Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve

vorgelegt von
Diplom-Mathematiker
Klaus Wildanger
aus Düsseldorf

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

Berlin 1997
D83

Promotionsausschuß

Vorsitzender:	Prof. Dr. J. Becker
Berichter:	Prof. Dr. M. E. Pohst
Berichter:	Prof. Dr. A. Leutbecher

Tag der wissenschaftlichen Aussprache: 16.07.1997

Inhaltsverzeichnis

Einleitung

Eine diophantische Gleichung ist gemeinhin eine Gleichung

$$f(x_1, x_2, \ldots, x_n) = 0,$$

wobei f ein Polynom mit ganzzahligen Koeffizienten ist. Das Hauptproblem bei der Untersuchung diophantischer Gleichungen besteht darin, festzustellen, ob eine solche Gleichung eine aus ganzen bzw. rationalen Zahlen bestehende Lösung besitzt. In seinem Vortrag auf dem Internationalen Mathematiker-Kongreß formulierte Hilbert als sein zehntes Problem die Frage, ob es einen Algorithmus gibt, der für jede explizit vorgelegte diophantische Gleichung entscheidet, ob die Gleichung eine ganzzahlige Lösung besitzt. Hilberts Problem blieb lange Zeit ungelöst. Erst 1970 zeigte Matiyasevich, daß solch ein Algorithmus nicht existieren kann. Diese negative Lösung des zehnten Hilbertschen Problems bedeutet, daß man sich beim Lösen diophantischer Gleichungen auf bestimmte Klassen dieser Gleichungen beschränken muß.
In dieser Arbeit werden wir das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern sowie die Bestimmung aller ganzen Punkte auf einer Mordellschen Kurve behandeln. Diesen Problemstellungen ist gemein, daß sie jeweils nur höchstens endlich viele Lösungen besitzen. Algorithmen zur vollständigen Berechnung dieser Lösungen wurden möglich durch Ergebnisse von A. Baker zu Linearformen in den Logarithmen algebraischer Zahlen.

Das Lösen einer Einheitengleichung besteht im wesentlichen aus drei Schritten. Zuerst leitet man anhand der Resultate Bakers große obere Schranken für die Lösungen her. Diese Schranken werden im zweiten Schritt des Verfahrens mit dem LLL-Algorithmus reduziert. Im letzten Schritt, welcher die weitaus meiste Rechenzeit beansprucht, müssen alle unterhalb der Schranken liegenden Einheiten daraufhin überprüft werden, ob sie Lösungen der Einheitengleichung sind. Wir beschreiben im ersten Kapitel ein neues Verfahren, mit dem diese Überprüfung sehr viel effizienter als bislang durchgeführt werden kann. Mit dem Verfahren, welches Methoden aus der Geometrie der Zahlen benutzt, lösten wir Einheitengleichungen in Zahlkörpern bis hin zum Einheitenrang 10. Im zweiten Kapitel setzen wir dann Einheitengleichungen zum Lösen von Indexformgleichungen ein. Erstmals konnten hierbei Indexformgleichungen in Zahlkörpern vom Grad 8,10,12,16,18 und 22 gelöst werden. Gegenstand des dritten Kapitels ist schließlich ein neues, auf der Lösung von kubischen Indexformgleichungen basierendes Verfahren zur Bestimmung aller ganzen Punkte auf einer Mordellschen Kurve.

Notationen

Wir fixieren einige Schreibweisen, die während der gesamten Arbeit beibehalten werden.

$\mathcal{K}$ bezeichne stets einen algebraischen Zahlkörper vom Grad $n > 1$ über $\mathbb{Q}$. Es sei jeweils $\mathcal{K} = \mathbb{Q}(\theta)$, wobei $\theta \in \mathbb{C}$ Nullstelle eines normierten und irreduziblen Polynoms mit ganzzahligen Koeffizienten sei, welches r_1 reelle und $2r_2$ komplexe Nullstellen habe. Die n verschiedenen $\mathbb{Q}$-Einbettungen (Konjugationen) von $\mathcal{K}$ in $\mathbb{C}$ seien gegeben durch $\sigma_1, \ldots, \sigma_n$. Ist $j \in \{1, \ldots, n\}$, so schreiben wir $\alpha^{(j)} = \sigma_j(\alpha)$ für die j-te Konjugierte einer algebraischen Zahl $\alpha \in \mathcal{K}$. Die Konjugationen seien in gewohnter Weise numeriert:

(i) $\theta^{(1)}, \ldots, \theta^{(r_1)} \in \mathbb{R}$,

(ii) $\theta^{(r_1+1)}, \ldots, \theta^{(r_1+r_2)} \in \mathbb{C} \setminus \mathbb{R}$,

(iii) $\theta^{(r_1+r_2+j)} = \overline{\theta^{(r_1+j)}}$ $(1 \leq j \leq r_2)$.

Für eine algebraische Zahl $\alpha \in \mathcal{K}$ schreiben wir $\mathrm{Tr}(\alpha) = \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha)$ und $\mathrm{N}(\alpha) = \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha)$ für Spur und Norm von α. Ferner bezeichne $m_\alpha(t)$ das Minimalpolynom von α über $\mathbb{Z}$, und es sei $\mathrm{T}_2(\alpha)$ die sogenannte T_2-Norm von α, also

$$\mathrm{T}_2(\alpha) = \sum_{i=1}^{n} |\alpha^{(i)}|^2 \,.$$

Den ganzen Abschluß von $\mathbb{Z}$ in $\mathcal{K}$ bezeichnen wir mit $\mathfrak{o}_\mathcal{K}$. Es sei $\mathrm{U}_\mathcal{K}$ die Einheitengruppe von $\mathfrak{o}_\mathcal{K}$, und $\mathrm{TU}_\mathcal{K}$ sei die endliche zyklische Gruppe der in $\mathfrak{o}_\mathcal{K}$ gelegenen Einheitswurzeln. Ist $\mathcal{L}$ ein weiterer algebraischer Zahlkörper, so verwenden wir analog die Bezeichnungen $\mathfrak{o}_\mathcal{L}$, $\mathrm{U}_\mathcal{L}$ und $\mathrm{TU}_\mathcal{L}$.

Ein unitärer Teilring R von $\mathfrak{o}_\mathcal{K}$ heißt Ordnung von $\mathcal{K}$, falls R ein freier $\mathbb{Z}$-Modul vom Rang n ist. Für die Diskriminante einer Ordnung R von $\mathcal{K}$ schreiben wir $\mathrm{disc}\, R$ und speziell $\mathrm{disc}_\mathcal{K}$ für die Diskriminante der Maximalordnung $\mathfrak{o}_\mathcal{K}$. Die Diskriminante eines Polynoms $f(t) \in \mathbb{Z}[\approx]$ notieren wir als $\mathrm{disc}\, f$.

Technik

Die praktische Nutzung der in den nächsten Kapiteln beschriebenen Algorithmen setzt voraus, daß wir in algebraischen Zahlkörpern *rechnen* können. Darunter verstehen wir neben der Arithmetik algebraischer Zahlen und Ideale beispielsweise auch die Berechnung von Ganzheitsbasen und Grundeinheitensystemen sowie das Lösen von Normgleichungen. Detaillierte und algorithmisch–orientierte Darstellungen hierzu findet der Leser in [44, 45]. Für die Implementierung unserer Verfahren wurde das Computeralgebra-System KANT [9] verwendet, welches die für das Rechnen in algebraischen Zahlkörpern notwendigen Routinen als C–Funktionen zur Verfügung stellt. Die Beispiele des ersten Kapitels und des Anhangs wurden auf einer SGI Origin 2000 gerechnet, die des zweiten und dritten Kapitels auf einer HP 735.

Kapitel 1

Einheitengleichungen

Als eine Einheitengleichung bezeichnet man eine Gleichung der Gestalt

$$\alpha\, a + \beta\, b = 1, \tag{1-1}$$

deren Koeffizienten α, β Elemente eines algebraischen Zahlkörpers $\mathcal{K}$ mit $\alpha\beta \neq 0$ sind und deren Unbekannten a, b Einheiten aus $\mathrm{U}_{\mathcal{K}}$ sind. Unter dem Lösen einer solchen Einheitengleichung ist die Bestimmung aller der nach einem Satz von Siegel [49] endlich vielen Tupel $(a, b) \in \mathrm{U}_{\mathcal{K}} \times \mathrm{U}_{\mathcal{K}}$ zu verstehen, welche der Gleichung (1-1) genügen.

Einheitengleichungen sind ein nützliches Werkzeug beim Lösen diophantischer Gleichungen. So lassen sich das Lösen von Indexform- und Thue-Gleichungen sowie die Berechnung der ganzen Punkte auf superelliptischen Kurven auf das Lösen von Einheitengleichungen zurückführen [25, 47, 52]. Einschränkend muß hierzu allerdings gesagt werden, daß bei solchen Problemtransformationen die algebraischen Zahlkörper, welche den zu lösenden Einheitengleichungen dann zugrunde liegen, oftmals so hohen Grad besitzen, daß in der Praxis eben diese Einheitengleichungen nicht gelöst werden können.

Sei nun für den Rest des Kapitels $\mathcal{K}$ ein beliebiger, aber fest gewählter algebraischer Zahlkörper. Es bezeichne $r := r_1 + r_2 - 1$ den Einheitenrang von $\mathcal{K}$ und $w \in 2\,\mathbb{Z}$ die Anzahl der Elemente von $\mathrm{TU}_{\mathcal{K}}$. Ferner seien $\zeta \in \mathrm{TU}_{\mathcal{K}}$ ein fest gewählter Erzeuger von $\mathrm{TU}_{\mathcal{K}}$ und $\varepsilon_1, \ldots, \varepsilon_r$ ein fest gewähltes Grundeinheitensystem von $\mathrm{U}_{\mathcal{K}}$.

Beliebig, aber gleichfalls fest gewählt für den Rest des Kapitels seien $\alpha, \beta \in \mathcal{K}^{\times}$. Die Lösungsmenge der Einheitengleichung aus (1-1) ist dann gegeben durch

$$\mathfrak{L} := \{\, (a, b) \in \mathrm{U}_{\mathcal{K}} \times \mathrm{U}_{\mathcal{K}} \;\mid\; \alpha a + \beta b = 1 \,\}.$$

Für Einheitenrang $r = 0$, also $\mathrm{TU}_{\mathcal{K}} = \mathrm{U}_{\mathcal{K}}$, ist die Bestimmung von $\mathfrak{L}$ trivial. Für $r = 1$ kann $\mathfrak{L}$ leicht anhand des folgenden Lemmas berechnet werden.

Lemma 1.1
Seien $r = 1$ und ε eine Grundeinheit von $\mathfrak{o}_{\mathcal{K}}$ mit $|\varepsilon| = |\varepsilon^{(1)}| > 1$. Ist $(a, b) \in \mathfrak{L}$, so gilt stets eine der folgenden drei Beziehungen:

(1) $b = \xi\varepsilon^{\mu}$ *mit* $\xi \in \mathrm{TU}_{\mathcal{K}}$ *und* $\mu \in \mathbb{Z}$, *wobei*

$$\frac{\log|\frac{1}{2\beta}|}{\log|\varepsilon|} \leq \mu \leq \frac{\log|\frac{2}{\beta}|}{\log|\varepsilon|}, \tag{1-2}$$

(2) $b = \dfrac{1}{\beta + \alpha\xi\varepsilon^{\kappa}}$ *mit* $\xi \in \mathrm{TU}_{\mathcal{K}}$ *und* $\kappa \in \mathbb{Z}$, *wobei*

$$\frac{\log|\frac{\beta}{2\alpha}|}{\log|\varepsilon|} < \kappa < \frac{\log|\frac{3\beta}{2\alpha}|}{\log|\varepsilon|}, \tag{1-3}$$

(3) $b = \dfrac{1 + \alpha\xi\varepsilon^{\nu}}{\beta}$ *mit* $\xi \in \mathrm{TU}_{\mathcal{K}}$ *und* $\nu \in \mathbb{Z}$, *wobei*

$$\frac{\log|\frac{1}{2\alpha}|}{\log|\varepsilon|} < \nu < \frac{\log|\frac{3}{2\alpha}|}{\log|\varepsilon|}. \tag{1-4}$$

Beweis Seien $a = \xi_a\varepsilon^{\nu}, b = \xi_b\varepsilon^{\mu}$ mit $\nu, \mu \in \mathbb{Z}, \xi_{\mathcal{D}}, \xi \in \mathrm{TU}_{\mathcal{K}}$. Falls μ der Bedingung aus (1-2) genügt, so ist nichts zu zeigen. Angenommen, es gilt

$$\frac{\log|\frac{2}{\beta}|}{\log|\varepsilon|} < \mu. \tag{1-5}$$

Dann ist $\left|\dfrac{2}{\beta}\right| < |b|$, also $\left|\dfrac{1}{\beta b}\right| < \dfrac{1}{2}$, und aus

$$\frac{a}{b} = \frac{\beta}{\alpha}\left(\frac{1}{\beta b} - 1\right)$$

folgt

$$\left|\frac{\beta}{\alpha}\right|\left(1 - \left|\frac{1}{\beta b}\right|\right) \leq \left|\frac{a}{b}\right| \leq \left|\frac{\beta}{\alpha}\right|\left(1 + \left|\frac{1}{\beta b}\right|\right),$$

also

$$\frac{1}{2}\left|\frac{\beta}{\alpha}\right| < |\varepsilon|^{\nu-\mu} < \frac{3}{2}\left|\frac{\beta}{\alpha}\right|.$$

Damit erfüllt b die zweite Beziehung mit $\kappa = \nu - \mu$.

Analog zeigt man die Gültigkeit der dritten Beziehung, falls μ weder (1-2) noch (1-5) erfüllt. □

Ist der Einheitenrang r — wie im folgenden stets vorausgesetzt — größer als 1, so ist das Lösen der Einheitengleichung (1-1) weitaus schwieriger. Die explizite Bestimmung von $\mathfrak{L}$ ist in diesem Fall erst durch die sogenannte bakersche Methode möglich geworden, welche auch Grundlage für das in den nächsten Abschnitten vorgestellte Verfahren ist. Bevor wir mit dessen Darstellung beginnen, fixieren wir einige Notationen:

Ist $\varepsilon = \xi\varepsilon_1^{e_1}\cdots\varepsilon_r^{e_r} \in \mathrm{U}_{\mathcal{K}}$ ($\xi \in \mathrm{TU}_{\mathcal{K}}, e_1, \ldots, e_r \in \mathbb{Z}$), so definieren wir $\bar{\varepsilon} \in \mathbb{Z}^{\geq \mathcal{K}}$ durch

$$\bar{\varepsilon} := \max_{1 \leq i \leq r} |e_i|.$$

Weiter setzen wir

$$\mathfrak{L}_\alpha := \{a \in \mathrm{U}_\mathcal{K} \mid \exists\, b \in \mathrm{U}_\mathcal{K} : (a,b) \in \mathfrak{L} \wedge \bar{a} \le \bar{b}\}, \tag{1-6}$$

$$\mathfrak{L}_\beta := \{b \in \mathrm{U}_\mathcal{K} \mid \exists\, a \in \mathrm{U}_\mathcal{K} : (a,b) \in \mathfrak{L} \wedge \bar{b} \le \bar{a}\}. \tag{1-7}$$

Es gilt offensichtlich

$$\mathfrak{L} = \{(a,b) \in \mathfrak{L} \mid a \in \mathfrak{L}_\alpha\} \cup \{(a,b) \in \mathfrak{L} \mid b \in \mathfrak{L}_\beta\}.$$

Mit Log bezeichnen wir fortan den Hauptzweig des komplexen Logarithmus, also $\mathrm{Log}\, z = \log|z| + i \operatorname{Arg} z \;\forall\, z \in \mathbb{C}^\times$, wobei das Argument durch die Bedingung $\operatorname{Arg}(\mathbb{C}^\times) = (-\pi, \pi]$ normiert sei. Zu $x \in \mathbb{R}$ bezeichne $\lfloor x \rceil \in \mathbb{Z}$ die nächstgelegene ganze Zahl, für $z \in \mathbb{C}$ sei $\Re z$ der Real- und $\Im z$ der Imaginärteil von z.

1.1 Bakersche Methode

In diesem Abschnitt bestimmen wir eine obere Schranke $A = A(\mathcal{K}, \alpha, \beta) \in \mathbb{Z}^{\ge \nu}$ mit

$$\bar{a} \le A \qquad \forall\, a \in \mathfrak{L}_\alpha. \tag{1-8}$$

Analog kann $B \in \mathbb{Z}^{\ge \nu}$ berechnet werden, so daß $\bar{b} \le B \;\forall\, b \in \mathfrak{L}_\beta$.

Die Schreibweise $A = A(\mathcal{K}, \alpha, \beta)$ soll verdeutlichen, daß A von $\mathcal{K}$ sowie von α und β abhängt, wobei für $\mathcal{K}$ ein fest gewähltes Grundeinheitensystem vorausgesetzt ist.

Lemma 1.2
Es existiert $c_1 = c_1(\mathcal{K}) > 0$, so daß es zu jedem $\varepsilon \in \mathrm{U}_\mathcal{K}$ mindestens ein $\mu = \mu(\varepsilon) \in \{1, \ldots, r_1 + r_2\}$ gibt mit

$$\log\bigl|\varepsilon^{(\mu)}\bigr| \le -c_1 \bar{\varepsilon}. \tag{1-9}$$

Beweis Sei $\varepsilon = \xi \varepsilon_1^{e_1} \cdots \varepsilon_r^{e_r} \in \mathrm{U}_\mathcal{K}$ ($\xi \in \mathrm{TU}_\mathcal{K}$, $e_1, \ldots, e_r \in \mathbb{Z}$) beliebig. Wähle $J \in \{1, \ldots, r\}$ so, daß

$$\bigl|\log\bigl|\varepsilon^{(J)}\bigr|\bigr| = \max_{1 \le j \le r} \bigl|\log\bigl|\varepsilon^{(j)}\bigr|\bigr|.$$

Ferner definiere $L \in \mathrm{GL}(r, \mathbb{R})$ durch

$$L := \begin{pmatrix} \log\bigl|\varepsilon_1^{(1)}\bigr| & \ldots & \log\bigl|\varepsilon_r^{(1)}\bigr| \\ \vdots & & \vdots \\ \log\bigl|\varepsilon_1^{(r)}\bigr| & \ldots & \log\bigl|\varepsilon_r^{(r)}\bigr| \end{pmatrix}.$$

Dann gilt

$$L \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} \log\bigl|\varepsilon^{(1)}\bigr| \\ \vdots \\ \log\bigl|\varepsilon^{(r)}\bigr| \end{pmatrix},$$

und ist $c > 0$ die Zeilensummennorm von L^{-1}, so folgt

$$\bar{\varepsilon} \le c \bigl|\log\bigl|\varepsilon^{(J)}\bigr|\bigr|. \tag{1-10}$$

Setze $c_1 := \frac{1}{(n-1)c}$. Angenommen, es gilt $\log\left|\varepsilon^{(j)}\right| > -c_1\bar{\varepsilon}\ \forall\, j \in \{1,\dots,r_1+r_2\}$. Aus (1-10) erhalten wir wegen $\varepsilon \in \mathrm{U}_{\mathcal{K}}$ dann

$$\left|\log\left|\varepsilon^{(J)}\right|\right| \geq \frac{\bar{\varepsilon}}{c} = (n-1)c_1\bar{\varepsilon} > -\sum_{\substack{j=1\\ j\neq J}}^{n} \log\left|\varepsilon^{(j)}\right| = \log\left|\varepsilon^{(J)}\right|,$$

also $\log\left|\varepsilon^{(J)}\right| < 0$. Nach (1-10) ist somit

$$-\bar{\varepsilon} \geq c\log\left|\varepsilon^{(J)}\right| \geq \frac{1}{c_1}\log\left|\varepsilon^{(J)}\right|,$$

was im Widerspruch zur Annahme steht. □

Bemerkung 1.3
Für $\mathcal{K}$ total komplex ist schärfer $c_1 := \frac{1}{(n/2-1)c}$ im Beweis zu 1.2 möglich.

Lemma 1.4
Sei $a \in \mathfrak{L}_\alpha$ beliebig. Dann existieren $\mu = \mu(a) \in \{1,\dots,r_1+r_2\}$ und $c_{2,\mu} = c_2(\mathcal{K},\beta,\mu) > 0$ mit

$$\left|(\alpha a)^{(\mu)} - 1\right| \leq c_{2,\mu}\exp(-c_1\bar{a}). \tag{1-11}$$

Beweis Sei $b \in \mathrm{U}_{\mathcal{K}}$ mit $\alpha a + \beta b = 1$. Nach 1.2 existiert ein $\mu \in \{1,\dots,r_1+r_2\}$ mit $\log|b^{(\mu)}| \leq -c_1\bar{b}$. Setzen wir $c_{2,\mu} := \left|\beta^{(\mu)}\right|$, so folgt wegen $\bar{a} \leq \bar{b}$ sogleich

$$\left|(\alpha a)^{(\mu)} - 1\right| = \left|(\beta b)^{(\mu)}\right| \leq c_{2,\mu}\exp(-c_1\bar{a}). \qquad \square$$

Definieren wir für jedes $\mu \in \{1,\dots,r_1+r_2\}$ die Menge $\mathfrak{L}_{\alpha,\mu} \subseteq \mathfrak{L}_\alpha$ durch

$$\mathfrak{L}_{\alpha,\mu} := \{a \in \mathfrak{L}_\alpha \mid \left|(\alpha a)^{(\mu)} - 1\right| \leq c_{2,\mu}\exp(-c_1\bar{a})\},$$

so folgt aus 1.4 unmittelbar

$$\mathfrak{L}_\alpha = \mathfrak{L}_{\alpha,1} \cup \ldots \cup \mathfrak{L}_{\alpha,r_1+r_2}. \tag{1-12}$$

Sei nun $\mu \in \{1,\dots,r_1+r_2\}$ für den Rest dieses Abschnitts beliebig, aber fest vorgegeben. Ohne Einschränkung sei der Erzeuger ζ von $\mathrm{TU}_{\mathcal{K}}$ so gewählt, daß $2\pi i = w\,\mathrm{Log}\,\zeta^{(\mu)}$. Wir werden ein Resultat von Baker zu Linearformen in den Logarithmen algebraischer Zahlen einsetzen, um eine obere Schranke $A_{2,\mu}$ herzuleiten, so daß

$$\bar{a} \leq A_{2,\mu} \qquad \forall\, a \in \mathfrak{L}_{\alpha,\mu}. \tag{1-13}$$

Für unsere Zwecke reicht es, wenn wir uns der Einfachheit halber auf homogene Linearformen in den Logarithmen algebraischer Zahlen beschränken, deren Koeffizienten ganzzahlig sind. Eine solche Linearform ist ein Ausdruck

$$\Lambda = g_1\,\mathrm{Log}\,\gamma_1 + \cdots + g_k\,\mathrm{Log}\,\gamma_k$$

mit algebraischen Zahlen $\gamma_i \neq 0$ $(1 \leq i \leq k)$ und $g_1,\dots,g_k \in \mathbb{Z}$. Wir setzen $G := \max_{1\leq i\leq k}|g_i|$. Eines der Resultate Bakers besteht darin, eine nur von $\gamma_1,\dots,\gamma_k$

abhängige, effektiv berechenbare Konstante $C > 0$ anzugeben, so daß unter der Voraussetzung $\Lambda \neq 0$ die Abschätzung

$$0 < G^{-C} \leq |\Lambda| \tag{1-14}$$

erfüllt ist. Der ursprünglich von Baker angegebene Wert für die Konstante C in (1-14) wurde mehrfach verbessert. Für unsere Rechnungen verwendeten wir ein Ergebnis von Baker und Wüstholz [5] aus dem Jahre 1993, dessen Formulierung hier an die obige Situation angepaßt ist.

Satz 1.5 (Baker/Wüstholz)
Seien $g_1, \ldots, g_k, \gamma_1, \ldots, \gamma_k$ und G wie oben gegeben. Es sei $h(\gamma_i)$ die absolute logarithmische Höhe von γ_i $(1 \leq i \leq k)$, also

$$h(\gamma_i) = \frac{1}{d_i} \log \left(a_{i,0} \prod_{j=1}^{d_i} \max\left(1, |\gamma_i^{(j)}|\right) \right),$$

wobei $a_{i,0} t^{d_i} + a_{i,1} t^{d_i - 1} + \cdots + a_{i,d_i} \in \mathbb{Z}[\approx]$, $a_{i,0} > 0$, $\mathrm{ggT}(a_{i,0}, \ldots, a_{i,d_i}) = 1$, das Minimalpolynom von γ_i sei. Ferner seien $d \in \mathbb{N}$ und $h_i > 0$ $(1 \leq i \leq k)$ definiert über

$$\begin{aligned} d &:= [\,\mathbb{Q}(\gamma_{\aleph}, \ldots, \gamma_{\beth}) : \mathbb{Q}], \\ h_i &:= \max\left(h(\gamma_i), \frac{|\operatorname{Log} \gamma_i|}{d}, \frac{1}{d}\right). \end{aligned}$$

Gelten dann $\Lambda \neq 0$ und $G \geq 3$, so kann C in (1-14) gewählt werden als

$$C = 18\,(k+1)!\,k^{k+1}\,32^{k+2}\,d^{k+1}\log(2kd)\,h_1 \cdots h_k.$$

Für den Rest dieses Abschnitts fixieren wir ein beliebiges

$$a = \zeta^{a_0} \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \in \mathfrak{L}_\alpha \qquad (a_0 \in \{-\tfrac{w}{2}+1, \ldots, \tfrac{w}{2}\}, a_1, \ldots, a_r \in \mathbb{Z}). \tag{1-15}$$

Es sei $b \in \mathrm{U}_{\mathcal{K}}$ mit $(a, b) \in \mathfrak{L}$. Um (1-14) zur Bestimmung der oberen Schranke $A_{2,\mu}$ einzusetzen, benötigen wir zunächst eine geeignete Linearform in den Logarithmen algebraischer Zahlen. Eine solche erhalten wir aus

$$\Lambda_\mu := \operatorname{Log}(\alpha a)^{(\mu)} \neq 0 \tag{1-16}$$

durch Anwendung der Funktionalgleichung

$$\operatorname{Log}(z_1 \cdots z_m) = \operatorname{Log} z_1 + \cdots + \operatorname{Log} z_m + k(z_1, \ldots, z_m)\pi i \qquad \forall\, z_1, \ldots, z_m \in \mathbb{C}^\times,$$

wobei $k(z_1, \ldots, z_m) \in 2\,\mathbb{Z}$ mit $|k(z_1, \ldots, z_m)| \leq m$.

Aufgrund von $a_0 \in \{-\frac{w}{2}+1, \ldots, \frac{w}{2}\}$ existiert $a_{r+1} = a_{r+1}(\mathcal{K}, \alpha, \mu, a) \in 2\,\mathbb{Z}$ mit $|a_{r+1}| \leq 1 + \frac{w}{2} + r\bar{a}$, so daß

$$\Lambda_\mu = \operatorname{Log} \alpha^{(\mu)} + a_0 \operatorname{Log} \zeta^{(\mu)} + \sum_{i=1}^{r} a_i \operatorname{Log} \varepsilon_i^{(\mu)} + a_{r+1}\, i\pi.$$

Indem wir $a_0' := a_0 + \frac{w}{2}a_{r+1}$ setzen, können wir die Terme $a_0 \operatorname{Log}\zeta^{(\mu)}$ und $a_{r+1}\, i\pi$ zusammenfassen, also

$$\Lambda_\mu = \operatorname{Log}\alpha^{(\mu)} + a_0'\frac{2\pi i}{w} + \sum_{i=1}^{r} a_i \operatorname{Log}\varepsilon_i^{(\mu)}.$$

Wir setzen $\bar{\bar{a}} := \max(|a_0'|, \bar{a})$ und

$$A_{1,\mu} := \max\left(3, \frac{\log(2c_{2,\mu})}{c_1}\right). \tag{1-17}$$

Lemma 1.6
Es existieren $c_3 = c_3(\mathcal{K}), c_{4,\mu} = c_4(\mathcal{K}, \beta, \mu) > 0$, so daß unter der Voraussetzung $\bar{a} \geq A_{1,\mu}$ gilt:

$$|\Lambda_\mu| \leq \frac{3}{2}c_{2,\mu}\exp(-c_1\bar{a}) \leq c_{4,\mu}\exp(-c_3\bar{\bar{a}}). \tag{1-18}$$

Beweis Mittels Lemma 1.4 folgt aus $\bar{a} \geq A_{1,\mu}$ zunächst

$$\left|(\alpha a)^{(\mu)} - 1\right| \leq \frac{1}{2}. \tag{1-19}$$

Beachten wir

$$|\operatorname{Log}(1+z)| \leq |z| + \frac{1}{2}\sum_{k=2}^{\infty}|z|^k = |z| + \frac{1}{2}\frac{|z|^2}{1-|z|} \leq \frac{3}{2}|z| \qquad \forall\, z \in \mathbb{C}, |\digamma| \leq \frac{1}{2},$$

so erhalten wir aus (1-19) und 1.4 mit

$$|\Lambda_\mu| = \left|\operatorname{Log}(1 + ((\alpha a)^{(\mu)} - 1))\right| \leq \frac{3}{2}\left|(\alpha a)^{(\mu)} - 1\right| \leq \frac{3}{2}c_{2,\mu}\exp(-c_1\bar{a}) \tag{1-20}$$

die linke Ungleichung in (1-18). Es ist $\bar{\bar{a}} \leq \frac{w}{2}(2 + \frac{w}{2} + r\bar{a})$, also

$$-\bar{a} \leq \frac{1}{r}(2 + \frac{w}{2}) - \frac{2}{rw}\bar{\bar{a}}.$$

Hieraus ergibt sich die rechte Ungleichung in (1-18), indem c_3 und $c_{4,\mu}$ definiert werden als

$$c_3 := c_1\frac{2}{rw}, \qquad c_{4,\mu} := \frac{3}{2}c_{2,\mu}\exp\left(\frac{c_1}{r}(2 + \frac{w}{2})\right). \qquad \square$$

Aus der Gegenüberstellung der unteren Schranke für $|\Lambda_\mu|$ aus (1-14) und der oberen Schranke in (1-18) erhalten wir unter der Voraussetzung $\bar{a} \geq A_{1,\mu}$ die Abschätzung

$$\bar{\bar{a}}^{-C} \leq |\Lambda_\mu| \leq c_{4,\mu}\exp(-c_3\bar{\bar{a}}), \tag{1-21}$$

womit implizit eine obere Schranke $A_{3,\mu}$ für $\bar{\bar{a}}$ gegeben ist. $A_{2,\mu} := \max(A_{1,\mu}, A_{3,\mu})$ erfüllt dann (1-13), und aufgrund von (1-12) kann A in (1-8) als

$$A := \max_{1 \leq \mu \leq r_1+r_2} \lfloor A_{2,\mu} \rfloor \tag{1-22}$$

gewählt werden.

Wiewohl mit der Bestimmung von oberen Schranken für die Exponenten im Prinzip alle Lösungen der Einheitengleichung (1-1) durch einfaches Ausprobieren berechnet werden können, so sind doch diese Schranken viel zu groß, um ein solches Ausprobieren in vertretbarer Zeit durchzuführen. Dies mag das folgende, in den nächsten Abschnitten fortgesetzte Beispiel illustrieren, dem wir eine Bemerkung voranstellen.

Bemerkung 1.7
Ist $\mu \in \{1,\dots,r_1\}$, so können wir zur Herleitung der oberen Schranke $A_{2,\mu}$ alternativ die reelle Linearform

$$\Lambda'_\mu = \log\left|(\alpha a)^{(\mu)}\right| = \log\left|\alpha^{(\mu)}\right| + \sum_{i=1}^{r} a_i \log\left|\varepsilon_i^{(\mu)}\right| \tag{1-23}$$

verwenden. Unter den Voraussetzungen $\bar{a} \geq A_{1,\mu}$ und $\alpha\, a \neq -1$ erhält man analog zum Beweis von 1.6 in Verbindung mit (1-14) die Abschätzung

$$\bar{a}^{-C} \leq |\Lambda'_\mu| \leq \frac{3}{2} c_{2,\mu} \exp(-c_1 \bar{a}). \tag{1-24}$$

In der Praxis liefert Λ'_μ eine etwas kleinere Schranke als Λ_μ, da einerseits die Anzahl der Summanden in Λ'_μ um eins kleiner ist und wir andererseits aus Λ'_μ direkt eine Schranke für $A_{2,\mu}$ bekommen, während uns Λ_μ nur eine Abschätzung für die abgeleitete Größe $A_{3,\mu}$ bietet. Ist $\mu \in \{r_1+1,\dots,r_1+r_2\}$, so kann Λ'_μ nicht zur Herleitung einer oberen Schranke $A_{3,\mu}$ verwendet werden, da a priori unklar ist, ob nicht unendlich viele $a \in \mathfrak{L}_\alpha$ existieren mit $\left|(\alpha a)^{(\mu)}\right| = 1$.

Beispiel 1.8
Für die primitive 19-te Einheitswurzel $\zeta_{19} = \exp\frac{2\pi i}{19}$ setzen wir $\theta := \zeta_{19} + \zeta_{19}^{-1}$. Dann ist $\mathcal{K} = \mathbb{Q}(\theta)$ der maximale reelle Teilkörper von $\mathbb{Q}(\zeta_{19})$ mit $[\mathcal{K}:\mathbb{Q}] = 9$, $r = 8$ und $\mathfrak{o}_\mathcal{K} = \mathbb{Z}[\theta]$. Die Konjugierten von θ seien numeriert als $\theta^{(i)} = 2\cos\frac{2\pi i}{19}$ $(1 \leq i \leq 9)$, und ein Grundeinheitensystem in $\mathfrak{o}_\mathcal{K}$ sei gegeben durch

$$\varepsilon_1 = 1 - 4\,\theta - 10\,\theta^2 + 10\,\theta^3 + 15\,\theta^4 - 6\,\theta^5 - 7\,\theta^6 + \theta^7 + \theta^8,$$

$$\varepsilon_2 = 3\,\theta - \theta^4, \quad \varepsilon_3 = 1 - 2\,\theta - 3\,\theta^2 + \theta^3 + \theta^4,$$

$$\varepsilon_4 = 2 - 9\,\theta^2 + 6\,\theta^4 - \theta^6, \quad \varepsilon_5 = \theta,$$

$$\varepsilon_6 = 2 - \theta^2, \quad \varepsilon_7 = 2 - 4\,\theta^2 + \theta^4,$$

$$\varepsilon_8 = -5\,\theta + 5\,\theta^2 + 10\,\theta^3 - 5\,\theta^4 - 6\,\theta^5 + \theta^6 + \theta^7.$$

Wir wollen alle Einheiten $\varepsilon \in \mathrm{U}_\mathcal{K}$ bestimmen, für welche auch jeweils $1-\varepsilon$ eine Einheit aus $\mathrm{U}_\mathcal{K}$ ist. Dazu genügt es offensichtlich, in $\mathfrak{o}_\mathcal{K}$ die Einheitengleichung

$$1 \cdot a + 1 \cdot b = 1 \tag{1-25}$$

mit Koeffizienten $\alpha = 1 = \beta$ zu lösen.

Aus der bakerschen Methode erhalten wir bei Verwendung der Linearform Λ'_μ aus 1.7 über $A_{2,\mu} = 10^{38}$ $(1 \leq \mu \leq 9)$ die obere Exponentenschranke $A = 10^{38}$ (zur Bestimmung von $A_{2,\mu}$ haben wir jeweils das minimale $x \in \mathbb{N}$ bestimmt, so daß (1-24) für $\bar{a} = 10^x$ nicht erfüllt ist). Wegen $\alpha = \beta$ ist natürlich ebenso $B = 10^{38}$. Die Rechenzeit zur Ermittlung von A betrug weniger als eine Sekunde.

1.2 Reduktion der oberen Exponentenschranken

Der zweite Schritt beim Lösen der Einheitengleichung (1-1) besteht darin, die oberen Exponentenschranken A und B *deutlich* zu reduzieren. Hierzu verwenden wir die im nächsten Lemma enthaltene Reduktionsmethode, welche im wesentlichen dem Buch „Algorithms for diophantine equations“ von de Weger [58] entnommen ist, ergänzt um Überlegungen aus [50]. Wir formulieren das Vorgehen nur für die Reduktion von A, zur Reduktion von B kann analog verfahren werden.

Lemma 1.9
Zu beliebigem $\mu \in \{1, \ldots, r_1 + r_2\}$ sei $K \in \mathbb{N}$ gegeben, so daß

$$\begin{vmatrix} 0 & \lfloor K \Re \operatorname{Log} \varepsilon_1^{(\mu)} \rceil \\ \lfloor K \frac{2\pi}{w} \rceil & \lfloor K \Im \operatorname{Log} \varepsilon_1^{(\mu)} \rceil \end{vmatrix} \neq 0, \tag{1-26}$$

und es sei $\Gamma = \Gamma_{\mu,K} \subset \mathbb{R}^{\nu+\kappa}$ das Gitter, welches von den Spalten der Matrix

$$\begin{pmatrix} 0 & \lfloor K \Re \operatorname{Log} \varepsilon_1^{(\mu)} \rceil & \lfloor K \Re \operatorname{Log} \varepsilon_2^{(\mu)} \rceil & \ldots & \lfloor K \Re \operatorname{Log} \varepsilon_r^{(\mu)} \rceil \\ \lfloor K \frac{2\pi}{w} \rceil & \lfloor K \Im \operatorname{Log} \varepsilon_1^{(\mu)} \rceil & \lfloor K \Im \operatorname{Log} \varepsilon_2^{(\mu)} \rceil & \ldots & \lfloor K \Im \operatorname{Log} \varepsilon_r^{(\mu)} \rceil \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & & 1 \end{pmatrix}. \tag{1-27}$$

erzeugt wird. Ferner sei $\tilde{z}_0, \ldots, \tilde{z}_r$ eine LLL-reduzierte Basis [29] von Γ.

(1) Sei $\alpha \neq 1$ in (1-1). Es sei $z_\alpha \in \mathbb{Z}^{\nu+\kappa}$ definiert durch

$$z_\alpha = \begin{pmatrix} \lfloor K \Re \operatorname{Log} \alpha^{(\mu)} \rceil \\ \lfloor K \Im \operatorname{Log} \alpha^{(\mu)} \rceil \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

und z_α habe die Darstellung

$$z_\alpha = \sum_{i=0}^{r} \alpha_i \tilde{z}_i \qquad (\alpha_0, \ldots, \alpha_r \in \mathbb{Q}),$$

wobei $j \in \{0, \ldots, r\}$ mit $\alpha_j \notin \mathbb{Z}$ existiere. Ist dieser Index j maximal gewählt, und ist ferner

$$\delta := |\alpha_j - \lfloor \alpha_j \rceil| \cdot 2^{-\frac{r}{2}} \|\tilde{z}_0\|_2 - \sqrt{2}\,(1 + A_{3,\mu} + rA_{2,\mu}) > 0, \tag{1-28}$$

so gelten für jedes $a \in \mathfrak{L}_{\alpha,\mu}$ mit $\bar{a} \geq A_{1,\mu}$ die Abschätzungen

$$\bar{a} \leq \frac{1}{c_1} \log\left(\frac{3Kc_{2,\mu}}{2\delta}\right), \tag{1-29}$$

$$\bar{\bar{a}} \leq \frac{1}{c_3} \log\left(\frac{Kc_{4,\mu}}{\delta}\right). \tag{1-30}$$

(2) Sei $\alpha = 1$. Ist

$$\delta := 2^{-\frac{r}{2}}\|\tilde{z}_0\|_2 - \sqrt{2}\,(A_{3,\mu} + rA_{2,\mu}) > 0, \tag{1-31}$$

so gelten für jedes $a \in \mathfrak{L}_{\alpha,\mu}$ mit $\bar{a} \geq A_{1,\mu}$ die Abschätzungen in (1-29) und (1-30).

Beweis Wir beweisen zuerst die Aussage (1). Sei also $\alpha \neq 1$, und seien $z_0, \ldots, z_r$ die Spaltenvektoren der Matrix aus (1-27). Wir definieren $z'_\alpha, z'_0, z'_i \in \mathbb{R}^{\diagdown+\nVdash}$ ($\nVdash \leq \beth \leq \diagdown$) durch

$$z'_\alpha = \begin{pmatrix} K\Re \operatorname{Log} \alpha^{(\mu)} \\ K\Im \operatorname{Log} \alpha^{(\mu)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad z'_0 = \begin{pmatrix} 0 \\ K\frac{2\pi}{w} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad z'_i = \begin{pmatrix} K\Re \operatorname{Log} \varepsilon_i^{(\mu)} \\ K\Im \operatorname{Log} \varepsilon_i^{(\mu)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Sei $a \in \mathfrak{L}_{\alpha,\mu}$ beliebig wie in (1-15) gegeben mit $\bar{a} \geq A_{1,\mu}$. Einerseits ist dann

$$\begin{aligned} \min_{x\in\Gamma} \|z_\alpha - x\|_2 &\leq \|z_\alpha + a'_0 z_0 + a_1 z_1 + \cdots + a_r z_r\|_2 \\ &\leq \|z_\alpha - z'_\alpha\|_2 + |a'_0| \cdot \|z_0 - z'_0\|_2 \\ &\qquad + \sum_{i=1}^{r} |a_i| \cdot \|z_i - z'_i\|_2 + K|\Lambda_\mu| \\ &\leq \sqrt{2}\big(1 + A_{3,\mu} + rA_{2,\mu}\big) + \tfrac{3}{2}Kc_{2,\mu}\exp(-c_1\bar{a}) \qquad (1\text{-}32) \\ &\leq \sqrt{2}\big(1 + A_{3,\mu} + rA_{2,\mu}\big) + Kc_{4,\mu}\exp(-c_3\bar{\bar{a}}), \qquad (1\text{-}33) \end{aligned}$$

andererseits gilt nach [58, Lemma 3.5] die Abschätzung

$$|\alpha_j - \lfloor \alpha_j \rceil| \;\; 2^{-\frac{r}{2}}\|\tilde{z}_0\|_2 \leq \min_{x\in\Gamma} \|z_\alpha - x\|_2. \tag{1-34}$$

Fügen wir (1-28), (1-32) und (1-34) zusammen, so folgt

$$\delta \leq Kc_{2,\mu}\exp(-c_1\bar{a}),$$

womit (1-29) gezeigt ist. Zum Beweis von (1-30) kombiniert man entsprechend (1-28), (1-33) und (1-34).

Aussage (2), also $\alpha = 1$, zeigt man analog, wobei man anstatt (1-34) die nach [58, Lemma 3.4] gültige Abschätzung $2^{-r/2}\|\tilde{z}_0\|_2 \leq \|x\|_2 \;\forall\; x \in \Gamma,\; x \neq 0$, verwendet. □

Wir erläutern kurz, wie anhand von 1.9 die obere Schranke A reduziert werden kann. Sei dazu $\mu \in \{1, \ldots, r_1 + r_2\}$ beliebig, aber fest vorgegeben. Zur Verwendung von 1.9 benötigen wir zunächst ein geeignetes $K \in \mathbb{N}$. Aufgrund praktischer Erfahrung wählen wir $K = A_{2,\mu}^{r+1}$ (siehe auch [58, Kapitel 3]). Ist dann die Bedingung (1-26) erfüllt, so bestimmen wir eine LLL-reduzierte Basis des Gitters $\Gamma_{\mu,K}$ und prüfen anschließend, ob δ der Bedingung (1-28) bzw. (1-31) genügt. Sofern letzteres der Fall ist, können wir $A_{2,\mu}$ und $A_{3,\mu}$ anhand von (1-29) und (1-30) ersetzen durch

$$\begin{aligned} A_{2,\mu} &\leftarrow \min\left(A_{2,\mu}, \left\lfloor \frac{1}{c_1}\log\left(\frac{3Kc_{2,\mu}}{2\delta}\right)\right\rfloor\right), \qquad (1\text{-}35) \\ A_{3,\mu} &\leftarrow \min\left(A_{3,\mu}, \left\lfloor \frac{1}{c_3}\log\left(\frac{Kc_{4,\mu}}{\delta}\right)\right\rfloor\right). \end{aligned}$$

Diesen Reduktionsvorgang wiederholen wir solange, bis durch die Ersetzung in (1-35) keine weitere Verringerung von $A_{2,\mu}$ mehr eintritt. Nach Abschluß des Reduktionsvorgangs setzen wir dann

$$A := \max_{1 \le \mu \le r_1+r_2} \max(A_{1,\mu}, A_{2,\mu}).$$

Bei diesem Reduktionsverfahren ist nicht gesichert, ob mit ihm überhaupt eine Reduktion der Schranken $A_{2,\mu}$ erreicht werden kann. Gleichwohl hat das Verfahren in der Praxis bei allen gerechneten Beispielen die gewünschte deutliche Reduktion der Ausgangsschranken bewirkt.

Bemerkung 1.10

1. *Die obere Schranke $A_{3,\mu}$ muß während des gesamten Reduktionsverfahrens mitverwaltet werden, um mit ihr den Koeffizienten a'_0 in der Linearform abzuschätzen.*

2. *Das Reduktionsverfahren besteht im wesentlichen daraus, mittels LLL-Reduktion eine untere Schranke für*

$$\min_{x \in \Gamma} \|z_\alpha - x\|_2 \qquad \text{bzw.} \qquad \min_{\substack{x \in \Gamma \\ x \neq 0}} \|x\|_2 \tag{1-36}$$

   zu erhalten (siehe (1-34)). Ist diese untere Schranke im Hinblick auf (1-28) bzw. (1-31) groß genug, so kann die obere Exponentenschranke anhand von (1-29) reduziert werden. Die Grundidee des Verfahrens ist dabei der Zusammenhang, daß die untere Schranke für (1-36) wegen (1-32) umso kleiner sein muß, je größer $\bar{a}$ für ein $a \in \mathfrak{L}_\alpha$ ist.

   Ist $\alpha = \xi \varepsilon^{a_1} \cdots \varepsilon_r^{a_r} \in \mathrm{U}_\mathcal{K}$ ($\xi \in \mathrm{TU}_\mathcal{K}, a_1, \ldots, a_r \in \mathbb{Z}$) mit $\alpha \neq 1$, so funktioniert diese Kopplung in der Praxis nicht, da man leicht zeigt, daß für ein passendes $\tilde{a}_0 \in \mathbb{Z}$ der Abstand

$$\|z_\alpha - a_1 z_1 - \cdots - a_r z_r + \tilde{a}_0 z_0\|_2$$

   durch einen von K unabhängigen Ausdruck in $\bar{\alpha}$ nach oben abgeschätzt werden kann. Dieses Problem läßt sich dadurch umgehen, daß man im Falle $\alpha \in \mathrm{U}_\mathcal{K} \setminus \{1\}$ die Einheitengleichung $a + \beta b = 1$ betrachtet, deren Lösungen man leicht in Lösungen der Ausgangsgleichung $\alpha a + \beta b = 1$ transformiert.

3. *Ist bei Wahl von $K = A_{2,\mu}^{r+1}$ die zur Reduktion notwendige Bedingung (1-28) bzw. (1-31) nicht erfüllt, so ersetzt man K durch einen größeren Wert und prüft nach erneuter LLL-Reduktion wiederum die Bedingung aus (1-28) bzw. (1-31). Iteriert man dieses Vorgehen, so hat sich in der Praxis gezeigt, daß für ein genügend großes K stets (1-28) bzw. (1-31) erfüllt werden kann. Sofern dann aus einem solchen K keine kleinere obere Schranke für $A_{2,\mu}$ in (1-35) resultiert, bricht man die Reduktion ab.*

4. *Für $\mu \in \{1, \ldots, r_1\}$ empfiehlt es sich wegen der in 1.7 genannten Gründe, zur Reduktion der oberen Exponentenschranke $A_{2,\mu}$ die Linearform Λ'_μ aus (1-23) einzusetzen. Lemma 1.9 kann leicht dahingehend angepaßt werden.*

Beispiel 1.11 (Fortsetzung von 1.8)
Setzen wir 1.9 zur Reduktion von $A_{2,1}$ *ein, so bekommen wir durch wiederholte Anwendung von 1.9 schrittweise die Werte* 14739, 2367, 2037 *und* 2031 *als neue obere Schranken für* $A_{2,1}$, *wobei ein erneuter Reduktionsschritt keine weitere Verringerung der Schranke* $A_{2,1} = 2031$ *bewirkt. Für* $A_{2,2}, \ldots, A_{2,9}$ *liefert die wiederholte Reduktion mit 1.9 die neuen Schranken*

$$A_{2,2} = 2026, \quad A_{2,3} = 2035, \quad A_{2,4} = 2076, \quad A_{2,5} = 2056,$$

$$A_{2,6} = 2028, \quad A_{2,7} = 2027, \quad A_{2,8} = 2029, \quad A_{2,9} = 2062.$$

Somit erhalten wir insgesamt die neue Schranke $A = 2076 = B$. *Die Rechenzeit zur Reduktion der Schranken betrug 305s.*

1.3 Auszählen der Lösungen

Nach Herleitung und Reduktion der oberen Exponentenschranken in den beiden vorangehenden Abschnitten verbleibt als dritter und letzter Schritt die explizite Berechnung aller Lösungen der Einheitengleichung, also die Bestimmung von $\mathfrak{L}$. Dieser letzte Schritt ist der weitaus aufwendigste beim Lösen der Einheitengleichung. Ein naives systematisches Ausprobieren aller für $a \in \mathfrak{L}_\alpha$ und $b \in \mathfrak{L}_\beta$ in Frage kommenden Einheiten stößt bei Einheitenrang $r \geq 3$ schnell an die Grenze der praktischen Durchführbarkeit, da $w(2A+1)^r$ Möglichkeiten für $a \in \mathfrak{L}_\alpha$ und analog $w(2B+1)^r$ Möglichkeiten für $b \in \mathfrak{L}_\beta$ zu berücksichtigen sind. Als in der Praxis wesentlich effizienter erweist sich das folgende Verfahren, welches auf Methoden aus der Geometrie der Zahlen basiert.

Dieser Abschnitt ist in drei Teile untergliedert. Im ersten Teil werden einige technische Hilfsmittel bereitgestellt. Danach beschäftigen wir uns im zweiten Teil mit der speziellen Situation, daß die Koeffizienten α, β der Einheitengleichung (1-1) gegeben sind als $\alpha = 1 = \beta$. Gegenstand des dritten Teils ist abschließend die allgemeine Einheitengleichung mit $\alpha, \beta \in \mathcal{K}^\times$ beliebig.

1.3.1 Technische Hilfsmittel

Wir fixieren einige Notationen. Für $s > 1$ setzen wir

$$\langle\langle s \rangle\rangle := \left\{ (x_1, \ldots, x_{r_1+r_2})^t \in \mathbb{R}^{r_1+r_2} \;\middle|\; \frac{1}{s} \leq x_i \leq s \;(1 \leq i \leq r_1 + r_2) \right\} \tag{1-37}$$

Wir sagen, daß $\gamma \in \mathcal{K}$ in $M \subseteq \mathbb{R}^{r_1+r_2}$ liegt, und schreiben dafür kurz $\gamma \in M$, sofern

$$(|\gamma^{(1)}|, \ldots, |\gamma^{(r_1+r_2)}|)^t \in M.$$

Sind $j \in \{1, \ldots, r_1 + r_2\}$, $\rho \in \mathcal{K}^\times$, $\delta \in (0,1)$ und $s > 1$ gegeben, so sei $U_j(\rho, \delta, s) \subseteq \mathrm{U}_\mathcal{K}$ definiert als

$$U_j(\rho, \delta, s) := \left\{ \varepsilon \in \mathrm{U}_\mathcal{K} \mid \left|(\rho\varepsilon)^{(j)} - 1\right| < \delta \wedge \rho\varepsilon \in \langle\langle s \rangle\rangle \right\}. \tag{1-38}$$

Zur späteren Verwendung notieren wir ein einfaches Lemma.

Lemma 1.12
Sei $\mathcal{K}$ normal über $\mathbb{Q}$ (also $r_1 = 0$ oder $r_2 = 0$), seien $\rho \in \mathbb{Q}$, $\delta \in (0,1)$ sowie $s > 1$. Dann operiert die Galoisgruppe von $\mathcal{K}/\mathbb{Q}$ transitiv auf $\{U_j(\rho,\delta,s) \mid 1 \le j \le r_1+r_2\}$.

Die Mengen $U_j(\rho,\delta,s)$ aus (1-38) werden die entscheidende Rolle bei der expliziten Berechnung aller Lösungen der Einheitengleichung (1-1) spielen. Wir beschreiben im folgenden, wie die Elemente dieser Mengen bestimmt werden können. Hierzu benötigen wir ein technisches Lemma.

Lemma 1.13
Seien $\delta \in (0,1)$, $s > 1$ und $z \in \mathbb{C}$.

(1) Ist $|z-1| \le \delta$, so gilt $|\log|z|| \le \log \frac{1}{1-\delta}$.

(2) Ist $|z| \in [\frac{1}{s}, s]$, so gilt $|\log|z|| \le \log s$.

(3) Ist $|z-1| \le \delta$, so gilt $|\operatorname{Arg} z| \le \arccos\sqrt{1-\delta^2}$.

Beweis Ist $z \in \mathbb{C}$ mit $|z-1| \le \delta$, so folgt aus $1-\delta \le |z| \le 1+\delta$ wegen

$$|\log|z|| \le \log\left(\max\left(\frac{1}{1-\delta}, 1+\delta\right)\right) = \log\frac{1}{1-\delta}$$

die erste Aussage des Lemmas. Die zweite Aussage ist trivial. Zum Beweis von (3) sei $z = x+iy \in \mathbb{C}$ mit $|z-1| \le \delta$. Setzen wir $\sigma := |z-1|^2 \in (0,1)$, und definieren wir weiter $h : [1-\sqrt{\sigma}, 1+\sqrt{\sigma}\,] \to \mathbb{R}$ durch

$$h(\eta) := \frac{\eta}{\sqrt{\sigma+2\eta-1}},$$

so ist

$$|\operatorname{Arg} z| = \arccos\frac{x}{\sqrt{x^2+y^2}} = \arccos h(x). \tag{1-39}$$

Aufgrund von

$$h'(\eta) = \frac{\eta-(1-\sigma)}{(\sigma+2\eta-1)^{3/2}},$$

$$h(1-\sqrt{\sigma}) = 1, \quad h(1-\sigma) = \sqrt{1-\sigma} < 1, \quad h(1+\sqrt{\sigma}) = 1$$

besitzt h an der Stelle $\eta = 1-\sigma$ ein globales Minimum. Aus (1-39) folgt also

$$|\operatorname{Arg} z| \le \arccos h(1-\sigma) = \arccos\sqrt{1-\sigma} \le \arccos\sqrt{1-\delta^2}. \qquad \square$$

Seien j, ρ, δ, s wie bei der Definition von $U_j(\rho,\delta,s)$ in (1-38) gegeben. Definiere $\lambda_1, \ldots, \lambda_{r_1+r_2+1} > 0$ durch

$$\lambda_i := \frac{1}{\log s} \qquad (1 \le i \le r_1+r_2, i \ne j),$$

$$\lambda_j := \frac{1}{\log\frac{1}{1-\delta}}, \qquad \lambda_{r_1+r_2+1} := \frac{1}{\arccos\sqrt{1-\delta^2}},$$

und damit weiter die Abbildung

$$L_\lambda : \mathcal{K}^\times \to \mathbb{R}^{r_1+r_2+1} : \varepsilon \mapsto \begin{pmatrix} \lambda_1 \log|x^{(1)}| \\ \vdots \\ \lambda_{r_1+r_2} \log|x^{(r_1+r_2)}| \\ \lambda_{r_1+r_2+1} \operatorname{Arg} x^{(j)} \end{pmatrix}. \tag{1-40}$$

Gemäß 1.13 gilt für jedes $\varepsilon \in U_j(\rho, \delta, s)$ die Abschätzung

$$\|L_\lambda(\rho\varepsilon)\|_2^2 = \sum_{i=1}^{r_1+r_2} \lambda_i^2 \log^2\left|(\rho\varepsilon)^{(i)}\right| + \lambda_{r_1+r_2+1}^2 \operatorname{Arg}^2(\rho\varepsilon)^{(j)} \le r_1 + r_2 + 1. \tag{1-41}$$

Es bezeichne Λ_λ das $(r+1)$-dimensionale Gitter im $\mathbb{R}^{r_1+r_2+1}$, welches von den Vektoren $v = (0, \ldots, 0, \frac{2\pi}{w})^t$ und $L_\lambda(\varepsilon_1), \ldots, L_\lambda(\varepsilon_r)$ aufgespannt wird. Wir setzen

$$V(\rho, \lambda) := \left\{ x \in \Lambda_\lambda \mid \|x - L_\lambda(\tfrac{1}{\rho})\|_2^2 \le r_1 + r_2 + 1 \right\}. \tag{1-42}$$

Ist $\varepsilon = \xi\varepsilon^{e_1} \cdots \varepsilon^{e_r} \in U_j(\rho, \delta, s)$, so existiert $e_0 \in \mathbb{Z}$ mit

$$L_\lambda(\rho\varepsilon) = \underbrace{e_0\, v + e_1\, L_\lambda(\varepsilon_1) + \cdots + e_r L_\lambda(\varepsilon_r)}_{=:\, e \in \Lambda_\lambda} + L_\lambda(\rho).$$

Wegen $L_\lambda(\rho) = -L_\lambda(\frac{1}{\rho})$ gilt nach (1-41) also $e \in V(\rho, \lambda)$. Damit erhält man alle Einheiten aus $U_j(\rho, \delta, s)$ leicht aus den Elementen der Menge $V(\rho, \lambda)$. Diese entsprechen gerade den Gitterpunkten von Λ_λ, welche innerhalb eines Ellipsoids mit Mittelpunkt $L_\lambda(\frac{1}{\rho})$ liegen. Daher ist $V(\rho, \lambda)$ endlich und kann mit dem Auszählalgorithmus von Fincke und Pohst [14, 45] bestimmt werden.

Bemerkung 1.14
Ist $\mathrm{N}(\rho) \neq \pm 1$, *so berechnet man zur Anwendung des Auszählalgorithmus von Fincke und Pohst zunächst die orthogonale Projektion* p *des Punktes* $L_\lambda(\frac{1}{\rho})$ *in den von* Λ_λ *erzeugten* $(r+1)$*-dimensionalen Unterraum des* $\mathbb{R}^{r_1+r_2+1}$ *und bestimmt anschließend mit dem Auszählalgorithmus alle Gitterpunkte* $x \in \Lambda_\lambda$ *mit* $\|x - p\|_2^2 \le r_1 + r_2 + 1$. *Gilt* $\|L_\lambda(\frac{1}{\rho}) - p\|_2^2 > r_1 + r_2 + 1$, *so ist natürlich* $V(\rho, \lambda) = \emptyset$, *also auch* $U_j(\rho, \delta, s) = \emptyset$.

Bemerkung 1.15
Für jedes $\varepsilon \in U_j(\rho, \delta, s)$ *gilt nach 1.13 analog zu (1-41) die Abschätzung*

$$\sum_{i=1}^{r_1+r_2} \lambda_i^2 \log^2\left|(\rho\varepsilon)^{(i)}\right| \le r_1 + r_2.$$

Somit kann der Bestimmung von $U_j(\rho, \delta, s)$ *anstatt* Λ_λ *aus (1-40) in gleicher Weise das* r*-dimensionale Gitter* $\Lambda'_\lambda \subseteq \mathbb{R}^{r_1+r_2}$ *zugrunde gelegt werden, welches erzeugt wird von den Vektoren*

$$\begin{pmatrix} \lambda_1 \log|\varepsilon_i^{(1)}| \\ \vdots \\ \lambda_{r_1+r_2} \log|\varepsilon_i^{(r_1+r_2)}| \end{pmatrix} \qquad (1 \le i \le r).$$

Wir haben Λ_λ aus (1-40) betrachtet, weil für ein $j \in \{r_1+1,\ldots,r_1+r_2\}$ das Gewicht $\lambda_{r_1+r_2}$ „groß" ist, wodurch in der Praxis die Anzahl der zur Bestimmung von $U_j(\rho,\delta,s)$ auszuzählenden Elemente reduziert wird (für $j \in \{1,\ldots,r_1\}$ ergibt sich dagegen kein Vorteil aus der Verwendung von Λ_λ gegenüber Λ'_λ).

Bevor wir uns in den nächsten beiden Teilen der expliziten Berechnung aller Lösungen der Einheitengleichung zuwenden, vermerken wir, daß für $s > 1$ alle Einheiten ε in $\langle\langle s\rangle\rangle$ mit dem Auszählalgorithmus von Fincke und Pohst berechnet werden können, denn für jedes solche ε gilt

$$\sum_{i=1}^{r_1+r_2} \frac{1}{\log^2 s} \log\left|\varepsilon^{(i)}\right|^2 \leq r_1 + r_2. \tag{1-43}$$

1.3.2 Ausnahmeeinheiten

Wie bereits angekündigt, werden wir bei der expliziten Berechnung aller Lösungen der Einheitengleichung (1-1) zunächst den Spezialfall betrachten, daß die Koeffizienten gegeben sind durch $\alpha = 1 = \beta$. Der Grund für die gesonderte Behandlung dieses Spezialfalls ist einerseits die Tatsache, daß das Lösungsverfahren für diesen Fall einfacher und auch effizienter ist als im allgemeinen Fall. Auf der anderen Seite ist der Fall $\alpha = 1 = \beta$ von besonderem Interesse, wie wir später kurz erläutern werden. Wir definieren zunächst den auf Nagell zurückgehenden Begriff der „Ausnahmeeinheit".

Definition 1.16
Eine Einheit $\varepsilon \in \mathrm{U}_\mathcal{K}$ heißt Ausnahmeeinheit von $\mathcal{K}$, falls $1-\varepsilon$ ebenso eine Einheit aus $\mathrm{U}_\mathcal{K}$ ist.

Die Menge der Ausnahmeeinheiten von $\mathcal{K}$ bezeichnen wir mit $\mathrm{X}_\mathcal{K}$. Ist $\varepsilon \in \mathrm{X}_\mathcal{K}$, so nennen wir

$$\Omega(\varepsilon) := \left\{\varepsilon, \frac{1}{\varepsilon}, 1-\varepsilon, 1-\frac{1}{\varepsilon}, \frac{1}{1-\varepsilon}, \frac{\varepsilon}{\varepsilon-1}\right\}$$

den Orbit von ε. Für eine Ausnahmeeinheit $\varepsilon \in \mathrm{X}_\mathcal{K}$ gilt stets $\Omega(\varepsilon) \subseteq \mathrm{X}_\mathcal{K}$, und es ist

$$|\Omega(\varepsilon)| = \begin{cases} 2 & : \ \varepsilon \text{ ist eine primitive dritte Einheitswurzel} \\ 6 & : \ \text{sonst} \end{cases}.$$

Die Bestimmung von $\mathrm{X}_\mathcal{K}$ ist äquivalent zum Lösen der Einheitengleichung $a+b=1$. Zu dieser Einheitengleichung seien obere Exponentenschranken $A = B$ gegeben, wie wir sie im ersten und zweiten Abschnitt bestimmt haben. Wir setzen

$$\bar{S} := \max_{1\leq i\leq r_1+r_2} \exp\left(A \sum_{j=1}^{r} \left|\log\left|\varepsilon_j^{(i)}\right|\right|\right). \tag{1-44}$$

Für jedes $\varepsilon \in \mathrm{X}_\mathcal{K}$ gilt $\varepsilon \in \langle\langle \bar{S} \rangle\rangle$ oder $1-\varepsilon \in \langle\langle \bar{S} \rangle\rangle$, in jedem Fall also $\left|\varepsilon^{(i)}\right| \leq \bar{S}+1$ $(1 \leq i \leq r_1 + r_2)$, und weiter

$$\mathrm{X}_\mathcal{K} \subseteq \langle\langle \bar{S}+1 \rangle\rangle, \tag{1-45}$$

da für $\varepsilon \in \mathrm{X}_\mathcal{K}$ auch stets $\frac{1}{\varepsilon} \in \mathrm{X}_\mathcal{K}$ ist.

Das entscheidende Hilfsmittel zur Berechnung von $\mathrm{X}_\mathcal{K}$ ist das nachfolgende Lemma, in dem für $X \subseteq \mathrm{X}_\mathcal{K}$ die Menge $\Omega(X)$ definiert sei als

$$\Omega(X) := \bigcup_{\varepsilon \in X} \Omega(\varepsilon).$$

Lemma 1.17
Es seien $S > 1$ und $X \subseteq \mathrm{X}_\mathcal{K}$ gegeben mit

$$\mathrm{X}_\mathcal{K} \subseteq \langle\langle S \rangle\rangle \cup \Omega(X). \tag{1-46}$$

Ferner sei $s > 1$ beliebig mit $s \leq S$.

Mit $T := U_1(1, \frac{1}{s}, S) \cup \ldots \cup U_{r_1+r_2}(1, \frac{1}{s}, S)$ gilt dann

$$\mathrm{X}_\mathcal{K} \subseteq \langle\langle s \rangle\rangle \ \cup \ \Omega(X \cup (T \cap \mathrm{X}_\mathcal{K})).$$

Beweis Sei $\varepsilon \in \mathrm{X}_\mathcal{K}$ beliebig. Gilt $\varepsilon \in \langle\langle s \rangle\rangle \cup \Omega(X)$, so ist nichts zu zeigen. Sei also $\varepsilon \notin \langle\langle s \rangle\rangle \cup \Omega(X)$. Indem wir gegebenenfalls ε durch $\frac{1}{\varepsilon} \in \mathrm{X}_\mathcal{K}$ ersetzen, können wir ohne Einschränkung annehmen, daß $j \in \{1, \ldots, r_1 + r_2\}$ mit $\left|\varepsilon^{(j)}\right| > s$ existiert. Für $\eta := 1 - \frac{1}{\varepsilon} \in \mathrm{X}_\mathcal{K}$ gilt dann

$$\left|\eta^{(j)} - 1\right| = \left|\frac{1}{\varepsilon^{(j)}}\right| < \frac{1}{s}.$$

Aus $\eta \in \Omega(\varepsilon)$ und $\varepsilon \notin \Omega(X)$ folgt gemäß Voraussetzung $\eta \in \langle\langle S \rangle\rangle$, also

$$\frac{1}{S} \leq \left|\eta^{(i)}\right| \leq S \qquad (1 \leq i \leq r_1 + r_2).$$

Somit $\eta \in U_j(1, \frac{1}{s}, S)$, also $\varepsilon \in \Omega(\eta) \subseteq \Omega(T \cap \mathrm{X}_\mathcal{K})$. □

Die Grundidee bei der Berechnung von $\mathrm{X}_\mathcal{K}$ ist wie folgt: Wir geben uns zuerst ein $m \in \mathbb{N}_{\not=}$ sowie $S_0 > S_1 > \ldots > S_m > 1$ vor und berechnen anschließend schrittweise endliche Mengen $X_0, \ldots, X_m \subseteq \mathrm{X}_\mathcal{K}$ so, daß für jedes $k \in \{0, \ldots, m\}$ die Implikation

$$\varepsilon \in \mathrm{X}_\mathcal{K} \quad \Longrightarrow \quad \varepsilon \in \Omega(X_k) \vee \varepsilon \in \langle\langle S_k \rangle\rangle \tag{1-47}$$

erfüllt ist.

Dazu setzen wir $S_0 := \bar{S} + 1$ und $X_0 := \emptyset$. Die Implikation (1-47) entspricht dann gerade (1-45). Wir wollen nun davon ausgehen, daß wir $m \in \mathbb{N}_{\not=}$ und $S_1, \ldots, S_m > 1$ bereits vorgegeben haben, und erläutern jetzt die Konstruktion von $X_1, \ldots, X_m$. Wie m und $S_1, \ldots, S_m$ in der Praxis zu wählen sind, beschreiben wir weiter unten.

Ist für $k \in \{0, \ldots, m-1\}$ die Menge X_k bekannt, so berechnen wir $T \subseteq \mathrm{U}_\mathcal{K}$ aus 1.17, wobei dort jetzt $s = S_{k+1}$ und $S = S_k$, und setzen

$$X_{k+1} := X_k \cup (T \cap \mathrm{X}_\mathcal{K}).$$

Aufgrund von 1.17 ist die geforderte Implikation (1-47) erfüllt.

Unser Vorgehen fassen wir in einem kurzen Algorithmus zur Berechnung von $\mathrm{X}_\mathcal{K}$ zusammen.

Algorithmus 1.18

Eingabe: *Ein algebraischer Zahlkörper $\mathcal{K}$, $m \in \mathbb{N}_{\geq}$ und $S_0 > S_1 > \ldots > S_m > 1$ mit $\mathrm{X}_\mathcal{K} \subseteq \langle\langle S_0 \rangle\rangle$.*

Ausgabe: $\mathrm{X}_\mathcal{K}$.

Schritt 1

$X_0 \leftarrow \emptyset$.

Schritt 2 (Konstruktion von $X_1, \ldots, X_m$)

`foreach` $k \in \{1, \ldots, m\}$ `do`
  $X_k \leftarrow X_{k-1}$.
  `foreach` $j \in \{1, \ldots, r_1 + r_2\}$ `do`
    Bestimme durch Auszählen die Menge $X_{k,j}$ aller Ausnahmeeinheiten in $U_j(1, \frac{1}{S_k}, S_{k-1})$ und setze $X_k \leftarrow X_k \cup X_{k,j}$.
  `end`
`end`

Schritt 3 (Ausnahmeeinheiten in $\langle\langle S_m \rangle\rangle$)

Bestimme durch Auszählen (vergleiche 1-43) die Menge X'_{m+1} aller Ausnahmeeinheiten in $\langle\langle S_m \rangle\rangle$.

Schritt 4

Setze $\mathrm{X}_\mathcal{K} \leftarrow \Omega(X_m) \cup X'_{m+1}$ und terminiere.

Anhand einer Betrachtung zur Komplexität von Algorithmus 1.18 werden wir jetzt die Wahl von m und $S_1, \ldots, S_m$ in der Praxis beschreiben.

Liegt eine Einheit $\varepsilon \in \mathrm{U}_\mathcal{K}$ in einer der im zweiten Schritt von 1.18 durch Auszählen zu bestimmenden Mengen $U_j(1, \frac{1}{S_k}, S_{k-1})$, so gelten für ε gemäß 1.13 die Abschätzungen

$$\left|\log\left|\varepsilon^{(j)}\right|\right| \leq \log \frac{S_k}{S_k - 1}, \qquad \left|\log\left|\varepsilon^{(i)}\right|\right| \leq \log S_{k-1} \ (1 \leq i \leq r_1 + r_2).$$

Es ist also der Vektor $(\log\left|\varepsilon^{(1)}\right|, \ldots, \log\left|\varepsilon^{(r_1+r_2)}\right|)^t$ in einem Quader des $\mathbb{R}^{r_1+r_2}$ mit Volumen $2^{r+1} \log \frac{S_k}{S_k-1} \log^r S_{k-1}$ gelegen. Wir wollen daher im folgenden annehmen, daß der Aufwand für das Auszählen aller in $U_j(1, \frac{1}{S_k}, S_{k-1})$ gelegenen Einheiten proportional zu $\log \frac{S_k}{S_k-1} \log^r S_{k-1}$ ist (der nur von r abhängige Faktor 2^{r+1} beim Quadervolumen ist für unsere Betrachtungen ohne Bedeutung).

Im dritten Schritt von 1.18 müssen alle Einheiten $\varepsilon \in \mathrm{U}_\mathcal{K}$ ausgezählt werden, welche in $\langle\langle S_m \rangle\rangle$ liegen. Da für jedes solche ε die Abschätzung $\left|\log\left|\varepsilon^{(i)}\right|\right| \leq \log S_m$ $(1 \leq$

$i \leq r_1 + r_2$) erfüllt ist, setzen wir den Aufwand für die Durchführung des dritten Schrittes von 1.18 entsprechend mit $\log^{r+1} S_m$ an.
Der Gesamtaufwand von Algorithmus 1.18 ist bei den gemachten Annahmen also proportional zu

$$F_m(S_0; S_1, \ldots, S_m) := (r+1) \sum_{k=1}^{m} \log \frac{S_k}{S_k - 1} \log^r S_{k-1} \quad + \quad \log^{r+1} S_m. \qquad (1\text{-}48)$$

Im Hinblick auf die Effizienz sind also $m \in \mathbb{N}_{\not\vdash}$ und $S_1 > \ldots > S_m > 1$ so zu wählen, daß $F_m(S_0; S_1, \ldots, S_m)$ unter der Nebenbedingung $S_1 < S_0$ minimal ist. Es ist allerdings (zumindest dem Verfasser dieser Arbeit) nicht klar, ob eine solche minimierende Wahl von m und $S_1, \ldots, S_m$ im allgemeinen existiert. Im folgenden beschreiben wir unser Vorgehen, mit dem wir in der Praxis versucht haben, eine zumindest befriedigende Wahl dieser Werte zu erreichen.
Wir fixieren m und betrachten die Funktion

$$f : V \to \mathbb{R} : (\curvearrowright_{\not\vdash}, \ldots, \curvearrowright_{\gtrdot})^{\approx} \mapsto \mathbb{F}_{\gtrdot}(\mathbb{S}_{\not\vdash}; \curvearrowright_{\not\vdash}, \ldots, \curvearrowright_{\gtrdot}),$$

wobei $V := \{x \in \mathbb{R}^{\gtrdot} \mid \curvearrowright_{\beth} > \not\vdash \ (\not\vdash \leq \beth \leq \gtrdot)\}$. Sei $S = (S_1, \ldots, S_m) \in V$ eine lokale Minimalstelle von f. Da der Gradient von f in S verschwindet, folgt für jedes $i \in \{1, \ldots, m-1\}$ über

$$\frac{\partial f}{\partial x_i}(S_1, \ldots, S_m) = (r+1) \left(\left(\frac{1}{S_i} - \frac{1}{S_i - 1} \right) \log^r S_{i-1} + \log \frac{S_{i+1}}{S_{i+1} - 1} \frac{r \log^{r-1} S_i}{S_i} \right)$$

die rekursive Beziehung

$$S_{i+1} = \frac{g(S_i)}{g(S_i) - 1}, \qquad \text{wo} \quad g(S_i) := \exp \left(\frac{\log^r S_{i-1}}{r(S_i - 1) \log^{r-1} S_i} \right). \qquad (1\text{-}49)$$

Es ist ferner

$$0 = \frac{\partial f}{\partial x_m}(S_1, \ldots, S_m) = (r+1) \left(\left(\frac{1}{S_m} - \frac{1}{S_m - 1} \right) \log^r S_{m-1} + \frac{\log^r S_m}{S_m} \right), \qquad (1\text{-}50)$$

wobei wir die rechte Seite in (1-50) anhand von (1-49) als eine Funktion h in S_1 auffassen können.
Zur Bestimmung der lokalen Minimalstellen von f genügt es demnach, wenn wir jede Nullstelle S_1 von h im Intervall $(1, +\infty)$ ermitteln und anschließend überprüfen, ob für die aus S_1 vermöge (1-49) resultierenden Werte $S_2, \ldots, S_m$ die Hessesche-Matrix von f an der Stelle $(S_1, \ldots, S_m)$ positiv definit ist.
Bei den in der Praxis aufgetretenen Werten von S_0 — zumeist $S_0 > 10^r$ — lassen numerische Untersuchungen vermuten, daß h im Intervall $(1, +\infty)$ stets genau eine Nullstelle S_1 besitzt. In allen gerechneten Fällen korrespondierte S_1 zu einer lokalen Minimalstelle $(S_1, \ldots, S_m)^t$ von f, für welche zusätzlich $S_1 > \ldots > S_m$ galt (der Verfasser nimmt an, daß es sich bei $(S_1, \ldots, S_m)^t$ sogar stets um die globale Minimalstelle von f auf V handelte). Es konnte beobachet werden, daß ab einer gewissen Größe von m die Nullstelle S_1 von h nicht mehr im Intervall $(1, S_0)$ liegt (etwa $S_1 > 10^{20} = S_0$ für $m \geq 20$ und $r = 2$).
Nachdem wir die Wahl von $S_1, \ldots, S_m$ beschrieben haben, müssen wir nun noch m festlegen. Dazu betrachten wir die folgende Tabelle, welche für einige Werte von m

und r den jeweils entsprechenden Wert $F_m(S_0; S_1, \ldots, S_m)$ an der mit obigem Verfahren numerisch berechneten lokalen Minimalstelle $(S_1, \ldots, S_m)^t \in V$ wiedergibt, wobei für $S_0 = 10^{10r}$ dort stets $S_1 < S_0$ erfüllt ist (da wir m jetzt variieren, werden wir von nun an gelegentlich korrekter $(S_1(m), \ldots, S_m(m))$ schreiben).

m	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$
0	97664.57	$2.28 \cdot 10^7$	$6.63 \cdot 10^9$	$2.33 \cdot 10^{12}$	$9.61 \cdot 10^{14}$
1	102.66	2113.26	56712.77	$1.87 \cdot 10^6$	$7.36 \cdot 10^7$
2	16.54	136.28	1540.35	22009.94	$3.79 \cdot 10^5$
3	8.72	46.37	344.06	3267.78	37750.99
4	6.72	28.13	165.44	1252.33	11576.74
5	6.01	21.83	111.53	735.35	5932.61
6	5.75	19.10	89.09	536.94	3964.05
7	5.67	17.80	78.08	442.74	3076.11
8	5.65	17.18	72.22	392.35	2611.37
9	5.64	16.89	69.00	363.55	2345.53
10	5.64	16.78	67.24	346.57	2185.36

In der Praxis haben wir m jeweils so gewählt, daß die von m abhängige Funktion h eine Nullstelle in $(1, S_0)$ besitzt und darüberhinaus $F_m(S_0; S_1(m), \ldots, S_m(m)) < 0.9 \cdot F_{m-1}(S_0; S_1(m-1), \ldots, S_{m-1}(m-1))$ gilt. Der zweiten Bedingung liegt die Beobachtung zugrunde, daß ein noch größeres m den mit $F_m(S_0; S_1(m), \ldots, S_m(m))$ angesetzten Aufwand von Algorithmus 1.18 zwar weiter geringfügig reduziert, andererseits aber der Initialisierungs- und Verwaltungsaufwand für das Auszählen linear in m zunimmt.

Die Diskussion zur Wahl von m und $S_1, \ldots, S_m$ beschließen wir mit einer zweiten Tabelle, welche bei diesmal festem Einheitenrang $r = 5$ aufzeigt, wie sich die Größe der Ausgangsschranke S_0 auf die Werte von $F_m(S_0; S_1(m), \ldots, S_m(m))$ auswirkt.

S_0	$m = 5$	$m = 10$	$m = 15$	$m = 20$
10^{10}	539.46	335.26	323.99	323.85
10^{20}	639.17	341.72	324.30	323.85
10^{50}	735.35	346.57	324.53	323.85
10^{100}	791.66	349.04	324.65	323.85
10^{500}	890.44	352.88	324.85	323.86
10^{1000}	923.91	354.07	324.92	323.86
10^{5000}	988.24	356.24	325.04	323.86

Wir entnehmen dieser Tabelle, daß die Größe der Ausgangsschranke für die Komplexität von 1.18 nur von untergeordneter Bedeutung zu sein scheint (für andere Einheitenränge ergibt sich ein ähnliches Bild).

Bemerkung 1.19

Für $m = 0$ entspricht Algorithmus 1.18 annäherend dem eingangs erwähnten naiven systematischen Auszählen aller Lösungen der Einheitengleichung. Aus der ersten Tabelle ersehen wir, warum das vorgestellte Verfahren bei passender Wahl von m weitaus effizienter ist.

Der Anwendung von Algorithmus 1.18 auf das in 1.8 begonnene Beispiel stellen wir zwei Bemerkungen voran.

Bemerkung 1.20
Sei K normal über $\mathbb{Q}$ mit Galoisgruppe G. Dann genügt in Schritt 2 von 1.18 die Bestimmung von $X_{1,1},\ldots,X_{m,1}$, d.h. der in

$$U_1(1,\tfrac{1}{S_1},S_0)\cup\ldots\cup U_1(1,\tfrac{1}{S_m},S_{m-1})$$

liegenden Ausnahmeeinheiten, da wir wegen 1.12 jede Menge $X_{k,j}$ $(2\le j\le r_1+r_2)$ anhand eines passenden $\sigma\in G$ erhalten können aus $X_{k,j}=\sigma(X_{k,1})$. Dementsprechend entfällt in (1-48) der Faktor $r+1$ vor dem Summenzeichen.

Bemerkung 1.21
In den Schritten 2 und 3 von 1.18 ist für jede der ausgezählten Einheiten ε zu testen, ob ε eine Ausnahmeeinheit ist. Weil es sich erfahrungsgemäß bei der Mehrzahl der ausgezählten Einheiten nicht um Ausnahmeeinheiten handelt, kann die Laufzeit von 1.18 merklich dadurch reduziert werden, wenn man ein Testverfahren einsetzt, welches schnell Nicht-Ausnahmeeinheiten erkennt. Ein solches, auf Smart [50] zurückgehendes Verfahren wollen wir hier kurz erläutern.

Für ein fest vorgegebenes $a=\zeta^{a_0}\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$ $(a_0\in\{1,\ldots,w-1\},a_1,\ldots,a_r\in\mathbb{Z})$ soll getestet werden, ob a eine Ausnahmeeinheit ist. Da wir im Algorithmus 1.18 die zu testenden Einheiten durch Auszählen erhalten, wollen wir davon ausgehen, daß a nicht als algebraische Zahl vorliegt, sondern daß nur die Exponenten $a_0,\ldots,a_r$ bekannt sind (den Exponenten a_0 erhalten wir zwar nicht aus dem Auszählverfahren, aber für ihn gibt es nur endlich viele Möglichkeiten).

Seien $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ paarweise verschiedene Primideale in $\mathfrak{o}_K$ mit Normen $n_1,\ldots,n_s$. Für $i\in\{1,\ldots,s\}$ und $\gamma\in\mathfrak{o}_K$ bezeichne $\log_i\gamma$ den diskreten Logarithmus von γ in $\mathfrak{o}_K/\mathfrak{p}_i$. Setze

$$A:=\begin{pmatrix}\log_1\zeta & \log_1\varepsilon_1 & \ldots & \log_1\varepsilon_r & n_1-1 & & \\ \vdots & \vdots & & \vdots & & \ddots & \\ \log_s\zeta & \log_s\varepsilon_1 & \ldots & \log_s\varepsilon_r & & & n_s-1\end{pmatrix}.$$

Wenn a eine Ausnahmeeinheit ist, etwa $1-a=\zeta^{b_0}\varepsilon_1^{b_1}\cdots\varepsilon_r^{b_r}$ $(b_0,\ldots,b_r\in\mathbb{Z})$, so existieren $b_{r+1},\ldots,b_s\in\mathbb{Z}$ mit

$$\begin{pmatrix}\log_1(1-a)\\ \vdots\\ \log_s(1-a)\end{pmatrix}=A\cdot\begin{pmatrix}b_1\\ \vdots\\ b_s\end{pmatrix}. \tag{1-51}$$

In der Praxis berechnen wir zunächst $\log_1(1-a),\ldots,\log_s(1-a)$. Hierzu genügt es, jeweils $1-a$ modulo $\mathfrak{p}_\mathfrak{i}$ $(\mathfrak{1}\le\mathfrak{i}\le\mathfrak{s})$ zu bestimmen, wodurch die wesentlich aufwendigere Berechnung der algebraischen Zahl $1-a=1-\zeta^{a_0}\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$ vermieden wird. Danach prüfen wir die Lösbarkeit von (1-51), und erst wenn diese gegeben ist, wird die algebraische Zahl a explizit bestimmt, um dann anschließend $\mathrm{N}(1-a)=\pm1$ zu testen.

Bei unserer Implementierung haben wir die Anzahl s der Primideale gewählt als $s = 3r$.

Beispiel 1.22 (Fortsetzung von 1.8 und 1.11)
Die eingangs in 1.8 formulierte Aufgabe entspricht gerade der Berechnung von $\mathrm{X}_{\mathcal{K}}$. Mit der oberen Exponentenschranke $A = 2076$ aus 1.11 erhalten wir über (1-44) zunächst $S_0 = 6.9 \cdot 10^{4843}$. Da $\mathcal{K}$ normal ist, können wir 1.20 mit der dort beschriebenen Modifikation von F_m einsetzen. Es ist

$$\begin{aligned} F_9(S_0; S_1, \ldots, S_9) &= 172680.33 \\ F_{10}(S_0; S_1, \ldots, S_{10}) &= 149210.18 \\ F_{11}(S_0; S_1, \ldots, S_{11}) &= 134811.60 \\ F_{12}(S_0; S_1, \ldots, S_{12}) &= 125593.54, \end{aligned}$$

und bei Verwendung von $m = 10$ erhalten wir

$$S_1 = 1.49 \cdot 10^{30}, \quad S_2 = 3.89 \cdot 10^{11}, \quad S_3 = 5.52 \cdot 10^{7}, \quad S_4 = 982337.37,$$

$$S_5 = 73360.74, \quad S_6 = 9896.88, \quad S_7 = 1780.14, \quad S_8 = 365.36,$$

$$S_9 = 74.25, \quad S_{10} = 11.47.$$

Benutzen wir diese Werte in Algorithmus 1.18, so ergeben sich dort in Schritt 2 die folgenden Rechenzeiten.

k	$\log \frac{S_k}{S_k - 1} \log^8 S_k$	t
1	*160.83*	*2s*
2	*1396.70*	*2s*
3	*4659.05*	*14s*
4	*10831.82*	*48s*
5	*17905.66*	*97s*
6	*25075.13*	*160s*
7	*28837.78*	*224s*
8	*26986.93*	*275s*
9	*19933.12*	*203s*
10	*10805.69*	*147s*

Die Rechenzeit für Schritt 3 ($\log^9 S_{10} = 3067.47$) betrug 25s, und insgesamt ergab sich eine Rechenzeit von 1555s für die Berechnung von $\mathrm{X}_{\mathcal{K}}$. Auf die Wiedergabe der 28398 Ausnahmeeinheiten in $\mathcal{K}$ sei hier verzichtet.

Man kann das Ergebnis aus Beispiel 1.22 einsetzen, um anhand des folgenden Lemmas von Győry [25, Lemme 12] leicht alle Ausnahmeeinheiten in $\mathbb{Q}(\zeta_{\mathcal{K}^-})$ zu berechnen.

Lemma 1.23 (Győry)
Sei $\mathcal{K}$ ein CM-Körper. Dann besitzt jede nicht-reelle Ausnahmeeinheit von $\mathcal{K}$ die Gestalt

$$\frac{1 - \xi_2}{\xi_1 - \xi_2}$$

mit Einheitswurzeln $\xi_1, \xi_2 \in \mathrm{TU}_{\mathcal{K}}$.

In Verbindung mit 1.23 haben wir mit unserem Verfahren die Ausnahmeeinheiten in allen Kreisteilungskörpern vom Grad ≤ 22 bestimmt. Die Ergebnisse sind in der folgenden Tabelle aufgelistet. Für eine primitive m-te Einheitswurzel ζ_m mit $m \in \mathbb{N}$, $m \not\equiv 2 \bmod 4$, bezeichnet dort $\mathcal{K}_m$ den Kreisteilungskörper $\mathbb{Q}(\zeta_m)$ mit maximalem reellen Teilkörper $\mathcal{K}_m^+$. Wir haben jeweils zuerst die Ausnahmeeinheiten in $\mathcal{K}_m^+$ bestimmt (Rechenzeit t_1) und diese dann mit 1.23 zur Menge aller Ausnahmeeinheiten in $\mathcal{K}_m$ erweitert. Die Rechenzeit t_2 zeigt lediglich die zur Einbettung von $X_{K_m^+}$ in $\mathcal{K}_m$ und der Anwendung von 1.23 benötigte Zeit an. Da für $m = 8, 16, 24, 32, 48$ ein Primideal der Norm 2 in $\mathfrak{o}_{\mathcal{K}_m^+}$ existiert, ist $X_{\mathcal{K}_m^+}$ in diesem Fall leer, wodurch sich die Rechenzeiten von 0 Sekunden in der Tabelle erklären. Der Fall $m = 23$ mit Einheitenrang 10 zeigt die Grenzen unseres Verfahrens auf.

m	$[\mathcal{K}_m^+ : \mathbb{Q}]$	$\lvert X_{K_m^+}\rvert$	t_1	$[\mathcal{K}_m : \mathbb{Q}]$	$\lvert X_{K_m}\rvert$	t_2
1	1	0	0s	1	0	0s
3	1	0	0s	2	2	0s
4	1	0	0s	2	0	0s
5	2	6	0s	4	18	0s
7	3	42	1s	6	72	0s
8	2	0	0s	4	0	0s
9	3	18	1s	6	38	0s
11	5	570	4s	10	660	0s
12	2	0	0s	4	14	0s
13	6	1830	14s	12	1962	2s
15	4	90	1s	8	440	1s
16	4	0	0s	8	0	0s
17	8	11700	246s	16	11940	30s
19	9	28398	1492s	18	28704	128s
20	4	54	1s	8	138	0s
21	6	1416	16s	12	2192	6s
23	11	130812	160941s	22	131274	47026s
24	4	0	0s	8	86	0s
25	10	47766	12405s	20	48078	332s
27	9	8676	1096s	18	8858	32s
28	6	678	15s	12	888	2s
32	8	0	0s	16	0	0s
33	10	73110	16635s	20	75242	514s
36	6	354	14s	12	710	3s
40	8	4398	196s	16	4914	14s
44	10	30030	7335s	20	30660	133s
48	8	0	0s	16	422	16s
60	8	14274	275s	16	16340	46s

Wir hatten eingangs geäußert, daß das Lösen der Einheitengleichung $a + b = 1$, d.h. der Berechnung aller Ausnahmeeinheiten, von besonderem Interesse ist. Dies werden wir jetzt kurz erläutern, wobei wir uns auf eine Arbeit von Niklasch [40]

stützen.
Für einen Zahlkörper $\mathcal{K}$ vorgegebener Signatur (n,r), d.h., $\mathcal{K}$ besitzt den Grad n und Einheitenrang r, ist nach einem Resultat von Evertse [13] die Anzahl der Ausnahmeeinheiten von $\mathcal{K}$ nach oben begrenzt durch $|\mathrm{X}_{\mathcal{K}}| \leq 3 \cdot 7^{n+2r+2}$. Es existiert also eine nur von (n,r) abhängige Konstante *

$$C_1(n,r) := \max\{\ |\mathrm{X}_{\mathcal{K}}| \mid \mathcal{K} \text{ ein algebraischer Zahlkörper der Signatur } (n,r)\ \}.$$

Für $r \leq 1$ erhält man die exakten Werte von $C_1(n,r)$ aus dem folgenden Resultat von Nagell [36, 37].

Satz 1.24 (Nagell)

(1) Ist $\mathcal{K}$ ein quadratischer Zahlkörper, so gilt

$$|\mathrm{X}_{\mathcal{K}}| = \begin{cases} 6 & : \quad \mathrm{disc}_{\mathcal{K}} = 5 \\ 2 & : \quad \mathrm{disc}_{\mathcal{K}} = -3 \\ 0 & : \quad \textit{sonst} \end{cases} .$$

(2) Ist $\mathcal{K}$ ein kubischer Zahlkörper mit $r = 1$, so gilt

$$|\mathrm{X}_{\mathcal{K}}| = \begin{cases} 12 & : \quad \mathrm{disc}_{\mathcal{K}} = -23 \\ 6 & : \quad \mathrm{disc}_{\mathcal{K}} = -31 \\ 0 & : \quad \textit{sonst} \end{cases} .$$

(3) Ist $\mathcal{K}$ ein quartischer Zahlkörper mit $r = 1$ und bezeichnet $\mathrm{P}_{\mathcal{K}}$ die Menge der primitiven Ausnahmeeinheiten in $\mathcal{K}$, so gilt

$$|\mathrm{P}_{\mathcal{K}}| = \begin{cases} 18 & : \quad \mathrm{disc}_{\mathcal{K}} = 117 \\ 12 & : \quad \mathrm{disc}_{\mathcal{K}} = 125, 144 \\ 6 & : \quad \mathrm{disc}_{\mathcal{K}} = 189 \\ 0 & : \quad \textit{sonst} \end{cases} .$$

Betrachtet man 1.24 genauer, so fällt auf, daß $C_1(n,r)$ jeweils von dem Körper angenommen wird, welcher innerhalb der Signatur die kleinste Absolutdiskriminante besitzt. Für $r > 1$ sind die exakten Werte von $C_1(n,r)$ bislang unbekannt. Allerdings lassen umfangreiche Beispielrechnungen, deren Resultate im Anhang wiedergegeben sind, vermuten, daß die Situation ähnlich wie bei den Einheitenrängen 0 und 1 ist. Innerhalb einer Signatur scheinen es stets Körper mit kleiner Absolutdiskriminante zu sein, welche über die meisten Ausnahmeeinheiten verfügen. Die Aussage von 1.24, die Resultate zu $\mathrm{X}_{\mathcal{K}_m^+}$ von Seite 24 und die Ergebnisse aus dem Anhang sind in der folgenden Tabelle zusammengefaßt, welche für $r \leq 1$ die exakten Werte von $C_1(n,r)$ und für $r > 1$ untere Abschätzungen für $C_1(n,r)$ enthält. Man beachte, daß zu jedem in der Tabelle angegebenen Wert ein entsprechender Körper mit eben genau dieser Anzahl von Ausnahmeeinheiten existiert.

*Auf die in [40] definierte Konstante $C_2(n,r)$ werden wir hier nicht eingehen.

	$r=0$	1	2	3	4	5	6	7	8	9	10
$n=1$	0	–	–	–	–	–	–	–	–	–	–
$n=2$	2	6	–	–	–	–	–	–	–	–	–
$n=3$	–	12	42	–	–	–	–	–	–	–	–
$n=4$	–	20	54	162	–	–	–	–	–	–	–
$n=5$	–	–	78	228	570	–	–	–	–	–	–
$n=6$	–	–	110	288	750	2070	–	–	–	–	–
$n=7$	–	–	–	366	960	2310	2892	–	–	–	–
$n=8$	–	–	–	440	?	?	?	15804	–	–	–
$n=9$	–	–	–	–	1266	3366	7848	14844	28398	–	–
$n=10$	–	–	–	–	?	?	?	?	?	73110	–
$n=11$	–	–	–	–	–	?	?	?	?	?	130812

1.3.3 Allgemeine Einheitengleichungen

Nachdem wir im vorangehenden Unterabschnitt zur Bestimmung aller Lösungen der Einheitengleichung $a+b=1$ Methoden aus der Geometrie der Zahlen eingesetzt haben, formulieren wir jetzt ein ähnliches Verfahren für die allgemeine Einheitengleichung $\alpha\, a+\beta\, b=1$ mit $\alpha,\beta\in\mathcal{K}^\times$ beliebig.

Unter Verwendung der oberen Exponentenschranken A und B aus dem ersten und zweiten Abschnitt setzen wir analog zu (1-44) zunächst

$$\bar{A} := \max_{1\le i\le r_1+r_2} \exp\left(A\,\sum_{j=1}^{r}\left|\log\left|\varepsilon_j^{(i)}\right|\right|\right),$$

$$\bar{B} := \max_{1\le i\le r_1+r_2} \exp\left(B\,\sum_{j=1}^{r}\left|\log\left|\varepsilon_j^{(i)}\right|\right|\right),$$

also $\mathfrak{L}_\alpha\subseteq\langle\!\langle\bar{A}\rangle\!\rangle$ und $\mathfrak{L}_\beta\subseteq\langle\!\langle\bar{B}\rangle\!\rangle$ mit den Bezeichnungen aus (1-6), (1-7) und (1-37). Ferner legen wir $s_\alpha, s_\beta\ge 1$ fest durch

$$s_\alpha := \max_{1\le i\le r_1+r_2}\max\left(\left|\alpha^{(i)}\right|,\left|\alpha^{(i)}\right|^{-1}\right),\quad s_\beta := \max_{1\le i\le r_1+r_2}\max\left(\left|\beta^{(i)}\right|,\left|\beta^{(i)}\right|^{-1}\right).$$

Lemma 1.25
Definiere $S_0>1$ durch

$$S_0 := \max_{1\le i\le r_1+r_2}\max\left(\bar{A},\frac{1+\left|\beta^{(i)}\right|\bar{B}}{\left|\alpha^{(i)}\right|}\right). \tag{1-52}$$

Für jedes $j\in\{1,\dots,r_1+r_2\}$ setze mittels (1-38) ferner

$$V_j := U_j\left(\beta,\ \frac{\left|\alpha^{(j)}\right|}{S_0},\ s_\beta\bar{B}\right).$$

Mit $V := V_1\cup\ldots\cup V_{r_1+r_2}$ gilt dann

$$\mathfrak{L}\subseteq\{(a,b)\in\mathfrak{L}\mid a\in\langle\!\langle S_0\rangle\!\rangle\}\cup\{(a,b)\in\mathfrak{L}\mid b\in V\}.$$

Beweis Sei $(a,b) \in \mathfrak{L}$ beliebig. Es gelte ohne Einschränkung $a \notin \langle\langle S_0 \rangle\rangle$, also $b \in \mathfrak{L}_\beta$ wegen $\mathfrak{L}_\alpha \subseteq \langle\langle S_0 \rangle\rangle$. Aus der Definition von S_0 folgt

$$\left|a^{(i)}\right| = \left|\frac{1-(\beta b)^{(i)}}{\alpha^{(i)}}\right| \leq S_0 \qquad (1 \leq i \leq r_1+r_2).$$

Aufgrund von $a \notin \langle\langle S_0 \rangle\rangle$ existiert demnach ein $j \in \{1,\ldots,r_1+r_2\}$ mit $\left|a^{(j)}\right| < \frac{1}{S_0}$. Also

$$\left|(\beta b)^{(j)} - 1\right| = \left|(\alpha a)^{(j)}\right| < \frac{\left|\alpha^{(j)}\right|}{S_0}, \tag{1-53}$$

und damit $b \in V_j$. □

Lemma 1.26
Es seien $s, S > 1$ gegeben mit $s_\alpha < s < S$. Für jedes $j \in \{1,\ldots,r_1+r_2\}$ definiere

$$\begin{aligned}
T_{1,j} &:= U_j\left(\alpha,\, \frac{1}{1+s_\alpha S}\,, s_\alpha S\right),\\
T_{2,j} &:= U_j\left(\frac{1}{\alpha},\, \frac{1}{1+s_\alpha S},\, s_\alpha S\right),\\
T_{3,j} &:= U_j\left(\beta, \frac{s_\alpha}{s}, 1+s_\alpha S\right),\\
T_{4,j} &:= U_j\left(-\frac{\beta}{\alpha}, \frac{s_\alpha}{s}, 1+s_\alpha S\right).
\end{aligned}$$

Mit $T_i := T_{i,1} \cup \ldots \cup T_{i,r_1+r_2}$ $(1 \leq i \leq 4)$ gilt dann

$$\begin{aligned}
\{(a,b) \in \mathfrak{L} \mid a \in \langle\langle S \rangle\rangle\} \quad \subseteq \quad & \{(a,b) \in \mathfrak{L} \mid a \in \langle\langle s \rangle\rangle\}\\
& \cup \{(a,b) \in \mathfrak{L} \mid a \in T_1\} \cup \{(a,b) \in \mathfrak{L} \mid \tfrac{1}{a} \in T_2\}\\
& \cup \{(a,b) \in \mathfrak{L} \mid b \in T_3\} \cup \{(a,b) \in \mathfrak{L} \mid \tfrac{b}{a} \in T_4\}.
\end{aligned}$$

Beweis Sei $(a,b) \in \mathfrak{L}$ beliebig mit $a \in \langle\langle S \rangle\rangle$. Es gelte ohne Einschränkung $a \notin \langle\langle s \rangle\rangle$ sowie $a \notin T_1$ und $\frac{1}{a} \notin T_2$. Wegen $a \notin T_1$ und $\frac{1}{a} \notin T_2$ erhält man für jedes $i \in \{1,\ldots,r_1+r_2\}$ die Abschätzungen

$$\left|(\beta b)^{(i)}\right| = \left|(\alpha a)^{(i)} - 1\right| \quad \geq \quad \frac{1}{1+s_\alpha S}\,, \tag{1-54}$$

$$\left|\frac{(\beta b)^{(i)}}{(\alpha a)^{(i)}}\right| = \left|\frac{1}{(\alpha a)^{(i)}} - 1\right| \quad \geq \quad \frac{1}{1+s_\alpha S}\,. \tag{1-55}$$

Ist $\left|a^{(j)}\right| < \dfrac{1}{s}$ für ein $j \in \{1,\ldots,r_1+r_2\}$, so folgt

$$\left|(\beta b)^{(j)} - 1\right| = \left|(\alpha a)^{(j)}\right| < \frac{s_\alpha}{s}, \tag{1-56}$$

und $a \in \langle\langle S \rangle\rangle$ impliziert

$$\left|(\beta b)^{(i)}\right| = \left|(\alpha a)^{(i)} - 1\right| \leq 1 + s_\alpha S \qquad (1 \leq i \leq r_1+r_2). \tag{1-57}$$

Die Kombination von (1-54), (1-56) und (1-57) liefert dann $b \in T_{3,j}$.

Ist $\left|a^{(j)}\right| > s$ für ein $j \in \{1,\ldots,r_1+r_2\}$, so gilt

$$\left|-\frac{(\beta b)^{(j)}}{(\alpha a)^{(j)}} - 1\right| = \left|\frac{-1}{(\alpha a)^{(j)}}\right| < \frac{s_\alpha}{s}, \tag{1-58}$$

und aus

$$\left|-\frac{(\beta b)^{(i)}}{(\alpha a)^{(i)}}\right| = \left|\frac{1}{(\alpha a)^{(i)}} - 1\right| \leq 1 + s_\alpha S \qquad (1 \leq i \leq r_1 + r_2)$$

folgt zusammen mit (1-55) und (1-58) dann $\frac{b}{a} \in T_{4,j}$. □

Ähnlich wie bei der Berechnung von $\mathrm{X}_\mathcal{K}$ im vorangehenden Unterabschnitt geben wir uns jetzt zunächst $m \in \mathbb{N}_{\not=}$ und $S_1 > \ldots > S_m$ vor, wobei hier zusätzlich $S_1 < S_0$ mit S_0 aus 1.25 und $S_m > s_\alpha$ gelte. Wir werden schrittweise endliche Mengen $A_0, \ldots, A_m \subseteq \mathrm{U}_\mathcal{K}$ konstruieren, so daß für jedes $k \in \{1, \ldots, m\}$ die Implikation

$$(a,b) \in \mathfrak{L} \quad \Longrightarrow \quad a \in A_k \vee a \in \langle\!\langle S_k \rangle\!\rangle \tag{1-59}$$

erfüllt ist.

S_0 hatten wir bereits in Lemma 1.25 festgelegt. Wählen wir A_0 als

$$A_0 := \left\{ \frac{1-\beta\varepsilon}{\alpha} \in \mathrm{U}_\mathcal{K} \mid \varepsilon \in V \right\}$$

mit V wie in 1.25, so entspricht (1-59) gerade der Aussage von Lemma 1.25.

Ist für $k \in \{0, \ldots, m-1\}$ die Menge A_k bereits bekannt, so bestimmen wir $T_1, \ldots, T_4$ aus 1.26, wobei dort $s = S_{k+1}$ und $s = S_k$, und setzen

$$\begin{aligned} A_{k+1} \quad := \quad & A_k \cup \left\{ \varepsilon \in \mathrm{U}_\mathcal{K} \mid \varepsilon \in T_1 \wedge \frac{1-\alpha\varepsilon}{\beta} \in \mathrm{U}_\mathcal{K} \right\} \\ & \cup \left\{ \varepsilon \in \mathrm{U}_\mathcal{K} \mid \frac{1}{\varepsilon} \in T_2 \wedge \frac{1-\alpha\varepsilon}{\beta} \in \mathrm{U}_\mathcal{K} \right\} \\ & \cup \left\{ \frac{1-\beta\varepsilon}{\alpha} \in \mathrm{U}_\mathcal{K} \mid \varepsilon \in T_3 \right\} \\ & \cup \left\{ \frac{1}{\alpha+\beta\varepsilon} \in \mathrm{U}_\mathcal{K} \mid \varepsilon \in T_4 \right\}. \end{aligned} \tag{1-60}$$

Die Implikation (1-59) gilt dann aufgrund von 1.26.

Da der sich aus diesem Vorgehen ergebende Algorithmus in seinem Aufbau mit Algorithmus 1.18 übereinstimmt, verzichten wir hier auf seine Wiedergabe. Die Komplexitätsbetrachtung, mit der die Wahl von m und $S_1, \ldots, S_m$ vorgenommen wird, ist im allgemeinen Fall etwas unübersichtlicher. Vereinfachend kann man allerdings annehmen, daß die Bestimmung der Mengen T_1 und T_2 in 1.26 für die Komplexität von untergeordneter Bedeutung ist, da nämlich das Volumen der hier auszuzählenden Mengen klein ist im Vergleich zu dem der Mengen, welche bei der Bestimmung von T_3 und T_4 ausgezählt werden müssen. Unter dieser Annahme ergibt sich bei der Komplexitätsbetrachtung für das Vorgehen im allgemeinen Fall ein von der Struktur her zu (1-48) identischer Ausdruck. Dementsprechend kann bei der Wahl von m und $S_1, \ldots, S_m$ wie im Spezialfall $\alpha = 1 = \beta$ verfahren werden.

Bemerkung 1.27

1. *Ist $\mathcal{K}$ normal und sind α, β rationale Zahlen, so läßt sich Bemerkung 1.20 ohne Schwierigkeiten übertragen, d.h., in 1.26 genügt es, V_1 auszuzählen und analog müssen in 1.26 jeweils nur die Mengen $T_{i,1}$ $(1 \leq i \leq 4)$ durch Auszählen berechnet werden.*

2. *Der in Bemerkung 1.21 beschriebene Test für die schnelle Erkennung von Nicht-Ausnahmeeinheiten läßt sich leicht so verallgemeinern, daß mit ihm für eine wie in 1.21 gegebene Einheit* $a = \zeta^{a_0}\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$ *geprüft werden kann, ob für* $x, y, z \in \mathcal{K}^\times$ *der Quotient* $\frac{x+y\alpha}{z}$ *eine Einheit ist. Damit lassen sich die bei der Konstruktion von* A_{k+1} *in (1-60) notwendigen Tests entsprechend beschleunigen.*

3. *Sind* $\rho \in \mathcal{K}^\times$ *und* $\lambda_1, \ldots, \lambda_{r_1+r_2} > 0$ *gegeben, so gilt für* $V(\rho, \lambda)$ *aus (1-42) die Gleichheit* $V(\rho, \lambda) = -V(\frac{1}{\rho}, \lambda)$. *Daher erhält man* $T_{2,j}$ $(1 \le j \le r_1 + r_2)$ *in 1.26 leicht aus* $T_{1,j}$, *d.h. ohne erneutes Auszählen.*

4. *Sei* $d \in \mathbb{N}$ *mit* $d\alpha, d\beta \in \mathfrak{o}_\mathcal{K}$. *Ein einfaches Kriterium, mit dem man oftmals sehr schnell feststellen kann, daß die Einheitengleichung (1-1) keine Lösung besitzt, besteht darin, zu prüfen, ob* d *in* $\alpha\,\mathfrak{o}_\mathcal{K} + \beta\,\mathfrak{o}_\mathcal{K}$ *liegt.*

Wir beschließen das Kapitel mit einem einfachen Beispiel.

Beispiel 1.28
Für die primitive elfte Einheitswurzel $\zeta_{11} = \exp\frac{2\pi i}{11}$ *setzen wir* $\theta := \zeta_{11} + \zeta_{11}^{-1}$. *Dann ist* $\mathcal{K} = \mathbb{Q}(\theta)$ *der maximale reelle Teilkörper von* $\mathbb{Q}(\zeta_{\not 1\not 1})$ *mit* $[\mathcal{K} : \mathbb{Q}] = \not 4$, $r = 4$ *und* $\mathfrak{o}_\mathcal{K} = \mathbb{Z}[\theta]$. *Die Konjugierten von* θ *seien numeriert als* $\theta^{(i)} = 2\cos\frac{2\pi i}{11}$ $(1 \le i \le 5)$, *und ein Grundeinheitensystem in* $\mathfrak{o}_\mathcal{K}$ *sei gegeben durch*

$$\varepsilon_1 = 1 - 2\,\theta - 3\,\theta^2 + \theta^3 + \theta^5, \quad \varepsilon_2 = -1 + \theta + \theta^2, \quad \varepsilon_3 = \theta, \quad \varepsilon_4 = 2 - \theta^2.$$

Wir wollen alle $(a, b) \in \mathrm{U}_\mathcal{K} \times \mathrm{U}_\mathcal{K}$ *mit*

$$1 \cdot a + 2 \cdot b = 3 \tag{1-61}$$

bestimmen. Durch Division mit 3 kann (1-61) auf eine Einheitengleichung der Form (1-1) mit $\alpha = \frac{1}{3}$ *und* $\beta = \frac{2}{3}$ *gebracht werden.*

Aus der bakerschen Methode erhalten wir zunächst die oberen Exponentenschranken $A = 10^{25} = B$, *die wir mit dem Verfahren aus dem zweiten Abschnitt auf* $A = 593$ *und* $B = 523$ *reduzieren. Es ist dann* $S_0 = 8.97 \cdot 10^{694}$. *Da* $\mathcal{K}$ *normal ist, können wir wegen* $\alpha, \beta \in \mathbb{Q}$ *die erste Bemerkung aus 1.27 verwenden. Wir wählen* $m = 6$ *mit*

$$S_1 = 10^{40}, \quad S_2 = 3.44 \cdot 10^8, \quad S_3 = 38779.02,$$

$$S_4 = 823.79, \quad S_5 = 63.99, \quad S_6 = 7.42.$$

Allein anhand des Kriteriums aus 1.14, also ohne auszählen zu müssen, stellen wir fest, daß V *aus 1.25 leer ist. In den weiteren Schritten ergeben sich für die Bestimmung der jeweiligen Mengen* T_i *aus 1.26 nachstehende Rechenzeiten* t_i, *wobei wir gemäß der dritten Bemerkung in 1.27 die Bestimmung von* T_1 *und* T_2 *zusammengefaßt haben.*

k	t_1	t_3	t_4
1	*1s*	*1s*	*1s*
2	*1s*	*0s*	*0s*
3	*1s*	*0s*	*0s*
4	*0s*	*1s*	*1s*
5	*0s*	*1s*	*1s*
6	*0s*	*4s*	*4s*

Für die Berechnung aller in $\langle\langle S_6 \rangle\rangle$ gelegenen Einheiten a aus (1-61) benötigten wir weniger als eine Sekunde Rechenzeit.

Die 21 Lösungen von (1-61) sind gegeben durch

$$
\begin{aligned}
\mathfrak{L} \;=\; \{\; & (-43+24\,\theta+50\,\theta^2-10\,\theta^3-12\,\theta^4, 23-12\,\theta-25\,\theta^2+5\,\theta^3+6\,\theta^4),\\
& (-15-40\,\theta-12\,\theta^2+14\,\theta^3+6\,\theta^4, 9+20\,\theta+6\,\theta^2-7\,\theta^3-3\,\theta^4),\\
& (-11+10\,\theta+16\,\theta^2-4\,\theta^3-4\,\theta^4, 7-5\,\theta-8\,\theta^2+2\,\theta^3+2\,\theta^4),\\
& (-5-10\,\theta+10\,\theta^2+6\,\theta^3-4\,\theta^4, 4+5\,\theta-5\,\theta^2-3\,\theta^3+2\,\theta^4),\\
& (-5+6\,\theta+8\,\theta^2-2\,\theta^3-2\,\theta^4, 4-3\,\theta-4\,\theta^2+\theta^3+\theta^4),\\
& (-3-12\,\theta-4\,\theta^2+4\,\theta^3+2\,\theta^4, 3+6\,\theta+2\,\theta^2-2\,\theta^3-\theta^4),\\
& (-3-2\,\theta+8\,\theta^2-2\,\theta^4, 3+\theta-4\,\theta^2+\theta^4),\\
& (-1-4\,\theta+2\,\theta^2+2\,\theta^3, 2+2\,\theta-\theta^2-\theta^3),\\
& (-1-4\,\theta+6\,\theta^2+2\,\theta^3-2\,\theta^4, 2+2\,\theta-3\,\theta^2-\theta^3+\theta^4),\\
& (-1+6\,\theta^2-2\,\theta^4, 2-3\,\theta^2+\theta^4),\\
& (1-6\,\theta-6\,\theta^2+2\,\theta^3+2\,\theta^4, 1+3\,\theta+3\,\theta^2-\theta^3-\theta^4),\\
& (1, 1),\\
& (1+2\,\theta-6\,\theta^2+2\,\theta^4, 1-\theta+3\,\theta^2-\theta^4),\\
& (1+4\,\theta-2\,\theta^3, 1-2\,\theta+\theta^3),\\
& (3-2\,\theta-2\,\theta^2, \theta+\theta^2),\\
& (3+10\,\theta-4\,\theta^2-8\,\theta^3-2\,\theta^4, -5\,\theta+2\,\theta^2+4\,\theta^3+\theta^4),\\
& (5+2\,\theta-4\,\theta^2-2\,\theta^3, -1-\theta+2\,\theta^2+\theta^3),\\
& (5+4\,\theta-14\,\theta^2+4\,\theta^4, -1-2\,\theta+7\,\theta^2-2\,\theta^4),\\
& (5+6\,\theta-2\,\theta^2-2\,\theta^3, -1-3\,\theta+\theta^2+\theta^3),\\
& (7-4\,\theta-8\,\theta^2+2\,\theta^3+2\,\theta^4, -2+2\,\theta+4\,\theta^2-\theta^3-\theta^4),\\
& (11+16\,\theta-44\,\theta^2-2\,\theta^3+12\,\theta^4, -4-8\,\theta+22\,\theta^2+\theta^3-6\,\theta^4)\}.
\end{aligned}
$$

Die Gesamtrechenzeit betrug 41s.

Kapitel 2

Indexformgleichungen

Ist $\mathcal{K}$ ein algebraischer Zahlkörper, so besitzt für ein beliebiges $I \in \mathbb{N}$ die Menge $\{\alpha \in \mathfrak{o}_\mathcal{K} \mid (\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) = \mathbb{I}\}$ nach einem Resultat von Győry [25] ein endliches Vertretersystem $\mathfrak{I}_\mathcal{K}(I)$ bzgl. $\mathbb{Z}$-Äquivalenz, wobei zwei ganze algebraische Zahlen $\alpha, \beta \in \mathfrak{o}_\mathcal{K}$ $\mathbb{Z}$-äquivalent heißen, sofern $\alpha \pm \beta \in \mathbb{Z}$. Die Berechnung von $\mathfrak{I}_\mathcal{K}(I)$ bezeichnet man als das Lösen einer Indexformgleichung. Diese Bezeichnung rührt daher, weil zu einer Ganzheitsbasis $\omega_1 = 1, \omega_2, \ldots, \omega_n$ von $\mathfrak{o}_\mathcal{K}$ eine Form $I_\mathcal{K}(t_2, \ldots, t_n) \in \mathbb{Z}[\approx_{\not\in}, \ldots, \approx_{\ltimes}]$ mit der Eigenschaft existiert, daß für alle $\alpha = x_1\omega_1 + \cdots + x_n\omega_n \in \mathfrak{o}_\mathcal{K}$ mit $(\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) < \infty$ jeweils

$$(\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) = \pm\, \mathbb{I}_\mathcal{K}(\curvearrowleft_{\not\in}, \ldots, \curvearrowleft_{\ltimes}). \tag{2-1}$$

gilt. Die Form $I_\mathcal{K}$ nennt man Indexform von $\mathcal{K}$ bzgl. $\omega_1, \ldots, \omega_n$.

Wir werden in diesem Kapitel unser Verfahren für Einheitengleichungen auf das Lösen von Indexformgleichungen anwenden. Dazu benutzen wir hauptsächlich die klassische Methode, mit welcher Győry die Endlichkeit von $\mathfrak{I}_\mathcal{K}(I)$ dadurch bewies, daß er die effektive Berechnung von $\mathfrak{I}_\mathcal{K}(I)$ auf das Lösen endlich vieler Einheitengleichungen in der galoisschen Hülle von $\mathcal{K}$ zurückführte. Mit unserer Ausarbeitung von Győrys Methode zu einem Algorithmus, welche sich teilweise auf zwei Arbeiten von Smart [50, 51] stützt, lösten wir erstmals Indexformgleichungen in Zahlkörpern von Grad 8, 10 und 12. Daneben verwendeten wir eine Idee von Niklasch [39], um in den Kreisteilungskörpern $\mathbb{Q}(\zeta_{\not\in\not\ni})$, $\mathbb{Q}(\zeta_{\not\in\rightarrow})$ und $\mathbb{Q}(\zeta_{\not\in\not\in})$ alle Potenzganzheitsbasen zu berechnen.

Die Anwendbarkeit von Győrys Methode ist in der Praxis eingeschränkt durch die Notwendigkeit, Rechnungen in der galoisschen Hülle von $\mathcal{K}$ durchführen zu müssen. Alternative Verfahren zum Lösen von Indexformgleichungen, welche nicht der galoisschen Hülle bedürfen, existieren bislang nur für Zahlkörper vom Grad ≤ 4. Für kubische Zahlkörper zeigten Gaál und Schulte [20], daß die Bestimmung von $\mathfrak{I}_\mathcal{K}(I)$ äquivalent ist zum Lösen einer kubischen Thue-Gleichung, für quartische Zahlkörper entwickelten Gaál, Pethő und Pohst [17, 18] ein Verfahren, bei dem die Berechnung von $\mathfrak{I}_\mathcal{K}(I)$ im wesentlichen auf das Lösen eines Systems ternärer quadratischer Formen zurückgeführt wird. Darüber hinaus existieren Verfahren von Gaál [15, 16] sowie von Gaál und Pohst [19] für spezielle Körper sechsten Grades.

Zur weiteren Formulierung legen wir einige Notationen fest. Wie üblich in dieser Arbeit sei $\mathcal{K}$ gegeben als $\mathcal{K} = \mathbb{Q}(\theta)$ mit einer ganzen algebraischen Zahl θ. Wir wählen $d \in \mathbb{N}$ mit $d\mathfrak{o}_\mathcal{K} \subseteq \mathbb{Z}[\theta]$. Ferner bezeichnen wir die galoissche Hülle von $\mathcal{K}$ mit $\mathcal{L}$ und setzen $m := [\mathcal{L} : \mathbb{Q}]$. Für die Galoisgruppe von $\mathcal{L}/\mathbb{Q}$ schreiben wir G. Da das Lösen einer Indexformgleichung für $n = [\mathcal{K} : \mathbb{Q}] \leq 4$ trivial ist, sei ohne Einschränkung $n \geq 3$.

Wir setzen

$$\begin{aligned} N &:= \{1, \ldots, n\}, \\ N_2 &:= \{\{i,j\} \mid 1 \leq i < j \leq n\}, \\ N_3 &:= \{\{i,j,k\} \mid 1 \leq i < j < k \leq n\}. \end{aligned}$$

Die Galoisgruppe G operiere auf den Mengen N, N_2 und N_3 vermöge

$$G \times N \to N : (\sigma, i) \mapsto \sigma \cdot i := i', \quad \text{wo } \sigma(\theta^{(i)}) = \theta^{(i')},$$

$$G \times N_2 \to N_2 : (\sigma, \{i,j\}) \mapsto \sigma \cdot \{i,j\} := \{\sigma \cdot i, \sigma \cdot j\},$$

$$G \times N_3 \to N_3 : (\sigma, \{i,j,k\}) \mapsto \sigma \cdot \{i,j,k\} := \{\sigma \cdot i, \sigma \cdot j, \sigma \cdot k\}.$$

Es seien

$$\begin{aligned} \Omega_2 &:= \{w_1, \ldots, w_s\} := \{G \cdot \tau \mid \tau \in N_2\}, \\ \Omega_3 &:= \{W_1, \ldots, W_t\} := \{G \cdot \pi \mid \pi \in N_3\} \end{aligned}$$

die Mengen der jeweiligen Orbits bzgl. der Operationen von G auf N_2 und N_3. Die Werte s und t, welche ausschließlich von n und G abhängen, notieren wir bisweilen auch als $s(n,G)$ und $t(n,G)$.

Wir wählen für jedes $j \in \{1, \ldots, s\}$ ein festes $\tau_j \in \omega_j$ und analog für jedes $k \in \{1, \ldots, t\}$ ein festes $\pi_k \in W_k$. Ist $\pi = \{i,j,k\} \in N_3$ gegeben mit $i < j < k$, so definieren wir $\pi(1) := \{i,j\}$, $\pi(2) := \{j,k\}$ und $\pi(3) := \{i,k\}$. Zu $\tau \in N_2$ sei $\mathcal{F}_\tau$ der Fixkörper des Stabilisators von τ bzgl. der Operation von G auf N_2. Schließlich setzen wir $\mathcal{K}_\tau := \mathbb{Q}(\theta^{(\beth)}, \theta^{(\beth\!\!\beth)})$ für $\tau = \{i,j\} \in N_2$ und weiter $\mathcal{K}_\pi := \mathbb{Q}(\theta^{(\beth)}, \theta^{(\beth\!\!\beth)}, \theta^{(\gimel)})$ für $\pi = \{i,j,k\} \in N_3$.

Für jedes $\alpha \in \mathfrak{I}_\mathcal{K}(I)$ und jedes $\tau = \{i,j\} \in N_2$ ist nach Wahl von d

$$\alpha_\tau := \frac{d(\alpha^{(i)} - \alpha^{(j)})}{\theta^{(i)} - \theta^{(j)}} \tag{2-2}$$

eine ganze algebraische Zahl aus $\mathcal{F}_\tau$. Es gilt

$$d^{n(n-1)} I^2 \mathrm{disc}_\mathcal{K} = d^{n(n-1)} \prod_{\{i,j\} \in N_2} (\alpha^{(i)} - \alpha^{(j)})^2 = \prod_{\{i,j\} \in N_2} (\theta^{(i)} - \theta^{(j)})^2 \alpha_{ij}^2,$$

wobei wir im rechten Produkt α_{ij} anstatt $\alpha_{\{i,j\}}$ geschrieben haben — eine schreibtechnische Vereinfachung, die wir im folgenden bei Indizierungen mit Elementen aus N_2 und N_3 beibehalten. Setzen wir

$$I' := I^2 \frac{d^{n(n-1)} \mathrm{disc}_\mathcal{K}}{\mathrm{disc}\, \mathbb{Z}[\theta]} \in \mathbb{N}$$

und wählen wir $G_j \subseteq G$ minimal mit $G_j \cdot \tau_j = w_j$ $(1 \leq j \leq s)$, so erhalten wir für jedes $\alpha \in \mathfrak{I}_{\mathcal{K}}(I)$ die Gleichung

$$I' = \prod_{\{i,j\} \in N_2} \alpha_{ij}^2 = \prod_{j=1}^{s} \prod_{\sigma \in G_j} \sigma(\alpha_{\tau_j})^2. \tag{2-3}$$

Der **erste** Schritt bei der Berechnung von $\mathfrak{I}_{\mathcal{K}}(I)$ wird darin bestehen, eine endliche Menge $A \subseteq \mathcal{F}_{\tau_1} \times \cdots \times \mathcal{F}_{\tau_s}$ zu ermitteln, so daß zu jedem $\alpha \in \mathfrak{I}_{\mathcal{K}}(I)$ ein $a = (a_{\tau_1}, \ldots, a_{\tau_s}) \in A$ existiert mit

$$\alpha_{\tau_j} \in a_{\tau_j} \mathrm{U}_{\mathcal{F}_{\tau_j}} \qquad (1 \leq j \leq s). \tag{2-4}$$

Im Fall $I = d = 1$, also $I' = 1$, leistet offensichtlich $A = \{(1, \ldots, 1)\}$ das Gewünschte. Ist dagegen $I' > 1$, so gestaltet sich die Bestimmung von A weitaus schwieriger, zumal A im Hinblick auf den noch folgenden zweiten Schritt zur Berechnung von $\mathfrak{I}_{\mathcal{K}}(I)$ möglichst wenige Einträge enthalten sollte, welche nicht zu einer Lösung aus $\mathfrak{I}_{\mathcal{K}}(I)$ gemäß (2-4) gehören.

Ist $I'\,\mathfrak{o}_{\mathcal{L}} = \mathfrak{p}_1^{\mathfrak{e}_1} \cdots \mathfrak{p}_{\mathfrak{r}}^{\mathfrak{e}_{\mathfrak{r}}}$ die Primidealzerlegung von I' in $\mathfrak{o}_{\mathcal{L}}$, so existiert zu jedem $\alpha \in \mathfrak{I}_{\mathcal{K}}(I)$ aufgrund von (2-3) ein

$$e = (e_{11}, \ldots, e_{r1}, \ldots, e_{1s}, \ldots, e_{rs})^t \in \mathbb{N}_{\curlywedge}^{\curlyvee} \tag{2-5}$$

mit $\alpha_{\tau_j}\,\mathfrak{o}_{\mathcal{L}} = \mathfrak{p}_1^{\mathfrak{e}_{1\mathfrak{j}}} \cdots \mathfrak{p}_{\mathfrak{r}}^{\mathfrak{e}_{\mathfrak{r}\mathfrak{j}}} (1 \leq \mathfrak{j} \leq \mathfrak{s})$. Aus (2-3) folgt dann weiter

$$\mathfrak{p}_1^{\mathfrak{e}_1} \cdots \mathfrak{p}_{\mathfrak{r}}^{\mathfrak{e}_{\mathfrak{r}}} = \prod_{\mathfrak{j}=1}^{\mathfrak{s}} \prod_{\sigma \in \mathfrak{G}_{\mathfrak{j}}} \sigma(\mathfrak{p}_1^{\mathfrak{e}_{1\mathfrak{j}}} \cdots \mathfrak{p}_{\mathfrak{r}}^{\mathfrak{e}_{\mathfrak{r}\mathfrak{j}}})^2 = \mathfrak{p}_1^{\lambda_1(\mathfrak{e})} \cdots \mathfrak{p}_{\mathfrak{r}}^{\lambda_{\mathfrak{r}}(\mathfrak{e})},$$

wobei für jedes $i \in \{1, \ldots, r\}$ der Exponent $\lambda_i(e)$ eine in $e_{\mu\nu}$ lineare Funktion

$$\lambda_i(e) = \sum_{\mu=1}^{r} \sum_{\nu=1}^{s} \lambda_{i\mu\nu} e_{\mu\nu}$$

ist, deren Koeffizieten $\lambda_{i\mu\nu} \in \mathbb{N}_{\curlywedge}$ festgelegt sind durch

$$\prod_{\sigma \in G_\nu} \sigma(\mathfrak{p}_\mu)^2 = \mathfrak{p}_1^{\lambda_{1\mu\nu}} \cdots \mathfrak{p}_{\mathfrak{r}}^{\lambda_{\mathfrak{r}\mu\nu}} \qquad (1 \leq \mu \leq \mathfrak{r}, 1 \leq \nu \leq \mathfrak{s}).$$

Setzen wir

$$L := \begin{pmatrix} \lambda_{111} & \ldots & \lambda_{1r1} & \ldots & \lambda_{11s} & \ldots & \lambda_{1rs} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \lambda_{r11} & \ldots & \lambda_{rr1} & \ldots & \lambda_{r1s} & \ldots & \lambda_{rrs} \end{pmatrix}, \tag{2-6}$$

so ist demnach die Menge

$$\mathfrak{L} := \{x \in \mathbb{N}_{\curlywedge}^{\curlyvee} \mid (\curlywedge, \ldots, \curlyvee)^{\approx} = \mathbb{L} \cdot \curvearrowleft\} \tag{2-7}$$

endlich, und es ist $e \in \mathfrak{L}$. Um aus $\mathfrak{L}$ die gewünschte Menge A zu erhalten, testen wir für jedes $(x_{11}, \ldots, x_{r1}, \ldots, x_{1s}, \ldots, x_{rs})^t \in \mathfrak{L}$, ob für alle $j \in \{1, \ldots, s\}$ ein $a_{\tau_j} \in \mathcal{F}_{\tau_j}$ existiert mit $a_{\tau_j}\,\mathfrak{o}_{\mathcal{L}} = \mathfrak{p}_1^{\mathfrak{x}_{1\mathfrak{j}}} \cdots \mathfrak{p}_{\mathfrak{r}}^{\mathfrak{x}_{\mathfrak{r}\mathfrak{j}}}$ und fügen bei Bestehen dieses Tests $(a_{\tau_1}, \ldots, a_{\tau_s})$ zur Menge A hinzu.

Bemerkung 2.1
Die so konstruierte Menge A enthält üblicherweise eine Vielzahl von Elementen, welche nicht zu Lösungen aus $\mathfrak{I}_K(I)$ gemäß (2-4) gehören. Einige dieser Elemente können anhand der folgenden beiden Kriterien aussortiert werden:

1. *Sei $I = 1$, und sei ferner $\alpha \in \mathfrak{I}_K(I)$ beliebig. Dann gilt $\mathbb{Z}[\theta] \subseteq \mathbb{Z}[\alpha]$. Für jedes $\tau = \{i,j\} \in N_2$ teilt also $\alpha^{(i)} - \alpha^{(j)}$ die Differenz $\theta^{(i)} - \theta^{(j)}$ in $\mathfrak{o}_{\mathcal{F}_\tau}$. Somit muß für ein $(a_{\tau_1}, \ldots, a_{\tau_s}) \in A$ jeweils a_{τ_j} ein Teiler von d in $\mathfrak{o}_{\mathcal{F}_\tau}$ sein $(1 \le j \le s)$. Ist $\mathfrak{p}_1^{\mathfrak{d}_1} \cdots \mathfrak{p}_t^{\mathfrak{d}_t}$ die Primidealzerlegung von d in $\mathfrak{o}_\mathcal{L}$, so gilt für jedes $(x_{11}, \ldots, x_{r1}, \ldots, x_{1s}, \ldots, x_{rs})^t \in \mathfrak{L}$, welches mit einer Lösung aus $\mathfrak{I}_K(I)$ korrespondiert, also $x_{\nu j} \le d_\nu$ $(1 \le \nu \le r, 1 \le j \le s)$.*

2. *Sei K normal mit G abelsch, und seien ferner $\alpha \in \mathfrak{I}_K(I)$ sowie $\{i,j\} \in N_2$ beliebig vorgegeben. Für jedes $\sigma \in G$ ist dann wegen*

$$\sigma(d(\alpha^{(i)} - \alpha^{(j)})) = d((\sigma(\alpha))^{(i)} - (\sigma(\alpha))^{(j)})$$

die Differenz $\theta^{(i)} - \theta^{(j)}$ ein Teiler von $\sigma(d(\alpha^{(i)} - \alpha^{(j)}))$ in $\mathfrak{o}_K$.

Für ein $(a_{\tau_1}, \ldots, a_{\tau_s}) \in A$ muß also

$$\frac{\sigma(\theta^{(i)} - \theta^{(j)})\,\sigma(a_{\tau_\nu})}{\theta^{(i)} - \theta^{(j)}} \qquad (1 \le \nu \le s, \{i,j\} = \tau_\nu)$$

stets eine ganze algebraische Zahl aus $\mathfrak{o}_K$ sein.

Beispiel 2.2
Sei $K = \mathbb{Q}(\theta)$, wo θ Nullstelle von $t^5 - 10\,t^3 + 5\,t^2 + 10\,t + 1$. Dann ist K normal mit Galoisgruppe $C(5)$, und K besitzt Klassenzahl 1. Eine Ganzheitsbasis von $\mathfrak{o}_K$ ist gegeben durch

$$\omega_1 = 1, \quad \omega_2 = \theta, \quad \omega_3 = \theta^2, \quad \omega_4 = \theta^3, \quad \omega_5 = \frac{2 + 2\,\theta + 6\,\theta^2 + 3\,\theta^3 + \theta^4}{7},$$

und wegen $(\mathfrak{o}_K : \mathbb{Z}[\theta]) = \not\vartriangleright$ können wir $d = 7$ wählen.
Wir wollen $i_K \in \mathbb{N}$ minimal mit $\mathfrak{I}_K(i_K) \neq \emptyset$ berechnen und das Vertretersystem $\mathfrak{I}_K(i_K)$ explizit berechnen. Da K nicht der maximale reelle Teilkörper eines Kreisteilungskörpers ist, gilt $\mathfrak{I}_K(1) = \emptyset$ nach einem Resultat von Gras [24]. Wegen $\theta \in \mathfrak{I}_K(7)$ müssen wir also herausfinden, für welches minimale $I \in \{2,3,4,5,6,7\}$ die Menge $\mathfrak{I}_K(I)$ nicht leer ist. Dazu geben wir zunächst die Zerlegungen von $2, 3, 5, 7$ in jeweils paarweise verschiedene Primideale aus $\mathfrak{o}_K$ an:

$$2\,\mathfrak{o}_K = \mathfrak{p}_1, \quad 3\,\mathfrak{o}_K = \mathfrak{p}_2, \quad 5\,\mathfrak{o}_K = \mathfrak{p}_3^5, \quad 7\,\mathfrak{o}_K = \mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6\mathfrak{p}_7\mathfrak{p}_8.$$

Es ist insbesondere

$$\frac{d^{n(n-1)}\mathrm{disc}_K}{\mathrm{disc}\,\mathbb{Z}[\theta]}\,\mathfrak{o}_K = 7^{18}\,\mathfrak{o}_K = \mathfrak{p}_4^{18}\mathfrak{p}_5^{18}\mathfrak{p}_6^{18}\mathfrak{p}_7^{18}\mathfrak{p}_8^{18}.$$

Ferner notieren wir

$$\Omega_2 = \{\{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{1,5\}\},\{\{1,3\},\{2,4\},\{3,5\},\{1,4\},\{2,5\}\}\},$$

also ist $G_1 = G = G_2$.

1.Fall $I = 2$

Es ist $\mathfrak{I}_{\mathcal{K}}(2) = \emptyset$*, da das lineare Gleichungssystem*

$$\begin{pmatrix} 2 \\ 18 \\ 18 \\ 18 \\ 18 \\ 18 \end{pmatrix} = \begin{pmatrix} 10 & 0 & 0 & 0 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} \cdot x$$

aus (2-7) keine Lösung in $\mathbb{N}_{\not<}^{\not<\not=}$ *besitzt.*

2.Fall $I = 3$

Es ist $\mathfrak{I}_{\mathcal{K}}(3) = \emptyset$*, da sich dasselbe Gleichungssystem wie im Fall* $I = 2$ *ergibt.*

3.Fall $I = 4, 6$

Es ist $\mathfrak{I}_{\mathcal{K}}(4) = \emptyset = \mathfrak{I}_{\mathcal{K}}(6)$*, wie man leicht anhand der Gleichungssysteme aus den Fällen* $I = 2$ *und* $I = 3$ *folgert.*

4.Fall $I = 5$

Wir erhalten das lineare Gleichungssystem

$$\begin{pmatrix} 10 \\ 18 \\ 18 \\ 18 \\ 18 \\ 18 \end{pmatrix} = \begin{pmatrix} 10 & 0 & 0 & 0 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} \cdot x$$

mit 97240 Lösungen in $\mathbb{N}_{\not<}^{\not<\not=}$*. Von diesen können wir 93236 viele vermöge des zweiten Kriteriums aus 2.1 aussortieren. Für* $I = 5$ *enthält* A *also 4004 Elemente.*

5.Fall $I = 7$

Wir erhalten das lineare Gleichungssystem

$$\begin{pmatrix} 20 \\ 20 \\ 20 \\ 20 \\ 20 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} \cdot x$$

mit 92378 Lösungen in $\mathbb{N}_{\not<}^{\not<\not<}$*. Von diesen können wir 87373 viele vermöge des zweiten Kriteriums aus 2.1 aussortieren. Für* $I = 7$ *enthält* A *also 5005 Elemente.*

Wir werden dieses Beispiel später fortsetzen.

Für den Rest dieses Kapitels sei $a = (a_{\tau_1}, \ldots, a_{\tau_s}) \in A$ beliebig, aber fest vorgegeben. Setzen wir

$$\mathfrak{I}_{\mathcal{K}}(I, a) := \{\alpha \in \mathfrak{I}_{\mathcal{K}}(a) \mid \alpha \text{ ist äquivalent zu } a \text{ vermöge (2-4)}\}$$

und weiter

$$a_{\sigma \cdot \tau_j} := \sigma(a_{\tau_j}) \qquad (\sigma \in G, 1 \leq j \leq s),$$

wobei $a_{\sigma\cdot\tau_j}$ aufgrund von $a_{\tau_j} \in \mathcal{F}_{\tau_j}$ wohldefiniert ist, so gilt für ein $\alpha \in \mathfrak{I}_K(I,a)$ jeweils

$$\alpha_\tau \in a_\tau \mathrm{U}_{\mathcal{F}_\tau} \qquad \forall\, \tau \in N_2. \tag{2-8}$$

Im **zweiten** Schritt zur Berechnung von $\mathfrak{I}_K(I)$ berechnen wir für jedes $\pi \in N_3$ eine endliche Menge $U_\pi \subseteq \mathrm{U}_{\mathcal{F}_{\pi(1)}} \times \mathrm{U}_{\mathcal{F}_{\pi(2)}} \times \mathrm{U}_{\mathcal{F}_{\pi(3)}}$, so daß zu jedem $\alpha \in \mathfrak{I}_K(I,a)$ ein Tripel $\varepsilon_\pi = (\varepsilon_{\pi(1)}, \varepsilon_{\pi(2)}, \varepsilon_{\pi(3)}) \in U_\pi$ und eine Einheit $\eta_\pi \in \mathrm{U}_\mathcal{L}$ existieren mit

$$\alpha_{\pi(i)} = a_{\pi(i)} \varepsilon_{\pi(i)} \eta_\pi \qquad (1 \le i \le 3). \tag{2-9}$$

Sind $\pi = \{i,j,k\} \in N_3$ mit $i < j < k$ und $\alpha \in \mathfrak{I}_K(I,a)$ beliebig gegeben, so gilt

$$\alpha^{(i)} - \alpha^{(j)} + \alpha^{(j)} - \alpha^{(k)} = \alpha^{(i)} - \alpha^{(k)},$$

also

$$(\theta^{(i)} - \theta^{(j)})\, \alpha_{ij} + (\theta^{(j)} - \theta^{(k)})\, \alpha_{jk} = (\theta^{(i)} - \theta^{(k)})\, \alpha_{ik}.$$

Setzen wir $\varepsilon_{\pi(i)} := \alpha_{\pi(i)} a_{\pi(i)}^{-1}$ $(1 \le i \le 3)$, so ist $\varepsilon_{\pi(i)} \in \mathrm{U}_{\mathcal{K}_{\pi(i)}}$ $(1 \le i \le 3)$ gemäß (2-8). Wir bekommen damit die Einheitengleichung

$$\frac{(\theta^{(i)} - \theta^{(j)})\, a_{ij}}{(\theta^{(i)} - \theta^{(k)})\, a_{ik}} \, \frac{\varepsilon_{ij}}{\varepsilon_{ik}} + \frac{(\theta^{(j)} - \theta^{(k)})\, a_{jk}}{(\theta^{(i)} - \theta^{(k)})\, a_{ik}} \, \frac{\varepsilon_{jk}}{\varepsilon_{ik}} = 1$$

über dem Körper $\mathcal{K}_\pi$, deren Lösungsmenge wir mit $\mathfrak{L}_\pi$ bezeichnen. Für jedes $(\varepsilon,\eta) \in \mathfrak{L}_\pi$ prüfen wir, ob $\xi \in \mathrm{U}_{\mathcal{F}_{\pi(3)}}$ existiert mit $\varepsilon\xi \in \mathrm{U}_{\mathcal{F}_{\pi(1)}}, \eta\xi \in \mathrm{U}_{\mathcal{F}_{\pi(2)}}$, und fügen bei Vorhandensein eines solchen ξ den Tripel $(\varepsilon\xi, \eta\xi, \xi)$ zur Menge U_π hinzu.

Der **dritte** und letzte Schritt bei der Lösung der Indexformgleichung besteht darin, durch einen Abgleich der Mengen U_π alle $\alpha \in \mathfrak{I}_K(I,a)$ zu bestimmen. Dazu prüfen wir für jedes Element $(\varepsilon_\pi)_{\pi\in N_3}$ der endlichen Menge $\prod_{\pi\in N_3} U_\pi$, ob ein $\alpha \in \mathfrak{o}_K$ konstruiert werden kann, so daß im Hinblick auf (2-9) gilt:

$$\forall\, \pi \in N_3\ \exists\, \eta_\pi \in \mathrm{U}_\mathcal{L}\ \forall\, i \in \{1,2,3\} : \alpha_{\pi(i)} = a_{\pi(i)} \varepsilon_{\pi(i)} \eta_\pi. \tag{2-10}$$

Sei also zu jedem $\pi \in N_3$ ein beliebiger, aber fest gewählter Tupel $\varepsilon_\pi \in \mathrm{U}_\pi$ gegeben. Wir wollen annehmen, daß ein $\alpha \in \mathfrak{I}_K(I,a)$ existiert, welches (2-10) leistet. Zur Konstruktion von α berechnen wir zuerst schrittweise Mengen

$$N_2^{(1)} \subsetneqq N_2^{(2)} \subsetneqq \cdots \subsetneqq N_2^{(\kappa)} = N_2$$

und hierzu simultan für jedes $\tau \in N_2^{(\nu)}$ $(1 \le \nu \le \kappa)$ Einheiten $u_\tau \in \mathrm{U}_\mathcal{L}$, so daß jeweils ein $\varepsilon \in \mathrm{U}_\mathcal{L}$ existiert mit

$$\alpha_\tau = a_\tau u_\tau \varepsilon \qquad \forall\, \tau \in N_2^{(\nu)}. \tag{2-11}$$

Für ein $\pi \in N_3$ beliebig setzen wir zunächst $N_2^{(1)} := \{\pi(1), \pi(2), \pi(3)\}$ und weiter $u_{\pi(i)} := \varepsilon_{\pi(i)}$ $(1 \le i \le 3)$. Die Bedingung (2-11) entspricht dann gerade (2-9).

Für ein $\nu \in \mathbb{N}$ sei nun die Menge $N_2^{(\nu)}$ mit Einheiten u_τ bereits bekannt, und es gelte ohne Einschränkung $N_2^{(\nu)} \neq N_2$, da wir sonst fertig sind. Es existieren dann

$\tau = \{i,j\} \in N_2^{(\nu)}$ und $\tau' = \{j,k\} \in N_2 \setminus N_2^{(\nu)}$. Sei ohne Einschränkung $i < j < k$. Zu $\pi = \{i,j,k\} \in N_3$ gibt es gemäß (2-9) nach Vorgabe von ε_π eine Einheit $\eta_\pi \in \mathrm{U}_\mathcal{L}$ mit

$$\begin{aligned} \alpha_{ij} &= \alpha_{\pi(1)} = a_{\pi(1)}\varepsilon_{\pi(1)}\eta_\pi = a_{ij}\varepsilon_{ij}\eta_\pi, \\ \alpha_{jk} &= \alpha_{\pi(2)} = a_{\pi(2)}\varepsilon_{\pi(2)}\eta_\pi = a_{jk}\varepsilon_{jk}\eta_\pi, \\ \alpha_{ik} &= \alpha_{\pi(3)} = a_{\pi(3)}\varepsilon_{\pi(3)}\eta_\pi = a_{ik}\varepsilon_{ik}\eta_\pi. \end{aligned}$$

Ist $\varepsilon \in \mathrm{U}_\mathcal{L}$ wie in (2-11) gegeben, so folgt hieraus

$$\eta_\pi = \frac{u_{ij}}{\varepsilon_{ij}}\varepsilon.$$

Setzen wir also

$$u_{jk} := \varepsilon_{jk}\frac{u_{ij}}{\varepsilon_{ij}}, \qquad u_{ik} := \varepsilon_{ik}\frac{u_{ij}}{\varepsilon_{ij}}, \tag{2-12}$$

und

$$N_2^{(\nu+1)} := N_2^{(\nu)} \cup \{\{j,k\},\{i,k\}\},$$

so ist die Bedingung (2-11) offenbar erfüllt.

Bemerkung 2.3
Galt bereits $\{i,k\} \in N_2^{(\nu)}$ und stimmt die Festlegung von u_{ik} in (2-12) nicht mit dem schon bekannten Wert für u_{ik} überein, so kann $(\varepsilon_\pi)_{\pi\in N_3}$ nicht mit einem $\alpha \in \mathfrak{I}_\mathcal{K}(I,a)$ korrespondieren.

Mit der obigen Konstruktion haben wir für jedes $\tau \in N_2$ eine Einheit $u_\tau \in \mathrm{U}_\mathcal{L}$ bestimmt, so daß

$$\alpha_\tau = a_\tau u_\tau \varepsilon \qquad \forall\, \tau \in N_2 \tag{2-13}$$

mit einer noch unbekannten Einheit $\varepsilon \in \mathrm{U}_\mathcal{L}$ gilt. Indem wir (2-3) und (2-13) kombinieren, erhalten wir ε modulo Torsionseinheiten aus

$$I' = \varepsilon^{n(n-1)} \prod_{\tau\in N_2} a_\tau^2 u_\tau^2.$$

Aufgrund von (2-13) und (2-2) kennen wir mit ε für alle $\{i,j\} \in N_2$ die Differenzen $\alpha^{(i)} - \alpha^{(j)}$, wodurch α natürlich modulo $\mathbb{Z}$-Äquivalenz eindeutig bestimmt ist. Um α anhand dieser Differenzen effektiv zu berechnen, gehen wir folgendermaßen vor. Zu einer Ganzheitsbasis $\omega_1 = 1, \ldots, \omega_n$ von $\mathfrak{o}_\mathcal{K}$ und einer Ganzheitsbasis $\upsilon_1 = 1, \ldots, \upsilon_m$ von $\mathfrak{o}_\mathcal{L}$ sei $T \in \mathbb{Z}^{\geqslant\times\ltimes}$ gegeben mit

$$(\omega_1, \ldots, \omega_n) = (\upsilon_1, \ldots, \upsilon_m) \cdot T.$$

Ferner seien $T_1, \ldots, T_m \in \mathrm{GL}(m,\mathbb{Z})$ gegeben mit

$$(\sigma_i(\upsilon_1), \ldots, \sigma_i(\upsilon_m)) = (\upsilon_1, \ldots, \upsilon_m) \cdot T_i \qquad (1 \leq i \leq n),$$

wobei die Automorphismen $\sigma_1, \ldots, \sigma_m \in G$ so numeriert seien, daß $\sigma_j(\theta) = \theta^{(j)}$ für alle $j \in \{1, \ldots, n\}$.

Wir setzen α an als $\alpha = x_1\omega_1 + \cdots + x_n\omega_n$ mit Unbekannten $x_1, \ldots, x_n \in \mathbb{Z}$. Besitzt für ein $\{i,j\} \in N_2$ dann $\alpha^{(i)} - \alpha^{(j)}$ die Darstellung

$$\alpha^{(i)} - \alpha^{(j)} = \xi_{ij1}\upsilon_1 + \cdots + \xi_{ijm}\upsilon_m$$

mit $\xi_{ijk} \in \mathbb{Z}$ ($\mathbb{1} \leq \mathbb{7} \leq \mathbb{9}$), so folgt

$$\begin{aligned}
(\upsilon_1, \ldots, \upsilon_m) \cdot \begin{pmatrix} \xi_{ij1} \\ \vdots \\ \xi_{ijm} \end{pmatrix} &= \alpha^{(i)} - \alpha^{(j)} \\
&= \left((\omega_1^{(i)}, \ldots, \omega_n^{(i)}) - (\omega_1^{(j)}, \ldots, \omega_n^{(j)})\right) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\
&= \left((\upsilon_1^{(i)}, \ldots, \upsilon_m^{(j)}) - (\upsilon_1^{(j)}, \ldots, \upsilon_m^{(j)})\right) \cdot T \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\
&= ((\upsilon_1, \ldots, \upsilon_m)) \cdot (T_i - T_j) \cdot T \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},
\end{aligned}$$

d.h., wir bekommen für $x_1, \ldots, x_n$ das lineare Gleichungssystem

$$\begin{pmatrix} \xi_{ij1} \\ \vdots \\ \xi_{ijm} \end{pmatrix} = (T_i - T_j) \cdot T \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \tag{2-14}$$

Da α durch die Differenzen $\alpha^{(i)} - \alpha^{(j)}$ modulo $\mathbb{Z}$-Äquivalenz eindeutig festgelegt ist, erhalten wir die Koeffizienten $x_2, \ldots, x_n$ von $\pm\alpha$ dadurch, indem wir für jedes $\{i,j\} \in N_2$ das lineare Gleichungssystem (2-14) lösen und anschließend die Schnittmenge der jeweiligen Lösungsmengen $\mathfrak{L}_{ij} \subseteq \mathbb{Z}^{\mathbb{K}}$ berechnen. Es ist

$$\bigcap_{\{i,j\} \in N_2} \mathfrak{L}_{ij} = \pm \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Mit dem dritten Schritt ist die Ausarbeitung von Győrys Methode zu einem Algorithmus abgeschlossen. Dessen Effizienz kann allerdings durch zwei einfache, im folgenden dargestellte Modifikationen deutlich gesteigert werden.

Die **erste** Modifikation, welche von Smart [50] stammt, besteht darin, im zweiten und dritten Schritt die Operation von G auf N_3 auszunutzen. Hintergrund ist hierbei die Tatsache, daß für $\alpha, \pi, \varepsilon_\pi$ und η_π gegeben wie bei (2-9) stets

$$\alpha_{\sigma\cdot(\pi(i))} = a_{\sigma\cdot(\pi(i))}\sigma(\varepsilon_{\pi(i)})\sigma(\eta_\pi) \qquad (1 \leq i \leq 3)$$

für jedes $\sigma \in G$ gilt. Anstatt nun im zweiten Schritt für jedes $\pi \in N_3$ die Menge U_π durch das Lösen einer Einheitengleichung zu bestimmen, werden dort nur die Mengen $U_{\pi_1}, \ldots, U_{\pi_t}$ so berechnet. Zur Ermittlung von $\mathfrak{I}_\mathcal{K}(I,a)$ im dritten Schritt setzen wir dann für jedes $(\varepsilon_{\pi_1}, \ldots, \varepsilon_{\pi_t}) \in U_{\pi_1} \times \cdots \times U_{\pi_t}$ zunächst

$$\varepsilon_{\sigma\cdot\pi_i} := (\sigma(\varepsilon_{\pi_i(j_1)}), \sigma(\varepsilon_{\pi_i(j_2)}, \sigma(\varepsilon_{\pi_i(j_3)})) \qquad (1 \le i \le t, \sigma \in G),$$

wobei $j_k = j_k(i,\sigma) \in \{1,2,3\}$ mit $\sigma \cdot (\pi_i(j_k)) = (\sigma \cdot \pi)(k)$ $(1 \le k \le 3)$, und untersuchen anschließend mit der bereits beschriebenen Methode, ob mit $(\varepsilon_\pi)_{\pi\in N_3}$ ein $\alpha \in \mathfrak{I}_\mathcal{K}(I,a)$ vermöge (2-10) korrespondiert. Durch dieses Vorgehen wird einerseits die Anzahl der im zweiten Schritt zu lösenden Einheitengleichungen von $\binom{n}{3} = |N_3|$ auf $t = |\Omega_3|$ reduziert, zum anderen sind im dritten Schritt anstatt $\prod_{\pi\in\mathbb{N}_{\not\le}} |U_\pi|$ nur noch $\prod_{i=1}^{t} |U_{\pi_i}|$ viele Tupel $(\varepsilon_\pi)_{\pi\in N_3}$ zu untersuchen.

Grundlage der **zweiten** Modifikation ist die Beobachtung, daß für die sukzessive Konstruktion der Mengen $N_2^{(\nu)}$ im dritten Schritt des Verfahrens nicht notwendig alle $\pi \in N_3$ benötigt werden. Für $W \subseteq N_3$ beliebig definieren wir dazu den Graphen $\Gamma(W)$, dessen Eckenmenge N_2 sei und in dem zwei Ecken $\tau_1, \tau_2 \in N_2$ miteinander verbunden seien, sofern $\pi \in W$ existiert mit $\pi = \tau_1 \cup \tau_2$. Ist der Graph $\Gamma(W)$ zusammenhängend, so zeigt eine Inspektion des dritten Schrittes, daß es dort zur Berechnung von $\mathfrak{I}_\mathcal{K}(I,a)$ genügt, im zweiten Schritt für jedes $\pi \in W$ die Menge U_π zu bestimmen. Wir illustrieren diesen Sachverhalt an einem einfachen Beispiel.

Beispiel 2.4
Sei $n = 5$ mit $G \simeq C(5)$. Ist $G = \langle\sigma\rangle$, so gilt bei passender Numerierung der Konjugierten

$$\sigma^k \cdot i \equiv i + k \bmod 5 \qquad (0 \le k < 5, 1 \le i \le 5).$$

Es ist dann

$$\begin{aligned}\Omega_3 \;=\; \{\, & W_1 = \{\pi_1 = \{1,2,3\},\{2,3,4\},\{3,4,5\},\{1,4,5\},\{1,2,5\}\,\},\\ & W_2 = \{\pi_2 = \{1,2,4\},\{2,3,5\},\{1,3,4\},\{2,4,5\},\{1,3,5\}\}\},\end{aligned}$$

also $t(5, C(5)) = 2$.
Da $\Gamma(W_1)$ zusammenhängend ist, reicht es im zweiten Schritt, für jedes $\pi \in W_1$ die Menge U_π zu berechnen. Wir können etwa $N_2^{(1)}, \ldots, N_2^{(5)}$ wie folgt wählen, wobei wir die Bezeichnungen aus dem Iterationsschritt von Seite 36 verwenden:

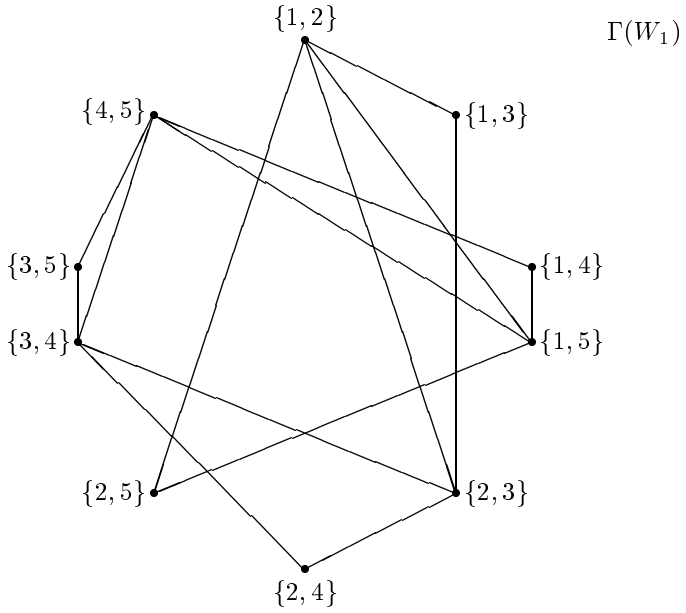
$\nu = 1:\ \pi = \{1,2,3\}$
$\quad\Longrightarrow N_2^{(1)} = \{\{1,2\},\{1,3\},\{2,3\}\}.$

$\nu = 2:\ \tau = \{2,3\}, \tau' = \{2,4\} \Longrightarrow \pi = \{2,3,4\}$
$\quad\Longrightarrow N_2^{(2)} = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}.$

$\nu = 3:\ \tau = \{3,4\}, \tau' = \{3,5\} \Longrightarrow \pi = \{3,4,5\}$
$\quad\Longrightarrow N_2^{(3)} = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\},\{3,5\},\{4,5\}\}.$

$\nu = 4:\ \tau = \{4,5\}, \tau' = \{1,5\} \Longrightarrow \pi = \{1,4,5\}$
$\quad\Longrightarrow N_2^{(4)} = \{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{3,4\},\{3,5\},\{4,5\}\}.$

$\nu = 5: \ \tau = \{1,2\}, \tau' = \{2,5\} \Longrightarrow \pi = \{1,2,5\}$
$\Longrightarrow N_2^{(5)} = N_2.$



Kombinieren wir dieses Vorgehen mit der ersten Modifikation, so genügt es wegen $W_1 = G \cdot \pi_1$*, im zweiten Schritt die Menge* U_{π_1} *zu berechnen.*

Sei nun $u = u(n,G) \in \mathbb{N}$ minimal mit der Eigenschaft, daß für passende $i_1, \ldots, i_u \in \{1, \ldots, t\}$ der Graph $\Gamma(W_{i_1} \cup \ldots \cup W_{i_u})$ zusammenhängend ist. Aufgrund der ersten Modifikation ist es dann ausreichend, im zweiten Schritt jeweils u viele Einheitengleichungen zu lösen. Im dritten Schritt sind dementsprechend $|U_{\pi_{i_1}}| \cdots |U_{\pi_{i_u}}|$ viele Tupel $(\varepsilon_\pi)_{\pi \in N_3}$ zu untersuchen.

Für alle möglichen Kombinationen von $n \leq 12$ und $|G| < 20$ liefert die Tabelle auf der nächsten Seite eine Übersicht der Werte von $t(n,G)$ und $u(n,G)$, wobei die Namen der Galoisgruppen aus [8] übernommen wurden.

Die Schritte 2 und 3 aus unserer Ausarbeitung von Győrys Methode setzen wir nun bei der Fortsetzung des Beispiels 2.2 ein.

Beispiel 2.5 (Fortsetzung von 2.2)
Entsprechend den schon erzielten Ergebnissen verbleibt die Bestimmung von $\mathfrak{I}_\mathcal{K}(I)$ *für* $I \in \{5,7\}$*. Ist* $I = 5$*, so sind 4004 Einheitengleichungen im zweiten Schritt zu lösen. Bei den meisten dieser Gleichungen kann man sehr schnell anhand des Kriteriums aus 1.27 feststellen, daß sie keine Lösungen besitzen. Lediglich für eine Einheitengleichung müssen alle drei Schritte des Verfahrens aus dem ersten Kapitel durchgeführt werden. Da aus den Lösungen dieser Gleichungen kein* $\alpha \in \mathfrak{o}_\mathcal{K}$ *mit* $(\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) = \not\exists$ *konstruiert werden kann, gilt* $\mathfrak{I}_\mathcal{K}(5) = \emptyset$*. Die für dieses Ergebnis notwendige Rechenzeit betrug insgesamt 743s. Davon entfallen 139 Sekunden auf den zweiten Schritt, also auf das Lösen der Einheitengleichung, weniger als eine*

n	G	$\|G\|$	$t(n,G)$	$u(n,G)$
3	A_3	3	1	1
	S_3	6	1	1
4	$C(4)$	4	1	1
	$E(4)$	4	1	1
	$D(4)$	8	1	1
5	$C(5)$	5	2	1
	$D(5)$	10	2	1
6	$C(6)$	6	4	2
	$D_6(6)$	6	4	2
	$D(6)$	12	3	1
	$A_4(6)$	12	4	2
	$F_{18}(6)$	18	2	1
7	$C(7)$	7	5	2
	$D(7)$	14	4	1
8	$C(8)$	8	7	2
	$4[\times]2$	8	7	3
	$E(8)$	8	7	3
	$D_8(8)$	8	7	3
	$Q_8(8)$	8	7	3
	$D(8)$	16	5	2
	$\frac{1}{2}[2^3]4$	16	5	2
	$2D_8(8)$	16	5	2
	$E(8):2$	16	5	2
	$[2^4]2$	16	5	2
	$\frac{1}{2}[2^3]E(4)$	16	5	2
9	$C(9)$	9	10	≤ 3
	$E(9)$	9	12	≤ 4
	$D(9)$	18	7	2
	$S(3)[\times]3$	18	8	2
	$S(3)[\frac{1}{2}]S(3)$	18	8	2
10	$C(10)$	10	12	≤ 4
	$D(10)$	10	12	≤ 4
11	$C(11)$	11	15	≤ 4
12	$C(4)[\times]C(3)$	12	19	≤ 5
	$E(4)[\times]C(3)$	12	19	≤ 5
	$D_6(6)[\times]2$	12	19	≤ 5
	$A_4(12)$	12	21	≤ 6
	$\frac{1}{2}[3:2]4$	12	19	≤ 5

Sekunde auf den dritten Schritt und der große Rest auf den ersten Schritt, d.h. die Bestimmung vom A.

Es ist jetzt bereits $i_{\mathcal{K}} = 7$ bekannt. Wie im Fall $I = 5$ kann für den Großteil der 5005 Einheitengleichungen, welche zur expliziten Berechnung von $\mathfrak{I}_{\mathcal{K}}(7)$ zu betrachten sind, leicht entschieden werden, daß sie keine Lösungen besitzen. Aus den restlichen zehn Einheitengleichungen, welche mit den Methoden des ersten Kapitels gelöst werden müssen, ergibt sich für $\mathfrak{I}_{\mathcal{K}}(7)$ das folgende 25-elementige Vetretersystem:

$$\begin{aligned}\mathfrak{I}_{\mathcal{K}}(7) = \{\ & \omega_4 + \omega_5, \quad 4\,\omega_3 - 3\,\omega_4 - 4\,\omega_5, \quad \omega_2, \quad \omega_2 + \omega_3 - \omega_4 - \omega_5,\\ & 2\,\omega_2 - 3\,\omega_3 + 2\,\omega_4 + 3\,\omega_5, \quad 2\,\omega_2 + \omega_3 - \omega_4 - \omega_5, \quad 2\,\omega_2 + 6\,\omega_3 - 5\,\omega_4 - 6\,\omega_5,\\ & 3\,\omega_2 - 3\,\omega_3 + \omega_4 + 2\,\omega_5, \quad 3\,\omega_2 - 3\,\omega_3 + 2\,\omega_4 + 3\,\omega_5, \quad 3\,\omega_2 - 2\,\omega_3 + \omega_4 + 2\,\omega_5,\\ & 4\,\omega_2 - 3\,\omega_3 + \omega_4 + 2\,\omega_5, \quad 4\,\omega_2 - 2\,\omega_3 + \omega_4 + 2\,\omega_5, \quad 5\,\omega_2 - 2\,\omega_3 + \omega_5,\\ & 5\,\omega_2 - 2\,\omega_3 + \omega_4 + 2\,\omega_5, \quad 6\,\omega_2 - 6\,\omega_3 + 3\,\omega_4 + 5\,\omega_5, \quad 6\,\omega_2 - 2\,\omega_3 + \omega_5,\\ & 7\,\omega_2 - 6\,\omega_3 + 3\,\omega_4 + 5\,\omega_5, \quad 8\,\omega_2 - 5\,\omega_3 + 2\,\omega_4 + 4\,\omega_5,\\ & 9\,\omega_2 - 5\,\omega_3 + 2\,\omega_4 + 4\,\omega_5, \quad 10\,\omega_2 - 9\,\omega_3 + 4\,\omega_4 + 7\,\omega_5,\\ & 13\,\omega_2 - 7\,\omega_3 + 3\,\omega_4 + 6\,\omega_5, \quad 14\,\omega_2 - 12\,\omega_3 + 7\,\omega_4 + 11\,\omega_5,\\ & 15\,\omega_2 - 8\,\omega_3 + 3\,\omega_4 + 6\,\omega_5, \quad 22\,\omega_2 - 13\,\omega_3 + 4\,\omega_4 + 9\,\omega_5,\\ & 23\,\omega_2 - 11\,\omega_3 + 3\,\omega_4 + 8\,\omega_5\ \}.\end{aligned}$$

Die Rechenzeit betrug insgesamt 1442s mit 779s für den zweiten Schritt und etwa einer Sekunde für den dritten Schritt.

Eine Inspektion des Resultats zeigt im übrigen, daß $\mathfrak{o}_{\mathcal{K}}$ genau 2 Klassen nichtisomorpher Gleichungsordnungen vom Index 7 besitzt. Die Ordnungen der ersten Klasse besitzen modulo $\mathbb{Z}$-Äquivalenz 2 Potenzbasiserzeuger, während die Ordnungen der zweiten Klasse jeweils über 3 Potenzbasiserzeuger modulo $\mathbb{Z}$-Äquivalenz verfügen.

Neben diesem Beispiel haben wir mit Győrys Methode Indexformgleichungen in Kreisteilungskörpern und ihren maximalen reellen Teilkörpern gelöst. Und zwar bestimmten wir dort jeweils alle Potenzganzheitsbasen modulo $\mathbb{Z}$-Äquivalenz, d.h. genauer, wir berechneten $\mathfrak{I}_{\mathcal{K}_m}(1)$ und $\mathfrak{I}_{\mathcal{K}_m^+}(1)$ für alle $m \in \mathbb{N}, \gg \not\equiv \not\models \bmod \not\supseteq$, mit $[\mathcal{K}_m : \mathbb{Q}] \leq \not\Vdash\not\models$, wobei an die im Unterabschnitt 1.3.2 eingeführte Notation für Kreisteilungskörper erinnert sei. Die Ergebnisse dieser Rechungen sind in der Tabelle auf Seite 43 festgehalten.

Für Kreisteilungskörper höheren Grades ist der Einsatz von Győrys Methode sehr aufwendig (siehe etwa $\mathbb{Q}(\zeta_{\not\Vdash\not\models})$ in der Tabelle). Die Ursache hierfür liegt sowohl im zweiten Schritt, also dem Lösen der Einheitengleichungen, als auch bei der Kombination der $u(n, G)$ vielen Mengen U_π im dritten Schritt, wobei die Mächtigkeit dieser Mengen mit wachsendem Einheitenrang erfahrungsgemäß stark zunimmt.

Für spezielle Kreisteilungskörper, nämlich dann, wenn m eine Primzahl ist, kann allerdings ein von Niklasch [39, Abschnitt II-4.3] entwickeltes Verfahren eingesetzt werden, welches anhand der Ausnahmeeinheiten alle Potenzganzbasen von $\mathcal{K}_m$ modulo $\mathbb{Z}$-Äquivalenz bestimmt. Der große Vorteil dieses Verfahrens besteht darin, daß

m	$[\mathcal{K}_m^+ : \mathbb{Q}]$	$\lvert\mathfrak{J}_{\mathcal{K}_m^+}(1)\rvert$	t	$[\mathcal{K}_m : \mathbb{Q}]$	$\lvert\mathfrak{J}_{K_m}(1)\rvert$	t
1	1	1	–	1	1	–
3	1	1	–	2	1	–
4	1	1	–	2	1	–
5	2	1	–	4	6	0s
7	3	9	3s	6	9	15s
8	2	1	–	4	2	0s
9	3	6	2s	6	9	50s
11	5	25	47s	10	15	2900s
12	2	1	–	4	4	0s
13	6	36	2576s	12	18	34195s
15	4	12	27s	8	16	891s
16	4	6	24s	8	4	303s
20	4	10	23s	8	8	951s
21	6	30	1750s	12	24	32872s
24	4	6	27s	8	8	804s
28	6	15	639s	12	12	31004s
36	6	15	681s	12	12	21066s

sein Aufwand linear ist in der Anzahl der Ausnahmeeinheiten. Wir werden dieses Verfahren jetzt kurz darstellen und damit alle Potenzganzheitsbasen von $\mathbb{Q}(\zeta_{\not\equiv\not\diamond})$, $\mathbb{Q}(\zeta_{\not\equiv\not\to})$ und $\mathbb{Q}(\zeta_{\not=\not\equiv})$ berechnen.

Für eine beliebige Primzahl $p > 3$ sei ζ_p eine primitive p-te Einheitswurzel. Die Konjugierten von ζ_p seien numeriert als $\zeta_p^{(j)} = \zeta_p^j$ $(1 \le j < p)$.
Wir setzen $\varpi := 1 - \zeta_p$. Für jedes $k \in \{1, \ldots, p-1\}$ ist $1 - \zeta_p^{(k)}$ assoziiert zu ϖ wegen $\mathrm{N}(1 - \zeta_p^k) = \mathrm{N}(1 - \zeta_p)$ und

$$\frac{1 - \zeta_p^k}{1 - \zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{k-1} \in \mathfrak{o}_{\mathcal{K}_p}.$$

Also ist für $i, j \in \{1, \ldots, p-1\}$, $i \ne j$, beliebig auch $\zeta_p^{(i)} - \zeta_p^{(j)}$ assoziiert zu ϖ wegen

$$\zeta_p^{(i)} - \zeta_p^{(j)} = \zeta_p^i\,(1 - \zeta_p^{j-i}).$$

Sei $\alpha \in \mathfrak{J}_{\mathcal{K}_p}(1)$ beliebig, aber fest gewählt. Gemäß (2-2) und (2-4) ist $\alpha^{(i)} - \alpha^{(j)}$ für $i, j \in \{1, \ldots, p-1\}$, $i \ne j$, assoziiert zu $\zeta_p^{(i)} - \zeta_p^{(j)}$, und damit auch assoziiert zu ϖ. Für jedes $k \in \mathbb{Z}, \not| \neg$, ist somit

$$\omega_k := \frac{\alpha^{(k)} - \alpha^{(1)}}{\alpha^{(-1)} - \alpha^{(1)}} \tag{2-15}$$

eine Einheit in $\mathfrak{o}_{\mathcal{K}_p}$, wobei die Konjugierten in (2-15) modulo p zu lesen sind — eine Konvention, die wir im folgenden beibehalten. Für $j, k \in \mathbb{Z}, p \not| jk$, gilt dann

$$\omega_k^{(j)} = \frac{\omega_{jk} - \omega_j}{\omega_{-j} - \omega_j},$$

also weiter

$$\omega_{jk} = (\omega_{-j} - \omega_j)\,\omega_k^{(j)} + \omega_j, \tag{2-16}$$

und für $j = -1$ speziell

$$\omega_{-k} + \omega_k^{(-1)} = 1. \tag{2-17}$$

Sei nun $g \in \mathbb{N}$ eine primitive Wurzel modulo p, d.h. $g^i \not\equiv g^j \bmod p$ $(0 \le i < j < p-1)$. Da ω_g nach (2-17) eine Ausnahmeeinheit ist, können alle Möglichkeiten für ω_g durch die Berechnung von $\mathrm{X}_{\mathcal{K}_p}$ durchlaufen werden. Wir werden nun sehen, daß α modulo $\mathbb{Z}$-Äquivalenz allein durch Vorgabe von ω_g rekonstruiert werden kann. Dazu bestimmen wir zuerst ω_{-g} anhand von (2-17) und danach mittels (2-16) schrittweise

$$\begin{aligned}
\omega_{g^2} &= (\omega_{-g} - \omega_g)\,\omega_g^{(g)} + \omega_g,\\
\omega_{g^3} &= (\omega_{-g} - \omega_g)\,\omega_{g^2}^{(g)} + \omega_g,\\
&\vdots \qquad\qquad \vdots\\
\omega_{g^{p-2}} &= (\omega_{-g} - \omega_g)\,\omega_{g^{p-3}}^{(g)} + \omega_g.
\end{aligned}$$

Wir setzen α an als $\alpha = a_2\zeta_p + \cdots + a_{p-1}\zeta_p^{p-2}$ mit Unbekannten $a_2, \ldots, a_{p-1} \in \mathbb{Z}$. Ferner sei $\alpha^{(-1)} - \alpha^{(1)} = \varepsilon\,\varpi$ mit einer noch unbekannten Einheit $\varepsilon \in \mathfrak{o}_{\mathcal{K}_p}$. Setzen wir

$$A := \begin{pmatrix} \zeta_p^2 - \zeta_p & \zeta_p^4 - \zeta_p^2 & \cdots & \zeta_p^{(p-2)\cdot 2} - \zeta_p^{p-2} \\ \vdots & & & \vdots \\ \zeta_p^{p-1} - \zeta_p & \zeta_p^{2(p-1)} - \zeta_p^2 & \cdots & \zeta_p^{(p-2)(p-1)} - \zeta_p^{p-2} \end{pmatrix},$$

so ist A regulär wegen $\det^2 A = \mathrm{disc}_{\mathcal{K}_p}$. Aus

$$\begin{pmatrix} \varepsilon\varpi\omega_2 \\ \vdots \\ \varepsilon\varpi\omega_{p-1} \end{pmatrix} = A \cdot \begin{pmatrix} a_2 \\ \vdots \\ a_{p-1} \end{pmatrix}$$

folgt dann weiter

$$A^{-1} \begin{pmatrix} \varpi\omega_2 \\ \vdots \\ \varpi\omega_{p-1} \end{pmatrix} = \begin{pmatrix} \varepsilon^{-1}\,a_2 \\ \vdots \\ \varepsilon^{-1}\,a_{p-1} \end{pmatrix},$$

wodurch ε und $a_2, \ldots, a_{p-1} \in \mathbb{Z}$ eindeutig bis aufs Vorzeichen festgelegt sind.

Anhand der im letzten Kapitel erzielten Resultate zu Ausnahmeeinheiten in Kreisteilungskörpern haben wir mit diesem Verfahren alle Potenzganzheitsbasen in $\mathbb{Q}(\zeta_{\not\vdash\not\vdash})$, $\mathbb{Q}(\zeta_{\not\vdash\twoheadrightarrow})$ und $\mathbb{Q}(\zeta_{\not=\not\vdash})$ bestimmt. Die Ergebnisse dieser Rechnungen und die der Tabelle von Seite 43 entsprechen einer von Bremner [7] geäußerten Vermutung, welche bislang nur für $p \le 7$ verifiziert war:

Vermutung 2.6 (Bremner)
Sei $\zeta_p' \in \mathfrak{o}_{\mathcal{K}_p}$ definiert durch $\zeta_p' := \zeta_p + \cdots + \zeta_p^{(p-1)/2}$. Dann existiert zu jedem $\alpha \in \mathfrak{I}_{\mathcal{K}_p}(1)$ ein Automorphismus σ aus der Galoisgruppe von $\mathcal{K}_p/\mathbb{Q}$, so daß α entweder $\mathbb{Z}$-äquivalent ist zu $\sigma(\zeta_p)$ oder zu $\sigma(\zeta_p')$.

Kapitel 3

Ganze Punkte auf Mordellschen Kurven

Zu Beginn dieses Jahrhunderts zeigte Mordell [32, 33], daß die ganzen Punkte einer elliptischen Kurve über $\mathbb{Q}$ sich aus den Lösungen endlich vieler Thue-Gleichungen ergeben. Die ersten expliziten Schranken für die Lösungen von Thue-Gleichungen wurden rund 55 Jahre später von Baker hergeleitet [1]. Indem Baker sein Ergebnis mit den alten Resultaten Mordells kombinierte, erhielt er erstmals explizite Schranken [2, 3] für die ganzen Punkte auf einer elliptischen Kurve über $\mathbb{Q}$. Da diese Schranken für eine direkte Bestimmung der ganzen Punkte zu groß sind, benutzt man stattdessen für praktische Rechnungen bislang zwei andere Verfahren. Bei dem älteren dieser Verfahren [53, 54, 57] erhält man alle ganzen Punkte aus den Lösungen eines Systems quartischer Thue-Gleichungen, zu welchem man über eine Idealgleichung in einem kubischen Zahlkörper gelangt. Das System quartischer Thue-Gleichungen ist dabei gänzlich verschieden von den Thue-Gleichungen, welche Mordell und Baker in ihren Arbeiten betrachteten. Nachteilig bei dieser Methode ist es, daß die Koeffizienten der zu lösenden quartischen Thue-Gleichungen oftmals sehr groß sind. Dies führt häufig dazu, daß das Verfahren in der Praxis nicht durchführbar ist [56]. Das jüngere, auf Lang und Zagier zurückgehende Verfahren, welches von Gebel, Pethő und Zimmer [22] sowie von Stroeker und Tzanakis [55] zu einem Algorithmus ausgearbeitet wurde, basiert auf Linearformen in elliptischen Logarithmen und setzt die Kenntnis einer Basis der Mordell-Weil-Gruppe der elliptischen Kurve voraus. Ist eine solche Basis bekannt, so hat sich dieses Verfahren in der Praxis als deutlich effizienter erwiesen als der ältere Ansatz über ein System quartischer Thue-Gleichungen. Allerdings ist die Bestimmung einer Basis der Mordell-Weil-Gruppe oftmals schwierig und kann in vielen Fällen nur anhand der bislang unbewiesenen Vermutung von Birch und Swinnerton-Dyer erfolgen.

In diesem Kapitel wird ein neues und sehr einfaches Verfahren zur Bestimmung der ganzen Punkte einer Mordellschen Kurve über $\mathbb{Q}$ vorgestellt, mit welchem etliche Beispiele gerechnet werden konnten, bei denen die beiden bislang bekannten Methoden scheiterten. Unser Verfahren beruht im wesentlichen auf Ideen, welche in den eingangs genannten Arbeiten Mordells enthalten sind, und kombiniert diese mit

Methoden zum Lösen von Indexformgleichungen in kubischen Zahlkörpern.

Bei der Formulierung des Verfahrens werden wir zwei Polynome $f(t), g(t) \in \mathbb{Z}[\approx]$ als $\mathbb{Z}$-äquivalent bezeichnen, falls $\gamma \in \mathbb{Z}$ existiert mit $f(t) = \pm g(\pm t + \gamma)$. Wir weisen darauf hin, daß für zwei $\mathbb{Z}$-äquivalente algebraische Zahlen $\alpha, \beta \in \mathbb{C}$ ihre Minimalpolynome dann gleichfalls $\mathbb{Z}$-äquivalent sind.

Eine Mordellsche Kurve ist eine elliptische Kurve der Gestalt $E_k : y^2 = x^3 + k$ mit $k \in \mathbb{Z}$, $k \neq 0$. Die ganzen Punkte von E_k sind gegeben durch die Menge

$$\mathfrak{L}_k = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \curvearrowright^{\not\vDash} = \curvearrowleft^{\not\vDash} + \urcorner\}.$$

Für jedes $(x, y) \in \mathfrak{L}_k$ gilt nach Baker [2] die Abschätzung

$$\max\bigl(|x|, |y|\bigr) < \exp\left(\bigl(10^{10}|k|\bigr)^{10^4}\right).$$

Grundlage für unser Verfahren zur Bestimmung von $\mathfrak{L}_k$ ist die Beobachtung Mordells, daß für jedes $(x, y) \in \mathfrak{L}_k$ die Diskriminante von $t^3 - 3xt - 2y \in \mathbb{Z}[\approx]$ stets $-108\,k$ ist. Definieren wir P_k als die Menge aller normierten kubischen Polynome aus $\mathbb{Z}[\approx]$ mit Diskriminante $-108\,k$ und wählen wir als Vertretersystem für P_k bzgl. $\mathbb{Z}$-Äquivalenz die Menge

$$\bar{P}_k := \bigl\{t^3 + a_1t^2 + a_2t + a_3 \in P_k \mid a_1 = 1 \vee (a_1 = 0 \wedge a_3 \geq 0)\bigr\},$$

so gilt also $t^3 - 3xt - 2y \in \bar{P}_k$ für alle $(x, y) \in \mathfrak{L}_k$ mit $y \leq 0$. Zur Berechnung von $\mathfrak{L}_k$ reicht es demnach, die Menge $\bar{P}_k$ zu bestimmen, die, wie wir gleich sehen werden, endlich ist.

Es sei R_k die Menge der reduziblen und I_k die Menge der irreduziblen Polynome aus P_k. Ist $f(t) \in R_k$, so existiert zu $f(t)$ ein $\mathbb{Z}$-äquivalentes Polynom $g(t) \in P_k$ der Gestalt $g(t) = t(t^2 + at + b)$. Es ist dann $-108\,k = \operatorname{disc} g = b^2(a^2 - 4b)$, woraus man leicht die höchstens endlich vielen Möglichkeiten für $g(t)$ erhält. Aus ihnen ergeben sich unmittelbar alle reduziblen Vertreter von $\bar{P}_k$.

Um die irreduziblen Vertreter von $\bar{P}_k$ zu ermitteln, werden wir zunächst eine endliche Menge $\mathfrak{K}$ kubischer Zahlkörper bestimmen, so daß zu jedem $f(t) \in I_k$ ein Zahlkörper $\mathcal{K} \in \mathfrak{K}$ existiert, welcher eine Nullstelle von $f(t)$ enthält. Unter der Bestimmung eines Zahlkörpers verstehen wir dabei stets die Angabe eines erzeugenden Polynoms und die Berechnung seiner Maximalordnung. Das folgende, auf einem Resultat von Pohst [42] beruhende Lemma liefert uns die Menge $\mathfrak{K}$.

Lemma 3.1
Sei $f(t) \in I_k$ mit einer Nullstelle $\rho \in \mathbb{C}$. Dann existiert $\theta \in \mathbb{Z}[\rho]$, $\theta \notin \mathbb{Z}$, mit

$$\mathrm{T}_2(\theta) \leq \sqrt{\frac{2}{3}|108\,k|}, \tag{3-1}$$

wobei $\mathrm{T}_2(\theta)$ die in der Einleitung auf Seite 3 definierte T_2-Norm von θ ist. Für die Koeffizienten des Minimalpolynoms $m_\theta(t) = t^3 + a_1t^2 + a_2t + a_3 \in \mathbb{Z}[\approx]$ von θ gelten

$$a_1 \in \{0, 1\}, \qquad |a_2| \leq \frac{\mathrm{T}_2(\theta) + 1}{2}, \qquad |a_3| \leq \left(\frac{\mathrm{T}_2(\theta)}{3}\right)^{3/2}. \tag{3-2}$$

Insbesondere ist

$$\operatorname{disc} m_\theta = (\mathbb{Z}[\rho] : \mathbb{Z}[\theta])^2 \cdot (-108\,k). \tag{3-3}$$

Zur Bestimmung von $\mathfrak{K}$ kann man nun so vorgehen, daß man für jedes Polynom $t^3 + a_1 t^2 + a_2 t + a_3 \in \mathbb{Z}[\approx]$, dessen Koeffizienten die Bedingungen aus (3-2) erfüllen, testet, ob es irreduzibel ist und ob seine Diskriminante gemäß (3-3) ein ganzzahliges quadratisches Vielfaches von $-108\,k$ ist, und bei Bestehen dieses Tests den von f erzeugten Zahlkörper in $\mathfrak{K}$ abspeichert. Nachteilig bei diesem Vorgehen ist es, daß $O(|k|^{5/4})$ viele kubische Polynome getestet werden müssen, wodurch wir bei größeren Werten von k schnell an die Grenze der praktischen Durchführbarkeit stoßen. Um diesen Nachteil zumindest etwas abzuschwächen, gehen wir bei der Bestimmung von $\mathfrak{K}$ in der Praxis geringfügig anders vor. Seien dazu $f(t)$ mit ρ und θ wie in 3.1 gegeben.

Lemma 3.2
Es ist $(\mathbb{Z}[\rho] : \mathbb{Z}[\theta]) \le \mathbb{C}$, *wobei* $C \in \mathbb{N}$ *definiert sei durch*

$$C := \left\lfloor 2 \left(\frac{2}{3}\right)^{3/4} |108\,k|^{1/4} \right\rfloor .$$

Beweis Aus

$$\begin{aligned} \operatorname{disc} m_\theta &= \left((\theta^{(1)} - \theta^{(2)})(\theta^{(1)} - \theta^{(3)})(\theta^{(2)} - \theta^{(3)})\right)^2 \\ &= \left(\theta^{(2)}{\theta^{(1)}}^2 - \theta^{(1)}{\theta^{(2)}}^2 + \theta^{(3)}{\theta^{(2)}}^2 - \theta^{(3)}{\theta^{(1)}}^2 + \theta^{(1)}{\theta^{(3)}}^2 - \theta^{(2)}{\theta^{(3)}}^2\right)^2. \end{aligned}$$

folgt unmittelbar $|\operatorname{disc} m_\theta| \le 4\,\mathrm{T}_2(\theta)^3$, woraus sich mit (3-1) und (3-3) die Behauptung ergibt. □

Die Indexabschätzung aus 3.2 gestattet es, zur Bestimmung von $\mathfrak{K}$ alle möglichen Kombinationen von a_1, a_2 und $(\mathbb{Z}[\rho] : \mathbb{Z}[\theta])$ durchzuprobieren, und den Koeffizienten a_3 jeweils anhand der quadratischen Gleichung

$$(\mathbb{Z}[\rho] : \mathbb{Z}[\theta])^2 \cdot (-108\,k) = -4a_1^3a_3 + (a_1^2a_2^2 - 4a_2^3)a_3 + a_2^4a_1^2 - 4a_2^5 \tag{3-4}$$

zu berechnen. Geht man auf diese Weise vor, so sind $O(|k|^{3/4})$ viele quadratische Gleichungen zu lösen, was in der Praxis deutlich effizienter ist, als das zuerst erwähnte Durchprobieren aller nach (3-2) und (3-3) möglichen Polynome.

Nach der Berechnung von $\mathfrak{K}$ besteht der zweite und abschließende Schritt zur Ermittlung der irreduziblen Vertreter von $\bar{P}_k$ darin, eben diese Vertreter durch das Lösen von Indexformgleichungen in kubischen Zahlkörpern aus $\mathfrak{K}$ zu berechnen. Seien dazu $\mathcal{K} \in \mathfrak{K}$ beliebig und $f(t) \in I_k$ mit einer in $\mathcal{K}$ liegenden Nullstelle ρ gegeben. Wegen

$$-108\,k = \operatorname{disc} m_\rho = (\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\rho])^2 \operatorname{disc}_\mathcal{K}$$

besitzt $\mathbb{Z}[\rho]$ dann den Index

$$(\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\rho]) = \sqrt{\frac{-108\,k}{\operatorname{disc}_\mathcal{K}}}.$$

Die Ermittlung derjenigen Vertreter aus $\bar{P}_k$, welche eine Nullstelle in $\mathcal{K}$ besitzen, ist also gleichbedeutend zur Bestimmung der Menge $I_{\mathcal{K}}(\sqrt{\frac{-108\,k}{\mathrm{disc}_{\mathcal{K}}}})$. Zu deren Berechnung setzt man in der Praxis aus Effizienzgründen allerdings nicht die im zweiten Kapitel beschriebene Methode Győrys ein, sondern man löst hierzu stattdessen eine kubische Thue-Gleichung [20]. Wird nämlich $\mathcal{K}$ durch das Polynom $t^3 + a_1 t^2 + a_2 t + a_3 \in \mathbb{Z}[\approx]$ mit Nullstelle θ erzeugt, und ist

$$\omega_1 = 1, \qquad \omega_2 = \frac{a_{12} + \theta}{d_2}, \qquad \omega_3 = \frac{a_{13} + a_{23}\theta + \theta^2}{d_3}$$

eine Ganzheitsbasis von $\mathfrak{o}_{\mathcal{K}}$ ($a_{12}, a_{13}, a_{23} \in \mathbb{Z}, \not\approx, \not\asymp \in \mathbb{N}$), so erhält man als Indexform von $\mathcal{K}$ bzgl. der Basis $\omega_1, \omega_2, \omega_3$ die Form

$$\begin{aligned} I_{\mathcal{K}}(X,Y) \;=\; & \frac{d_3}{d_2^2}\,X^3 \;+\; \frac{3d_3^2 d_2 a_{23} - 2d_2 d_3^2 a_1}{d_2^2 d_3^2}\,X^2Y \\ & + \frac{-4d_2^2 d_3 a_{23} a_1 + 3d_3 d_2^2 a_{23}^2 + d_2^2 d_3 a_2 + d_2^2 d_3 a_1^2}{d_2^2 d_3^2}\,XY^2 \\ & + \frac{d_2^3 a_{23} a_1^2 + d_2^3 a_3 + d_2^3 a_{23}^3 - 2d_2^3 a_{23}^2 a_1 - d_2^3 a_1 a_2 + d_2^3 a_{23} a_2}{d_2^2 d_3^2}\,Y^3. \end{aligned} \tag{3-5}$$

Also ist für jedes $z + x\,\omega_2 + y\,\omega_3 \in \mathfrak{I}_{\mathcal{K}}\left(\sqrt{\frac{-108\,k}{\mathrm{disc}_K}}\right)$ der Tupel (x, y) eine Lösung der kubischen Thue-Gleichung

$$I_{\mathcal{K}}(X,Y) = \pm\sqrt{\frac{-108\,k}{\mathrm{disc}_K}}. \tag{3-6}$$

Zum effektiven Lösen der Thue-Gleichung (3-6) benötigt man Resultate Bakers zu unteren Schranken für Linearformen in den Logarithmen algebraischer Zahlen. Detailliertere Informationen hierzu sowie einen sehr effizienten Algorithmus zum Lösen von Thue-Gleichungen findet der Leser in [6]. Wir bemerken an dieser Stelle nur, daß das Lösen einer Thue-Gleichung in der Praxis problemlos ist, sofern im zugrunde liegenden Zahlkörper ein Grundeinheitensystem bekannt ist und dort die zur Thue-Gleichung korrespondierende Normgleichung gelöst werden kann.

Unser Vorgehen zur Berechnung der ganzen Punkte von E_k fassen wir in einem Algorithmus zusammen, dem wir zwei Beispiele folgen lassen werden. Für $f(t) \in P_k$ bezeichnen wir innerhalb des Algorithmus mit $\overline{f(t)}$ den entsprechenden Vertreter aus $\bar{P}_k$.

Algorithmus 3.3
Eingabe: $k \in \mathbb{Z}, \daleth \neq \aleph$.
Ausgabe: $\mathfrak{L}_k = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid \curvearrowright^{\not\asymp} = \curvearrowleft^{\not\asymp} + \daleth\}$.

Schritt 1

$\bar{P}_k \leftarrow \emptyset$.

Schritt 2 (Berechung der reduziblen Vertreter aus $\bar{P}_k$)

`foreach` $b \in \mathbb{Z}$ mit $b^2 \mid -108\,k$ `do`
Falls $a \in \mathbb{Z}$ existiert mit $-108\,k = b^2(a^2 - 4b)$ existiert,
so setze $\bar{P}_k \leftarrow \bar{P}_k \cup \{\overline{t(t^2 + at + b)}\}$.
`end`

Schritt 3 (Berechnung von $\mathfrak{K}$)

$\mathfrak{K} \leftarrow \emptyset$.
$A_2 \leftarrow \lfloor \frac{1}{2}(\sqrt{\frac{2}{3}|108\,k|}+1)\rfloor$.
$C \leftarrow \lfloor 2\left(\frac{2}{3}\right)^{3/4}|108\,k|^{1/4}\rfloor$.
`foreach` $(a_1,a_2,c) \in \{0,1\}\times\{-A_2,\ldots,A_2\}\times\{1,\ldots,C\}$ `do`
Falls $a_3 \in \mathbb{Z}$ existiert mit $\mathrm{disc}(t^3+a_1t^2+a_2t+a_3) = c^2(-108\,k)$ und falls $t^3+a_1t^2+a_2t+a_3$ irreduzibel ist, so setze $\mathfrak{K} \leftarrow \mathfrak{K}\cup\{\mathcal{K}\}$, wobei $\mathcal{K}$ der von einer Nullstelle von $t^3+a_1t^2+a_2t+a_3$ erzeugte Zahlkörper sei.
`end`

Schritt 4 (Berechung der irreduziblen Vertreter aus $\bar{P}_k$)

`foreach` $\mathcal{K} \in \mathfrak{K}$ `do`
`foreach` $\rho \in I_{\mathcal{K}}\left(\sqrt{\frac{-108k}{\mathrm{disc}_{\mathcal{K}}}}\right)$ `do`
$\bar{P}_k \leftarrow \bar{P}_k \cup \{\overline{m_\rho}\}$.
`end`
`end`

Schritt 5 (Berechnung von $\mathfrak{L}_k$)

$\mathfrak{L}_k \leftarrow \emptyset$.
`foreach` $t^3+a_1t^2+a_2t+a_3 \in \bar{P}_k$ `do`
Falls $a_1 = 0$ und $3 \mid a_2$ und $2 \mid a_3$, so setze $\mathfrak{L}_k \leftarrow \mathfrak{L}_k \cup \{(\frac{a_2}{3}, \pm\frac{a_3}{2})\}$.
`end`

Beispiel 3.4
Wir betrachten die Kurve $y^2 = x^3 - 999$, *also* $k = -999$.

Wegen $-108\,k = 2^2\,3^6\,37 = 107892$ *muß für jedes* $t(t^2+at+b) \in R_{-999}$ *der Koeffizient* b *ein Teiler von* $2\cdot 3^3 = 54$ *sein. Eine einfache Rechnung liefert für* $t(t^2+at+b)$ *die Lösungen* $t(t^2+36t-9)$ *und* $t(t^2+16t+27)$, *so daß die reduziblen Vertreter aus* $\bar{P}_{-999}$ *gegeben sind durch* $t^3-441t+3564$ *und* $t^3+t^2-58t+140$.

Zur Bestimmung von $\mathfrak{K}$ *berechnen wir zuerst die Schranken* A_2 *und* C *aus Schritt 3 in 3.3. Es ist* $A_2 = 134$ *und* $C = 26$. *Aus der Suchschleife erhalten wir dann als mögliche erzeugende Polynome für Körper aus* $\mathfrak{K}$ *die folgenden sieben Kandidaten:*

$$\begin{aligned}
f_1(t) &= t^3-120t+502 \qquad (\mathrm{disc}\, f_1 = 107892),\\
f_2(t) &= t^3-120t+16 \qquad (\mathrm{disc}\, f_2 = 8^2\,107892),\\
f_3(t) &= t^3-90t+90 \qquad (\mathrm{disc}\, f_3 = 5^2\,107892),\\
f_4(t) &= t^3-84t+268 \qquad (\mathrm{disc}\, f_4 = 2^2\,107892),\\
f_5(t) &= t^3-48t+20 \qquad (\mathrm{disc}\, f_5 = 2^2\,107892),\\
f_6(t) &= t^3-36t+54 \qquad (\mathrm{disc}\, f_6 = 107892),\\
f_7(t) &= t^3-30t+2 \qquad (\mathrm{disc}\, f_7 = 107892).
\end{aligned}$$

Zu f_1 *gehört ein kubischer Zahlkörper* $\mathcal{K}$ *mit Diskriminante* 148, *den wir in die Liste* $\mathfrak{K}$ *aufnehmen. Da* $f_2, f_4, \ldots, f_7$ *ebenfalls erzeugende Polynome von* $\mathcal{K}$ *sind, werden diese Polynome nicht weiter berücksichtigt. Aussortieren können wir das Polynom*

f_3, weil der von f_3 erzeugte Körper die Diskriminante 299700 besitzt und daher keine Gleichungsordnung mit Diskriminante $-108\,k = 107892$ enthalten kann. Wir haben also $\mathfrak{K} = \{\mathcal{K}\}$.

Um die irreduziblen Vektoren aus $\bar{P}_k$ zu ermitteln, müssen wir die Menge

$$\mathfrak{I}_{\mathcal{K}}\left(\sqrt{\frac{107892}{148}}\right) = \mathfrak{I}_{\mathcal{K}}(27)$$

bestimmen. Bezeichnet θ eine Nullstelle von f_1, so ist eine Ganzheitsbasis von $\mathfrak{o}_{\mathcal{K}}$ gegeben durch $\omega_1 = 1$, $\omega_2 = \frac{-2+\theta}{3}$, $\omega_3 = \frac{1+2\,\theta+\theta^2}{9}$, und die Bestimmung von $\mathfrak{I}_{\mathcal{K}}(27)$ ist nach (3-5) gleichbedeutend mit dem Lösen der Thue-Gleichung

$$x^3 + 2yx^2 - 12xy^2 + 10y^3 = 27.$$

Deren Lösungen sind gegeben durch $\{(3,0),(3,3),(9,6),(27,21),(363,228)\}$. Also kann das Vertretersystem $\mathfrak{I}_{\mathcal{K}}(27)$ gewählt werden als

$$\mathfrak{I}_{\mathcal{K}}(27) = \{3\,\omega_2, 3\,\omega_2 + 3\,\omega_3, 9\,\omega_2 + 6\,\omega_3, 27\,\omega_2 + 21\,\omega_3, 363\,\omega_2 + 228\,\omega_3\}.$$

Aus den Minimalpolynomen der Elemente aus $\mathfrak{I}_{\mathcal{K}}(27)$ berechnen wir leicht die entsprechenden irreduziblen Vertreter aus $\bar{P}_{-999}$. Insgesamt erhalten wir

$$\begin{aligned}\bar{P}_{-999} \quad = \quad & \{\, t^3 - 441t + 3564, t^3 + t^2 - 58t + 140, t^3 - 36t + 54, t^3 - 30t + 2, \\ & t^3 - 120t + 502, t^3 - 522t + 4590, t^3 - 67440t + 6741002 \,\}.\end{aligned}$$

Aus $\bar{P}_{-999}$ lesen wir leicht die ganzen Punkte auf $y^2 = x^3 - 999$ ab:

$$\begin{aligned}\mathfrak{L}_{-999} \quad = \quad & \{\, (10, \pm 1), (12, \pm 27), (40, \pm 251), \\ & (147, \pm 1782), (174, \pm 2295), (22480, \pm 3370501) \,\}.\end{aligned}$$

Die Gesamtrechenzeit für das Beispiel 3.4 betrug 12s. Wir hätten dieses Beispiel auch mit einer der bislang bekannten Methoden rechnen können. Um die Leistungsfähigkeit unseres Verfahrens zu demonstrieren, geben wir ein weiteres Beispiel.

In [23] haben Gebel, Pethő und Zimmer die ganzen Punkte auf fast allen Mordellschen Kurven mit $|k| \leq 10^5$ bestimmt. Sie benutzten dazu die Methode, welche auf elliptischen Logarithmen beruht und zu deren Durchführung man eine Basis der Mordell-Weil-Gruppe benötigt. Für 1182 viele dieser Kurven scheiterte dieses Verfahren, da — alle diese Kurven haben Rang 1 — ein Erzeuger der Mordell-Weil-Gruppe nicht berechnet werden konnte. Gebel, Pethő und Zimmer vermuteten, daß keine dieser 1182 Kurven einen ganzen Punkt besitzt. Diese Vermutung ist richtig, wie mit unserem Verfahren gezeigt werden konnte. Im folgenden, etwas kürzer gehaltenen Beispiel betrachten wir eine dieser Kurven, und zwar wählen wir dort für k den betraglich kleinsten Wert, bei dem der Ansatz über elliptische Logarithmen scheiterte.

Beispiel 3.5

Wir betrachten die Kurve $y^2 = x^3 + 7823$.

Man rechnet zunächst leicht $R_{7823} = \emptyset$ nach. Aus der Suchschleife erhalten wir dann $\mathfrak{K} = \{\mathcal{K}\}$, wobei $\mathcal{K}$ von einer Nullstelle des Polynoms $t^3 - 39t + 366$ erzeugt wird. Es ist $\omega_1 = 1, \omega_2 = \theta, \omega_3 = \frac{\theta+\theta^2}{2}$ eine Ganzheitsbasis von $\mathfrak{o}_\mathcal{K}$. Wegen $\mathrm{disc}_K = -108 \cdot 7823$ müssen wir $\mathfrak{I}_\mathcal{K}(1)$ berechnen und betrachten dazu die Thue-Gleichung

$$2X^3 + 3X^2Y - 18XY^2 + 82Y^3 = 1.$$

Da diese keine Lösung besitzt, folgt $\mathfrak{L}_{7823} = \emptyset$. Die Rechenzeit bei diesem Beispiel betrug 15s.

Wir hatten zu Beginn dieses Kapitels neben dem Ansatz über elliptische Logarithmen noch ein älteres Verfahren zur Berechnung der ganzen Punkte auf elliptischen Kurven genannt, welches über eine Idealgleichung in einem kubischen Körper ein System quartischer Thue-Gleichungen berechnet und aus dessen Lösungen die ganzen Punkte bestimmt. Die Durchführbarkeit dieses Verfahrens hängt in der Praxis entscheidend davon ab [56], daß die Grundeinheiten desjenigen kubischen Körpers $\mathcal{K} = \mathbb{Q}(\theta)$, in dem die Idealgleichung zu lösen ist, kleine Koeffizienten in der Darstellung bzgl. der $\mathbb{Q}$-Basis $1, \theta, \theta^2$ besitzen. Versuchen wir dieses Verfahren zum Beweis von $\mathfrak{L}_{7823} = \emptyset$ einzusetzen, so scheitern wir daran, daß in dem zu betrachtenden kubischen Zahlkörper $\mathbb{Q}(\sqrt[3]{7823})$ die Koeffizienten der Grundeinheiten außerordentlich groß sind. Es ist etwa

$$\begin{aligned}
\varepsilon = {} & 208399981911487168690387163002166487651591965014819930628143805363058341543647236666884578970 \\
& 673416349040119362326561305568880508738966902319776111670292648802993388311506529912783213771 \\
& 157522388019086949628971551424042659566131334476167845203055319563651408640396973678652003699 \\
& 599666656992564871239247581563459975027682884938838956345192448887561081917368569214320205162 \\
& 297891694644340572192161077979973592441653194336998769333323406115893349439952825409164289725 \\
& 634832715941712935408754291537908503459228364548333830266140875568306853472282879498264780603 \\
& 612045057582094895010329122654594233035293518993285818521253422182408778048266747217852326985 \\
& 693815725946772035264295729469025818346235133937719790337114455030110595666569420759195519750 \\
& 319296860661005475439924205927041527754705431789664943971114256796344613657594615412858454439 \\
& 026762492493020449824236577957341884193823349839832078508652094150099864111302793228016054708 \\
& 119340452602064720266451591650727517647162149951526347966253963327088964168093863653462776052 \\
& 073685276986635729698649063087838976949020903924853869758455280037066733195549850345428676559 \\
& 403576648041451015291944556829533718410529320531872693775092013828122883427258825645367670270 \\
& 303886624852346425059224420132143274310595795080326700671789927312955190540154966016408270952 \\
& 405094956365477167861027189889865373367013744161662606903491869183 35 \\
+ {} & 109727557035788192103578244433107312850514715670914396468792049390701002750882554736583209505 \\
& 430033931217624912929970326741887428355072121620768766037171877755672535373503024796318655646 \\
& 356927764946725921286783245316190692524741622432153220954981506366999031845991015985665562294 \\
& 338278066674492621861533204349342028072487765960182673285540342311203630720715931537732729785 \\
& 454534234747685104107288269523119717244915626130124136819581089111458942131962764520933306382 \\
& 694913605743366868201209538313564223396912115733131279575410082631887265373477622028055425183 \\
& 268300086733915871867870544624627508937724475151879165547878696654168350583729072695379728157 \\
& 393459375433686726737786240032031246251806582797784844279712771236001478704449312874740029773 \\
& 723104064702342012333789353215592943324207217502801592730785368419308549572594774362923205388 \\
& 890939735869411714123409502895947078122537667681999849411894996297562880080346865522689554728 \\
& 751183457361769790655354591811653273569720366830324494029828290887819097808138176824328104668 \\
& 108871774171422942562042595960863253358678669234577037285563750357091730030114180144399637942 \\
& 496774533878032760646255700191587114823512258556559404812039168291115501440690421543298423302 \\
& 566295776274167908256987343358270479924454490107312157388861863770806881826984233127378368365 \\
& 086529837281687830604286983147654617320121906664032917943920348706 \sqrt[3]{7823} \\
- {} & 473554764238342248779907268459543973749379449771955093715271960237870235986156933231803073969 \\
& 622464259795531479231240881726107089177105514261305631285700834694010067380649660846156586653 \\
& 486418124663820920076958351995039477725000145465160673206028837958836009592525573399687662023 \\
& 105833898603459755786837762562825726737948994285394329183300688601901478465251245969261429 88 \\
& 221516804461626181113724031452144031030846630989020724504886106948766159880485464097806183971 \\
& 517022872581522205564883345371787863955820893852525444130765153253074505560728884307087720337 \\
& 603612192697001277970871383628744170135637279544896448588552195067169581565884303745785058660 \\
& 948617728944817263924805835080902510878207434851122014727969856299812303968817686861605765538 \\
& 794588375790577903513126184633689855434107637453962816553275238561643137761256185556445275207 6 \\
& 296386863877170383598448476597233534187369667030741212218363083040867769183360518105069908408 \\
& 520462714485278050727639368278863599202121872189203822371149535843311016613613006427729041070 \\
& 622157881387353288696169316833698664789703258924992668804217972512600537296771798288283824447 \\
& 891021648699380477509451657933850278503101495849837198856452522022103210982987517952197877373 53 \\
& 717573157538240039513814950246134722472179732655105371037812680943132061714343277000411812219 \\
& 502794383881695155209878027646692115498283193578089208313382381 88 \sqrt[3]{7823^2}
\end{aligned}$$

eine bzgl. Koeffizientengröße minimale Grundeinheit von $\mathbb{Q}(\sqrt[3]{7823})$.

Abschließend wollen wir kurz versuchen, die Leistungsgrenzen unseres Verfahrens einzuschätzen. Dadurch, daß zur Bestimmung von $\mathfrak{K}$ jeweils $O(|k|^{3/4})$ viele qua-

dratische Gleichungen (3-4) gelöst werden müssen, ist von Beginn an eine obere Schranke für den Parameter k vorgegeben, bis zu dem unser Verfahren in der Praxis noch durchführbar sein kann. Diesem Hauptnachteil steht gegenüber, daß die bei unserem Verfahren involvierten Zahlkörper nur maximal Absolutdiskriminante $|108\,k|$ besitzen, wohingegen bei dem älteren Ansatz über Thue-Gleichungen für die dort auftretenden Zahlkörper $\mathbb{Q}(\sqrt[3]{k})$ die Absolutdiskriminante $108\,k^2$ möglich ist. Neben der Tatsache, daß wir keine unbewiesenen Vermutungen benutzen, ist dies ein wesentlicher Vorteil unseres Verfahrens, da der Aufwand für die meisten Rechnungen in algebraischen Zahlkörpern — etwa Grundeinheitenberechnung — erfahrungsgemäß mit wachsender Absolutdiskriminante stark zunimmt. Eine Übersicht über die Entwicklung der Rechenzeit unseres Verfahrens liefern die Tabellen am Ende des Kapitels.

Bemerkung 3.6
Die Mordellschen Kurven sind eine spezielle Familie der in kurzer Weierstraß-Normalform gegebenen elliptischen Kurven über $\mathbb{Q}$. Für eine solche allgemeinere Kurve $E : y^2 = x^3+ax+b$ kann die Menge ihrer ganzen Punkte wie bei den Mordellschen Kurven durch das Lösen von Indexformgleichungen bestimmt werden. Legen wir $P_{a,b}$ fest als die Menge aller normierten quartischen Polynome aus $\mathbb{Z}[\approx]$ mit Diskriminante $-4096\,(4a^3+27b^2)$ und ist bzgl. $\mathbb{Z}$-Äquivalenz ein Vertretersystem von $P_{a,b}$ gewählt als

$$\bar{P}_{a,b} = \left\{ t^4 + a_1 t^3 + a_2 t^2 + a_3 t + a_4 \mid a_1 \in \{1,2\} \vee (a_1 = 0 \wedge a_3 \geq 0) \right\},$$

so genügt zur Bestimmung aller ganzen Punkte von E die Berechnung der Menge $\bar{P}_{a,b}$, denn für jeden ganzen Punkt (x,y) von E mit $y \geq 0$ gilt

$$t^4 - 6x\,t^2 + 8y\,t - (4a + 3x^2) \in \bar{P}_{a,b}.$$

Ist $f(t) \in \bar{P}_{a,b}$ reduzibel, so ist $f(t)$ $\mathbb{Z}$-äquivalent zu einem Polynom der Gestalt $g(t) = g_1(t)\,g_2(t)$ oder $h(t) = t\,h_2(t)$, wo $g_1(t), g_2(t) \in \mathbb{Z}[\approx]$ quadratische Polynome und $h_2(t) = t^3 + a_1 t^2 + a_2 t + a_3 \in \mathbb{Z}[\approx]$ irreduzibel. Aufgrund von $\operatorname{disc} g = \operatorname{disc} g_1 \operatorname{disc} g_2 \operatorname{res}^2(g_1, g_2)$ existieren nur endlich viele Möglichkeiten für die Diskriminanten von $g_1(t)$ und $g_2(t)$, die man leicht durchprobiert. Zur Ermittlung der Kandidaten von $h_2(t)$ kann man wegen $\operatorname{disc} f = a_3^2 \operatorname{disc} h_2$ wie bei den Mordellschen Kurven verfahren.

Für ein irreduzibles $f(t) \in \bar{P}_{a,b}$ erzeugt eine Nullstelle θ von $f(t)$ einen quartischen Zahlkörper $\mathcal{K} = \mathbb{Q}(\theta)$, wobei

$$-4096\,(4\,a^3 + 27\,b^2) = \operatorname{disc} f = (\mathfrak{o}_{\mathcal{K}} : \mathbb{Z}[\theta])^2 \operatorname{disc}_{\mathcal{K}}. \tag{3-7}$$

Analog zur Bestimmung von $\mathfrak{K}$ bei den Mordellschen Kurven, lassen sich anhand von [42] alle quartischen Zahlkörper berechnen, deren Diskriminante der Gleichung (3-7) genügt. Um aus diesen Körpern dann die irreduziblen Vertreter von $\bar{P}_{a,b}$ zu erhalten, ist für jeden dieser Körper eine — diesmal quartische — Indexformgleichung zu lösen.

In der Praxis hat sich dieses Verfahren zur Bestimmung der ganzen Punkte auf einer in allgemeiner kurzer Weierstraß-Normalform gegebenen elliptischen Kurve

nicht bewährt. Dies liegt daran, daß sowohl für die reduziblen, als auch für die irreduziblen Vertreter von $\bar{P}_{a,b}$ zeitaufwendige Schleifen zu durchlaufen sind, um die zugrunde liegenden kubischen und quartischen Zahlkörper zu bestimmen. Bei Anwendung des allgemeinen Verfahrens auf eine Mordellsche Kurve $y^2 = x^3 + k$ müssen etwa kubische Zahlkörper bis zur möglichen Diskriminante $-110592\,k^2$ berücksichtigt werden.

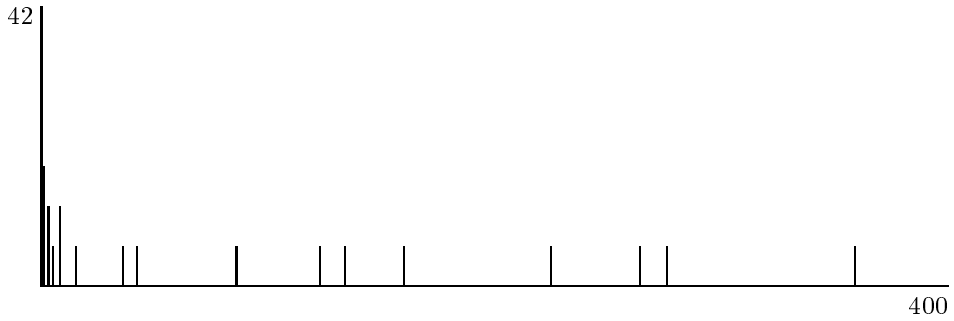
k	t	$\mathfrak{L}_k$
-7000025	1564s	$\emptyset$
-6000025	666s	$\emptyset$
-5000025	895s	$\emptyset$
-4000025	400s	$\emptyset$
-3000025	405s	$\{ (1225, \pm 42840) \}$
-2000025	240s	$\{ (505, \pm 11260) \}$
-1000025	156s	$\{ (101, \pm 174) \}$
-900025	196s	$\emptyset$
-800025	208s	$\emptyset$
-700025	104s	$\emptyset$
-600025	403s	$\emptyset$
-500025	86s	$\emptyset$
-400025	98s	$\emptyset$
-300025	76s	$\{ (665, \pm 17140) \}$
-200025	66s	$\emptyset$
-100025	39s	$\{ (69, \pm 478) \}$
-90025	50s	$\emptyset$
-80025	46s	$\emptyset$
-70025	49s	$\emptyset$
-60025	26s	$\emptyset$
-50025	17s	$\emptyset$
-40025	42s	$\{ (165, \pm 2110) \}$
-30025	61s	$\emptyset$
-20025	81s	$\emptyset$
-10025	22s	$\emptyset$
-9025	13s	$\{ (10685, \pm 1104490) \}$
-8025	39s	$\emptyset$
-7025	13s	$\{ (45, \pm 290) \}$
-6025	18s	$\emptyset$
-5025	6s	$\emptyset$
-4025	26s	$\emptyset$
-3025	1s	$\emptyset$
-2025	11s	$\emptyset$
-1025	19s	$\emptyset$

k	t	$\mathfrak{L}_k$
-925	1s	$\emptyset$
-825	1s	$\emptyset$
-725	17s	$\{ (9, \pm 2) \}$
-625	10s	$\emptyset$
-525	5s	$\emptyset$
-425	1s	$\{ (21, \pm 94) \}$
-325	1s	$\emptyset$
-225	10s	$\emptyset$
-125	0s	$\{ (5, \pm 0) \}$
-25	7s	$\{ (5, \pm 10) \}$
25	22s	$\{ (0, \pm 5) \}$
125	4s	$\{ (-5, \pm 0) \}$
225	83s	$\{ (-6, \pm 3), (-5, \pm 10), (0, \pm 15), (4, \pm 17), (6, \pm 21), (10, \pm 35), (15, \pm 60), (30, \pm 165), (60, \pm 465), (180, \pm 2415), (336, \pm 6159), (351, \pm 6576), (720114, \pm 611085363) \}$
325	1s	$\{ (-1, \pm 18) \}$
425	8s	$\{ (-4, \pm 19) \}$
525	26s	$\{ (-5, \pm 20) \}$
625	30s	$\{ (0, \pm 25), (6, \pm 29), (75, \pm 650) \}$
725	39s	$\emptyset$
825	7s	$\emptyset$
925	2s	$\{ (-9, \pm 14) \}$
1025	86s	$\{ (-10, \pm 5), (-5, \pm 30), (-4, \pm 31), (-1, \pm 32), (4, \pm 33), (10, \pm 45), (20, \pm 95), (40, \pm 255), (50, \pm 355), (64, \pm 513), (155, \pm 1930), (166, \pm 2139), (446, \pm 9419), (920, \pm 27905), (3631, \pm 218796), (3730, \pm 227805) \}$
2025	88s	$\{ (-9, \pm 36), (0, \pm 45), (10, \pm 55), (90, \pm 855) \}$
3025	104s	$\{ (-10, \pm 45), (-6, \pm 53), (0, \pm 55), (11, \pm 66), (15, \pm 80), (20, \pm 105), (44, \pm 297), (66, \pm 539), (110, \pm 1155), (330, \pm 5995), (1334, \pm 48723) \}$
4025	78s	$\{ (-10, \pm 55) \}$
5025	81s	$\{ (-5, \pm 70) \}$
6025	89s	$\{ (6, \pm 79) \}$
7025	79s	$\emptyset$
8025	97s	$\{ (-20, \pm 5), (10, \pm 95), (19, \pm 122), (14440, \pm 1735205) \}$
9025	81s	$\{ (0, \pm 95) \}$
10025	91s	$\{ (-20, \pm 45), (-16, \pm 77), (-10, \pm 95), (10, \pm 105), (14, \pm 113), (35, \pm 230), (55, \pm 420), (100, \pm 1005), (226, \pm 3399) \}$
20025	85s	$\{ (10, \pm 145) \}$
30025	151s	$\{ (-30, \pm 55), (-25, \pm 120), (20, \pm 195), (35, \pm 270), (54, \pm 433), (224, \pm 3357), (906, \pm 27271), (1280, \pm 45795) \}$
40025	138s	$\emptyset$
50025	143s	$\{ (-20, \pm 205) \}$
60025	98s	$\{ (0, \pm 245), (30, \pm 295), (294, \pm 5047) \}$
70025	144s	$\emptyset$
80025	184s	$\{ (4, \pm 283), (400, \pm 8005) \}$
90025	204s	$\{ (90, \pm 905) \}$

k	t	$\mathfrak{L}_k$
100025	229s	{ (40, ± 405) }
200025	1032s	{ (-45, ± 330), (-6, ± 447), (60, ± 645) }
300025	421s	{ (20, ± 555) }
400025	394s	{ (-25, ± 620), (80, ± 955), (170, ± 2305), (230, ± 3545), (590, ± 14345) }
500025	523s	∅
600025	435s	{ (39, ± 812) }
700025	792s	∅
800025	997s	{ (10, ± 895) }
900025	1064s	∅
1000025	1277s	{ (-100, ± 5), (-64, ± 859), (55, ± 1080), (94, ± 1353), (166, ± 2361), (740, ± 20155), (9000200, ± 27000900005) }
2000025	943s	∅
3000025	1052s	{ (1010, ± 32145) }
4000025	3297s	{ (260, ± 4645) }
5000025	3780s	{ (-170, ± 295) }
6000025	3477s	{ (-60, ± 2405), (30, ± 2455), (36, ± 2459), (2946, ± 159919), (670695, ± 549272180), (745470, ± 643643305) }
7000025	5008s	∅
8000025	5588s	{ (-200, ± 5), (144000400, ± 1728007200005) }
9000025	8032s	∅
10000025	8163s	{ (10000, ± 1000005) }
20000025	5466s	∅

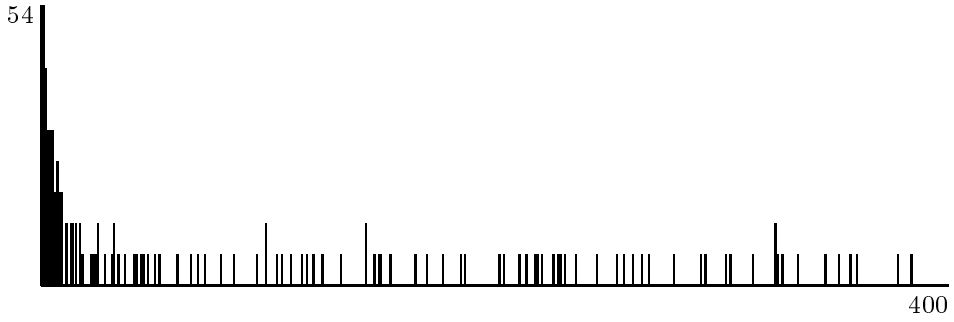
$n = 3$ **und** $r = 2$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
49	$t^3 + t^2 - 2t^1 - 1$	42	0s
81	$t^3 - 3t^1 + 1$	18	0s
148	$t^3 + t^2 - 3t^1 - 1$	0	0s
169	$t^3 + t^2 - 4t^1 + 1$	12	0s
229	$t^3 - 4t^1 + 1$	0	0s
257	$t^3 - 5t^1 + 3$	6	0s
316	$t^3 + t^2 - 4t^1 - 2$	0	0s
321	$t^3 + t^2 - 4t^1 - 1$	0	0s
361	$t^3 + t^2 - 6t^1 - 7$	12	0s
404	$t^3 + t^2 - 5t^1 + 1$	0	0s



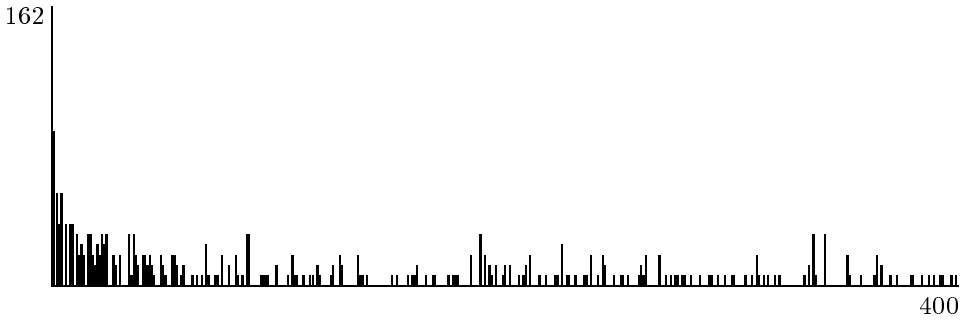
$n = 4$ **und** $r = 2$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-275	$t^4 - t^3 + 2t^1 - 1$	54	1s
-283	$t^4 - t^1 - 1$	54	1s
-331	$t^4 - t^3 - t^2 + t^1 - 1$	42	1s
-400	$t^4 - t^2 - 1$	30	1s
-448	$t^4 - 2t^3 + t^2 + 2t^1 - 1$	30	1s
-475	$t^4 - t^3 - 2t^2 - 2t^1 - 1$	30	1s
-491	$t^4 - t^3 - 2t^2 + 2t^1 - 1$	18	1s
-507	$t^4 - t^3 - t^2 - t^1 + 1$	24	1s
-563	$t^4 - t^3 - t^2 - t^1 - 1$	18	1s
-643	$t^4 - t^3 - 2t^1 + 1$	18	1s



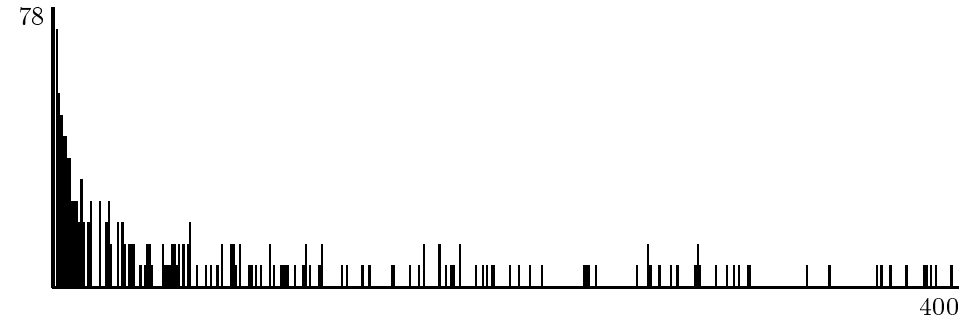
$n = 4$ **und** $r = 3$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
725	$t^4 - t^3 - 3t^2 + t^1 + 1$	162	2s
1125	$t^4 - t^3 - 4t^2 + 4t^1 + 1$	90	2s
1600	$t^4 + 2t^3 - 5t^2 - 6t^1 - 1$	54	2s
1957	$t^4 - 4t^2 - t^1 + 1$	36	2s
2000	$t^4 - 5t^2 + 5$	54	2s
2048	$t^4 - 4t^2 + 2$	0	0s
2225	$t^4 - t^3 - 5t^2 + 2t^1 + 4$	36	2s
2304	$t^4 - 4t^2 + 1$	0	0s
2525	$t^4 - t^3 - 6t^2 + 5$	36	2s
2624	$t^4 - 2t^3 - 3t^2 + 2t^1 + 1$	36	2s



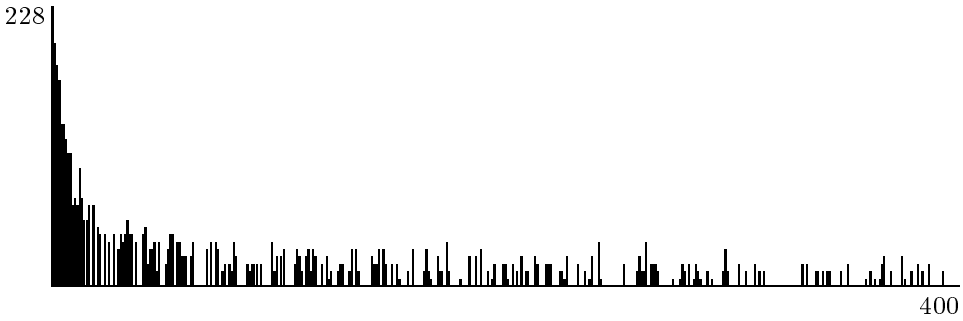
$n = 5$ **und** $r = 2$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
1609	$t^5 - t^3 + t^2 + t^1 - 1$	78	1s
1649	$t^5 + t^4 - t^3 + t^1 - 1$	78	1s
1777	$t^5 - 2t^3 + t^2 + 2t^1 - 1$	72	1s
2209	$t^5 - t^3 + 2t^2 - 2t^1 + 1$	54	1s
2297	$t^5 + t^3 + t^2 + t^1 + 1$	48	1s
2617	$t^5 + t^3 + 2t^2 + 1$	42	1s
2665	$t^5 + t^3 - 2t^1 + 1$	42	1s
2869	$t^5 - t^1 + 1$	36	1s
3017	$t^5 - t^3 + 1$	36	1s
3089	$t^5 - t^3 + 2t^1 + 1$	24	1s



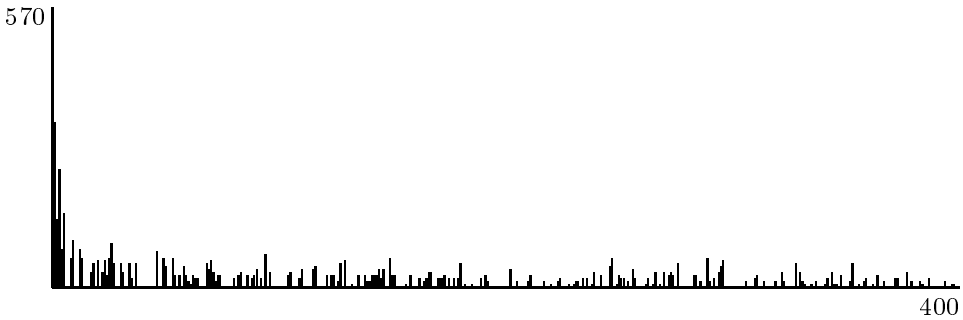
$n = 5$ **und** $r = 3$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-4511	$t^5 - 2t^3 + t^2 - 1$	228	3s
-4903	$t^5 + t^4 - 2t^3 + t^2 + t^1 - 1$	198	3s
-5519	$t^5 - 3t^3 + t^2 + t^1 - 1$	180	3s
-5783	$t^5 + t^4 - 3t^3 + t^2 + 2t^1 - 1$	168	3s
-7031	$t^5 - t^3 + t^2 - t^1 - 1$	132	3s
-7367	$t^5 - 4t^3 + t^2 + 2t^1 - 1$	132	3s
-7463	$t^5 + 2t^4 - t^2 - 2t^1 - 1$	120	3s
-8519	$t^5 + t^4 - t^3 - t^1 - 1$	108	3s
-8647	$t^5 + 2t^4 - t^3 - 2t^1 + 1$	108	3s
-9439	$t^5 + t^4 - t^3 - t^2 - 2t^1 - 1$	66	3s



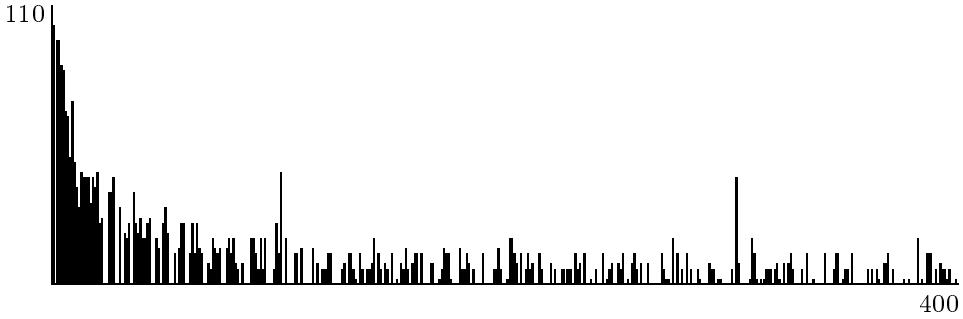
$n = 5$ **und** $r = 4$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
14641	$t^5 + t^4 - 4t^3 - 3t^2 + 3t^1 + 1$	570	7s
24217	$t^5 - 5t^3 + t^2 + 3t^1 - 1$	336	7s
36497	$t^5 - 6t^3 + t^2 + 4t^1 + 1$	138	7s
38569	$t^5 - 5t^3 + 4t^1 + 1$	240	7s
65657	$t^5 + t^4 - 7t^3 - t^2 + 4t^1 - 1$	78	7s
70601	$t^5 + t^4 - 5t^3 - 2t^2 + 3t^1 + 1$	150	7s
81509	$t^5 - 6t^3 + t^2 + 5t^1 - 2$	0	0s
81589	$t^5 - 8t^3 + 4t^2 + 2t^1 - 1$	0	0s
89417	$t^5 + 2t^4 - 7t^3 - 4t^2 + 2t^1 + 1$	60	7s
101833	$t^5 + t^4 - 5t^3 - 5t^2 + 2t^1 + 1$	96	7s



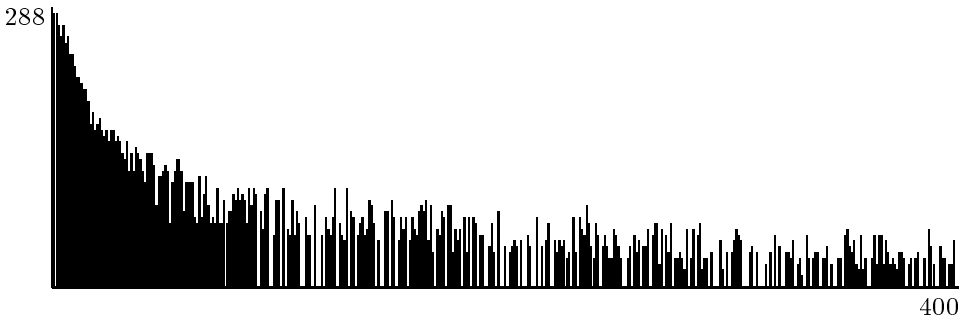
$n = 6$ und $r = 2$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-9747	$t^6 - t^5 + t^4 - 2t^3 + 4t^2 - 3t^1 + 1$	110	1s
-10051	$t^6 - t^5 + 2t^4 - 2t^3 + 2t^2 - 2t^1 + 1$	102	1s
-10571	$t^6 - t^5 - t^4 + 2t^3 - t^1 + 1$	96	1s
-10816	$t^6 - t^4 - 2t^3 + 2t^1 + 1$	96	1s
-11691	$t^6 - t^5 - t^2 + t^1 + 1$	86	1s
-12167	$t^6 - 3t^5 + 5t^4 - 5t^3 + 5t^2 - 3t^1 + 1$	84	1s
-14283	$t^6 - t^5 + t^4 - 2t^3 + t^2 + 1$	68	1s
-14731	$t^6 - t^5 + t^3 - t^2 + 1$	66	1s
-16551	$t^6 - t^5 - t^4 + 3t^3 - 2t^1 + 1$	50	1s
-16807	$t^6 - t^5 + t^4 - t^3 + t^2 - t^1 + 1$	72	1s



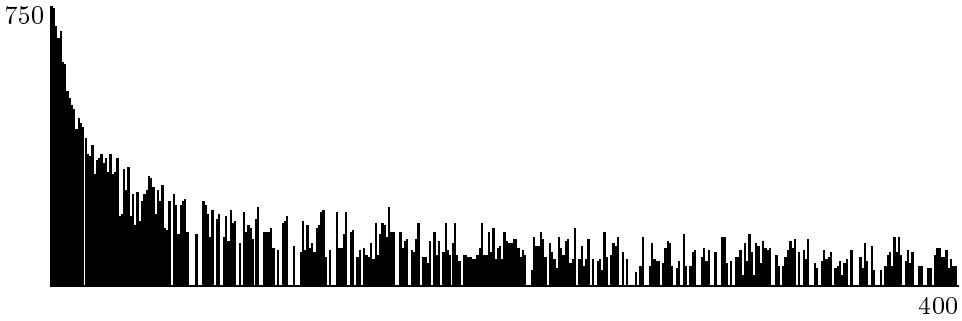
$n = 6$ und $r = 3$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
28037	$t^6 - 2t^5 + 3t^3 - 2t^1 - 1$	288	5s
29077	$t^6 - t^5 + t^4 - t^2 + 2t^1 - 1$	282	4s
29189	$t^6 - 2t^5 + t^4 + t^3 - 2t^2 + t^1 + 1$	282	4s
30125	$t^6 - t^5 + t^4 - 2t^2 + t^1 - 1$	270	4s
31133	$t^6 - 2t^4 - t^3 + 2t^1 + 1$	258	4s
31213	$t^6 - 2t^5 + 2t^4 - 3t^3 + 2t^2 - 2t^1 + 1$	270	4s
31709	$t^6 - t^5 + 2t^3 - 2t^2 + 1$	252	4s
32269	$t^6 - 3t^5 + 4t^4 - 3t^3 + t^2 - 1$	258	4s
33856	$t^6 + t^4 - 1$	240	4s
35125	$t^6 - t^5 - t^4 + 2t^3 - t^2 + 1$	240	4s



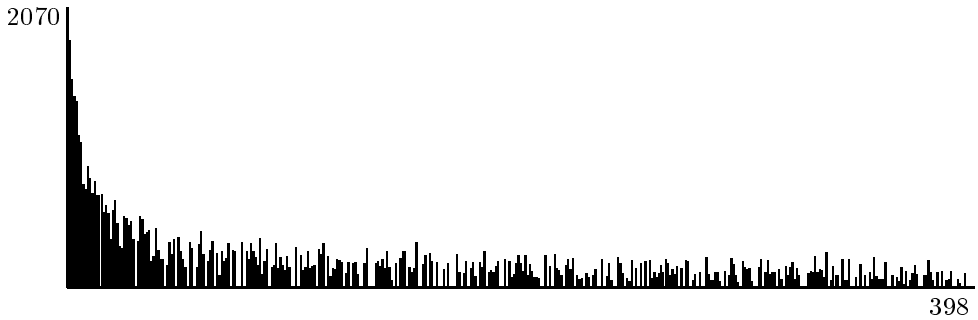
$n = 6$ **und** $r = 4$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-92779	$t^6 - t^5 - 2t^4 + 3t^3 - t^2 - 2t^1 + 1$	750	12s
-94363	$t^6 - 2t^4 - 2t^3 + 3t^1 + 1$	744	11s
-103243	$t^6 - t^5 - t^4 - 2t^3 + 2t^2 + 3t^1 - 1$	696	10s
-104483	$t^6 - t^5 - t^4 + 2t^3 - 2t^2 - t^1 + 1$	666	12s
-104875	$t^6 - 2t^5 - t^4 + t^3 + 2t^2 + t^1 - 1$	684	12s
-118987	$t^6 - t^5 + 4t^3 - 2t^2 - 2t^1 + 1$	600	12s
-124659	$t^6 - 3t^4 - 2t^3 + 3t^2 + 3t^1 - 1$	594	10s
-133787	$t^6 - 3t^5 + 2t^4 - t^2 + 3t^1 - 1$	522	12s
-144875	$t^6 - 2t^5 - t^4 + 5t^3 - 2t^2 - 3t^1 + 1$	504	12s
-149875	$t^6 - 3t^4 - 2t^3 + t^2 + 3t^1 + 1$	486	12s



$n = 6$ **und** $r = 5$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
300125	$t^6 - t^5 - 7t^4 + 2t^3 + 7t^2 - 2t^1 - 1$	2070	29s
371293	$t^6 - t^5 - 5t^4 + 4t^3 + 6t^2 - 3t^1 - 1$	1830	28s
434581	$t^6 - 2t^5 - 4t^4 + 5t^3 + 4t^2 - 2t^1 - 1$	1542	28s
453789	$t^6 - t^5 - 6t^4 + 6t^3 + 8t^2 - 8t^1 + 1$	1416	29s
485125	$t^6 - 2t^5 - 4t^4 + 8t^3 + 2t^2 - 5t^1 + 1$	1380	28s
592661	$t^6 - t^5 - 5t^4 + 4t^3 + 5t^2 - 2t^1 - 1$	1122	26s
703493	$t^6 - 2t^5 - 5t^4 + 11t^3 + 2t^2 - 9t^1 + 1$	1074	26s
722000	$t^6 - t^5 - 6t^4 + 7t^3 + 4t^2 - 5t^1 + 1$	762	26s
810448	$t^6 - 3t^5 - 2t^4 + 9t^3 - 5t^1 + 1$	726	27s
820125	$t^6 - 9t^4 - 4t^3 + 9t^2 + 3t^1 - 1$	894	28s

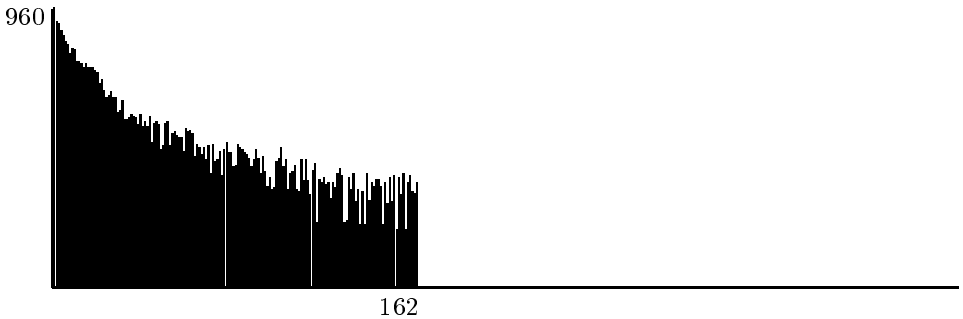


$n = 7$ **und** $r = 3$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-184607	$t^7 - t^6 - t^5 + t^4 - t^2 + t^1 + 1$	366	6s
-193327	$t^7 - t^6 + 2t^4 - 2t^3 + 2t^1 - 1$	348	6s
-193607	$t^7 - t^4 - t^3 + t^2 + 1$	348	6s
-196127	$t^7 - 2t^6 + 2t^5 - t^4 + 2t^2 - 2t^1 + 1$	342	6s
-199559	$t^7 - t^6 + t^3 - t^1 + 1$	336	6s
-201671	$t^7 - t^6 + 2t^5 - 2t^4 + 2t^3 - 2t^2 + 2t^1 - 1$	336	6s
-202471	$t^7 - t^6 - t^5 + 2t^4 - t^2 + 1$	330	6s
-207911	$t^7 - t^5 - t^4 - t^3 + t^2 + t^1 + 1$	324	7s
-211831	$t^7 - t^6 + 2t^5 - t^4 + t^2 - 2t^1 + 1$	324	6s
-214607	$t^7 - t^6 + 2t^5 - 2t^4 + 2t^3 - 2t^2 - 1$	318	6s

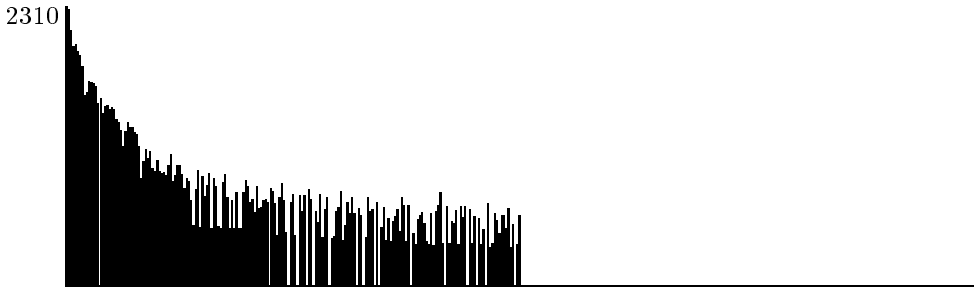
$n = 7$ **und** $r = 4$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
612233	$t^7 - t^6 + t^5 - t^3 + t^2 - t^1 - 1$	954	17s
612569	$t^7 - 3t^5 - t^4 + 3t^3 + 1$	960	19s
640681	$t^7 - 2t^6 + 2t^5 - 3t^3 + 2t^2 - 1$	912	19s
649177	$t^7 - t^6 - t^4 + 3t^2 - 1$	906	19s
661033	$t^7 - t^6 - t^5 + 2t^3 + t^2 - 2t^1 - 1$	882	18s
674057	$t^7 - 3t^6 + 5t^5 - 6t^4 + 3t^3 - t^2 - t^1 + 1$	864	19s
689033	$t^7 - t^5 - 3t^4 - t^3 + 2t^2 + 2t^1 + 1$	846	19s
696401	$t^7 - t^6 + 2t^4 - 4t^3 + 4t^2 - 4t^1 + 1$	834	18s
724873	$t^7 - t^6 + t^4 - 2t^3 + t^2 - 1$	804	17s
726721	$t^7 - t^6 + 2t^4 - 5t^3 + 4t^2 - 3t^1 + 1$	822	19s



$n = 7$ **und** $r = 5$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-2306599	$t^7 - 3t^5 - t^4 + t^3 + 3t^2 + t^1 - 1$	2310	46s
-2369207	$t^7 - 4t^5 + 3t^3 - t^2 + t^1 + 1$	2286	46s
-2616839	$t^7 - t^6 - 3t^5 + 4t^4 + t^3 - 5t^2 + t^1 + 1$	2112	46s
-2790047	$t^7 - t^6 - 2t^5 + 3t^4 - 2t^3 - 3t^2 + 4t^1 + 1$	1980	47s
-2790551	$t^7 - 2t^5 - 3t^3 - t^2 + 3t^1 + 1$	1998	48s
-2894039	$t^7 - t^6 - t^5 - 2t^3 + 3t^2 + 2t^1 - 1$	1938	43s
-2932823	$t^7 - t^6 - 4t^3 + 2t^2 + 2t^1 - 1$	1908	47s
-3063719	$t^7 - 3t^6 + t^5 + 4t^4 - 5t^3 + t^2 + 3t^1 - 1$	1818	46s
-3373751	$t^7 - 2t^5 - 2t^4 - t^3 + 3t^2 + t^1 - 1$	1578	47s
-3394343	$t^7 - 2t^6 - 2t^5 + 6t^4 - t^3 - 5t^2 + t^1 + 1$	1602	45s



$n = 7$ **und** $r = 6$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
20134393	$t^7 - t^6 - 6t^5 + 4t^4 + 10t^3 - 4t^2 - 4t^1 + 1$	2892	105s
25164057	$t^7 - 2t^6 - 5t^5 + 9t^4 + 7t^3 - 10t^2 - 2t^1 + 1$	1320	100s
25367689	$t^7 - t^6 - 6t^5 + 4t^4 + 9t^3 - 4t^2 - 3t^1 + 1$	2652	108s
28118369	$t^7 - 2t^6 - 5t^5 + 9t^4 + 7t^3 - 9t^2 - 3t^1 + 1$	2118	104s
30653489	$t^7 - 7t^5 - t^4 + 11t^3 + 3t^2 - 3t^1 - 1$	1146	98s
31056073	$t^7 - 3t^6 - 3t^5 + 11t^4 + t^3 - 9t^2 + 1$	2028	98s
32354821	$t^7 - 2t^6 - 5t^5 + 9t^4 + 6t^3 - 8t^2 - t^1 + 1$	1518	103s
32567681	$t^7 - 7t^5 - 2t^4 + 10t^3 + 3t^2 - 3t^1 - 1$	2016	105s
34554953	$t^7 - 2t^6 - 5t^5 + 9t^4 + 5t^3 - 8t^2 + 1$	1890	98s
35269513	$t^7 - 2t^6 - 5t^5 + 10t^4 + 5t^3 - 10t^2 - t^1 + 1$	1866	98s

$n = 8$ **und** $r = 3$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
1257728	$t^8 - 2t^7 + 4t^5 - 4t^4 + 3t^2 - 2t^1 + 1$	438	8s
1265625	$t^8 - t^7 + t^5 - t^4 + t^3 - t^1 + 1$	440	6s
1282789	$t^8 - t^7 + 2t^6 - 3t^5 + 3t^4 - 3t^3 + 3t^2 - 2t^1 + 1$	432	8s
1327833	$t^8 - t^7 + t^6 - 2t^5 + 3t^4 - 4t^3 + 4t^2 - 2t^1 + 1$	434	8s
1342413	$t^8 - t^7 + t^6 + t^4 - 2t^3 + 3t^2 - 3t^1 + 1$	422	9s
1361513	$t^8 - t^7 + 2t^6 - 3t^5 + 3t^4 - 3t^3 + 2t^2 - t^1 + 1$	414	7s
1385533	$t^8 - 2t^7 + 3t^6 - 3t^5 + t^4 + 1$	396	8s
1424293	$t^8 - 2t^7 + 2t^6 - t^5 + t^4 - t^3 + 2t^2 - 2t^1 + 1$	390	7s
1474013	$t^8 - t^7 + t^6 - t^4 + t^3 - t^2 + 1$	384	8s
1492101	$t^8 - t^7 + t^6 - 3t^5 + t^4 - 2t^3 + 3t^2 + 1$	368	8s

$n = 8$ **und** $r = 7$

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
282300416	$t^8 + 2t^7 - 7t^6 - 8t^5 + 15t^4 + 8t^3 - 9t^2 - 2t^1 + 1$	15804	739s
309593125	$t^8 + 3t^7 - 5t^6 - 21t^5 - 3t^4 + 35t^3 + 28t^2 + 4t^1 - 1$	14742	701s
324000000	$t^8 - 8t^6 + 14t^4 - 7t^2 + 1$	14274	688s

$n = 9$ und $r = 4$ (imprimitive Körper)

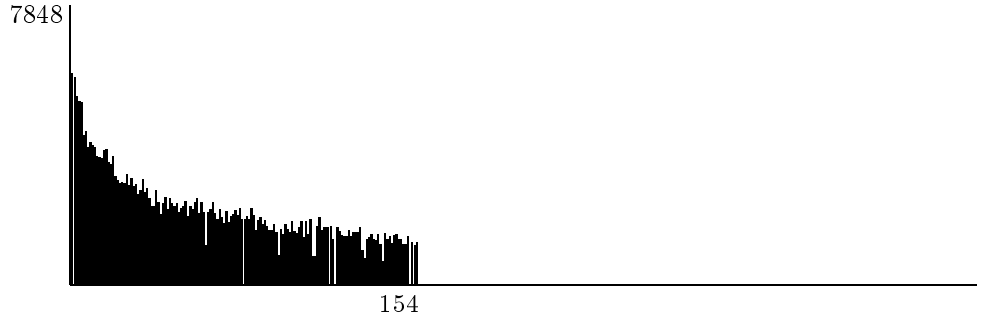
$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
32206049	$t^9+3t^8+7t^7+9t^6+10t^5+9t^4+7t^3+4t^2+2t^1+1$	1266	30s
33860761	$t^9-2t^8+2t^7-2t^5+2t^4-t^1+1$	1206	30s
35028793	$t^9+4t^8+8t^7+11t^6+11t^5+10t^4+7t^3+4t^2+2t^1+1$	1188	29s
38817673	$t^9+2t^8-7t^6-12t^5-11t^4-7t^3-5t^2-3t^1-1$	1044	30s
43302353	$t^9-3t^8+7t^7-12t^6+17t^5-18t^4+16t^3-10t^2+4t^1-1$	978	29s
44656709	$t^9+t^8-4t^7-2t^6+7t^5-6t^3+t^2+2t^1+1$	918	28s
44908397	$t^9-t^8-2t^7-2t^6+t^5+6t^4+8t^3+7t^2+4t^1+1$	912	30s
47159153	$t^9-3t^8+9t^7-18t^6+26t^5-28t^4+24t^3-15t^2+6t^1-1$	906	28s
49483189	$t^9+t^8+t^7+2t^6+4t^5+3t^4+2t^3+2t^2+2t^1+1$	852	29s
50797225	$t^9-2t^8+t^7+2t^6-4t^5+t^4+3t^3-2t^2+1$	810	28s

$n = 9$ und $r = 5$ (imprimitive Körper)

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-110852311	$t^9+t^8-4t^7-2t^6+8t^5+t^4-8t^3+2t^2+3t^1-1$	3366	90s
-114479303	$t^9-9t^7-3t^6+54t^5-59t^4+3t^3+10t^2+3t^1+1$	3246	97s
-129079703	$t^9+4t^8-19t^6-28t^5-13t^4-t^3+3t^2+3t^1+1$	2994	102s
-133731799	$t^9-2t^8+5t^6-5t^5-5t^4+4t^3+3t^2-t^1-1$	2880	108s
-147184199	$t^9+2t^8-5t^7-15t^6-12t^5+5t^4+8t^3-2t^2-4t^1-1$	2700	107s
-157505216	$t^9-t^8-5t^7+2t^6+16t^5-7t^4-17t^3+5t^2+6t^1+1$	2454	92s
-164590951	$t^9+2t^8+3t^7+t^6-2t^5-5t^4-4t^3+2t^1+1$	2454	92s
-177767639	$t^9-4t^8+7t^7-4t^6-5t^5+9t^4-5t^3-t^2+2t^1-1$	2274	88s
-180181103	$t^9-4t^8-t^7+16t^6-4t^5-18t^4+10t^3+5t^2-5t^1+1$	2238	89s
-181543807	$t^9-3t^8+2t^7+3t^6-3t^5+2t^4-4t^2+1$	2232	91s

$n = 9$ und $r = 6$ (imprimitive Körper)

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
467890073	$t^9 + 2t^8 + t^7 - 2t^6 - 5t^5 - 2t^4 + t^3 + 3t^2 + t^1 - 1$	7848	308s
672128737	$t^9 + 4t^8 + 4t^7 - t^6 - 5t^5 - 4t^4 - t^3 + 2t^2 + 2t^1 - 1$	5916	300s
689278977	$t^9 - 6t^7 + 2t^6 + 3t^5 - 6t^4 + 2t^3 + 6t^2 - 1$	5820	296s
741306349	$t^9 - 4t^7 + 18t^6 - 4t^5 - 48t^4 + 67t^3 - 38t^2 + 10t^1 - 1$	5280	303s
823660649	$t^9 - 3t^8 - 2t^7 + 8t^6 + 3t^5 - 6t^4 - 4t^3 + t^1 + 1$	5154	291s
830248993	$t^9 + t^8 - 2t^7 - 3t^6 + t^5 + 6t^4 - t^3 - 5t^2 + 1$	5106	283s
960133489	$t^9 + 4t^8 + 6t^7 - 4t^6 - 14t^5 - t^4 + 12t^3 - 4t^1 + 1$	4182	268s
1021310969	$t^9 + t^8 - 5t^7 - t^6 + 4t^5 - 2t^4 + 6t^3 - 3t^2 + t^1 - 1$	4308	272s
1058958649	$t^9 + 4t^8 + 5t^7 - 2t^6 - 12t^5 - 6t^4 + 12t^3 + 3t^2 - 5t^1 + 1$	3852	260s
1087194409	$t^9 + t^8 - 4t^7 + t^6 + 8t^5 - 7t^4 - 3t^3 + 6t^2 - t^1 - 1$	3990	255s



$n = 9$ und $r = 7$ (imprimitive Körper)

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
-2668161671	$t^9 - 2t^8 - 7t^7 + 10t^6 + 8t^5 - 24t^4 + 2t^3 + 17t^2 - 3t^1 - 1$	14844	1287s
-2964637151	$t^9 - 2t^8 - 8t^7 + 17t^6 + 9t^5 - 31t^4 + 6t^3 + 17t^2 - 7t^1 - 1$	13938	1233s
-3030520591	$t^9 - 3t^7 + t^6 - 18t^5 - 23t^4 + 32t^3 + 36t^2 + 2t^1 - 1$	13692	1265s
-3616883207	$t^9 + 2t^8 - 6t^7 - 15t^6 - 6t^5 + 27t^4 + 27t^3 - 6t^2 - 10t^1 - 1$	12096	1155s
-4475250311	$t^9 - 4t^8 + t^7 + 16t^6 - 21t^5 - 12t^4 + 26t^3 - 5t^2 - 4t^1 + 1$	9450	972s
-4591118799	$t^9 + 3t^8 + 6t^7 + 20t^6 + 18t^5 - 21t^4 - 19t^3 + 9t^2 + 3t^1 - 1$	10242	1010s
-4664429903	$t^9 - 4t^8 - t^7 + 15t^6 - 6t^5 - 15t^4 + 8t^3 + 6t^2 - 2t^1 - 1$	9846	932s
-4951022867	$t^9 - 2t^7 + 4t^6 - 8t^5 - 10t^4 + 11t^3 + 8t^2 - 2t^1 - 1$	8844	953s
-5382559399	$t^9 + 2t^8 - 6t^7 - 6t^6 + 27t^5 + 8t^4 - 73t^3 - 53t^2 + 16t^1 + 13$	8892	938s
-5520914623	$t^9 + t^8 - 5t^7 - 2t^6 + 8t^5 - 4t^4 - 6t^3 + 5t^2 + 2t^1 - 1$	8808	903s

$n = 9$ und $r = 8$ (imprimitive Körper)

$\mathrm{disc}_{\mathcal{K}}$	f	$\lvert X_{\mathcal{K}}\rvert$	t
16240385609	$t^9 + 2t^8 - 14t^7 - 32t^6 + 16t^5 + 61t^4 + 15t^3 - 18t^2 - 5t^1 + 1$	28296	6187s
16440305941	$t^9 + t^8 - 12t^7 - 10t^6 + 38t^5 + 34t^4 - 23t^3 - 27t^2 - 4t^1 + 1$	26718	5882s
16983563041	$t^9 + t^8 - 8t^7 - 7t^6 + 21t^5 + 15t^4 - 20t^3 - 10t^2 + 5t^1 + 1$	28398	5690s
17515230173	$t^9 + 4t^8 - 6t^7 - 36t^6 - 16t^5 + 70t^4 + 99t^3 + 52t^2 + 12t^1 + 1$	25170	5342s
19936446593	$t^9 + t^8 - 13t^7 - 18t^6 + 28t^5 + 48t^4 + 6t^3 - 17t^2 - 8t^1 - 1$	24900	5328s
22384826361	$t^9 + 3t^8 - 12t^7 - 32t^6 + 51t^5 + 105t^4 - 100t^3 - 114t^2 + 78t^1 + 19$	22752	5152s
29430250297	$t^9 - 3t^8 - 11t^7 + 39t^6 + 11t^5 - 86t^4 - 15t^3 + 64t^2 + 28t^1 + 1$	19200	4322s
31381059609	$t^9 - 9t^7 + 27t^5 - 30t^3 + 9t^1 + 1$	8676	3289s
35896709933	$t^9 + 2t^8 - 12t^7 - 22t^6 + 34t^5 + 70t^4 + t^3 - 30t^2 - 4t^1 + 1$	14976	3763s
36446755221	$t^9 - 15t^7 - 7t^6 + 66t^5 + 48t^4 - 70t^3 - 30t^2 + 27t^1 - 1$	14976	3740s

Literaturverzeichnis

[1] A. Baker, *Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms*, Phil. Trans. Royal Soc. London, Ser. **A263** (1968), 173–191.

[2] A. Baker, *Contributions to the theory of Diophantine equations II. The Diophantine equation* $y^2 = x^3 + k$, Phil. Trans. Royal Soc. London, Ser. **A263** (1968), 193–208.

[3] A. Baker, *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. **43** (1968), 1–9.

[4] A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975.

[5] A. Baker und G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Mathematik **442** (1993), 19–62.

[6] Y. Bilu und G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.

[7] A. Bremner, *On power bases in cyclotomic number fields*, J. Number Theory **28** (1988), 288–298.

[8] J. Conway, A. Hulpke und J. McKay, *On transitive permutation groups*, Manuskript.

[9] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegener und K. Wildanger, *KANT V4*, erscheint in J. Symbolic Comp.

[10] F. Diaz y Diaz, *Petits discriminants des corps de nombres totalement imaginaires de degré 8*, J. Number Theory **25** (1987), 34–52.

[11] F. Diaz y Diaz, J. Martinet und M. Pohst, *The minimum discriminant of totally real octic fields*, J. Number Theory **36** (1990), 145–159.

[12] F. Diaz y Diaz und M. Olivier, *Imprimitive ninth-degree number fields with small discriminants*, Math. Comp. **64** (1995), 305–321.

[13] J. H. Evertse, *Upper bounds for the number of solutions of Diophantine equations*, CWI Tract **168**, Stichting Mathematisch Centrum, Amsterdam 1983.

[14] U. Fincke und M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.

[15] I. Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp. **65** (1996), 801–822.

[16] I. Gaál, *Computing elements of given index in totally complex cyclic sextic fields*, J. Symbolic Computation **20** (1995), 61–69.

[17] I. Gaál, A. Pethő und M. Pohst, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comp. **16** (1993), 563–584.

[18] I. Gaál, A. Pethő und M. Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms — with an application to index form equations in quartic number fields*, J. Number Theory **57** (1996), 90–104.

[19] I. Gaál und M. Pohst, *On the resolution of index form equations in sextic fields with an imaginary subfield*, J. Symbolic Computation **22** (1996), 425–434.

[20] I. Gaál und N. Schulte, *Computing all power integral bases of cubic fields*, Math. Comp. **53** (1989), 689–696.

[21] J. Gebel, *Bestimmung aller ganzen und S-ganzen Punkte auf einer elliptischen Kurve über den rationalen Zahlen mit Anwendung auf die Mordellschen Kurven*, Dissertation, Universität des Saarlandes, Saarbrücken 1996.

[22] J. Gebel, A. Pethő und H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.

[23] J. Gebel, A. Pethő und H. G. Zimmer, *On Mordell's equation*, erscheint in Composito Math.

[24] M. N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$*, J. Number Theory **23** (1986), 347–353.

[25] K. Győry, *Sur l'irréductibilité d'une class des polynômes I*, Publ. Math. Debrecen **18** (1971), 289–307.

[26] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné II*, Publ. Math. Debrecen **21** (1974), 125–144.

[27] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer, 1978.

[28] H. W. Lenstra, *Euclidean number fields of large degree*, Invent. Math. **38** (1977), 237–254.

[29] A. K. Lenstra, H. W. Lenstra Jr. und L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[30] A. Leutbecher und J. Martinet, *Lenstra's constant and Euclidean number fields*, Astérisque **94** (1982), 87–131.

[31] Y. V. Matiyasevich, *Hilbert's Tenth Problem*, The MIT Press, 1993.

[32] L. J. Mordell, *The Diophantine equation* $y^2 - k = x^3$, Proc. London Math. Soc. (2) **13** (1913), 60–80.

[33] L. J. Mordell, *Intedeterminate equations of the third and fourth degrees*, Quart. J. Pure and Appl. Math. **45** (1914), 170–186.

[34] L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.

[35] T. Nagell, *Sur une proprieté des unités d'un corps algébrique*, Ark. Mat. **5** (1964), 343–356.

[36] T. Nagell, *Sur les unités dans les corps biquadratiques primitifs du premier rang*, Ark. Mat. **7** (1968), 359–394.

[37] T. Nagell, *Sur un type particular d'unités algébriques*, Ark. Mat. **8** (1969), 163–184.

[38] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.

[39] G. Niklasch, *Einheitengleichungen in kommutativen Ringen*, Dissertation, Technische Universität München, München 1991.

[40] G. Niklasch, *Family portraits of exceptional units*, Manuskript.

[41] G. Niklasch und R. Quême, *An improvement of Lenstra's criterion for Euclidean number fields: The totally real case*, Acta Arith. **53** (1991), 157–168.

[42] M. Pohst, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), 99–117.

[43] M. Pohst, *On the determination of algebraic number fields of given discriminant*, in „Computer Algebra“, Springer Lecture Notes in Computer Science **144** (1982), 71–76.

[44] M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar, Birkhäuser, 1993.

[45] M. Pohst und H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

[46] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics **785**, Springer, 1996.

[47] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics **1467**, Springer, 1996.

[48] A. Schwarz, M. Pohst und F. Diaz y Diaz, *A table of quintic number fields*, Math. Comp. **63** (1994), 361–376.

[49] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. preuß. Akad. Wiss., Phys.-math. Klasse 1929, Nr. 1, 209–266.

[50] N. P. Smart, *The solution of triangularly connected decomposable form equations*, Math. Comp. **64** (1995), 819–840.

[51] N. P. Smart, *Discriminant form equations in number fields of degree greater than four*, J. Symbolic Comp. **21** (1996), 367–374.

[52] V. G. Sprindžuk, *Classical Diophantine Equations*, Lecture Notes in Mathematics **1559**, Springer, 1990.

[53] R. J. Stroeker, *How to solve a Diophantine equation*, Amer. Math. Monthly **91** (1984), 385–392.

[54] R. J. Stroeker und N. Tzanakis, *On the application of Skolem's p-adic method to the solution of Thue equations*, J. Number Theory **29** (1988), 165–195.

[55] R. J. Stroeker und N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), 177–196.

[56] R. J. Stroeker und B. M. M. de Weger, *On elliptic Diophantine equations that defy Thue's method: The case of the Ochoa curve*, Exp. Math. **3** (1994), 209–220.

[57] N. Tzanakis und B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132.

[58] B. M. M. de Weger, *Algorithms for diophantine equations*, CWI Tract **65**, Stichting Mathematisch Centrum, Amsterdam 1989.

[59] K. Wildanger, *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, Heinrich-Heine-Universität Düsseldorf, Düsseldorf 1993.

Viele Menschen haben auf ganz unterschiedliche Weise zum Entstehen dieser Arbeit beigetragen. Ihnen allen sei an dieser Stelle herzlich gedankt.

Zusammenfassung

Diese Arbeit behandelt das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern sowie die Bestimmung aller ganzen Punkte auf einer Mordellschen Kurve. Den drei Problemstellungen ist gemein, daß sie jeweils nur höchstens endlich viele Lösungen besitzen. Algorithmen zur vollständigen Berechnung dieser Lösungen wurden möglich durch Ergebnisse von A. Baker zu Linearformen in den Logarithmen algebraischer Zahlen.

Das Lösen einer Einheitengleichung besteht im wesentlichen aus drei Schritten. Zuerst leitet man anhand der Resultate Bakers große obere Schranken für die Lösungen her. Diese Schranken werden im zweiten Schritt des Verfahrens mit dem LLL-Algorithmus reduziert. Im letzten Schritt, welcher die weitaus meiste Rechenzeit beansprucht, müssen alle unterhalb der Schranken liegenden Einheiten daraufhin überprüft werden, ob sie Lösungen der Einheitengleichung sind. Das ersten Kapitel beschreibt ein neues Verfahren, mit dem diese Überprüfung sehr viel effizienter als bislang durchgeführt werden kann. Mit dem Verfahren, welches Methoden aus der Geometrie der Zahlen benutzt, wurden Einheitengleichungen in Zahlkörpern bis hin zum Einheitenrang 10 gelöst. Das zweite Kapitel behandelt den Einsatz von Einheitengleichungen beim Lösen von Indexformgleichungen. Erstmals konnten hierbei Indexformgleichungen in Zahlkörpern vom Grad 8,10,12,16,18 und 22 gelöst werden. Gegenstand des dritten Kapitels ist schließlich ein neues, auf der Lösung von kubischen Indexformgleichungen basierendes Verfahren zur Bestimmung aller ganzen Punkte auf einer Mordellschen Kurve.

Alle Algorithmen wurden im Computeralgebra-System KANT implementiert.

Lebenslauf

Name	Klaus Wildanger
geboren am	15.12.1966 in Düsseldorf
Schulbesuch	1973 - 1986: Grundschule und Gymnasium in Düsseldorf
Zivildienst	1.10.1986 - 31.5.1988
Studium	ab Wintersemester 1988/1989 Mathematik mit Nebenfach Informatik an der Heinrich-Heine-Universität Düsseldorf Studienschwerpunkt: Konstruktive Zahlentheorie Diplom am 27.1.1994
Berufstätigkeit	1.2.1994 - 14.9.1997: wissenschaftlicher Mitarbeiter an der Technischen Universität Berlin