leibniz–Gymnasium Dormagen Abitur am 25.06.1988
Studium:	Oktober 1988 – Mai 1993: Studium der Mathematik an der Heinrich–Heine–Universität, Düsseldorf 16.10.1990: Vordiplom in Mathematik 06.05.1993: Diplom in Mathematik 10.10.1993: Auszeichnung der Diplomarbeit im Rahmen der Studentenkonferenz der DMV 1993
	Seit 07.05.1993: Wissenschaftlicher Mitarbeiter von Herrn Prof. Pohst an der TU-Berlin