ZUR BERECHNUNG VON STRAHLKLASSENGRUPPEN

Diplomarbeit
von

Sebastian Pauli

Angefertigt am Fachbereich Mathematik
der Technischen Universität Berlin
Berlin 1996

Inhaltsverzeichnis

Einleitung

Eines der Hauptziele der Klassenkörpertheorie ist die Bestimmung aller endlichen abelschen Erweiterungen eines algebraischen Zahlkörpers. Alle diese Erweiterungen eines algebraischen Zahlkörpers sind Unterkörper von Strahlklassenkörpern über diesem algebraischen Zahlkörper. Für den Spezialfall des Hilbertschen Klassenkörpers wurden von M. Daberkow und M.E Pohst Algorithmen entwickelt [DP96]. Dieses Verfahren läßt sich zur Berechnung von Strahlklassenkörpern verallgemeinern. Der erste Schritt zur Berechnung der Strahlklassenkörper ist die Berechnung der Strahlklassengruppen. Zwei Verfahren zur Berechnung von Strahlklassengruppen wurden parallel von H. Cohen, F. Diaz y Diaz und M. Olivier [CDyDO95] und von uns erarbeitet.

Beide Verfahren nutzen die Struktur der Strahlklassengruppe, wie sie in Kapitel II vorgestellt wird, aus.

Um diese Strukturaussagen algorithmisch verwerten zu können, ist es notwendig, sowohl endliche abelsche Gruppen, die durch Erzeugende und Relationen gegeben sind, nach Untergruppen zu faktorisieren, als auch, wenn für drei endliche abelsche Gruppen F, G, H die Erzeugenden und für F, H auch die Relationen bekannt sind und die Isomorphie $G/F \cong H$ gegeben ist, Relationen von G zu berechnen. In Kapitel I werden wir zunächst grundlegende Tatsachen zu algebraischen Zahlkörpern und $\mathfrak{p}$ - adischen Körpern vorstellen und uns dann mit dem Rechnen mit endlichen abelschen Gruppen beschäftigen.

Das Verfahren von H. Cohen, F. Diaz y Diaz und M. Olivier und unser Verfahren unterscheiden sich im wesentlichen in der Berechnung der multiplikativen Gruppe von Restklassenringen. Unser Verfahren beruht auf der expliziten Darstellung der multiplikativen Gruppe eines $\mathfrak{p}$ - adischen Zahlkörpers von H. Hasse [Has63]. Das andere Verfahren basiert auf einer recht einfachen Isomorphie. Wir stellen beide Verfahren zur Bewältigung dieses wohl wichtigsten Schrittes bei der Berechnung von Strahlklassengruppen in Kapitel III vor und vergleichen sie.

In Kapitel IV ergänzen wir die Algorithmen, die noch zur Berechnung der Strahlklassengruppe fehlen. In Kapitel V stellen wir ein Verfahren zur Berechnung des Führers einer Strahlklassengruppe vor, das auf der Darstellung der multiplikativen Gruppe von Restklassenringen mit unserem Verfahren basiert.

Das Verfahren mit Einseinheiten wurde von uns in dem Computeralgebrasystem KANT [DFK+96] implementiert, das Verfahren von Cohen ist in dem Computeralgebrasystem **PARI** [BBCO96] enthalten. In Kapitel VI vergleichen wir die Rechenzeiten der beiden Verfahren und geben einige Beispiele für die Struktur von Restklassenringen und Strahlklassengruppen an.

Ich danke Herrn Professor Dr. M.E. Pohst für die Überlassung des interessanten Themas. Besonders bedanke ich mich bei Florin Nicolae für die vielen fruchtbaren Diskussionen während der Durchführung dieser Arbeit. Weiterhin danke ich den Mitarbeitern des KANT -Projektes.

KAPITEL I

Grundlagen

Algebraische Zahlkörper

Wir geben in diesem Abschnitt einen kurzen Überblick über algebraische Zahlkörper, eine ausführliche Behandlung dieses Themas und Algorithmen zur Berechnung der meisten in diesem Kapitel beschriebenen Objekte findet man in [Coh93], [PZ89] und [Poh93].

Ein algebraischer Zahlkörper ist eine endliche Körpererweiterung von $\mathbb{Q}$. Es sei $f(t)$ ein normiertes, irreduzibles Polynom aus $\mathbb{Z}[t]$ vom Grad n. Einen algebraischen Zahlkörper $\mathbf{K}$ erhält man durch die Adjunktion einer Nullstelle $\rho = t + f(t)\mathbb{Q}[t]$ von $f(t)$ zu $\mathbb{Q}$:

$$\mathbf{K} = \mathbb{Q}(\rho) = \mathbb{Q}[t]/\mathrm{f}(t)\mathbb{Q}[t].$$

Die n Nullstellen von $f(t)$ seien folgendermaßen durchnumeriert: $\rho^{(1)}, \ldots, \rho^{(r_1)}$ seien die reellen Nullstellen, $\rho^{(r_1+1)}, \ldots, \rho^{(r_1+2r_2)}$ die komplexen Nullstellen, wobei $\rho^{(r_1+r_2+i)} = \overline{\rho^{(r_1+i)}}$ für $1 \leq i \leq r_2$ gilt. Es existieren genau $r_1 + 2r_2$ $\mathbb{Q}$-lineare Einbettungen

$$\sigma^{(i)} : \mathbf{K} \longrightarrow \mathbb{C} \text{ mit } \sigma^{(i)}(\rho) = \rho^{(i)}.$$

Für $i \leq r_1$ ist $\sigma^{(i)}$ eine reelle Einbettung, für $i > r_1$ eine komplexe Einbettung. Das i-te Konjugierte $a^{(i)}$ von $a \in \mathbf{K}$ ist das Bild $\sigma^{(i)}(a)$. Der ganze Abschluß von $\mathbb{Z}$ in $\mathbf{K}$ heißt Maximalordnung von $\mathbf{K}$, wir bezeichnen die Maximalordnung von $\mathbf{K}$ mit $\mathfrak{o}_{\mathbf{K}}$. Die Maximalordnung $\mathfrak{o}_{\mathbf{K}}$ ist ein freier $\mathbb{Z}$-Modul. Jede $\mathbb{Z}$-Basis von $\mathfrak{o}_{\mathbf{K}}$ wird als Ganzheitsbasis bezeichnet.

Die Ideale von $\mathfrak{o}_{\mathbf{K}}$ sind ebenfalls freie $\mathbb{Z}$-Moduln. Es sei $\mathfrak{a}$ ein Ideal von $\mathfrak{o}_{\mathbf{K}}$ und $a_1, \ldots, a_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$. Es sei $w_1, \ldots, w_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{o}_{\mathbf{K}}$, dann ist die Übergangsmatrix $A \in \mathbb{Z}^{n \times n}$ mit $A(w_1, \ldots, w_n)^T = (a_1, \ldots, a_n)^T$ eine Darstellung von $\mathfrak{a}$. Ein Integritätsring R heißt Dedekindring, wenn sich jedes Ideal von R, ungleich dem Nullideal als eindeutiges Produkt von Primidealen darstellen läßt. Die Maximalordnung ist ein Dedekindring. da sie nach Definition ganz abgeschlossen ist. Insbesondere hat für eine Primzahl p das Hauptideal $p\mathfrak{o}_{\mathbf{K}}$ von $\mathfrak{o}_{\mathbf{K}}$ die Faktorisierung:

$$p\mathfrak{o}_{\mathbf{K}} = \mathfrak{p}_1^{\mathrm{e}_1} \cdots \mathfrak{p}_l^{\mathrm{e}_l}.$$

Die Ideale $\mathfrak{p}_i$ liegen über der Primzahl p, e_i heißt der Verzweigungsindex von $\mathfrak{p}_i$. Es sei $\mathfrak{a}$ ein Ideal von $\mathfrak{o}_{\mathbf{K}}$, wir definieren die Idealnorm $\mathbf{N}(\mathfrak{a})$ von $\mathfrak{a}$ als die Kardinalität des Restklassenringes $\mathfrak{o}_{\mathbf{K}}/\mathfrak{a}$. Die Idealnorm ist multiplikativ. Es sei $\mathfrak{p}$ ein Primideal von $\mathfrak{o}_{\mathbf{K}}$ über der Primzahl p, dann ist der Restklassenring $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ ein endlicher Körper der Charakteristik p. Er heißt Restklassenkörper von $\mathfrak{p}$ und hat die Ordnung $\mathbf{N}(\mathfrak{p})$,

$$|\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}| = \mathbf{N}(\mathfrak{p}) = p^{\mathrm{f}}.$$

Der Exponent f heißt der Trägheitsgrad von $\mathfrak{p}$.

Für die Berechnung der Strahlklassengruppe benötigen wir die Einheitengruppe $\mathbf{U}_{\mathbf{K}}$ von $\mathfrak{o}_{\mathbf{K}}$.

Satz I.1 (Dirichtlescher Einheitensatz). *Die Einheitengruppe $\mathbf{U}_{\mathbf{K}}$ der Maximalordnung $\mathfrak{o}_{\mathbf{K}}$ eines algebraischen Zahlkörpers $\mathbf{K}$ ist das direkte Produkt der Gruppe der Torsionseinheiten und einer freien abelschen Gruppe vom Rang $r_1 + r_2 - 1$.*

Die Algorithmen zur Berechnung von $\mathbf{U}_{\mathbf{K}}$ liefern eine Einheitswurzel als Erzeugendes der Gruppe der Torsionseinheiten und $\mathrm{r}_1 + \mathrm{r}_2 - 1$ sogenannte Fundamentaleinheiten, die den zweiten Faktor von $\mathbf{U}_{\mathbf{K}}$ erzeugen.

Die Klassengruppe algebraischer Zahlkörper. Es sei $\mathbf{K}$ ein algebraischer Zahlkörper mit Maximalordnung $\mathfrak{o}_{\mathbf{K}}$. Wir definieren die Menge der gebrochenen Ideale von $\mathbf{K}$ durch

$$\mathbf{I}_{\mathbf{K}} = \{\mathfrak{a} \subseteq \mathbf{K} \mid \text{ es existiert } x \in \mathbf{K}^*, \text{ so daß } x\mathfrak{a} \text{ ein Ideal von } \mathfrak{o}_{\mathbf{K}} \text{ ist } \}.$$

Die Menge der gebrochenen Hauptideale ist gegeben durch

$$\mathbf{H}_{\mathbf{K}} = \{\mathfrak{a} \subseteq \mathbf{K} \mid \text{ es existiert ein } x \in \mathbf{K}^*, \text{ so daß } \mathfrak{a} = x\mathfrak{o}_{\mathbf{K}} \text{ ist } \}.$$

Für jedes gebrochene Ideal $\mathfrak{a} \in \mathbf{I}_{\mathbf{K}}$ von $\mathbf{K}$ existiert wieder eine eindeutige Faktorisierung in ein Produkt von Primidealen, wenn man Exponenten kleiner als Null zuläßt:

$$\mathfrak{a} = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(\mathfrak{a})} \cdots \mathfrak{p}_l^{v_{\mathfrak{p}_l}(\mathfrak{a})}$$

Die gebrochenen Ideale $\mathbf{I}_{\mathbf{K}}$ von $\mathbf{K}$ bilden eine kommutative, multiplikative Gruppe. Die gebrochenen Hauptideale sind eine Untergruppe von $\mathbf{I}_{\mathbf{K}}$.

Definition I.2 (Klassengruppe). *Die Gruppe $\mathbf{Cl}_{\mathbf{K}} := \mathbf{I}_{\mathbf{K}}/\mathbf{H}_{\mathbf{K}}$ heißt Klassengruppe von $\mathbf{K}$.*

SATZ I.3. *Die Klassengruppe* $\mathbf{Cl_K}$ *von* $\mathbf{K}$ *ist endlich und wird von den Idealklassen endlich vieler Primideale von* $\mathfrak{o}_\mathbf{K}$ *erzeugt.*

Die Ordnung $\mathbf{h_K} = |\mathbf{Cl_K}|$ von $\mathbf{Cl_K}$ heißt die Klassenzahl von $\mathbf{K}$.

Die Algorithmen zur Berechnung der Klassengruppe liefern Vertreter der Idealklassen einer Basis der Klassengruppe und die Ordnungen dieser Idealklassen. Weiterhin gibt es Algorithmen, die zu jeder Idealklasse eine Darstellung dieser Klasse bezüglich der Basis der Klassengruppe bestimmen. Siehe dazu zum Beispiel [Hes96].

Bewertungen und $\mathfrak{p}$-adische Zahlkörper

Beweise der Aussagen und weitere Ausführungen über $\mathfrak{p}$-adische Körper findet man in [Has63], [Lan86] und [Nar90].

DEFINITION I.4 (BEWERTUNG). *Es sei* $\mathbf{K}$ *ein Körper. Eine Abbildung* $|\cdot| : \mathbf{K} \to \mathbb{R}$ *heißt Bewertung, falls für alle* $x, y \in \mathbf{K}$ *gilt:*

(i) $|1| = 1$
(ii) $0 \leq |x|, |x| = 0 \Leftrightarrow x = 0$
(iii) $|xy| \leq |x||y|$
(iv) $|x + y| \leq |x| + |y|$

Gilt statt (iv) *die stärkere Bedingung*

(v) $|x + y| \leq \max(|x|, |y|)$

so bezeichnen wir $|\cdot|$ *als nicht-archimedische Bewertung von* $\mathbf{K}$. *Gilt* (v) *nicht, so heißt* $|\cdot|$ *archimedische Bewertung.*

BEISPIEL I.5. (1) *Die Abbildung*

$$|a| = \begin{cases} 0 & \textit{falls} \quad a = 0 \\ 1 & \textit{falls} \quad a \neq 0 \end{cases}$$

ist eine nicht-archimedische Bewertung, sie heißt die triviale Bewertung.

(2) *Es sei* $\mathbf{K}$ *ein algebraischer Zahlkörper, bezeichnet* $a^{(i)}$ *das i-te Konjugierte von* $a \in \mathbf{K}$ *und* $|\cdot|$ *den Betrag von* $\mathbb{C}$, *dann ist* $|a|_{\mathfrak{p}_\infty^{(i)}} = |a^{(i)}|$ *eine archimedische Bewertung von* $\mathbf{K}$.

(3) *Es sei* $\mathbf{K}$ *ein algebraischer Zahlkörper, es sei* $\mathfrak{p}$ *eine Primideal von* $\mathfrak{o}_\mathbf{K}$, *es sei* $v_\mathfrak{p}$ *wie oben und es sei* $\gamma \in \mathbb{R}$ *mit* $0 < \gamma < 1$, *dann ist*

$$|a|_\mathfrak{p} = \begin{cases} 0 & \textit{falls} \quad \mathfrak{a} = \{0\} \\ \gamma^{v_\mathfrak{p}(\mathfrak{a})} & \textit{falls} \quad \mathfrak{a} \neq 0 \end{cases}$$

eine nicht-archimedische Bewertung von $\mathbf{K}$.

Definition I.6. *Zwei Bewertungen* $|\cdot|_1$ *und* $|\cdot|_2$ *eines Körpers* $\mathbf{K}$ *heißen äquivalent, wenn* $|x|_1 < |y|_1 \Leftrightarrow |x|_2 < |y|_2$ *für alle* $x, y \in \mathbf{K}$ *ist.*

Man stellt fest, daß jede beliebige Bewertung auf einem algebraischen Zahlkörper äquivalent zu einer der Bewertungen aus Beispiel I.5 ist. Die nichttrivialen Bewertungen werden entweder durch Primideale $\mathfrak{p}$, wir bezeichnen diese Bewertungen mit $|\cdot|_{\mathfrak{p}}$, oder durch die konjugierten Körper $\mathbf{K}^{(i)}$ von $\mathbf{K}$ gegeben, wir bezeichnen diese Bewertungen mit $|\cdot|_{\mathfrak{p}_\infty^{(i)}}$. Eine Klasse äquivalenter Bewertungen von $\mathbf{K}$ heißt eine Stelle von $\mathbf{K}$, wir bezeichnen diese mit $\mathfrak{p}$ bzw. $\mathfrak{p}_\infty^{(i)}$. Wir fassen die endlichen Stellen $\mathfrak{p}$ und die sogenannten unendlichen Stellen $\mathfrak{p}_\infty^{(i)}$ zur Menge der Primstellen $\mathbf{P}_{\mathbf{K}}$ von $\mathbf{K}$ zusammen.

Der Approximationssatz verallgemeinert den Chinesischen Restsatz auf die unendlichen Primstellen:

Satz I.7 (Approximationssatz). *Es seien* $|\cdot|_1, \ldots, |\cdot|_n$ *nichtäquivalente, nichttriviale Bewertungen eines algebraischen Zahlkörpers* $\mathbf{K}$. *Es seien* $a_1, \ldots, a_n \in \mathbf{K}$. *E sei* $\varepsilon > 0$ *gegeben. Dann gibt es ein* $a \in \mathbf{K}$, *so daß*

$$|a - a_i|_i < \varepsilon \quad (i = 1, \ldots, n)$$

gilt.

$\mathfrak{p}$-adische Zahlkörper. Die Vervollständigung eines Zahlkörper bezüglich einer archimedischen Bewertung $|\cdot|_{\mathfrak{p}_\infty^{(i)}}$ ist $\mathbb{R}$, wenn $\sigma^{(i)}$ eine reelle Einbettung ist, und $\mathbb{C}$, wenn $\sigma^{(i)}$ eine komplexe Einbettung ist.

Der nicht-archimedische Fall bedarf einer genaueren Betrachtung, dazu betrachten wir zunächst einen bewerteten Körper:

Satz I.8. *Es sei* $|\cdot|$ *eine nicht-archimedische Bewertung des Körpers* $\mathbf{K}$. *Dann ist*

$$B = \{a \in \mathbf{K} \mid |a| \leq 1\}$$

ein lokaler Ring mit dem maximalen Ideal

$$\mathfrak{b} = \{a \in \mathbf{K} \mid |a| < 1\}$$

und der Einheitengruppe

$$U = \{a \in \mathbf{K} \mid |a| = 1\}.$$

B heißt der Bewertungsring und $\mathfrak{b}$ das Bewertungsideal der Bewertung $|\cdot|$.

Satz I.9. *Es sei* $\mathbf{K}$ *ein algebraischer Zahlkörper und* $\mathfrak{p}$ *ein Primideal seiner Maximalordnung. Dann existiert ein Körper* $\mathbf{K}_{\mathfrak{p}}$ *mit den folgenden Eigenschaften:*

(1) $\mathbf{K}_{\mathfrak{p}}$ *ist die Vervollständigung von* $\mathbf{K}$ *bezüglich* $|\cdot|_{\mathfrak{p}}$.

(2) *Ist R ein Vertretersystem von $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ in $\mathfrak{o}_{\mathbf{K}}$ mit $0 \in R$ und ist $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, so gilt*

$$\mathbf{K}_{\mathfrak{p}} = \{\sum_{i=m}^{\infty} \rho_i \pi^i \mid \rho_i \in R, m \in \mathbb{Z}, \rho_m \neq 0\}.$$

Damit ist

$$\mathfrak{o}_{\mathfrak{p}} = \{\sum_{i=m}^{\infty} \rho_i \pi^i \mid \rho_i \in R, m \in \mathbb{Z}, m \geq 0, \rho_m \neq 0\}$$

der Bewertungsring der Fortsetzung von $|\cdot|_{\mathfrak{p}}$ auf $\mathbf{K}_{\mathfrak{p}}$. Er ist ein lokaler Hauptidealring mit dem maximalen Ideal

$$\mathfrak{b}_{\mathfrak{p}} = \{\sum_{i=m}^{\infty} \rho_i \pi^i \mid \rho_i \in R, m \in \mathbb{Z}, m \geq 1, \rho_m \neq 0\} = \pi \mathfrak{o}_{\mathfrak{p}}.$$

Lemma I.10. *Es sei $\mathbf{K}$ ein algebraischer Zahlkörper, $\mathfrak{p}$ ein Primideal seiner Maximalordnung $\mathfrak{o}_{\mathbf{K}}$ und $\mathbf{K}_{\mathfrak{p}}$ die Vervollständigung von $\mathbf{K}$ bezüglich $|\cdot|_{\mathfrak{p}}$ mit Bewertungsring $\mathfrak{o}_{\mathfrak{p}}$ und Bewertungsideal $\mathfrak{b}_{\mathfrak{p}}$. Dann gilt*

$$\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^m \cong \mathfrak{o}_{\mathfrak{p}}/{\mathfrak{b}_{\mathfrak{p}}}^m.$$

Beweis. Die Abbildung $\mathfrak{o}_{\mathbf{K}} \to \mathfrak{o}_{\mathfrak{p}}/{\mathfrak{b}_{\mathfrak{p}}}^m$, $a \mapsto [a]$ ist ein Homomorphismus. Es sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Jede Klasse $[a]$ von $\mathfrak{o}_{\mathfrak{p}}/{\mathfrak{b}_{\mathfrak{p}}}^m$ besitzt eine Darstellung $[a] = [\sum_{i=0}^{m-1} \alpha_i \pi^i]$, wobei α_i aus einem Vertretersystem von $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ in $\mathfrak{o}_{\mathbf{K}}$ ist. Damit ist die Abbildung surjektiv.

Aus $b \in {\mathfrak{b}_{\mathfrak{p}}}^m$ und $b \in \mathfrak{o}_{\mathbf{K}}$ folgt $b \in \mathfrak{p}^m$, also ist der Kern der Abbildung $\mathfrak{p}^m$. □

Ist p die Primzahl unter $\mathfrak{p}$, dann gilt $|\mathfrak{o}_{\mathfrak{p}}/\mathfrak{b}_{\mathfrak{p}}| = |\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}| = p^{\mathrm{f}}$, wobei f der Trägheitsgrad von $\mathfrak{p}$ ist. Wir nennen f auch den Trägheitsgrad von $\mathfrak{b}_{\mathfrak{p}}$.

Weiterhin gilt $p\mathfrak{o}_{\mathfrak{p}} = {\mathfrak{b}_{\mathfrak{p}}}^{\mathrm{e}}$, e heißt der Verzweigungsindex von $\mathfrak{b}_{\mathfrak{p}}$. Der Verzweigungsindex von $\mathfrak{b}_{\mathfrak{p}}$ ist gleich dem Verzweigungsindex von $\mathfrak{p}$.

Rechnen mit endlichen abelschen Gruppen

Jede endliche abelsche Gruppe läßt sich durch Erzeugende und Relationen zwischen den Erzeugenden darstellen. Um wirklich mit einer Gruppe in dieser Darstellung umgehen zu können, benötigen wir ein Verfahren, das jedem Element aus der Gruppe eine Darstellung bezüglich den Erzeugenden zuordnet. Weitere Ausführungen zu diesem Thema findet man in [Sim94] und [CDyDO95].

Es sei G eine endliche abelsche Gruppe, es sei $g = (g_i) \in G^m$ ein Spaltenvektor von Erzeugenden von G. Eine Relation von G schreiben wir als $vg = v_1 g_1 + \cdots + v_m g_m = 0$, wobei $v^{tr} \in \mathbb{Z}^m$ ist. Die Gruppe G stellen wir durch den Vektor g der Erzeugenden und eine Relationenmatrix M dar, deren Zeilen die Relationen von G repräsentieren.

Wenn die Matrix $M = (M_{ij})$ Diagonalgestalt hat, sind die Erzeugenden $g = (g_i)$ der Gruppe G sogar eine Basis von G, wobei das Erzeugende g_i die Ordnung M_{ii} hat. Wir wollen uns damit beschäftigen, wie wir aus gegebenen Erzeugenden und Relationen eine Basis der Gruppe erhalten. Doch zunächst werden wir uns ein Kriterium für die Gleichheit von Gruppen ansehen.

Definition I.11 (Hermite Normalform). *Eine Matrix $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$ vom Rang r ist in oberer Zeilen Hermite Normalform, wenn gilt:*

(i) *Ist $1 \leq i \leq r$ und ist A_{ij_i} der erste Eintrag ungleich Null in der i-ten Zeile, dann gilt $j_1 < j_2 < \cdots < j_r$.*
(ii) $A_{ij_i} > 0, 1 \leq i \leq r$.
(iii) *Falls $1 \leq k \leq i \leq r$, dann ist $0 \leq A_{kj_i} < A_{ij_i}$.*

Satz I.12. *Es sei $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$, dann gibt es eine unimodulare Matrix $T_L \in \mathbb{Z}^{m\times m}$, so daß $H = T_L A$ in oberer Zeilen Hermite Normalform ist. H ist durch A eindeutig bestimmt.*

Wir können die Relationenmatrix einer Gruppe in Hermite Normalform bringen, ohne an den Erzeugenden etwas zu ändern, da wir durch Zeilenoperationen nur einen Satz Relationen in einen anderen überführen.

Die folgende Aussage werden wir später dazu benutzen, um Gruppen zu vergleichen.

Bemerkung I.13. *Zwei endliche abelsche Gruppen sind isomorph, wenn die Hermite Normalformen ihrer Relationenmatrizen übereinstimmen. Zwei endliche abelsche Gruppen sind gleich, wenn ihre Relationenmatrizen in Hermite Normalform bis auf Nullzeilen und ihre Erzeugenden übereinstimmen.*

Wie oben schon erwähnt, ist es zum Konstruieren einer Basis aus Erzeugenden und Relationen notwendig, die Relationenmatrix zu diagonalisieren. Die Smith Normalform liefert eine eindeutige Diagonalgestalt für Matrizen über $\mathbb{Z}$.

Definition I.14 (Smith Normalform). *Eine Matrix $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$ vom Rang r ist in Smith Normalform, wenn gilt:*

(i) $a_{ij} = 0$, *für* $i \neq j$
(ii) $a_{ii} = 0$, *für* $i > r$
(iii) $a_{ii} > 0$, *für* $i \leq r$
(iv) $a_{11} \mid a_{22} \mid \ldots \mid a_{rr}$

Satz I.15. *Es sei $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$, dann gibt es unimodulare Matrizen $T_L \in \mathbb{Z}^{m\times m}$ und $T_R \in \mathbb{Z}^{n\times n}$, so daß $S = T_L A T_R$ in Smith Normalform ist. S ist eindeutig durch A bestimmt.*

Bemerkung I.16. *Zwei endliche abelsche Gruppen sind genau dann isomorph, wenn die Smith Normalform ihrer Relationenmatrizen bis auf Nullzeilen übereinstimmen.*

Es sei G eine durch (g, M) gegebene endliche abelsche Gruppe. Nach I.15 gibt es unimodulare Matrizen $T_L \in \mathbb{Z}^{m\times m}$ und $T_R \in \mathbb{Z}^{n\times n}$, so daß $T_L M T_R = D$ eine Diagonalmatrix ist. Es sei $N = T_L M$, dann ist (g, N) eine weitere Darstellung von G. $(T_R^{-1}g, D)$ ist eine Basisdarstellung der Gruppe, da $NT_R T_R^{-1} g = DT_R^{-1}g = 0$ gilt. Die Matrix D ist also die Relationenmatrix zu den Erzeugenden $T_R^{-1}g$. Es sei $a \in G$ und $v \in \mathbb{Z}^n$ mit $a = vg$, dann ist vT_R eine Darstellung von a bezüglich der Basis $T_R^{-1}g$ von G.

Bemerkung I.17. *Zu jeder endlichen abelsche Gruppe, die durch Erzeugende und Relationen gegeben ist, läßt sich mit der Smith Normalform eine Basis finden.*

Wir werden im folgenden eine Darstellung der endlichen abelschen Gruppen durch Erzeugende und Relationen berechnen. In Kapitel IV werden wir auf Probleme eingehen, die sich beim Erstellen einer Basis der Gruppen, die wir betrachten, ergeben.

Faktorisieren. Die endliche abelsche Gruppe G sei durch (g, M) gegeben. F sei eine Untergruppe von G. Wir werden nun G/F berechnen, d.h. wir werden Erzeugende und Relationen von G/F bestimmen. Das Faktorisieren von G nach F bedeutet, daß wir zu den Relationen M von G noch weitere Relationen hinzufügen und die Erzeugenden als Vertreter von Äquivalenzklassen betrachten. Um die Elemente von F mit 0 zu identifizieren, brauchen wir nur die Darstellung der Erzeugenden von F bezüglich g an die Relationenmatrix anzuhängen. Sei also U eine Matrix, so daß die Komponenten von Ug ein Erzeugendensystem von F sind, dann ist

$$(g, \left(\begin{smallmatrix} M \\ U \end{smallmatrix}\right))$$

eine Darstellung von G/F.

Beim Berechnen der Strahlklassengruppen behandeln wir Faktorgruppen. Wenn eine Gruppe G durch Erzeugende und Relationen (g, M) dargestellt ist, betrachten wir die Erzeugenden g_i als Vertreter der Klassen von G.

Etwas allgemeiner können wir das Problem durch eine exakte Sequenz darstellen.

Lemma I.18. *Es seien F,G endliche abelsche Gruppen, es sei f ein Erzeugendensystem von F und G sei durch (g, M) dargestellt. Weiterhin sei die exakte Sequenz*

$$0 \longrightarrow F \xrightarrow{\Psi} G \xrightarrow{\Phi} H \longrightarrow 0$$

gegeben, dann ist $\left(\Phi(g), \binom{M}{P}\right)$ eine Darstellung von H, wobei $Pg = \Psi(f)$ gilt.

Die Darstellung von Klassen bezüglich der Erzeugenden $\Phi(g)$ in H ist die gleiche, wie die Darstellung der Elemente von G bezüglich g.

Erweitern. Beim Berechnen der Strahlklassengruppe werden wir auch auf folgende Situation stoßen: Uns sind die Erzeugenden und Relationen der endlichen abelschen Gruppen F und H und die Erzeugenden der endlichen abelschen Gruppe G bekannt. Es gilt $G/F \cong H$ und wir wollen Relationen für G bestimmen. Wir formulieren dies mit einer exakten Sequenz.

LEMMA I.19. *Es seien F, G, H endliche abelsche Gruppen, F, H seien durch Erzeugende und Relationenmatrizen (f, M_F) bzw. (h, M_H) gegeben, und es gelte die exakte Sequenz*

$$0 \longrightarrow F \xrightarrow{\Psi} G \xrightarrow{\Phi} H \longrightarrow 0,$$

dann ist $\left(\binom{g'}{\Psi(f)}, \begin{pmatrix} M_H & -P \\ 0 & M_F \end{pmatrix}\right)$ eine Darstellung von G. Hierbei ist g' ein Vektor mit Komponenten aus G mit $\Phi(g') = h$ und P eine Matrix über $\mathbb{Z}$ mit $M_H(g') = P\Psi(f)$.

Der Beweis stammt aus [CDyDO95].

BEWEIS. Wähle g' so, daß $\Phi(g') = h$ ist. Sei $\gamma \in G$, dann gibt es Vektoren x, y, so daß $\Phi(\gamma) = xh = x\Phi(g')$, also $\gamma - xg' \in \mathrm{Kern}(\Phi)$ und $\gamma - xg' = \Psi(yf)$ sind. Somit gilt $\gamma = xg' + y\Psi(f) = (x\ y)\binom{g'}{\Psi(f)}$, also sind $\binom{g'}{\Psi(f)}$ Erzeugende von G.

Wenn $(x\ \ y)$ eine Relation von G ist, so gilt $xg' + y\Psi(f) = 0$. Wenn wir Φ darauf anwenden, erhalten wir $x\Phi(g') = xh = 0$, also ist $x = x'M_H$. Damit gilt $x'M_H g' + y\Psi(f) = 0$.

Es sei $g'' = g'M_H$, dann gilt $\Phi(g'') = M_H\Phi(g') = M_H h = 0$. Damit sind die Komponenten von g'' in $\mathrm{Kern}(\Phi) = \mathrm{Bild}(\Psi)$ gegeben. Wir können nun eine Matrix P finden, so daß $g'' = \Psi(Pf) = P\Psi(f)$ ist. Es gilt also

$$x'P\Psi(f) + y\Psi(f) = 0 \Leftrightarrow (x'P + y)\Psi(f) = 0 \Leftrightarrow x'P + y \in \mathrm{Bild}(M_F).$$

Es gibt einen Vektor y', so daß

$$x'P + y = y'M_F$$

ist. Daher ist $(x\ \ y)$ genau dann eine Relation wenn $(x\ \ y) = (x'\ \ y')\begin{pmatrix} M_H & -P \\ 0 & M_F \end{pmatrix}$ gilt. $\square$

Im folgenden werden wir für Gruppen in multiplikativer Darstellung die Schreibweise

$$vg = (v_1, \dots, v_n)\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = g_1^{v_1} \cdots g_n^{v_n}$$

benutzen, wobei $v \in \mathbb{Z}^n$ und g der Vektor der Erzeugenden der Gruppe ist.

KAPITEL II

Die Strahlklassengruppe

Wir werden in diesem Kapitel die Strahlklassengruppe einführen und uns ihre Struktur ansehen. Durch die Aussagen über die Struktur wird ein Weg zur Berechnung der Strahlklassengruppe vorgezeichnet. Wir folgen in diesem Kapitel [Lan86].

Im folgenden sei $\mathbf{K}$ ein algebraischer Zahlkörper und $\mathfrak{o}_{\mathbf{K}}$ die Maximalordnung von $\mathbf{K}$, es sei $\mathbf{I}_{\mathbf{K}}$ die Gruppe der gebrochenen Ideale von $\mathbf{K}$, $\mathbf{H}_{\mathbf{K}}$ die Untergruppe der gebrochenen Hauptideale und $\mathbf{P}_{\mathbf{K}}$ die Menge der Primstellen von $\mathbf{K}$.

Definition II.1 (Multiplikative Kongruenz). *Es sei $a \in \mathbf{K}^*$.*

(i) *Es sei $\mathfrak{p} \in \mathbf{P}_{\mathbf{K}}$ eine endliche Stelle von $\mathbf{K}$, es sei $\mathbf{K}_{\mathfrak{p}}$ die Vervollständigung von $\mathbf{K}$ bezüglich $|\cdot|_{\mathfrak{p}}$ mit Bewertungsideal $\mathfrak{b}_{\mathfrak{p}}$. Dann definieren wir*

$$a \equiv 1 \bmod^* \mathfrak{p}^m :\Leftrightarrow a \equiv 1 \bmod {\mathfrak{b}_{\mathfrak{p}}}^m.$$

(ii) *Es sei $\mathfrak{p}_\infty^{(i)} \in \mathbf{P}_{\mathbf{K}}$ eine unendliche, reelle Stelle von $\mathbf{K}$, dann bedeute*

$$a \equiv 1 \bmod^* \mathfrak{p}_\infty^{(i)},$$

daß die i-te Konjugierte $a^{(i)}$ von a positiv ist. Für eine komplexe Stelle $\mathfrak{p}_\infty^{(i)} \in \mathbf{P}_{\mathbf{K}}$ sei die Kongruenz stets erfüllt. Ferner wird für Potenzen ${\mathfrak{p}_\infty}^m$ von unendlichen Stellen $\mathfrak{p}_\infty \in \mathbf{P}_{\mathbf{K}}$ definiert:

$$a \equiv 1 \bmod^* {\mathfrak{p}_\infty}^m :\Leftrightarrow a \equiv 1 \bmod^* \mathfrak{p}_\infty.$$

(iii) *Es sei $\mathfrak{p} \in \mathbf{P}_{\mathbf{K}}$ eine Stelle von $\mathbf{K}$, dann sei*

$$a \equiv b \bmod^* p :\Leftrightarrow \frac{a}{b} \equiv 1 \bmod^* \mathfrak{p} \textit{ mit } a, b \neq 0.$$

DEFINITION II.2 (KONGRUENZMODUL). *Es sei $S \subset \mathbf{P_K}$ eine endlich Teilmenge der Stellen von $\mathbf{K}$. Es sei $\mathfrak{m}$ das formale Produkt*

$$\mathfrak{m} = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{m_\mathfrak{p}} \quad (m_\mathfrak{p} \in \mathbb{N}).$$

Wir bezeichnen das Potenzprodukt der endlichen Stellen aus S mit $\mathfrak{m}_0$ und das formale Produkt der unendlichen Stellen mit $\mathfrak{m}_\infty$.

$$a \equiv b \bmod^* \mathfrak{m},$$

bedeute, daß

$$a \equiv b \bmod^* \mathfrak{p}^{m_\mathfrak{p}}$$

für alle $\mathfrak{p} \mid \mathfrak{m}$ gilt. $\mathfrak{m}$ heißt ein Kongruenzmodul von $\mathbf{K}$.

DEFINITION II.3 (STRAHLKLASSENGRUPPE). *Es sei $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ ein Kongruenzmodul und es sei:*

$$\begin{aligned} \mathbf{I}^\mathfrak{m} &:= \{\mathfrak{a} \in \mathbf{I_K} \mid \mathfrak{a} \textit{ ist teilerfremd zu } \mathfrak{m}_0\}, \\ \mathbf{H}_\mathfrak{m} &:= \{(a) \in \mathbf{H_K} \mid a \equiv 1 \bmod^* \mathfrak{m}\}. \end{aligned}$$

Die Faktorgruppe $\mathbf{Cl}_\mathbf{K}^\mathfrak{m} := \mathbf{I}^\mathfrak{m}/\mathbf{H}_\mathfrak{m}$ heißt die Strahlklassengruppe von $\mathbf{K}$ modulo $\mathfrak{m}$. $\mathbf{H}_\mathfrak{m}$ heißt der Strahl von $\mathbf{K}$ modulo $\mathfrak{m}$.

$\mathbf{I}^\mathfrak{m}$ ist eine Untergruppe von $\mathbf{I_K}$ und $\mathbf{H}_\mathfrak{m}$ ist eine Untergruppe von $\mathbf{H_K}$.

Wir werden mit Hilfe des folgenden Diagramms die Endlichkeit von $\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$ zeigen, desweiteren zeigt es uns einen Weg zur Berechnung der Strahlklassengruppe auf.

SATZ II.4. *Es seien $\mathbf{I}^\mathfrak{m}$ und $\mathbf{H}_\mathfrak{m}$ wie oben definiert. Es sei $\mathbf{H}^\mathfrak{m} := \{\mathfrak{a} \in \mathbf{H_K} \mid \mathfrak{a}$ ist teilerfremd zu $\mathfrak{m}_0\}$, $\mathbf{K}_\mathfrak{m} := \{a \in \mathbf{K} \mid a \equiv 1 \bmod^* \mathfrak{m}\}$, $\mathbf{K}^\mathfrak{m} := \{a \in \mathbf{K} \mid (a)$ ist teilerfremd zu $\mathfrak{m}_0\}$, $\mathbf{U_K}$ die Einheitengruppe von $\mathfrak{o}_\mathbf{K}$ und $\mathbf{U}_\mathfrak{m} := \{u \in \mathbf{U_K} \mid u \equiv 1 \bmod^* \mathfrak{m}\}$. Dann gilt:*

$$\begin{array}{ccccccc} & & & & \mathbf{I}^\mathfrak{m} & \to & \mathbf{I_K} \\ & & & & | & & | \\ & & \mathbf{K}^\mathfrak{m} & \to & \mathbf{H}^\mathfrak{m} & \to & \mathbf{H_K} \\ & & | & & | & & \\ \mathbf{U_K} & \to & \mathbf{U_K}\mathbf{K}_\mathfrak{m} & \to & \mathbf{H}_\mathfrak{m} & & \\ | & & | & & & & \\ \mathbf{U}_\mathfrak{m} & \to & \mathbf{K}_\mathfrak{m} & & & & \end{array}$$

Wobei parallele senkrechte Striche die Isomorphie der Faktorgruppen und die waagerechten Pfeile Gruppenhomomorphismen darstellen.

Wir werden die Isomorphismen einzeln beweisen. Zunächst zeigen wir, daß es in jeder Idealklasse von $\mathbf{I_K}/\mathbf{H_K} = \mathbf{Cl_K}$, einen Repräsentanten gibt, der teilerfremd zu $\mathfrak{m}_0$ ist.

Lemma II.5. *Es gilt*

$$\mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{\mathfrak{m}} \cong \mathbf{I_K}/\mathbf{H_K} = \mathbf{Cl_K}.$$

Beweis. Es sei $\mathfrak{a}$ ein Ideal aus einer gegebenen Klasse von $\mathbf{Cl_K}$, es sei $\pi_\mathfrak{p} \in \mathfrak{o}_\mathbf{K}$ mit $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. Für alle $\mathfrak{p}|\mathfrak{m}_0$ löse mit dem Chinesischen Restsatz die folgenden Kongruenzen

$$a \equiv \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \bmod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})+1},$$

dann ist $\mathfrak{b} = a^{-1}\mathfrak{a}$ teilerfremd zu $\mathfrak{m}_0$. Es gibt nun ein ganzes Ideal $\mathfrak{c}$ und einen Nenner $d \in \mathbb{Z}$, so daß d die kleinste positive ganze Zahl mit $d\mathfrak{b} \subset \mathfrak{o}_\mathbf{K}$ und $\mathfrak{b} = \frac{\mathfrak{c}}{d}$ ist. Da $\mathfrak{b}$ teilerfremd zu $\mathfrak{m}_0$ ist, sind auch d und $\mathfrak{c}$ teilerfremd zu $\mathfrak{m}_0$. $\mathfrak{c}$ ist also ein Ideal, das den gleichen zyklischen Faktor der Klassengruppe wie $\mathfrak{p}$ erzeugt. Damit erhalten wir Erzeugende der Gruppe $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{\mathfrak{m}}$. □

Lemma II.6. *Der Homomorphismus* $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}} \longrightarrow \mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{m}$ *ist surjektiv mit Kern* $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$.

Der Beweis ist eine einfache Anwendung des Isomorphiesatzes.

Lemma II.7. *Es gilt:*

$$\mathbf{K}^{\mathfrak{m}}/\mathbf{U_K}\mathbf{K}_{\mathfrak{m}} \cong \mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}.$$

Beweis. Wir betrachten die Abbildung $\mathbf{K}^* \to \mathbf{H}, a \mapsto (a)$, ihr Kern ist die Einheitengruppe $\mathbf{U_K}$ von $\mathbf{K}$. Dies gilt analog für die Abbildung $\mathbf{K}^{\mathfrak{m}} \to \mathbf{H}^{\mathfrak{m}}, a \mapsto (a)$. Das Urbild von $\mathbf{H}_{\mathfrak{m}}$ ist genau $\mathbf{U_K}\mathbf{K}_{\mathfrak{m}}$. □

Aus dem Isomorphiesatz folgt wiederum, daß gilt

$$\mathbf{U_K}\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}} \cong \mathbf{U_K}/(\mathbf{U_K} \cap \mathbf{K}_{\mathfrak{m}}) = \mathbf{U_K}/\mathbf{U}_{\mathfrak{m}}.$$

Lemma II.8. *Es sei* $\mathbb{R}^*$ *die multiplikative Gruppe von* $\mathbb{R}$ *und* $\mathbb{R}^{*>0}$ *die positiven Elemente dieser Gruppe. Dann gilt:*

$$\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}} \cong \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathfrak{o}_\mathbf{K}/\mathfrak{p}^{m_\mathfrak{p}})^* \times \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}.$$

Beweis. Betrachte die Abbildung

$$\mathbf{K}^{\mathfrak{m}} \to \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathfrak{o}_\mathbf{K}/\mathfrak{p}^{m_\mathfrak{p}})^* \times \prod_{\mathfrak{p}_\infty|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}.$$

Mit Hilfe des Approximationssatzes zeigt man, daß diese Abbildung surjektiv ist. Es ist klar, daß ihr Kern $\mathbf{K}_{\mathfrak{m}} = \{a \in \mathbf{K} \mid a \equiv 1 \bmod^* \mathfrak{m}\}$ ist. □

Insbesondere gilt $\mathbf{K}^{\mathfrak{m}_0}/\mathbf{K}_{\mathfrak{m}_0} \cong (\mathfrak{o}_\mathbf{K}/\mathfrak{p}^{m_\mathfrak{p}})^*$ und $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty} \cong \mathbb{R}^*/\mathbb{R}^{*>0}$.

LEMMA II.9 (φ - FUNKTION). *Für die Ordnung $\varphi(\mathfrak{m})$ von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ gilt:*

$$\varphi(\mathfrak{m}) = \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathbf{N}(\mathfrak{p}) - 1)(\mathbf{N}(\mathfrak{p})^{k-1} \prod_{\mathfrak{p}_\infty|\mathfrak{m}_\infty \textit{ reell}} 2.$$

BEWEIS. Nach Lemma II.8 läßt sich $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ in das direkte Produkt der multiplikativen Gruppen von Restklassenringen modulo $\mathfrak{p}^{m_{\mathfrak{p}}}$ und $\prod_{\mathfrak{p}_\infty|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}$ zerlegen. Die Ordnung von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m_{\mathfrak{p}}})^*$ ist $(\mathbf{N}(\mathfrak{p})-1)(\mathbf{N}(\mathfrak{p})^{k-1}$, da $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m_{\mathfrak{p}}})^*$ aus allen Elementen von $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m_{\mathfrak{p}}}$ besteht, die teilerfremd zu $\mathfrak{p}$ sind. $\mathbb{R}^*/\mathbb{R}^{*>0}$ besteht aus den Klassen von -1 und 1 und hat somit die Ordnung 2. □

SATZ II.10. *Es sei $\mathbf{h}_{\mathbf{K}}$ die Klassenzahl von $\mathbf{K}$, dann gilt*

$$\mathbf{h}_{\mathbf{K}}^{\mathfrak{m}} := \mathrm{ord}(\mathbf{Cl}_{\mathbf{K}}{}^{\mathfrak{m}}) = \frac{\varphi(\mathfrak{m})\mathbf{h}_{\mathbf{K}}}{[\mathbf{U}_{\mathbf{K}} : \mathbf{U}_{\mathfrak{m}}]}.$$

Mit dem Diagramm aus Satz II.4 ist auch diese Aussage bewiesen. $\mathbf{h}_{\mathbf{K}}^{\mathfrak{m}}$ heißt die Strahlklassenzahl von $\mathbf{K}$ modulo $\mathfrak{m}$.

Algorithmus. Es bietet sich an, zum Berechnen der Strahlklassengruppe dem soeben bewiesenen Diagramm zu folgen. Zunächst berechnet man die multiplikative Gruppe des Restklassenringes, um dann die Erzeugenden für die unendlichen Stellen hinzuzufügen. Dann faktorisiert man nach der durch das Bild der Einheitengruppe gegebenen Untergruppe. Man berechnet Erzeugende der Klassengruppe, die teilerfremd zu $\mathfrak{m}_0$ sind und mit diesen und Lemma I.19 Erzeugende und Relationen der Strahlklassengruppe.

ALGORITHMUS II.11 (STRAHLKLASSENGRUPPE).
Eingabe: $\mathfrak{o}_{\mathbf{K}}, \mathbf{U}_{\mathbf{K}}, \mathbf{Cl}_{\mathbf{K}}, \mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$
Ausgabe: $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$

- *Berechne* $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{m}_0)^*$.
- *Berechne* $\prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}$.
- *Berechne* $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}} \cong (\mathfrak{o}_{\mathbf{K}}/\mathfrak{m}_0)^* \times \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}$.
- *Bestimme* $\mathbf{U}_{\mathbf{K}}/\mathbf{U}_{\mathfrak{m}}$ *als Bild von* $\mathbf{U}_{\mathbf{K}}$ *in* $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$.
- *Faktorisiere* $(\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}})$ *nach* $(\mathbf{U}_{\mathbf{K}}/\mathbf{U}_{\mathfrak{m}})$.
- *Berechne Erzeugende von* $\mathbf{Cl}_{\mathbf{K}}$*, die teilerfremd zu* $\mathfrak{m}_0$ *sind.*
- *Berechne Erzeugende und Relationen von* $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$.
- *Berechne eine Basis von* $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$.

Beispiel II.12 (Strahlklassengruppen von $\mathbb{Q}$). *Es sei* $\mathfrak{p}_\infty$ *die unendliche Stelle von* $\mathbb{Q}$ *und* $(m) = m\mathbb{Z}$ *das von* $m \in \mathbb{Z}$ *erzeugte Ideal von* $\mathbb{Q}$. *Wir werden die Strahlklassengruppe von* $\mathbb{Q}$ *modulo* $\mathfrak{p}_\infty(m)$ *bestimmen. Zunächst gilt* $\mathbb{Q}^{(m)}/\mathbb{Q}_{(m)} \cong (\mathbb{Z}/m\mathbb{Z})^*$. $\mathbb{Q}^{\mathfrak{p}_\infty}/\mathbb{Q}_{\mathfrak{p}_\infty}$ *besteht aus den Klassen von* -1 *und* 1. *Damit besteht* $\mathbb{Q}^{\mathfrak{p}_\infty(m)}/\mathbb{Q}_{\mathfrak{p}_\infty(m)}$ *aus den Klassen* $\{[n] \mid -m < n < m, (n,m) = 1\}$. *Die Einheitengruppe* $\mathbf{U}_\mathbb{Q}$ *besteht aus* -1 *und* 1. *Da die Untergruppe* $\mathbf{U}_\mathbb{Q}/\mathbf{U}_{\mathfrak{p}_\infty(m))}$ *von* $[-1]$ *und* $[1]$ *erzeugt wird, sind* $\{[n\mathbb{Z}] \mid 0 < n < m, (n,m) = 1\}$ *die Klassen von* $\mathbf{I}^\mathbb{Q}/\mathbf{H}_\mathbb{Q}$. *Somit erhalten wir, da die Klassenzahl von* $\mathbb{Q}$ *eins ist,* $\mathbf{Cl}_\mathbb{Q}^{\mathfrak{p}_\infty(m)} \cong (\mathbb{Z}/m\mathbb{Z})^*$ *und* $\mathbf{h}_\mathbb{Q}^{\mathfrak{p}_\infty(m)} = \varphi(m)$.

Ohne die unendliche Stelle $\mathfrak{p}_\infty$ *ergibt sich für* $m \neq 2$ *die Strahlklassenzahl* $\mathbf{h}_\mathbb{Q}^{(m)} = \frac{\varphi(m)}{[\mathbf{U}_\mathbb{Q}:\mathbf{U}_{(m)}]} = \frac{\varphi(m)}{2}$, *wir erhalten also nur halb soviele Klassen. Es gilt* $\mathbf{h}_\mathbb{Q}^{(2)} = 1$.

KAPITEL III

Die multiplikative Gruppe von Restklassenringen

Es sei $\mathbf{K}$ ein algebraischer Zahlkörper und $\mathfrak{m}_0$ ein Ideal von $\mathbf{K}$. Nach dem Chinesischen Restsatz gilt:

$$(\mathfrak{o}_{\mathbf{K}}/\mathfrak{m}_0)^* \cong \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m_\mathfrak{p}})^*.$$

Ist $\mathfrak{p}$ ein Primideal über p von $\mathbf{K}$, $\mathbf{K}_\mathfrak{p}$ die Vervollständigung von $\mathbf{K}$ bezüglich $|\cdot|_\mathfrak{p}$ und $\mathfrak{o}_\mathfrak{p}$ der Bewertungsring von $\mathbf{K}_\mathfrak{p}$ mit Bewertungsideal $\mathfrak{b}_\mathfrak{p}$, dann gilt:

$$(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^m)^* \cong (\mathfrak{o}_\mathfrak{p}/{\mathfrak{b}_\mathfrak{p}}^m)^*.$$

Es sei $\mathbf{U}_\mathfrak{p}$ die Einheitengruppe von $\mathfrak{o}_\mathfrak{p}$. Jedes $a \in \mathbf{K}_\mathfrak{p}$ läßt sich schreiben als $a = \pi^k\varepsilon$, wobei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, $\varepsilon \in \mathbf{U}_\mathfrak{p}$ eine Einheit von $\mathfrak{o}_\mathfrak{p}$ und $k \in \mathbb{Z}$ ist.

Der folgenden Satz liefert uns eine Untergruppe von $\mathbf{U}_\mathfrak{p}$, die isomorph zur multiplikativen Gruppe von $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})$ ist. Einen Beweis findet man in [Nar90].

Satz III.1. *Die Gruppe Ξ aller Einheitswurzeln von $\mathbf{K}_\mathfrak{p}$ mit zu p teilerfremder Ordnung hat die Ordnung $\mathbf{N}(\mathfrak{p}) - 1$. Sie bildet ein vollständiges Vertretersystem für die multiplikative Gruppe $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^*$ von $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$.*

Damit können wir die Einheiten von $\mathbf{K}_\mathfrak{p}$ wiederum als $\varepsilon = \xi\eta$ schreiben, wobei $\xi \in \Xi$ und $\eta \equiv 1 \bmod \mathfrak{b}_\mathfrak{p}$ gilt. Die Einheiten von $\mathbf{K}_\mathfrak{p}$ sind also isomorph zum direkten Produkt $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^* \times (1 + \mathfrak{b}_\mathfrak{p})$ der multiplikativen Gruppe des Restklassenkörpers mit den Einseinheiten $(1 + \mathfrak{b}_\mathfrak{p})$ von $\mathbf{K}_\mathfrak{p}$.

Lemma III.2. *Es gilt*

$$(\mathfrak{o}_\mathfrak{p}/{\mathfrak{b}_\mathfrak{p}}^m)^* \cong (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^* \times (1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m).$$

Beweis. Die Abbildung $\mathbf{U}_\mathfrak{p} \to (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^* \times (1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$, $\xi\eta \mapsto ([\xi], [\eta])$ ist surjektiv mit Kern $1 + {\mathfrak{b}_\mathfrak{p}}^m$. Die Abbildung $\mathbf{U}_\mathfrak{p} \to (\mathfrak{o}_\mathfrak{p}/{\mathfrak{b}_\mathfrak{p}}^m)^*$, $\varepsilon \mapsto ([\varepsilon])$ hat ebenfalls den Kern $1 + {\mathfrak{b}_\mathfrak{p}}^m$. $\square$

Es gilt:

$$(1+\mathfrak{p})/(1+\mathfrak{p}^m) \cong (1+\mathfrak{b}_\mathfrak{p})/(1+{\mathfrak{b}_\mathfrak{p}}^m).$$

Somit ist

$$(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^* \cong (\mathfrak{o}_\mathbf{K}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m).$$

Die multiplikative Gruppe des Restklassenkörpers $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ ist zyklisch von der Ordnung $\mathbf{N}(\mathfrak{p}) - 1 = p^\mathrm{f} - 1$. Ein primitives Element von $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$ findet man mit dem Algorithmus von Gauss, siehe [PZ89]. Wir benötigen nun ein Element der Ordnung $p^\mathrm{f} - 1$ in $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$ als Erzeugendes für den Faktor $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$. Man erhält ein Element mit der gewünschten Eigenschaft, indem man einen Vertreter des primitiven Elementes in $\mathfrak{o}_\mathbf{K}$ mit der Ordnung des größten zyklischen Faktors von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ potenziert.

Wir werden Erzeugende und Relationen für die Gruppe $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ bestimmen und einen Algorithmus zur Darstellung der Gruppenelemente bezüglich dieser Basis angeben.

Das Verfahren von Cohen, Diaz y Diaz und Olivier [CDyDO95] basiert auf der Isomorphie

$$(1+\mathfrak{p}^m)/(1+\mathfrak{p}^l) \cong (\mathfrak{p}^m/\mathfrak{p}^l)^+, \text{ für } m \text{ mit } m \le l \le 2m.$$

und darauf, daß sich $(\mathfrak{p}^k/\mathfrak{p}^l)^+$ einfach berechnen läßt.

Unser Verfahren baut auf der expliziten Darstellung der multiplikativen Gruppe von $\mathfrak{p}$ - adischen Zahlkörpern von H. Hasse [Has63] auf, siehe dazu auch [Nak79].

Das Verfahren mit Einseinheiten

Eine Einseinheit $\eta_\nu \in 1 + \mathfrak{b}_\mathfrak{p}$ heißt Einseinheit ν - ter Stufe, wenn gilt:

$$\eta_\nu \equiv 1 \bmod {\mathfrak{b}_\mathfrak{p}}^\nu.$$

Die Einseinheiten einer Stufe bilden eine Untergruppe der Einseinheiten von $\mathbf{K}_\mathfrak{p}$. Für die Einseinheiten ν - ter Stufe gilt

$$\eta_\nu \equiv (1 + a_\nu \pi^\nu) \bmod {\mathfrak{b}_\mathfrak{p}}^{\nu+1}$$

mit ganzem modulo $\mathfrak{b}_\mathfrak{p}$ eindeutig bestimmten a_ν. Wenn $\eta_{\nu+1}$ Einseinheit $(\nu + 1)$ - ter Stufe ist und a_ν aus einem gegebenen Vertretersystem von $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$ ist, erhalten wir die eindeutige Darstellung

$$\eta_\nu = (1 + a_\nu \pi^\nu)\eta_{\nu+1}.$$

Wählt man nun für jede Stufe ein Vertretersystem R_ν von $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$, so erhält man für eine Einseinheit $\eta \in 1 + \mathfrak{b}_\mathfrak{p}$ die eindeutige Darstellung

$$\eta = \prod_{\nu=1}^{\infty} (1 + a_\nu \pi^\nu),$$

wobei $a_\nu \in R_\nu$ ist.

Damit erhalten wir auch eine eindeutige Darstellung der Elemente der Gruppe $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$ durch

$$[\eta] = \prod_{\nu=1}^{m-1} [1 + a_\nu \pi^\nu].$$

Lemma III.3. *Die Abbildung*

$$\begin{array}{llll} \Psi : & (1 + {\mathfrak{b}_\mathfrak{p}}^m)/(1 + {\mathfrak{b}_\mathfrak{p}}^{m+1}) & \longrightarrow & (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \\ \Psi : & [1 + a\pi^m] & \longmapsto & \overline{a} \end{array}$$

ist ein Isomorphismus.

Beweis. Für jedes $[\eta] \in (1+{\mathfrak{b}_\mathfrak{p}}^m)/(1+{\mathfrak{b}_\mathfrak{p}}^{m+1})$ ist a durch $[\eta] = [1+a\pi^m]$ modulo ${\mathfrak{b}_\mathfrak{p}}^{m+1}$ eindeutig bestimmt, somit ist die Abbildung wohldefiniert und bijektiv. Es seien $[1 + a\pi^m], [1 + b\pi^m] \in (1 + {\mathfrak{b}_\mathfrak{p}}^m)/(1 + {\mathfrak{b}_\mathfrak{p}}^{m+1})$, dann gilt: $\Psi([1 + a\pi^m][1 + b\pi^m]) = \Psi([1 + ab\pi^{2m} + a\pi^m + b\pi^m]) = \Psi([1 + (a + b)\pi^m]) = \overline{a + b} = \overline{a} + \overline{b} = \Psi([1 + a\pi^m]) + \Psi([1 + b\pi^m])$, womit die Abbildung ein Homomorphismus ist. □

Es sei $(\omega_1, \dots, \omega_\mathrm{f})$ ein Vertretersystem einer $\mathbb{Z}/\mathbb{Z}_p$-Basis von $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$, dann ist $([1 + \omega_1\pi^m], \dots, [1 + \omega_\mathrm{f}\pi^m])$ eine Basis von $(1 + {\mathfrak{b}_\mathfrak{p}}^m)/(1 + {\mathfrak{b}_\mathfrak{p}}^{m+1})$ und jedes $[a] \in (1 + {\mathfrak{b}_\mathfrak{p}}^m)/(1 + {\mathfrak{b}_\mathfrak{p}}^{m+1})$ besitzt die Basisdarstellung

$$[a] = \prod_{i=1}^{\mathrm{f}} [1 + \omega_i \pi^m]^{\alpha_i} \quad (0 \leq \alpha_i < p).$$

Für die Ordnung von $1+\omega_i\pi^m$ gilt $\operatorname{ord}([1+\omega_i\pi^m]) = p$.

Wir werden nun zeigen, daß die p-ten Potenzen von Repräsentanten einer Stufe Repräsentanten weiterer Stufen sind und hieraus eine Basisdarstellung der multiplikativen Gruppe $(1+\mathfrak{b}_\mathfrak{p})/(1+\mathfrak{b}_\mathfrak{p}{}^m)$ entwickeln.

Satz III.4 (p - Potenzierungsregel). *Es sei e der Verzweigungsindex von $\mathfrak{b}_\mathfrak{p}$. Es sei $\eta_\nu \equiv 1 + a\pi^\nu \bmod \mathfrak{b}_\mathfrak{p}{}^{\nu+1}$ mit $a\in\mathfrak{o}_\mathfrak{p}$, dann folgt:*

$$\eta_\nu^p \equiv \begin{cases} 1 \qquad\qquad + a^p\pi^{p\nu} & \bmod^* \ \mathfrak{b}_\mathfrak{p}{}^{p\nu+1} \quad falls \quad \nu < \frac{e}{p-1} \\ 1 + ap\pi^\nu + a^p\pi^{p\nu} & \bmod^* \ \mathfrak{b}_\mathfrak{p}{}^{p\nu+1} \quad falls \quad \nu = \frac{e}{p-1} \\ 1 + ap\pi^\nu & \bmod^* \ \mathfrak{b}_\mathfrak{p}{}^{\nu+e+1} \quad falls \quad \nu > \frac{e}{p-1}. \end{cases}$$

Wenn wir die Zerlegung von p als

$$p = -\pi^e\varepsilon$$

ansetzen, wobei $v_\mathfrak{p}(\pi)=1$ und $\epsilon\in\mathbf{U}_\mathfrak{p}$ sind, erhalten wir

$$\eta_\nu^p \equiv \begin{cases} 1 + a^p\pi^{p\nu} & \bmod^* \ \mathfrak{b}_\mathfrak{p}{}^{p\nu+1} \quad falls \quad \nu < \frac{e}{p-1} \\ 1 + (a^p-\varepsilon a)\pi^{p\nu} & \bmod^* \ \mathfrak{b}_\mathfrak{p}{}^{p\nu+1} \quad falls \quad \nu = \frac{e}{p-1} \\ 1 - \varepsilon a\pi^{\nu+e} & \bmod^* \ \mathfrak{b}_\mathfrak{p}{}^{\nu+e+1} \quad falls \quad \nu > \frac{e}{p-1}. \end{cases}$$

Der zweite Fall kommt nur vor, wenn $(p-1)|\mathrm{e}$ gilt. In diesem Fall gilt $p\nu = \nu+\mathrm{e}$. Der Beweis stammt aus [Has63].

Beweis. Es sei o.B.d.A. $\eta_\nu = 1+a\pi^\nu$, dann erhalten wir

$$\begin{aligned}(1+a\pi^\nu)^p &= \sum_{j=0}^{p}\binom{p}{j}(a\pi^\nu)^j \\ &= 1 + pa\pi^\nu + \binom{p}{2}a^2\pi^{2\nu} + \cdots + \binom{p}{p-1}a^{p-1}\pi^{(p-1)\nu} + a^p\pi^{p\nu}.\end{aligned}$$

Es gilt $p\mathfrak{o}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}{}^e$, also sind die Summanden der Reihenfolge nach in

$$\mathfrak{b}_\mathfrak{p}{}^{\nu+e}, \mathfrak{b}_\mathfrak{p}{}^{2\nu+e}, \ldots, \mathfrak{b}_\mathfrak{p}{}^{(p-1)\nu+e}, \mathfrak{b}_\mathfrak{p}{}^{p\nu}.$$

enthalten. Somit gilt:

(1) Für $\nu < \frac{\mathrm{e}}{p-1}$ sind alle Summanden bis auf $a^p\pi^{p\nu}$ in $\mathfrak{b}_\mathfrak{p}{}^{p\nu+1}$ enthalten
(2) Für $\nu = \frac{\mathrm{e}}{p-1}$ sind alle Summanden bis auf $pa\pi^\nu$ und $a^p\pi^{p\nu}$ in $\mathfrak{b}_\mathfrak{p}{}^{p\nu+1}$ enthalten
(3) Für $\nu < \frac{\mathrm{e}}{p-1}$ sind alle Summanden bis auf $pa\pi^\nu$ in $\mathfrak{b}_\mathfrak{p}{}^{\nu+e+1}$ enthalten.

Damit ist die Aussage bewiesen. □

Wir werden zeigen, daß ein Erzeugendensystem der ν - ten Stufe auch ein Erzeugendensystem der $p\nu$ - ten beziehungsweise der $\nu+1$ - ten Stufe ist, wenn $(p-1) \nmid \mathrm{e}$ gilt.

Lemma III.5. *Die Abbildungen*

$$h_1 : (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \longrightarrow (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \quad , \quad a + \mathfrak{b}_\mathfrak{p} \longmapsto a^p + \mathfrak{b}_\mathfrak{p}$$
$$h_3 : (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \longrightarrow (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \quad , \quad a + \mathfrak{b}_\mathfrak{p} \longmapsto -\varepsilon a + \mathfrak{b}_\mathfrak{p}$$

sind Gruppenisomorphismen und

$$h_2 : (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \longrightarrow (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+ \quad , \quad a + \mathfrak{b}_\mathfrak{p} \longmapsto a^p - \varepsilon a + \mathfrak{b}_\mathfrak{p}$$

ist ein Gruppenhomomorphismus.

Beweis. h_1 ist der Frobeniusautomorphismus; h_3 ist ein Homomorphismus in einer endlichen Gruppe mit $\mathrm{Kern}(h_3) = \{[0]\}$, also ein Automorphismus; h_2 ist als Summe zweier Gruppenhomomorphismen ein Gruppenhomomorphismus. $\square$

Ist $\eta_{1\nu}, \dots, \eta_{\mathrm{f}\nu}$ ein Erzeugendensystem für die Stufe $\nu < \frac{\mathrm{e}}{p-1}$ (für die Stufe $\nu > \frac{\mathrm{e}}{p-1}$), so ist $\eta_{1\nu}, \dots, \eta_{\mathrm{f}\nu}$ ein Erzeugendensystem für die Stufe $p\nu$ (für die Stufe $\nu + e$). Die Stufe $\nu = \frac{\mathrm{e}}{p-1}$ muß gesondert betrachtet werden, da h_2 im allgemeinen kein Isomorphismus ist.

Bemerkung III.6. *Der Kern von h_2 hat entweder die Ordnung eins oder p.*

Beweis. Die Abbildung $h_2 : \alpha \longmapsto \alpha^p - \varepsilon\alpha$ ist ein Homomorphismus von $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+$ auf eine Untergruppe von $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+$. Die Untergruppen von $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+$ haben Ordnungen $p^s, s \leq \mathrm{f}$. Das Polynom $x^p - \varepsilon x = 0$ über dem Körper $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ hat höchstens p Nullstellen. Also ist die Ordnung des Kerns von h_2 entweder eins oder p. $\square$

Wir unterscheiden im folgenden zwei Fälle:

- Fall I:
  - $(p-1)$ teilt nicht e oder
  - h_2 ist ein Isomorphismus oder
  - es gilt $m \leq \frac{p\mathrm{e}}{p-1}$.
- Fall II:
  - Es gilt $m > \frac{p\mathrm{e}}{p-1}$ und
  - es gilt $(p-1) \mid \mathrm{e}$ gilt und
  - h_2 ist kein Isomorphismus.

Im Fall I sind die p - Potenzen der Erzeugendensysteme einer Stufe wieder Erzeugendensysteme weiterer Stufen von $(1+\mathfrak{b}_\mathfrak{p})/(1+\mathfrak{b}_\mathfrak{p}{}^m)$. Diese weiteren Stufen erhalten wir durch wiederholtes Anwenden der Substitution

$$\nu \rightarrow \begin{cases} p\nu & \textit{für} \quad \nu < \frac{\mathrm{e}}{p-1} \\ p\nu = \nu + \mathrm{e} & \textit{für} \quad \nu = \frac{\mathrm{e}}{p-1} \\ \nu + \mathrm{e} & \textit{für} \quad \nu > \frac{\mathrm{e}}{p-1}. \end{cases}$$

Die Erzeugendensysteme für die Stufen $\nu \geq \frac{\mathrm{e}}{p-1} + \mathrm{e} = \frac{p\mathrm{e}}{p-1}$ gehen aus den Erzeugendensystemen der Stufen $\nu' < \frac{\mathrm{e}}{p-1} + \mathrm{e} = \frac{p\mathrm{e}}{p-1}$ hervor. Auch gehen Erzeugendensysteme der Stufen ν mit $p \mid \nu$ aus Erzeugendensystemen niedrigerer Stufen hervor. Wir definieren also

$$F_{\mathrm{e}} := \{\nu \mid 0 < \nu < \frac{p\mathrm{e}}{p-1}, p \not| \nu\}$$

als das System der Grundstufen für $\mathfrak{b}_\mathfrak{p}$. Alle Stufen lassen sich durch die Substitutionen von den Grundstufen aus erreichen. Die Anzahl der natürlichen Zahlen, die kleiner als $\frac{p\mathrm{e}}{p-1}$ sind, ist $\lfloor \frac{p\mathrm{e}}{p-1} \rfloor$, davon sind $\lfloor \frac{p\mathrm{e}}{p(p-1)} \rfloor$ durch p teilbar. Also besteht F_{e} aus $\lfloor \frac{p\mathrm{e}}{p-1} \rfloor - \lfloor \frac{p\mathrm{e}}{p(p-1)} \rfloor = p \lfloor \frac{e}{p-1} \rfloor - \lfloor \frac{\mathrm{e}}{(p-1)} \rfloor = \lfloor \frac{(p-1)e}{p-1} \rfloor = e$ Elementen.

Satz III.7 (Basisdarstellung im Fall I). *Wenn*

- $(p-1)$ *nicht* e *teilt oder*
- h_2 *ein Isomorphismus ist oder*
- $m < \frac{e}{p-1}$ *ist,*

ist die Klasse $[\eta] \in (1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$ *in Basisdarstellung gegeben durch:*

$$[\eta] = \prod_{\nu \in F_{\mathrm{e}}} \prod_{i=1}^{f} [\eta_{i\nu}]^{\alpha_{i\nu}} \quad (0 \leq \alpha_{i\nu} < \mathrm{ord}([\eta_{i\nu}])),$$

wobei $\eta_{i\nu} = 1 + \omega_i \pi^\nu$ *ist und* $\omega_1, \ldots, \omega_f$ *Vertretersystem einer* $\mathbb{Z}/p\mathbb{Z}$ *- Basis von* $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ *in* $\mathfrak{o}_\mathfrak{p}$ *ist. Für die Ordnung von* $\eta_{i\nu}$ *gilt* $\mathrm{ord}([\eta_{i\nu}]) = p^{s_\nu}$ *mit*

$$\begin{aligned}
s_\nu &= \begin{cases} 0, & \nu \geq m \\ s_{1\nu} + s_{2\nu} + 1, & \nu < m \end{cases} \\
s_{1\nu} &= \begin{cases} \lfloor \log_p(\frac{m-1}{\nu}) \rfloor, & m \leq \frac{pe}{p-1} \\ \lfloor \log_p(\frac{pe}{\nu(p-1)}) \rfloor, & m > \frac{pe}{p-1} \end{cases} \\
s_{2\nu} &= \begin{cases} 0, & m \leq \frac{pe}{p-1} \\ \lfloor \frac{m-1-\nu^{s_{1\nu}}}{e} \rfloor, & m > \frac{pe}{p-1}. \end{cases}
\end{aligned}$$

Beweis. Wir werden mit dem Beweis für die Ordnungen der $\eta_{i\nu}$ beginnen und danach zeigen, daß eine Basisdarstellung vorliegt.

Wenn $\nu \geq m$ ist, gilt $\mathrm{ord}([\eta_{i\nu}]) = 1$. Für $\nu < m \leq \frac{p\mathrm{e}}{p-1}$ sind die Erzeugenden der Grundstufe $\nu \in F_{\mathrm{e}}$ Erzeugende der Stufen $p^{s_1}\nu$, wobei $s_1 \in \mathbb{Z}^{>0}$ mit $p^{s_1}\nu < m$ ist. Wir suchen nun das größte $s_{1\nu}$, welches die letzte Ungleichung erfüllt. Mit $p^{s_{1\nu}}\nu \leq m - 1$ erhalten wir $s_{1\nu} = \lfloor \log_p(\frac{m-1}{\nu}) \rfloor$. Somit ist $p^{s_{1\nu}}\nu$ die höchste Stufe in $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$, zu der $\eta_{i\nu}$ ein Erzeugendensystem ist. Nach der p - Potenzierungsregel und der Wahl von $s_{1\nu}$ gilt $\eta_{i\nu}^{p^{s_{1\nu}+1}} \equiv 1 \bmod {\mathfrak{b}_\mathfrak{p}}^m$. Damit ist $p^{s_{1\nu}+1}$ die Ordnung der Klasse $[\eta_{i\nu}]$ in $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$.

Für $m > \frac{p\mathrm{e}}{p-1}$ sind die $\eta_{i\nu}$ die Erzeugenden der Stufen $p^{s_1}\nu + s_2\mathrm{e}$ mit $s_1, s_2 \in \mathbb{Z}^{>0}$, so daß $p^{s_1}\nu + s_2\mathrm{e} < m$ und $p^{s_1}\nu < \frac{p\mathrm{e}}{p-1}$ gilt. Wir suchen nun wieder die größte Stufe, deren Erzeugende p - Potenzen von $\eta_{i\nu}$ sind. Wir können $s_{1\nu}$ wie oben mit $m = \frac{p\mathrm{e}}{p-1}$ bestimmen. Es gilt also $p^{s_{1\nu}}\nu + s_2\mathrm{e} \leq m-1$ und somit erhalten wir für das größte $s_{2\nu}$, das die Ungleichung erfüllt, $s_{2\nu} = \lfloor \frac{m-1-p^{s_{1\nu}}\nu}{\mathrm{e}} \rfloor$. Wie oben ist die Ordnung von $[\eta_{i\nu}]$ um eine p - Potenz höher, also $s_\nu = s_{1\nu} + s_{2\nu} + 1$.

Wir zeigen durch Induktion nach m, daß eine Basisdarstellung vorliegt. Es sei $\eta \in 1 + \mathfrak{b}_\mathfrak{p}$ und $\omega_1, \ldots, \omega_\mathrm{f}$ Vertretersystem einer $\mathbb{Z}/p\mathbb{Z}$ - Basis von $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$. Wir bezeichnen mit $[\eta]_k$ die Klasse von η in $(1+\mathfrak{b}_\mathfrak{p})/(1+{\mathfrak{b}_\mathfrak{p}}^k)$. Wir betrachten zunächst den Fall $(p-1) \nmid \mathrm{e}$. In $(1+\mathfrak{b}_\mathfrak{p})/(1+{\mathfrak{b}_\mathfrak{p}}^2)$ ist die Klasse von η in Basisdarstellung gegeben durch

$$\eta \equiv \prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{\mathrm{f}} (1+\omega_i\pi^\nu)^{\alpha_{i\nu}} \bmod {\mathfrak{b}_\mathfrak{p}}^2 \quad \left(0 \leq \alpha_{i\nu} < \operatorname{ord}([1+\omega_i\pi^\nu]_1) = \begin{cases} 1, & \nu \neq 1 \\ p, & \nu = 1 \end{cases}\right).$$

Es sei für $k < m$ die Basisdarstellung von $[\eta]$ in $(1+\mathfrak{b}_\mathfrak{p})/(1+{\mathfrak{b}_\mathfrak{p}}^k)$ gegeben:

$$\eta \equiv \prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{\mathrm{f}} (1+\omega_i\pi^\nu)^{\alpha_{i\nu}} \bmod {\mathfrak{b}_\mathfrak{p}}^k \quad (0 \leq \alpha_{i\nu} < \operatorname{ord}([1+\omega_i\pi^\nu]_k)).$$

Wir werden nun $\beta_{11}, \ldots, \beta_{\mathrm{fe}}$ konstruieren, so daß

$$\eta \equiv \prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{\mathrm{f}} (1+\omega_i\pi^\nu)^{\beta_{i\nu}} \bmod {\mathfrak{b}_\mathfrak{p}}^{k+1} \quad (0 \leq \beta_{i\nu} < \operatorname{ord}([1+\omega_i\pi^\nu]_{k+1}))$$

gilt. Es sei $\nu' \in F_\mathrm{e}$ die Grundstufe der Stufe k, es gibt also s_1, s_2, so daß $k = \nu' p^{s_1} + s_2\mathrm{e}$ ist und $\max\{s \in \mathbb{Z} \mid \nu' p^s < \min(k, \frac{p\mathrm{e}}{p-1})\}$ gilt. Es sei

$$\eta' = \frac{\eta}{\prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{\mathrm{f}} (1+\omega_i\pi^\nu)^{\alpha_{i\nu}}}.$$

Damit ist η' eine Einseinheit k-ter Stufe. Es seien $\omega'_1, \ldots, \omega'_f$ gegeben durch $\omega'_i = h_3^{s_3}(h_1^{s_1}(\omega_i))$. Es existieren $\gamma_1, \ldots, \gamma_f$ mit $0 \leq \gamma_i < p$, so daß gilt:

$$\eta' \equiv \prod_{i=1}^{\mathrm{f}} (1+\omega'_i\pi^k)^{\gamma_i} \bmod {\mathfrak{b}_\mathfrak{p}}^{k+1}$$

Dann gilt:

$$\eta \equiv \prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{\mathrm{f}} (1+\omega_i\pi^\nu)^{\alpha_{i\nu}} \prod_{i=1}^{\mathrm{f}} (1+\omega'_i\pi^k)^{\gamma_i} \bmod {\mathfrak{b}_\mathfrak{p}}^{k+1}.$$

Die ω_i waren gerade so gewählt, daß $(1+\omega_i\pi^{\nu'})^{p^{s_1+s_2}} \equiv (1+\omega_i'\pi^k) \bmod \mathfrak{p}^{k+1}$ ist, also gilt:

$$\prod_{i=1}^{\mathrm{f}}(1+\omega_i'\pi^k)^{\gamma_i} \equiv \prod_{i=1}^{\mathrm{f}}(1+\omega_i'\pi^{\nu'})^{\gamma_i p^{s_1+s_2}} \bmod {\mathfrak{b}_{\mathfrak{p}}}^{k+1}.$$

Mit $\beta_{i\nu} := \begin{cases} \alpha_{i\nu}, & \nu \neq \nu' \\ \alpha_{i\nu}+\gamma_i p^{s_1+s_2}, & \nu = \nu' \end{cases}$ erhalten wir die Darstellung

$$\eta \equiv \prod_{\nu\in F_{\mathrm{e}}}\prod_{i=1}^{\mathrm{f}}(1+\omega_i\pi^\nu)^{\beta_{i\nu}} \bmod {\mathfrak{b}_{\mathfrak{p}}}^{k+1} \quad \left(0 \leq \beta_{i\nu} < \begin{cases} \operatorname{ord}([1+\omega_i\pi^\nu]_k), & \nu \neq \nu' \\ p\operatorname{ord}([1+\omega_i\pi^\nu]_k), & \nu = \nu' \end{cases}\right).$$

Die Erzeugenden der Stufe ν' sind die Erzeugenden der neuen Stufe k. Aus der p - Potenzierungsregel folgt, daß sich die Ordnung von $(1+\omega_i\pi^{\nu'})$ um den Faktor p erhöht und ebenso, daß sich die Ordnungen der anderen Erzeugenden nicht verändern. Es handelt sich also um die gesuchte Basisdarstellung.

Im Fall $(p-1) \mid \mathrm{e}$ geht man analog vor, man muß nur den Isomorphismus $h_2 : \omega \mapsto p\omega - \varepsilon\omega$ beim Schritt von der Stufe $\frac{\mathrm{e}}{p-1}$ zur Stufe $\frac{p\mathrm{e}}{p-1}$ benutzen. □

Wie wir wissen, gilt $(1+\mathfrak{p})/(1+\mathfrak{p}^m) \cong (1+\mathfrak{b}_{\mathfrak{p}})/(1+{\mathfrak{b}_{\mathfrak{p}}}^m)$. Wenn wir $\pi \in \mathfrak{o}_{\mathbf{K}}$ und $\omega_1,\dots,\omega_{\mathrm{f}} \in \mathfrak{o}_{\mathbf{K}}$ wählen, haben wir mit der Basisdarstellung in $(1+\mathfrak{b}_{\mathfrak{p}})/(1+{\mathfrak{b}_{\mathfrak{p}}}^m)$ eine Basisdarstellung in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$. Eine Darstellung in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ durch Erzeugende und Relationen ist damit gegeben. Die Erzeugenden sind die $\eta_{i\nu}$ und die Relationenmatrix eine Diagonalmatrix mit den Einträgen $\operatorname{ord}([\eta_{i\nu}])$.

Algorithmus III.8 (Erzeugende und Relationen im Fall I).

<u>Eingabe:</u> $\mathfrak{o}_{\mathbf{K}}$, $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{K}}$, *e, f, p,* $m \in \mathbb{Z}^{>0}$

<u>Ausgabe:</u> *Erzeugende und Relationen* (g, M) *von* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$,
Vertretersystem $(\omega_1,\dots,\omega_f)$ *einer Basis von* $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ *in* $\mathfrak{o}_{\mathbf{K}}$

- *Bestimme* F_e.
- *Wähle ein Vertretersystem* $\omega_1,\dots,\omega_f$ *einer Basis von* $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ *in* $\mathfrak{o}_{\mathbf{K}}$.
- *Setze* $g \leftarrow (\eta_{11},\dots,\eta_{fe})$ *mit* $\eta_{i\nu} = 1+\omega_i\pi^\nu$, *wobei* $i = 1,\dots,f$ *und* $\nu \in F_e$.
- *Setze* $M \leftarrow \operatorname{diag}(M_{11},\dots,M_{fe})$ *mit* $M_{i\nu} = \operatorname{ord}(\eta_{i\nu})$, *wobei* $i = 1,\dots,f$ *und* $\nu \in F_e$ *sind.*
- *Gib* (g, M) *und* $(\omega_1,\dots,\omega_f)$ *zurück.*

Das Verfahren, um die Klasse eines gegeben $\eta \in 1+\mathfrak{p}$ bezüglich der Erzeugenden von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ darzustellen, haben wir im Beweis von III.7 schon angewendet. Wenn eine Darstellung $[\eta] = [\alpha g_k]$ bezüglich der Erzeugenden g_k von $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$ gegeben ist, findet man eine Darstellung bezüglich der Erzeugenden g_{k+1} von $(1+\mathfrak{p})/(1+\mathfrak{p}^{k+1})$, indem man erst für die Einseinheit k - ter Stufe $\eta' = \frac{\eta}{\alpha g_k}$ eine Darstellung γ bezüglich einem bestimmten Erzeugendensystem von $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^{k+1})$ berechnet und dann β aus α und γ konstruiert. Das Erzeugendensystem von

$(1+\mathfrak{p}^k)/(1+\mathfrak{p}^{k+1})$ ist durch das anfangs gewählte Vertretersystem $\omega_1, \dots, \omega_{\mathrm{f}}$ einer $\mathbb{Z}/p\mathbb{Z}$ Basis von $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ und die Anzahl und Art der Substitutionsschritte bestimmt. Es seien s_1, s_2, s_3 so gewählt, daß

$$\begin{array}{lcl} k & = & \nu' p^{s_1} + s_2 \mathrm{e} + s_3 \mathrm{e} \\ \nu' & \in & F_{\mathrm{e}} \\ s_1 & = & \max\{s \in \mathbb{Z} \mid \nu' p^s < \min(k, \frac{p\mathrm{e}}{p-1})\} \\ s_2 & = & \begin{cases} 1 & \text{falls} \quad \nu' p^{s_1} = \frac{\mathrm{e}}{p-1} \\ 0 & \text{sonst} \end{cases} \end{array}$$

ist. Es sei $\omega_i' = h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$. Um $\gamma = (\gamma_1 \ \cdots \ \gamma_f)$ mit

$$\eta' \equiv \prod_{i=1}^{\mathrm{f}} (1 + \omega_i' \pi^k)^{\gamma_i} \bmod^* \mathfrak{p}^{k+1}$$

zu bestimmen, brauchen wir nur eine Lösung von

$$\frac{\eta' - 1}{\pi^k} \equiv \sum_{i=1}^{\mathrm{f}} \gamma_i \omega_i' \bmod^* \mathfrak{p}$$

zu berechnen. Dann ist die Darstellung von η in $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^{k+1})$ gegeben durch:

$$\beta = (\alpha_{11}, \dots, \alpha_{1\nu'} + p^{s_1+s_2+s_3}\gamma_1, \dots, \alpha_{\mathrm{f}\nu'} + p^{s_1+s_2+s_3}\gamma_{\mathrm{f}}, \cdots, \alpha_{\mathrm{fe}}).$$

Algorithmus III.9 (Basisdarstellung im Fall I).

Eingabe: $\eta \in 1 + \mathfrak{p}$,
$\mathfrak{o}_{\mathbf{K}}$, $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{K}}$, e, f, p, $m \in \mathbb{Z}^{>0}$,
Erzeugende und Relationen (g, M) *von* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$,
dazugehöriges Vertretersystem $(\omega_1, \cdots, \omega_n)$

Ausgabe: α *mit* $[\alpha g] = [\eta]$

- *Setze* α *auf den* $\mathbb{Z}^{fe}$ *Nullvektor.*
- *Für alle Stufen* $1 \le \nu < m$*:*
  - *Berechne Grundstufe* ν'.
  - *Berechne Anzahl der Substitutionen* s_1, s_2, s_3.
  - *Setze* $\omega_i' \leftarrow h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$ *für* $i = 1, \dots, f$.
  - *Bestimme* $\gamma_1, \dots, \gamma_f$, *so daß* $\frac{\eta'-1}{\pi^\nu} \equiv \sum_{i=1}^f \gamma_i \omega_i' \bmod \mathfrak{p}$.
  - *Setze* $\alpha \leftarrow (\alpha_{11}, \dots, \alpha_{1\nu'} + p^{s_1+s_2+s_3}\gamma_1, \dots, \alpha_{f\nu'} + p^{s_1+s_2+s_3}\gamma_f, \cdots, \alpha_{fe})$.
  - *Setze* $\eta \leftarrow \frac{\eta}{\prod_{i=1}^{\mathrm{f}} (1+\pi^{p^{s_1+s_2+s_3}} \omega_i')^{\gamma_i}}$.
- *Gib* α *zurück.*

Wenn $(p-1) \mid \mathrm{e}$ gilt und der Kern von h_2 nicht trivial ist, ist das Erzeugendensystem der Stufe $\frac{\mathrm{e}}{p-1}$ keines der Stufe $\frac{p\mathrm{e}}{p-1}$. Die Erzeugenden der Stufe $\frac{\mathrm{e}}{p-1}$ erhalten wir durch p^{μ_0-1} - maliges Anwenden der Substitution $h_1 : a+\mathfrak{p} \mapsto a^p + \mathfrak{p}$ auf die Erzeugenden der Grundstufe e_0 mit $p^{\mu_0-1}\mathrm{e}_0 = \frac{\mathrm{e}}{p-1}$, wobei p nicht e_0 teilt. Wir wissen, daß der Kern von h_2 eine Untergruppe von $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ der Ordnung p ist. Wir können also ein Vertretersystem $\omega_1, \ldots, \omega_\mathrm{f}$ einer Basis von $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ in $\mathfrak{o}_\mathbf{K}$ mit

$$\omega_1^{p^{\mu_0}} - \varepsilon\omega_1^{p^{\mu_0-1}} \equiv 0 \bmod \mathfrak{p}$$

finden, so daß $\omega_1^{p^{\mu_0}}$ den Kern von h_2 erzeugt. Um nun ein Erzeugendensystem der Stufe $\frac{p\mathrm{e}}{p-1}$ zu erhalten, benötigen wir ein zusätzliches Basiselement ω_* von $\mathfrak{o}/\mathfrak{p}$, das nicht im Bild von $h_2 : a+\mathfrak{p} \mapsto a^p - \varepsilon a + \mathfrak{p}$ liegt. Für ω_* muß also gelten:

$$x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p} \text{ ist nicht lösbar.}$$

Damit erhalten wir:

Satz III.10 (Eindeutige Darstellung im Fall II). *Es sei $\mathfrak{p}$ ein Primideal über p mit Verzweigungsindex e und Trägheitsgrad f. Es gelte $(p-1) \mid e$ und h_2 sei kein Isomorphismus.*

Es seien e_0 und μ_0 so gewählt, daß $e = p^{\mu_0-1}(p-1)\mathrm{e}_0$ ist und p nicht e_0 teilt. Es sei $\omega_1, \ldots, \omega_f$ ein Vertretersystem einer Basis von $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ in $\mathfrak{o}_\mathbf{K}$ mit $\omega_1^{p^{\mu_0}} - \varepsilon\omega_1^{p^{\mu_0-1}} \equiv 0 \bmod \mathfrak{p}$ und $\omega_* \in \mathfrak{o}_\mathbf{K}$ sei so gewählt, daß $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ nicht lösbar ist.

Dann ist die Klasse $[\eta] \in (1+\mathfrak{p})/(1+\mathfrak{p}^m)$ in eindeutiger Darstellung gegeben durch

$$[\eta] = \prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{f} [\eta_{i\nu}]^{\alpha_{i\nu}} [\eta_*]^{\alpha_*} \quad \left(\begin{array}{ccccl} 0 & \leq & \alpha_{1\mathrm{e}_0} & < & p^{\mu_0} \\ 0 & \leq & \alpha_{i\nu} & < & \mathrm{ord}([\eta_{i\nu}]) \quad \text{für } (i,\nu) \neq (1,\mathrm{e}_0) \\ 0 & \leq & \alpha_* & < & \mathrm{ord}([\eta_*]) \end{array} \right)$$

mit $\eta_{i\nu} = 1 + \omega_i \pi^\nu$ und $\eta_* = 1 + \omega_* \pi^{p^{\mu_0}\mathrm{e}_0}$.

Es gilt $\mathrm{ord}([\eta_{i\nu}]) = p^{s_\nu}$ für $(i,\nu) \neq (1,\mathrm{e}_0)$, wenn s_ν wie in Satz III.7 gegeben ist, und es gilt $\mathrm{ord}([\eta_*]) = p^{s_*+1}$ mit $s_* = \lfloor \frac{m-1-p^{\mu_0}\mathrm{e}_0}{e} \rfloor$.

Beweis. Nach der Wahl von ω_1 und ω_* handelt es sich um eine eindeutige Darstellung. Die Ordnung von $[\eta_*]$ erhält man folgendermaßen: e_0 und μ_0 waren so gewählt, daß $\frac{p\mathrm{e}}{p-1} = p^{\mu_0}\mathrm{e}_0$ ist, damit ist $\eta_* = 1 + \omega_0\pi^{p^{\mu_0}\mathrm{e}_0}$ eine Einseinheit $p^{\mu_0}\mathrm{e}_0$ - ter Stufe ist. Die p - Potenzen von $[\eta_*]$ sind Teil der Erzeugendensysteme der Stufen $p^{\mu_0}\mathrm{e}_0 + s\mathrm{e}$. Wir suchen das größte s, für das $p^{\mu_0}\mathrm{e}_0 + s\mathrm{e} \leq m-1$ erfüllt ist und erhalten $s_* = \lfloor \frac{m-1-p^{\mu_0}\mathrm{e}_0}{\mathrm{e}} \rfloor$. $\square$

Um die eindeutige Darstellung einer Klasse in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ bezüglich der Erzeugenden zu erhalten, geht man analog zu dem Verfahren im Fall I vor. Man muß nur beachten, daß für Stufen $\nu \geq \frac{p\mathrm{e}}{p-1}$ eines der Erzeugenden, der auf der

Grundstufe e_0 basierenden Stufen η_* ist. η_* ist eine Einseinheit der Stufe $\frac{p\mathrm{e}}{p-1}$. Es seien $\omega_1, \ldots, \omega_\mathrm{f}, \omega_*$ und $\eta_{11}, \ldots, \eta_{\mathrm{fe}}, \eta_*$ wie in Satz III.10 gegeben. Es sei $k \geq \frac{p\mathrm{e}}{p-1}$, so daß $\nu' = \mathrm{e}_0$ die Grundstufe der Stufe k ist. Es seien s_1, s_2, s_3 wie in der Beschreibung des Verfahrens im Fall I gegeben. Es sei $(\alpha_{11}, \ldots, \alpha_{\mathrm{fe}})$ eine Darstellung der Einseinheit η in $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$. Es sei

$$\eta' = \frac{\eta}{\prod_{\nu \in F_\mathrm{e}} \prod_{i=1}^{\mathrm{f}} \eta_{i\nu}^{\alpha_{i\nu}} \eta_*^{\alpha_*}}.$$

Es sei $\omega_1' = h_3^{s_3}(\omega_*)$ und für $i = 1, \ldots, \mathrm{f}$ sei $\omega_i' = h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$. Es sei $\gamma = \gamma_1, \ldots, \gamma_\mathrm{f}$ eine Lösung von

$$\frac{\eta' - 1}{\pi^k} \equiv \sum_{i=1}^{\mathrm{f}} \gamma_i \omega_i' \bmod^* \mathfrak{p}.$$

Dann erhalten wir als Darstellung von η in $(1+\mathfrak{p})/(1+\mathfrak{p}^{k+1})$

$$\beta = (\alpha_{11}, \ldots, \alpha_{1\nu'}, \alpha_{2\nu'} + p^{s_1+s_2+s_3}\gamma_2, \ldots, \alpha_{\mathrm{f}\nu'} + p^{s_1+s_2+s_3}\gamma_\mathrm{f}\mathrm{e}, \ldots, \alpha_{\mathrm{fe}}, \alpha_* + p^{s_3} v_1').$$

Algorithmus III.11 (Eindeutige Darstellung im Fall II).

Eingabe: $\eta \in 1 + \mathfrak{p}$,
$\mathfrak{o}_\mathbf{K}$,$\mathfrak{p}$,p,π,$m \in \mathbb{Z}^{>0}$,f,e,e_0,
Erzeugende g von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$,
$(\omega_1, \cdots, \omega_n, \omega_*)$

Ausgabe: *α mit $[\alpha g] = [\eta]$*

- *Setze α auf den $\mathbb{Z}^{fe+1}$ - Nullvektor.*
- *Für alle Stufen $1 \leq \nu < m$:*
  - *Berechne Grundstufe ν'.*
  - *Berechne Anzahl der Substitutionen s_1, s_2, s_3.*
  - *Wenn $\nu' = e_0$ und $\nu \geq \frac{pe}{p-1}$ ist:*
    - *Setze $\omega_i' \leftarrow h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$ für $i = 2, \ldots, f$.*
    - *Setze $\omega_1' \leftarrow h_3^{s_3}(\omega_*)$.*
    - *Bestimme $\gamma_1, \ldots, \gamma_f$, so daß $\frac{\eta'-1}{\pi^\nu} \equiv \sum_{i=1}^f \gamma_i \omega_i' \bmod \mathfrak{p}$.*
    - *Setze $\alpha \leftarrow (\alpha_{11}, \ldots, \alpha_{1\nu'}, \alpha_{2\nu'} + p^{s_1+s_2+s_3}\gamma_1, \ldots, \alpha_{f\nu'} + p^{s_1+s_2+s_3}\gamma_f, \ldots, \alpha_{fe}, \alpha_* + p^{s_3}\gamma_1)$.*
  - *ansonsten:*
    - *Setze $\omega_i' \leftarrow h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$ für $i = 1, \ldots, f$.*
    - *Bestimme $\gamma_1, \ldots, \gamma_f$, so daß $\frac{\eta'-1}{\pi^\nu} \equiv \sum_{i=1}^f \gamma_i \omega_i' \bmod \mathfrak{p}$.*
    - *$\alpha \leftarrow (\alpha_{11}, \ldots, \alpha_{1\nu'} + p^{s_1+s_2+s_3}\gamma_1, \ldots, \alpha_{f\nu'} + p^{s_1+s_2+s_3}\gamma_f, \cdots, \alpha_{fe})$.*
  - *Setze $\eta \leftarrow \frac{\eta}{\prod_{i=1}^{\mathrm{f}} (1+\pi^{p^{s_1+s_2+s_3}} \omega_i')^{\gamma_i}}$*
- *Gib α zurück.*

Wir werden zeigen, wie man im Fall II Erzeugende und Relationen der Gruppe $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ erhält. Zunächst behandeln wir Fall II im allgemeinen, danach betrachten wir zwei Fälle, in denen die eindeutige Darstellung schon eine Basisdarstellung ist.

In der eindeutigen Darstellung im Fall II war die Potenz $\alpha_{1\mathrm{e}_0}$ von $\eta_{1\mathrm{e}_0}$ auf $\alpha_{1\mathrm{e}_0} < p^{\mu_0}$ beschränkt. Wir erhalten mit Algorithmus III.11 $\alpha = (\alpha_{11}, \dots, \alpha_{\mathrm{fe}}, \alpha_*)$, so daß

$$[\eta_{1\mathrm{e}_0}^{p^{\mu_0}}] = \prod_{i \in F_\mathrm{e}} \prod_{j=1}^{\mathrm{f}} [\eta_{ij}]^{\alpha_{ij}} [\eta_*]^{\alpha_*} \text{ und } \alpha_{1\mathrm{e}_0} = 0 \text{ gelten.}$$

Es sei $g = (\eta_{11}, \cdots, \eta_{\mathrm{fe}}, \eta_*)^T$ der Spaltenvektor der Erzeugenden von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, dann erhalten wir mit $\beta_{i\nu} = \begin{cases} -\alpha_{i\nu} & (i,\nu) \neq (1, \mathrm{e}_0) \\ p^{\mu_0} & (i,\nu) = (1, \mathrm{e}_0) \end{cases}$ und $\beta_* = -\alpha^*$ die Relation

$$(\beta_{11}, \cdots, \beta_{\mathrm{fe}}, \beta_*) g = 0$$

Es sei $\gamma_{i\nu} = \mathrm{ord}([\eta_{i\nu}])$ und $\gamma_* = \mathrm{ord}([\eta_*])$, so ist (g, M) mit

$$(g, M) = \left(\begin{pmatrix} \eta_1 \\ \vdots \\ \eta_{1\mathrm{e}_0} \\ \vdots \\ \eta_{\mathrm{fe}} \\ \eta_* \end{pmatrix}, \begin{pmatrix} \gamma_{11} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & 0 & \cdots & \cdots & 0 \\ \beta_{11} & \cdots & \beta_{1\mathrm{e}_0} & \cdots & \beta_{\mathrm{fe}} & \beta_* \\ 0 & \cdots & 0 & \ddots & 0 & 0 \\ 0 & \cdots & \cdots & 0 & \gamma_{\mathrm{fe}} & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & \gamma_* \end{pmatrix} \right).$$

eine Darstellung von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ durch Erzeugende und Relationen.

Algorithmus III.12 (Erzeugende und Relationen im Fall II).

Eingabe: $\mathfrak{o}_\mathbf{K}$, $\mathfrak{p} \subset \mathfrak{o}_\mathbf{K}$, *e, f, p*

Ausgabe: *Erzeugende und Relationen* (g, M) *von* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, $(\omega_1, \cdots, \omega_n, \omega_*)$

- *Bestimme* F_e.
- *Bestimme* μ_0, e_0, *so daß* $e = p^{\mu_0 - 1}(p-1)\mathrm{e}_0$ *ist und* $p \nmid \mathrm{e}_0$ *gilt.*
- *Bestimme* ω_*, *so daß* $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ *nicht lösbar ist.*
- *Wähle ein Vertretersystem* $\omega_1, \dots, \omega_f$ *einer Basis von* $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ *in* $\mathfrak{o}_\mathbf{K}$ *mit* $\omega_1^{p^{\mu_0}} - \varepsilon \omega_1^{p^{\mu_0 - 1}} \equiv 0 \bmod \mathfrak{p}$.
- *Setze* $g \leftarrow (\eta_{11}, \dots, \eta_{fe}, \eta_*)$ *mit* $\eta_{i\nu} = 1 + \omega_i \pi^\nu$ *für alle* $i = 1, \dots, f$ *und* $\nu \in F_e$, *und* $\eta_* = 1 + \omega_* \pi^{p^{\mu_0}}$.
- *Finde* β *mit* $\beta g = 0$ *und* $\beta_{1\mathrm{e}_0} = p^{\mu_0}$.
- *Setze* $M \leftarrow \mathrm{diag}(M_{11}, \dots, M_{fe}, M_*)$ *mit* $M_{i\nu} = \mathrm{ord}(\eta_{i\nu})$ *für alle* $(i,\nu) \neq (1, \mathrm{e}_0)$ *und* $M_* = \mathrm{ord}(\eta_*)$
- *Setze die Zeile* $1\mathrm{e}_0$ *von* M *auf* β.
- *Gib* (g, M) *und* $(\omega_1, \cdots, \omega_n, \omega_*)$ *zurück.*

Die eindeutige Darstellung im Fall II unterscheidet sich von einer Basisdarstellung dadurch, daß die Auswahl der Exponenten von $\eta_{1\mathrm{e}_0}$ durch p^{μ_0} beschränkt ist. Wenn $\eta_{1\mathrm{e}_0}$ die Ordnung von p^{μ} hat, haben wir also schon eine Basisdarstellung. Wir nennen diesen Fall den Fall IIa.

KOROLLAR III.13 (BASISDARSTELLUNG IM FALL IIA). *Wenn $(p-1) \mid e$ gilt und der Kern von h_2 nicht - trivial ist und*

- *$p \leq 3$ und $m \leq 2e$ ist oder*
- *$p > 3$ und $(p-1)m \leq (p+1)e)$ ist,*

ist die Eindeutige Darstellung im Fall II eine Basisdarstellung. Es gilt $\mathrm{ord}([\eta_{1\,\mathrm{e}_0}]) = p^{\mu_0}$.

BEWEIS. Es sei $\nu = \frac{\mathrm{e}}{p-1} = p^{\mu_0-1}\mathrm{e}_0$ und $\eta = \eta_{1\mathrm{e}_0}^{p^{\mu_0-1}} = (1+\omega_1\pi^{\mathrm{e}_0})^{p^{\mu_0-1}}$, dann gilt $\eta \equiv 1 + a\pi^{\nu} \bmod \mathfrak{p}^{\nu+1}$. Wir werden nun feststellen, für welche m $\eta^p \equiv 1 \bmod \mathfrak{p}^m$ ist. Nach der p - Potenzierungsregel III.4 und der Wahl von ω_1 gilt $\eta^p \equiv 1 \bmod \mathfrak{p}^{p\nu+1}$. Betrachten wir nun die Summanden, die in den nächsthöheren p - Potenzen liegen, so lesen wir in dem Beweis der p - Potenzierungsregel ab, daß

$$m \leq \min(2\nu + \mathrm{e}, (p-1)\nu + \mathrm{e})$$

sein muß. $\square$

ALGORITHMUS III.14 (ERZEUGENDE UND RELATIONEN IM FALL IIA).

<u>Eingabe:</u> $\mathfrak{o}_{\mathbf{K}}, \mathfrak{p} \subset \mathfrak{o}_{\mathbf{K}}, e, f, p$

<u>Ausgabe:</u> *Erzeugende und Relationen (g, M) von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, $(\omega_1, \cdots, \omega_n, \omega_*)$*

- *Bestimme F_e.*
- *Bestimme μ_0, e_0, so daß. $e = p^{\mu_0-1}(p-1)e_0$ ist und $p \not| e_0$ gilt.*
- *Bestimme ω_0, so daß $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ nicht lösbar ist.*
- *Wähle ein Vertretersystem $\omega_1, \ldots, \omega_f$ einer Basis von $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ in $\mathfrak{o}_{\mathbf{K}}$ mit $\omega_1^{p^{\mu_0}} - \varepsilon\omega_1^{p^{\mu_0-1}} \equiv 0 \bmod \mathfrak{p}$.*
- *$g \leftarrow (\eta_{11}, \ldots, \eta_{fe}, \eta_*)$ mit $\eta_{i\nu} = 1 + \omega_i\pi^{\nu}$, wobei $i = 1, \ldots, f$ und $\nu \in F_e$ sind und $\eta_* = 1 + \omega_*\pi^{p^{\mu_0}e_0}$ ist.*
- *Setze $M \leftarrow \mathrm{diag}(M_{11}, \ldots, M_{fe}, M_*)$ mit $M_{i\nu} = \mathrm{ord}(\eta_{i\nu})$, wobei $i = 1, \ldots, f$ und $\nu \in F_e$ sind und $M_* = \mathrm{ord}(\eta_*)$ ist. Es gilt $\mathrm{ord}(\eta_{1\,e_0}) = p^{\mu_0}$.*
- *Gib (g, M) und $(\omega_1, \cdots, \omega_n, \omega_*)$ zurück.*

Wenn $\mathbf{K}$ die p^μ - ten Einheitswurzeln enthält, haben wir ein Element, das schon in $\mathbf{K}$ die Ordnung p^μ hat. Der folgende Satz zeigt, daß dieses dann auch eine Einseineinheit der Stufe e_0 ist, einen Beweis findet man in [Has63].

SATZ III.15 (EINHEITSWURZELN IN P - ADISCHEN KÖRPERN). *Es sei $\mathbf{K}_\mathfrak{p}$ ein $\mathfrak{p}$ - adischer Zahlkörper, dann ist eine p^μ - te Einheitswurzel von $\mathbf{K}_\mathfrak{p}$ Einseinheit der Stufe $\frac{e}{p^{\mu-1}(p-1)}$.*

Wenn $\mathbf{K}$ die p^μ - ten Einheitswurzeln enthält, enthält auch die Vervollständigung $\mathbf{K}_\mathfrak{p}$ die p^μ - ten Einheitswurzeln. Mit $\mu = p^{\mu_0}$ haben wir $\frac{\mathrm{e}}{p^{\mu_0-1}(p-1)} = \mathrm{e}_0$, also sind die p^{μ_0} - ten Einheitswurzeln, falls vorhanden, Einseinheiten der Stufe e_0. Damit erhalten wir also auch in diesem Fall, den wir mit Fall IIb bezeichnen, eine Basisdarstellung von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, wobei bei der Berechnung auf die richtige Wahl der Basis von $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ geachtet werden muß.

KOROLLAR III.16 (BASISDARSTELLUNG IM FALL IIB). *Wenn $(p-1) \mid e$ gilt, der Kern von h_2 nicht - trivial ist, $\mathbf{K}$ die p^{μ_0} - te Einheitswurzel ζ enthält und $\omega_1 = \frac{\zeta-1}{\pi^{\mathrm{e}_0}}$ gewählt wird, ist die Eindeutige Darstellung im Fall II eine Basisdarstellung.*

ALGORITHMUS III.17 (ERZEUGENDE UND RELATIONEN IM FALL IIB).

<u>Eingabe</u>: $\mathfrak{o}_\mathbf{K}$,$\mathfrak{p} \subset \mathfrak{o}_\mathbf{K}$,*e*,*f*,*p*,
p^{μ_0} - te Einheitswurzel ζ, wobei $e = p^{\mu_0-1}(p-1)\mathrm{e}_0$ und $p \nmid \mathrm{e}_0$ gilt

<u>Ausgabe</u>: *Erzeugende und Relationen (g, M) von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$,*
$(\omega_1, \cdots, \omega_n, \omega_*)$

- *Bestimme F_e.*
- *Bestimme μ_0, e_0, so daß $e = p^{\mu_0-1}(p-1)\mathrm{e}_0$ ist.*
- *Bestimme ω_*, so daß $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ nicht lösbar ist.*
- *Wähle ein Vertretersystem $\omega_1, \dots, \omega_f$ einer Basis von $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ in $\mathfrak{o}_\mathbf{K}$ mit $\omega_1 = \frac{\zeta-1}{\pi^{\mathrm{e}_0}}$.*
- *Setze $g \leftarrow (\eta_{11}, \dots, \eta_{fe}, \eta_*)$ mit $\eta_{i\nu} = 1+\omega_i\pi^\nu$, wobei $i = 1, \dots, f$ und $\nu \in F_e$ sind und $\eta_* = 1 + \omega_*\pi^{p^{\mu_0}\mathrm{e}_0}$ ist.*
- *Setze $M \leftarrow \mathrm{diag}(M_{11}, \dots, M_{fe}, M_*)$ mit $M_{i\nu} = \mathrm{ord}(\eta_{i\nu})$, wobei $i = 1, \dots, f$ und $\nu \in F_e$ sind und $M_* = \mathrm{ord}(\eta_*)$. Es gilt $\mathrm{ord}(\eta_{1\,\mathrm{e}_0}) = p^{\mu_0}$.*
- *Gib (g, M) und $(\omega_1, \cdots, \omega_n, \omega_*)$ zurück.*

Wir können nun im allgemeinen Erzeugende und Relationen von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ bestimmen. Wir fassen die Fallunterscheidungen in einem Algorithmus zusammen.

Algorithmus III.18 ($(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ mit Einseinheiten).
Eingabe: $\mathfrak{o}_{\mathbf{K}}, \mathfrak{p}, e, f, p$
Ausgabe: *Erzeugende und Relationen* (g, M) *von* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$

- *Benutze Algorithmus* III.8, *wenn*
  - $(p-1)$ *nicht* e *teilt oder*
  - $m \leq \frac{pe}{p-1}$ *ist oder*
  - $\mathrm{Kern}(h_2) = \{0\}$ *ist.*
- *Benutze Algorithmus* III.14, *wenn*
  - $(p-1) \mid e$ *gilt und* $\mathrm{Kern}(h_2) \neq \{0\}$ *ist und*
    - $p \leq 3$ *und* $m \leq 2e$ *oder*
    - $p > 3$ *und* $(p-1)m \leq (p+1)e)$)
- *Benutze Algorithmus* III.17, *wenn*
  - $(p-1) \mid e$ *und* $\mathrm{Kern}(h_2) \neq \{0\}$ *ist und* $\mathbf{K}$ *die* p^{μ_0} *- te Einheitswurzel* ζ *enthält.*
- *Benutze Algorithmus* III.12, *wenn keiner der anderen Fälle zutrifft.*

Das Verfahren von Cohen

Die ursprüngliche Darstellung dieses Verfahrens findet man in [CDyDO95]. Wie bereits erwähnt, basiert das Verfahren von Cohen auf folgender Tatsache:

LEMMA III.19. *Es seien* $\mathbf{K}$ *ein algebraischer Zahlkörper,* $\mathfrak{o}_{\mathbf{K}}$ *die Maximalordnung von* $\mathbf{K}$*,* $\mathfrak{p}$ *ein Primideal von* $\mathfrak{o}_{\mathbf{K}}$ *und* $l \leq m \leq 2l$*, dann ist*

$$\begin{array}{llcl} \Psi: & (1+\mathfrak{p}^l)/(1+\mathfrak{p}^m) & \to & (\mathfrak{p}^l/\mathfrak{p}^m)^+ \\ \Psi: & [1+a] & \mapsto & \overline{a} \end{array}$$

ein Isomorphismus.

BEWEIS. Es sei $\mathfrak{b}_{\mathfrak{p}}$ das Bewertungsideal der Vervollständigung von $\mathbf{K}$ bezüglich $|\cdot|_{\mathfrak{p}}$. Wir zeigen, daß

$$\begin{array}{llcl} \Psi_{\mathfrak{p}}: & (1+\mathfrak{b}_{\mathfrak{p}}{}^l)/(1+\mathfrak{b}_{\mathfrak{p}}{}^m) & \to & (\mathfrak{b}_{\mathfrak{p}}{}^l/\mathfrak{b}_{\mathfrak{p}}{}^m)^+ \\ \Psi_{\mathfrak{p}}: & [1+a] & \mapsto & \overline{a} \end{array}$$

ein Isomorphismus ist. Dann ist auch Ψ ein Isomorphismus. Es sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Es seien $[1+a], [1+b] \in (1+\mathfrak{b}_{\mathfrak{p}}{}^l)/(1+\mathfrak{b}_{\mathfrak{p}}{}^m)$ mit $a = \sum_{\nu=l}^{m-1} a_\nu \pi^\nu, b = \sum_{\nu=l}^{m-1} b_\nu \pi^\nu$, wobei a_ν, b_ν aus einem Vertretersystem von $\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}$ in $\mathfrak{o}_{\mathbf{K}}$ sind. Dann gilt $\Psi_{\mathfrak{p}}([1+a][1+b]) = \Psi_{\mathfrak{p}}([1+a+b+ab]) = \Psi_{\mathfrak{p}}([1+(a+b)]) = \overline{a+b} = \overline{a}+\overline{b} = \Psi_{\mathfrak{p}}([1+a]) + \Psi_{\mathfrak{p}}([1+b])$, da $ab = \sum_{\nu=2l}^{m-1} \prod_{i+j=\nu} a_i b_j \pi^\nu \in \mathfrak{b}_{\mathfrak{p}}{}^m$ ist. □

Die Berechnung von $\mathfrak{p}^l/\mathfrak{p}^m$ ist recht einfach. Es sei w eine Ganzheitsbasis von $\mathfrak{o}_{\mathbf{K}}$, es seien $\mathfrak{p}^l$ und $\mathfrak{p}^m$ $(1 \leq l \leq m)$ durch die Matrizen A bzw. B gegeben, so daß $w_l = Aw$ $(w_m = Bw)$ eine $\mathbb{Z}$ - Basis von $\mathfrak{p}^l$ $(\mathfrak{p}^m)$ ist. Die Matrix BA^{-1} stellt die Elemente von $\mathfrak{p}^m$ durch die Elemente von $\mathfrak{p}^l$ dar, denn es gilt $w_m = BA^{-1}Aw = BAw_l$. Damit ist BA^{-1} die Relationenmatrix der Gruppe $\mathfrak{p}^l/\mathfrak{p}^m$ und w_l sind ihre Erzeugenden, $\mathfrak{p}^l/\mathfrak{p}^m$ wird also durch (w_l, BA^{-1}) dargestellt. Ist $w_l = (w_{l1}, \cdots, w_{ln})^T$, dann erhalten wir mit Lemma III.19 die Darstellung

$$(g, M) := \left(\begin{pmatrix} 1+w_{l1} \\ \vdots \\ 1+w_{ln} \end{pmatrix}, BA^{-1} \right)$$

von $(1+\mathfrak{p}^m)/(1+\mathfrak{p}^l)$ durch Erzeugende und Relationen.

Um eine Darstellung von $[b] \in (1+\mathfrak{p}^l)/(1+\mathfrak{p}^m)$ bezüglich g zu erhalten brauchen wir nur $\alpha = (\alpha_1, \cdots, \alpha_n)$ mit $b - 1 = \sum_{i=1}^n \alpha_i w_i$ zu finden, dann gilt nach Lemma III.19 auch $b = \prod_{i=1}^n (1+w_l)^{\alpha_i}$. Es sei $\beta \in \mathbb{Z}^n$ mit $b - 1 = \beta w$ gegeben, dann gilt $\beta w = \alpha A w$. Eine Lösung des linearen Gleichungssystem $\beta = \alpha A$ liefert also die gewünschte Darstellung.

Es seien k, l, m mit $k \leq l \leq m$ und $l \leq m \leq 2l$ gegeben. Im folgenden bezeichnet $[1+a]_j$ die Klasse von $1+a$ modulo $(1+\mathfrak{p}^j)$.

Nach dem Isomorphiesatz ist die folgende Sequenz exakt:

$$\begin{array}{ccccccccc} 1 & \to & (1+\mathfrak{p}^l)/(1+\mathfrak{p}^m) & \overset{\Psi}{\to} & (1+\mathfrak{p}^k)/(1+\mathfrak{p}^m) & \overset{\Phi}{\to} & (1+\mathfrak{p}^k)/(1+\mathfrak{p}^l) & \to & 1 \\ & & [1+a]_m & \mapsto & [1+a]_m & \mapsto & [1+a]_l. & & \end{array}$$

Mit Lemma I.19 läßt sich, wenn Darstellungen (g, M) von $(1+\mathfrak{p}^l)/(1+\mathfrak{p}^m)$ und (h, N) von $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$ bekannt sind, eine Darstellung von $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^m)$ durch Erzeugende und Relationen berechnen. Nach Definition der Abbildung Φ ist $\Phi([h]_m) = [h]_l$. Wir benötigen eine Matrix P mit $N[h]_m = P\Psi([g]_m)$. Die Matrix P bestimmen wir, indem wir das obige Verfahren zur Darstellung von Klassen in $(1+\mathfrak{p}^l)/(1+\mathfrak{p}^m)$ auf die Komponenten von $N[h]_m$ anwenden. Wir erhalten für $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^m)$ die Darstellung:

$$\left(\begin{pmatrix} h \\ g \end{pmatrix}, \begin{pmatrix} N & -P \\ 0 & M \end{pmatrix}\right).$$

Um nun $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ zu berechnen, bestimmt man sukzessive die Gruppen

$$(1+\mathfrak{p})/(1+\mathfrak{p}^2), (1+\mathfrak{p})/(1+\mathfrak{p}^4), \ldots, (1+\mathfrak{p})/(1+\mathfrak{p}^{2^s}), (1+\mathfrak{p})/(1+\mathfrak{p}^m),$$

wobei $s = \lfloor \log_2(m) \rfloor$ ist.

Algorithmus III.20 ($(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ nach Cohen).

Eingabe: $\mathfrak{o}_{\mathbf{K}}, \mathfrak{p} \subset \mathfrak{o}_{\mathbf{K}}, m \in \mathbb{Z}^{>0}$, *w Ganzheitsbasis von* $\mathfrak{o}_{\mathbf{K}}$

Ausgabe: *Erzeugende und Relationen* (g, M) *von* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$

- *Berechne Erzeugende und Relationen* (g, M) *von* $(1+\mathfrak{p})/(1+\mathfrak{p}^2)$*:*
  - *Berechne Matrizendarstellungen* A, B *von* $\mathfrak{p}, \mathfrak{p}^2$.
  - *Setze* $g \leftarrow (g_1, \ldots, g_n)$ *mit* $g_i = 1 + Aw_i$ *für* $1 \le i \le n$.
  - *Setze* $M \leftarrow BA^{-1}$.
- *Setze* $k \leftarrow 2$, *setze* $s \leftarrow 1$.
- *Solange* $l \ne m$ *ist, wiederhole:*
  - *Setze* $l \leftarrow \min(2^s, m)$.
  - *Berechne Erzeugende und Relationen* (h, N) *von* $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$*:*
    - *Berechne Matrizendarstellungen* A, B *von* $\mathfrak{p}^k, \mathfrak{p}^l$.
    - *Setze* $h \leftarrow (h_1, \ldots, h_n)$ *mit* $h_i = 1 + Aw_i$ *für* $1 \le i \le n$.
    - *Setze* $N \leftarrow BA^{-1}$.
  - *Setze* $g \leftarrow \binom{g}{h}$.
  - *Berechne* P, *so daß* $Ph = Ng$.
  - *Setze* $M \leftarrow \begin{pmatrix} M & -P \\ 0 & N \end{pmatrix}$
  - *Setze* $k \leftarrow l$, *setze* $s \leftarrow s + 1$.
- *Gib* (g, M) *zurück.*

Eine Darstellung einer Klasse in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ bezüglich der Erzeugenden erhält man mit folgendem Algorithmus:

ALGORITHMUS III.21 (DARSTELLUNG IN $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ NACH COHEN).

Eingabe: $\eta \in 1+\mathfrak{p}$
$\mathfrak{o}_{\mathbf{K}}, \mathfrak{p} \subset \mathfrak{o}_{\mathbf{K}}, m \in \mathbb{Z}^{>0}$, *$w$ Ganzheitsbasis von* $\mathfrak{o}_{\mathbf{K}}$

Ausgabe: *α mit $[\alpha g] = [\eta]$, wobei g Erzeugende von* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ *sind, wie sie von* III.20 *geliefert werden.*

- *Berechne Darstellung* $(1+\mathfrak{p})/(1+\mathfrak{p}^2)$*:*
  - *Bestimme eine Matrizendarstellung A von* $\mathfrak{p}$.
  - *Bestimme β, so daß $a-1=\beta w$ ist.*
  - *Setze* $\alpha \leftarrow \beta A^{-1}$.
  - *Setze* $a \leftarrow a(\prod_{i=1}^{n}(1+Aw_i)^{\alpha_i})^{-1}$
- *Setze $k \leftarrow 2$, setze $s \leftarrow 1$.*
- *Solange $l \neq m$ ist, wiederhole:*
  - *Setze* $l \leftarrow \min(2^s, m)$.
  - *Berechne Darstellung in* $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$*:*
    - *Bestimme eine Matrizendarstellung A von* $\mathfrak{p}^k$.
    - *Bestimme β, so daß $a-1=\beta w$ ist.*
    - *Setze* $\gamma \leftarrow \beta A^{-1}$.
    - *Setze* $a \leftarrow a(\prod_{i=1}^{n}(1+Aw_i)^{\gamma_i})^{-1}$
  - *Setze* $\alpha \leftarrow (\alpha, \gamma)$.
  - *Setze $k \leftarrow l$.*
  - *Setze* $s \leftarrow s+1$
- *Gib α zurück.*

Berechnen der Multiplikativen Gruppe von Restklassenringen

Wir wissen, daß $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^* \cong (\mathfrak{o}_\mathbf{K}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m)$ ist. Wir haben zwei Verfahren zur Berechnung von Erzeugenden und Relationen von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ kennengelernt.

Eine Darstellung der Gruppe $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$ ist durch Erzeugende und Relationen $((\delta),(p^\mathrm{f}-1))$ gegeben, wobei δ ein primitives Element von $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$ ist. $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$ ist isomorph zur einzigen zyklischen Untergruppe der Ordnung $p^\mathrm{f}-1$ von $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$. Es sei p^μ die Ordnung der größten zyklischen Untergruppe von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, dann ist δ^{p^μ} ein Erzeugendes der zyklischen Untergruppe der Ordnung $p^\mathrm{f}-1$, da die Abbildung $\mathfrak{o}_\mathbf{K}/\mathfrak{p} \to \mathfrak{o}_\mathbf{K}/\mathfrak{p}$, $\overline{\delta} \mapsto \overline{\delta^p}$ in $\mathfrak{o}_\mathbf{K}/\mathfrak{p}$ ein Isomorphismus ist. Wenn (g_η, M_η) eine Darstellung von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ durch Erzeugende und Relationen ist, ist eine Darstellung von $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$ gegeben durch

$$(g_\mathfrak{p}, M_\mathfrak{p}) = \left(\begin{pmatrix} \delta^{p^\mu} \\ g_\eta \end{pmatrix}, \begin{pmatrix} p^\mathrm{f}-1 & 0 \\ 0 & M_\eta \end{pmatrix} \right).$$

Es sei $a \in \mathfrak{o}_\mathbf{K}$ mit $a \notin \mathfrak{p}$ gegeben. Die Darstellung von $\overline{a}$ in $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$ erhalten wir mit dem Logarithmus in dem endlichen Körper F_{p^f}. Hier kann man auf Algorithmen wie Shanks Baby Step Giant Step zurückgreifen. Es sei γ die Darstellung von $\overline{a}$ in $(\mathfrak{o}_\mathbf{K}/\mathfrak{p})^*$ bezüglich $\overline{\delta^{p^\mu}}$, dann ist $\eta := a(\delta^{p^\mu})^{-\gamma} \in 1+\mathfrak{p}$. Die Darstellung bezüglich den Erzeugenden von $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ erhalten wir mit Algorithmus III.21 oder Algorithmus III.9 beziehungsweise III.11. Es sei α eine Darstellung von η in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, dann ist (γ,α) eine Darstellung der Klasse von a bezüglich $g_\mathfrak{p}$ in $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$.

Es gilt $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^* \cong (\mathfrak{o}_\mathbf{K}/\mathfrak{p}_1^{m_1})^* \cdots (\mathfrak{o}_\mathbf{K}/\mathfrak{p}_t^{m_t})^*$. Die Erzeugenden der $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}_i^{m_i})^*$ für $1 \le i \le t$ sind Erzeugende von $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$. Wir könnten wieder I.19 anwenden um die Relationen für $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}_i^{m_i})^*$ zu bestimmen. Einfacher gestaltet es sich jedoch, wenn wir die Erzeugenden von $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}_i^{m_i})^*$ teilerfremd zu den anderen Teilern von $\mathfrak{m}_0$ machen, denn dann sind die Erzeugenden unabhängig. Wir werden ein Verfahren vorstellen, das zu gegebenem $\eta \in \mathfrak{o}_\mathbf{K}$ ein $\eta' \in \mathfrak{o}_\mathbf{K}$ liefert, so daß gilt:

$$\begin{array}{rcll} \eta' & \equiv & \eta & \bmod \quad \mathfrak{p}_i^{m_i} \\ \eta' & \equiv & 1 & \bmod \quad \mathfrak{m}_0\mathfrak{p}_i^{-m_i} \end{array}.$$

Die folgende Behauptung stammt aus [Coh95].

Lemma III.22. *Es seien zwei teilerfremde Ideale $\mathfrak{a}$,$\mathfrak{b}$ in $\mathfrak{o}_\mathbf{K}$ gegeben, mit polynomiellen Aufwand können wir zwei Elemente $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ bestimmen, so daß $a+b=1$ gilt.*

Beweis. Es seien $\mathfrak{a}$ und $\mathfrak{b}$ durch die $n \times n$ - Matrizen A beziehungsweise B über einer Ganzheitsbasis, deren erstes Element O.B.d.A. 1 ist, gegeben. Wenn wir die Hermite Normalform (dafür gibt es polynomielle Algorithmen) auf $\binom{A}{B}$

anwenden, erhalten wir, da $\mathfrak{a}$,$\mathfrak{b}$ teilerfremd sind, eine $2n \times 2n$ - Matrix T_L, so daß $T_L\binom{A}{B} = \binom{I_n}{0_n}$, wobei I_n die $n \times n$ - Einheitsmatrix und 0_n die $n \times n$ - Nullmatrix bezeichnet. Es sei L die erste Zeile von T_L. Dann gilt $L\binom{A}{B} = (1, 0, \dots, 0)$. Wenn wir L in zwei Vektoren $L_1, L_2 \in \mathbb{Z}^n$ aufspalten, erhalten wir $a = L_1 A$ und $b = L_2 B$ mit $a + b = 1$. □

Bemerkung III.23. *Es seien zwei teilerfremde Ideale* $\mathfrak{a}$,$\mathfrak{b}$ *in* $\mathfrak{o}_\mathbf{K}$ *und* $\alpha, \beta \in \mathfrak{o}_\mathbf{K}$ *gegeben. Dann erhalten wir mit polynomiellen Aufwand* $\gamma \in \mathfrak{o}_\mathbf{K}$*, so daß gilt:*

$$\begin{aligned} \gamma &\equiv \alpha \bmod \mathfrak{a} \\ \gamma &\equiv \beta \bmod \mathfrak{b}. \end{aligned}$$

Beweis. Mit Lemma III.22 erhalten wir $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$, so daß $a + b = 1$. Dann ist klar, daß $\gamma = b\alpha + a\beta$ die gewünschten Eigenschaften hat. □

Es sei (g_i, M_i) eine Darstellung von $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}_i^{m_i})^*$ und g_i' ein Erzeugendensystem, dessen Elemente teilerfremd zu den anderen Teilern von $\mathfrak{m}_0$ sind, dann erhalten wir für $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$ die Darstellung

$$(g_0, M_0) = \left(\begin{pmatrix} g_1' \\ \vdots \\ g_t' \end{pmatrix}, \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_t \end{pmatrix} \right).$$

Algorithmus III.24 (Erzeugende und Relationen von $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$).

Eingabe: $\mathfrak{o}_\mathbf{K}, \mathfrak{m}_0$

Ausgabe: *Erzeugende und Relationen* (g, M) *von* $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$

- *Setze* g *und* M *auf den leeren Vektor und die leere Matrix.*
- *Faktorisiere* $\mathfrak{m}_0$.
- *Für alle* $\mathfrak{p} \mid \mathfrak{m}_0$.
  - *Berechne Erzeugende und Relationen* $(g_\mathfrak{p}, M_\mathfrak{p})$ *von* $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$.
  - *Für alle Komponenten* η *von* $g_\mathfrak{p}$*:*
    - *Berechne mit Bemerkung* III.23 η'*, so daß* $\eta' \equiv \eta \bmod \mathfrak{p}^m$ *und* $\eta' \equiv \eta \bmod \mathfrak{m}_0\mathfrak{p}^{-m}$ *gilt.*
    - *Setze* $\eta \leftarrow \eta'$.
  - *Setze* $g \leftarrow \binom{g}{g_\mathfrak{p}}$.
  - *Setze* $M \leftarrow \begin{pmatrix} M & 0 \\ 0 & M_\mathfrak{p} \end{pmatrix}$.
- *Gib* (g, M) *zurück.*

Durch Aneinanderreihen der Darstellungen von Klassen bezüglich der $g'_{\mathfrak{p}_i}$, welche dieselben wie jene bezüglich der $g_{\mathfrak{p}_i}$ sind, erhalten wir eine Darstellung bezüglich g_0.

Vergleich der Verfahren

Das Verfahren von Cohen besticht durch seine Einfachheit. Das sehr übersichtliche Verfahren liefert Erzeugende und Relationen für alle Restklassenringe modulo $\mathfrak{p}^m$, dadurch läßt sich dieses Verfahren vergleichsweise einfach implementieren. In $\lceil \log_2(m) \rceil$ Schritten werden Erzeugende und Relationen der Gruppe $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ berechnet. In jedem dieser Schritte müssen Darstellungen der Erzeugenden der bis dahin berechneten Gruppe $(1+\mathfrak{p})/(1+\mathfrak{p}^{2^s})$ in $(1+\mathfrak{p}^{2^s})/(1+\mathfrak{p}^k)$ mit $k = \min(2^{s+1}, m)$ berechnet werden.

Bei dem hier vorgestellten Verfahren mit Einseinheiten werden die Erzeugenden und Relationen in den meisten Fällen (Fall I, Fall IIa und Fall IIb) in einem Schritt berechnet, der nicht viel Aufwendiger ist als einer der $\lceil \log_2(m) \rceil$ Schritte im Verfahren von Cohen. Es spielt keine Rolle wie groß der Exponent m ist, es ändern sich lediglich die Ordnungen der Erzeugenden, die sich ohne weiteren Aufwand berechnen lassen. Dies werden wir bei der Berechnung des Führers einer Strahlklassengruppe in Kapitel V ausnutzen.

Schon die Erzeugenden und Relationen, die unser Verfahren mit Einseinheiten liefert, beschreiben sehr gut die Struktur der Gruppe, während beim Verfahren von Cohen noch weitere Berechnungen notwendig sind. Beim Verfahren von Cohen wird die Basis immer mit Hilfe der Smith Normalform berechnet. Bei unserem Verfahren hingegen ist diese Berechnung nur notwendig, wenn wir nicht einen der Algorithmen für einen der häufig auftretenden Fälle I, IIa oder IIb anwenden können.

Der stufenweise Aufbau unseres Verfahrens zum Darstellen von Klassen bezüglich der Erzeugenden erweist sich als ungünstig. Hier braucht man mit dem Verfahren mit Einseinheiten m Schritte, während das Verfahren von Cohen nur $\lceil \log_2(m) \rceil$ Schritte erfordert. Bei beiden Verfahren enthalten diese Schritte gleich viele Multiplikationen/Divisionen von algebraischen Zahlen. Im Verfahren von Cohen wird in jedem Schritt ein Gleichungssystem über $\mathbb{Z}$ gelöst, im Verfahren mit Einseinheiten eines über $\mathbb{Z}/p\mathbb{Z}$.

Durch das langsame Berechnen der Darstellung bezüglich der Erzeugenden wird das Verfahren mit Einseinheiten, in den Fällen, in denen wir die Relation berechnen müssen langsamer, als in den anderen Fällen.

Beispiele, die diese Überlegungen wiederspiegeln findet man in dem Kapitel VI.

KAPITEL IV

Berechnen der Strahlklassengruppe

Um die Strahlklassengruppe berechnen zu können, fehlt uns noch

- die Gruppe $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$, womit dann die Gruppe $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ berechnet ist, da $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}} \cong \mathbf{K}^{\mathfrak{m}_0}/\mathbf{K}_{\mathfrak{m}_0} \times \mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$ ist.
- das Faktorisieren von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ nach $\mathbf{U}_{\mathbf{K}}/\mathbf{U}_{\mathfrak{m}}$, womit wir dann die Gruppe $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ berechnet haben.
- die Konstruktion von Erzeugenden der Klassengruppe $\mathbf{Cl}_{\mathbf{K}}$, die teilerfremd zu $\mathfrak{m}_0$ sind.
- das Berechnen von $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$ mit Hilfe der Isomorphie $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}/(\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}) \cong \mathbf{Cl}_{\mathbf{K}}$.
- ein Verfahren zur Darstellung von Repräsentanten der Strahlklassen bezüglich der Basis von $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$.

Unendliche Stellen. Es sei $\mathfrak{m}_\infty = \mathfrak{p}_\infty^{(\nu_1)} \cdots \mathfrak{p}_\infty^{(\nu_s)}$. Wir suchen Erzeugende ϑ_i für die Gruppe $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$, für die gilt $\vartheta_i \equiv 1 \bmod^* \mathfrak{m}_0$. Nach dem Approximationssatz gibt es $\vartheta_1, \dots, \vartheta_s$, so daß

$$\begin{array}{rcll} \vartheta_j & \equiv & -1 & \bmod^* \mathfrak{p}_\infty^{(\nu_j)} \\ \vartheta_j & \equiv & 1 & \bmod^* \mathfrak{p}_\infty^{(\nu_i)}, \quad i = 1 \dots s, \quad i \neq j \\ \vartheta_j & \equiv & 1 & \bmod^* \mathfrak{m}_0 \end{array}$$

sind. Es sei $w_1, \dots, w_n$ eine Basis von $\mathfrak{m}_0$, es sei λ eine Lösung des Ungleichungssytems

$$\begin{array}{rcl} 1 + \lambda_1 w_1^{(\nu_j)} + \cdots + \lambda_n w_n^{(\nu_j)} & < & 0 \\ 1 + \lambda_1 w_1^{(\nu_i)} + \cdots + \lambda_n w_n^{(\nu_i)} & > & 0, \quad i = 1 \dots s, \quad i \neq j \end{array}$$

über $\mathbb{Z}$, dann erfüllt $\vartheta_j = \lambda(w_1, \dots, w_n)^T$ die obigen Bedingungen.

Es sei nun $w := \frac{\sum_{i=1}^n |w_i|}{2}$, dann ist die gerundete Lösung des folgenden linearen Gleichungssystems eine Lösung des Ungleichungssystems, da man sich durch das runden der Lösung höchstens um w von einer Lösung des Ungleichungssystems entfernen kann:

$$\begin{array}{rcl} 1+\bar\lambda_1 w_1^{(\nu_j)}+\dots+\bar\lambda_n w_n^{(\nu_j)} & = & -w \\ 1+\bar\lambda_1 w_1^{(\nu_i)}+\dots+\bar\lambda_n w_n^{(\nu_i)} & = & w, \quad i=1\dots s, i\neq j \end{array}.$$

$\lambda = \lfloor\bar\lambda\rceil$ ist dann also eine Lösung des Ungleichungssystems und

$$\vartheta_j = \lambda(w_1.\dots,w_n)$$

ist eines der s Erzeugenden von $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$.

Wir erhalten damit die Darstellung

$$(g_\infty, M_\infty) = \left(\begin{pmatrix}\vartheta_1\\ \vdots \\ \vartheta_s\end{pmatrix}, \begin{pmatrix}2 & \dots & 0\\ \vdots & \ddots & \vdots\\ 0 & \dots & 2\end{pmatrix}\right)$$

für die Gruppe $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$ durch Erzeugende und Relationen. Die Erzeugenden g_∞ bilden eine Basis der Gruppe. Für $x\in\mathbb{R}$, definiere

$$\operatorname{sig}^*(x) := \begin{cases} 1 & \text{für } x<0 \\ 0 & \text{für } x>0\end{cases}.$$

Für $a\in\mathbf{K}$ nennen wir den Vektor

$$\operatorname{sig}^{\mathfrak{m}_\infty}(a) = (\operatorname{sig}^*(a^{(\nu_1)}),\dots,\operatorname{sig}^*(a^{(\nu_s)}))$$

die Signatur von a. Die Abbildung $\operatorname{sig}^{\mathfrak{m}_\infty}$ liefert uns die Darstellung der Klasse eines Elementes von $\mathfrak{o}_\mathbf{K}$ bezüglich der Basis von $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$

Wenn die Erzeugenden von $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$ an den Stellen von $\mathfrak{m}_\infty$ positiv sind, erhalten wir eine Darstellung von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ durch das Aneinanderreihen der Relationenmatrizen und Erzeugenden.

Wenn uns Erzeugende von $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$ bekannt sind, wenden wir, um Erzeugende von $(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$ zu erhalten, die an den Stellen von $\mathfrak{m}_\infty$ positiv sind, folgenden Algorithmus an:

Algorithmus IV.1 (Kantonesischer Restsatz).

Eingabe: $a\in\mathfrak{o}_\mathbf{K}$, *$\sigma$ gewünschte Signatur,* $\mathfrak{m}=\mathfrak{m}_0\mathfrak{m}_\infty$, g_∞

Ausgabe: $b\in\mathfrak{o}_\mathbf{K}$ *mit* $b\equiv a \bmod \mathfrak{m}_0$ *und* $\operatorname{sig}^{\mathfrak{m}_\infty}(b)=\sigma$

- *Setze* $b=a$
- *Reduziere* b *modulo* $\mathfrak{m}_0$
- *Für alle* $\mathfrak{p}_\infty^{(\nu_i)} \mid \mathfrak{m}_\infty$:
  - *Wenn* $\operatorname{sig}^*(a^{(\nu_i)})\neq\sigma_i$ *ist, multipliziere* b *mit* $g_{\infty i}$.
- *Gib* b *zurück.*

Es sei (g_0, M_0) eine Darstellung von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{m}_0{}^*)$, wobei Erzeugenden an den Stellen von $\mathfrak{m}_0$ positiv seien. Mit der Darstellung (g_∞, M_∞) von $\mathbf{K}^{\mathfrak{m}_\infty}/\mathbf{K}_{\mathfrak{m}_\infty}$ ist dann

$$(g, M) = \left(\begin{pmatrix} g_0 \\ g_\infty \end{pmatrix}, \begin{pmatrix} M_0 & 0 \\ 0 & M_\infty \end{pmatrix} \right)$$

eine Darstellung von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$.

Wir erhalten die Darstellung von $[a]$, $a \in \mathbf{K}$ bezüglich $\left(\begin{smallmatrix} g_0 \\ g_\infty \end{smallmatrix}\right)$ durch Aneinderhängen der Darstellungen bezüglich g_0 und g_∞.

Faktorisieren nach $\mathbf{U_K}/\mathbf{U_{\mathfrak{m}}}$. Zur Berechnung der Strahlklassengruppe benötigen wir als Nächstes $\mathbf{U_K}/\mathbf{U_{\mathfrak{m}}}$, um dann $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ nach $\mathbf{U_K}/\mathbf{U_{\mathfrak{m}}}$ zu faktorisieren. Es sei h der Homomorphismus $h : \mathbf{K}^{\mathfrak{m}} \to \mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$, dann haben wir $\mathbf{U_K}/\mathbf{U_{\mathfrak{m}}} = h(\mathbf{U_K})$. Es seien $u_0, u_1, \ldots, u_r$ ein Erzeugendensystem von $\mathbf{U_K}$. Es seien $v_0, v_1, \ldots, v_r$ die Darstellungen der Klassen von $u_0, u_1, \ldots, u_r$ bezüglich dem Erzeugendensystem g von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$. Nach Lemma I.18 ist dann

$$\left(\begin{pmatrix} g \end{pmatrix}, \begin{pmatrix} M \\ v_0 \\ \vdots \\ v_r \end{pmatrix} \right)$$

eine Darstellung der Gruppe $(\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}})/(\mathbf{U_K}/\mathbf{U_{\mathfrak{m}}})$.

Erzeugende der Klassengruppe, die teilerfremd zu $\mathfrak{m}_0$ sind. Um Erzeugende der Klassengruppe zu erhalten, die zu $\mathfrak{m}_0$ teilerfremd sind, lösen wir die im Beweis von Lemma II.5 angegebenen Kongruenzen mit dem in III.23 angegebenen Verfahren.

Berechnen der Strahlklassengruppe. Die Klasse eines Ideals $\mathfrak{a}$ modulo $\mathbf{H}_{\mathfrak{m}}$ sei mit $[\,\mathfrak{a}\,]_{\mathfrak{m}}$ und die Klasse von $\mathfrak{a}$ modulo $\mathbf{H}^{\mathfrak{m}}$ mit $[\,\mathfrak{a}\,]^{\mathfrak{m}}$ bezeichnet. Die Sequenz

$$\begin{array}{ccccccc} 1 \to & \mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}} & \xrightarrow{\Psi} & \mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}} & \xrightarrow{\Phi} & \mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{\mathfrak{m}} & \to 1 \\ & [\,(a)\,]_{\mathfrak{m}} & \mapsto & [\,(a)\,]_{\mathfrak{m}} & & & \\ & & & [\,\mathfrak{a}\,]_{\mathfrak{m}} & \mapsto & [\,\mathfrak{a}\,]^{\mathfrak{m}} & \end{array}$$

ist nach Satz II.4 exakt. Wir wenden Lemma I.19 an, um Erzeugende und Relationen für die Strahlklassengruppe zu bestimmen. Es seien (g, M) und (c, C) die Erzeugenden und Relationen von $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ beziehungsweise $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{\mathfrak{m}}$. Die Erzeugenden von $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ sind $\binom{c}{g}$. Wir erhalten die Matrix P für die $Cc = Pg$ gilt mit dem Verfahren zur Darstellung von Klassen bezüglich der Erzeugenden von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$. Damit ist

$$\left(\begin{pmatrix} c \\ g \end{pmatrix}, \begin{pmatrix} C & -P \\ 0 & G \end{pmatrix} \right)$$

eine Darstellung von $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$. Eine Darstellung einer Klasse von $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ bezüglich den Erzeugenden $\binom{c}{g}$ erhalten wir durch Aneinanderhängen der Darstellungen bezüglich c und g.

Reduzieren von Repräsentanten. Wenn wir aus einer Darstellung (g, M) einer endlichen abelschen Gruppe mit der Smith Normalform eine Basisdarstellung erstellen, sind die Basiselemente durch ein Potenzprodukt der Erzeugenden g gegeben. Diese Potenzprodukte führen zu großen Koeffizienten in den Darstellungen der algebraischen Zahlen und Ideale. Wir stellen einige Verfahren zur Reduktion der Repräsentanten vor:

- Wir wissen, daß $Mg = 1$ ist. Wir können also die Exponenten durch die Zeilen von M reduzieren.
- Es sei $w = (w_1, \dots, w_n)^T$ eine Basis von $\mathfrak{o}_{\mathbf{K}}$, es seien $a \in \mathfrak{o}_{\mathbf{K}}$ und $v \in \mathbb{Z}^n$ gegeben, so daß $a = vw$ ist. Es sei $\mathfrak{a}$ ein Ideal von $\mathfrak{o}_{\mathbf{K}}$ und $[a]$ die Klasse von a modulo $\mathfrak{a}$.
  - Wenn wir die Komponenten von v modulo der kleinsten positiven ganzen Zahl in $\mathfrak{a}$ reduzieren, erhalten wir einen Vertreter von $[a]$ mit kleineren Koeffizienten. Dieses Verfahren ist recht schnell.
  - Man reduziert v mit den Zeilen der Matrix A. Wenn A in oberer Zeilen Hermiter Normalform gegeben ist, beginnt man mit der obersten Zeile, reduzieren mit dieser so lange wie möglich und geht dann zur nächsten Zeile über. Dieses Verfahren hat den Vorteil, daß man so einen eindeutigen Repräsentanten in $\mathfrak{o}_{\mathbf{K}}/\mathfrak{a}$ erhält.
- Wenn wir einen Repräsentanten $a \in \mathbf{K}^{\mathfrak{m}}$ der Klasse $[a]$ in $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ reduzieren, speichern wir zunächst die Signatur von a. Mit Algorithmus IV.1 und der gespeicherten Signatur erhalten wir einen reduzierten Repräsentanten von a.
- Wenn wir aus der Darstellung der Strahlklassengruppe durch Erzeugende und Relationen eine Basisdarstellung konstruieren, berechnen wir Potenzprodukte von Idealen. Die Erzeugenden von $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ sind Hauptideale, deren Erzeugende wir, wie oben für die Repräsentanten von Klassen in $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ beschrieben, reduzieren können. Es sei $\mathfrak{a}$ eins der Erzeugenden der Klassengruppe und γ die Ordnung von $\mathfrak{a}$ in $\mathbf{Cl}_{\mathbf{K}}$. Es sei $\beta \in \mathbb{Z}^{>0}$ gegeben, dann gibt es $q, r \in \mathbb{Z}$, so daß $\beta = q\gamma + r$ ist und γ nicht r teilt. Um einen reduzierten Repräsentanten von $\mathfrak{a}^{\beta}$ zu erhalten, berechnet man zunächst $\mathfrak{a}^{q\gamma}$. $\mathfrak{a}^{q\gamma}$ ist ein Hauptideal, dessen Erzeugendes wir wieder wie oben reduzieren können. Danach multipliziert man das reduzierte Erzeugende mit $\mathfrak{a}^{r}$.

KAPITEL V

Der Führer einer Strahlklassengruppe

Wir wollen den Führer einer Strahlklassengruppe $\bmod^* \mathfrak{m}$ berechnen, d.h. den kleinsten Kongruenzmodul $\mathfrak{f}$ mit $\mathfrak{f} \mid \mathfrak{m}$ finden, der die gleiche Strahlklassengruppe erzeugt. Zunächst führen wir den Führer ein und entwickeln dann einen Algorithmus zur Berechnung des Führers. Die Einführung des Führers stammt im wesentlichen aus [Has67].

Wir verwenden die Bezeichnungen aus Kapitel II.

Definition V.1. *Unter einer modulo $\mathfrak{m}$ erklärten Idealgruppe versteht man irgendeine Untergruppe $\mathbf{J}_\mathfrak{m}$ der Gruppe $\mathbf{I}^\mathfrak{m}$, die den Strahl $\mathbf{H}_\mathfrak{m}$ mod $\mathfrak{m}$ enthält.*

Es ist klar, daß durch jede solche Idealgruppe $\mathbf{J}_\mathfrak{m}$ wieder eine Idealklasseneinteilung $\mathbf{I}^\mathfrak{m}/\mathbf{J}_\mathfrak{m}$ gegeben ist.

Um eine Definition der Gleichheit zweier Klasseneinteilungen zu entwickeln, betrachten wir eine Idealgruppe $\mathbf{J}_\mathfrak{m}$, die modulo einem Kongruenzmodul $\mathfrak{m}$ erklärt ist. Sei $\mathfrak{t}$ irgendein weiterer Kongruenzmodul, dann ist die kleinere Gruppe $\mathbf{J}_{\mathfrak{m}\mathfrak{t}} = \mathbf{J}_\mathfrak{m} \cap \mathbf{H}_\mathfrak{t}$ modulo $\mathfrak{t}$ erklärt, denn es gilt $\mathbf{I}^{\mathfrak{m}\mathfrak{t}} \supset \mathbf{J}_{\mathfrak{m}\mathfrak{t}} = \mathbf{J}_\mathfrak{m} \cap \mathbf{I}^\mathfrak{t} \supset \mathbf{H}_\mathfrak{m} \cap \mathbf{I}^\mathfrak{t} \supset \mathbf{H}_{\mathfrak{m}\mathfrak{t}}$.

Mit dem folgenden Lemma ist klar, daß $\mathbf{I}^{\mathfrak{m}\mathfrak{t}}/\mathbf{J}_{\mathfrak{m}\mathfrak{t}} \cong \mathbf{I}^\mathfrak{m}/\mathbf{J}_\mathfrak{m}$ ist.

Lemma V.2. *In jeder Klasse nach einer Idealgruppe $\mathbf{J}_\mathfrak{m}$ existieren unendliche viele zu $\mathfrak{t}$ prime Ideale.*

Wir definieren also:

Definition V.3. *Zwei Idealgruppen $\mathbf{J}_{\mathfrak{m}_1}$ und $\mathbf{J}_{\mathfrak{m}_2}$ heißen im wesentlichen gleich, $\mathbf{J}_{\mathfrak{m}_1} \approx \mathbf{J}_{\mathfrak{m}_2}$, wenn ein ganzes Ideal $\mathfrak{t}$ existiert, so daß die zu $\mathfrak{t}$ primen Ideale in $\mathbf{J}_{\mathfrak{m}_1}$ und $\mathbf{J}_{\mathfrak{m}_2}$ dieselben sind, d.h.:*

$$\mathbf{J}_{\mathfrak{m}_1} \cap \mathbf{I}^\mathfrak{t} = \mathbf{J}_{\mathfrak{m}_2} \cap \mathbf{I}^\mathfrak{t}.$$

Wir fassen nun die sämtlichen mit einer gegebenen Idealgruppe im wesentlichen gleichen Idealgruppen als Repräsentanten einer Idealgruppe $\mathbf{J}$ im weiteren Sinne auf. Diese bestimmen sämtlich isomorphe Idealklassengruppen. Wir sagen $\mathbf{J}$ sei nach dem Modul $\mathfrak{m}$ erklärt, wenn wir einen modulo $\mathfrak{m}$ erklärten Repräsentanten besonders hervorheben wollen, und nennen $\mathfrak{m}$ einen Erklärungsmodul von $\mathbf{H}$.

Satz V.4. *Wenn eine Idealgruppe nach zwei Kongruenzmoduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ erklärbar ist, so ist sie auch nach dem größten gemeinsamen Teiler $\mathfrak{m} = (\mathfrak{m}_1, \mathfrak{m}_2)$ erklärbar.*

Satz V.5. *Die sämtlichen Erklärungsmoduln einer Idealgruppe $\mathbf{J}$ sind mit den sämtlichen ganzen Multipla eines kleinsten Erklärungsmoduls $\mathfrak{f}$ identisch.*

Definition V.6 (Führer). *Dieser Erklärungsmodul $\mathfrak{f}$ heißt der Führer von $\mathbf{J}$.*

Wir nennen den Führer von $\mathbf{H}_\mathfrak{m}$ den Führer von $\mathbf{Cl}_\mathbf{K}^\mathfrak{m} = \mathbf{I}^\mathfrak{m}/\mathbf{H}_\mathfrak{m}$.

Beispiel V.7 (Führer von $6\mathfrak{p}_\infty$). *Betrachten wir die Strahlklassengruppe modulo $6\mathfrak{p}_\infty$ von $\mathbb{Q}$. $(\mathbb{Z}/6\mathbb{Z})^*$ besteht aus den Klassen von $1, 5$. Das Erzeugende für die unendliche Stelle $\mathfrak{p}_\infty$ ist -5, also ist $-1, -5, 1, 5$ ein Repräsentantensystem von $\mathbb{Q}^{6\mathfrak{p}_\infty}/\mathbb{Q}_{6\mathfrak{p}_\infty}$. -1 erzeugt die Einheitengruppe. Faktorisieren wir nach dem Bild der Einheiten, so erhalten wir die beiden durch $(1), (5)$ vertretenden Strahlklassen.*

Nun behaupten wir, daß nicht $6\mathfrak{p}_\infty$ der Führer der Strahlklassengruppe ist sondern $3\mathfrak{p}_\infty$. Gehen wir wie oben vor, sehen wir, daß auch die Strahlklassengruppe modulo $3\mathfrak{p}_\infty$ aus zwei Klassen, die von $(1), (2)$ oder auch $(1), (5)$ vertreten werden, besteht.

Berechnen des Führers. Für die Strahlklassengruppe $\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$ modulo $\mathfrak{m}$ von $\mathbf{K}$ gilt mit den Bezeichnungen aus Kapitel II

$$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}/(\mathbf{H}^\mathfrak{m}/\mathbf{H}_\mathfrak{m}) \cong \mathbf{I}_\mathbf{K}/\mathbf{H}_\mathbf{K} = \mathbf{Cl}_\mathbf{K}.$$

Wenn es einen Kongruenzmodul $\mathfrak{t} \mid \mathfrak{m}$ mit $\mathbf{H}^\mathfrak{t}/\mathbf{H}_\mathfrak{t} \cong \mathbf{H}^\mathfrak{m}/\mathbf{H}_\mathfrak{m}$ gibt, gilt $\mathbf{Cl}_\mathbf{K}^\mathfrak{t} \cong \mathbf{Cl}_\mathbf{K}^\mathfrak{m}$. Für einen Kongruenzmodul $\mathfrak{n} = \mathfrak{n}_0\mathfrak{n}_\infty$ sei $h_\mathfrak{n}$ der Homomorphismus

$$\begin{array}{rcc} h_\mathfrak{n} : \mathbf{K} & \to & ((\mathfrak{o}_\mathbf{K}/\mathfrak{n}_0)^* \times \prod_{\mathfrak{p}_\infty \mid \mathfrak{n}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}) \\ a & \mapsto & ([a], \mathrm{sig}^{\mathfrak{n}_\infty}(a)). \end{array}$$

Es gilt:

$$\mathbf{H}^\mathfrak{m}/\mathbf{H}_\mathfrak{m} \cong (\mathbf{K}^\mathfrak{m}/\mathbf{K}_\mathfrak{m})/(\mathbf{U}_\mathbf{K}/\mathbf{U}_\mathfrak{m}) \cong \left((\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^* \times \prod_{\mathfrak{p}_\infty \mid \mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}\right)/h_\mathfrak{m}(\mathbf{U}_\mathbf{K}).$$

Um den Führer von $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$ zu bestimmen, brauchen wir also nur das größte $\mathfrak{t}$ mit

$$\left((\mathfrak{o}_{\mathbf{K}}/\mathfrak{t}_0)^* \times \prod_{\mathfrak{p}_\infty|\mathfrak{t}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}\right)/h_{\mathfrak{t}}(\mathbf{U}_{\mathbf{K}}) \cong \left((\mathfrak{o}_{\mathbf{K}}/\mathfrak{m}_0)^* \times \prod_{\mathfrak{p}_\infty|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}\right)/h_{\mathfrak{m}}(\mathbf{U}_{\mathbf{K}})$$

zu berechnen. Es seien $u_0, \ldots, u_r$ Erzeugende der Einheitengruppe von $\mathfrak{o}_{\mathbf{K}}$ und die beiden Gruppen seien durch $(g_{\mathfrak{t}}, M_{\mathfrak{t}})$ bzw. $(g_{\mathfrak{m}}, M_{\mathfrak{m}})$ gegeben. Wenn $v_{i\mathfrak{m}}$ die Darstellung u_i bezüglich dem Erzeugendensystem $g_{\mathfrak{m}}$ ist, und die $v_{i\mathfrak{t}}$ analog ist, können wir das Problem darauf reduzieren das größte $\mathfrak{t}$ zu ermitteln, für das die Hermite Normalformen der folgenden Matrizen gleich sind:

$$\begin{pmatrix} M_{\mathfrak{t}} \\ V_{\mathfrak{t}} \end{pmatrix} = \begin{pmatrix} M_{\mathfrak{t}} \\ v_{0\mathfrak{t}} \\ \vdots \\ v_{r\mathfrak{t}} \end{pmatrix}, \begin{pmatrix} M_{\mathfrak{m}} \\ V_{\mathfrak{m}} \end{pmatrix} = \begin{pmatrix} M_{\mathfrak{m}} \\ v_{0\mathfrak{m}} \\ \vdots \\ v_{r\mathfrak{m}} \end{pmatrix}$$

Nach Satz V.4 ist es möglich für jede Primstelle $\mathfrak{p} \mid \mathfrak{m}$, jeweils zu versuchen, um eine Potenz herunterzugehen, d.h. für $\mathfrak{t} = \mathfrak{m}\mathfrak{p}^{-1}$ zu setzen, und dann die Hermite Normalformen der Matrizen $\left(\begin{smallmatrix} M_{\mathfrak{t}} \\ V_{\mathfrak{t}} \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} M_{\mathfrak{m}} \\ V_{\mathfrak{m}} \end{smallmatrix}\right)$ zu vergleichen. Wenn der erste erfolgreich war, versucht man es im nächsten Schritt mit $\mathfrak{t} = \mathfrak{m}\mathfrak{p}^{-2}$. Ansonsten geht man zur nächsten Primstelle über und versucht wieder um ein Potenz herunterzugehen.

Wir werden den Algorithmus zur Berechnung des Führers zunächst für $\mathfrak{m} = \mathfrak{p}^m$ im Fall I (siehe Satz III.7) mit $m > 1$ erläutern. Sei p die Primzahl unter $\mathfrak{p}$ und seien e, f der Verzweigungsindex und der Trägheitsgrad von $\mathfrak{p}$. Sei $M_{\mathfrak{p}^m}$ die Relationenmatrix von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^m)^*$. Sie hat die Gestalt

$$M_{\mathfrak{p}^m} = \begin{pmatrix} p^f - 1 & & & & & & & & \\ & p^{s_{11}} & & & & & 0 & & \\ & & \ddots & & & & & & \\ & & & p^{s_{1\nu}} & & & & & \\ & & & & \ddots & & & & \\ & & & & & p^{s_{\mathrm{f}\nu}} & & & \\ & 0 & & & & & \ddots & & \\ & & & & & & & p^{s_{\mathrm{fe}}} \end{pmatrix}.$$

Wenn ν die Grundstufe der Stufe $m - 1$ ist, ist die Relationenmatrix $M_{\mathfrak{p}^{m-1}}$ von

$(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m-1})^*$ gegeben durch

$$M_{\mathfrak{p}^{m-1}} = \begin{pmatrix} p^f-1 & & & & & & & \\ & p^{s_{11}} & & & & & 0 & \\ & & \ddots & & & & & \\ & & & p^{s_{1\nu}-1} & & & & \\ & & & & \ddots & & & \\ & & & & & p^{s_{\mathfrak{f}\nu}-1} & & \\ & 0 & & & & & \ddots & \\ & & & & & & & p^{s_{\mathfrak{f}\mathfrak{e}}} \end{pmatrix}.$$

Ist $v_{i\mathfrak{p}^m}$ wieder der Vektor, der die Einheit u_i bezüglich der Erzeugenden von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^m)^*$ darstellt, Dann ist $v_{i\mathfrak{p}^m}$ auch eine Darstellung bezüglich der Erzeugenden von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m-1})^*$ in $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^{m-1})^*$. Sei $V_{\mathfrak{p}^m}$ die Matrix, deren Zeilen die $v_{i\mathfrak{p}^m}$ sind. Wir brauchen nur noch die Hermite Normalformen von

$$\begin{pmatrix} M_{\mathfrak{p}^{m-1}} \\ V_{\mathfrak{p}^m} \end{pmatrix} \text{ und } \begin{pmatrix} M_{\mathfrak{p}^m} \\ V_{\mathfrak{p}^m} \end{pmatrix}$$

zu vergleichen, um festzustellen, ob $\mathfrak{p}^{m-1}$ ein Erklärungsmodul von $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$ ist.

Beim heruntergehen um eine Primidealpotenz verringert sich die Ordnung von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^m)^*$ um den Faktor p^{f}, und zwar ändern sich die Ordnungen von f Erzeugenden um den Faktor p. Ein einziges $v_{i\mathfrak{p}^m}$ kann somit nur eine Verringerung der Ordnung um p bewirken, es folgt

Bemerkung V.8. *Wenn f größer ist als die Anzahl der unabhängigen $v_{i\mathfrak{p}^m}$, die das Bild der Einheiten in $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p}^m)^*$ erzeugen, ist für dieses Primideal kein Abstieg möglich.*

Für Primideale im Fall IIa und IIb (siehe Korollar III.13 bzw. Korollar III.16) geht man analog vor, man muß jedoch den Wechsel der Erzeugenden beim Schritt von $\mathfrak{p}^{\frac{p\mathrm{e}}{p-1}+1}$ auf $\mathfrak{p}^{\frac{p\mathrm{e}}{p-1}}$ beachten.

Im Fall II benutzt man, wenn weder durch den Fall IIa noch durch den Fall IIb von vorneherein eine Basis vorliegt, die Darstellung die der Algorithmus III.12 liefert. In die Zeile mit der Relation wird im Schritt von $\mathfrak{p}^{\frac{p\mathrm{e}}{p-1}+1}$ auf $\mathfrak{p}^{\frac{p\mathrm{e}}{p-1}}$ an die entsprechende Stelle die Ordnung von $\eta_{1\mathrm{e}_0}$ geschrieben, der Rest der Zeile wird mit Nullen aufgefüllt, und danach wie die anderen behandelt. Bei allen anderen Schritten (Stufen größer als $\frac{p\mathrm{e}}{p-1}$) ändert sich diese Zeile nicht, denn für die Relation gilt das Gleiche wie für die Darstellung der Einheiten.

Im Schritt $\mathfrak{p}^1$ nach $\mathfrak{p}^0$ wird die Ordnung des primitiven Elementes von $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{p})^*$ auf 1 gesetzt.

Für die Unendlichen Stellen geht man ebenso vor.

Algorithmus V.9 (Führer der Strahlklassengruppe).

Eingabe: $\mathfrak{o}_{\mathbf{K}}, \mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty = \prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{m_\mathfrak{p}} \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathfrak{p}, \mathbf{U}_{\mathbf{K}}$

Ausgabe: *Führer* $\mathfrak{f}$ *von* $\mathbf{Cl}_{\mathbf{K}}^{\mathfrak{m}}$

- *Berechne mit Algorithmus* III.24 *und dem Verfahren mit Einseinheiten eine Darstellung* (g, M) *von* $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{m})^*$.
- *Berechne die Darstellungsmatrix* V *der Einheitengruppe in* $(\mathfrak{o}_{\mathbf{K}}/\mathfrak{m})^*$.
- *Für alle* $\mathfrak{p} \mid \mathfrak{m}_0$:
  - *Setze* $n_\mathfrak{p} \leftarrow m_\mathfrak{p}$.
  - *Wiederhole:*
    - *Berechne die Grundstufe* ν *der Stufe* $m-1$.
    - *Setze* $T \leftarrow M$
    - *Wenn* $m = 1$ *ist:*
      - *Setze die Ordnungen der* $g_{\mathfrak{p}(i\nu)}$ *für* $i = 1, \ldots, f$ *in* T *auf eins.*
    - *sonst, wenn* $\mathfrak{p}$ *im Fall IIc ist und* $\nu' = e_0$ *und* $m > \frac{pe}{p-1}$:
      - *Teile die Ordnungen der* $g_{i\nu'}$ *für* $i = 2, \ldots, f$ *in* T *durch* p.
      - *Teile die Ordnung von* g_* *in* T *durch* p.
    - *sonst, wenn* $\mathfrak{p}$ *im Fall IIc ist und* $\nu' = e_0$ *und* $m = \frac{pe}{p-1}$:
      - *Teile die Ordnungen der* $g_{i\nu'}$ *für* $i = 2, \ldots, f$ *in* T *durch* p.
      - *Setze die Ordnung von* g_* *auf eins.*
      - *Lösche die Zeile mit der Relation und setze die Ordnung von* $\eta_{1\nu'}$ *auf* p^{μ_0}.
    - *sonst*
      - *Teile die Ordnungen der* $g_{i\nu'}$ *für* $i = 1, \ldots, f$ *in* T *durch* p.
    - *Wenn die Hermite Normalform von* $\binom{T}{V}$ *gleich der Hermiten Normalform von* $\binom{M}{V}$ *ist:*
      - *Setze* $n_\mathfrak{p} \leftarrow n_\mathfrak{p} - 1$.
      - *Setze* $M \leftarrow T$.
  - *solange die Hermite Normalform von* $\binom{T}{V}$ *gleich der Hermiten Normalform von* $\binom{M}{V}$ *ist.*
- *Für alle* $\mathfrak{p} \mid \mathfrak{m}_\infty$:
  - *Setze* $n_\mathfrak{p} \leftarrow 1$.
  - *Setze* $T \leftarrow M$.
  - *Setze die Ordnung von* $g_\mathfrak{p}$ *in* T *auf eins.*
  - *Wenn die Hermite Normalform von* $\binom{T}{V}$ *gleich der Hermiten Normalform von* $\binom{M}{V}$ *ist:*
    - *Setze* $n_\mathfrak{p} \leftarrow 0$.
    - *Setze* $M \leftarrow T$.
- *Setze* $\mathfrak{f} \leftarrow \prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{n_\mathfrak{p}} \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathfrak{p}^{n_\mathfrak{p}}$. *Gib* $\mathfrak{f}$ *zurück.*

KAPITEL VI

Beispiele

Die Algorithmen zur Berechnung von Strahlklassengruppen und zur Berechnung der multiplikativen Gruppe von Restklassenringen mit unserem Verfahren mit Einseinheiten wurden von uns in dem Computeralgebrasystem KANT [DFK+96] implementiert. Das Verfahren von Cohen ist in dem Computeralgebrasystem **PARI** [BBCO96] implementiert.

Bei der Implementierung der Strahlklassengruppen in **PARI**, wurden zum Teil andere Verfahren, als die von uns vorgestellten, gewählt. So werden die Elemente von $\mathbf{K}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m}}$ nicht durch algebraische Zahlen, deren Konjugierte entsprechende Vorzeichenbedingungen erfüllen, dargestellt, sondern durch eine algebraische Zahl und die Signatur, die dieses Element haben sollte.

Die Rechenzeiten lassen sich nicht unbedingt absolut vergleichen, da die Computeralgebrasysteme **PARI** und KANT sich in ihrem grundlegendem Aufbau unterscheiden, und es dadurch zu Laufzeitunterschieden kommen kann, ohne daß diese direkt auf die unterschiedlichen Algorithmen zur Berechnung der multiplikativen Gruppe von Restklassenringen zurückzuführen sind.

Die Beispiele wurden auf einer HP9000/735 unter HPUX 9.01 mit 60 MB für einen Prozeß verfügbaren Arbeitspeicher gerechnet.

Die Einträge in den Tabellen sind folgendermaßen zu verstehen:

$f(t)$ .... gibt den jeweils betrachteten Körper $\mathbf{K} = \mathbb{Q}(\rho) = \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ an.

r_1 .... ist die Anzahl der reellen Nullstellen von $f(t)$.

$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$. ist ein Kongruenzmodul.

$\mathfrak{p}$,$\mathfrak{m}_0$ .... sind Ideale, die durch ein oder zwei Erzeugende angegeben werden. Ein Eintrag $(p) = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$ stellt die Faktorisierung des Ideals (p) in Primideale dar, die Faktoren werden dann in weiteren Beispielen verwendet.

e .... ist der Verzweigungsindex von $\mathfrak{p}$.

f .... ist der Trägheitsgrad von $\mathfrak{p}$.

$\mathfrak{m}_\infty$ .... ist ein formales Produkt unendlicher Stellen. Die Numerierung der unendlichen Stellen entspricht derjenigen, die in KANT für die Numerierung der Konjugierten benutzt wird.

$\mathfrak{f}$ .... ist der Führer der Strahlklassengruppe modulo $\mathfrak{m}$.

$[a]$.......... ist die Darstellung der Klasse von $a \in \mathfrak{o}_\mathbf{K}$ bezüglich der Erzeugenden der multiplikativen Gruppe $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$ des Restklassenringes $\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m$. Wir verwenden dies nur, um die Zeiten zu vergleichen, die KANT und **PARI** zur Berechnung der Darstellung benötigen. Es spielt im Grunde keine Rolle, für welches $a \in \mathfrak{o}_\mathbf{K}$ wir diese angeben, da die Anzahl der Operationen unabhängig von dem betrachteten Element ist.

$(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$ ... ist die Struktur der Gruppe $(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$ als Produkt zyklischer Untergruppen oder die Zeit, die zum Berechnen der Erzeugenden und Relationen benötigt wird.

$\mathbf{Cl}_\mathbf{K}$ .... ist die Struktur der Klassengruppe von $\mathbf{K}$ als Produkt zyklischer Untergruppen.

$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$ .... ist die Struktur der Strahlklassengruppe modulo $\mathfrak{m}$ als Produkt zyklischer Untergruppen oder die Zeit, die zum Berechnen der Erzeugenden und Relationen benötigt wird. Darin ist die Zeit zur Berechnung der multiplikativen Gruppe des Restklassenringes enthalten, die Zeiten für die Berechnung der Klassengruppe und der Einheitengruppe von $\mathbf{K}$ sind nicht enthalten.

PARI...... ist die Zeit, die für die jeweilige Berechnung in **PARI** benötigt wird.

KANT...... ist die Zeit, die für die jeweilige Berechnung in KANT benötigt wird.

Der Eintrag '>60 MB' besagt, daß der verfügbare Arbeitspeicher des Computers nicht ausreichend war, um die Berechnung fortzusetzen.

Ideal $\mathfrak{p}^m$		$(\mathfrak{o}_K/\mathfrak{p}^m)^*$		[a]		
$\mathfrak{p}$	m	**PARI**	KANT	a	**PARI**	KANT
$f(t) = t^3 + 23t^2 + 88t + 51$						
(7)	6	230 ms	30 ms	5	50 ms	60 ms
(7)	13	98 s	300 ms	5	90 ms	2340 ms
(7)	20	17 min	520 ms	5	130 ms	8110 ms
(7)	40	>60 MB	1420 ms	5	—	44 s
$(29, 18+\rho)$	13	450 ms	120 ms	5	40 ms	1080 ms
$(29, 18+\rho)$	40	16 s	340 ms	5	90 ms	17 s
$f(t) = t^4 + 14t^3 + 8t^2 + 4t + 11$						
$(2, 1+\rho)$	6	280 ms	20 ms	5	30 ms	10 ms
$(2, 1+\rho)$	13	570 ms	70 ms	5	30 ms	40 ms
$(2, 1+\rho)$	25	1330 ms	180 ms	5	40 ms	110 ms
$(2, 1+\rho)$	40	130 s	370 ms	5	50 ms	250 ms
$f(t) = t^6 + 11t^5 + 20t^4 + 3t^3 - 18t^2 + 7t + 11$						
$(3, 1+\rho^3)$	2	410 ms	40 ms	7	110 ms	10 ms
$(3, 1+\rho^3)$	6	1169 ms	100 ms	7	140 ms	190 ms
$(3, 1+\rho^3)$	13	1980 ms	130 ms	7	100 ms	840 ms
$(3, 1+\rho^3)$	25	4490 ms	1690 ms	7	220 ms	34 s
$(3, 1+\rho^3)$	40	147 s	3140 ms	7	310 ms	114 s
$(47, 40+20\rho+\rho^2)$	25	140 s	3970 ms	7	5070 ms	42 s
$(47, 40+20\rho+\rho^2)$	40	380 s	22 s	7	12 s	13 min
$f(t) = t^{14} - 15t^{13} + 14t^{12} - 5t^{11} - 17t^{10} + 17t^9 + 4t^8 + 8t^7 + 16t^6 - 17t^5 + 8t^4$ $+12t^3 - 4t^2 - 16t - 10$						
$(5, \rho)$	6	7480 ms	730 ms	6	1390 ms	1350 ms
$(5, \rho)$	13	13 s	2030 ms	6	1390 ms	57 s
$(5, \rho)$	25	22 s	3480 ms	6	2160 ms	196 s
$(5, \rho)$	40	41 s	7150 ms	6	2690 ms	18 min
$f(t) = t^{20} - 5t^{19} + 3t^{18} - 7t^{17} + 12t^{16} - 3t^{15} + 7t^{14} + 17t^{13} - 6t^{12} - 9t^{11}$ $+5t^{10} + 11t^9 + 3t^8 - 10t^7 - 18t^6 + 10t^5 + 17t^4 + 16t^3 - 14t^2 + 3t - 15$						
$(7, 1+\rho)$	2	11 s	1370 ms	6	4060 ms	420 ms
$(7, 1+\rho)$	6	27 s	2420 ms	6	4060 ms	4930 ms
$(7, 1+\rho)$	13	48 s	6070 ms	6	6740 ms	259 s
$(7, 1+\rho)$	25	90 s	11 s	6	8930 ms	20 min

Tabelle 1: Vergleich der Verfahren zur Berechnung der multiplikativen Gruppe von Restklassenringen. Das Ideal über der 2 im zweiten Abschnitt ist für $m > \frac{pe}{p-1} = 8$ ein Beispiel für den Fall II.

$f(t) = t^3 + 8t^2 + 6t - 17$		$\mathfrak{p} = (3)$	e = 1	f = 3
$\mathfrak{m}$	$\mathrm{ord}(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$		
1	26	C_{26}		
2	702	$C_{26} \times C_3 \times C_3 \times C_3$		
3	18954	$C_{26} \times C_9 \times C_9 \times C_9$		
4	511758	$C_{26} \times C_{27} \times C_{27} \times C_{27}$		
$f(t) = t^4 + 11t^3 - 19t^2 - 8t + 7$		$\mathfrak{p} = (3, 2 + \rho + \rho^2)$	e = 2	f = 2
m	$\mathrm{ord}(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$		
1	8	C_8		
2	72	$C_8 \times C_3 \times C_3$		
3	648	$C_8 \times C_3 \times C_3 \times C_3 \times C_3$		
4	5826	$C_8 \times C_3 \times C_3 \times C_3 \times C_3 \times C_9$		
5	52488	$C_8 \times C_3 \times C_3 \times C_9 \times C_9 \times C_9$		
6	472392	$C_8 \times C_3 \times C_9 \times C_9 \times C_9 \times C_{27}$		
$f(t) = t^6 + 6t^5 - 12 * t^4 - t^3 - 6t^2 + 9t + 20$		$\mathfrak{p} = (3, 2 + 2\rho + \rho^2)$	e = 3	f = 2
m	$\mathrm{ord}(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{p}^m)^*$		
1	8	C_8		
2	72	$C_8 \times C_3 \times C_3$		
3	648	$C_8 \times C_3 \times C_3 \times C_3 \times C_3$		
4	5832	$C_8 \times C_9 \times C_9 \times C_3 \times C_3$		
5	52488	$C_8 \times C_9 \times C_9 \times C_3 \times C_3 \times C_3 \times C_3$		
6	472392	$C_8 \times C_9 \times C_9 \times C_9 \times C_9 \times C_3 \times C_3$		

Tabelle 2: Struktur der multiplikativen Gruppe von Restklassenringen, wie man sie mit dem Verfahren mit Einseinheiten erhält. Das Ideal im zweiten Abschnitt ist für $m \geq 4$ ein Beispiel für den Fall II, für $m = 4$ ein Beispiel für den Fall IIa.

$f(t) = t^{12} + 7t^{11} - 97t^{10} - 859t^9 + 2558t^8 + 38839t^7 + 30012t^6 - 710649t^5$ $-2189082t^4 + 2534629t^3 + 23514673t^2 + 43623088t + 28168151$		
$\mathfrak{m}_0$	$\mathrm{ord}(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$
(3)	512000	${C_{80}}^3$
(4)	14745600	$C_{15} \times {C_2}^4 \times C_{15} \times {C_4}^4 \times {C_2}^4$
(5)	186500000	$C_{24} \times {C_5}^6 \times C_4 \times {C_5}^3$
(60)	$14155776 \cdot 10^{14}$	$C_{15} \times {C_2}^4 \times C_{15} \times {C_4}^4 \times {C_2}^4 \times {C_{80}}^3$ $\times C_{24} \times {C_5}^6 \times C_4 \times {C_5}^3$

Tabelle 3: Struktur von multiplikativen Gruppe von Restklassenringen, wie man sie mit dem Verfahren mit Einseinheiten erhält.

$a = 2$	**PARI**			KANT		
$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$	$[a]$	$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$	$[a]$	$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$
$f(t) = t^4 - 4t^2 + 1$					$\mathbf{Cl}_\mathbf{K} \cong \mathrm{C}_1$	$\mathrm{r}_1 = 4$
$(5)^2$	420 ms	100 ms	1100 ms	60 ms	10 ms	120 ms
$\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}\mathfrak{p}_\infty^{(4)}$	—	—	150 ms	—	—	80 ms
$(5)^2\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}\mathfrak{p}_\infty^{(4)}$	420 ms	100 ms	3310 ms	60 ms	10 ms	430 ms
$(5)^6$	1130 ms	170 ms	3310 ms	90 ms	130 ms	610 ms
$(5)^8$	1370 ms	200 ms	22 s	180 ms	260 ms	1250 ms
$(3)^8$	370 s	80 ms	387 s	290 ms	200 ms	1260 ms
$(3)^8\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}\mathfrak{p}_\infty^{(4)}$	370 s	80 ms	460 s	290 ms	200 ms	1580 ms
$f(t) = t^4 - 2t^3 + 7t^2 - 6t + 1$					$\mathbf{Cl}_\mathbf{K} \cong \mathrm{C}_2 \times \mathrm{C}_6$	$\mathrm{r}_1 = 0$
$(5)^2$	500 ms	120 ms	8580 ms	80 ms	10 ms	220 ms
$(5)^6$	1300 ms	200 ms	49 s	100 ms	130 ms	780 ms
$(5)^8$	1540 ms	240 ms	76 s	200 ms	280 ms	17 s
$(5)^{16}$	3100 ms	400 ms	overflow	1580 ms	16 s	70 s
$f(t) = t^7 + 2t^6 + t^5 - t^2 + 5t + 2$					$\mathbf{Cl}_\mathbf{K} \cong \mathrm{C}_2 \times \mathrm{C}_2$	$\mathrm{r}_1 = 1$
$(5)^3$	4820 ms	860 ms	55 s	810 ms	250 ms	2680 ms
$\mathfrak{p}_\infty$	—	—	3450 ms	—	—	250 ms
$(5)^3\mathfrak{p}_\infty$	4820 ms	860 ms	78 s	810 ms	250 ms	2960 ms
$(5)^6$	9090 ms	1180 ms	167 s	930 ms	1120 ms	8200 ms
(31)	1620 ms	32 s	160 s	380 ms	100 ms	1150 ms
$(31)^3$	7300 ms	33 s	370 s	1280 ms	560 ms	3850 ms
$(5)^3(31)^3$	63 min	36 s	2 h 13 min	4160 ms	870 ms	11 s
$f(t) = t^{10} - t^8 + 2t^7 + t^6 + t^5 - 2t^4 - t^3 + 5t^2 - 14t + 9$						$\mathbf{Cl}_\mathbf{K} \cong \mathrm{C}_2 \times \mathrm{C}_2$
$(3)^3$	14 s	3450 ms	110 s	2150 ms	710 ms	164 s
$(5)^3$	22 s	3790 ms	275 s	2700 ms	950 ms	151 s
$(7)^3$	20 s	13 s	5 min	2550 ms	1020 ms	52 s
$(7)^5$	16 min	14 s	21 min	3450 ms	4010 ms	72 s
$(7)^8$	>60 MB	—	—	6350 ms	10 s	115 s
$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (23)$	4780 ms	160 s	15 min	1230 ms	260 ms	47 s
$\mathfrak{p}_1^3 \quad (\mathrm{f}_{\mathfrak{p}_1} = 1)$	1980 ms	490 ms	17 s	160 ms	170 ms	44 s
$\mathfrak{p}_2^3 \quad (\mathrm{f}_{\mathfrak{p}_2} = 3)$	5430 ms	3260 ms	35 s	500 ms	440 ms	46 s
$\mathfrak{p}_3^3 \quad (\mathrm{f}_{\mathfrak{p}_3} = 6)$	11 s	157 s	15 min	1350 ms	890 ms	50 s
$(23)^3$	27 s	162 s	34 min	3510 ms	1560 ms	59 s

Tabelle 4: Vergleich der Verfahren in der Anwendung der Berechnung von Strahlklassengruppen.

$f(t)$	r_1	$\mathbf{Cl_K}$	$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$	$(\mathfrak{o}_\mathbf{K}/\mathfrak{m}_0)^*$	$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$
$t^2 - t + 15$	0	C_3	(2)	C_3	C_9
$t^2 - t + 15$	0	C_3	(4)	$C_3 \times {C_2}^2$	C_{18}
$t^2 - t + 15$	0	C_3	(5)	${C_4}^2$	$C_2 \times C_{12}$
$t^2 - t + 15$	0	C_3	(20)	$C_3 \times {C_2}^2 \times {C_4}^2$	$C_2 \times C_4 \times C_{36}$
$t^3 + 3t^2 - 7t - 4$	3	C_1	$\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}$	C_1	C_1
$t^3 + 3t^2 - 7t - 4$	3	C_1	(5)	$C_4 \times {C_5}^2$	C_2
$t^3 + 3t^2 - 7t - 4$	3	C_1	$(5)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}$	$C_4 \times {C_5}^2$	C_4
$t^3 + 3t^2 - 7t - 4$	3	C_1	(25)	$C_4 \times {C_{25}}^2 \times C_5$	C_{10}
$t^4 + t^2 - 9t + 1$	2	C_2	(1)	C_1	C_2
$t^4 + t^2 - 9t + 1$	2	C_2	$\mathfrak{p}_\infty^{(1)}$	C_1	C_2
$t^4 + t^2 - 9t + 1$	2	C_2	$\mathfrak{p}_\infty^{(2)}$	C_1	C_2
$t^4 + t^2 - 9t + 1$	2	C_2	$\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$	C_1	$C_2 \times C_2$
$t^4 + t^2 - 9t + 1$	2	C_2	(9)	$C_2 \times {C_3}^3 \times C_2 \times {C_3}^3$	$C_6 \times {C_3}^3$
$t^4 + t^2 - 9t + 1$	2	C_2	$(9)\mathfrak{p}_\infty^{(1)}$	$C_2 \times {C_3}^3 \times C_2 \times {C_3}^3$	$C_{12} \times {C_3}^3$
$t^4 + t^2 - 9t + 1$	2	C_2	$(9)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$	$C_2 \times {C_3}^3 \times C_2 \times {C_3}^3$	$C_{12} \times {C_3}^2 \times C_6$

Tabelle 5: Struktur einiger Strahlklassengruppen.

$f(t)$	$\mathfrak{m}$	$\mathfrak{f}$	$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$
$t^4 - 4t^2 + 1$	$\mathfrak{p}^4 = (2)$	(1)	C_1
$t^4 - 4t^2 + 1$	$\mathfrak{p}^4\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}$	$\mathfrak{p}^4\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$	C_2
$t^4 - 4t^2 + 1$	$\mathfrak{p}^7$	(1)	C_1
$t^4 - 4t^2 + 1$	$\mathfrak{p}^8$	$\mathfrak{p}^8$	C_2
$t^4 - 4t^2 + 1$	$\mathfrak{p}^{11}$	$\mathfrak{p}^8$	C_2
$t^4 - 4t^2 + 1$	$\mathfrak{p}^{12}$	$\mathfrak{p}^{12}$	C_4
$t^4 - 4t^2 + 1$	$\mathfrak{p}_1\mathfrak{p}_2 = (5)$	(5)	C_4
$t^4 - 4t^2 + 1$	$\mathfrak{p}_1^{13}$	(1)	C_1
$t^4 - 4t^2 + 1$	$\mathfrak{p}_2^{12}$	(1)	C_1
$t^4 - 4t^2 + 1$	$\mathfrak{p}_1\mathfrak{p}_2^9$	(5)	C_4
$t^4 - 4t^2 + 1$	$\mathfrak{p}_1^2\mathfrak{p}_2^9$	(25)	C_{20}
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$\mathfrak{p}_1\mathfrak{p}_2 = (3)$	(1)	C_1
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$\mathfrak{p}_1^5\mathfrak{p}_2^5 = (3)^5$	$(3)^5$	$C_{81} \times C_3$
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$\mathfrak{p}_1^2\mathfrak{p}_2^5$	$(3)^2$	$C_3 \times C_3$
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$\mathfrak{p}_1^5$	(1)	C_1
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$\mathfrak{p}_2^5$	$\mathfrak{p}_2^2$	C_3
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$\mathfrak{p}_1^5\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}\mathfrak{p}_\infty^{(4)}$	$\mathfrak{p}_1\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}\mathfrak{p}_\infty^{(3)}$	C_2
$t^5 + 6t^4 + 5t^3 - 16t^2 - 10t + 8$	$(5)^2\mathfrak{p}_2^5$	$(5)^2\mathfrak{p}_2^2$	$C_{30} \times C_5$

Tabelle 6: Führer von Strahlklassengruppen.

Symbolverzeichnis

$\mathfrak{b}_\mathfrak{p}$	Bewertungsideal von $\mathfrak{o}_\mathfrak{p}$
C_n	Zyklische Gruppe der Ordnung n
$\mathbb{C}$	Körper der komplexen Zahlen
$\mathbf{Cl}_\mathbf{K}$	Klassengruppe von $\mathbf{K}$
$\mathbf{Cl}_\mathbf{K}^\mathfrak{m}$	Strahlklassengruppe von $\mathbf{K}$ modulo $\mathfrak{m}$
$\mathrm{diag}(a_1, \dots, a_n)$	Diagonalmatrix mit Einträgen $a_1, \dots, a_n$
e	Verzweigungsindex von $\mathfrak{p}$
f	Trägheitsgrad von $\mathfrak{p}$
$\mathfrak{f}$	Führer einer Strahlklassengruppe
$\mathbf{h}_\mathbf{K}$	Klassenzahl von $\mathbf{K}$
$\mathbf{h}_\mathbf{K}^\mathfrak{m}$	Strahlklassenzahl modulo $\mathfrak{m}$
$\mathbf{H}_\mathbf{K}$	Gruppe der gebrochenen Hauptideale von $\mathbf{K}$
$\mathbf{H}^\mathfrak{m}$	Gruppe der zu $\mathfrak{m}$ teilerfremden Hauptideale von $\mathbf{K}$
$\mathbf{H}_\mathfrak{m}$	$= \{(a) \in \mathbf{H}_\mathbf{K} \mid a \equiv 1 \bmod^* \mathfrak{m}\}$
$\mathbf{I}_\mathbf{K}$	Gruppe der Ideale von $\mathbf{K}$
$\mathbf{K}$	algebraischer Zahlkörper
$\mathbf{K}^\mathfrak{m}$	Elemente von $\mathbf{K}$, die teilerfremd zu $\mathfrak{m}$ sind
$\mathbf{K}_\mathfrak{m}$	$= \{a \in \mathbf{K} \mid a \equiv 1 \bmod^* \mathfrak{m}\}$
$\mathbf{K}_\mathfrak{p}$	Vervollständigung von $\mathbf{K}$ bezüglich $\lvert \cdot \rvert_\mathfrak{p}$
$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$	Kongruenzmodul
$\mathfrak{m}_0$	Ideal
$\mathfrak{m}_\infty$	formales Produkt von unendlichen Primstellen
$\bmod^*$	multiplikative Kongruenz
$\mathbb{N}$	Menge der natürliche Zahlen
$\mathbf{N}(\cdot)$	Idealnorm
$\mathfrak{o}_\mathbf{K}$	Maximalordnung von $\mathbf{K}$
$\mathfrak{o}_\mathfrak{p}$	Bewertungsring von $\mathbf{K}_\mathfrak{p}$

p	Primzahl
$\mathfrak{p}$	Primideal über p
$\lvert\cdot\rvert_{\mathfrak{p}}$	$\mathfrak{p}$ - Bewertung
$\mathfrak{p}_\infty$	unendliche Primstelle
$\mathbf{P_K}$	Menge aller Primstellen von $\mathbf{K}$
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{R}$	Körper der reellen Zahlen
$\mathbb{R}^*$	multiplikative Gruppe von $\mathbb{R}$
$\mathbb{R}^{*>0}$	positive Elemente von $\mathbb{R}^*$
$\mathbf{U_K}$	Einheitengruppe von $\mathfrak{o}_\mathbf{K}$
$\mathbf{U}_\mathfrak{p}$	Einheitengruppe von $\mathfrak{o}_\mathfrak{p}$
$\mathbb{Z}$	Ring der ganzen Zahlen
(a,b)	größter gemeinsamer Teiler von a und b.

Literaturverzeichnis

[BBCO96] C. Batut, D. Bernadi, H. Cohen, and M. Olivier, **PARI-GP** *version 1.39.13*, 1996.

[CDyDO95] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Computing ray class groups, conductors and discriminants*, preprint, 1995.

[Coh93] H. Cohen, *A course in computional algebraic number theory*, Springer Verlag, New York, 1993.

[Coh95] H. Cohen, *Algorithms for modules over dedekind domains and relative extensions of number fields*, preprint, 1995.

[DFK+96] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, KANT V4, J. Symbolic Computation **11** (1996).

[DP96] M. Daberkow and M. Pohst, *On the computation of Hilbert class fields*, submitted for publication, 1996.

[Has63] H. Hasse, *Zahlentheorie*, Akademie Verlag, Berlin, 1963.

[Has67] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physika Verlag, Würzburg, 1967.

[Hes96] F. Hess, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, TU - Berlin, 1996.

[Lan86] S. Lang, *Algebraic number theory*, Springer Verlag, New York, 1986.

[Nak79] N. Nakagoshi, *The structure of the multiplicative group of residue classes modulo* $\mathfrak{p}^{\nu+1}$, Nagoya Math. J. **73** (1979), 41 – 60.

[Nar90] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Verlag, Berlin, 1990.

[Poh93] M. Pohst, *Computational algebraic number theory*, Birkhäuser, Basel, 1993.

[PZ89] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[Sim94] C. Sims, *Computation with finitely presented groups*, Cambridge University Press, 1994.