Quadratische Diophantische Gleichungen über algebraischen Zahlkörpern

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
„Doctor rerum naturalium“
der Georg-August-Universität Göttingen

im Promotionsprogramm Mathematical Sciences
der Georg-August University School of Science (GAUSS)

vorgelegt von

Lutz Carsten Helfrich
aus Schleswig

Göttingen, 2015

Betreuungsausschuss

Prof. Jörg Brüdern, Mathematisches Institut

Prof. Valentin Blomer, Mathematisches Institut

Mitglieder der Prüfungskommission

Referent: Prof. Jörg Brüdern, Mathematisches Institut

Korreferent: Prof. Valentin Blomer, Mathematisches Institut

Weitere Mitglieder der Prüfungskommission:

Prof. Preda Mihăilescu, Mathematisches Institut

Prof. Thomas Schick, Mathematisches Institut

Prof. Dominic Schuhmacher, Institut für Mathematische Stochastik

Prof. Max Wardetzky, Institut für Numerische und Angewandte Mathematik

Tag der mündlichen Prüfung: 20. März 2015

Inhaltsverzeichnis

1 Einleitung

Bereits im antiken Griechenland wurden diophantische Gleichungen untersucht und auch über die Jahrtausende haben die nach Diophantos von Alexandria benannten Gleichungen nichts von ihrer Faszination verloren. Dabei hat sich die Aufgabe, die Lösung einer diophantischen Gleichung anzugeben oder alternativ nachzuweisen, dass keine existiert, als verhältnismäßig schwer herausgestellt. Aus diesem Grund stellte David Hilbert als zehntes Problem seiner berühmt gewordenen Liste [Hil00] lediglich die Aufgabe, einen Algorithmus zu finden, der die Lösbarkeit jeder diophantischen Gleichung entscheiden kann.

Hilbert ahnte Gödels Unvollständigkeitssatz [Göd31] und damit auch die von Matijasevič [Mat70] im Jahr 1970 gefundene Antwort auf sein zehntes Problem nicht voraus. Matijasevič zeigte nach Vorarbeiten von Davis, Putnam und Robinson [DPR61], dass es keinen Algorithmus geben kann, der die gestellte Aufgabe bewältigt. Aus seiner Arbeit folgt sogar, dass man für jeden solchen Algorithmus eine diophantische Gleichung konstruieren kann, an der der Algorithmus scheitert.

Diese negative Antwort schließt nicht aus, dass es Klassen von diophantischen Gleichungen gibt, deren Lösbarkeit algorithmisch entscheidbar ist. Es ist schon lange bekannt, dass die Lösbarkeit linearer diophantischer Gleichungen mithilfe des euklidischen Algorithmus entschieden werden kann. Für quadratische Gleichungen zeigte Siegel [Sie72] die algorithmische Entscheidbarkeit. Bisher wurde nur für einige Arten von kubischen Gleichungen die Entscheidbarkeit bewiesen (vergleiche [Maz94]). Jones [Jon80] konnte zeigen, dass die Lösbarkeit von Gleichungen vierten Grades nicht algorithmisch entscheidbar ist.

Wenn die diophantischen Gleichungen nach der Anzahl der Variablen unterschieden werden, ist weniger bekannt. Im Fall einer Variablen ist das Problem leicht zu beantworten, während es im Fall von zwei Variablen Teilresultate gibt (vergleiche [DMR76]). Die Unentscheidbarkeit ist bisher lediglich für Gleichungen in mindestens neun Variablen [Mat77] bewiesen worden.

Es gibt zahlreiche Ad-hoc-Methoden um die algorithmische Entscheidbarkeit zu beweisen, die jeweils auf spezifischen Eigenschaften der untersuchten

diophantischen Gleichungen basieren. Von diesen abgesehen gibt es nur wenige systematische Ansätze.

Einer beruht auf der Kreismethode. Mit ihr wird versucht, das Hasse-Prinzip für die untersuchten Gleichungen derart zu verifizieren, dass die lokale Lösbarkeit nur für Primzahlen überprüft werden muss, die kleiner als eine effektive Schranke sind. Dadurch kann ein Algorithmus die Lösbarkeit in endlich vielen Schritten entscheiden.

Eine weitere Möglichkeit die algorithmische Entscheidbarkeit zu beweisen ist das Herleiten einer effektiven Suchschranke für die kleinste Lösung. Dann muss ein Algorithmus nur noch endlich viele Möglichkeiten testen, um entweder eine Lösung zu finden oder die Lösbarkeit auszuschließen. Solche Suchschranken können nicht nur dazu genutzt werden, die Entscheidbarkeit zu beweisen, sondern auch zur Untersuchung diophantischer Ungleichungen.

Es gibt eine Reihe solcher Suchschranken. Cassels [Cas55] bewies eine Suchschranke für die kleinste nicht triviale Nullstelle einer quadratischen Form. Der Autor leitete in seiner Masterarbeit [Hel12] eine Suchschranke für die kleinste Lösung einer kubischen Form in mindestens 14 Variablen her.

Siegel [Sie72] hat mithilfe einer Suchschranke gezeigt, dass die Lösbarkeit quadratischer Gleichungen der Form

$$\sum_{i,j=1}^{s} a_{ij}x_ix_j + \sum_{i=1}^{s} h_ix_i = n \tag{1.1}$$

mit Koeffizienten $a_{ij}, h_i, n \in \mathbb{Z}$ entscheidbar ist. Hierbei kann davon ausgegangen werden, dass die Matrix $A = (a_{ij}) \in \mathbb{Z}^{s\times s}$ symmetrisch ist. Wie Straumann in seiner Diplomarbeit [Str99] zeigen konnte, wächst die aus Siegels Methode resultierende Suchschranke exponentiell in der Höhe der Koeffizienten

$$H = \max\{|a_{ij}|, |h_i|, |n| : 1 \leq i, j \leq s\}.$$

Nach Vorarbeiten von Kornhauser ([Kor90a], [Kor90b]) konnte Dietmann in seiner Dissertation [Die03] die Suchschranke

$$\Lambda_s(H) = \begin{cases} C_2H^{10H}, & s = 2, \\ C_3H^{2100}, & s = 3, \\ C_4H^{84}, & s = 4, \\ C_sH^{5s+19+74/(s-4)}, & s \geq 5 \end{cases}$$

für die kleinste Lösung einer quadratischen Gleichung mit nichtsingulärem quadratischen Anteil A herleiten. Die Einschränkung auf nichtsinguläre Matrizen ist keine wesentliche Beschränkung, denn Grunewald und Segal [GS81, §2]

haben gezeigt, dass sich die Lösbarkeit einer quadratischen Gleichung, deren quadratischer Anteil singulär ist, stets auf die Lösbarkeit einer quadratischen Gleichung mit nichtsingulärem quadratischen Anteil in weniger Variablen zurückführen lässt.

Kornhauser führt in seinen Arbeiten Beispiele für quadratische diophantische Gleichungen an, die zeigen, dass jede Suchschranke im binären Fall mindestens die Größenordnung $2^{H/5}$ und im Fall von mehr als zwei Variablen mindestens die Größenordnung $H^{s/2}$ haben muss. Demnach hat Dietmanns Suchschranke in etwa die richtige Größenordnung.

Indem sowohl für die Koeffizienten als auch für die Lösungen Werte aus dem Ganzheitsring $\mathcal{O}$ eines algebraischen Zahlkörpers K vom Grad d zugelassen werden, ist es möglich, die Definition diophantischer Gleichungen auf Zahlkörper zu verallgemeinern. Aufgrund Matijasevičs negativer Antwort auf das zehnte hilbertsche Problem kann es selbstverständlich keinen Algorithmus geben, der für jede diophantische Gleichung über jedem Zahlkörper die Lösbarkeit entscheidet. Dies schließt allerdings noch nicht aus, dass es Zahlkörper gibt, über denen die Lösbarkeit jeder diophantischen Gleichung algorithmisch entscheidbar ist. Auf einige Zahlkörper wurde Matijasevičs Resultat bereits übertragen (vergleiche [PZ00]) und unter der Annahme der schwachen Shafarevich–Tate Vermutung konnten Mazur und Rubin [MR10] das Resultat für alle algebraischen Zahlkörper zeigen. Allerdings bewies Rumely [Rum86], dass es einen Algorithmus gibt, der die Lösbarkeit jeder diophantischen Gleichung über dem algebraischen Abschluss von $\mathbb{Q}$ entscheiden kann.

Auch bei diophantischen Gleichungen über Zahlkörpern kann untersucht werden, welche Klassen von Gleichungen algorithmisch entscheidbar sind. Cassels' Suchschranke für die kleinste Lösung einer quadratischen Form wurde von Raghavan [Rag75] auf Zahlkörper verallgemeinert.

In dieser Arbeit werden wir eine Suchschranke für die kleinste Lösung einer quadratischen diophantischen Gleichung über Zahlkörpern in mindestens drei Variablen herleiten. Im Folgenden gelte $a_{ij}, h_i, n \in \mathcal{O}$ und wir definieren die Höhe der Koeffizienten mithilfe der Einbettungen $\rho_1, \ldots, \rho_d$ des Zahlkörpers als

$$H_K = \max\{|\rho_l(a_{ij})|, |\rho_l(h_i)|, |\rho_l(n)| : 1 \leq i, j \leq s,\ l = 1, \ldots, d\}.$$

Das Ergebnis unserer Untersuchungen verallgemeinert Dietmanns Resultat im Fall $s \geq 3$ und liefert im Fall $K = \mathbb{Q}$ sogar eine kleinere Suchschranke.

Satz 1. *Sei $\varepsilon > 0$. Wenn die Matrix A nichtsingulär ist und die Anzahl r_0 der Einbettungen, in denen A definit ist, kleiner als d ist, ist die diophan-*

tische Gleichung (1.1) *genau dann im Ganzheitsring lösbar, wenn sie eine Lösung* $\mathbf{x} \in \mathcal{O}^s$ *mit*

$$|\rho_l(\mathbf{x})| \leq \begin{cases} C_{3,K} H_K^{36d+1080d/(d-r_0)-7/2+\varepsilon}, & s = 3, \\ C_{4,K} H_K^{84} + C_{4,K} H_K^{32d/(d-r_0)+1+\varepsilon} / |d_{min}^{(l)}|, & s = 4, \\ C_{s,K} H_K^{\max\{2s^2/(s-4), 2s^2 d/((d-r_0)(s-3))+1\}+\varepsilon} / |d_{min}^{(l)}|, & s \geq 5 \end{cases}$$

für alle $l = 1, \ldots, d$ *besitzt. Wenn* A *dagegen in jeder Einbettung definit ist, erfüllt jede Lösung*

$$|\rho_l(\mathbf{x})| \leq C_{s,K} H_K / |d_{min}^{(l)}|$$

für alle $s \geq 3$ *und* $l = 1, \ldots, d$*. Hierbei bezeichnet* $d_{min}^{(l)}$ *jeweils den betragsmäßig kleinsten Eigenwert beziehungsweise Singulärwert von* $\rho_l(A)$*. Die nur von* s*,* K *und* ε *abhängende Konstante* $C_{s,K}$ *ist effektiv.*

Genau wie bei Dietmann ist weniger die genaue Größe der Suchschranke von Bedeutung, sondern viel mehr die Tatsache, dass sie polynomiell in der Höhe der Koeffizienten wächst. Bemerkenswert ist, dass der Exponent unter der Voraussetzung einer vollständig indefiniten Matrix A außer bei $s = 3$ vom Zahlkörper unabhängig ist. Vermutlich ist es auch im Fall von drei Variablen möglich, einen vom Zahlkörper unabhängigen Exponenten zu erreichen.

Die Suchschranke impliziert insbesondere, dass die Lösbarkeit jeder quadratischen diophantischen Gleichung über einem Zahlkörper in mindestens drei Variablen und mit nichtsingulärem quadratischen Anteil algorithmisch entscheidbar ist. Da das schon oben erwähnte Argument von Grunewald und Segal [GS81] problemlos auf Zahlkörper übertragen werden kann, fehlt für den Beweis, dass die Lösbarkeit aller quadratischen Gleichungen über Zahlkörpern algorithmisch entscheidbar ist, nur noch die Behandlung des binären Falls.

Die Grundidee des Beweises von Satz 1 ist die gleiche wie bei Dietmann. Nach einiger Vorbereitung werden wir im zweiten Kapitel den linearen Term von (1.1) durch eine Kongruenzbedingung ersetzen und danach nur noch Gleichungen der Form

$$\sum_{i,j=1}^{s} a_{ij} x_i x_j = \kappa, \qquad x_i \equiv \xi_i \pmod{\eta} \tag{1.2}$$

mit $a_{ij}, \xi_i, \kappa, \eta \in \mathcal{O}$ betrachten.

Wenn die Anzahl der Variablen größer als fünf ist oder im Fall von vier Variablen der konstante Term κ nicht verschwindet, werden wir im dritten Kapitel ein Lokal-Global-Prinzip bei gleichzeitiger Größenkontrolle beweisen. Dazu nutzen wir die von Browning und Vishe [BV14] auf Zahlkörper übertragene Kloosterman-Verfeinerung der Kreismethode. Auf diese Weise können wir eine Schranke für die kleinste Lösung von (1.2) ermitteln.

Auf der Geometrie der Zahlen basiert ein Resultat von Raghavan [Rag75], das eine Suchschranke für die kleinsten nicht trivialen Nullstellen von quadratischen Formen über Zahlkörpern liefert. Im vierten Kapitel werden wir im Fall von drei oder vier Variablen Raghavans Resultat so modifizieren, dass die gefundene Lösung zusätzlich einer Kongruenzbedingung genügt und somit (1.2) im Fall von $s = 3, 4$ und $\kappa = 0$ erfüllt.

Den letzten verbliebenen Fall, in dem $s = 3$ und $\kappa \neq 0$ gilt, werden wir im fünften Kapitel betrachten. Da sich die Automorphismengruppe der ternären quadratischen Formen mithilfe von quadratischen Formen in vier Variablen parametrisieren lässt, können wir Satz 1 im Fall $s = 4$ nutzen, um einen Automorphismus für ternäre quadratische Formen zu finden, der in konkretisierbarer Hinsicht klein ist und eine Kongruenzbedingung erfüllt. Unter Zuhilfenahme der Reduktionstheorie quadratischer Formen können wir mit diesem Automorphismus aus einer gegebenen Lösung von (1.2) eine kleinere konstruieren. Wenn eine Lösung existiert, garantiert dieses Verfahren eine Lösung unter einer effektiv berechenbaren Suchschranke.

Danksagung: Mein Dank gebührt allen, die mich während meiner Promotion unterstützt haben. Zu großem Dank verpflichtet bin ich insbesondere Herrn Professor Brüdern, ohne den diese Arbeit nicht existieren würde, und Herrn Professor Blomer, der mir den entscheidenden Impuls für das fünfte Kapitel gab. Danken möchte ich auch Herrn Dr. Dietmann, mit dem ich während meines Aufenthalts am Royal Holloway College viele fruchtbare Diskussionen führen konnte.

2 Vorarbeiten

In diesem Kapitel führen wir die notwendige Notation und einige den Zahlkörper beschreibende Lemmata ein. Außerdem werden den linearen Term in (1.1) durch eine Kongruenzbedingung ersetzen und damit Satz 1 auf eine mit unseren Methoden besser handhabbare Proposition zurückführen.

Wie üblich ist ε im Folgenden stets eine kleine positive reelle Zahl, die an unterschiedlichen Stellen verschiedene Werte annehmen kann. Alle in dieser Arbeit auftretenden impliziten Konstanten dürfen sowohl von ε als auch vom Zahlkörper abhängen.

Die den algebraischen Zahlkörper K betreffende Notation ist größtenteils der Arbeit von Browning und Vishe [BV14] entnommen. Bezeichne D_K die absolute Diskriminante von K. Sei r_1 beziehungsweise $2r_2$ die Anzahl verschiedener reeller beziehungsweise komplexer Einbettungen von K. Es gilt $d = r_1 + 2r_2$. Seien $\rho_1, \dots, \rho_{r_1}$ die reellen Einbettungen und seien die komplexen Einbettungen $\rho_{r_1+1}, \dots, \rho_d$ so sortiert, dass für alle $1 \leq i \leq r_2$ die Einbettungen ρ_{r_1+i} und $\rho_{r_1+r_2+i}$ zueinander konjugiert sind. Wir bezeichnen mit V die d-dimensionale kommutative $\mathbb{R}$-Algebra

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \bigoplus_{l=1}^{r_1+r_2} K_l.$$

Die K_l sind jeweils die Vervollständigung von K bezüglich ρ_l und folglich gilt $K_l = \mathbb{R}$ für $l \leq r_1$ und $K_l = \mathbb{C}$ für $l > r_1$. Die $\mathbb{R}$-Algebra V hat für den Zahlkörper K die gleiche Bedeutung wie die reellen Zahlen für $\mathbb{Q}$. Wir identifizieren K mit seinem Bild in V bezüglich der kanonischen Einbettung

$$\alpha \mapsto (\rho_1(\alpha), \dots, \rho_{r_1+r_2}(\alpha)).$$

Insbesondere können wir jedes gebrochene Ideal aus K als ein Gitter in V auffassen.

Wir schreiben $v^{(l)} \in K_l$ für die Projektion von $v \in V$ auf die l-te Komponente. Es gilt also $v = \bigoplus_l v^{(l)}$. Diese Schreibweise werden wir auch für Vektoren und Matrizen verwenden. Die normalen Rechenoperationen, den Absolutbetrag, die komplexe Konjugation, aber auch das Transponieren von Matrizen setzen wir von K auf V (beziehungsweise $V^{s\times s}$) fort, indem wir

die Operationen auf V einbettungsweise definieren. Es gilt also für $v \in V$ und $A \in V^{s\times s}$ beispielsweise

$$|v| = \bigoplus_{l=1}^{r_1+r_2} |v^{(l)}| \in V, \qquad A^T = \bigoplus_{l=1}^{r_1+r_2} A^{(l)T} \in V^{s\times s}.$$

Die Norm und die Spur setzen wir auf $v \in V$ fort, indem wir

$$\begin{aligned} \mathrm{Nm}(v) &= v^{(1)} \cdots v^{(r_1)} |v^{(r_1+1)}|^2 \cdots |v^{(r_1+r_2)}|^2, \\ \mathrm{Tr}(v) &= v^{(1)} + \ldots + v^{(r_1)} + 2\Re(v^{(r_1+1)}) + \ldots + 2\Re(v^{(r_1+r_2)}) \end{aligned}$$

definieren.

Als Nächstes führen wir einige Höhen auf V und V^s ein. Sei

$$c_l = \begin{cases} 1, & l \le r_1, \\ 2, & l > r_1. \end{cases}$$

Für $v \in V$ definieren wir die Maximumsnorm $\langle v \rangle = \max_l |v^{(l)}|$ und setzen sie auf die offensichtliche Art und Weise auf Vektoren und Matrizen fort. Des Weiteren definieren wir für $\mathbf{v} \in V^s$ die euklidische Norm

$$\|\mathbf{v}\| = \sqrt{\sum_l c_l |\mathbf{v}^{(l)}|^2}$$

mithilfe der normalen euklidischen Norm $|\cdot|$ auf K_l^s. Von der Norm $\mathrm{Nm}(\cdot)$ können wir die Höhe

$$\mathscr{H} : V \to \mathbb{R}_{>0}, \quad v \mapsto \prod_{l=1}^{r_1+r_2} \max\{1, |v^{(l)}|\}^{c_l}$$

ableiten. Für diese folgt aus Lemma 5.3 von Browning und Vishe [BV14], dass für $a > 0$ und $\alpha < -1$ die Abschätzung

$$\int_{\{v\in V : \mathscr{H}(v) \le a\}} \mathscr{H}(v)^\alpha \, \mathrm{d}v \ll_\alpha 1 \tag{2.1}$$

gleichmäßig in a gilt. Die hierbei verwendete Volumenform auf V leiten wir vom Lebesguemaß auf $\mathbb{R}$ beziehungsweise auf $\Re(\mathbb{C})$ und $\Im(\mathbb{C})$ ab, indem wir

$$\mathrm{d}v = \mathrm{d}v^{(1)} \cdots \mathrm{d}v^{(r_1)} \mathrm{d}\Re(v^{(r_1+1)}) \mathrm{d}\Im(v^{(r_1+1)}) \cdots \mathrm{d}\Re(v^{(r_1+r_2)}) \mathrm{d}\Im(v^{(r_1+r_2)})$$

setzen. Diese Volumenform und die zugehörige Volumenform auf V^s werden wir auch im Folgenden verwenden.

Die Idealnorm eines ganzen Ideals $\mathfrak{a}$ sei $\mathrm{N}\,\mathfrak{a} = \#\mathcal{O}/\mathfrak{a}$. Wir ordnen jedem gebrochenen Ideal $\mathfrak{a}$ aus K sein duales Ideal

$$\widehat{\mathfrak{a}} = \{\alpha \in K : \mathrm{Tr}(\alpha\mathfrak{a}) \subset \mathbb{Z}\}$$

zu. Wenn

$$\mathfrak{d} = \{\alpha \in K : \alpha\widehat{\mathcal{O}} \subset \mathcal{O}\}$$

die Differente von K bezeichnet, gilt $\widehat{\mathfrak{a}} = \mathfrak{a}^{-1}\mathfrak{d}^{-1}$.

Um die Notation zu vereinfachen, setzen wir

$$(\mathbf{x}) = (x_1, \dots, x_s), \qquad (\mathbf{x}, \mathfrak{b}) = (x_1, \dots, x_s) + \mathfrak{b}$$

für beliebige Vektoren $\mathbf{x} \in K^s$ und gebrochene Ideale $\mathfrak{b} \subset K$. Für $a, b \in K$ schreiben wir $(a \cap b)$ anstelle von $(a) \cap (b)$. Außerdem bezeichne $\mathfrak{p}$ stets ein ganzes Primideal.

Des Weiteren wenden wir die Evaluation $\mathrm{v}_\mathfrak{p}(\cdot)$ bezüglich $\mathfrak{p}$ nicht nur auf Ideale, sondern auch auf Vektoren und Matrizen an, indem wir bei ihnen den größten gemeinsamen Teiler der Einträge betrachten.

2.1 Die Struktur des Ganzheitsrings

Obwohl der Ganzheitsring typischerweise kein Hauptidealring ist, kann er in den meisten Fällen trotzdem näherungsweise so behandelt werden, als ob er einer wäre. Die dafür notwendigen Resultate fasst das nächste Lemma zusammen.

Lemma 2.1. *Sei $\mathfrak{a}$ ein gebrochenes und seien $\mathfrak{b}$ und $\mathfrak{c}$ ganze Ideale. Weiterhin sei $x \in V$.*

(i) Für alle $i \geq 1$ existiert eine Einheit $\alpha \in \mathcal{O}$ mit $\langle \alpha^i x\rangle \asymp_i |\mathrm{Nm}\, x|^{1/d}$.

(ii) Es existiert ein zu $\mathfrak{b}$ teilerfremdes Primideal $\mathfrak{p}$ mit $\mathrm{N}\,\mathfrak{p} \ll \mathrm{N}\,\mathfrak{b}^\varepsilon$ und ein $z \in K$, sodass $\mathfrak{p}\mathfrak{a} = (z)$ und $\langle xz\rangle \asymp |\mathrm{Nm}\, xz|^{1/d}$ gilt.

(iii) Es gibt ein zu $\mathfrak{b}$ teilerfremdes $u \in \mathcal{O} \setminus \{0\}$ und ein $v \in \mathfrak{c}$, sodass

$$\langle u\rangle^d \asymp |\mathrm{Nm}\, u| \ll \mathrm{N}\,\mathfrak{b}^\varepsilon, \qquad \langle vx\rangle^d \asymp |\mathrm{Nm}\, vx| \ll |\mathrm{Nm}\, x|\,\mathrm{N}\,\mathfrak{c}\,\mathrm{N}\,\mathfrak{b}^\varepsilon$$

gilt und $uv^{-1}\mathfrak{c}$ ein zu $\mathfrak{b}$ teilerfremdes ganzes Ideal ist.

Beweis. Der erste Teil der Aussage ist eine geringfügige Verallgemeinerung von Lemma 2.1 von Browning und Vishe [BV14], bei der der Beweis sich nicht wesentlich ändert.

Die Idee für den Rest des Beweises entstammt dem Beweis von Lemma 2.2 von Browning und Vishe [BV14]. Das Ideal $\mathfrak{b}$ hat $O(\log \mathrm{N}\,\mathfrak{b})$ Primidealteiler und es gibt $\gg \mathrm{N}\,\mathfrak{b}^{\varepsilon/2}$ Primideale, deren Norm kleiner gleich $\mathrm{N}\,\mathfrak{b}^{\varepsilon}$ ist. Da die Primideale in den Idealklassen gleichverteilt sind, gibt es also ein Primideal $\mathfrak{p}$ mit $\mathrm{N}\,\mathfrak{p} \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}$, sodass $\mathfrak{p}\mathfrak{a}$ ein ganzes Hauptideal ist. Der Erzeuger z dieses Hauptideals ist nur bis auf eine Einheit bestimmt, sodass der Rest von (ii) aus (i) folgt.

Um auch den dritten Punkt zu zeigen, verwenden wir das eben verwendete Argument zweifach. Wir finden ein zu $\mathfrak{b}$ teilerfremdes Primideal $\mathfrak{p}_1$, sodass $\mathfrak{c}\mathfrak{p}_1 = (v)$ ein ganzes Hauptideal ist und

$$\langle vx\rangle^d \asymp |\mathrm{Nm}\, vx| \ll |\mathrm{Nm}\, x|\, \mathrm{N}\,\mathfrak{c}\, \mathrm{N}\,\mathfrak{b}^{\varepsilon}$$

gilt. Weiterhin gibt es ein zu $\mathfrak{b}$ teilerfremdes Primideal $\mathfrak{p}_2$, sodass $\mathfrak{p}_1\mathfrak{p}_2 = (u)$ ein ganzes Hauptideal mit

$$\langle u\rangle^d \asymp |\mathrm{Nm}\, u| \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}$$

ist. Der Rest folgt aus $uv^{-1}\mathfrak{c} = \mathfrak{p}_2$. □

Der Punkt (iii) dieses Lemmas ist insbesondere dann hilfreich, wenn wir $\mathfrak{c} = (\mathbf{y})$ oder $\mathfrak{c} = (\mathbf{y}, \mathfrak{b})$ für ein $\mathbf{y} \in \mathcal{O}^s$ setzen. Dann ist $(uv^{-1}\mathbf{y})$ teilerfremd zu $\mathfrak{b}$ beziehungsweise $\mathfrak{b}\mathfrak{c}^{-1}$ und es gilt $uv^{-1}\mathbf{y} \in \mathcal{O}^s$. Wir können also den größten gemeinsamen Teiler der Einträge eines Vektors fast vollständig herausteilen.

Das folgende Lemma zeigt, dass es in den Äquivalenzklassen bezüglich ganzer Ideale jeweils kleine Elemente gibt.

Lemma 2.2 ([Coc87, Theorem 3(b)])**.** *Sei $\mathfrak{b}$ ein ganzes Ideal und $\alpha \in \mathcal{O}$ eine Einheit. Dann gibt es zu jedem $x \in K$ ein $y \in K$ mit*

$$y \equiv x \pmod{\mathfrak{b}}, \qquad \langle \alpha y\rangle \ll N\mathfrak{b}^{1/d}.$$

Das vollständige Restsystem bezüglich eines zusammengesetzten Ideals verhält sich ebenso, wie man es in Analogie zu $\mathbb{Z}$ erwarten würde.

Lemma 2.3 ([BV14, Lemma 7.1])**.** *Seien $\mathfrak{a}$ und $\mathfrak{b}$ ganze Ideale.*

(i) Wenn $a \in \mathcal{O}$ für alle $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ stets $\mathrm{v}_{\mathfrak{p}}(a) = \mathrm{v}_{\mathfrak{p}}(\mathfrak{a})$ erfüllt, gilt

$$\mathcal{O}/\mathfrak{a}\mathfrak{b} = \{\alpha + \beta a : \alpha \in \mathcal{O}/\mathfrak{a}, \beta \in \mathcal{O}/\mathfrak{b}\}.$$

(ii) Wenn $\mathfrak{a}$ *und* $\mathfrak{b}$ *teilerfremd sind und wenn* $a, b \in \mathcal{O}$ *für alle* $\mathfrak{p} \mid \mathfrak{ab}$ *stets* $\mathrm{v}_\mathfrak{p}(a) = \mathrm{v}_\mathfrak{p}(\mathfrak{a})$ *und* $\mathrm{v}_\mathfrak{p}(b) = \mathrm{v}_\mathfrak{p}(\mathfrak{b})$ *erfüllen, gilt*

$$\mathcal{O}/\mathfrak{ab} = \{\beta a + \alpha c : \alpha \in \mathcal{O}/\mathfrak{a}, \beta \in \mathcal{O}/\mathfrak{b}\}.$$

Die hier notwendigen ganzen Zahlen a und b kann uns Lemma 2.1(ii) liefern. Insbesondere gibt es zu jedem Primideal $\mathfrak{p}$ ein $p \in \mathcal{O}$, sodass für $i \leq j$ stets

$$\mathcal{O}/\mathfrak{p}^j = \{\beta + \mu p^i : \beta \in \mathcal{O}/\mathfrak{p}^i, \mu \in \mathcal{O}/\mathfrak{p}^{j-i}\} \tag{2.2}$$

gilt. Daraus können wir folgern, dass zu jedem von $\mathfrak{p}^i$ geteilten $a \in \mathcal{O}$ ein $b \in \mathcal{O}$ mit

$$p^i b \equiv a \pmod{\mathfrak{p}^j} \tag{2.3}$$

existiert.

2.2 Glatte Gewichtsfunktionen

Im Rahmen dieser Arbeit werden wir eine unendlich oft differenzierbare Funktion $w : V^s \to \mathbb{C}$ mit kompaktem Träger als glatte Gewichtsfunktion auf V^s bezeichnen. Sei $\boldsymbol{\beta} \in \mathbb{Z}^d_{\geq 0}$ und w eine glatte Gewichtsfunktion auf V. Dann setzen wir

$$\partial^{\boldsymbol{\beta}} w(v) = \prod_{l=1}^{r_1} \partial_{v^{(l)}}^{\beta_l} \prod_{l=r_1+1}^{r_1+r_2} \partial_{\Re(v^{(l)})}^{\beta_l} \partial_{\Im(v^{(l)})}^{\beta_{r_2+l}} w(v).$$

In diesem Kontext sei $|\boldsymbol{\beta}| = \beta_1 + \ldots + \beta_d$ der Grad von $\boldsymbol{\beta}$. Wir werden diese Definition auch auf V^s verallgemeinert verwenden. Für jedes $N \geq 0$ und beliebige glatte Gewichtsfunktionen w auf V^s setzen wir außerdem

$$\lambda_w^N = \sup_{\substack{\mathbf{x} \in V^s \\ |\boldsymbol{\beta}| \leq N}} \left| \partial^{\boldsymbol{\beta}} w(\mathbf{x}) \right|.$$

Bezeichne $\mathscr{W}_s(V)$ die Menge aller glatten Gewichtsfunktionen w auf V^s, bei denen λ_w^N durch eine Konstante $a_N > 0$ beschränkt ist. Zudem sei $\mathscr{W}_s^+(V)$ die Teilmenge der nicht negativen Funktionen aus $\mathscr{W}_s(V)$.

2.3 Additive Charaktere über Zahlkörpern

Ein additiver Charakter modulo eines ganzen Ideals $\mathfrak{b}$ ist eine nicht überall verschwindende Funktion σ auf $\mathcal{O}/\mathfrak{b}$, für die $\sigma(x+y) = \sigma(x)\sigma(y)$ für alle $x, y \in \mathcal{O}$ gilt. Wenn σ nicht gleichzeitig ein Charakter modulo eines Ideals ist, das $\mathfrak{b}$ echt teilt, nennen wir σ primitiv. Für alle $x \in \mathcal{O}$ gilt die Orthogonalitätsrelation

$$\sum_{\sigma \pmod{\mathfrak{b}}} \sigma(x) = \begin{cases} \mathrm{N}\,\mathfrak{b}, & \mathfrak{b} \mid x, \\ 0, & \text{sonst.} \end{cases}$$

Hierbei bedeutet die Notation $\sum_{\sigma \pmod{\mathfrak{b}}}$, dass über alle additiven Charaktere modulo $\mathfrak{b}$ summiert wird. Wenn σ_0 ein primitiver Charakter modulo $\mathfrak{b}$ ist und x die Werte aus $\mathcal{O}/\mathfrak{b}$ durchläuft, liefert $\sigma_0(x\,\cdot)$ jeden Charakter modulo $\mathfrak{b}$ genau einmal. Derselbe Zusammenhang besteht zwischen $(\mathcal{O}/\mathfrak{b})^*$ und den primitiven Charakteren.

Wenn wir $\phi(\cdot) = e(\mathrm{Tr}\,\cdot) = \exp(2\pi\mathrm{i}\,\mathrm{Tr}(\cdot))$ schreiben, können wir aus Lemma 2.3 von Browning und Vishe [BV14] das folgende Resultat ableiten.

Lemma 2.4. *Zu jedem ganzen Ideal $\mathfrak{b}$ gibt es ein $\alpha \in \mathfrak{b}\mathfrak{d}$ und ein zu $\mathfrak{b}\mathfrak{d}$ teilerfremdes $\nu \in \mathcal{O}$, sodass $\phi(\nu/\alpha\,\cdot)$ ein nicht trivialer primitiver Charakter modulo $\mathfrak{b}$ ist. Sei $\gamma_\mathfrak{b} = \nu/\alpha$, dann gilt*

$$\sum_{\sigma \pmod{\mathfrak{b}}}^{*} \sigma(x) = \sum_{a \in (\mathcal{O}/\mathfrak{b})^*} \phi(a\gamma_\mathfrak{b} x)$$

für alle $x \in \mathcal{O}$.

Dabei darf $\gamma_\mathfrak{b}$ mit einer beliebigen zu $\mathfrak{b}\mathfrak{d}$ teilerfremden ganzen Zahl multipliziert werden, ohne dass $\gamma_\mathfrak{b}$ die genannten Eigenschaften verliert. Deshalb können wir $\gamma_{\mathfrak{p}^l}$ für alle $l \geq 0$ so wählen, dass für das p aus (2.2) jeweils $\gamma_{\mathfrak{p}^l} = p\gamma_{\mathfrak{p}^{l+1}}$ gilt.

2.4 Quadratische Formen

Für jede Matrix $A = (a_{ij}) \in K^{s\times s}$ setzen wir

$$\|A^{(l)}\| = \max_{ij} |a_{ij}^{(l)}|, \qquad \mathrm{den}(A) = \{x \in \mathcal{O} : xa_{ij} \in \mathcal{O}\ \forall i, j\}.$$

Mit $\mathrm{den}(A)$ wird also das kleinste ganze Ideal bezeichnet, bei dem $\mathrm{den}(A)a_{ij}$ für alle i und j ein ganzes Ideal ist. Des Weiteren sei $\mathrm{adj}\,A = (\det A)A^{-1}$ die Adjunkte der nichtsingulären Matrix A.

Für beliebige Matrizen $A, B \in V^{s\times s}$ und Vektoren $\mathbf{x} \in V^s$ setzen wir außerdem $A[B] = B^T AB$ und $A[\mathbf{x}] = \mathbf{x}^T A\mathbf{x}$.

Solange nicht explizit etwas anderes erwähnt wird, sei $A \in \mathcal{O}^{s\times s}$ im Folgenden eine symmetrische, nichtsinguläre Matrix mit Determinante Δ. Weiterhin seien $d_i^{(l)}$ für $l \le r_1$ die Eigenwerte und für $l > r_1$ die Singulärwerte von $A^{(l)} = (a_{ij}^{(l)}) \in K_l^{s\times s}$. Es gilt $\Delta^{(l)} = \prod d_i^{(l)}$ und wir setzen

$$d_i = \bigoplus_l d_i^{(l)}, \qquad\qquad d_{\max} = \bigoplus_l \max_i |d_i^{(l)}|.$$

Für $l \le r_1$ folgt aus dem Satz von Gershgorin (siehe z. B. [SB90, Satz 6.9.4]) die Abschätzung $|d_i^{(l)}| \ll \langle A\rangle$. Durch Anwendung des gleichen Satzes auf die Eigenwerte der hermiteschen Matrix $A^{(l)H}A^{(l)}$ folgt dieselbe Aussage auch für $l > r_1$. Zusätzlich setzen wir

$$\sigma_i^{(l)} = d_i^{(l)}/|d_i^{(l)}|, \qquad\qquad \sigma = \bigoplus_l \sigma^{(l)} \in V.$$

Für $l > r_1$ gilt $\sigma_i^{(l)} = 1$ für alle $i = 1, \dots, s$. Wir sortieren die Einbettungen von K so, dass $A^{(l)}$ genau dann definit ist, wenn $l \le r_0$ gilt. Schließlich setzen wir noch

$$\gamma(r_0) = \begin{cases} 0, & r_0 = d, \\ 1/(d - r_0), & \text{sonst.} \end{cases}$$

Der in der Einleitung postulierte Satz 1 folgt leicht aus dem folgenden Resultat, das Proposition 1 von Dietmann [Die03] verallgemeinert.

Proposition 1. *Sei $s \ge 3$. Es gelte $\eta \in \mathcal{O} \setminus \{0\}$, $\kappa \in \mathcal{O}$ und $\boldsymbol{\xi} \in \mathcal{O}^s$. Wenn*

$$A[\mathbf{x}] = \kappa, \qquad\qquad \mathbf{x} \equiv \boldsymbol{\xi} \quad (\eta) \tag{2.4}$$

im Ganzheitsring lösbar ist, dann existiert eine Lösung $\mathbf{x} \in \mathcal{O}^s$, bei der $|\mathbf{x}^{(l)}/\Delta^{(l)}|$ für alle l kleiner ist als

$$\ll \begin{cases} \langle A\rangle^2 \,|\mathrm{Nm}\,\eta^3\Delta|^{1/d+\varepsilon}, & s = 3, \kappa = 0, \\ |\kappa^{(l)}/\Delta^{(l)2}|^{1/2}(\langle A\rangle^d + |\mathrm{Nm}\,\kappa| + |\mathrm{Nm}\,\Delta|)^{9/2+108\gamma(r_0)+\varepsilon} & \\ \quad \times(\langle A\rangle^{24d}\,|\mathrm{Nm}\,\Delta^{40}\eta^6|)^{2\gamma(r_0)+\varepsilon}/\min_i\{1, |\Delta^{(l)}d_i^{(l)}|\}, & s = 3, \kappa \ne 0, \\ \langle A\rangle^5\,|\mathrm{Nm}\,\eta^9\Delta^3|^{1/d+\varepsilon} + \langle A\rangle^8\,|\mathrm{Nm}\,\eta|^{20/d+\varepsilon}|\mathrm{Nm}\,\Delta|^{-1/d}, & s = 4, \kappa = 0, \\ |\kappa^{(l)}/\Delta^{(l)2}|^{1/2}/\min_i|d_i^{(l)}|^{1/2} & \\ \quad \times \mathrm{N}(d_{max}^s\Delta(\eta\cap\Delta)^{2(s-1)})^{\gamma(r_0)/(s-3)+\varepsilon}, & s \ge 4, \kappa \ne 0, \\ |\mathrm{Nm}\,\eta/\Delta|^{1/d}/\min_i|d_i^{(l)}|^{1/2} & \\ \quad \times \mathrm{N}(d_{max}^s\Delta(\eta\cap\Delta)^{2(s-1)})^{1/(s-4)d+\varepsilon}, & s \ge 5, \kappa = 0. \end{cases}$$

Bevor wir jedoch zu dem Beweis dieser Proposition kommen, dem der gesamte Rest dieser Arbeit gewidmet ist, leiten wir mithilfe dieser Proposition Satz 1 her.

Beweis von Satz 1. Der Beweis basiert auf §1.3 von Dietmann [Die03]. Wegen

$$A[2\Delta\mathbf{x}+\boldsymbol{\xi}] = 4\Delta^2 A[\mathbf{x}] + 4\Delta\mathbf{x}^T A\boldsymbol{\xi} + A[\boldsymbol{\xi}]$$

ist $\mathbf{x} \in \mathcal{O}^s$ genau dann eine Lösung der quadratischen diophantischen Gleichung (1.1), wenn

$$\mathbf{y} = 2\Delta\mathbf{x} + \boldsymbol{\xi}$$

eine ganze Lösung von (2.4) für

$$\eta = 2\Delta, \qquad \boldsymbol{\xi} = (\operatorname{adj} A)\mathbf{h}, \qquad \kappa = 4\Delta^2 n + A[\boldsymbol{\xi}]$$

ist.

Da wir A in jeder Einbettung mithilfe unitärer Matrizen diagonalisieren können und die Einträge unitärer Matrizen beschränkt sind, ist für alle l stets $\|A^{(l)-1}\| \ll |d_{\min}^{(l)}|^{-1}$ erfüllt. Außerdem gilt

$$\frac{|\kappa^{(l)}|^{1/2}}{|\Delta^{(l)}|} \ll |n^{(l)}|^{1/2} + \|A^{(l)-1}\|^{1/2} H_K$$

für alle l. Mithilfe der Abschätzung aus dem vorhergehenden Lemma folgt die Behauptung für $r_0 < d$.

Wenn A vollständig definit ist, gilt für jede Lösung $\mathbf{y}$ von (2.4) die Abschätzung

$$|\mathbf{y}^{(l)}| \ll \frac{|\kappa^{(l)}|^{1/2}}{|d_{\min}^{(l)}|^{1/2}}, \qquad l = 1, \dots, r_1 + r_2.$$

Entsprechend erfüllt jede Lösung $\mathbf{x}$ von (1.1) die Ungleichung

$$|\mathbf{x}^{(l)}| \ll \frac{|n^{(l)}|^{1/2} + |A^{(l)-1}[\mathbf{h}]|^{1/2}}{|d_{\min}^{(l)}|^{1/2}} + |A^{(l)-1}\mathbf{h}| \ll \frac{H_K}{|d_{\min}^{(l)}|}$$

für alle l. □

Wie in der Einleitung bereits erwähnt, werden wir abhängig von s und κ drei grundsätzlich verschiedene Methoden verwenden, um Proposition 1 zu beweisen. Jeder dieser Methoden ist ein eigenes Kapitel gewidmet.

3 Die Kreismethode über Zahlkörpern

Die klassische Kreismethode ist nicht dazu geeignet, eine quadratische Form in weniger als fünf Variablen zu behandeln. Erst die von Kloosterman entwickelte Kloosterman-Verfeinerung der Kreismethode [Klo26] macht es möglich, auch für vier Variablen einen ausreichend kleinen Fehlerterm zu erhalten. Eine moderne Variante der Kloosterman-Verfeinerung hat Heath-Brown [Hea96] aufbauend auf der glatten Deltafunktion von Duke, Friedlander und Iwaniec [DFI93] entwickelt. Es war diese Methode, die Dietmann dazu verwendet hat, seine Version von Proposition 1 im Fall $s \geq 5$ oder $s = 4$ und $\kappa \neq 0$ zu beweisen. In Analogie dazu werden wir die Verallgemeinerung von Heath-Browns Methode auf Zahlkörper von Browning und Vishe [BV14] einsetzen, um Dietmanns Resultat auf Zahlkörper zu übertragen. Das Ziel ist dabei die folgende Proposition.

Proposition 2. *Sei $s \geq 4$ und sei $A \in \mathcal{O}^{s\times s}$ eine symmetrische, nichtsinguläre und nicht vollständig definite Matrix. Weiterhin seien $\eta \in \mathcal{O} \setminus \{0\}$, $\kappa \in \mathcal{O}$ und $\boldsymbol{\xi} \in \mathcal{O}^s$. Für diese gelte $A[\boldsymbol{\xi}] = \kappa$. Außerdem gelte $s = 4$ nur, wenn κ nicht verschwindet. Wenn der Parameter*

$$P = \bigoplus_l P^{(l)} \in \bigoplus_l \mathbb{R}_{>0} \subset V$$

sowohl $P^{(l)} \gg |\kappa^{(l)}|^{1/2}$ für alle l als auch $P^{(l)} \ll |\kappa^{(l)}|^{1/2}$ für alle $l \leq r_0$ erfüllt und

$$\frac{\operatorname{Nm} P}{\langle P\rangle^{\varepsilon}} \gg \begin{cases} \mathrm{N}\left(d_{max}^s \Delta(\eta\cap\Delta)^{2(s-1)}(\boldsymbol{\xi})^{2(s-1)}\right)^{1/(s-3)}, & \kappa \neq 0, \\ \mathrm{N}\left(d_{max}^s \Delta(\eta\cap\Delta)^{2(s-1)}(\boldsymbol{\xi})^{2(s-1)}\right)^{1/(s-4)}, & \kappa = 0 \end{cases}$$

gilt, hat (2.4) *eine Lösung $\mathbf{x} \in \mathcal{O}^s$ mit*

$$|\mathbf{x}^{(l)}| \ll \frac{P^{(l)}}{\min_i |d_i^{(l)}|^{1/2}}, \qquad l = 1, \dots, r_1 + r_2.$$

Als Erstes werden wir dieses Resultat dazu nutzen, Proposition 1 für den Fall zu beweisen, dass $s \geq 5$ oder sowohl $s = 4$ als auch $\kappa \neq 0$ gilt.

Teilbeweis von Proposition 1. Wir können o. B. d. A. davon ausgehen, dass (2.4) im Ganzheitsrings lösbar ist. Da $\boldsymbol{\xi}$ in die zu beweisende Proposition nur modulo η eingeht, dürfen wir sogar $A[\boldsymbol{\xi}] = \kappa$ annehmen.

Wenn A vollständig definit ist, gilt analog zum rationalen Fall für jede Lösung in jeder Einbettung

$$|\mathbf{x}^{(l)}| \ll \frac{|\kappa^{(l)}|^{1/2}}{\min_i |d_i^{(l)}|^{1/2}}.$$

Deswegen können wir im Folgenden davon ausgehen, dass A nicht vollständig definit ist.

Aus Lemma 2.1(iii) folgt die Existenz eines $v \in (\boldsymbol{\xi})$ und eines zu η teilerfremden $u \in \mathcal{O} \setminus \{0\}$, sodass

$$\boldsymbol{\xi}' = \frac{u}{v}\boldsymbol{\xi} \in \mathcal{O}^s, \qquad \kappa' = \frac{u^2}{v^2}\kappa = A[\boldsymbol{\xi}'] \in \mathcal{O}, \qquad \mathrm{N}(\boldsymbol{\xi}') \ll |\mathrm{Nm}\,\eta|^{\varepsilon}$$

gilt. Um mithilfe von Proposition 2 eine kleine Lösung $\mathbf{x}' \in \mathcal{O}^s$ von

$$A[\mathbf{x}'] = \kappa', \qquad \mathbf{x}' \equiv \boldsymbol{\xi}' \pmod{\eta}$$

finden zu können, müssen wir $P = \bigoplus_l P^{(l)}$ geeignet wählen.

Im Fall $\kappa \neq 0$ sei

$$P^{(l)} \asymp \begin{cases} |\kappa'^{(l)}|^{1/2}, & l \leq r_0, \\ |\kappa'^{(l)}|^{1/2}\,\mathrm{N}\left(d_{\max}^s \Delta(\eta \cap \Delta)^{2(s-1)}\right)^{\gamma(r_0)/(s-3)+\varepsilon}, & l > r_0. \end{cases}$$

Wegen $\mathrm{N}(\boldsymbol{\xi}') \ll |\mathrm{Nm}\,\eta|^{\varepsilon}$ gilt

$$\frac{\mathrm{Nm}\,P}{\langle P \rangle^{\varepsilon}} \gg \mathrm{N}\left(d_{\max}^s \Delta(\eta \cap \Delta)^{2(s-1)} (\boldsymbol{\xi})^{2(s-1)}\right)^{1/(s-3)}.$$

Also gibt es eine Lösung $\mathbf{x}' \in \mathcal{O}^s$ mit

$$|\mathbf{x}'^{(l)}| \ll \frac{P^{(l)}}{\min_i |d_i^{(l)}|^{1/2}}, \qquad l = 1, \ldots, r_1 + r_2.$$

Demnach ist $\mathbf{x} = vu^{-1}\mathbf{x}'$ eine Lösung von (2.4) und für alle l gilt die Abschätzung

$$|\mathbf{x}^{(l)}| \ll \frac{|\kappa^{(l)}|^{1/2}}{\min_i |d_i^{(l)}|^{1/2}}\,\mathrm{N}\left(d_{\max}^s \Delta(\eta \cap \Delta)^{2(s-1)}\right)^{\gamma(r_0)/(s-3)+\varepsilon}.$$

Im Fall $\kappa = 0$ können wir davon ausgehen, dass A in keiner Einbettung definit ist, da andernfalls höchstens $\mathbf{x} = \mathbf{0}$ eine Lösung von (2.4) ist. Wir setzen

$$P^{(l)} \asymp \mathrm{N}\left(d_{\max}^s \Delta(\eta \cap \Delta)^{2(s-1)}\right)^{1/(s-4)d+\varepsilon}, \qquad l = 1, \dots, r_1 + r_2.$$

Analog zu dem obigen Vorgehen können wir die Existenz einer Lösung $\mathbf{x}'$ mit

$$|\mathbf{x}'^{(l)}| \ll \frac{P^{(l)}}{\min_i |d_i^{(l)}|^{1/2}}, \qquad l = 1, \dots, r_1 + r_2$$

folgern. Da u und η teilerfremd sind, finden wir mithilfe des Lemmas 2.2 ein $m \in \mathcal{O}$ mit

$$\left\langle m \frac{\mathrm{Nm}\, \Delta^{1/d}}{\Delta} \right\rangle \ll |\mathrm{Nm}\, \eta|^{1/d}, \qquad mu \equiv v \quad (\eta),$$

sodass $\mathbf{x} = m\mathbf{x}'$ die Abschätzung

$$\left| \frac{\mathbf{x}^{(l)}}{\Delta^{(l)}} \right| \ll \frac{|\mathrm{Nm}\, \eta/\Delta|^{1/d}}{\min_i |d_i^{(l)}|^{1/2}} \mathrm{N}\left(d_{\max}^s \Delta(\eta \cap \Delta)^{2(s-1)}\right)^{1/(s-4)d+\varepsilon}$$

für alle l erfüllt und eine Lösung von (2.4) ist. □

Nun widmen wir uns dem Beweis von Proposition 2. Im Rest dieses Kapitels gelte stets

$$s \geq 4, \qquad \eta \in \mathcal{O} \setminus \{0\}, \qquad \kappa \in \mathcal{O}, \qquad \boldsymbol{\xi} \in \mathcal{O}^s.$$

Außerdem sei nicht gleichzeitig $s = 4$ und $\kappa = 0$ erfüllt.

3.1 Die Kreismethode von Browning und Vishe

Die Kreismethode von Browning und Vishe baut auf eine Formel für die Indikatorfunktion

$$\delta_K(\mathfrak{a}) = \begin{cases} 1, & \mathfrak{a} = (0), \\ 0, & \text{sonst} \end{cases}$$

auf ganzen Idealen $\mathfrak{a}$ auf.

Satz 2 ([BV14, Theorem 1.2])**.** *Sei $Q > 1$. Dann existiert eine positive Konstante c_Q und eine unendlich oft differenzierbare Funktion*

$$h(x, y) : (0, \infty) \times \mathbb{R} \to \mathbb{R},$$

sodass

$$\delta_K(\mathfrak{a}) = \frac{c_Q}{Q^{2d}} \sum_{(0)\neq\mathfrak{b}\subset\mathcal{O}} \sideset{}{^*}\sum_{\sigma \pmod{\mathfrak{b}}} \sigma(\mathfrak{a}) h\left(\frac{\mathrm{N}\,\mathfrak{b}}{Q^d}, \frac{\mathrm{N}\,\mathfrak{a}}{Q^{2d}}\right)$$

für alle ganzen Ideale $\mathfrak{a}$ erfüllt ist. Es gilt

$$c_Q = 1 + O_N(Q^{-N})$$

und $h(x, y) \ll x^{-1}$ für alle y. Weiterhin gilt $h(x, y) \neq 0$ nur dann, wenn $x \leq \max\{1, 2|y|\}$ erfüllt ist.

Die Funktion $h(x, y)$ besitzt eine Reihe hilfreicher Eigenschaften. Bereits die Definition der Funktion in der Arbeit von Browning und Vishe [BV14] impliziert $h(x, y) = h(x, |y|)$. Sei $j \in \mathbb{Z}_{\geq 0}$. Aus Lemma 3.2 von Browning und Vishe [BV14] folgt

$$\frac{\partial^j}{\partial y^j} h(x, y) \ll_j x^{-j-1}. \tag{3.1}$$

Browning und Vishe [BV14] beweisen in ihrem Lemma 4.1 außerdem, dass für beliebige Gewichtsfunktionen $f \in \mathscr{W}_1(V)$ stets

$$\int_V f(v) h(x, \mathrm{Nm}(v))\, \mathrm{d}v = \frac{\sqrt{D_K}}{2^{r_2}} f(0) + O_j(\lambda_f^{2d(j+1)} x^j) \tag{3.2}$$

gilt. Wenn wir uns auf eine nicht negative Gewichtsfunktion $w_1 \in \mathscr{W}_1^+(V)$ beschränken, können wir aus den Lemmata 6.3 und 6.4 von Browning und Vishe [BV14] folgern, dass für

$$\begin{aligned} 0 < Q^{-1} \leq \rho \ll 1, \qquad v \in V, \\ p_\rho(v) = \int_V w_1(x) h(\rho, \mathrm{Nm}(x)) \phi(-vx)\, \mathrm{d}x \end{aligned} \tag{3.3}$$

sowohl

$$p_\rho(v) \ll_{w_1, j} \rho^{-1} (\rho^{-1} Q^\varepsilon |\mathscr{H}(v)|^{-1})^j \tag{3.4}$$

als auch

$$p_\rho(v) \ll_{w_1} |\log \rho|^{r_1+r_2-1} \tag{3.5}$$

gilt. Mithilfe von (2.1) können wir insbesondere

$$\int_V p_\rho(v)\,\mathrm{d}v \ll_{w_1} \rho^{-3}Q^\varepsilon \tag{3.6}$$

schließen.

Wir werden die Formel für die Indikatorfunktion dazu nutzen, die gewichtete Zählfunktion

$$N(P) = \sum_{\substack{\mathbf{x}\in\mathcal{O}^s \\ \mathbf{x}\equiv\boldsymbol{\xi}(\eta)}} \delta_K(A[\mathbf{x}]-\kappa)W\left(\frac{\mathbf{x}}{P}\right)$$

für eine Gewichtsfunktion $W : V^s \to \mathbb{R}_{\geq 0}$ und einen Parameter $P = \bigoplus_l P^{(l)}$ mit $P^{(l)} \in \mathbb{R}_{>0}$ zu untersuchen. Abkürzend werden wir im Folgenden $\mathfrak{L} = \log\langle P\rangle$ schreiben.

Bei der Gewichtsfunktion verbinden wir Ideen von Dietmann mit Ideen von Browning und Vishe, um so einerseits die Diagonalisierbarkeit quadratischer Formen wie Dietmann [Die03] ausnutzen und andererseits möglichst viele Teile des Arguments von Browning und Vishe [BV14] wiederverwenden zu können.

Sei $\widetilde{w}_0 \in \mathscr{W}_1^+(\mathbb{R})$ eine glatte Gewichtsfunktion, die $\widetilde{w}_0(y) = 1$ für $y \leq 1/4$ und $\widetilde{w}_0(y) = 0$ für $y > 1$ erfüllt. Im Folgenden darf jede implizite Konstante von dieser Gewichtsfunktion abhängen. Für jedes $l = 1, \dots, r_1 + r_2$ definieren wir die Gewichtsfunktionen

$$w^{(l)} : K_l^s \to \mathbb{R}_{\geq 0}, w^{(l)}(\mathbf{x}^{(l)}) = \exp\left(-c_l\mathfrak{L}^4\sum_{i=1}^s |d_i^{(l)}x_i^{(l)2}|\right),$$
$$w_0^{(l)} : K_l^s \to \mathbb{R}_{\geq 0}, w_0^{(l)}(\mathbf{x}^{(l)}) = \widetilde{w}_0\left(\sum_{i=1}^s |d_i^{(l)}x_i^{(l)2}|\right).$$

Weiterhin seien $R^{(l)} \in K_l^{s\times s}$ für $l \leq r_1$ orthogonale und für $l > r_1$ unitäre Matrizen, sodass A durch $R = \bigoplus_l R^{(l)} \in V^{s\times s}$ diagonalisiert wird und somit

$$R^T AR = \operatorname{diag}(d_1, \dots, d_s) \in V^{s\times s}$$

gilt. Für $\mathbf{x} \in V^s$ setzen wir

$$w(\mathbf{x}) = \prod_{l=1}^{r_1+r_2} w^{(l)}(R^{(l)H}\mathbf{x}^{(l)}), \qquad w_0(\mathbf{x}) = \prod_{l=1}^{r_1+r_2} w_0^{(l)}(R^{(l)H}\mathbf{x}^{(l)})$$

und wählen ein geeignetes $\mathbf{h} \in V^s$. Dann ist

$$W(\mathbf{x}) = w(\mathbf{x} - \mathbf{h}) w_0(\mathbf{x} - \mathbf{h})$$

eine für unsere Zwecke verwendbare Gewichtsfunktion. Es wird sich herausstellen, dass ein $\mathbf{h}$ geeignet ist, wenn

$$\mathbf{h}' = \operatorname{diag}\left(|d_1|^{1/2}, \dots, |d_s|^{1/2}\right) R^H \mathbf{h} \in V^s$$

die Eigenschaften

$$\langle \mathbf{h}' \rangle \ll 1, \qquad \sum_i \sigma_i h_i'^2 = \frac{\kappa}{P^2}, \qquad \min_l |h_1'^{(l)}| \geq 2 \tag{3.7}$$

besitzt. Wir werden im Folgenden stets annehmen, dass $\mathbf{h}$ in diesem Sinne geeignet gewählt ist und zusätzlich auch dass $\langle P \rangle \gg 1$ gilt. Dies impliziert insbesondere $P^{(l)} \gg |\kappa^{(l)}|^{1/2}$ für alle l und $P^{(l)} \ll |\kappa^{(l)}|^{1/2}$ für alle $l \leq r_0$.

Das folgende an Theorem 5.1 von Browning und Vishe [BV14] angelehnte Lemma bildet unseren Startpunkt für die Kreismethode.

Lemma 3.1. *Es gilt*

$$N(P) = \frac{c_P 2^{r_2 s}}{D_K^{s/2} \operatorname{Nm} P^2} \sum_{\substack{(0) \neq \mathfrak{b} \subseteq \mathcal{O} \\ \mathrm{N}\,\mathfrak{b} \ll \operatorname{Nm} P}} \sum_{\mathbf{m} \in \widehat{\mathfrak{b} \cap \eta}^s} \frac{S_\mathfrak{b}(\mathbf{m}) I_\mathfrak{b}(\mathbf{m})}{\mathrm{N}(\mathfrak{b} \cap \eta)^s} \tag{3.8}$$

mit

$$S_\mathfrak{b}(\mathbf{m}) = \sideset{}{^*}\sum_{a\ (\mathfrak{b})} \sum_{\substack{\mathbf{x}\ (\mathfrak{b} \cap \eta) \\ \mathbf{x} \equiv \boldsymbol{\xi}\ (\eta)}} \phi\Big(a\gamma_\mathfrak{b}(A[\mathbf{x}] - \kappa) + \mathbf{m}^T \mathbf{x}\Big),$$

$$I_\mathfrak{b}(\mathbf{m}) = \int_{V^s} W\left(\frac{\mathbf{x}}{P}\right) h\left(\frac{\mathrm{N}\,\mathfrak{b}}{\operatorname{Nm} P}, \frac{\operatorname{Nm}(A[\mathbf{x}] - \kappa)}{\operatorname{Nm} P^2}\right) \phi(-\mathbf{m}^T \mathbf{x})\, \mathrm{d}\mathbf{x}.$$

Beweis. Aus Satz 2 folgt die Gleichheit von $N(P)$ zu

$$\frac{c_P}{\operatorname{Nm} P^2} \sum_{(0) \neq \mathfrak{b} \subseteq \mathcal{O}\sigma} \sideset{}{^*}\sum_{(\mathrm{mod}\ \mathfrak{b})} \sum_{\substack{\mathbf{x} \in \mathcal{O}^s \\ \mathbf{x} \equiv \boldsymbol{\xi}(\eta)}} \sigma(A[\mathbf{x}] - \kappa) W\left(\frac{\mathbf{x}}{P}\right) h\left(\frac{\mathrm{N}\,\mathfrak{b}}{\operatorname{Nm} P}, \frac{\operatorname{Nm}(A[\mathbf{x}] - \kappa)}{\operatorname{Nm} P^2}\right).$$

Da für alle $\mathbf{x}/P \in \operatorname{supp}(W)$ und jedes l stets

$$\begin{aligned}
&\left|A^{(l)}[\mathbf{x}^{(l)}] - \kappa^{(l)}\right| \\
&\leq \max\left\{\left|A^{(l)}[\mathbf{y}^{(l)}] - \kappa^{(l)}\right| : w_0^{(l)}\left(R^{(l)H}(\mathbf{y}^{(l)}/P^{(l)} - \mathbf{h}^{(l)})\right) \neq 0\right\} \\
&\leq \max\left\{\sum_{i=1}^s \left|d_i^{(l)}(y_i^{(l)} + P^{(l)} R^{(l)H} h_i^{(l)})^2\right| + \left|\kappa^{(l)}\right| : w_0^{(l)}(\mathbf{y}^{(l)}/P^{(l)}) \neq 0\right\} \\
&\ll P^{(l)2}
\end{aligned} \tag{3.9}$$

gilt, lässt sich die obige Summation auf diejenigen $\mathfrak{b}$ beschränken, die $\mathrm{N}\,\mathfrak{b} \ll \mathrm{Nm}\,P$ erfüllen. Außerdem ist im obigen Ausdruck die innere Summe gleich

$$\sum_{\substack{\mathbf{x}\ (\mathfrak{b}\cap\eta)\\ \mathbf{x}\equiv\boldsymbol{\xi}(\eta)}} \sigma(A[\mathbf{a}]-\kappa) \sum_{\mathbf{y}\in(\mathfrak{b}\cap\eta)^s} W\left(\frac{\mathbf{x}+\mathbf{y}}{P}\right) h\left(\frac{\mathrm{N}\,\mathfrak{b}}{\mathrm{Nm}\,P}, \frac{\mathrm{Nm}(A[\mathbf{x}+\mathbf{y}]-\kappa)}{\mathrm{Nm}\,P^2}\right).$$

Für die innere Summe dieses Ausdrucks folgt aus der mehrdimensionalen poissonschen Summenformel (vergleiche [Ski94, §5] beziehungsweise [MF80]) die Gleichheit zu

$$\frac{2^{r_2 s}}{D_K^{s/2}\,\mathrm{N}(\mathfrak{b}\cap\eta)^s} \sum_{\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{\,s}} \phi(\mathbf{m}^T\mathbf{x}) I_{\mathfrak{b}}(\mathbf{m}).$$

Wegen Lemma 2.4 ist damit alles bewiesen. □

Um aus (3.8) eine asymptotische Formel herleiten zu können, benötigen wir ein genaueres Verständnis der Fourierintegrale $I_{\mathfrak{b}}(\mathbf{m})$ und der Exponentialsummen $S_{\mathfrak{b}}(\mathbf{m})$. Diese werden wir in den nächsten vier Kapiteln eingehend untersuchen. Es wird sich herausstellen, dass der Hauptterm nur aus den Termen mit $\mathbf{m} = \mathbf{0}$ entsteht und alle anderen Terme lediglich zum Fehlerterm beitragen.

3.2 Fourierintegrale

Die Fourierintegrale können wir wie in §6 von Browning und Vishe [BV14] abschätzen. Um die Notation zu vereinfachen, schreiben wir für beliebige Ideale $\mathfrak{b}$ des Ganzheitsrings $\rho = \mathrm{N}\,\mathfrak{b}/\,\mathrm{Nm}\,P$.

Analog zu Lemma 5.2 von Browning und Vishe [BV14] erhalten wir durch mehrfache partielle Integration das folgende Lemma.

Lemma 3.2. *Wenn $\mathfrak{b} \neq (0)$ ein Ideal des Ganzheitsrings mit $\mathrm{N}\,\mathfrak{b} \ll \mathrm{Nm}\,P$ ist, gilt für alle $\mathbf{m} \in V^s \setminus \{\mathbf{0}\}$ und jedes $N \in \mathbb{Z}_{\geq 0}$ die Abschätzung*

$$I_{\mathfrak{b}}(\mathbf{m}) \ll_N \rho^{-1} \frac{\mathrm{Nm}\,P^s}{|\mathrm{Nm}\,\Delta|^{1/2}} \left(\rho\mathfrak{L}^{-2}\left\langle \frac{P\mathbf{m}}{d_{max}^{1/2}}\right\rangle\right)^{-N}.$$

Beweis. Es gilt

$$\begin{aligned}|I_{\mathfrak{b}}(\mathbf{m})| &= \operatorname{Nm} P^s \left| \int_{V^s} W(\mathbf{x}) h\left(\rho, \frac{\operatorname{Nm}(A[P\mathbf{x}]-\kappa)}{\operatorname{Nm} P^2}\right) \phi(-P\mathbf{m}^T\mathbf{x})\,\mathrm{d}\mathbf{x}\right| \\ &= \frac{\operatorname{Nm} P^s}{|\operatorname{Nm}\Delta|^{1/2}} \left| \int_{V^s} \exp(-\mathfrak{L}^4\|\mathbf{x}\|^2) \prod_{l=1}^{r_1+r_2} \widetilde{w}_0(|\mathbf{x}^{(l)}|^2) \right. \\ &\quad \left. \cdot\, h\left(\rho, \operatorname{Nm}\Big(\sum_i \sigma_i(x_i+h_i')^2 - \kappa/P^2\Big)\right) \phi(-P\widetilde{\mathbf{m}}^T\mathbf{x})\,\mathrm{d}\mathbf{x}\right| \qquad (3.10)\end{aligned}$$

mit

$$\widetilde{\mathbf{m}} = \operatorname{diag}\Big(|d_1|^{-1/2}, \dots, |d_s|^{-1/2}\Big) R^T\mathbf{m} \in V^s.$$

Daraus dass die Multiplikation mit R die euklidische Norm $\|\cdot\|$ erhält, können wir

$$\left\langle \frac{P\mathbf{m}}{d_{\max}^{1/2}} \right\rangle \ll \langle P\widetilde{\mathbf{m}}\rangle$$

folgern. Für $\boldsymbol{\beta} \in \mathbb{Z}_{\geq 0}^{ds}$ gilt

$$\begin{aligned}&\partial^{\boldsymbol{\beta}} \left(\exp(-\mathfrak{L}^4\|\mathbf{x}\|^2) \prod_{l=1}^{r_1+r_2} \widetilde{w}_0(|\mathbf{x}^{(l)}|^2) h\left(\rho, \operatorname{Nm}\Big(\sum_i \sigma_i(x_i+h_i')^2 - \kappa/P^2\Big)\right)\right) \\ &\ll \sum_{\substack{\boldsymbol{\beta}_1,\boldsymbol{\beta}_2 \in \mathbb{Z}_{\geq 0}^{ds}: \\ \boldsymbol{\beta}=\boldsymbol{\beta}_1+\boldsymbol{\beta}_2}} \left|\partial^{\boldsymbol{\beta}_1}\left(\exp(-\mathfrak{L}^4\|\mathbf{x}\|^2) \prod_{l=1}^{r_1+r_2} \widetilde{w}_0(|\mathbf{x}^{(l)}|^2)\right)\right| \\ &\qquad \cdot \left|\partial^{\boldsymbol{\beta}_2} h\left(\rho, \operatorname{Nm}\Big(\sum_i \sigma_i(x_i+h_i')^2 - \kappa/P^2\Big)\right)\right|.\end{aligned}$$

Aus (3.1) folgt

$$\partial^{\boldsymbol{\beta}_2} h\left(\rho, \operatorname{Nm}\Big(\sum_i \sigma_i(x_i+h_i')^2 - \kappa/P^2\Big)\right) \ll \rho^{-|\boldsymbol{\beta}_2|-1}.$$

Da

$$\partial^{\boldsymbol{\beta}_1}\left(\exp(-\mathfrak{L}^4\|\mathbf{x}\|^2) \prod_{l=1}^{r_1+r_2} \widetilde{w}_0(|\mathbf{x}^{(l)}|^2)\right) \ll_{|\boldsymbol{\beta}_1|} \mathfrak{L}^{2|\boldsymbol{\beta}_1|}$$

für alle $\mathbf{x} \in V^s$ gilt, erhalten wir

$$\partial^{\boldsymbol{\beta}} \left(\exp(-\mathfrak{L}^4 \|\mathbf{x}\|^2) \prod_{l=1}^{r_1+r_2} \widetilde{w}_0(|\mathbf{x}^{(l)}|^2) h\left(\rho, \mathrm{Nm}\left(\sum_i \sigma_i (x_i + h_i')^2 - \kappa/P^2\right)\right)\right) \ll_{|\boldsymbol{\beta}|} \rho^{-1}(\rho^{-1}\mathfrak{L}^2)^{|\boldsymbol{\beta}|}.$$

Indem wir (3.10) N-mal partiell integrieren, können wir auf das behauptete Ergebnis schließen. □

Für große $\mathbf{m}$ ist diese Abschätzung bereits ausreichend. Für die restlichen Terme benötigen wir jedoch ein weiteres Resultat.

Dazu folgern wir zuerst aus (3.9), dass eine von P, A und κ unabhängige Funktion $w_1 \in \mathscr{W}_1^+(V)$ existiert, die $w_1(v) = 1$ für alle

$$\langle v \rangle \leq 2 \max \left\{ \left\langle \frac{A[\mathbf{x}] - \kappa}{P^2} \right\rangle : \frac{\mathbf{x}}{P} \in \mathrm{supp}(W) \right\}$$

erfüllt. Jede der folgenden impliziten Konstanten darf von dieser Funktion w_1 abhängen.

In dem folgenden Lemma, das auf Ideen aus §6 von Browning und Vishe [BV14] basiert, nutzen wir die in (3.3) definierte Funktion $p_\rho(v)$ mit dem soeben erzeugten w_1, um die Fourierintegrale zu vereinfachen.

Lemma 3.3. *Sei*

$$I(v, \mathbf{m}) = \int_{V^s} w\left(\frac{\mathbf{x}}{P} - \mathbf{h}\right) \phi\left(v(A[\mathbf{x}] - \kappa) - \mathbf{m}^T\mathbf{x}\right) \mathrm{d}\mathbf{x}.$$

Dann gilt

$$I_{\mathfrak{b}}(\mathbf{m}) = \int_V p_\rho(v) I(v/P^2, \mathbf{m}) \, \mathrm{d}v + O\left(\exp(-\mathfrak{L}^2/6)\right).$$

Beweis. Es gilt

$$I_{\mathfrak{b}}(\mathbf{m}) = \int_{V^s} W\left(\frac{\mathbf{x}}{P}\right) w_1\left(\frac{A[\mathbf{x}] - \kappa}{P^2}\right) h\left(\rho, \mathrm{Nm}\left(\frac{A[\mathbf{x}] - \kappa}{P^2}\right)\right) \phi(-\mathbf{m}^T\mathbf{x}) \, \mathrm{d}\mathbf{x}.$$

Aus der inversen Fouriertransformation folgt

$$w_1\left(\frac{A[\mathbf{x}] - \kappa}{P^2}\right) h\left(\rho, \mathrm{Nm}\left(\frac{A[\mathbf{x}] - \kappa}{P^2}\right)\right) = \int_V p_\rho(v) \phi\left(v(A[\mathbf{x}] - \kappa)/P^2\right) \mathrm{d}v.$$

Weiterhin können wir wegen

$$\begin{aligned}\int_{V^s} \left| w\left(\frac{\mathbf{x}}{P} - \mathbf{h}\right) - W\left(\frac{\mathbf{x}}{P}\right)\right| \mathrm{d}\mathbf{x} &= \mathrm{Nm}\, P^s \int_{V^s} w\left(\mathbf{x}\right) |1 - w_0\left(\mathbf{x}\right)| \,\mathrm{d}\mathbf{x} \\ &\ll \mathrm{Nm}\, P^s \int_{z>1/2} \exp(-\mathfrak{L}^4 z^2)\,\mathrm{d}z \\ &\ll \exp(-\mathfrak{L}^4/6)\end{aligned}$$

in $I_{\mathfrak{b}}(\mathbf{m})$ die Gewichtsfunktion W durch die Gewichtsfunktion w ersetzen und erhalten dadurch

$$\begin{aligned}I_{\mathfrak{b}}(\mathbf{m}) &= \int_V p_\rho(v) \int_{V^s} W\left(\frac{\mathbf{x}}{P}\right) \phi\left(v(A[\mathbf{x}] - \kappa)/P^2 - \mathbf{m}^T\mathbf{x}\right) \mathrm{d}\mathbf{x}\mathrm{d}v \\ &= \int_V p_\rho(v) I(v/P^2, \mathbf{m})\,\mathrm{d}v + O\left(\exp(-\mathfrak{L}^4/6) \int_V p_\rho(v)\,\mathrm{d}v\right).\end{aligned}$$

Nun folgt aus (3.6) die Behauptung. □

Für die Abschätzung von $I(v, \mathbf{m})$ wird ein eher technisches Lemma benötigt, das an Lemma 19 von Skinner [Ski94] angelehnt ist. Da wir anders als Skinner quadratische Formen behandeln, müssen wir den Beweis mit kleinen Veränderungen neu führen.

Lemma 3.4. *Sei $r \in \mathbb{Z}_{>0}$ und $P_0 \in \mathbb{R}_{>0}$ erfülle $\langle P\rangle \geq P_0$. Für zwei reelle quadratische Formen $f_1(\mathbf{t})$ und $f_2(\mathbf{t})$ in r Variablen und ein $\mathbf{z} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$ setzen wir $f_{\mathbf{z}}(\mathbf{t}) = z_1 f_1(\mathbf{t}) + z_2 f_2(\mathbf{t})$.*

Wenn die Hesse-Matrix $M(f_{\mathbf{z}})$ von $f_{\mathbf{z}}$ sowohl $\|M(f_{\mathbf{z}})\| \ll |\mathbf{z}|$ als auch $\|M(f_{\mathbf{z}})^{-1}\| \ll |\mathbf{z}|^{-1}$ erfüllt, gilt für $\mathbf{w} \in \mathbb{R}^r$ stets

$$\begin{aligned}&\int_{\mathbb{R}^r} \exp(-|\mathbf{t}|^2/P_0^2) e(f_{\mathbf{z}}(\mathbf{t}) + \mathbf{w}^T\mathbf{t})\,\mathrm{d}\mathbf{t} \\ &\ll \begin{cases}\exp(-\mathfrak{L}^2/2) + \mathfrak{L}^{3r} \min\{|\mathbf{z}|^{-r/2}, P_0^r\}, & |\mathbf{w}| \ll \mathfrak{L}^3(P_0^{-1} + |\mathbf{z}|P_0), \\ \exp(-\mathfrak{L}^2/2), & \textit{sonst.}\end{cases}\end{aligned}$$

Beweis. Als Erstes werden wir dem abzuschätzenden Term künstlich ein weiteres Integral hinzufügen. Sei $P_1 = \min\{P_0/2, |\mathbf{z}|^{-1/2}\}$. Für beliebige $0 < k < 1$ und $\mathbf{u} \in \mathbb{R}^r$ gilt

$$\exp(-|\mathbf{u}|^2) = \left(\pi k(1-k)\right)^{-r/2} \int_{\mathbb{R}^r} \exp\left(-\frac{|\mathbf{v}|^2}{1-k} - \frac{|\mathbf{v}-\mathbf{u}|^2}{k}\right) \mathrm{d}\mathbf{v}.$$

Wenn wir in diese Gleichung $\mathbf{u} = \mathbf{t}/P_0$ und $k = P_1^2/P_0^2$ einsetzen und im Integral $\mathbf{t}_1 = P_0\mathbf{v}$ substituieren, erhalten wir die Identität

$$\exp\left(-\frac{|\mathbf{t}|^2}{P_0^2}\right) = \left(\pi P_1^2\left(1 - \frac{P_1^2}{P_0^2}\right)\right)^{-r/2} \int_{\mathbb{R}^r} \exp\left(-\frac{|\mathbf{t}_1|^2}{P_0^2 - P_1^2} - \frac{|\mathbf{t}_1 - \mathbf{t}|^2}{P_1^2}\right) \mathrm{d}\mathbf{t}_1.$$

Wir schreiben

$$W_0(\mathbf{t}_1) = \exp\left(-\frac{|\mathbf{t}_1|^2}{P_0^2 - P_1^2}\right),$$
$$I'(\mathbf{t}_1) = \int_{\mathbb{R}^r} \exp\left(-\frac{|\mathbf{t}_1 - \mathbf{t}|^2}{P_1^2}\right) e(f_{\mathbf{z}}(\mathbf{t}) + \mathbf{w}^T\mathbf{t})\,\mathrm{d}\mathbf{t}$$

und erhalten damit

$$\int_{\mathbb{R}^r} \exp(-|\mathbf{t}|^2/P_0^2) e(f_{\mathbf{z}}(\mathbf{t}) + \mathbf{w}^T\mathbf{t})\,\mathrm{d}\mathbf{t} \ll P_1^{-r} \int_{\mathbb{R}^r} W_0(\mathbf{t}_1) I'(\mathbf{t}_1)\,\mathrm{d}\mathbf{t}_1. \quad (3.11)$$

Als Nächstes werden wir $I'(\mathbf{t}_1)$ abschätzen. Es gilt

$$\int_{|\mathbf{t}-\mathbf{t}_1|>P_1\mathfrak{L}} \exp\left(-\frac{|\mathbf{t}_1 - \mathbf{t}|^2}{P_1^2}\right) e(f_{\mathbf{z}}(\mathbf{t}) + \mathbf{w}^T\mathbf{t})\,\mathrm{d}\mathbf{t}$$
$$\ll P_1^r \left(\int_0^\infty \exp(-x^2)\,\mathrm{d}x\right)^{r-1} \int_{|x|\gg\mathfrak{L}} \exp(-x^2)\,\mathrm{d}t_j \ll P_1^r \exp(-\mathfrak{L}^2).$$

Für ein beliebiges $i \le r$ schreiben wir

$$\widetilde{f}_{\mathbf{z}}(x) = f_{\mathbf{z}}(t_1, \dots, t_{i-1}, x, t_{i+1}, \dots, t_r).$$

Damit gilt

$$\int_{|\mathbf{t}-\mathbf{t}_1|\le P_1\mathfrak{L}} \exp\left(-\frac{|\mathbf{t}_1 - \mathbf{t}|^2}{P_1^2}\right) e(f_{\mathbf{z}}(\mathbf{t}) + \mathbf{w}^T\mathbf{t})\,\mathrm{d}\mathbf{t}$$
$$\ll P_1^{r-1} \max \left| \int_{|t_i - t_{1,i}|\le P_1\mathfrak{L}} \exp\left(-\frac{(t_{1,i} - t_i)^2}{P_1^2}\right) e(\widetilde{f}_{\mathbf{z}}(t_i) + w_i t_i)\,\mathrm{d}t_i \right|,$$

wobei das Maximum hier über $|t_j - t_{1,j}| \le P_1\mathfrak{L}$ für $j \ne i$ gebildet wird. Um dieses Integral abschätzen zu können, verschieben wir den Integrationsweg und integrieren für ein $c \in \mathbb{R}$ über die Verbindungslinien von

$$t_{1,i} - P_1\mathfrak{L}, \qquad t_{1,i} - P_1\mathfrak{L} + \mathrm{i}c,$$
$$t_{1,i} + P_1\mathfrak{L} + \mathrm{i}c, \qquad t_{1,i} + P_1\mathfrak{L}.$$

Wir setzen

$$u + \mathrm{i}v = t_i - t_{1,i}, \qquad h = \widetilde{f}'_{\mathbf{z}}(t_{1,i}) + w_i$$

und wählen c so, dass $ch \ge 0$ und

$$|c| = \min\{P_1, (|\mathbf{z}|P_1\mathfrak{L})^{-1}\}$$

erfüllt ist. Damit erhalten wir

$$\Re\left(-\frac{(t_{1,i}-t_i)^2}{P_1^2}\right) = -\frac{u^2}{P_1^2} + \frac{v^2}{P_1^2} = -\frac{u^2}{P_1^2} + O(1),$$
$$\Im(\widetilde{f}_{\mathbf{z}}(t_i) + m_i t_i) = \widetilde{f}'_{\mathbf{z}}(t_{1,i}+u)v + m_i v = hv + O(1).$$

Also gilt

$$\begin{aligned}
&\max\left|\int_{|t_i-t_{1,i}|\le P_1\mathfrak{L}} \exp\left(-\frac{(t_{1,i}-t_i)^2}{P_1^2}\right) e(\widetilde{f}_{\mathbf{z}}(t_i)+w_i t_i)\,\mathrm{d}t_i\right| \\
&\ll \exp(-\mathfrak{L}^2)|c| + \exp(-2\pi hc)\int_{|u|\le P_1\mathfrak{L}} \exp\left(-\frac{u^2}{P_1^2}\right)\mathrm{d}u \\
&\ll P_1\exp(-\mathfrak{L}^2) + P_1\exp(-2\pi hc).
\end{aligned}$$

Wenn $I'(\mathbf{t}_1) \gg P_1^r\exp(-\mathfrak{L}^2)$ gilt, können wir $hc < \mathfrak{L}^2$ und damit auch

$$|\widetilde{f}'_{\mathbf{z}}(t_{1,i}) + w_i| < \mathfrak{L}^3(P_1^{-1} + |\mathbf{z}|P_1)$$

folgern. Da i beliebig gewählt wurde und $\|M(f_{\mathbf{z}})\| \ll |\mathbf{z}|$ gilt, folgt in diesem Fall

$$|\nabla f_{\mathbf{z}}(\mathbf{t}_1) + \mathbf{w}| \ll \mathfrak{L}^3(P_1^{-1} + |\mathbf{z}|P_1).$$

Zusammen mit der trivialen Abschätzung können wir

$$I'(\mathbf{t}_1) \ll \begin{cases} P_1^r, & |\nabla f_{\mathbf{z}}(\mathbf{t}_1) + \mathbf{w}| \ll \mathfrak{L}^3(P_1^{-1} + |\mathbf{z}|P_1), \\ P_1^r\exp(-\mathfrak{L}^2), & \text{sonst} \end{cases}$$

schließen. Setzen wir diese Abschätzung in (3.11) ein, erhalten wir

$$\begin{aligned}
P_1^{-r}\int_{|\mathbf{t}_1|\ge P_0\mathfrak{L}} W_0(\mathbf{t}_1)I'(\mathbf{t}_1)\,\mathrm{d}\mathbf{t}_1 &\ll \int_{|\mathbf{t}_1|\ge P_0\mathfrak{L}} \exp\left(-\frac{|\mathbf{t}_1|^2}{P_0^2-P_1^2}\right)\mathrm{d}\mathbf{t}_1 \\
&\ll P_0^r\int_{x\ge\mathfrak{L}}\exp(-x^2)\,\mathrm{d}x \\
&\ll \exp(-\mathfrak{L}^2/2)
\end{aligned}$$

und

$$\begin{aligned}
&P_1^{-r}\int_{|\mathbf{t}_1|<P_0\mathfrak{L}} W_0(\mathbf{t}_1)I'(\mathbf{t}_1)\,\mathrm{d}\mathbf{t}_1 \\
&\ll \exp(-\mathfrak{L}^2)\int_{|\mathbf{t}_1|<P_0\mathfrak{L}} W_0(\mathbf{t}_1)\,\mathrm{d}\mathbf{t}_1 + \int_{\substack{|\nabla f_{\mathbf{z}}(\mathbf{t}_1)+\mathbf{w}|\ll\mathfrak{L}^3(P_1^{-1}+|\mathbf{z}|P_1) \\ |\mathbf{t}_1|<P_0\mathfrak{L}}} \mathrm{d}\mathbf{t}_1 \\
&\ll \exp(-\mathfrak{L}^2/2) + \mathrm{meas}\left\{\mathbf{t}_1 :\ \begin{array}{l} |\nabla f_{\mathbf{z}}(\mathbf{t}_1)+\mathbf{w}| \ll \mathfrak{L}^3(P_1^{-1}+|\mathbf{z}|P_1), \\ |\mathbf{t}_1| < P_0\mathfrak{L} \end{array}\right\}.
\end{aligned}$$

Hierbei bezeichnet meas$\{\cdot\}$ das Maß der Menge. Damit haben wir

$$\begin{aligned}&\int_{\mathbb{R}^r} \exp(-|\mathbf{t}|^2/P_0^2) e(f_{\mathbf{z}}(\mathbf{t}) + \mathbf{w}^T\mathbf{t})\,\mathrm{d}\mathbf{t}\\ &\ll \exp(-\mathfrak{L}^2/2) + \mathrm{meas}\left\{\mathbf{t}_1 :\ \begin{array}{l}|\nabla f_{\mathbf{z}}(\mathbf{t}_1) + \mathbf{w}| \ll \mathfrak{L}^3(P_1^{-1} + |\mathbf{z}|P_1),\\ |\mathbf{t}_1| < P_0\mathfrak{L}\end{array}\right\} \quad (3.12)\end{aligned}$$

gezeigt.

Um den Beweis abzuschließen, müssen wir noch das Maß dieser Menge abschätzen. Sei $\mathbf{t}_1$ ein Element dieser Menge. Wenn $|\mathbf{w}| \geq 2|\nabla f_{\mathbf{z}}(\mathbf{t}_1)|$ gilt, dann ist

$$|\mathbf{w}| \leq 2\Big(|\mathbf{w}| - |\nabla f_{\mathbf{z}}(\mathbf{t}_1)|\Big) \leq 2\Big|\nabla f_{\mathbf{z}}(\mathbf{t}_1) + \mathbf{w}\Big| \ll \mathfrak{L}^3(P_0^{-1} + |\mathbf{z}|P_0).$$

Jedoch gilt auch im komplementären Fall

$$|\mathbf{w}| < 2|\nabla f_{\mathbf{z}}(\mathbf{t}_1)| \ll |\mathbf{z}|P_0\mathfrak{L} \ll \mathfrak{L}^3(P_0^{-1} + |\mathbf{z}|P_0).$$

Wenn $|\mathbf{w}| \gg \mathfrak{L}^3(P_0^{-1} + |\mathbf{z}|P_0)$ erfüllt ist, verschwindet also der zweite Summand von (3.12).

Wenn $\mathbf{t}_2$ ein weiteres Element der Menge ist, gilt

$$\begin{aligned}|\mathbf{t}_1 - \mathbf{t}_2| &\ll |\mathbf{z}|^{-1}|M(f_{\mathbf{z}})(\mathbf{t}_1 - \mathbf{t}_2)|\\ &= |\mathbf{z}|^{-1}|\nabla f_{\mathbf{z}}(\mathbf{t}_1) - \nabla f_{\mathbf{z}}(\mathbf{t}_2)|\\ &\ll \mathfrak{L}^3(P_1^{-1}|\mathbf{z}|^{-1} + P_1)\\ &\ll \mathfrak{L}^3(P_0^{-1}|\mathbf{z}|^{-1} + |\mathbf{z}|^{-1/2}).\end{aligned}$$

Dies impliziert

$$\begin{aligned}&\mathrm{meas}\left\{\mathbf{t}_1 :\ \begin{array}{l}|\nabla f_{\mathbf{z}}(\mathbf{t}_1) + \mathbf{w}| \ll \mathfrak{L}^3(P_1^{-1} + |\mathbf{z}|P_1),\\ |\mathbf{t}_1| < P_0\mathfrak{L}\end{array}\right\}\\ &\ll \min\{\mathfrak{L}^{3r}(P_0^{-1}|\mathbf{z}|^{-1} + |\mathbf{z}|^{-1/2})^r, P_0^r\mathfrak{L}^r\}\\ &\ll \mathfrak{L}^{3r}\min\{|\mathbf{z}|^{-r/2}, P_0^r\}\end{aligned}$$

und damit ist die Behauptung gezeigt. □

Wenn wir dieses Lemma in Anlehnung an §6 von Skinner [Ski94] dazu verwenden, $I(v, \mathbf{m})$ abzuschätzen, können wir der Argumentation in §6.3 von Browning und Vishe [BV14] folgend das nächste Lemma herleiten.

Lemma 3.5. *Sei* $B(v) = \oplus_l B^{(l)}(v^{(l)})$ *und*

$$B^{(l)}(v^{(l)}) = d_{max}^{(l)1/2}\mathfrak{L}^5 P^{(l)-1}(1+|v^{(l)}|).$$

Es gilt

$$I_{\mathfrak{b}}(\mathbf{m}) \ll \exp(-\mathfrak{L}^2/6) + \frac{\langle P\rangle^{\varepsilon}\operatorname{Nm} P^s}{|\operatorname{Nm}\Delta|^{1/2}} \int_{\substack{v\in V;\\ |\mathbf{m}^{(l)}|\ll B^{(l)}(v^{(l)})}} \frac{|p_\rho(v)|}{\mathscr{H}(v)^{s/2}}\,\mathrm{d}v.$$

Beweis. Sei wie zuvor

$$\widetilde{\mathbf{m}} = \operatorname{diag}\left(|d_1|^{-1/2},\dots,|d_s|^{-1/2}\right)R^T\mathbf{m} \in V^s.$$

Dann erhalten wir durch Diagonalisieren

$$\begin{aligned}
&|\operatorname{Nm}\Delta|^{1/2}|I(v,\mathbf{m})|\\
&= \left|\int_{V^s} \exp\big(-\mathfrak{L}^4\|\mathbf{x}/P-\mathbf{h}'\|^2\big)\phi\Big(v\sum_i \sigma_i x_i^2 - \widetilde{\mathbf{m}}^T\mathbf{x}\Big)\,\mathrm{d}\mathbf{x}\right|\\
&= \left|\int_{V^s} \exp\big(-\mathfrak{L}^4\|\mathbf{x}/P\|^2\big)\phi\Big(v\sum_i \sigma_i x_i^2 - \widetilde{\mathbf{m}}^T\mathbf{x} + 2vP\sum_i \sigma_i h_i x_i\Big)\,\mathrm{d}\mathbf{x}\right|.
\end{aligned}$$

Wir können auf dieses Integral das vorhergehende Lemma anwenden, wenn wir es einzeln bezüglich der Einbettungen integrieren. Dazu setzen wir für die reellen Einbettungen

$$r = s, \qquad P_0 = P^{(l)}/\mathfrak{L}^2, \qquad \mathbf{z} = (v^{(l)},0), \qquad f_1(\mathbf{t}) = \sum_{i=1}^{s}\sigma_i^{(l)}t_i^2$$

und

$$\mathbf{w} = -\widetilde{\mathbf{m}}^{(l)} + 2v^{(l)}P^{(l)}\begin{pmatrix}\sigma_1^{(l)}h_1^{(l)}\\ \vdots\\ \sigma_s^{(l)}h_s^{(l)}\end{pmatrix}.$$

Unter der Annahme $v\neq 0$ erhalten wir dadurch

$$\begin{aligned}
&\int_{\mathbb{R}^s}\exp(-\mathfrak{L}^4|\mathbf{t}|^2/P^{(l)2})\phi\Big(v^{(l)}\sum_i\sigma_i^{(l)}t_i^2 - \widetilde{\mathbf{m}}^{(l)T}\mathbf{t} + 2v^{(l)}P^{(l)}\sum_i\sigma_i^{(l)}h_i'^{(l)}t_i\Big)\,\mathrm{d}\mathbf{t}\\
&\ll \exp(-\mathfrak{L}^2/2) + \begin{cases}\mathfrak{L}^{3s}\min\{|v^{(l)}|^{-1/2},P^{(l)}\}^s, & |\mathbf{w}|\ll\mathfrak{L}^5(P^{(l)-1}+|v^{(l)}|P^{(l)}),\\ 0, & \text{sonst.}\end{cases}
\end{aligned}$$

Wegen $\langle \mathbf{h}' \rangle \ll 1$ und $|\mathbf{m}^{(l)}| \ll d_{\max}^{(l)1/2} |\widetilde{\mathbf{m}}^{(l)}|$ können wir die Bedingung in der Fallunterscheidung durch $|\mathbf{m}^{(l)}| \ll B^{(l)}(P^{(l)2} v^{(l)})$ ersetzen.

Für die komplexen Einbettungen setzen wir

$$r = 2s, \qquad P_0 = \sqrt{2} P^{(l)} / \mathfrak{L}^2, \qquad \mathbf{z} = (\Re(v^{(l)}), \Im(v^{(l)})),$$
$$f_1(\mathbf{t}) = 2 \sum_{i=1}^{s} (t_i^2 - t_{i+s}^2), \qquad f_2(\mathbf{t}) = -4 \sum_{i=1}^{s} t_i t_{i+s}$$

und

$$\mathbf{w} = \begin{pmatrix} 2\Re(-\widetilde{\mathbf{m}}^{(l)} + 2v^{(l)} P^{(l)} \mathbf{h}^{(l)}) \\ -2\Im(-\widetilde{\mathbf{m}}^{(l)} + 2v^{(l)} P^{(l)} \mathbf{h}^{(l)}) \end{pmatrix}.$$

Wie oben folgt damit für $v \neq 0$ aus dem vorhergehenden Lemma

$$\int_{\mathbb{C}^s} \exp(-\mathfrak{L}^4 |\mathbf{t}|^2 / P^{(l)2}) \phi\Big(v^{(l)} \sum_i \sigma_i^{(l)} t_i^2 - \widetilde{\mathbf{m}}^{(l)T} \mathbf{t} + 2v^{(l)} P^{(l)} \sum_i \sigma_i^{(l)} h_i'^{(l)} t_i\Big) \, \mathrm{d}\mathbf{t}$$
$$\ll \exp(-\mathfrak{L}^2/2) + \begin{cases} \mathfrak{L}^{6s} \min\{|v^{(l)}|^{-1/2}, P^{(l)}\}^{2s}, & |\mathbf{m}^{(l)}| \ll B^{(l)}(P^{(l)2} v^{(l)}), \\ 0, & \text{sonst.} \end{cases}$$

Also gilt

$$|\mathrm{Nm}\, \Delta|^{1/2} I(v/P^2, \mathbf{m})$$
$$\ll \exp(-\mathfrak{L}^2/3) + \begin{cases} \langle P \rangle^{\varepsilon} \, \mathrm{Nm}\, P^s \mathscr{H}(v)^{-s/2}, & |\mathbf{m}^{(l)}| \ll B^{(l)}(v^{(l)}), \\ 0, & \text{sonst.} \end{cases}$$

Wenn wir diese Abschätzung in Lemma 3.3 einsetzen, erhalten wir

$$I_{\mathfrak{b}}(\mathbf{m}) \ll \frac{\langle P \rangle^{\varepsilon} \, \mathrm{Nm}\, P^s}{|\mathrm{Nm}\, \Delta|^{1/2}} \int_{\substack{v \in V: \\ |\mathbf{m}^{(l)}| \ll B^{(l)}(v^{(l)})}} \frac{|p_\rho(v)|}{\mathscr{H}(v)^{s/2}} \, \mathrm{d}v$$
$$+ \exp(-\mathfrak{L}^2/3) \int_V p_\rho(v) \, \mathrm{d}v + \exp(-\mathfrak{L}^2/6).$$

Wegen (3.6) folgt damit die Behauptung. □

Wir sind nun in der Lage, die Fourierintegrale für alle $\mathbf{m} \neq \mathbf{0}$ geeignet abzuschätzen.

3.3 Das singuläre Integral

Wir müssen die Fourierintegrale nur noch für $\mathbf{m} = \mathbf{0}$ auswerten. Wie Browning und Vishe werden wir sie zuerst durch das singuläre Integral approximieren und dann dessen Größe abschätzen.

Für jedes ganze Ideal $\mathfrak{b} \neq (0)$ gilt

$$\begin{aligned} I_{\mathfrak{b}}(\mathbf{0}) &= \operatorname{Nm} P^s \int_{V^s} W(\mathbf{x}) h\left(\rho, \operatorname{Nm}\left(A[\mathbf{x}] - \kappa/P^2\right)\right) \mathrm{d}\mathbf{x} \\ &= \frac{\operatorname{Nm} P^s}{|\operatorname{Nm}\Delta|^{1/2}} \int_{V^s} \frac{\prod_l \widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)}{\exp(\mathfrak{L}^4 \|\mathbf{x} - \mathbf{h}'\|^2)} h\Big(\rho, \operatorname{Nm}\Big(\sum_i \sigma_i x_i^2 - \kappa/P^2\Big)\Big) \mathrm{d}\mathbf{x} \\ &= \frac{\operatorname{Nm} P^s}{|\operatorname{Nm}\Delta|^{1/2}} \int_V \mathfrak{I}(v) h(\rho, \operatorname{Nm} v) \, \mathrm{d}v, \end{aligned}$$

wobei der Integrationsbereich in

$$\mathfrak{I}(v) = \int_{\mathbf{x}_0 \in V^{s-1}} \frac{\prod_l \widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)}{\exp(\mathfrak{L}^4 \|\mathbf{x} - \mathbf{h}'\|^2) |\operatorname{Nm}(2x_1)|} \, \mathrm{d}\mathbf{x}_0$$

auf solche $\mathbf{x}_0 = (x_2, \dots, x_s)$ beschränkt ist, für die ein x_1 als Lösung von $\sum \sigma_i x_i^2 - \kappa/P^2 = v$ existiert. Wegen (3.7) gilt im Träger von $\widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)$ stets $|x_1^{(l)}| \gg 1$ und somit ist dieses x_1 eindeutig. Da für alle l die Funktion $x_1^{(l)} = x_1^{(l)}(\mathbf{x}_0^{(l)}, v^{(l)})$ im Träger von $\widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)$ glatt ist, ist $\mathfrak{I}(v)$ unendlich oft reell differenzierbar.

Für ein $N \geq 1$ nutzen wir (3.2) und erhalten

$$I_{\mathfrak{b}}(\mathbf{0}) = \frac{\sqrt{D_K} \operatorname{Nm} P^s}{2^{r_2} |\operatorname{Nm}\Delta|^{1/2}} \mathfrak{I}(0) + O_N\left(\frac{\lambda_{\mathfrak{I}}^{2d(N+1)} \rho^N \operatorname{Nm} P^s}{|\operatorname{Nm}\Delta|^{1/2}}\right).$$

Nun werden wir $\lambda_{\mathfrak{I}}^N$ wie in §5 von Browning und Vishe [BV14] abschätzen. Bei $l \leq r_1$ folgt aus

$$\frac{\partial x_1^{(l)}}{\partial v^{(l)}} = \left(\frac{\partial v^{(l)}}{\partial x_1^{(l)}}\right)^{-1} = \frac{1}{2\sigma_1^{(l)} x_1^{(l)}},$$

dass im Träger von $\widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)$ die N-te Ableitung von $x_1^{(l)}$ nach $v^{(l)}$ in $O_N(1)$ liegt. Deswegen impliziert

$$\frac{\partial^N}{\partial x_1^{(l)N}} \frac{\widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)}{\exp(\mathfrak{L}^4 |\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)} \ll \mathfrak{L}^{4N}$$

die Abschätzung

$$\frac{\partial^N}{\partial v^{(l)N}} \int_{\mathbb{R}^{s-1}} \frac{\widetilde{w}_0(|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)}{\exp(\mathfrak{L}^4|\mathbf{x}^{(l)} - \mathbf{h}'^{(l)}|^2)|2x_1^{(l)}|} \, \mathrm{d}\mathbf{x}_0^{(l)} \ll \mathfrak{L}^{4N}.$$

Um das entsprechende Resultat für $l > r_1$ zu erhalten, nutzen wir

$$\begin{pmatrix} \frac{\partial \Re(x_1^{(l)})}{\partial \Re(v^{(l)})} & \frac{\partial \Re(x_1^{(l)})}{\partial \Im(v^{(l)})} \\ \frac{\partial \Im(x_1^{(l)})}{\partial \Re(v^{(l)})} & \frac{\partial \Im(x_1^{(l)})}{\partial \Im(v^{(l)})} \end{pmatrix} = \frac{1}{2|x_1^{(l)}|^2} \begin{pmatrix} \Re(x_1^{(l)}) & \Im(x_1^{(l)}) \\ -\Im(x_1^{(l)}) & \Re(x_1^{(l)}) \end{pmatrix}$$

und argumentieren ansonsten wie im Reellen. Auf diese Weise erhalten wir schließlich

$$\lambda_{\mathfrak{J}}^N \ll_N \mathfrak{L}^{4N},$$

sodass wir insgesamt das folgende Analogon zu (8.4) von Browning und Vishe [BV14] bewiesen haben.

Lemma 3.6. *Für $N \geq 1$ gilt*

$$I_{\mathfrak{b}}(\mathbf{0}) = \frac{D_K^{1/2} \operatorname{Nm} P^s}{2^{r_2}|\operatorname{Nm} \Delta|^{1/2}} \mathfrak{J}(0) + O\left(\frac{\operatorname{Nm} P^s \langle P \rangle^{\varepsilon} \rho^N}{|\operatorname{Nm} \Delta|^{1/2}}\right).$$

Damit haben wir das zu unserem Problem gehörende singuläre Integral $\mathfrak{J}(0)$ erzeugt. Der nächste Schritt ist, die Größe des singulären Integrals abzuschätzen. Das folgende Resultat ist unsere Version von Lemma 8.2 von Browning und Vishe [BV14]. Wie verwenden allerdings lediglich die triviale obere Schranke.

Lemma 3.7. *Es gilt*

$$\mathfrak{L}^{2d(1-s)} \ll \mathfrak{J}(0) \ll 1.$$

Beweis. Die obere Schranke ergibt sich leicht aus

$$\mathfrak{J}(0) \ll \int_{\mathbf{x}_0 \in V^{s-1} : \langle \mathbf{x} - \mathbf{h}' \rangle \leq 1} \mathrm{d}\mathbf{x}_0 \ll 1$$

und die Voraussetzungen an $\mathbf{h}$ implizieren

$$\begin{aligned} \mathfrak{J}(0) &\gg \int_{\substack{\mathbf{x}_0 \in V^{s-1} : \langle \mathbf{x} - \mathbf{h}' \rangle \leq \mathfrak{L}^{-2} \\ \sum_i \sigma_i x_i^2 = \kappa / P^2}} \mathrm{d}\mathbf{x}_0 \\ &\gg \int_{\substack{\mathbf{x}_0 \in V^{s-1} : \langle \mathbf{x} \rangle \leq \mathfrak{L}^{-2} \\ \sum_i \sigma_i (x_i^2 + 2h_i' x_i) = 0}} \mathrm{d}\mathbf{x}_0 \\ &\gg \int_{\substack{\mathbf{x}_0 \in V^{s-1} : \langle \mathbf{x}_0 \rangle \leq \mathfrak{L}^{-2} \\ |\sum_i \sigma_i (x_i^2 + 2h_i' x_i)| \leq |h_1| \mathfrak{L}^{-2} - \mathfrak{L}^{-4}}} \mathrm{d}\mathbf{x}_0 \\ &\gg \mathfrak{L}^{2d(1-s)}. \end{aligned}$$

□

Wir haben somit das singuläre Integral und damit insgesamt alle Fourierintegrale abschließend behandelt.

3.4 Exponentialsummen

In diesem Abschnitt untersuchen wir die Exponentialsumme $S_{\mathfrak{b}}(\mathbf{m})$ aus Lemma 3.1. Auf Ideen aus §7 von Browning und Vishe [BV14] und §2.4 von Dietmann [Die03] aufbauend verwenden wir dazu die Exponentialsumme

$$\widetilde{S}(\mathfrak{b},\mathbf{m},\boldsymbol{\xi},\kappa)=\sum_{r\ (\mathfrak{b})}^{*}\sum_{\substack{\mathbf{x}\ (\mathfrak{b})\\ \mathbf{x}\equiv\boldsymbol{\xi}\ (\mathfrak{b},\eta)}}\phi\Big(\gamma_{\mathfrak{b}}\Big(r(A[\mathbf{x}]-\kappa)+\mathbf{m}^T\mathbf{x}\Big)\Big)$$

für $\mathbf{m}\in\widehat{\mathcal{O}}^s$. Der Zusammenhang dieser Exponentialsumme mit $S_{\mathfrak{b}}(\mathbf{m})$ ist der Folgende.

Lemma 3.8. *Für alle $\mathfrak{b}\neq(0)$, $\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{\,s}$ existieren $\widetilde{\mathbf{m}}\in\widehat{\mathcal{O}}^s$, $\widetilde{\kappa}\in\mathcal{O}$ und $\widetilde{\boldsymbol{\xi}}\in\mathcal{O}^s$ mit*

$$|S_{\mathfrak{b}}(\mathbf{m})|=|\widetilde{S}(\mathfrak{b},\widetilde{\mathbf{m}},\widetilde{\boldsymbol{\xi}},\widetilde{\kappa})|.$$

Beweis. Wegen Lemma 2.1(ii) existiert ein $\beta\in\mathcal{O}$ mit $\mathrm{v}_{\mathfrak{p}}(\beta)=\mathrm{v}_{\mathfrak{p}}(\mathfrak{b})$ für alle $\mathfrak{p}\mid\mathfrak{b}\cap\eta$. Also folgt aus Lemma 2.3(i), dass

$$\begin{aligned}&\sum_{\substack{\mathbf{x}\ (\mathfrak{b}\cap\eta)\\ \mathbf{x}\equiv\boldsymbol{\xi}\ (\eta)}}\phi\Big(r\gamma_{\mathfrak{b}}(A[\mathbf{x}]-\kappa)+\mathbf{m}^T\mathbf{x}\Big)\\ &=\sum_{\substack{\mathbf{y}\ (\mathfrak{b})\\ \mathbf{y}\equiv\boldsymbol{\xi}\ (\eta,\beta)}}\phi\Big(r\gamma_{\mathfrak{b}}(A[\mathbf{y}]-\kappa)\Big)\sum_{\substack{\mathbf{z}\ ((\mathfrak{b}\cap\eta)/\mathfrak{b})\\ \mathbf{y}+\beta\mathbf{z}\equiv\boldsymbol{\xi}\ (\eta)}}\phi\Big(\mathbf{m}^T(\mathbf{y}+\beta\mathbf{z})\Big).\end{aligned}$$

Wegen $(\eta,\mathfrak{b})=(\eta,\beta)$ gilt $(\mathfrak{b}\cap\eta)/\mathfrak{b}=\mathcal{O}\cap(\eta/\beta)$. Zusammen mit $\mathbf{y}\equiv\boldsymbol{\xi}\ (\eta,\beta)$ folgt daraus, dass die innere Summe genau einen Summanden hat. Des Weiteren gibt es ein $\delta\in(\mathfrak{b}\cap\eta)/\mathfrak{b}$ mit $\delta\equiv1\ ((\mathfrak{b}\cap\eta)/\eta)$ und folglich gilt

$$\mathbf{y}+\beta\mathbf{z}\equiv\delta(\mathbf{y}+\beta\mathbf{z}-\boldsymbol{\xi})+\boldsymbol{\xi}\equiv\delta\mathbf{y}+(1-\delta)\boldsymbol{\xi}\quad(\mathfrak{b}\cap\eta).$$

Damit haben wir bereits

$$S_{\mathfrak{b}}(\mathbf{m})=\phi\Big((1-\delta)\mathbf{m}^T\boldsymbol{\xi}\Big)\sum_{r\ (\mathfrak{b})}^{*}\sum_{\substack{\mathbf{y}\ (\mathfrak{b})\\ \mathbf{y}\equiv\boldsymbol{\xi}\ (\mathfrak{b},\eta)}}\phi\Big(r\gamma_{\mathfrak{b}}(A[\mathbf{y}]-\kappa)+\delta\mathbf{m}^T\mathbf{y}\Big)\tag{3.13}$$

gezeigt.

Seien $\alpha\in\mathfrak{b}$ und ν definiert wie in Lemma 2.4. Es gelte also insbesondere $\gamma_{\mathfrak{b}}=\nu/\alpha$ und ν sei teilerfremd zu $\mathfrak{b}$. Wenn wir bei der Summation $\nu^2r=r'$ und $\mathbf{y}=\nu\mathbf{x}$ substituieren, erhalten wir wegen $\alpha\delta m\in\widehat{\mathcal{O}}$ die Behauptung. □

Aus (3.13) können wir außerdem noch die später hilfreiche Identität

$$S_{\mathfrak{b}}(\mathbf{0}) = \sideset{}{^*}\sum_{r\ (\mathfrak{b})} \sum_{\substack{\mathbf{y}\ (\mathfrak{b})\\ \mathbf{y}\equiv\boldsymbol{\xi}\ (\mathfrak{b},\eta)}} \phi\Big(r\gamma_{\mathfrak{b}}(A[\mathbf{y}]-\kappa)\Big) \tag{3.14}$$

ableiten.

Wir werden uns im Rest dieses Abschnitts nur noch mit der soeben definierten Exponentialsumme beschäftigen. Wie in §7 von Browning und Vishe [BV14] lässt sich zeigen, dass sie semimultiplikativ ist.

Lemma 3.9. *Sei $\mathbf{m} \in \widehat{\mathcal{O}}^s$. Wenn $\mathfrak{b}_1$ und $\mathfrak{b}_2$ teilerfremde ganze Ideale sind, ist*

$$\widetilde{S}(\mathfrak{b}_1\mathfrak{b}_2, \mathbf{m}, \boldsymbol{\xi}, \kappa) = \widetilde{S}(\mathfrak{b}_1, \mathbf{m}, \boldsymbol{\xi}_1, \kappa_1)\widetilde{S}(\mathfrak{b}_2, \mathbf{m}, \boldsymbol{\xi}_2, \kappa_2)$$

für geeignete $\boldsymbol{\xi}_1$, $\boldsymbol{\xi}_2$, κ_1 und κ_2 erfüllt.

Beweis. Sei $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$. Wegen Lemma 2.1(ii) gibt es α und β, bei denen $\mathrm{v}_{\mathfrak{p}}(\alpha) = \mathrm{v}_{\mathfrak{p}}(\mathfrak{b}_1)$ und $\mathrm{v}_{\mathfrak{p}}(\beta) = \mathrm{v}_{\mathfrak{p}}(\mathfrak{b}_2)$ für alle $\mathfrak{p} \mid \mathfrak{b}$ erfüllt sind. Für $\bar{\alpha} \in \mathcal{O}$ und $\bar{\beta} \in \mathcal{O}$ mit $\bar{\alpha}\alpha + \bar{\beta}\beta \equiv 1(\mathfrak{b})$ folgt aus Lemma 2.3(ii), dass

$$\begin{aligned}
&\widetilde{S}(\mathfrak{b}_1\,\mathfrak{b}_2, \mathbf{m}, \xi, \kappa)\\
&= \sideset{}{^*}\sum_{\substack{r_1\ (\mathfrak{b}_1)\\ r_2\ (\mathfrak{b}_2)}} \sum_{\substack{\mathbf{y}\ (\mathfrak{b}_1)\\ \mathbf{z}\ (\mathfrak{b}_2)\\ \beta\mathbf{y}+\alpha\mathbf{z}\equiv\boldsymbol{\xi}\ (\mathfrak{b},\eta)}} \phi\Big(\gamma_{\mathfrak{b}}\Big((\beta r_1+\alpha r_2)(A[\beta\mathbf{y}+\alpha\mathbf{z}]-\kappa) + \mathbf{m}^T(\beta\mathbf{y}+\alpha\mathbf{z})\Big)\Big)\\
&= \sideset{}{^*}\sum_{r_1\ (\mathfrak{b}_1)} \sum_{\substack{\mathbf{y}\ (\mathfrak{b}_1)\\ \mathbf{y}\equiv\bar{\beta}\boldsymbol{\xi}\ (\mathfrak{b}_1,\eta)}} \phi\Big(\beta\gamma_{\mathfrak{b}}\Big(r_1(A[\mathbf{y}]-\bar{\beta}^2\kappa) + \mathbf{m}^T\mathbf{y}\Big)\Big)\\
&\quad\cdot \sideset{}{^*}\sum_{r_2\ (\mathfrak{b}_2)} \sum_{\substack{\mathbf{z}\ (\mathfrak{b}_2)\\ \mathbf{z}\equiv\bar{\alpha}\boldsymbol{\xi}\ (\mathfrak{b}_2,\eta)}} \phi\Big(\alpha\gamma_{\mathfrak{b}}\Big(r_2(A[\mathbf{z}]-\bar{\alpha}^2\kappa) + \mathbf{m}^T\mathbf{z}\Big)\Big).
\end{aligned}$$

Da $\phi(\alpha\gamma_{\mathfrak{b}}\cdot)$ und $\phi(\beta\gamma_{\mathfrak{b}}\cdot)$ primitive Charaktere modulo $\mathfrak{b}_2$ beziehungsweise $\mathfrak{b}_1$ sind, ist das Lemma damit bewiesen. □

Wegen der Semimultiplikativität ist es ausreichend, die Exponentialsummen auf Primidealpotenzen $\mathfrak{p}^l$ für $l \geq 1$ zu betrachten. Dazu folgen wir dem Argument aus §2.4 von Dietmann [Die03].

Zuerst nehmen wir an, dass $\mathfrak{p}$ nicht 2 teilt. Damit wir uns auf Diagonalformen beschränken können, nutzen wir die folgende Verallgemeinerung von Theorem 31 von Watson [Wat60]. Watsons Beweis bleibt wegen (2.3) unverändert gültig.

Lemma 3.10. *Wenn $\mathfrak{p} \nmid 2$ gilt, gibt es eine Matrix $U \in \mathcal{O}^{s\times s}$ mit zu $\mathfrak{p}$ teilerfremder Determinante, sodass $U^T AU$ diagonal modulo $\mathfrak{p}^l$ ist.*

Wir benötigen ein Analogon zu Lemma 8 von Dietmann [Die03].

Lemma 3.11. *Seien $\mathbf{a}, \mathbf{b} \in \mathcal{O}^s$. Dann gilt für $\mathfrak{p} \nmid 2$ stets*

$$\sum_{r\ (\mathfrak{p}^l)}^{*} \left(\prod_{i=1}^{s} \sum_{x_i\ (\mathfrak{p}^l)} \phi\Big(\gamma_{\mathfrak{p}^l}(ra_ix_i^2 + b_ix_i)\Big)\right) \phi(-\gamma_{\mathfrak{p}^l} r\kappa) \ll \mathrm{N}\,\mathfrak{p}^{l(s+1)/2} T_\kappa(\mathfrak{p}^l, \mathbf{a}).$$

Hierbei sei $T_\kappa(\mathfrak{p}^l, \mathbf{a}) = \mathrm{N}\left((\mathfrak{p}^l, \kappa)(\mathfrak{p}^l, a_1)\cdots(\mathfrak{p}^l, a_s)\right)^{1/2}$.

Beweis. Der Beweis basiert auf §6 bis §8 von Estermann [Est62]. Es sind allerdings so viele Anpassungen notwendig, dass wir ihn hier vollständig führen werden.

Für alle i sei $v_i = \mathrm{v}_\mathfrak{p}(a_i)$ und $\mu_i = \min\{v_i, l\}$. Unabhängig von r und i gilt wegen (2.2) für ganze Zahlen a_i und b_i, die $p^{\mu_i} a_i' \equiv a_i (\mathfrak{p}^l)$ und $p^{\mu_i} b_i' \equiv b_i (\mathfrak{p}^l)$ erfüllen, dass

$$\begin{aligned}
&\sum_{x_i\ (\mathfrak{p}^l)} \phi\Big(\gamma_{\mathfrak{p}^l}(ra_ix_i^2 + b_ix_i)\Big) \\
&= \sum_{y_i\ (\mathfrak{p}^{l-\mu_i})} \sum_{z_i\ (\mathfrak{p}^{\mu_i})} \phi\Big(\gamma_{\mathfrak{p}^l}\Big(ra_i(y_i + p^{l-\mu_i}z_i)^2 + b_i(y_i + p^{l-\mu_i}z_i)\Big)\Big) \\
&= \sum_{y_i\ (\mathfrak{p}^{l-\mu_i})} \phi\Big(\gamma_{\mathfrak{p}^l}(ra_iy_i^2 + b_iy_i)\Big) \sum_{z_i\ (\mathfrak{p}^{\mu_i})} \phi(\gamma_{\mathfrak{p}^{\mu_i}} b_i z_i) \\
&= \begin{cases} \mathrm{N}\,\mathfrak{p}^{\mu_i} \sum_{x_i\ (\mathfrak{p}^{l-\mu_i})} \phi\Big(\gamma_{\mathfrak{p}^{l-\mu_i}}(ra_i'x_i^2 + b_i'x_i)\Big), & \mathfrak{p}^{\mu_i} \mid b_i, \\ 0, & \mathfrak{p}^{\mu_i} \nmid b_i. \end{cases}
\end{aligned}$$

Im Folgenden können wir o. B. d. A. davon ausgehen, dass $\mathfrak{p}^{\mu_i} \mid b_i$ für alle i erfüllt ist, da ansonsten die zu beweisende Abschätzung trivialerweise richtig ist. Ebenso können wir von $\mu_i = v_i$ für alle i ausgehen, da $\mu_i = l$ unabhängig von r stets

$$\sum_{x_i\ (\mathfrak{p}^l)} \phi\Big(\gamma_{\mathfrak{p}^l}(ra_ix_i^2 + b_ix_i)\Big) = \mathrm{N}\,\mathfrak{p}^l$$

impliziert und die Summe für solche i damit ausreichend abgeschätzt ist.

Also gilt $\mathfrak{p} \nmid a_i'$ und somit existieren die multiplikativ Inversen von $2ra_i'$ und $4ra_i'$ bezüglich $\mathfrak{p}^l$. Für diese schreiben wir $\overline{2ra_i'}$ beziehungsweise $\overline{4ra_i'}$. Es

gilt

$$\begin{aligned}
&\sum_{x_i \ (\mathfrak{p}^{l-v_i})} \phi\Big(\gamma_{\mathfrak{p}^{l-v_i}}(ra_i'x_i^2 + b_i'x_i)\Big) \\
&= \sum_{x_i \ (\mathfrak{p}^{l-v_i})} \phi\Big(\gamma_{\mathfrak{p}^{l-v_i}}\Big(ra_i'(x_i - \overline{2ra_i'}b_i')^2 + b_i'(x_i - \overline{2ra_i'}b_i')\Big)\Big) \\
&= \phi(-\gamma_{\mathfrak{p}^{l-v_i}}\overline{4ra_i'}b_i'^2) \sum_{x_i \ (\mathfrak{p}^{l-v_i})} \phi(\gamma_{\mathfrak{p}^{l-v_i}} ra_i'x_i^2).
\end{aligned}$$

Diese Gaußsche Summe können wir mithilfe der von Hecke entwickelten Rekursionsformel (siehe §54 Hilfssatz b) und Satz 155 von Hecke [Hec54]) auswerten und erhalten

$$\begin{aligned}
&\sum_{x_i \ (\mathfrak{p}^{l-v_i})} \phi(\gamma_{\mathfrak{p}^{l-v_i}} ra_i'x_i^2) \\
&= \begin{cases} \mathrm{N}\,\mathfrak{p}^{(l-v_i)/2}, & 2 \mid l - v_i, \\ \mathrm{N}\,\mathfrak{p}^{(l-v_i-1)/2} \left(\frac{ra_i'}{\mathfrak{p}}\right) \sum_{x_i \ (\mathfrak{p})} \phi(\gamma_{\mathfrak{p}} x_i^2), & 2 \nmid l - v_i. \end{cases}
\end{aligned} \tag{3.15}$$

Es zeigt sich außerdem, dass

$$\Big| \sum_{x_i \ (\mathfrak{p})} \phi(\gamma_{\mathfrak{p}} x_i^2)\Big|^2 = \sum_{x_i, y \ (\mathfrak{p})} \phi\Big(\gamma_{\mathfrak{p}}(x_i^2 - y^2)\Big) = \sum_{z \ (\mathfrak{p})} \phi(\gamma_{\mathfrak{p}} z^2) \sum_{y \ (\mathfrak{p})} \phi(\gamma_{\mathfrak{p}} 2zy) = \mathrm{N}\,\mathfrak{p}.$$

Das Zusammenfügen der bisherigen Ergebnisse liefert

$$\begin{aligned}
&\left| \sum_{r \ (\mathfrak{p}^l)}^{*} \left(\prod_{i=1}^{s} \sum_{x_i \ (\mathfrak{p}^l)} \phi\Big(\gamma_{\mathfrak{p}^l}(ra_ix_i^2 + b_ix_i)\Big)\right) \phi(-\gamma_{\mathfrak{p}^l} r\kappa) \right| \\
&= \mathrm{N}\,\mathfrak{p}^{\sum_i (l+v_i)/2} \left| \sum_{r \ (\mathfrak{p}^l)}^{*} \left(\prod_{\substack{i=1 \\ 2 \nmid l - v_i}}^{s} \left(\frac{ra_i'}{\mathfrak{p}}\right)\right) \phi\left(-\gamma_{\mathfrak{p}^l}\Big(\sum_{i=1}^{s} \overline{4ra_i'} p^{v_i} b_i'^2 + r\kappa\Big)\right) \right|.
\end{aligned}$$

Diese verallgemeinerte Kloostermansumme kann mithilfe von Proposition 9 von Bruggeman und Miatello [BM95] abgeschätzt werden. Es gilt

$$\begin{aligned}
\sum_{r \ (\mathfrak{p}^l)}^{*} \left(\prod_{\substack{i=1 \\ 2 \nmid l - v_i}}^{s} \left(\frac{ra_i'}{\mathfrak{p}}\right)\right) \phi\left(-\gamma_{\mathfrak{p}^l}\Big(\sum_{i=1}^{s} \overline{4ra_i'} p^{v_i} b_i'^2 + r\kappa\Big)\right) &\ll \mathrm{N}\,\mathfrak{p}^{l - \max\{l - \mathrm{v}_{\mathfrak{p}}(\kappa), 0\}/2} \\
&= \mathrm{N}\,\mathfrak{p}^{(l + \min\{\mathrm{v}_{\mathfrak{p}}(\kappa), l\})/2}
\end{aligned}$$

und damit ist das Lemma vollständig bewiesen. □

Es bietet sich an dieser Stelle an, auch das folgende Lemma zu beweisen, das wir allerdings erst später benötigen werden.

Lemma 3.12. *Seien* $\mathbf{a}, \mathbf{b} \in \mathcal{O}^s$. *Dann gilt für* $\mathfrak{p} \nmid 2$ *stets*

$$\left| \sum_{r\ (\mathfrak{p}^l)}^{*} \left(\prod_{i=1}^{s} \sum_{x_i\ (\mathfrak{p}^l)} \phi\Big(r\gamma_{\mathfrak{p}^l}(a_i x_i^2 + b_i x_i)\Big)\right)\right| \leq \mathrm{N}\,\mathfrak{p}^{l(s/2+1)} \prod_i \mathrm{N}(\mathfrak{p}^l, a_i)^{1/2}.$$

Beweis. Der Beweis ist im Wesentlichen identisch mit dem des vorherigen Lemmas.

Da wir oben bis zur Abschätzung der verallgemeinerten Kloostermansumme nicht verwendet haben, dass b_i und b_i' unabhängig von $r \in (\mathcal{O}/\mathfrak{p}^l)^*$ sind, können wir diese Variablen überall durch rb_i beziehungsweise rb_i' ersetzen. Des Weiteren gilt in diesem Lemma $\kappa = 0$. Wenn wir mit $\overline{4a_i'}$ das multiplikativ Inverse von $4a_i'$ bezüglich $\mathfrak{p}^l$ bezeichnen, folgt aus

$$\left| \sum_{r\ (\mathfrak{p}^l)}^{*} \left(\prod_{\substack{i=1 \\ 2\nmid l-v_i}}^{s} \left(\frac{ra_i'}{\mathfrak{p}}\right)\right) \phi\Big(- r\gamma_{\mathfrak{p}} \sum_{i=1}^{s} \overline{4a_i'} p^{v_i} b_i'^2\Big)\right| \leq \mathrm{N}\,\mathfrak{p}^l$$

die Behauptung. □

Wir können nun die Exponentialsumme für ungerade Ideale abschätzen und damit (14) von Dietmann [Die03] auf Zahlkörper verallgemeinern.

Lemma 3.13. *Sei* $\mathfrak{b}$ *ein zu* 2 *teilerfremdes ganzes Ideal und sei* $\mathbf{m} \in \widehat{\mathcal{O}}^s$. *Dann gilt*

$$\widetilde{S}(\mathfrak{b}, \mathbf{m}, \xi, \kappa) \ll \mathrm{N}\,\mathfrak{b}^{(s+1)/2+\varepsilon}\, \mathrm{N}(\mathfrak{b}, \kappa)^{1/2}\, \mathrm{N}(\mathfrak{b}^s, \Delta)^{1/2}.$$

Beweis. Dietmanns Beweis benötigt nur kleine Anpassungen. Wir haben bereits gezeigt, dass die Exponentialsumme semimultiplikativ ist, und wegen Lemma 3.10 können wir quadratische Formen modulo einer Primzahlpotenz diagonalisieren. Also können wir uns in diesem Beweis auf Primzahlpotenzen $\mathfrak{p}^l$ und Diagonalformen

$$A[\mathbf{x}] = a_1 x_1^2 + \ldots + a_s x_s^2$$

beschränken.

Für alle i seien $\varrho_i : \mathcal{O} \to \mathbb{C}$ Funktionen mit Periode $\mathfrak{p}^l$. Deren endliche Fourierentwicklung und deren Umkehrung

$$\widehat{\varrho}_i(y) = \frac{1}{\mathrm{N}\,\mathfrak{p}^l} \sum_{x\ (\mathfrak{p}^l)} \varrho_i(x)\phi(-\gamma_{\mathfrak{p}^l} xy)$$

können wir wie im Beweis von Lemma 2 von Brüdern und Fouvry [BF94] dazu nutzen, aus dem vorhergehenden Lemma

$$\begin{aligned}&\sum_{r\ (\mathfrak{p}^l)}\Bigg(\prod_{i=1}^{s}\sum_{x_i\ (\mathfrak{p}^l)}\varrho_i(x_i)\phi\Big(\gamma_{\mathfrak{p}^l}(ra_ix_i^2+b_ix_i)\Big)\Bigg)\phi(-\gamma_{\mathfrak{p}^l}r\kappa)\\&\ll \mathrm{N}\,\mathfrak{p}^{l(s+1)/2}T_\kappa(\mathfrak{p}^l,\mathbf{a})\prod_{i=1}^{s}\sum_{y\ (\mathfrak{p}^l)}|\widehat{\varrho}_i(y)|\end{aligned}$$

zu folgern. Weiterhin ergibt sich aus

$$\varrho_i(x)=\begin{cases}1, & x\equiv\xi_i \pmod{\mathfrak{p}^l,\eta},\\ 0, & \text{sonst}\end{cases}$$

durch einfaches Einsetzen und Nachrechnen

$$\sum_{y\ (\mathfrak{p}^l)}|\widehat{\varrho}_i(y)|=1.$$

Wegen $T_\kappa(\mathfrak{p}^l,\mathbf{a})\ll \mathrm{N}(\mathfrak{p}^l,\kappa)^{1/2}\,\mathrm{N}(\mathfrak{p}^{ls},\Delta)$ folgt damit die Behauptung. □

Um diejenigen Primideale behandeln zu können, die 2 teilen, benötigen wir eine Verallgemeinerung von Lemma 10 aus Dietmanns Arbeit [Die03].

Lemma 3.14. *Sei $B\in\mathcal{O}^{s\times s}$ eine symmetrische und nichtsinguläre Matrix. Weiterhin sei $\mathbf{b}\in\mathcal{O}^s$ und es gelte $\mathfrak{p}\mid 2$. Dann gilt*

$$\sum_{\mathbf{x}\ (\mathfrak{p}^l)}\phi\Big(\gamma_{\mathfrak{p}^l}(B[\mathbf{x}]+\mathbf{b}^T\mathbf{x})\Big)\ll \mathrm{N}\,\mathfrak{p}^{ls/2}\,\mathrm{N}(\mathfrak{p}^{ls},\det B)^{1/2}.$$

Beweis. Das Vorgehen in diesem Beweis orientiert sich an dem in §1 von Pommerenke [Pom59]. Es gilt

$$\left|\sum_{\mathbf{x}\ (\mathfrak{p}^l)}\phi\Big(\gamma_{\mathfrak{p}^l}(B[\mathbf{x}]+\mathbf{b}^T\mathbf{x})\Big)\right|^2=\sum_{\mathbf{x}\ (\mathfrak{p}^l)}\sum_{\mathbf{y}\ (\mathfrak{p}^l)}\phi\Big(\gamma_{\mathfrak{p}^l}\Big(B[\mathbf{x}]-B[\mathbf{y}]+\mathbf{b}^T(\mathbf{x}-\mathbf{y})\Big)\Big).$$

Wenn wir $\mathbf{x}=\mathbf{y}+\mathbf{z}$ setzen, ist dies gleich

$$\sum_{\mathbf{z}\ (\mathfrak{p}^l)}\phi\Big(\gamma_{\mathfrak{p}^l}(B[\mathbf{z}]+\mathbf{b}^T\mathbf{z})\Big)\sum_{\mathbf{y}\ (\mathfrak{p}^l)}\phi(2\gamma_{\mathfrak{p}^l}\mathbf{z}^TB\mathbf{y}).$$

Da $\mathcal{O}/\mathfrak{p}^l$ ein Hauptidealring ist, folgt aus dem Elementarteilersatz für Matrizen die Existenz von ganzen Matrizen U und V mit zu $\mathfrak{p}$ teilerfremden Determinanten, für die $D=U^TBV$ modulo $\mathfrak{p}^l$ eine Diagonalmatrix ist.

Wenn wir in obiger Summation $\mathbf{y}$ und $\mathbf{z}$ durch $V\mathbf{y}$ beziehungsweise $U\mathbf{z}$ ersetzen, erhalten wir

$$\begin{aligned}&\sum_{\mathbf{z}\ (\mathfrak{p}^l)} \phi\Big(\gamma_{\mathfrak{p}^l}(B[U\mathbf{z}]+\mathbf{b}^TU\mathbf{z})\Big)\sum_{\mathbf{y}\ (\mathfrak{p}^l)}\phi(2\gamma_{\mathfrak{p}^l}\mathbf{z}^TD\mathbf{y})\\&\le \mathrm{N}\,\mathfrak{p}^{ls}\#\{\mathbf{z}\in(\mathcal{O}/\mathfrak{p}^l)^s : 2\mathbf{z}^TD\equiv\mathbf{0}(\mathfrak{p}^l)\}\\&\ll \mathrm{N}\,\mathfrak{p}^{ls}\,\mathrm{N}(\mathfrak{p}^{ls},\det D).\end{aligned}$$

Da $\det B$ und $\det D$ gleich oft durch $\mathfrak{p}$ teilbar sind, ist damit die Behauptung gezeigt. □

Indem wir Dietmanns Vorgehen imitieren, erhalten wir mithilfe dieses Lemmas unser Analogon zu (15) von Dietmann [Die03].

Lemma 3.15. *Sei $\mathbf{m}\in\widehat{\mathcal{O}}^s$ und sei $\mathfrak{b}$ ein ganzes Ideal, dessen Primfaktoren alle 2 teilen. Dann gilt*

$$\widetilde{S}(\mathfrak{b},\mathbf{m},\boldsymbol{\xi},\kappa)\ll \mathrm{N}\,\mathfrak{b}^{s/2+1+\varepsilon}\,\mathrm{N}(\mathfrak{b}^s,\Delta)^{1/2}.$$

Beweis. Wieder genügt es, dies für Primidealpotenzen $\mathfrak{p}^l$ zu zeigen. Sei $j=l-\mathrm{v}_{\mathfrak{p}}(\mathfrak{p}^l,\eta)$. Wegen (2.2) gilt für beliebige $r\in(\mathcal{O}/\mathfrak{p}^l)^*$ die Gleichung

$$\begin{aligned}&\left|\sum_{\substack{\mathbf{x}\ (\mathfrak{b})\\ \mathbf{x}\equiv\boldsymbol{\xi}\ (\mathfrak{b},\eta)}}\phi\Big(\gamma_{\mathfrak{b}}\big(r(A[\mathbf{x}]-\kappa)+\mathbf{m}^T\mathbf{x}\big)\Big)\right|\\&=\left|\sum_{\mathbf{y}\ (\mathfrak{p}^j)}\phi\Big(\gamma_{\mathfrak{p}^l}\big(r(A[\boldsymbol{\xi}+p^{l-j}\mathbf{y}]-\kappa)+\mathbf{m}^T(\boldsymbol{\xi}+p^{l-j}\mathbf{y})\big)\Big)\right|\\&=\left|\sum_{\mathbf{y}\ (\mathfrak{p}^j)}\phi\Big(\gamma_{\mathfrak{p}^j}\big(r\beta A[\mathbf{y}]+(2r\boldsymbol{\xi}^TA+\mathbf{m})^T\mathbf{y}\big)\Big)\right|.\end{aligned}$$

Das vorhergehende Lemma liefert uns zusammen mit einer trivialen Abschätzung über r die Behauptung

$$\begin{aligned}\widetilde{S}(\mathfrak{p}^l,\mathbf{m},\boldsymbol{\xi},\kappa)&\ll \mathrm{N}\,\mathfrak{p}^{l+js/2}\,\mathrm{N}(\mathfrak{p}^{js},p^{s(l-j)}\Delta)^{1/2}\\&\ll \mathrm{N}\,\mathfrak{p}^{l(1+s/2)}\,\mathrm{N}(\mathfrak{p}^{ls},\Delta)^{1/2}.\end{aligned}$$

□

Wenn wir die Resultate dieses Abschnitts zusammensetzen, erhalten wir das folgende, Lemma 7 von Dietmann [Die03] verallgemeinernde, Resultat.

Lemma 3.16. *Seien $\mathfrak{b}=\mathfrak{b}_1\mathfrak{b}_2$ ganze Ideale mit $(\mathfrak{b}_1,2)=\mathcal{O}$ und $\mathfrak{b}_2+\mathfrak{p}=\mathcal{O}$ für alle $\mathfrak{p}\nmid 2$. Für $\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{\,s}$ gilt*

$$S_{\mathfrak{b}}(\mathbf{m})\ll|\mathrm{Nm}\,\Delta|^{1/2}\,\mathrm{N}\,\mathfrak{b}^{(s+1)/2+\varepsilon}\,\mathrm{N}\,\mathfrak{b}_2^{1/2}\,\mathrm{N}(\mathfrak{b}_1,\kappa)^{1/2}.$$

Diese Schranke ist für unsere Zwecke ausreichend.

3.5 Die singuläre Reihe

Als Nächstes werden wir die singuläre Reihe einführen und eine untere Schranke für sie herleiten. Für das folgende Lemma vergleiche §2.5 von Dietmann [Die03].

Lemma 3.17. *Die singuläre Reihe*

$$\mathfrak{S} = \sum_{(0)\neq\mathfrak{b}\subseteq\mathcal{O}} \frac{|\operatorname{Nm}\eta|^s}{\operatorname{N}(\mathfrak{b}\cap\eta)^s} S_{\mathfrak{b}}(\mathbf{0})$$

konvergiert absolut und es gilt

$$\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \operatorname{N}\mathfrak{b}\gg\operatorname{Nm}P}} \frac{|S_{\mathfrak{b}}(\mathbf{0})|}{\operatorname{N}(\mathfrak{b}\cap\eta)^s} \ll \begin{cases} |\operatorname{Nm}\Delta|^{1/2}|\operatorname{Nm}\kappa|^{\varepsilon}\operatorname{Nm}P^{(3-s)/2+\varepsilon}, & \kappa\neq 0,\\ |\operatorname{Nm}\Delta|^{1/2}\operatorname{Nm}P^{2-s/2+\varepsilon}, & \kappa = 0. \end{cases}$$

Beweis. Aus Lemma 3.16 folgt

$$\begin{aligned} &\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \operatorname{N}\mathfrak{b}\gg\operatorname{Nm}P}} \frac{|S_{\mathfrak{b}}(\mathbf{0})|}{\operatorname{N}(\mathfrak{b}\cap\eta)^s}\\ &\ll |\operatorname{Nm}\Delta|^{1/2}\sum_{\mathfrak{b}_2}\operatorname{N}\mathfrak{b}_2^{1-s/2+\varepsilon}\sum_{\operatorname{N}\mathfrak{b}_1\gg\operatorname{Nm}P/\operatorname{N}\mathfrak{b}_2}\operatorname{N}\mathfrak{b}_1^{(1-s)/2+\varepsilon}\operatorname{N}(\mathfrak{b}_1,\kappa)^{1/2}, \end{aligned} \tag{3.16}$$

wobei $\mathfrak{b}_1$ und $\mathfrak{b}_2$ den gleichen Einschränkungen unterliegen, wie in dem soeben verwendeten Lemma.

Es sei vorerst $\kappa\neq 0$. Wie in §8.1 von Browning und Vishe [BV14] können wir ausnutzen, dass κ höchstens $O(|\operatorname{Nm}\kappa|^{\varepsilon})$ Idealteiler besitzt und somit für jedes M stets

$$\begin{aligned} \sum_{M\leq\operatorname{N}\mathfrak{b}_1<2M}\operatorname{N}(\mathfrak{b}_1,\kappa)^{1/2} &\leq \sum_{\mathfrak{c}\mid\kappa}\operatorname{N}\mathfrak{c}^{1/2}\sum_{\substack{\mathfrak{c}\mid\mathfrak{b}_1\\ M\leq\operatorname{N}\mathfrak{b}_1<2M}} 1\\ &\ll \sum_{\mathfrak{c}\mid\kappa}\operatorname{N}\mathfrak{c}^{1/2}\frac{M}{\operatorname{N}\mathfrak{c}}\\ &\ll M|\operatorname{Nm}\kappa|^{\varepsilon} \end{aligned} \tag{3.17}$$

gilt. Also können wir mithilfe einer dyadischen Unterteilung

$$\begin{aligned} \sum_{\operatorname{N}\mathfrak{b}_1\gg\operatorname{Nm}P/\operatorname{N}\mathfrak{b}_2}\operatorname{N}\mathfrak{b}_1^{(1-s)/2+\varepsilon}\operatorname{N}(\mathfrak{b}_1,\kappa)^{1/2} &\ll |\operatorname{Nm}\kappa|^{\varepsilon}\sum_{r\geq 0}\left(2^r\frac{\operatorname{Nm}P}{\operatorname{N}\mathfrak{b}_2}\right)^{(3-s)/2+\varepsilon}\\ &\ll |\operatorname{Nm}\kappa|^{\varepsilon}\left(\frac{\operatorname{Nm}P}{\operatorname{N}\mathfrak{b}_2}\right)^{(3-s)/2+\varepsilon} \end{aligned}$$

folgern. Also ist die rechte Seite von (3.16) wegen $\prod_{\mathfrak{p}|2} \mathrm{N}\,\mathfrak{p} = 2^d$ stets

$$\begin{aligned}
&\ll |\mathrm{Nm}\,\Delta|^{1/2} |\mathrm{Nm}\,\kappa|^{\varepsilon}\, \mathrm{Nm}\, P^{(3-s)/2+\varepsilon} \sum_{\mathfrak{b}_2} \mathrm{N}\,\mathfrak{b}_2^{-1/2} \\
&\ll |\mathrm{Nm}\,\Delta|^{1/2} |\mathrm{Nm}\,\kappa|^{\varepsilon}\, \mathrm{Nm}\, P^{(3-s)/2+\varepsilon} \left(\sum_{r\geq 0} 2^{-r/2} \right)^d \\
&\ll |\mathrm{Nm}\,\Delta|^{1/2} |\mathrm{Nm}\,\kappa|^{\varepsilon}\, \mathrm{Nm}\, P^{(3-s)/2+\varepsilon}
\end{aligned}$$

und damit ist die behauptete Ungleichung für $\kappa \neq 0$ gezeigt.

Im Fall $\kappa = 0$ impliziert (3.16) wegen $s \geq 5$ direkt

$$\begin{aligned}
\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O} \\ \mathrm{N}\,\mathfrak{b}\gg \mathrm{Nm}\, P}} \frac{|S_{\mathfrak{b}}(\mathbf{0})|}{\mathrm{N}(\mathfrak{b}\cap\eta)^s} &\ll |\mathrm{Nm}\,\Delta|^{1/2}\, \mathrm{Nm}\, P^{2-s/2+\varepsilon} \sum_{\mathfrak{b}_2} \mathrm{N}\,\mathfrak{b}_2^{-1} \\
&\ll |\mathrm{Nm}\,\Delta|^{1/2}\, \mathrm{Nm}\, P^{2-s/2+\varepsilon}.
\end{aligned}$$

Die absolute Konvergenz der singulären Reihe folgt in beiden Fällen aus der bewiesenen Ungleichung. □

Da wir die singuläre Reihe auf die gleiche Art und Weise wie Dietmann auswerten können, basiert der restliche Abschnitt auf §2.6 seiner Arbeit [Die03]. Wie üblich hat die singuläre Reihe eine Produktentwicklung.

Lemma 3.18. *Für beliebige ganze Ideale $\mathfrak{b}$ sei*

$$\varrho(\mathfrak{b}) = \#\left\{\mathbf{x} \in (\mathcal{O}/\mathfrak{b})^s : \mathbf{x} \equiv \boldsymbol{\xi} \pmod{(\mathfrak{b},\eta)}, A[\mathbf{x}] \equiv \kappa \pmod{\mathfrak{b}}\right\}.$$

Dann gilt $\mathfrak{S} = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}$ mit

$$\chi_{\mathfrak{p}} = \sum_{l=0}^{\infty} \frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{p}^l\cap\eta)^s} S_{\mathfrak{p}^l}(\mathbf{0}) = \mathrm{N}\,\mathfrak{p}^{s\,\mathrm{v}_{\mathfrak{p}}(\eta)} \lim_{l\to\infty} \mathrm{N}\,\mathfrak{p}^{(1-s)l} \varrho(\mathfrak{p}^l).$$

Insbesondere ist

$$\frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{b}\cap\eta)^s} S_{\mathfrak{b}}(\mathbf{0})$$

als Funktion von $\mathfrak{b}$ multiplikativ.

Beweis. Zuerst leiten wir wie im Beweis von Lemma 15 von Dietmann [Die03] einen Zusammenhang zwischen $S_{\mathfrak{b}}$ und $\varrho(\mathfrak{b})$ her.

Wir setzen

$$U(\mathfrak{b}, r) = \sum_{\substack{\mathbf{x} \bmod \mathfrak{b} \\ \mathbf{x} \equiv \boldsymbol{\xi} \bmod (\mathfrak{b}, \eta)}} \phi\Big(r\gamma_{\mathfrak{b}}(A[\mathbf{x}] - \kappa)\Big)$$

und erhalten

$$\varrho(\mathfrak{b}) = \mathrm{N}\,\mathfrak{b}^{-1} \sum_{r \bmod \mathfrak{b}} U(\mathfrak{b}, r).$$

Sei μ die Möbiusfunktion auf den ganzen Idealen. Aus (3.14) folgt

$$S_{\mathfrak{b}}(\mathbf{0}) = \sum_{r \bmod \mathfrak{b}}^{*} U(\mathfrak{b}, r) = \sum_{r \bmod \mathfrak{b}} \sum_{\mathfrak{c} \mid (\mathfrak{b}, r)} \mu(\mathfrak{c}) U(\mathfrak{b}, r) = \sum_{\mathfrak{c} \mid \mathfrak{b}} \mu(\mathfrak{c}) \sum_{\substack{r \bmod \mathfrak{b} \\ \mathfrak{c} \mid r}} U(\mathfrak{b}, r).$$

Wir betrachten nun die innere Summe. Wegen Lemma 2.1(ii) existieren α und β mit $\mathrm{v}_{\mathfrak{p}}(\alpha) = \mathrm{v}_{\mathfrak{p}}(\mathfrak{c})$ und $\mathrm{v}_{\mathfrak{p}}(\beta) = \mathrm{v}_{\mathfrak{p}}(\mathfrak{b}/\mathfrak{c})$ für alle $\mathfrak{p} \mid \mathfrak{b}$. Aus Lemma 2.3(i) folgt

$$\begin{aligned}
\sum_{\substack{r \bmod \mathfrak{b} \\ \mathfrak{c} \mid r}} U(\mathfrak{b}, r) &= \sum_{r \bmod (\mathfrak{b}/\mathfrak{c})} U(\mathfrak{b}, \alpha r) \\
&= \sum_{r \bmod (\mathfrak{b}/\mathfrak{c})} \sum_{\substack{\mathbf{y} \bmod (\mathfrak{b}/\mathfrak{c}) \\ \mathbf{y} \equiv \boldsymbol{\xi} \bmod (\mathfrak{b}/\mathfrak{c}, \eta)}} \phi\Big(\alpha r \gamma_{\mathfrak{b}}(A[\mathbf{y}] - \kappa)\Big) \sum_{\substack{\mathbf{z} \bmod \mathfrak{c} \\ \mathbf{y} + \beta\mathbf{z} \equiv \boldsymbol{\xi} \bmod (\mathfrak{b}, \eta)}} 1 \\
&= \frac{\mathrm{N}\,\mathfrak{c}^s\, \mathrm{N}(\mathfrak{b}/\mathfrak{c}, \eta)^s}{\mathrm{N}(\mathfrak{b}, \eta)^s} \sum_{r \bmod (\mathfrak{b}/\mathfrak{c})} U(\mathfrak{b}/\mathfrak{c}, r).
\end{aligned}$$

Also gilt

$$\begin{aligned}
\frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{b} \cap \eta)^s} S_{\mathfrak{b}}(\mathbf{0}) &= \sum_{\mathfrak{c} \mid \mathfrak{b}} \mu(\mathfrak{c}) \frac{\mathrm{N}(\mathfrak{b}/\mathfrak{c}, \eta)^s}{\mathrm{N}(\mathfrak{b}/\mathfrak{c})^s} \sum_{r \bmod (\mathfrak{b}/\mathfrak{c})} U(\mathfrak{b}/\mathfrak{c}, r) \\
&= \sum_{\mathfrak{c} \mid \mathfrak{b}} \mu(\mathfrak{c}) \frac{\mathrm{N}(\mathfrak{b}/\mathfrak{c}, \eta)^s}{\mathrm{N}(\mathfrak{b}/\mathfrak{c})^{s-1}} \varrho(\mathfrak{b}/\mathfrak{c}).
\end{aligned}$$

Da wir aus dem chinesischen Restsatz folgern können, dass $\varrho(\mathfrak{b})$ multiplikativ ist, ist auch die linke Seite der obigen Gleichung als Funktion von $\mathfrak{b}$ multiplikativ.

Wie bei Lemma 16 von Dietmann [Die03] können wir darauf aufbauend wie folgt argumentieren. Weil

$$\chi_{\mathfrak{p}} = \sum_{l=0}^{\infty} \frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{p}^l \cap \eta)^s} S_{\mathfrak{p}^l}(\mathbf{0})$$

als Teilfolge von $\mathfrak{S}$ ebenfalls absolut konvergiert, haben wir damit $\mathfrak{S} = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}$ gezeigt. Des Weiteren gilt

$$\begin{aligned}\sum_{k=0}^{l} \frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{p}^k \cap \eta)^s} S_{\mathfrak{p}^k}(\mathbf{0}) &= \sum_{k=0}^{l}\sum_{j=0}^{k} \mu(\mathfrak{p}^j) \frac{\mathrm{N}(\mathfrak{p}^{k-j}, \eta)^s}{\mathrm{N}\,\mathfrak{p}^{(k-j)(s-1)}} \varrho(\mathfrak{p}^{k-j}) \\ &= \frac{\mathrm{N}(\mathfrak{p}^l, \eta)^s}{\mathrm{N}\,\mathfrak{p}^{l(s-1)}} \varrho(\mathfrak{p}^l),\end{aligned}$$

sodass der Grenzübergang von l gegen unendlich die Behauptung liefert. □

Wir werden die $\chi_{\mathfrak{p}}$ einzeln abschätzen. Dabei beschränken wir uns zuerst auf diejenigen $\mathfrak{p}$ die $2\eta\Delta$ nicht teilen. Da Dietmann dabei Resultate von Iwaniec [Iwa97] verwendet, werden wir auch diese auf Zahlkörper übertragen.

Das folgende Lemma verallgemeinert (11.72) von Iwaniec [Iwa97].

Lemma 3.19. *Sei $s = 4$ und $\kappa \neq 0$. Wenn $2\eta\Delta$ nicht von $\mathfrak{p}$ geteilt wird, gilt*

$$\chi_{\mathfrak{p}} = \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}^2}\left(\frac{\Delta}{\mathfrak{p}}\right)\right)\left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}}\left(\frac{\Delta}{\mathfrak{p}}\right)\right)^{-1}\left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\kappa)+1}}\left(\frac{\Delta}{\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\kappa)+1}}\right)\right).$$

Beweis. Vorerst nehmen wir nur $s \geq 4$ an.

Als Erstes berechnen wir wie in Lemma 10.5 von Iwaniec [Iwa97] Gaußsummen. Sei $l \in \mathbb{N}$ und sei $r \in \mathcal{O}$ teilerfremd zu $\mathfrak{p}$. Dann können wir Lemma 3.10 nutzen, um lokal zu diagonalisieren. Also existieren $m_i \in \mathcal{O}$ mit $\prod m_i = \Delta$ und

$$\sum_{\mathbf{x}\,(\mathfrak{p}^l)} \phi(r\gamma_{\mathfrak{p}^l} A[\mathbf{x}]) = \prod_{j=1}^{s}\left(\sum_{x\,(\mathfrak{p}^l)} \phi(r\gamma_{\mathfrak{p}^l} m_j x^2)\right).$$

Analog zu unserem Vorgehen bei (3.15) folgt die Gleichheit zu

$$\left(\frac{\Delta}{\mathfrak{p}^l}\right)\left(\left(\frac{r}{\mathfrak{p}^l}\right)\sum_{x\,(\mathfrak{p}^l)} \phi(\gamma_{\mathfrak{p}^l} x^2)\right)^s = \left(\frac{\Delta}{\mathfrak{p}^l}\right)\left(\frac{r}{\mathfrak{p}^l}\right)^s \mathrm{N}\,\mathfrak{p}^{ls/2}\varepsilon_{\mathfrak{p},l}^s,$$

wobei $\varepsilon_{\mathfrak{p},l} = 1$ für gerade l und $|\varepsilon_{\mathfrak{p},l}| = 1$ für ungerade l gilt.

Damit können wir im restlichen Beweis analog zu dem Vorgehen in §11.5 von Iwaniec [Iwa97] argumentieren. Zusammen mit (3.14) folgt

$$\begin{aligned}S_{\mathfrak{p}^l}(\mathbf{0}) &= \sideset{}{^*}\sum_{r\,(\mathfrak{p}^l)}\sum_{\mathbf{x}\,(\mathfrak{p}^l)} \phi\Big(r\gamma_{\mathfrak{p}^l}(A[\mathbf{x}] - \kappa)\Big) \\ &= \left(\frac{\Delta}{\mathfrak{p}^l}\right)\mathrm{N}\,\mathfrak{p}^{ls/2}\varepsilon_{\mathfrak{p},l}^s \sideset{}{^*}\sum_{r\,(\mathfrak{p}^l)}\left(\frac{r}{\mathfrak{p}^l}\right)^s \phi(-r\gamma_{\mathfrak{p}^l}\kappa). \qquad (3.18)\end{aligned}$$

Sei $\mu(\cdot)$ wie zuvor die Möbiusfunktion für ganze Ideale. Dann folgt für alle l aus der Möbiusschen Umkehrformel

$$\sum_{r\ (\mathfrak{p}^l)}^{*} \phi(-r\gamma_{\mathfrak{p}^l}\kappa) = \sum_{j=0}^{\min\{l,\mathrm{v}_\mathfrak{p}(\kappa)\}} \mu(\mathfrak{p}^{l-j})\,\mathrm{N}\,\mathfrak{p}^j.$$

Wenn s gerade ist, folgt aus Lemma 3.18, dass

$$\begin{aligned}
\chi_\mathfrak{p} &= \sum_{l=0}^{\infty} \mathrm{N}\,\mathfrak{p}^{-ls/2} \left(\frac{\Delta}{\mathfrak{p}^l}\right) \varepsilon_{\mathfrak{p},l}^s \sum_{r\ (\mathfrak{p}^l)}^{*} \phi(-r\gamma_{\mathfrak{p}^l}\kappa) \\
&= \sum_{j=0}^{\mathrm{v}_\mathfrak{p}(\kappa)} \mathrm{N}\,\mathfrak{p}^j \sum_{l=j}^{\infty} \mu(\mathfrak{p}^{l-j})\,\mathrm{N}\,\mathfrak{p}^{-ls/2} \left(\frac{\Delta}{\mathfrak{p}^l}\right) \varepsilon_{\mathfrak{p},l}^s \\
&= \sum_{j=0}^{\mathrm{v}_\mathfrak{p}(\kappa)} \mathrm{N}\,\mathfrak{p}^{j(1-s/2)} \left(\frac{\Delta}{\mathfrak{p}^j}\right) \left(\varepsilon_{\mathfrak{p},j}^s - \mathrm{N}\,\mathfrak{p}^{-s/2} \left(\frac{\Delta}{\mathfrak{p}}\right) \varepsilon_{\mathfrak{p},j+1}^s\right).
\end{aligned}$$

Da dies für beliebige κ richtig ist und $\chi_\mathfrak{p} \in \mathbb{R}$ gilt, folgt aus den Fällen $\mathrm{v}_\mathfrak{p}(\kappa) = 0$ und $s \in \{4, 6\}$, dass sowohl $\varepsilon_\mathfrak{p}^4$ als auch $\varepsilon_\mathfrak{p}^6$ reelle Zahlen sind. Wegen $|\varepsilon_\mathfrak{p}| = 1$ gilt also $\varepsilon_\mathfrak{p}^4 = 1$.

Für $s = 4$ können wir daher

$$\begin{aligned}
\chi_\mathfrak{p} &= \sum_{j=0}^{\mathrm{v}_\mathfrak{p}(\kappa)} \mathrm{N}\,\mathfrak{p}^{-j} \left(\frac{\Delta}{\mathfrak{p}^j}\right) \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}^2} \left(\frac{\Delta}{\mathfrak{p}}\right)\right) \\
&= \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}^2} \left(\frac{\Delta}{\mathfrak{p}}\right)\right) \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}} \left(\frac{\Delta}{\mathfrak{p}}\right)\right)^{-1} \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\kappa)+1}} \left(\frac{\Delta}{\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\kappa)+1}}\right)\right)
\end{aligned}$$

folgern. Damit ist die Behauptung bewiesen. □

Aus diesem Lemma können wir nach kurzer Rechnung folgern, dass für $s = 4$ und $\kappa \neq 0$ stets

$$\begin{aligned}
\prod_{\mathfrak{p}\nmid\eta} \chi_p &\gg \prod_{\mathfrak{p}\mid\kappa} \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}}\right) \gg \prod_{\substack{p\mid\mathrm{Nm}\,\kappa \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right)^d = \frac{\varphi(\mathrm{Nm}\,\kappa)^d}{|\mathrm{Nm}\,\kappa|^d} \\
&\gg \frac{1}{(\log\log 3|\mathrm{Nm}\,\kappa|)^d}
\end{aligned}$$

gilt.

Im Fall $s \geq 5$ nutzen wir für kleine Primideale ein Liftingargument, das Dietmann erst später benötigt. Das folgende Lemma verallgemeinert und verbessert Proposition 2 von Dietmann [Die03] und den darauf folgenden Absatz. Es gilt unabhängig davon, ob $2\eta\Delta$ von $\mathfrak{p}$ geteilt wird.

Lemma 3.20. *Es sei $l > \mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi}) \geq \mathrm{v}_\mathfrak{p}(\eta)$. Dann gilt*

$$\chi_\mathfrak{p} \geq \mathrm{N}\,\mathfrak{p}^{s\,\mathrm{v}_\mathfrak{p}(\eta)-(\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})+1)(s-1)}.$$

Beweis. Wir betrachten

$$\varrho^*(\mathfrak{p}^l) = \#\left\{\mathbf{x} \in \left(\mathcal{O}/\mathfrak{p}^l\right)^s : \mathbf{x} \equiv \boldsymbol{\xi} \pmod{\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})+1}}, A[\mathbf{x}] \equiv \kappa \pmod{\mathfrak{p}^{l+\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})}}\right\}.$$

Da $\mathbf{x} \equiv \boldsymbol{\xi} \pmod{\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})+1}}$ insbesondere $\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})} \mid 2A\mathbf{x}$ impliziert, ist diese Definition für $l > \mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})$ unabhängig vom gewählten Repräsentantensystem für $\mathcal{O}/\mathfrak{p}^l$. Wegen $A[\boldsymbol{\xi}] = \kappa$ gilt also $\varrho^*(\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})+1}) \geq 1$.

Wir werden zeigen, dass sich jede für $\varrho^*(\mathfrak{p}^l)$ mitgezählte Lösung $\mathbf{x}$ zu $\mathrm{N}\,\mathfrak{p}^{s-1}$ Lösungen für $\varrho^*(\mathfrak{p}^{l+1})$ liften lässt. Wegen (2.3) gilt

$$\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})} \parallel 2A\mathbf{x}, \qquad A[\mathbf{x}] - \kappa \equiv ap^{l+\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})} \pmod{\mathfrak{p}^{l+1+\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})}}$$

für ein $a \in \mathcal{O}$.

Für jedes $\mathbf{u} \in (\mathcal{O}/\mathfrak{p})^s$ gilt $\mathbf{y} = \mathbf{x} + p^l\mathbf{u} \in (\mathcal{O}/\mathfrak{p}^{l+1})^s$. Es folgt

$$\begin{aligned} \mathbf{y} &\equiv \boldsymbol{\xi} \pmod{\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})+1}}, \\ A[\mathbf{y}] - \kappa &\equiv ap^{l+\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})} + 2p^l\mathbf{u}^T A\mathbf{x} \pmod{\mathfrak{p}^{l+1+\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})}}. \end{aligned} \tag{3.19}$$

Also gibt es ein $\mathbf{v} \not\equiv 0 \pmod{\mathfrak{p}}$, sodass die rechte Seite von (3.19) genau dann kongruent zu 0 modulo $\mathfrak{p}^{l+1+\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})}$ ist, wenn $a + \mathbf{u}^T\mathbf{v} \equiv 0 \pmod{\mathfrak{p}}$ gilt. Da diese Kongruenz für $\mathrm{N}\,\mathfrak{p}^{s-1}$ verschiedene $\mathbf{u} \in (\mathcal{O}/\mathfrak{p})^s$ erfüllt ist und bei diesem Verfahren aus unterschiedlichen $\mathbf{x}$ verschiedene $\mathbf{y}$ entstehen, impliziert dies

$$\varrho^*(\mathfrak{p}^l) \geq \mathrm{N}\,\mathfrak{p}^{(l-\mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})-1)(s-1)}.$$

Wegen $\varrho(\mathfrak{p}^l) \geq \varrho^*(\mathfrak{p}^l)$ folgt die Behauptung aus Lemma 3.18. □

Dieses Resultat können wir auf dieselbe Art wie Iwaniec [Iwa97] nutzen. Aus Lemma 3.18 folgt, dass $S_\mathfrak{b}(\mathbf{0})$ für zu η teilerfremde Ideale multiplikativ in $\mathfrak{b}$ ist. Triviales Abschätzen von (3.18) liefert für solche $\mathfrak{b}$ deshalb $|S_\mathfrak{b}(\mathbf{0})| \leq \mathrm{N}\,\mathfrak{b}^{s/2+1}$. Also gilt im Fall $s \geq 5$ für eine geeignete untere Schranke für $\mathrm{N}\,\mathfrak{p}$ die Abschätzung

$$\begin{aligned} \prod_{\substack{\mathfrak{p}\nmid 2\eta\Delta \\ \mathrm{N}\,\mathfrak{p}\gg 1}} \chi_\mathfrak{p} &= \sum_{\substack{(\mathfrak{b},2\eta\Delta)=\mathcal{O} \\ \mathfrak{p}\nmid\mathfrak{b}\forall\mathfrak{p}:\mathrm{N}\,\mathfrak{p}\ll 1}} \mathrm{N}\,\mathfrak{b}^{-s} S_\mathfrak{b}(\mathbf{0}) \geq 1 - \sum_{\substack{(\mathfrak{b},2\eta\Delta)=\mathcal{O} \\ \mathfrak{p}\nmid\mathfrak{b}\forall\mathfrak{p}:\mathrm{N}\,\mathfrak{p}\ll 1}} \mathrm{N}\,\mathfrak{b}^{-s/2-1} \\ &\geq 1 - \sum_{\mathrm{N}\,\mathfrak{b}\gg 1} \mathrm{N}\,\mathfrak{b}^{-3/2} \geq \frac{1}{2}. \end{aligned}$$

Für kleine $\mathfrak{p} \nmid 2\eta\Delta$ können wir wegen

$$\mathrm{v}_\mathfrak{p}(\boldsymbol{\xi}) = \mathrm{v}_\mathfrak{p}(2\Delta\boldsymbol{\xi}) = \mathrm{v}_\mathfrak{p}(\Delta A^{-1} 2A\boldsymbol{\xi}) \geq \mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})$$

aus dem vorhergehenden Lemma

$$\prod_{\substack{\mathfrak{p}\nmid 2\eta\Delta \\ \mathrm{N}\,\mathfrak{p}\ll 1}} \chi_\mathfrak{p} \geq \prod_{\substack{\mathfrak{p}\nmid 2\eta\Delta \\ \mathrm{N}\,\mathfrak{p}\ll 1}} \mathrm{N}\,\mathfrak{p}^{(\mathrm{v}_\mathfrak{p}(\boldsymbol{\xi})+1)(1-s)} \gg \prod_{\mathfrak{p}\nmid 2\eta\Delta} \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\boldsymbol{\xi})(1-s)}$$

folgern und haben damit insgesamt

$$\prod_{\mathfrak{p}\nmid 2\eta\Delta} \chi_\mathfrak{p} \gg \prod_{\mathfrak{p}\nmid 2\eta\Delta} \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\boldsymbol{\xi})(1-s)}$$

gezeigt.

Bei Primidealen, die $2\eta\Delta$ teilen, müssen wir anders argumentieren. Wir beginnen damit,

$$S_{\mathfrak{p}^l}(\mathbf{0}) = \sideset{}{^*}\sum_{a\ (\mathfrak{p}^l)} \sum_{\substack{\mathbf{x}\ (\mathfrak{p}^l\cap\eta) \\ \mathbf{x}\equiv\boldsymbol{\xi}\ (\eta)}} \phi\Big(a\gamma_{\mathfrak{p}^l}(A[\mathbf{x}]-\kappa)\Big)$$

abhängig von l genauer auszuwerten.

Für $l \leq \mathrm{v}_\mathfrak{p}(\eta)$ gilt

$$S_{\mathfrak{p}^l}(\mathbf{0}) = \sideset{}{^*}\sum_{a\ (\mathfrak{p}^l)} \phi\Big(a\gamma_{\mathfrak{p}^l}(A[\boldsymbol{\xi}]-\kappa)\Big) = \varphi(\mathfrak{p}^l). \tag{3.20}$$

Im Fall von $l > \mathrm{v}_\mathfrak{p}(\eta)$ nutzen wir (2.2) und ersetzen $\mathbf{x}$ durch $\boldsymbol{\xi} + p^{\mathrm{v}_\mathfrak{p}(\eta)}\mathbf{y}$. Wir erhalten

$$S_{\mathfrak{p}^l}(\mathbf{0}) = \sideset{}{^*}\sum_{a\ (\mathfrak{p}^l)} \sum_{\mathbf{y}\ (\mathfrak{p}^{l-\mathrm{v}_\mathfrak{p}(\eta)})} \phi\Big(a\gamma_{\mathfrak{p}^{l-\mathrm{v}_\mathfrak{p}(\eta)}}(p^{\mathrm{v}_\mathfrak{p}(\eta)}A[\mathbf{y}] + 2\boldsymbol{\xi}^T A\mathbf{y})\Big).$$

Für $\mathrm{v}_\mathfrak{p}(\eta) < l \leq 2\,\mathrm{v}_\mathfrak{p}(\eta)$ gilt folglich

$$S_{\mathfrak{p}^l}(\mathbf{0}) = \begin{cases} 0, & 2A\boldsymbol{\xi} \not\equiv \mathbf{0} \pmod{\mathfrak{p}^{l-\mathrm{v}_\mathfrak{p}(\eta)}}, \\ \varphi(\mathfrak{p}^l)\,\mathrm{N}\,\mathfrak{p}^{s(l-\mathrm{v}_\mathfrak{p}(\eta))}, & 2A\boldsymbol{\xi} \equiv \mathbf{0} \pmod{\mathfrak{p}^{l-\mathrm{v}_\mathfrak{p}(\eta)}}. \end{cases} \tag{3.21}$$

Im Fall $l > 2\,\mathrm{v}_\mathfrak{p}(\eta)$ substituieren wir $\mathbf{y} = \mathbf{z} + p^{l-2\,\mathrm{v}_\mathfrak{p}(\eta)}\mathbf{u}$ und erhalten so die Gleichheit von $S_{\mathfrak{p}^l}(\mathbf{0})$ zu

$$\sideset{}{^*}\sum_{a\ (\mathfrak{p}^l)} \sum_{\mathbf{z}\ (\mathfrak{p}^{l-2\,\mathrm{v}_\mathfrak{p}(\eta)})} \phi\Big(a\gamma_{\mathfrak{p}^{l-\mathrm{v}_\mathfrak{p}(\eta)}}(p^{\mathrm{v}_\mathfrak{p}(\eta)}A[\mathbf{z}] + 2\boldsymbol{\xi}^T A\mathbf{z})\Big) \sum_{\mathbf{u}\ (\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)})} \phi(2a\gamma_{\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)}}\boldsymbol{\xi}^T A\mathbf{u}).$$

Also verschwindet $S_{\mathfrak{p}^l}(\mathbf{0})$ für $\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)} \nmid 2A\boldsymbol{\xi}$ und im Fall $\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)} \mid 2A\boldsymbol{\xi}$ haben wir

$$\begin{aligned} S_{\mathfrak{p}^l}(\mathbf{0}) &= \mathrm{N}\,\mathfrak{p}^{s\,\mathrm{v}_\mathfrak{p}(\eta)} \sideset{}{^*}\sum_{a\,(\mathfrak{p}^l)} \sum_{\mathbf{z}\,(\mathfrak{p}^{l-2\,\mathrm{v}_\mathfrak{p}(\eta)})} \phi\Big(a\gamma_{\mathfrak{p}^{l-\mathrm{v}_\mathfrak{p}(\eta)}}(p^{\mathrm{v}_\mathfrak{p}(\eta)}A[\mathbf{z}] + 2\boldsymbol{\xi}^T A\mathbf{z})\Big) \\ &= \mathrm{N}\,\mathfrak{p}^{(s+2)\,\mathrm{v}_\mathfrak{p}(\eta)} \sideset{}{^*}\sum_{a\,(\mathfrak{p}^{l-2\,\mathrm{v}_\mathfrak{p}(\eta)})} \sum_{\mathbf{z}\,(\mathfrak{p}^{l-2\,\mathrm{v}_\mathfrak{p}(\eta)})} \phi\Big(a\gamma_{\mathfrak{p}^{l-2\,\mathrm{v}_\mathfrak{p}(\eta)}}(A[\mathbf{z}] + \mathbf{w}^T\mathbf{z})\Big) \quad (3.22) \end{aligned}$$

für ein wegen (2.3) existierendes $\mathbf{w} \in \mathcal{O}^s$. Dies können wir dazu nutzen, $\chi_\mathfrak{p}$ für $\mathfrak{p} \mid 2\eta\Delta$ nach unten abzuschätzen. Wenn $\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)} \nmid 2A\boldsymbol{\xi}$ gilt, folgt aus dem Obigen leicht

$$\chi_\mathfrak{p} = \sum_{l=0}^{2\,\mathrm{v}_\mathfrak{p}(\eta)} \frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{p}^l \cap \eta)^s} S_{\mathfrak{p}^l}(\mathbf{0}) \geq \sum_{l=0}^{\mathrm{v}_\mathfrak{p}(\eta)} \varphi(\mathfrak{p}^l) = \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)}.$$

Wenn $2A\boldsymbol{\xi}$ dagegen nicht von $\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)}$ geteilt wird, müssen wir aufwändiger argumentieren.

Lemma 3.21. *Es gelte* $\mathfrak{p} \mid 2\eta\Delta$ *und* $\mathrm{v}_\mathfrak{p}(\eta) \leq \mathrm{v}_\mathfrak{p}(2A\boldsymbol{\xi})$. *Aus* $\mathfrak{p} \nmid 30$ *folgt*

$$\chi_\mathfrak{p} \geq \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)+(\mathrm{v}_\mathfrak{p}(\eta)-\mathrm{v}_\mathfrak{p}(2\Delta\boldsymbol{\xi}))(s-1)}$$

und $\mathfrak{p} \mid 30$ *impliziert*

$$\chi_\mathfrak{p} \gg \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\eta)+(\mathrm{v}_\mathfrak{p}(\eta)-\mathrm{v}_\mathfrak{p}(2\Delta\boldsymbol{\xi}))(s-1)}.$$

Beweis. Wir untersuchen zunächst den Fall $\mathfrak{p} \nmid 30$. Diese Bedingung impliziert insbesondere $\mathrm{N}\,\mathfrak{p} > 5$. Aus (3.20) und (3.21) folgt

$$\begin{aligned} \sum_{l=0}^{2\,\mathrm{v}_\mathfrak{p}(\eta)} \frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{p}^l \cap \eta)^s} S_{\mathfrak{p}^l}(\mathbf{0}) &= \sum_{l=0}^{\mathrm{v}_\mathfrak{p}(\eta)} \varphi(\mathfrak{p}^l) + \sum_{l=\mathrm{v}_\mathfrak{p}(\eta)+1}^{2\,\mathrm{v}_\mathfrak{p}(\eta)} \frac{\mathrm{N}(\mathfrak{p}^l, \eta)^s}{\mathrm{N}\,\mathfrak{p}^{ls}} \mathrm{N}\,\mathfrak{p}^{s(l-\mathrm{v}_\mathfrak{p}(\eta))}\varphi(\mathfrak{p}^l) \\ &= \sum_{l=0}^{2\,\mathrm{v}_\mathfrak{p}(\eta)} \varphi(\mathfrak{p}^l) = \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_\mathfrak{p}(\eta)}, \end{aligned}$$

während (3.22) die Gleichung

$$\begin{aligned} &\sum_{l=1}^{\infty} \frac{|\mathrm{Nm}\,\eta|^s}{\mathrm{N}(\mathfrak{p}^{l+2\,\mathrm{v}_\mathfrak{p}(\eta)} \cap \eta)^s} S_{\mathfrak{p}^{l+2\,\mathrm{v}_\mathfrak{p}(\eta)}}(\mathbf{0}) \\ &= \sum_{l=1}^{\infty} \mathrm{N}\,\mathfrak{p}^{-ls+2\,\mathrm{v}_\mathfrak{p}(\eta)} \sideset{}{^*}\sum_{a\,(\mathfrak{p}^l)} \sum_{\mathbf{z}\,(\mathfrak{p}^l)} \phi\Big(a\gamma_{\mathfrak{p}^l}(A[\mathbf{z}] + \mathbf{w}^T\mathbf{z})\Big) \end{aligned}$$

impliziert. Also gilt

$$\chi_{\mathfrak{p}} = \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_{\mathfrak{p}}(\eta)} \sum_{l=0}^{\infty} \mathrm{N}\,\mathfrak{p}^{-ls} \sideset{}{^*}\sum_{a\ (\mathfrak{p}^l)} \sum_{\mathbf{z}\ (\mathfrak{p}^l)} \phi\Big(a\gamma_{\mathfrak{p}^l}(A[\mathbf{z}] + \mathbf{w}^T\mathbf{z})\Big).$$

Wegen Lemma 3.10 können wir o. B. d. A. davon ausgehen, dass A eine Diagonalmatrix ist. Diese Diagonalisierung lässt $\mathrm{v}_{\mathfrak{p}}(\Delta)$, $\mathrm{v}_{\mathfrak{p}}(A\boldsymbol{\xi})$ und $\mathrm{v}_{\mathfrak{p}}(\boldsymbol{\xi})$ unverändert.

Wenn höchstens $s-3$ Diagonaleinträge von A durch $\mathfrak{p}$ teilbar sind, impliziert Lemma 3.12 die Abschätzung

$$\left|\sideset{}{^*}\sum_{a\ (\mathfrak{p}^l)} \sum_{\mathbf{z}\ (\mathfrak{p}^l)} \phi\Big(a\gamma_{\mathfrak{p}^l}(A[\mathbf{z}] + \mathbf{w}^T\mathbf{z})\Big)\right| \leq \mathrm{N}\,\mathfrak{p}^{l(s-1/2)}.$$

Wegen $\mathrm{N}\,\mathfrak{p} > 5$ folgt daraus

$$\chi_{\mathfrak{p}} \geq \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_{\mathfrak{p}}(\eta)} \left(1 - \sum_{l=1}^{\infty} \mathrm{N}\,\mathfrak{p}^{-l/2}\right) \geq \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_{\mathfrak{p}}(\eta)} \left(1 - \frac{1}{\mathrm{N}\,\mathfrak{p}^{1/2}-1}\right) \geq \mathrm{N}\,\mathfrak{p}.$$

Wenn hingegen mindestens $s-2$ Diagonaleinträge durch $\mathfrak{p}$ teilbar sind, gilt

$$\mathrm{v}_{\mathfrak{p}}(A\boldsymbol{\xi}) \leq \mathrm{v}_{\mathfrak{p}}(\Delta) + \mathrm{v}_{\mathfrak{p}}(\boldsymbol{\xi}) - s + 3,$$

sodass aus Lemma 3.20 die untere Schranke

$$\chi_{\mathfrak{p}} \geq \mathrm{N}\,\mathfrak{p}^{s\,\mathrm{v}_{\mathfrak{p}}(\eta) - (\mathrm{v}_{\mathfrak{p}}(2A\boldsymbol{\xi})+1)(s-1)} \geq \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\eta) + (\mathrm{v}_{\mathfrak{p}}(\eta) - \mathrm{v}_{\mathfrak{p}}(2\Delta\boldsymbol{\xi}))(s-1)}$$

folgt. Wegen $\mathrm{v}_{\mathfrak{p}}(\eta) \leq \mathrm{v}_{\mathfrak{p}}(2A\boldsymbol{\xi}) \leq \mathrm{v}_{\mathfrak{p}}(2\Delta\boldsymbol{\xi})$ haben wir damit den ersten Teil der Behauptung gezeigt.

Im Fall von $\mathfrak{p} \mid 30$ können wir aus $\mathrm{v}_{\mathfrak{p}}(A\boldsymbol{\xi}) \leq \mathrm{v}_{\mathfrak{p}}(\Delta) + \mathrm{v}_{\mathfrak{p}}(\boldsymbol{\xi})$ analog

$$\chi_{\mathfrak{p}} \gg \mathrm{N}\,\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\eta) + (\mathrm{v}_{\mathfrak{p}}(\eta) - \mathrm{v}_{\mathfrak{p}}(\Delta\boldsymbol{\xi}))(s-1)}$$

schließen. □

Das nächste Lemma fasst die in diesem Abschnitt bewiesenen Resultate zusammen und liefert die benötigte untere Schranke für die singuläre Reihe.

Lemma 3.22. *Sei*

$$K_s = \begin{cases} (\log\log 3|\mathrm{Nm}\,\kappa|)^{-d}, & s = 4, \\ 1, & s \geq 5. \end{cases}$$

Es gilt

$$\mathfrak{S} \gg \frac{K_s |\mathrm{Nm}\,\eta|^s}{\mathrm{N}((\eta \cap \Delta)(\boldsymbol{\xi}))^{s-1}}.$$

3.6 Die asymptotische Formel

Nachdem wir in den letzten vier Abschnitten die Fourierintegrale und die Exponentialsummen eingehend untersucht haben, werden wir diese Ergebnisse nun dazu nutzen, eine asymptotische Formel für die Anzahl der Lösungen von (2.4) herzuleiten. Der gesamte Abschnitt basiert auf der Arbeit von Browning und Vishe [BV14].

Doch bevor wir damit beginnen können, benötigen wir noch das folgende technische Lemma, dessen Ideen sämtlich von Browning und Vishe [BV14] stammen.

Lemma 3.23. *Seien $N, K \in \mathbb{R}_{>0}$ mit $N > ds$ und sei*

$$M = \bigoplus_l M^{(l)} \in \bigoplus_l \mathbb{R}_{>0}.$$

Für jedes ganze Ideal $\mathfrak{q}$ gilt

$$\sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{q}}^s \\ |\mathbf{m}^{(l)}|_\infty \ll M^{(l)}}} 1 \ll \mathrm{N}\,\mathfrak{q}^s \,\mathrm{Nm}\, M^s$$

und

$$\sum_{\substack{\mathbf{m}\in\widehat{\mathfrak{q}}^s \\ \langle\mathbf{m}\rangle > K}} \langle M\mathbf{m}\rangle^{-N} \ll \mathrm{N}\,\mathfrak{q}^s K^{ds-N} \,\mathrm{Nm}\, M^{-s}.$$

Beweis. Wegen Lemma 2.1(ii) gibt es ein Primideal $\mathfrak{p}$ mit $\mathrm{N}\,\mathfrak{p} \ll 1$, sodass $\mathfrak{q}\mathfrak{d}\mathfrak{p} = (\alpha)$ für ein $\alpha \in \mathcal{O}$ erfüllt ist. Daraus folgt

$$|\mathrm{Nm}\,\alpha| \asymp \mathrm{N}\,\mathfrak{q}, \qquad\qquad \widehat{\mathfrak{q}} = (\mathfrak{q}\mathfrak{d})^{-1} = \alpha^{-1}\mathfrak{p}.$$

Also ist

$$\sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{q}}^s \\ |\mathbf{m}^{(l)}|_\infty \ll M^{(l)}}} 1 = \sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\mathfrak{p}^s \\ |\mathbf{m}^{(l)}|_\infty \ll |\alpha^{(l)}| M^{(l)}}} 1 \ll \Bigg(\sum_{\substack{m\in\mathcal{O} \\ |m^{(l)}| \ll |\alpha^{(l)}| M^{(l)}}} 1 \Bigg)^s \ll \mathrm{N}\,\mathfrak{q}^s \,\mathrm{Nm}\, M^s.$$

Ebenso gilt

$$\begin{aligned}\sum_{\substack{\mathbf{m}\in\widehat{\mathfrak{q}}^s\\ \langle\mathbf{m}\rangle>K}} \langle M\mathbf{m}\rangle^{-N} &\ll \langle\alpha\rangle^N \sum_{\substack{\mathbf{m}\in\mathcal{O}^s\\ \langle\mathbf{m}\rangle>\langle\alpha\rangle K}} \langle M\mathbf{m}\rangle^{-N}\\ &\ll \langle\alpha\rangle^N \sum_{j\geq\langle\alpha\rangle K} \#\{\mathbf{m}\in\mathcal{O}^s : j\leq\langle M\mathbf{m}\rangle<j+1\}j^{-N}\\ &\ll \langle\alpha\rangle^N \sum_{j\geq\langle\alpha\rangle K} \frac{j^{ds-1}}{\operatorname{Nm} M^s}j^{-N}\\ &\ll \operatorname{N}\mathfrak{q}^s K^{ds-N}\operatorname{Nm} M^{-s}.\end{aligned}$$

□

Der Startpunkt für die asymptotische Formel ist Lemma 3.1. Als Erstes werden wir zeigen, dass in der dortigen Summation alle Terme mit $\mathbf{m}\neq\mathbf{0}$ lediglich zum Fehlerterm beitragen. Dazu beweisen wir ein Analogon zu Lemma 6.6 von Browning und Vishe [BV14].

Lemma 3.24. *Es gelte* $\operatorname{Nm} P\geq\operatorname{Nm} d_{max}^{1/2}$. *Weiterhin sei*

$$Q_0=\frac{\operatorname{Nm} P}{|\operatorname{Nm}\eta d_{max}^{1/2}|\,\langle P\rangle^{\varepsilon}\,\mathscr{H}(v)},\qquad Q_1=\frac{\operatorname{Nm} P\,\langle P\rangle^{\varepsilon}}{\mathscr{H}(v)}.$$

Dann gilt

$$\operatorname{Nm} P^{-2}\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \operatorname{N}\mathfrak{b}\ll\operatorname{Nm} P}}\sum_{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^s}\frac{S_{\mathfrak{b}}(\mathbf{m})I_{\mathfrak{b}}(\mathbf{m})}{\operatorname{N}(\mathfrak{b}\cap\eta)^s}\ll 1+\frac{\langle P\rangle^{\varepsilon}\operatorname{Nm} P^{s-2}}{|\operatorname{Nm}\Delta|^{1/2}}\int_R E(v,P)\,\mathrm{d}v$$

mit $R=\{v\in V:\mathscr{H}(v)\ll\operatorname{Nm} P\langle P\rangle^{\varepsilon}\}$ *und*

$$E(v,P)=\mathscr{H}(v)^{-s/2}\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ Q_0\ll\operatorname{N}\mathfrak{b}\ll Q_1}}\sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^s\\ |\mathbf{m}^{(l)}|_\infty\ll B^{(l)}(v^{(l)})}}\frac{|S_{\mathfrak{b}}(\mathbf{m})|}{\operatorname{N}(\mathfrak{b}\cap\eta)^s}.$$

Beweis. Zum Abschätzen der Exponentialsumme nutzen wir in diesem Beweis Lemma 3.16 und erhalten so

$$S_{\mathfrak{b}}(\mathbf{m})\ll|\operatorname{Nm}\Delta|^{1/2}\operatorname{N}\mathfrak{b}^{s/2+1+\varepsilon}.$$

Des Weiteren werden wir in diesem Beweis mehrfach das eben bewiesene Lemma verwenden, ohne dies jedes Mal explizit zu erwähnen.

Bei den Termen mit großem $\mathbf{m}$ nutzen wir Lemma 3.2 mit $N = ds+1$, um die Fourierintegrale abzuschätzen. Unter Zuhilfenahme des vorhergehenden Lemmas folgt, dass für $\lambda > 0$ stets

$$\begin{aligned}
&\operatorname{Nm} P^{-2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \sum_{\substack{\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}\\ \langle\mathbf{m}\rangle>\operatorname{Nm} P^{\lambda}}} \frac{S_{\mathfrak{b}}(\mathbf{m})I_{\mathfrak{b}}(\mathbf{m})}{\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\\
&\ll \operatorname{Nm} P^{s(d+1)}\mathfrak{L}^{2ds+2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \frac{\mathrm{N}\,\mathfrak{b}^{s(1/2-d)}}{\mathrm{N}(\mathfrak{b}\cap\eta)^{s}} \sum_{\substack{\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}\\ \langle\mathbf{m}\rangle>\operatorname{Nm} P^{\lambda}}} \left\langle \frac{P\mathbf{m}}{d_{\max}^{1/2}} \right\rangle^{-ds-1}\\
&\ll \operatorname{Nm} P^{-\lambda+ds}\mathfrak{L}^{2ds+2} \operatorname{Nm} d_{\max}^{s/2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \mathrm{N}\,\mathfrak{b}^{s(1/2-d)}
\end{aligned}$$

gilt. Wir können λ so groß wählen, dass dies in $O(1)$ liegt.

Wenn $\mathbf{m}$ klein ist, nutzen wir für die Fourierintegrale Lemma 3.5 und erhalten

$$\begin{aligned}
&\operatorname{Nm} P^{-2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}\\ \langle\mathbf{m}\rangle\leq\operatorname{Nm} P^{\lambda}}} \frac{S_{\mathfrak{b}}(\mathbf{m})I_{\mathfrak{b}}(\mathbf{m})}{\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\\
&\ll 1 + \frac{\langle P\rangle^{\varepsilon}\operatorname{Nm} P^{s-2}}{|\operatorname{Nm}\Delta|^{1/2}} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \int_{V} \sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}\\ \langle\mathbf{m}\rangle\leq\operatorname{Nm} P^{\lambda}\\ |\mathbf{m}^{(l)}|_{\infty}\ll B^{(l)}(v^{(l)})}} \frac{|p_{\rho}(v)S_{\mathfrak{b}}(\mathbf{m})|}{\mathscr{H}(v)^{s/2}\,\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\,\mathrm{d}v.
\end{aligned}$$

Sei $R_\rho = \{v \in V : \mathscr{H}(v) \ll \rho^{-1}\langle P\rangle^{\varepsilon}\}$. Der Beitrag von $v \in V \setminus R_\rho$ zum obigen Integral ist wegen (3.4) für jedes j kleiner als

$$\begin{aligned}
&\ll \langle P\rangle^{\varepsilon}\operatorname{Nm} P^{sd\lambda+s-2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \mathrm{N}\,\mathfrak{b}^{s/2+1+\varepsilon} \int_{V\setminus R_\rho} \frac{|p_\rho(v)|}{\mathscr{H}(v)^{s/2}}\,\mathrm{d}v\\
&\ll_j \langle P\rangle^{(2-j)\varepsilon/2}\operatorname{Nm} P^{sd\lambda+s-1} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \mathrm{N}\,\mathfrak{b}^{s/2+\varepsilon} \int_{V\setminus R_\rho} \mathscr{H}(v)^{-s/2}\,\mathrm{d}v.
\end{aligned}$$

Aus (2.1) folgt, dass dieses Integral durch eine Konstante beschränkt werden kann. Deswegen können wir ein nur vom Körper K und ε abhängiges j so wählen, dass der gesamte Ausdruck in $O(1)$ liegt.

Damit haben wir bereits

$$\begin{aligned}&\operatorname{Nm} P^{-2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \sum_{\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}} \frac{S_{\mathfrak{b}}(\mathbf{m})I_{\mathfrak{b}}(\mathbf{m})}{\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\\ &\ll 1+\frac{\langle P\rangle^{\varepsilon}\operatorname{Nm} P^{s-2}}{|\operatorname{Nm}\Delta|^{1/2}} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}} \int_{R_\rho} \sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}\\ |\mathbf{m}^{(l)}|_\infty\ll B^{(l)}(v^{(l)})}} \frac{|p_\rho(v)S_{\mathfrak{b}}(\mathbf{m})|}{\mathscr{H}(v)^{s/2}\,\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\,\mathrm{d}v\end{aligned}$$

gezeigt. Im Rest des Beweises leiten wir lediglich noch Einschränkungen an die Summation über $\mathfrak{b}$ her.

Aus $v\in R_\rho$ folgt

$$\mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P\,\langle P\rangle^{\varepsilon}\,\mathscr{H}(v)^{-1}=Q_1.$$

Erfülle $\mathbf{m}$ die obigen Summationsbedingungen und o. B. d. A. sei $m_1\neq 0$. Dann gilt

$$0<|\operatorname{Nm} m_1|\ll\operatorname{Nm}(d_{\max}^{1/2}P^{-1})\,\langle P\rangle^{\varepsilon}\,\mathscr{H}(v)$$

und $m_1\in(\mathfrak{b}\cap\eta)^{-1}\mathfrak{d}^{-1}$. Also ist $m_1(\mathfrak{b}\cap\eta)\mathfrak{d}$ ein ganzes Ideal und somit gilt $|\operatorname{Nm} m_1|\,\mathrm{N}(\mathfrak{b}\cap\eta)\gg 1$. Folglich gilt

$$\mathrm{N}\,\mathfrak{b}\gg\frac{\mathrm{N}(\mathfrak{b}\cap\eta)}{|\operatorname{Nm}\eta|}\gg\frac{\operatorname{Nm} P}{|\operatorname{Nm}(\eta d_{\max}^{1/2})|\,\langle P\rangle^{\varepsilon}\,\mathscr{H}(v)}=Q_0.$$

Wegen $R_\rho\subseteq R=\{v\in V:\mathscr{H}(v)\ll\operatorname{Nm} P\,\langle P\rangle^{\varepsilon}\}$ können wir aus (3.5) die Abschätzung

$$\operatorname{Nm} P^{-2}\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}}\sum_{\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}}\frac{S_{\mathfrak{b}}(\mathbf{m})I_{\mathfrak{b}}(\mathbf{m})}{\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\ll 1+\frac{\langle P\rangle^{\varepsilon}\operatorname{Nm} P^{s-2}}{|\operatorname{Nm}\Delta|^{1/2}}\int_R E(v,P)\,\mathrm{d}v$$

folgern. Damit ist die Behauptung gezeigt. □

Das Integral im letzten Lemma können wir wie in §8 von Browning und Vishe [BV14] abhandeln.

Lemma 3.25. *Aus* $\operatorname{Nm} P\geq\operatorname{Nm} d_{max}^{1/2}$ *folgt*

$$\begin{aligned}&\operatorname{Nm} P^{-2}\sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ \mathrm{N}\,\mathfrak{b}\ll\operatorname{Nm} P}}\sum_{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{s}}\frac{S_{\mathfrak{b}}(\mathbf{m})I_{\mathfrak{b}}(\mathbf{m})}{\mathrm{N}(\mathfrak{b}\cap\eta)^{s}}\\ &\ll\begin{cases}\operatorname{Nm} d_{max}^{s/2}|\operatorname{Nm}\kappa|^{\varepsilon}\,\langle P\rangle^{\varepsilon}\operatorname{Nm} P^{(s-1)/2+\varepsilon}, & \kappa\neq 0,\\ \operatorname{Nm} d_{max}^{s/2}\,\langle P\rangle^{\varepsilon}\operatorname{Nm} P^{s/2+\varepsilon}, & \kappa=0.\end{cases}\end{aligned}$$

Beweis. Sei $E(v,P)$ wie im vorherigen Lemma definiert. Mithilfe der Abschätzung aus Lemma 3.16 und unter Verwendung von Lemma 3.23 können wir

$$\begin{aligned} E(v,P) &= \mathscr{H}(v)^{-s/2} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ Q_0\ll \mathrm{N}\,\mathfrak{b}\ll Q_1}} \sum_{\substack{\mathbf{0}\neq\mathbf{m}\in\widehat{\mathfrak{b}\cap\eta}^{\,s}\\ |\mathbf{m}^{(l)}|_\infty\ll B^{(l)}(v^{(l)})}} \frac{|S_{\mathfrak{b}}(\mathbf{m})|}{\mathrm{N}(\mathfrak{b}\cap\eta)^s} \\ &\ll \frac{|\mathrm{Nm}\,\Delta|^{1/2}}{\mathscr{H}(v)^{s/2}} \sum_{\substack{(0)\neq\mathfrak{b}\subseteq\mathcal{O}\\ Q_0\ll \mathrm{N}\,\mathfrak{b}\ll Q_1}} \mathrm{Nm}\,B^s\,\mathrm{N}\,\mathfrak{b}^{(s+1)/2+\varepsilon}\,\mathrm{N}\,\mathfrak{b}_2^{1/2}\,\mathrm{N}(\mathfrak{b}_1,\kappa)^{1/2} \\ &\ll \frac{|\mathrm{Nm}\,\Delta d_{\max}^s|^{1/2}\mathscr{H}(v)^{s/2}\langle P\rangle^{\varepsilon}}{\mathrm{Nm}\,P^s} \max_{Q_0\ll M_1M_2\ll Q_1} \Sigma_1\Sigma_2 \end{aligned}$$

mit

$$\begin{aligned} \Sigma_1 &= \sum_{\substack{(0)\neq\mathfrak{b}_1\subseteq\mathcal{O}\\ M_1\leq \mathrm{N}\,\mathfrak{b}_1<2M_1}} \mathrm{N}\,\mathfrak{b}_1^{(s+1)/2+\varepsilon}\,\mathrm{N}(\mathfrak{b}_1,\kappa)^{1/2}, \\ \Sigma_2 &= \sum_{\substack{(0)\neq\mathfrak{b}_2\subseteq\mathcal{O}\\ M_2\leq \mathrm{N}\,\mathfrak{b}_2<2M_2}} \mathrm{N}\,\mathfrak{b}_2^{s/2+1+\varepsilon} \end{aligned}$$

folgern. Dies impliziert

$$\begin{aligned} &\frac{\langle P\rangle^{\varepsilon}\,\mathrm{Nm}\,P^{s-2}}{|\mathrm{Nm}\,\Delta|^{1/2}} \int_R E(v,P)\,\mathrm{d}v \\ &\ll \frac{\mathrm{Nm}\,d_{\max}^{s/2}\langle P\rangle^{2\varepsilon}}{\mathrm{Nm}\,P^2} \int_R \mathscr{H}(v)^{s/2} \max_{Q_0\ll M_1M_2\ll Q_1} \Sigma_1\Sigma_2\,\mathrm{d}v. \end{aligned}$$

Um den Beweis abzuschließen reicht es aufgrund des vorhergehenden Lemmas aus, diesen Ausdruck abzuschätzen. Einerseits gilt wie bei (3.17), dass

$$\Sigma_1 \ll M_1^{(s+1)/2+\varepsilon} \sum_{\substack{(0)\neq\mathfrak{b}_1\subseteq\mathcal{O}\\ M_1\leq \mathrm{N}\,\mathfrak{b}_1<2M_1}} \mathrm{N}(\mathfrak{b}_1,\kappa)^{1/2} \ll \begin{cases} M_1^{(s+3)/2+\varepsilon}|\mathrm{Nm}\,\kappa|^{\varepsilon}, & \kappa\neq 0, \\ M_1^{s/2+2+\varepsilon}, & \kappa = 0, \end{cases}$$

und andererseits gilt, dass

$$\Sigma_2 \ll M_2^{s/2+1+\varepsilon} \sum_{\substack{(0)\neq\mathfrak{b}_2\subseteq\mathcal{O}\\ M_2\leq \mathrm{N}\,\mathfrak{b}_2<2M_2}} 1 \ll M_2^{s/2+1+\varepsilon}(\log_2 2M_2)^d \ll M_2^{s/2+1+2\varepsilon}.$$

Also erhalten wir

$$\max_{Q_0\ll M_1M_2\ll Q_1} \Sigma_1\Sigma_2 \ll \begin{cases} Q_1^{(s+3)/2+\varepsilon}|\mathrm{Nm}\,\kappa|^{\varepsilon}, & \kappa\neq 0, \\ Q_1^{s/2+2+\varepsilon}, & \kappa = 0 \end{cases}$$

und damit folgt mithilfe von (2.1) die Behauptung. □

Nun können wir wie in §8.3 von Browning und Vishe [BV14] die asymptotische Formel beweisen.

Lemma 3.26. *Wenn* $\operatorname{Nm} P \geq \operatorname{Nm} d_{max}$ *erfüllt ist, gilt*

$$N(P) = \frac{c_P 2^{r_2(s-1)} \operatorname{Nm} P^{s-2}}{D_K^{(s-1)/2} |\operatorname{Nm} \Delta \eta^{2s}|^{1/2}} \mathfrak{I}(0)\mathfrak{S} + \begin{cases} O\left(\operatorname{Nm} d_{max}^{s/2} |\operatorname{Nm} \kappa|^{\varepsilon} \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{(s-1)/2+\varepsilon}\right), & \kappa \neq 0, \\ O\left(\operatorname{Nm} d_{max}^{s/2} \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{s/2+\varepsilon}\right), & \kappa = 0. \end{cases}$$

Beweis. Wir nutzen Lemma 3.6 dazu, die Fourierintegrale durch das singuläre Integral zu ersetzen. Für beliebige $N \geq 1$ gilt

$$\begin{aligned} &\frac{c_P 2^{r_2 s}}{D_K^{s/2} \operatorname{Nm} P^2} \sum_{\substack{(0) \neq \mathfrak{b} \subseteq \mathcal{O} \\ \mathrm{N}\,\mathfrak{b} \ll \operatorname{Nm} P}} \frac{S_{\mathfrak{b}}(\mathbf{0}) I_{\mathfrak{b}}(\mathbf{0})}{\mathrm{N}(\mathfrak{b} \cap \eta)^s} \\ &= \frac{c_P 2^{r_2(s-1)} \operatorname{Nm} P^{s-2}}{D_K^{(s-1)/2} |\operatorname{Nm} \Delta|^{1/2}} \mathfrak{I}(0) \sum_{\substack{(0) \neq \mathfrak{b} \subseteq \mathcal{O} \\ \mathrm{N}\,\mathfrak{b} \ll \operatorname{Nm} P}} \frac{S_{\mathfrak{b}}(\mathbf{0})}{\mathrm{N}(\mathfrak{b} \cap \eta)^s} \\ &\quad + O\left(\frac{\langle P \rangle^{\varepsilon} \operatorname{Nm} P^{s-2+\varepsilon}}{|\operatorname{Nm} \Delta|^{1/2}} \sum_{\substack{(0) \neq \mathfrak{b} \subseteq \mathcal{O} \\ \mathrm{N}\,\mathfrak{b} \ll \operatorname{Nm} P}} \frac{\rho^N |S_{\mathfrak{b}}(\mathbf{0})|}{\mathrm{N}(\mathfrak{b} \cap \eta)^s} \right). \end{aligned}$$

Sobald N genügend groß ist, können wir die Summation über $\mathfrak{b}$ im Fehlerterm auf die gleiche Art wie zuvor abhandeln. Der Fehlerterm ist kleiner als

$$\begin{aligned} &\ll \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{s-2-N+\varepsilon} \sum_{\substack{(0) \neq \mathfrak{b} \subseteq \mathcal{O} \\ \mathrm{N}\,\mathfrak{b} \ll \operatorname{Nm} P}} \mathrm{N}\,\mathfrak{b}^{(-s+1)/2+N+\varepsilon} \mathrm{N}\,\mathfrak{b}_2^{1/2} \mathrm{N}(\mathfrak{b}_1, \kappa)^{1/2} \\ &\ll \begin{cases} |\operatorname{Nm} \kappa|^{\varepsilon} \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{(s-1)/2+\varepsilon}, & \kappa \neq 0, \\ \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{s/2+\varepsilon}, & \kappa = 0. \end{cases} \end{aligned}$$

Des Weiteren erhalten wir mithilfe des Lemmas 3.17 die singuläre Reihe. Es gilt

$$\begin{aligned} &\frac{c_P 2^{r_2(s-1)} \operatorname{Nm} P^{s-2}}{D_K^{(s-1)/2} |\operatorname{Nm} \Delta|^{1/2}} \mathfrak{I}(0) \sum_{\substack{(0) \neq \mathfrak{b} \subseteq \mathcal{O} \\ \mathrm{N}\,\mathfrak{b} \ll \operatorname{Nm} P}} \frac{S_{\mathfrak{b}}(\mathbf{0})}{\mathrm{N}(\mathfrak{b} \cap \eta)^s} \\ &= \frac{c_P 2^{r_2(s-1)} \operatorname{Nm} P^{s-2}}{D_K^{(s-1)/2} |\operatorname{Nm} \Delta \eta^{2s}|^{1/2}} \mathfrak{I}(0)\mathfrak{S} + \begin{cases} O\left(|\operatorname{Nm} \kappa|^{\varepsilon} \operatorname{Nm} P^{(s-1)/2+\varepsilon}\right), & \kappa \neq 0, \\ O\left(\operatorname{Nm} P^{s/2+\varepsilon}\right), & \kappa = 0. \end{cases} \end{aligned}$$

Da wir alle Terme mit $\mathbf{m} \neq \mathbf{0}$ bereits in Lemma 3.25 abgehandelt haben, folgt die Behauptung aus Lemma 3.1. □

Mithilfe dieser asymptotischen Formel können wir Proposition 2 beweisen und dadurch den Beweis von Proposition 1 in dem Fall vervollständigen, dass $s \geq 5$ oder sowohl $s = 4$ als auch $\kappa \neq 0$ gilt.

Beweis von Proposition 2. Wegen $A[\boldsymbol{\xi}] = \kappa$ und aufgrund der Voraussetzungen an P existiert ein $\mathbf{h} \in V$, sodass (3.7) erfüllt ist. Da ansonsten nichts zu beweisen wäre, können wir außerdem $\operatorname{Nm} P \geq \operatorname{Nm} d_{\max}$ annehmen. Also folgt aus dem vorhergehenden Lemma

$$N(P) = \frac{c_P 2^{r_2(s-1)} \operatorname{Nm} P^{s-2}}{D_K^{(s-1)/2} |\operatorname{Nm} \Delta \eta^{2s}|^{1/2}} \mathfrak{J}(0)\mathfrak{S} + \begin{cases} O\left(\operatorname{Nm} d_{\max}^{s/2} \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{(s-1)/2+\varepsilon}\right), & \kappa \neq 0, \\ O\left(\operatorname{Nm} d_{\max}^{s/2} \langle P \rangle^{\varepsilon} \operatorname{Nm} P^{s/2+\varepsilon}\right), & \kappa = 0. \end{cases}$$

Den Hauptterm können wir mithilfe der unteren Schranke für das singuläre Integral aus Lemma 3.7 und der für die singuläre Reihe aus Lemma 3.22 nach unten abschätzen. Es gilt

$$\frac{c_P 2^{r_2(s-1)} \operatorname{Nm} P^{s-2}}{D_K^{(s-1)/2} |\operatorname{Nm} \Delta \eta^{2s}|^{1/2}} \mathfrak{J}(0)\mathfrak{S} \gg \frac{\operatorname{Nm} P^{s-2-\varepsilon}}{|\operatorname{Nm} \Delta|^{1/2} \operatorname{N}((\eta \cap \Delta)(\boldsymbol{\xi}))^{s-1}}.$$

Deswegen folgt aus

$$\frac{\operatorname{Nm} P}{\langle P \rangle^{\varepsilon}} \gg \begin{cases} \operatorname{N}\left(d_{\max}^{s} \Delta (\eta \cap \Delta)^{2(s-1)} (\boldsymbol{\xi})^{2(s-1)}\right)^{1/(s-3)}, & \kappa \neq 0, \\ \operatorname{N}\left(d_{\max}^{s} \Delta (\eta \cap \Delta)^{2(s-1)} (\boldsymbol{\xi})^{2(s-1)}\right)^{1/(s-4)}, & \kappa = 0, \end{cases}$$

dass $N(P) > 0$ gilt und somit dass eine Lösung $\mathbf{x}$ mit $W(\mathbf{x}/P) \neq 0$ existiert. Diese erfüllt

$$\left|\operatorname{diag}\left(|d_1^{(l)}|^{1/2}, \ldots, |d_s^{(l)}|^{1/2}\right) R^{H(l)} \mathbf{x}^{(l)}\right| \leq P^{(l)}, \qquad l = 1, \ldots, r_1 + r_2$$

und damit ist die Behauptung gezeigt. □

4 Raghavans Lemma mit Kongruenzbedingung

Dietmann [Die03] modifiziert in seinem dritten Kapitel ein Lemma von Cassels [Cas55], welches eine Suchschranke für die Lösung einer quadratischen Form mit ganzzahligen Koeffizienten liefert, derart, dass die kleinste Lösung zusätzlich einer Kongruenzbedingung genügt. Auf diesem Weg beweist er seine Version von Proposition 1 im Fall $3 \leq s \leq 4$ und $\kappa = 0$. Da Raghavan [Rag75] das Lemma von Cassels bereits auf algebraische Zahlkörper verallgemeinert hat, werden wir analog zu Dietmanns Vorgehen Raghavans Lemma eine Kongruenzbedingung hinzufügen.

Aus technischen Gründen werden wir dazu als Zwischenschritt die folgende, Proposition 3 von Dietmann [Die03] verallgemeinernde, Proposition beweisen.

Proposition 3. *Sei $3 \leq s \leq 4$ und $\boldsymbol{\xi} \in \mathcal{O}^s$. Weiterhin sei $\mathfrak{b} \subset \mathcal{O}$ ein zu $(\boldsymbol{\xi})$ teilerfremdes Ideal. Wenn*

$$A[\mathbf{x}] = 0, \qquad \mathbf{x} \equiv \boldsymbol{\xi} \pmod{\mathfrak{b}}$$

für eine symmetrische und nichtsinguläre Matrix $A \in \mathcal{O}^{s \times s}$ im Ganzheitsring lösbar ist, gibt es ein $\mathbf{y} \in \mathcal{O}^s$ und ein zu $\mathfrak{b}$ teilerfremdes $m \in \mathcal{O}$ mit

$$A[\mathbf{y}] = 0, \qquad \mathbf{y} \equiv m\boldsymbol{\xi} \pmod{\mathfrak{b}} \tag{4.1}$$

und

$$\langle \mathbf{y} \rangle \ll \begin{cases} \langle A \rangle^2 \, \mathrm{N}\, \mathfrak{b}^{2/d+\varepsilon} |\mathrm{Nm}\, \Delta|^{2/d}, & s = 3, \\ \langle A \rangle^5 \, \mathrm{N}\, \mathfrak{b}^{8/d+\varepsilon} |\mathrm{Nm}\, \Delta|^{4/d} + \langle A \rangle^8 \, \mathrm{N}\, \mathfrak{b}^{19/d+\varepsilon}, & s = 4. \end{cases}$$

Bevor wir diese Proposition beweisen, werden wir aus ihr Proposition 1 im Fall $3 \leq s \leq 4$ und $\kappa = 0$ folgern.

Teilbeweis von Proposition 1. Es sei $\mathfrak{b} = \eta/(\boldsymbol{\xi}, \eta)$. Lemma 2.1(iii) ermöglicht es uns, ein zu η teilerfremdes $u \in \mathcal{O} \setminus \{0\}$ und ein $v \in (\boldsymbol{\xi}, \eta)$ mit

$$\langle v/\Delta \rangle \ll \frac{\mathrm{N}(\boldsymbol{\xi}, \eta)^{1/d}}{|\mathrm{Nm}\, \Delta|^{1/d}} |\mathrm{Nm}\, \eta|^{\varepsilon}, \qquad \boldsymbol{\xi}' = uv^{-1}\boldsymbol{\xi} \in \mathcal{O}^s, \qquad (\boldsymbol{\xi}', \mathfrak{b}) = \mathcal{O}$$

zu finden. Aus der obigen Proposition folgt die Existenz von $\mathbf{y}' \in \mathcal{O}^s$ und einem zu $\mathfrak{b}$ teilerfremden $m \in \mathcal{O}$ mit

$$A[\mathbf{y}'] = 0, \qquad \mathbf{y}' \equiv m\boldsymbol{\xi}' \quad (\mathfrak{b})$$

und

$$\langle \mathbf{y}' \rangle \ll \begin{cases} \langle A \rangle^2 \, \mathrm{N}\, \mathfrak{b}^{2/d+\varepsilon} |\mathrm{Nm}\, \Delta|^{2/d}, & s = 3, \\ \langle A \rangle^5 \, \mathrm{N}\, \mathfrak{b}^{8/d+\varepsilon} |\mathrm{Nm}\, \Delta|^{4/d} + \langle A \rangle^8 \, \mathrm{N}\, \mathfrak{b}^{19/d+\varepsilon}, & s = 4. \end{cases}$$

Wegen Lemma 2.2 finden wir ein $\bar{m} \in \mathcal{O}$ mit

$$\bar{m}mu \equiv 1 \quad (\mathfrak{b}), \qquad \langle \bar{m} \rangle \ll \mathrm{N}\, \mathfrak{b}^{1/d}.$$

Wenn wir $\mathbf{y} = v\bar{m}\mathbf{y}'$ setzen, gilt $A[\mathbf{y}] = 0$ und

$$\mathbf{y} \equiv v\bar{m}m\boldsymbol{\xi}' \equiv \bar{m}mu\boldsymbol{\xi} \equiv \boldsymbol{\xi} \quad (\eta).$$

Da u und η teilerfremd sind, ist $\mathbf{y}$ eine Lösung von (2.4), die

$$\begin{aligned} \left\langle \frac{\mathbf{y}}{\Delta} \right\rangle &\ll \frac{|\mathrm{Nm}\, \eta|^{1/d+\varepsilon}}{|\mathrm{Nm}\, \Delta|^{1/d}} \langle \mathbf{y}' \rangle \\ &\ll \begin{cases} \langle A \rangle^2 \, |\mathrm{Nm}\, \eta^3 \Delta|^{1/d+2\varepsilon}, & s = 3, \\ \langle A \rangle^5 \, |\mathrm{Nm}\, \eta^9 \Delta^3|^{1/d+2\varepsilon} + \langle A \rangle^8 \, |\mathrm{Nm}\, \eta|^{20/d+2\varepsilon} |\mathrm{Nm}\, \Delta|^{-1/d}, & s = 4 \end{cases} \end{aligned}$$

erfüllt. Damit ist dieser Teil der Behauptung gezeigt. □

Im Rest dieses Kapitels werden wir uns nur noch mit dem Beweis von Proposition 3 beschäftigen. Dabei gelte $3 \le s \le 4$ und $\boldsymbol{\xi} \in \mathcal{O}^s$. Außerdem bezeichne $\mathfrak{b}$ stets ein ganzes Ideal.

4.1 Konstruktion einer kleinen Lösung

In diesem Abschnitt werden wir aus einer Lösung $\mathbf{a} \in \mathcal{O}^s \setminus \{\mathbf{0}\}$ von (4.1), deren Existenz wir ab jetzt voraussetzen, eine weitere möglichst kleine Lösung konstruieren. Dazu modifizieren wir das Argument aus §3 von Dietmann [Die03] mit Ideen von Raghavan [Rag75]. Wie bei Raghavan sei $L(l)$ so gewählt, dass

$$|a_{L(l)}^{(l)}| = \max_{1 \le i \le s} |a_i^{(l)}|$$

für alle l erfüllt ist.

Das folgende Lemma ist unsere Alternative zu den Lemmata 19 und 20 von Dietmann [Die03], die auf Ideen aus §2 von Raghavan [Rag75] basiert.

Lemma 4.1. *Sei* $\mathbf{z} \in \mathcal{O}^s$. *Wenn* $A[\mathbf{z}] \neq 0$ *gilt, gibt es ein* $\mathbf{b} \in \mathcal{O}^s \setminus \{\mathbf{0}\}$ *mit* $A[\mathbf{b}] = 0$ *und*

$$\langle \mathbf{b} \rangle \ll \max_{l=1,\dots,d} \left| \mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right|^2 \langle A \rangle \langle \mathbf{a} \rangle .$$

Beweis. Der Vektor

$$\mathbf{b} = A[\mathbf{z}]\mathbf{a} - 2(\mathbf{a}^T A\mathbf{z})\mathbf{z}$$

erfüllt $A[\mathbf{b}] = 0$ und wegen

$$A[\mathbf{z}]\mathbf{b} - 2(\mathbf{b}^T A\mathbf{z})\mathbf{z} = A[\mathbf{z}]^2\mathbf{a} \neq \mathbf{0}$$

gilt $\mathbf{b} \neq \mathbf{0}$.

Für alle $l = 1, \dots, d$ und alle $i, j = 1, \dots, s$ gilt sowohl

$$\begin{aligned} |a_i^{(l)}\mathbf{z}^{(l)} - z_i^{(l)}\mathbf{a}^{(l)}| &= |a_i^{(l)} \left(\mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right) - \left(z_i^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} a_i^{(l)} \right) \mathbf{a}^{(l)}| \\ &\ll |a_{L(l)}^{(l)}| \left| \mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right| \end{aligned}$$

als auch

$$\begin{aligned} |a_i^{(l)} b_j^{(l)} + a_j^{(r)} b_i^{(l)}| &= 2|(a_i^{(l)}\mathbf{z}^{(l)} - z_i^{(l)}\mathbf{a}^{(l)})^T A^{(l)} (a_j^{(l)}\mathbf{z}^{(l)} - z_j^{(l)}\mathbf{a}^{(l)})| \\ &\ll |a_{L(l)}^{(l)}|^2 \left| \mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right|^2 \langle A \rangle , \end{aligned}$$

sodass wegen

$$\begin{aligned} |a_{L(l)}^{(l)} b_j^{(l)}| &\ll |a_{L(l)}^{(l)} b_j^{(l)} + a_j^{(r)} b_{L(l)}^{(l)}| + |a_{L(l)}^{(r)} b_{L(l)}^{(l)}| \\ &\ll |a_{L(l)}^{(l)}|^2 \left| \mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right|^2 \langle A \rangle \end{aligned}$$

die Behauptung folgt. □

Wie in §3.3 von Dietmann [Die03] können wir aus dem $\mathbf{b}$ des vorherigen Lemmas eine Lösung von (4.1) konstruieren.

Lemma 4.2. *Der Vektor* $\mathbf{z} \in \mathcal{O}^s$ *erfülle* $A[\mathbf{z}] \neq 0$. *Dann gibt es eine Lösung* $\mathbf{c} \in \mathcal{O}^s$ *von* (4.1) *mit*

$$\langle \mathbf{c} \rangle \ll \mathrm{N}\,\mathfrak{b}^{2/d+\varepsilon} \langle A \rangle^2 \prod_{\mathfrak{p}|\mathfrak{b}} \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_\mathfrak{p}(A[\mathbf{z}])/d} \max_{l=1,\dots,d} \left| \mathbf{z}^{(l)} - \frac{z^{(l)}_{L(l)}}{a^{(l)}_{L(l)}} \mathbf{a}^{(l)} \right|^2 \langle \mathbf{a} \rangle .$$

Beweis. Wegen Lemma 2.1(iii) gibt es $u \in \mathcal{O} \setminus \{0\}$ und $v \in \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{2\,\mathrm{v}_\mathfrak{p}(A[\mathbf{z}])}$ mit

$$\langle u \rangle \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}, \qquad \langle v \rangle \asymp |\mathrm{Nm}\, v|^{1/d} \ll \prod_{\mathfrak{p}|\mathfrak{b}} \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_\mathfrak{p}(A[\mathbf{z}])/d}\, \mathrm{N}\,\mathfrak{b}^{\varepsilon},$$

sodass $uv^{-1} \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{2\,\mathrm{v}_\mathfrak{p}(A[\mathbf{z}])}$ teilerfremd zu $\mathfrak{b}$ ist. Nun definieren wir ausgehend von dem $\mathbf{b}$ des vorherigen Lemmas und einem mit Lemma 2.2 gewähltem $\mathbf{z}' \equiv \mathbf{z}\ (v\mathfrak{b})$, das $\langle \mathbf{z}' \rangle \ll \mathrm{N}(v\mathfrak{b})^{1/d}$ erfüllt, den Vektor

$$\mathbf{c} = \frac{u}{v} \left(A[\mathbf{z}']\mathbf{b} - 2(\mathbf{z}'^T A \mathbf{b})\mathbf{z}' \right).$$

Es gilt $\mathbf{c} \equiv uv^{-1} A[\mathbf{z}]^2 \mathbf{a}\ (\mathfrak{b})$ und folglich insbesondere auch $\mathbf{c} \in \mathcal{O}^s$. Außerdem ist $uv^{-1}A[\mathbf{z}]^2$ teilerfremd zu $\mathfrak{b}$ und es gilt

$$\begin{aligned} \langle \mathbf{c} \rangle &\ll \frac{\mathrm{N}\,\mathfrak{b}^{\varepsilon}}{|\mathrm{Nm}\, v|^{1/d}} \langle A \rangle\, \mathrm{N}(v\mathfrak{b})^{2/d} \langle \mathbf{b} \rangle \\ &\ll \mathrm{N}\,\mathfrak{b}^{2/d+2\varepsilon} \langle A \rangle^2 \prod_{\mathfrak{p}|\mathfrak{b}} \mathrm{N}\,\mathfrak{p}^{2\,\mathrm{v}_\mathfrak{p}(A[\mathbf{z}])/d} \max_{l=1,\dots,d} \left| \mathbf{z}^{(l)} - \frac{z^{(l)}_{L(l)}}{a^{(l)}_{L(l)}} \mathbf{a}^{(l)} \right|^2 \langle \mathbf{a} \rangle . \end{aligned}$$

□

4.2 Geometrie der Zahlen

Um ein geeignetes $\mathbf{z}$ für die Konstruktion aus dem vorherigen Abschnitt zu erhalten, benutzen wir wie Dietmann die Geometrie der Zahlen. Allerdings verwenden wir sie auf eine Art und Weise, die eher an Raghavans Arbeit [Rag75] angelehnt ist.

Ausgehend von Chalks Resultat für sukzessive Minima von Linearformen über algebraischen Zahlkörpern erhalten wir folgendes Lemma.

Lemma 4.3. *Es existieren ganze Zahlen* $\lambda_2, \dots, \lambda_s \in \mathcal{O}$ *mit*

$$\lambda_2 \cdots \lambda_s \ll \max_{\alpha \neq 0 : \alpha\mathbf{a} \in \mathcal{O}^s} \langle \alpha \mathbf{a} \rangle^{-1}$$

und linear unabhängige Vektoren $\mathbf{x}_1, \dots, \mathbf{x}_s \in \mathcal{O}^s$*, sodass*

$$\left| \mathbf{x}_j^{(l)} - \frac{x_{j,L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right|_\infty \leq \lambda_j, \qquad j = 2, \dots, s, \qquad l = 1, \dots, d$$

und $A[\mathbf{x}_1] = 0$ *gilt. Außerdem ist*

$$\mathrm{N}\left(\mathbf{x}_i^T A \mathbf{x}_j : 1 \leq i, j \leq s-1\right) \ll |\mathrm{Nm}\, \Delta|$$

und es existiert ein $\mathbf{w} \in \mathcal{O}^s$ *mit*

$$(\mathbf{w}, \mathfrak{b}) = \mathcal{O}, \qquad \mathbf{w}^T \mathbf{a} = 0, \qquad 0 < \left\langle \mathbf{w}^T \mathbf{x}_2 \right\rangle \asymp |\mathrm{Nm}\, \mathbf{w}^T \mathbf{x}_2|^{1/d} \ll \mathrm{N}\, \mathfrak{b}^\varepsilon.$$

Beweis. Zuerst werden wir die $\lambda_2, \dots, \lambda_s$ als sukzessive Minima konstruieren. Für einen Parameter $\tau \in \mathbb{R}_{>0}$ betrachten wir die ds Linearformen

$$\begin{aligned} \mathcal{L}_{l,i}(\mathbf{X}_l) &= X_{l,i} - \frac{a_i^{(l)}}{a_{L(l)}^{(l)}} X_{l,L(l)}, && 1 \leq l \leq d, 1 \leq i \leq s, i \neq L(l), \\ \mathcal{L}_{l,L(l)}(\mathbf{X}_l) &= \tau^{-1} X_{l,L(l)}, && 1 \leq l \leq d \end{aligned}$$

in den ds Variablen

$$\mathbf{X}_1 = (X_{1,1}, \dots, X_{1,s}), \qquad \dots, \qquad \mathbf{X}_d = (X_{d,1}, \dots, X_{d,s})$$

mit Determinante τ^{-d}.

Für $j = 1, \dots, s$ wählen wir iterativ Vektoren $\mathbf{x}_j \in \mathcal{O}^s \setminus \{\mathbf{0}\}$ jeweils minimal bezüglich

$$\lambda_j = \max_{l,i} |\mathcal{L}_{l,i}(\mathbf{x}_j^{(l)})|$$

und $\mathcal{O}$-linear unabhängig von $\mathbf{x}_1, \dots, \mathbf{x}_{j-1}$.

Aus (8) von Chalk [Cha80a] (vergleiche das Lemma von Chalk [Cha80b]) folgt, dass diese sukzessiven Minima $\lambda_1 \cdots \lambda_s \leq \tau^{-1} D_K^{s/2d}$ erfüllen. Wenn $\mathbf{a}$ und $\mathbf{x}_j$ für ein $j = 1, \dots, s$ linear unabhängig sind, gilt

$$\lambda_j \geq \langle \mathbf{a} \rangle^{-1} \max_{1 \leq i \leq s, 1 \leq l \leq d} \left| a_{L(l)}^{(l)} x_{j,i}^{(l)} - a_i^{(l)} x_{j,L(l)}^{(l)} \right| \geq \langle \mathbf{a} \rangle^{-1}.$$

Also können wir τ so groß wählen, dass $\mathbf{a}$ und $\mathbf{x}_1$ linear abhängig sind. Dann folgt

$$\lambda_2 \cdots \lambda_s \ll \max_{\alpha \neq 0 : \alpha \mathbf{a} \in \mathcal{O}^s} \langle \alpha \mathbf{a} \rangle^{-1}.$$

Außerdem können wir durch Vergrößern von τ erzwingen, dass für beliebige implizite Konstanten und alle $l = 1, \dots, d$ die Abschätzungen

$$\tau^{-1} \sum_{i=1}^{j} |x_{i,L(l)}^{(l)}| \ll \lambda_j, \qquad\qquad j = 2, 3$$

gelten.

Als Nächstes werden wir die Norm des Ideals $(\mathbf{x}_i^T A \mathbf{x}_j : 1 \le i, j \le s-1)$ abschätzen. Dazu zeigen wir, dass die Norm des Ideals

$$\mathfrak{P}_1 = \left(\det \begin{pmatrix} x_{1,i} & x_{2,i} \\ x_{1,j} & x_{2,j} \end{pmatrix} : 1 \le i < j \le s \right)$$

durch eine Konstante beschränkt ist. Da $\mathbf{x}_1$ minimal bezüglich $\langle \cdot \rangle$ ist, gilt wegen Lemma 2.1(iii) die Abschätzung $\mathrm{N}(\mathbf{x}_1) \ll 1$. Daher liefert Lemma 2.1(i) einen Vektor $\boldsymbol{\omega} \in \mathcal{O}^s$ und eine ganze Zahl $\beta \in \mathcal{O}$ mit $\beta = \boldsymbol{\omega}^T \mathbf{x}_1 \neq 0$ und $\langle \beta \rangle \ll 1$. Wegen Lemma 2.2 finden wir zusätzlich ein $\alpha \equiv -\boldsymbol{\omega}^T \mathbf{x}_2 \ (\mathfrak{P}_1)$ mit $\langle \alpha \rangle \ll \mathrm{N}\,\mathfrak{P}_1^{1/d}$. Es gilt

$$\alpha \mathbf{x}_1 + \beta \mathbf{x}_2 \equiv \mathbf{0} \quad (\mathfrak{P}_1).$$

Aus Lemma 2.1(iii) folgt die Existenz von $\mu \in K$ mit $\langle \mu \rangle \ll \mathrm{N}\,\mathfrak{P}_1^{-1/d}$ und $\mathbf{z} = \mu(\alpha \mathbf{x}_1 + \beta \mathbf{x}_2) \in \mathcal{O}^s$. Daraus resultieren für alle $l = 1, \dots, d$ die Abschätzungen

$$\Big| \mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \Big|_\infty = |\mu^{(l)} \beta^{(l)}| \Big| \mathbf{x}_2^{(l)} - \frac{x_{2,L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \Big|_\infty \ll \lambda_2 \,\mathrm{N}\,\mathfrak{P}_1^{-1/d},$$
$$|\tau^{-1} z_{L(l)}^{(l)}| \ll \tau^{-1} (|x_{1,L(l)}^{(l)}| + |x_{2,L(l)}^{(l)}| \,\mathrm{N}\,\mathfrak{P}_1^{-1/d}).$$

Sobald wir τ ausreichend groß gewählt haben, folgt $\mathrm{N}\,\mathfrak{P}_1 \ll 1$ aus der Minimalität von $\mathbf{x}_1$.

Auf ähnliche Art und Weise lässt sich zeigen, dass die Norm des Ideals

$$\mathfrak{P}_2 = \left(\det \begin{pmatrix} x_{1,i} & x_{2,i} & x_{3,i} \\ x_{1,j} & x_{2,j} & x_{3,j} \\ x_{1,k} & x_{2,k} & x_{3,k} \end{pmatrix} : 1 \le i < j < k \le s \right)$$

ebenfalls durch eine Konstante beschränkt ist. Analog zu der Existenz von $\boldsymbol{\omega}$ und β gibt es

$$\gamma = \sum_{1 \le i < j \le s} \omega_{i,j} \det \begin{pmatrix} x_{1,i} & x_{2,i} \\ x_{1,j} & x_{2,j} \end{pmatrix} \neq 0 \tag{4.2}$$

mit $\langle\gamma\rangle \ll 1$. Wegen Lemma 2.2 finden wir

$$\alpha \equiv \sum \omega_{i,j} \det \begin{pmatrix} x_{2,i} & x_{3,i} \\ x_{2,j} & x_{3,j} \end{pmatrix} \quad (\mathfrak{P}_2),$$
$$\beta \equiv -\sum \omega_{i,j} \det \begin{pmatrix} x_{1,i} & x_{3,i} \\ x_{1,j} & x_{3,j} \end{pmatrix} \quad (\mathfrak{P}_2)$$

mit $\langle\alpha\rangle, \langle\beta\rangle \ll \mathrm{N}\,\mathfrak{P}_2^{1/d}$. Wiederum gilt

$$\alpha\mathbf{x}_1 + \beta\mathbf{x}_2 + \gamma\mathbf{x}_3 \equiv \mathbf{0} \quad (\mathfrak{P}_2). \tag{4.3}$$

Sei $p \in \mathfrak{P}_2$ ein Element, für das $|\mathrm{Nm}\, p| \asymp \mathrm{N}\,\mathfrak{P}_2^{1/d}$ gilt. Wir können Chalks Resultat [Cha80a] auf die $2d$ Linearformen

$$\begin{aligned} &Y_{1,l}, && l = 1, \ldots, d, \\ &\beta^{(l)} Y_{1,l} - p^{(l)} Y_{2,l}, && l = 1, \ldots, d \end{aligned}$$

in den $2d$ Variablen $Y_{1,1}, \ldots, Y_{2,d}$ mit Determinante $\mathrm{Nm}\, p$ anwenden. Es zeigt sich, dass $y_1, y_2 \in \mathcal{O}$ mit

$$\langle y_1\rangle \ll \mathrm{N}\,\mathfrak{P}_2^{1/2d}, \qquad \langle\beta y_1 - p y_2\rangle \ll \mathrm{N}\,\mathfrak{P}_2^{1/2d}$$

existieren. Wenn wir $\mathrm{N}\,\mathfrak{P}_2 \gg 1$ annehmen, können wir durch Multiplikation von (4.3) mit y_1 und mithilfe von Lemma 2.2 die Existenz von $\widetilde{\alpha}, \widetilde{\beta}, \widetilde{\gamma} \in \mathcal{O}$ mit

$$\begin{aligned} \widetilde{\alpha}\mathbf{x}_1 + \widetilde{\beta}\mathbf{x}_2 + \widetilde{\gamma}\mathbf{x}_3 \equiv \mathbf{0} \quad (\mathfrak{P}_2), \qquad & \widetilde{\gamma} \not\equiv 0 \quad (\mathfrak{P}_2), \\ \langle\widetilde{\alpha}\rangle \ll \mathrm{N}\,\mathfrak{P}_2^{1/d}, \qquad & \left\langle\widetilde{\beta}\right\rangle, \langle\widetilde{\gamma}\rangle \ll \mathrm{N}\,\mathfrak{P}_2^{1/2d} \end{aligned}$$

folgern. Wie oben können wir hieraus ein im Widerspruch zur Minimalität von λ_3 stehendes $\mathbf{z}' \in \mathcal{O}^s$ konstruieren. Also gilt $\mathrm{N}\,\mathfrak{P}_2 \ll 1$.

Aus dem Satz von Gustafson, Moore und Reiner [GMR81] folgt die Existenz einer Matrix $T \in \mathcal{O}^{s\times s}$ mit

$$|\mathrm{Nm}\det T| \ll \mathrm{N}\,\mathfrak{P}_{s-2} \ll 1,$$

deren ersten Spalten die Vektoren $\mathbf{x}_1, \ldots, \mathbf{x}_{s-1}$ sind. Wie im Beweis von Lemma 21 von Dietmann [Die03] folgt aus

$$A[T] = \begin{pmatrix} \mathbf{x}_1^T A\mathbf{x}_1 & \ldots & \mathbf{x}_1^T A\mathbf{x}_{s-1} & * \\ \vdots & & \vdots & \vdots \\ \mathbf{x}_{s-1}^T A\mathbf{x}_1 & \ldots & \mathbf{x}_{s-1}^T A\mathbf{x}_{s-1} & * \\ * & \ldots & * & * \end{pmatrix},$$

dass

$$\left(\mathbf{x}_i^T A\mathbf{x}_j : 1 \le i,j \le s-1\right) \mid \det(A[T]) = \Delta \det T^2$$

und somit

$$\mathrm{N}\left(\mathbf{x}_i^T A\mathbf{x}_j : 1 \le i,j \le s-1\right) \ll |\mathrm{Nm}\,\Delta|$$

gilt.

Als Letztes werden wir $\mathbf{w}$ konstruieren. Ausgehend von (4.2) können wir

$$w_j' = \sum_{1\le i<j} \omega_{i,j}x_{1,i} - \sum_{j<i\le s} \omega_{j,i}x_{1,i}, \qquad j = 1,\dots,s$$

setzen. Dann erfüllt der Vektor $\mathbf{w}' = (w_1',\dots,w_s')$ sowohl

$$\mathbf{w}'^T\mathbf{a} = \sum_{1\le i<j\le s} \omega_{i,j} \det\begin{pmatrix} x_{1,i} & a_i \\ x_{1,j} & a_j \end{pmatrix} = 0$$

als auch

$$0 < \left\langle \mathbf{w}'^T\mathbf{x}_2 \right\rangle = \Big\langle \sum_{1\le i<j\le s} \omega_{i,j} \det\begin{pmatrix} x_{1,i} & x_{2,i} \\ x_{1,j} & x_{2,j} \end{pmatrix} \Big\rangle \ll 1.$$

Wegen Lemma 2.1(i) und (iii) gibt es ein $\lambda \neq 0$ mit

$$(\lambda\mathbf{w}, \mathfrak{b}) = \mathcal{O}, \qquad \left\langle \lambda\mathbf{w}'^T\mathbf{x}_2 \right\rangle \asymp |\mathrm{Nm}\,\lambda\mathbf{w}'^T\mathbf{x}_2|^{1/d} \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}.$$

Also hat $\mathbf{w} = \lambda\mathbf{w}'$ die gewünschten Eigenschaften. □

Das gesuchte $\mathbf{z}$ entsteht wie in §3.3 von Dietmann [Die03] als Linearkombination der obigen $\mathbf{x}_1,\dots,\mathbf{x}_{s-1}$. Zusammen mit den vorherigen Lemmata erhalten wir das folgende Resultat.

Lemma 4.4. *Wenn* (4.1) *keine Lösung* $\mathbf{c} \in \mathcal{O}^s$ *mit*

$$\langle\mathbf{c}\rangle \ll \langle A\rangle^{(s+1)/2}\,\mathrm{N}\,\mathfrak{b}^{2(s-2)/d+\varepsilon}|\mathrm{Nm}\,\Delta|^{2/d}\,\langle\mathbf{a}\rangle^{(s-1)/2} \max_{\alpha\neq 0:\alpha\mathbf{a}\in\mathcal{O}^s} \langle\alpha\mathbf{a}\rangle^{-1} \tag{4.4}$$

besitzt, gilt $s = 4$ *und* $\mathbf{x}_2^T A\mathbf{x}_2 = \mathbf{a}^T A\mathbf{x}_2 = 0$.

Beweis. Wenn wir den Ansatz

$$\mathbf{z} = \sum_{i=1}^{s-1} \beta_i\mathbf{x}_i$$

mit $\beta_i \in \mathcal{O}$ verwenden, gilt

$$A[\mathbf{z}] = \sum_{i,j=1}^{s-1} \beta_i \beta_j \mathbf{x}_i^T A \mathbf{x}_j.$$

Für $s = 3$ können wir $\beta_2 = 1$ setzen und β_1 mithilfe des chinesischen Restsatzes so wählen, dass

$$\mathrm{v}_{\mathfrak{p}}(A[\mathbf{z}]) \leq \mathrm{v}_{\mathfrak{p}}\left(2\mathbf{x}_i^T A \mathbf{x}_j : 1 \leq i, j \leq s-1\right) \tag{4.5}$$

für alle $\mathfrak{p} \mid \mathfrak{b}$ gilt.

Für $s = 4$ können wir über den chinesischen Restsatz $\beta_1, \beta_2, \beta_3$ ebenfalls so wählen, dass (4.5) für alle $\mathfrak{p} \mid \mathfrak{b}$ erfüllt ist. Da es dabei bei β_2 und β_3 nur auf die Restklasse bezüglich $\mathfrak{b}$ ankommt, können wir wegen Lemma 2.2 von $\langle \beta_2 \rangle, \langle \beta_3 \rangle \ll \mathrm{N}\,\mathfrak{b}^{1/d}$ ausgehen.

In beiden Fällen gilt also

$$\mathrm{N}\left(\prod_{\mathfrak{p}\mid\mathfrak{b}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(A[\mathbf{z}])}\right) \ll |\mathrm{Nm}\,\Delta|$$

und ferner auch

$$\max_{l=1,\dots,d} \left| \mathbf{z}^{(l)} - \frac{z_{L(l)}^{(l)}}{a_{L(l)}^{(l)}} \mathbf{a}^{(l)} \right|_\infty \ll \mathrm{N}\,\mathfrak{b}^{(s-3)/d} \lambda_{s-1}.$$

Aus Lemma 4.2 folgt damit die Existenz einer Lösung $\mathbf{c} \in \mathcal{O}^s$ von (4.1) mit

$$\langle \mathbf{c} \rangle \ll \langle A \rangle^2 \,\mathrm{N}\,\mathfrak{b}^{2(s-2)/d+\varepsilon} |\mathrm{Nm}\,\Delta|^{2/d} \langle \mathbf{a} \rangle \lambda_{s-1}^2.$$

Des Weiteren impliziert Lemma 4.3, dass

$$\lambda_{s-1} \ll \begin{cases} \max_{\alpha \neq 0 : \alpha\mathbf{a} \in \mathcal{O}^s} \langle \alpha \mathbf{a} \rangle^{-1/2}, & s = 3, \\ \lambda_2^{-1/2} \max_{\alpha \neq 0 : \alpha\mathbf{a} \in \mathcal{O}^s} \langle \alpha \mathbf{a} \rangle^{-1/2}, & s = 4. \end{cases}$$

Wenn $\mathbf{x}_2^T A \mathbf{x}_2 = \mathbf{a}^T A \mathbf{x}_2 = 0$ nicht gilt, können wir Lemma 4.1 auf $\mathbf{x}_2$ oder $\mathbf{a} + \mathbf{x}_2$ anwenden, um $1 \ll \lambda_2^2 \langle A \rangle \langle \mathbf{a} \rangle$ zu schließen. Damit folgt die Behauptung. □

Solange nicht $s = 4$ und gleichzeitig $\mathbf{x}_2^T A \mathbf{x}_2 = \mathbf{a}^T A \mathbf{x}_2 = 0$ gilt, können wir das obige Lemma dazu nutzen, die Größe der kleinsten Lösung abzuschätzen. Hierzu bietet es sich an, gleich mit einer kleinsten Lösung als Startlösung $\mathbf{a}$ anzufangen. Dann gilt $\langle \mathbf{a} \rangle \leq \langle \mathbf{c} \rangle$ und wir können aus (4.4) eine obere Schranke für die Größe dieser kleinsten Lösung herleiten.

Beweis von Proposition 3, wenn nicht $s = 4$ und $\mathbf{x}_2^T A\mathbf{x}_2 = \mathbf{a}^T A\mathbf{x}_2 = 0$ gilt. Da $(\boldsymbol{\xi})$ zu $\mathfrak{b}$ teilerfremd ist, ist dies auch $(\mathbf{a})$. Weiterhin finden wir wegen Lemma 2.1(iii) zu $\mathfrak{b}$ teilerfremde $u, v \in \mathcal{O}$ mit $\langle u/v\rangle \ll \mathrm{N}(\mathbf{a})^{-1/d}\,\mathrm{N}\,\mathfrak{b}^{\varepsilon}$ und $uv^{-1}\mathbf{a} \in \mathcal{O}^s$. Da $uv^{-1}\mathbf{a}$ eine Lösung von (4.1) ist, folgt aus der Minimalität von $\mathbf{a}$, dass

$$\langle \mathbf{a}\rangle \le \left\langle \frac{u}{v}\mathbf{a}\right\rangle \ll \mathrm{N}(\mathbf{a})^{-1/d}\,\mathrm{N}\,\mathfrak{b}^{\varepsilon}\,\langle \mathbf{a}\rangle$$

und damit auch $\mathrm{N}(\mathbf{a}) \ll \mathrm{N}\,\mathfrak{b}^{d\varepsilon}$.

Die Zahl $\alpha \in K \setminus \{0\}$ erfülle $\alpha\mathbf{a} \in \mathcal{O}^s$. Dann gilt $|\mathrm{Nm}\,\alpha|^{-1} \le \mathrm{N}(\mathbf{a})$ und aufgrund der Minimalität von $\mathbf{a}$ auch

$$\max_{\alpha\neq 0:\alpha\mathbf{a}\in\mathcal{O}^s} \langle \alpha\mathbf{a}\rangle^{-1} \ll \frac{1}{|\mathrm{Nm}\,\alpha|^{1/d}\,\langle \mathbf{a}\rangle} \ll \frac{\mathrm{N}\,\mathfrak{b}^{\varepsilon}}{\langle \mathbf{a}\rangle}.$$

Aus Lemma 4.3 folgt deshalb

$$\langle \mathbf{a}\rangle \ll \langle A\rangle^{(s+1)/2}\,\mathrm{N}\,\mathfrak{b}^{2(s-2)/d+2\varepsilon}|\mathrm{Nm}\,\Delta|^{2/d}\,\langle \mathbf{a}\rangle^{(s-3)/2}$$

und somit auch

$$\langle \mathbf{a}\rangle \ll \langle A\rangle^{(s+1)/(5-s)}\,\mathrm{N}\,\mathfrak{b}^{4(s-2)/d/(5-s)+4\varepsilon/(5-s)}|\mathrm{Nm}\,\Delta|^{4/d/(5-s)}.$$

Dies zeigt in diesem Fall die Behauptung. □

4.3 Singuläre ternäre Formen

Den noch nicht abgehandelten Fall werden wir auf den ternären Fall zurückführen. Da wir dabei unter Umständen eine singuläre Matrix erhalten, werden wir in diesem auf §3.1 von Dietmann [Die03] basierenden Abschnitt ein zu Proposition 3 analoges Resultat für den singulären ternären Fall herleiten.

Das folgende Lemma und sein Beweis ist eine fast wörtliche Übernahme von Lemma 17 von Dietmann [Die03].

Lemma 4.5. *Seien a_1, a_2 und a_3 Elemente des Ganzheitsrings. Wenn*

$$\sum_{i=1}^{3} a_i x_i = 0, \qquad \mathbf{x} \equiv \boldsymbol{\xi} \quad (\mathfrak{b}) \tag{4.6}$$

lösbar ist, gibt es eine Lösung $\mathbf{x} \in \mathcal{O}^3$ mit

$$\langle \mathbf{x}\rangle \ll \mathrm{N}\,\mathfrak{b}^{1/d}\max\{1, \langle a_1\rangle, \langle a_2\rangle, \langle a_3\rangle\}.$$

Beweis. Wenn keine Lösung existiert, ist die Aussage trivial und im Fall von $a_1 = a_2 = a_3 = 0$ folgt die Behauptung leicht aus Lemma 2.2. Sei $\mathbf{y} \in \mathcal{O}^3$ eine Lösung von (4.6) und o. B. d. A. gelte $a_1 \neq 0$. Aus Lemma 2.2 können wir die Existenz von z_2, $z_3 \in K$ mit

$$z_i \equiv y_i/a_1 \quad (\mathfrak{b}), \qquad \langle z_i \rangle \ll \mathrm{N}\,\mathfrak{b}^{1/d}, \qquad i = 2, 3$$

folgern. Dann ist $\mathbf{x} \in \mathcal{O}^3$ mit

$$x_1 = -a_2 z_2 - a_3 z_3, \qquad x_2 = a_1 z_2, \qquad x_3 = a_1 z_3$$

eine Lösung von (4.6) und verfügt über die geforderte Größe. □

Auch das nächste Lemma ist eine fast wörtliche Übernahme von Lemma 18 von Dietmann [Die03].

Lemma 4.6. *Seien a_1, a_2, a_3, b_2 und b_3 ganze Zahlen. Wenn*

$$\sum_{i=1}^{3} a_i x_i = \sum_{i=2}^{3} b_i x_i = 0, \qquad \mathbf{x} \equiv \boldsymbol{\xi} \quad (\mathfrak{b})$$

lösbar ist, gibt es eine Lösung $\mathbf{x} \in \mathcal{O}^3$ mit

$$\langle \mathbf{x} \rangle \ll \mathrm{N}\,\mathfrak{b}^{1/d} \max\{1, \langle a_1 \rangle, \langle a_2 \rangle, \langle a_3 \rangle\} \max\{1, \langle b_2 \rangle, \langle b_3 \rangle\}.$$

Beweis. Wenn $a_1 = 0$ gilt, sind die Vektoren (a_2, a_3) und (b_2, b_3) entweder linear abhängig, sodass die Behauptung aus dem vorherigen Lemma folgt, oder jede Lösung erfüllt $x_2 = x_3 = 0$, sodass die Behauptung von Lemma 2.2 impliziert wird. Da die Behauptung für $b_2 = b_3 = 0$ direkt aus dem vorhergehenden Lemma folgt, können wir o. B. d. A. von $a_1, b_2 \neq 0$ ausgehen. Außerdem können wir wie oben davon ausgehen, dass eine Lösung $\mathbf{y}$ existiert.

Wegen Lemma 2.2 können wir $z_3 \in K$ mit

$$z_3 \equiv \frac{y_3}{a_1 b_2} \quad (\mathfrak{b}), \qquad \langle z_3 \rangle \ll \mathrm{N}\,\mathfrak{b}^{1/d}$$

finden. Dann ist

$$x_1 = a_2 b_3 z_3 - a_3 b_2 z_3, \qquad x_2 = -a_1 b_3 z_3, \qquad x_3 = a_1 b_2 z_3$$

eine Lösung $\mathbf{x} \in \mathcal{O}^3$ der richtigen Größe. □

Diese Lemmata liefern die gesuchte Suchschranke für den singulären ternären Fall.

Lemma 4.7. *Sei $A \in \mathcal{O}^{3\times 3}$ singulär. Wenn*

$$A[\mathbf{x}] = 0, \qquad \mathbf{x} \equiv \boldsymbol{\xi} \quad (\mathfrak{b})$$

in $\mathcal{O}^3$ lösbar ist, dann existiert eine $\langle \mathbf{x} \rangle \ll \mathrm{N}\,\mathfrak{b}^{1/d}(1+\langle A\rangle)^3$ erfüllende Lösung.

Beweis. Der Beweis ist fast wörtlich §3.1 von Dietmann [Die03] entnommen. Wenn $A = 0$ gilt, folgt die Aussage aus Lemma 2.2. Im Fall $A \neq 0$ können wir o. B. d. A. von $a_{11} \neq 0$ ausgehen. Es gilt

$$a_{11}A[\mathbf{x}] = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + \sum_{i,j=2}^{3} (a_{11}a_{ij} - a_{1i}a_{1j})x_i x_j.$$

Des Weiteren erfüllt

$$B = (b_{ij})_{i,j=1}^2 = (a_{11}a_{i+1,j+1} - a_{1,i+1}a_{1,j+1})_{i,j=1}^2$$

stets

$$\det B = a_{11} \det A = 0, \qquad \langle B\rangle \ll \langle A\rangle^2 .$$

Da die Behauptung für $B = 0$ aus Lemma 4.5 folgt, können wir o. B. d. A. $b_{11} \neq 0$ annehmen. Wegen $\det B = 0$ gilt

$$a_{11}b_{11}A[\mathbf{x}] = b_{11}(a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + (b_{11}x_2 + b_{12}x_3)^2.$$

Wenn $-b_{11}$ in $\mathcal{O}$ kein Quadrat ist, folgt die Behauptung aus dem vorherigen Lemma und, wenn ein $u \in \mathcal{O}$ mit $u^2 = -b_{11}$ existiert, können wir auf

$$u(a_{11}x_1 + a_{12}x_2 + a_{13}x_3) = b_{11}x_2 + b_{12}x_3$$

und

$$-u(a_{11}x_1 + a_{12}x_2 + a_{13}x_3) = b_{11}x_2 + b_{12}x_3$$

jeweils Lemma 4.5 anwenden und so das gewünschte Resultat erhalten. □

4.4 Der letzte Fall von Proposition 3

In diesem Abschnitt werden wir den Fall $s = 4$ und $\mathbf{x}_2^T A\mathbf{x}_2 = \mathbf{a}^T A\mathbf{x}_2 = 0$ wie in §3.3 von Dietmann [Die03] auf den ternären Fall zurückführen. Dazu nutzen wir das folgende auf Lemma 2 von Kornhauser [Kor90a] basierende Resultat.

Lemma 4.8. *Sei $\mathbf{y} \in \mathcal{O}^s \setminus \{\mathbf{0}\}$. Wenn $(\mathbf{y})$ teilerfremd zu $\mathfrak{b}$ ist, gibt es eine Matrix $W \in \mathcal{O}^{s\times s}$ mit*

$$1 \le |\mathrm{Nm}\det W| \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}, \qquad\qquad \langle W\rangle \ll \langle \mathbf{y}\rangle\,\mathrm{N}\,\mathfrak{b}^{\varepsilon}$$

und zu $\mathfrak{b}$ teilerfremder Determinante, sodass

$$\mathbf{y}^T W = (m, 0, \dots, 0), \qquad\qquad |\mathrm{Nm}\, m| \ll \mathrm{N}(\mathbf{y})\,\mathrm{N}\,\mathfrak{b}^{\varepsilon}$$

für ein zu $\mathfrak{b}$ teilerfremdes $m \in \mathcal{O}$ gilt.

Beweis. O. B. d. A. gelte $y_1 \neq 0$. Wir betrachten die Vektoren

$$\mathbf{v}_1 = \begin{pmatrix} y_s/y_1 \\ 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix}, \qquad \dots, \qquad \mathbf{v}_{s-1} = \begin{pmatrix} y_2/y_1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \mathbf{v}_s = \begin{pmatrix} 1/y_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Wegen Lemma 2.1(ii) lassen sich für $1 \le j \le s$ in den Idealen

$$\mathfrak{t}_j = \Big\{ t \in \mathcal{O} : \exists \mu_1, \dots, \mu_{j-1} \in \mathcal{O} : \sum_{i=1}^{j-1} \mu_i \mathbf{v}_i + t\mathbf{v}_j \in \mathcal{O}^s \Big\} \supset (y_1)$$

stets Elemente $t_{jj} \neq 0$ mit $t_{jj}\mathfrak{t}_j^{-1} + \mathfrak{b} = \mathcal{O}$ und

$$\left\langle \frac{t_{jj}}{y_1} \right\rangle \ll |\mathrm{Nm}(t_{jj}/y_1)|^{1/d} \ll |\mathrm{N}\,\mathfrak{t}_j/\,\mathrm{Nm}\, y_1|^{1/d}\,\mathrm{N}\,\mathfrak{b}^{\varepsilon} \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}$$

finden. Aus dem gleichen Grund gibt es zu $\mathfrak{b}$ teilerfremde und von 0 verschiedene $m_j \in t_{jj}\mathfrak{t}_j^{-1}$ mit $|\mathrm{Nm}\, m_j| \ll \mathrm{N}\,\mathfrak{b}^{\varepsilon}$.

Wegen $t_{jj} \in \mathfrak{t}_j$ gibt es $t_{j1}, \dots, t_{j,j-1} \in \mathcal{O}$ mit

$$\mathbf{w}_j = t_{j1}\mathbf{v}_1 + \ldots + t_{jj}\mathbf{v}_j \in \mathcal{O}^s.$$

Da bei t_{ji} für $i < j$ jeweils nur die Restklasse modulo y_1 relevant ist, können wir wegen Lemma 2.2 o. B. d. A. von $\langle t_{ji}/y_1\rangle \ll 1$ ausgehen. Folglich ist $\langle \mathbf{w}_j\rangle \ll \langle \mathbf{y}\rangle\,\mathrm{N}\,\mathfrak{b}^{\varepsilon}$.

Als Nächstes zeigen wir

$$\left(\prod_{j=1}^{s} m_j\right)\mathcal{O}^s \subset \mathrm{span}_{\mathcal{O}}(\mathbf{w}_1, \dots, \mathbf{w}_s).$$

Da $\operatorname{span}_{\mathcal{O}}(\mathbf{v}_1, \ldots, \mathbf{v}_s)$ jeden Vektor aus $\mathcal{O}^s$ enthält, lässt sich jedes Element aus $\left(\prod_j m_j\right)\mathcal{O}^s$ schreiben als $\left(\prod_{j=1}^s m_j\right)\mathbf{w}$ mit

$$\mathbf{w} = \mu_1\mathbf{v}_1 + \ldots + \mu_s\mathbf{v}_s \in \mathcal{O}^s$$

und $\mu_i \in \mathcal{O}$. Hierbei gilt $\mu_s \in \mathfrak{t}_s$ und somit auch $m_s\mu_s/t_{ss} \in \mathcal{O}$. Entsprechend gilt

$$m_s\mathbf{w} - \frac{m_s\mu_s}{t_{ss}}\mathbf{w}_s = \mu_1'\mathbf{v}_1 + \ldots + \mu_{s-1}'\mathbf{v}_{s-1} \in \mathcal{O}^s$$

mit $\mu_i' \in \mathcal{O}$. Es folgt $\mu_{s-1}' \in \mathfrak{t}_{s-1}$ und durch Iteration dieses Arguments erhalten wir schließlich

$$\left(\prod_{j=1}^s m_j\right)\mathbf{w} = \sum_{i=1}^s \left(\prod_{j\le i} m_j\right)\frac{\mu_i}{t_{ii}}\mathbf{w}_i \in \operatorname{span}_{\mathcal{O}}(\mathbf{w}_1, \ldots, \mathbf{w}_s).$$

Deshalb teilt die Determinante der Matrix $W = (\mathbf{w}_1, \ldots, \mathbf{w}_s) \in \mathcal{O}^{s\times s}$ stets $\prod_{j=1}^s m_j^s$ und ist teilerfremd zu $\mathfrak{b}$. Außerdem gilt

$$1 \le |\operatorname{Nm}\det W| \ll \operatorname{N}\mathfrak{b}^{\varepsilon}, \qquad \mathbf{y}^T W = (t_{ss}, 0, \ldots, 0).$$

Schlussendlich erfüllen W und $m = t_{ss}$ wegen $T_s = (\mathbf{y})$ auch die restlichen in der Behauptung geforderten Eigenschaften. □

Mithilfe dieses Lemmas können wir den im Abschnitt 4.2 begonnenen Beweis von Proposition 3 wie in §3.3 von Dietmann [Die03] zu Ende führen.

Beweis von Proposition 3 für $s = 4$ und $\mathbf{x}_2^T A\mathbf{x}_2 = \mathbf{a}^T A\mathbf{x}_2 = 0$. Wir können o. B. d. A. $\mathfrak{b} \neq \mathcal{O}$ annehmen. Aus Lemma 4.3 folgt die Existenz eines $\mathbf{w} \in \mathcal{O}^s$ mit

$$(\mathbf{w}, \mathfrak{b}) = \mathcal{O}, \qquad \mathbf{w}^T\mathbf{a} = 0, \qquad 0 < \left\langle \mathbf{w}^T\mathbf{x}_2 \right\rangle \asymp |\operatorname{Nm}\mathbf{w}^T\mathbf{x}_2|^{1/d} \ll \operatorname{N}\mathfrak{b}^{\varepsilon}.$$

Wir schreiben $m_1 = \mathbf{w}^T\mathbf{x}_2$ und nutzen Lemma 2.2, um ein $\mathbf{y} \in \mathcal{O}^s$ mit $\mathbf{y} \equiv \mathbf{w}\ (m_1\mathfrak{b})$ und $\langle\mathbf{y}\rangle \le \operatorname{N}\mathfrak{b}^{1/d+\varepsilon}$ zu wählen. Dann gilt

$$\mathbf{y}^T\mathbf{a} \equiv 0 \quad (m_1\mathfrak{b}), \qquad \mathbf{y}^T\mathbf{x}_2 \equiv m_1 \quad (m_1\mathfrak{b})$$

und $(\mathbf{y}, \mathfrak{b}) = \mathcal{O}$.

Wenn $m_1\mathbf{b} \mid \mathbf{w}$ gelten würde, würde $\mathbf{w}$ auch von $(\mathbf{w})\mathfrak{b}$ geteilt werden. Wegen $\mathfrak{b} \neq \mathcal{O}$ gilt also $\mathbf{y} \neq \mathbf{0}$. Folglich können wir $W \in \mathcal{O}^{s\times s}$ und $m \in \mathcal{O}$ wie im vorhergehenden Lemma wählen. Wenn wir

$$B = A[W], \qquad \mathbf{a}' = m(\operatorname{adj} W)\mathbf{a}, \qquad \mathbf{x}_2' = m(\operatorname{adj} W)\mathbf{x}_2$$

setzen, gilt

$$\begin{aligned} B[\mathbf{a}'] = B[\mathbf{x}_2'] &= \mathbf{a}'^T B\mathbf{x}_2' = 0, \\ a_1' &= (m, 0, \dots, 0)(\operatorname{adj} W)\mathbf{a} = (\det W)\mathbf{y}^T\mathbf{a} \equiv 0 \pmod{m_1\mathfrak{b}}, \\ x_{2,1}' &\equiv (\det W)m_1 \pmod{m_1\mathfrak{b}}. \end{aligned}$$

Für $\mathbf{z} = x_{2,1}'\mathbf{a}' - a_1'\mathbf{x}_2' \neq \mathbf{0}$ gilt $z_1 = 0$ und $B[\mathbf{z}] = 0$. Da wir den ternären Fall schon vollständig behandelt haben, folgt entweder aus Proposition 3 oder aus Lemma 4.7, dass ein $\mathbf{x} \in \mathcal{O}^4$ mit

$$x_1 = 0, \qquad B[\mathbf{x}] = 0, \qquad \mathbf{x} \equiv m_2\mathbf{z} \pmod{m_1\mathfrak{b}}$$

für ein zu $m_1\mathfrak{b}$ teilerfremdes $m_2 \in \mathcal{O}$ existiert, das

$$\begin{aligned} \langle \mathbf{x} \rangle &\ll \max\left\{ \langle B \rangle^2 \operatorname{N}(m_1\mathfrak{b})^{2/d+\varepsilon} \langle B \rangle^6, \operatorname{N}(m_1\mathfrak{b})^{1/d}(1 + \langle B \rangle)^3 \right\} \\ &\ll \langle A \rangle^8 \operatorname{N}\mathfrak{b}^{18/d+2\varepsilon} \end{aligned}$$

erfüllt. Weiterhin gilt

$$W\mathbf{x} \equiv m_2 m_1 (\det W) W\mathbf{a}' \equiv m_2 m_1 m (\det W)^2 \mathbf{a} \pmod{m_1\mathfrak{b}}.$$

Da $m_2 m (\det W)^2$ zu $\mathfrak{b}$ teilerfremd ist, ist $m_1^{-1} W\mathbf{x}$ eine Lösung von (4.1) und erfüllt

$$\left\langle m_1^{-1} W\mathbf{x} \right\rangle \ll \langle A \rangle^8 \operatorname{N}\mathfrak{b}^{19/d+4\varepsilon}.$$

Damit ist alles gezeigt. □

5 Äquivalenz quadratischer Formen

Wir werden den verbliebenen Fall von Proposition 1 auf demselben Weg wie Dietmann beweisen. Entsprechend sind alle Propositionen und Lemmata dieses Kapitels Verallgemeinerungen derjenigen aus §4 von Dietmann [Die03]. Wir werden uns den Umstand zunutze machen, dass wir die folgende Proposition über die Äquivalenz quadratischer Formen auf einen bereits vollständig bewiesenen Fall von Proposition 1 zurückführen können.

Proposition 4. *Seien $A, B \in \mathcal{O}^{3\times 3}$ symmetrische und nichtsinguläre Matrizen, sodass $B = A[R]$ für eine Matrix $R \in \mathcal{O}^{3\times 3}$ gilt. Weiterhin sei $\eta \in \mathcal{O} \setminus \{0\}$ und $G = \langle A\rangle + \langle B\rangle$. Dann gibt es eine Matrix $R' \in \mathcal{O}^{3\times 3}$ mit*

$$B = A[R'], \qquad\qquad R' \equiv R \pmod{\eta}$$

und

$$\|R'^{(l)}\| \ll \frac{\left(\langle A\rangle^{24d}\,|\mathrm{Nm}(\Delta^{40}\eta^6)|G^{54d}\right)^{2\gamma(r_0)+\varepsilon} G^{9d/2}}{\min_i\{1, |\Delta^{(l)} d_i^{(l)}|\}}, \qquad l = 1, \dots, d.$$

5.1 Der letzte Fall von Proposition 1

Wie auch bei den anderen Fällen werden wir zuerst zeigen, wie man mithilfe der obigen Proposition den letzten Fall von Proposition 1 beweisen kann. Dazu müssen wir von $\boldsymbol{\xi}$ ausgehend eine geeignete Matrix R konstruieren.

Zunächst verwenden wir Humberts Reduktionstheorie quadratischer Formen über Zahlkörpern ([Hum39], [Hum49]), um das folgende Lemma zu beweisen.

Lemma 5.1. *Sei die Matrix $E \in \mathcal{O}^{2\times 2}$ symmetrisch und nichtsingulär. Dann existiert für jedes $\alpha \in \mathcal{O} \setminus \{0\}$ eine unimodulare Matrix $T \in \mathcal{O}^{2\times 2}$ mit*

$$\langle \alpha E[T]\rangle \ll |\mathrm{Nm}(\alpha \det E)|^{1/d}.$$

Beweis. Die Idee des Beweises ist die gleiche wie bei dem von Lemma 23 von Dietmann [Die03]. Jedoch ist die Anwendung der Reduktionstheorie aufwändiger. Wir unterscheiden zwei Fälle.

Fall 1: Es gibt kein $\mathbf{x} \in \mathcal{O}^2$ mit $(\mathbf{x}) = \mathcal{O}$ und $E[\mathbf{x}] = 0$.
Wie in §2 von Humbert [Hum49] können wir E ein Tupel positiv definiter symmetrischer beziehungsweise hermitescher Matrizen zuordnen.

Für $l \leq r_1$ schreiben wir $E^{(l)} = U_l^T \mathfrak{F}_l U_l$ mit einer reellen Matrix U_l und einer Diagonalmatrix $\mathfrak{F}_l$ mit Diagonaleinträgen ± 1. Die Matrix $\widetilde{E}_l = U_l^T U_l$ ist symmetrisch und positiv definit.

Für $r_1 < l \leq r_1 + r_2$ zerlegen wir $E^{(l)} = U_l^T U_l$ in das Produkt einer komplexen Matrix U_l und deren Transponierten. Dann ist die Matrix $\widetilde{E}_l = \overline{U_l}^T U_l$ hermitesch und positiv definit.

Auf das Tupel $\widetilde{E} = (\widetilde{E}_1, \dots, \widetilde{E}_{r_1+r_2}) \in V^{2\times 2}$ können wir Humberts Reduktionstheorie [Hum39] so anwenden, wie sie im Beweis der Proposition 2 von Icaza [Ica97] zitiert wird. Aus ihr folgt die Existenz einer unimodularen Matrix $T \in \mathcal{O}^{2\times 2}$ und für alle $l = 1, \dots, r_1 + r_2$ die Existenz von Matrizen

$$F_l = \begin{pmatrix} 1 & \beta_l \\ 0 & 1 \end{pmatrix} \in K_l^{2\times 2}, \qquad D_l = \operatorname{diag}(t_1^{(l)}, t_2^{(l)}) \in \mathbb{R}_+^{2\times 2}$$

mit

$$|\beta_l| \ll 1, \qquad t_1^{(l)} \ll t_2^{(l)}, \qquad \overline{T^{(l)}}^T \widetilde{E}_l T^{(l)} = \overline{F_l}^T D_l F_l.$$

Wir schreiben $t_i = (t_i^{(1)}, \dots, t_i^{(r_1+r_2)}) \in V$ und können wegen Lemma 2.1(iii) o. B. d. A. von $\langle \alpha t_2 \rangle \asymp |\operatorname{Nm} \alpha t_2|^{1/d}$ ausgehen.

Als Nächstes zeigen wir

$$|\operatorname{Nm} t_1| \geq 1. \tag{5.1}$$

Wegen

$$\overline{F_l}^T D_l F_l = \begin{pmatrix} t_1^{(l)} & \beta_l \\ \overline{\beta_l} t_1^{(l)} & |\beta_l|^2 t_1^{(l)} + t_2^{(l)} \end{pmatrix}$$

und $T^T E T \in \mathcal{O}^{2\times 2}$ reicht es dazu aus,

$$\left|(1,0)\overline{T^{(l)}}^T \widetilde{E}_l T^{(l)} \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right| \geq \left|(1,0) T^{(l)T} E^{(l)} T^{(l)} \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right| > 0$$

für alle l zu zeigen. Die rechte Ungleichung folgt direkt aus der Bedingung dieses Falls. Um die linke Ungleichung zu beweisen, schreiben wir

$$U_l T^{(l)} = \begin{pmatrix} a_{11}^{(l)} & a_{12}^{(l)} \\ a_{21}^{(l)} & a_{22}^{(l)} \end{pmatrix}.$$

Für $l \le r_1$ erhalten wir dann

$$\begin{aligned}\left|(1,0)T^{(l)T}\widetilde{E}_l T^{(l)}\begin{pmatrix}1\\0\end{pmatrix}\right| &= |a_{11}^{(l)2} + a_{12}^{(l)2}| \\ &\ge |a_{11}^{(l)2} \pm a_{12}^{(l)2}| = \left|(1,0)T^{(l)T}E^{(l)}T^{(l)}\begin{pmatrix}1\\0\end{pmatrix}\right|\end{aligned}$$

und für $l > r_1$ bekommen wir

$$\begin{aligned}\left|(1,0)\overline{T^{(l)}}^T\widetilde{E}_l T^{(l)}\begin{pmatrix}1\\0\end{pmatrix}\right| &= |a_{11}^{(l)}|^2 + |a_{12}^{(l)}|^2 \\ &\ge |a_{11}^{(l)2} + a_{12}^{(l)2}| = \left|(1,0)T^{(l)T}E^{(l)}T^{(l)}\begin{pmatrix}1\\0\end{pmatrix}\right|.\end{aligned}$$

Damit haben wir (5.1) gezeigt, sodass wir aus

$$|\det E^{(l)}| = |\det U_l|^2 = |\det \widetilde{E}_l| = |t_1^{(l)}t_2^{(l)}|$$

die Abschätzung

$$\langle \alpha t_1\rangle \ll \langle \alpha t_2\rangle \asymp \left|\mathrm{Nm}\,\frac{\alpha \det E}{t_1}\right|^{1/d} \le |\mathrm{Nm}\,\alpha \det E|^{1/d}$$

folgern können. Wegen

$$(\overline{U_l T^{(l)}})^T U_l T^{(l)} = \overline{T^{(l)}}^T \widetilde{E}_l T^{(l)} = (\overline{D_l^{1/2}F_l})^T D_l^{1/2}F_l$$

ist die Matrix $V_l = U_l T^{(l)}(D_l F_l)^{-1}$ für jedes l unitär und erfüllt folglich $\|V_l\| \ll 1$. Deshalb gilt

$$\langle \alpha E[T]\rangle \le \max_l |\alpha^{(l)}|\|U_l T^{(l)}\|^2 \le \max_l |\alpha^{(l)}|\|D_l^{1/2}\|^2 \ll |\mathrm{Nm}\,\alpha \det E|^{1/d}.$$

Fall 2: Es gibt ein $\mathbf{x} \in \mathcal{O}^2$ mit $(\mathbf{x}) = \mathcal{O}$ und $E[\mathbf{x}] = 0$.
Dann folgt aus dem Satz von Gustafson, Moore und Reiner [GMR81], dass eine unimodulare Matrix $T_1 \in \mathcal{O}^{2\times 2}$ existiert, deren erste Spalte $\mathbf{x}$ ist und die deshalb

$$E[T_1] = \begin{pmatrix}0 & b\\ b & c\end{pmatrix}$$

für geeignete $b, c \in \mathcal{O}$ erfüllt. Es gilt $b^2 = -\det E$ und wegen Lemma 2.1(iii) können wir spätestens nach einer Multiplikation von T_1 mit einer Einheit

von $\langle \alpha b \rangle \asymp |\mathrm{Nm}\, \alpha b|^{1/d}$ ausgehen. Also ist $\langle \alpha b \rangle \ll |\mathrm{Nm}\, \alpha \det E|^{1/d}$. Außerdem gibt es wegen Lemma 2.2 ein $m \in \mathcal{O}$ mit

$$\langle \alpha c + 2\alpha m b \rangle \ll |\mathrm{Nm}\, \alpha b|^{1/d} \leq |\mathrm{Nm}\, \alpha \det E|^{1/d}.$$

Die unimodulare Matrix

$$T = T_1 \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

erfüllt also

$$\langle \alpha E[T] \rangle = \left\langle \begin{pmatrix} 0 & \alpha b \\ \alpha b & \alpha c + 2\alpha m b \end{pmatrix} \right\rangle \ll |\mathrm{Nm}\, \alpha \det E|^{1/d}. \qquad \square$$

Mithilfe dieses Lemmas können wir eine geeignete Matrix R konstruieren.

Lemma 5.2. *Der Vektor $\boldsymbol{\xi} \in \mathcal{O}^3$ erfülle $\kappa = A[\boldsymbol{\xi}] \neq 0$. Dann existiert eine Matrix $R \in \mathcal{O}^{3\times 3}$, deren erste Spalte $\boldsymbol{\xi}$ ist und die*

$$1 \leq |\mathrm{Nm} \det R| \ll \mathrm{N}(\boldsymbol{\xi}),$$
$$\langle A[R] \rangle \ll \max\left\{ \langle \kappa \rangle, \mathrm{N}(\Delta(\boldsymbol{\xi})^2)^{1/d} \right\}$$

erfüllt.

Beweis. Der Beweis verläuft im Wesentlichen genau wie der von Lemma 24 aus Dietmanns Arbeit [Die03].

Aus der Arbeit von Gustafson, Moore und Reiner [GMR81] folgt die Existenz einer Matrix $R_1 \in \mathcal{O}^{3\times 3}$ mit erster Spalte $\boldsymbol{\xi}$ und

$$1 \leq |\mathrm{Nm} \det R_1| \ll \mathrm{N}(\boldsymbol{\xi}).$$

Also gibt es $\mathbf{c} \in \mathcal{O}^2$ und $D \in \mathcal{O}^{2\times 2}$ mit

$$B = A[R_1] = \begin{pmatrix} \kappa & \mathbf{c}^T \\ \mathbf{c} & D \end{pmatrix}.$$

Wenn wir

$$E = D - \mathbf{c}\mathbf{c}^T/\kappa, \qquad S = \begin{pmatrix} 1 & -\mathbf{c}^T/\kappa \\ \mathbf{0} & I \end{pmatrix}$$

setzen, erhalten wir außerdem

$$B[S] = \begin{pmatrix} \kappa & \mathbf{0}^T \\ \mathbf{0} & E \end{pmatrix}.$$

Wegen $\kappa E \in \mathcal{O}^{2\times 2}$ und

$$\det(\kappa E) = \kappa \det B = \kappa\Delta \det R_1^2$$

folgt aus Lemma 5.1 die Existenz einer unimodularen Matrix $T \in \mathcal{O}^{2\times 2}$ mit

$$\langle E[T]\rangle = \left\langle \kappa^{-1}(\kappa E)[T]\right\rangle \ll |\mathrm{Nm}\,\kappa^{-1}\det(\kappa E)|^{1/d} \ll \mathrm{N}(\Delta(\mathbf{y})^2)^{1/d}.$$

Wir wählen $\mathbf{r} \in \mathcal{O}^2$ so, dass $\mathbf{s} = \mathbf{r} + (T^T\mathbf{c})/\kappa$ der Abschätzung $\langle \mathbf{s}\rangle \ll 1$ genügt. Wenn wir

$$R_2 = \begin{pmatrix} 1 & \mathbf{r}^T \\ \mathbf{0} & T \end{pmatrix} \in \mathcal{O}^{3\times 3}$$

setzen, erhalten wir

$$\begin{aligned} A[R_1R_2] &= \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{r} & T^T \end{pmatrix}\begin{pmatrix} \kappa & \mathbf{c}^T \\ \mathbf{c} & D \end{pmatrix}\begin{pmatrix} 1 & \mathbf{r}^T \\ \mathbf{0} & T \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{r} & T^T \end{pmatrix}\begin{pmatrix} \kappa & \kappa\mathbf{s}^T \\ \mathbf{c} & \mathbf{c}\mathbf{r}^T + DT \end{pmatrix} \\ &= \begin{pmatrix} \kappa & \kappa\mathbf{s}^T \\ \kappa\mathbf{c} & \kappa\mathbf{r}\mathbf{s}^T + T\mathbf{c}\mathbf{r}^T + D[T] \end{pmatrix} = \begin{pmatrix} \kappa & \kappa\mathbf{s}^T \\ \kappa\mathbf{s} & \kappa\mathbf{s}\mathbf{s}^T + E[T] \end{pmatrix}. \end{aligned}$$

Also hat $R = R_1R_2$ die in der Behauptung geforderten Eigenschaften. □

Nun können wir den letzten verbliebenen Fall ($s = 3$ und $\kappa \neq 0$) von Proposition 1 beweisen.

Teilbeweis von Proposition 1. Die Grundidee des Beweises entstammt §4.5 von Dietmann [Die03].

Wie im Beweis des im Kapitel 3 behandelten Falls können wir im Folgenden davon ausgehen, dass A nicht vollständig definit ist und dass $A[\boldsymbol{\xi}] = \kappa$ gilt. Wieder folgt aus Lemma 2.1(i) die Existenz von einem zu η teilerfremden Ideal $\mathfrak{p}$ und einer Zahl $\beta \in K$ mit

$$\mathrm{N}\,\mathfrak{p} \ll |\mathrm{Nm}\,\eta|^{\varepsilon}, \qquad \mathfrak{p}(\boldsymbol{\xi})^{-1} = (\beta), \qquad \left\langle \beta^2\kappa\right\rangle \asymp |\mathrm{Nm}\,\beta^2\kappa|^{1/d}.$$

Sei

$$\boldsymbol{\xi}' = \beta\boldsymbol{\xi} \in \mathcal{O}^s, \qquad \kappa' = \beta^2\kappa = A[\boldsymbol{\xi}'] \in \mathcal{O}.$$

Aus Lemma 5.2 folgt die Existenz einer Matrix $R \in \mathcal{O}^{3\times 3}$, deren erste Spalte $\boldsymbol{\xi}'$ ist und die

$$\begin{aligned} 1 \le |\mathrm{Nm}\det R| \ll \mathrm{N}(\boldsymbol{\xi}') \ll |\mathrm{Nm}\,\eta|^{\varepsilon}, \\ \langle A[R]\rangle \ll \max\{\langle\kappa'\rangle, |\mathrm{Nm}\,\Delta|^{1/d}|\mathrm{Nm}\,\eta|^{\varepsilon}\} \end{aligned}$$

erfüllt. Für $B = A[R]$ gilt $b_{11} = \kappa'$ und aus Proposition 4 folgt, dass es eine Matrix $R' \in \mathcal{O}^{3\times 3}$ mit

$$B = A[R'], \qquad R' \equiv R \pmod{\eta}$$

und

$$\|R'^{(l)}\| \ll \frac{\left(\langle A\rangle^{24d} |\mathrm{Nm}\, \Delta^{40}\eta^6| G^{54d}\right)^{2\gamma(r_0)+\varepsilon} G^{9d/2}}{\min\{1, |\Delta^{(l)} d_i^{(l)}|\}}$$

gibt. Es gilt hierbei

$$\begin{aligned} G = \langle A\rangle + \langle B\rangle &\ll \max\{\langle A\rangle, \langle \kappa'\rangle, |\mathrm{Nm}\, \Delta|^{1/d} |\mathrm{Nm}\, \eta|^{\varepsilon}\} \\ &\ll |\mathrm{Nm}\, \eta|^{\varepsilon} (\langle A\rangle^d + |\mathrm{Nm}\, \kappa| + |\mathrm{Nm}\, \Delta|)^{1/d}. \end{aligned}$$

Für die erste Spalte $\mathbf{x}' \in \mathcal{O}^3$ von R' erhalten wir

$$A[\mathbf{x}'] = \kappa', \qquad \mathbf{x}' \equiv \boldsymbol{\xi}' \pmod{\eta}$$

und

$$\begin{aligned} |\mathbf{x}'^{(l)}| \ll \frac{\left(\langle A\rangle^{24d} |\mathrm{Nm}\, \Delta^{40}\eta^6|\right)^{2\gamma(r_0)+\varepsilon}}{\min\{1, |\Delta^{(l)} d_i^{(l)}|\}} \\ \cdot \left(\langle A\rangle^d + |\mathrm{Nm}\, \kappa| + |\mathrm{Nm}\, \Delta|\right)^{9/2+108\gamma(r_0)+\varepsilon}. \end{aligned}$$

Also ist $\mathbf{x} = \beta^{-1}\mathbf{x}'$ eine Lösung von (2.4) und erfüllt damit insbesondere $\mathbf{x} \in \mathcal{O}^3$. Außerdem gilt

$$|\mathbf{x}^{(l)}| \ll |\kappa^{(l)}|^{1/2} |\mathbf{x}'^{(l)}|,$$

sodass Proposition 1 damit vollständig bewiesen ist. □

5.2 Parametrisierung quadratischer Automorphismen

Die Hauptidee für den Beweis von Proposition 4 ist durch die Beobachtung inspiriert, dass sich die Automorphismen quadratischer Formen in drei Variablen mithilfe einer quadratischen Gleichung in vier Variablen parametrisieren lassen. Deshalb können wir das Resultat aus Kapitel 3 dazu nutzen, einen

kleinen Automorphismus zu finden, mit dem wir eine kleine Lösung für Proposition 4 konstruieren können.

Das folgende Lemma liefert die gesuchte Parametrisierung. Dabei wurde ein kleiner Fehler bei der Definition von v in Lemma 25 von Dietmann [Die03] korrigiert.

Lemma 5.3. *Sei $A \in \mathcal{O}^{3\times 3}$ symmetrisch und nichtsingulär. Für alle $t_0 \in \mathcal{O}$ und $\mathbf{t} \in \mathcal{O}^3$ mit $v = t_0^2 + \Delta A[\mathbf{t}]/4 \neq 0$ ist die Matrix*

$$U = \frac{1}{v}\left(t_0^2 I - \frac{\Delta}{4}A[\mathbf{t}]I + t_0(\operatorname{adj} A)Z(\mathbf{t}) + \frac{\Delta}{2}\mathbf{t}\mathbf{t}^T A\right) \in K^{3\times 3} \tag{5.2}$$

mit

$$Z(\mathbf{t}) = \begin{pmatrix} 0 & -t_3 & t_2 \\ t_3 & 0 & -t_1 \\ -t_2 & t_1 & 0 \end{pmatrix}$$

ein echter Automorphismus von A, d.h. es gilt $A[U] = A$ und $\det U = 1$.

Außerdem ist jeder echte Automorphismus U von A von dieser Form.

Beweis. Die wesentlichen Ideen für diesen Beweis entstammen dem von Dietmann zitierten Beweis von Lemma 1 von Jones und Watson [JW56]. Wir unterscheiden drei Fälle.

Fall 1: Wenn t_0 und $\mathbf{t}$ gegeben sind, gilt $t_0 \neq 0$ und, wenn ein echter Automorphismus U gegeben ist, gilt $\det(I + U) \neq 0$.
Jede schiefsymmetrische Matrix mit Koeffizienten in K lässt sich in der Form

$$-\frac{\Delta}{2t_0}Z(\mathbf{t})$$

mit $t_0 \in \mathcal{O} \setminus \{0\}$ und $\mathbf{t} \in \mathcal{O}^3$ schreiben. Des Weiteren zeigt Nachrechnen

$$v = \frac{t_0^2}{\Delta}\det\left(A - \frac{\Delta}{2t_0}Z(\mathbf{t})\right).$$

Deshalb folgt aus Theorem 37.1 von MacDuffee [Mac33], dass für alle $t_0 \in \mathcal{O} \setminus \{0\}$ und $\mathbf{t} \in \mathcal{O}^3$ mit $v \neq 0$ durch

$$U = \left(A - \frac{\Delta}{2t_0}Z(\mathbf{t})\right)^{-1}\left(A + \frac{\Delta}{2t_0}Z(\mathbf{t})\right) \tag{5.3}$$

ein Automorphismus von A definiert wird, für den wegen $Z(\mathbf{t})^T = -Z(\mathbf{t})$ sogar $\det U = 1$ gilt. Außerdem gilt im Fall von $\det(I + U) \neq 0$ auch die

Umkehrung, sodass wir dieses Resultat als Grundlage für den ersten Fall nehmen können.

Um (5.3) geeignet umformen zu können, zeigen wir zuerst für alle $\mathbf{t} \in \mathcal{O}^3$ die Identität

$$Z(\mathbf{t})(\operatorname{adj} A)Z(\mathbf{t}) + A[\mathbf{t}]A = A\mathbf{t}\mathbf{t}^T A. \tag{5.4}$$

Dazu betrachten wir für $1 \leq l \leq d$ und beliebige Matrizen $T \in \mathbb{C}^{3\times 3}$ die schiefsymmetrische Matrix $T^T Z(T\mathbf{t}^{(l)})T$. Aus $T^T Z(T\mathbf{t})T\mathbf{t} = \mathbf{0}$ folgt, dass

$$T^T Z(T\mathbf{t}^{(l)})T = g(T)Z(\mathbf{t}^{(l)})$$

für ein nur von T abhängiges $g(T) \in \mathbb{C}$ gilt. Dieses $g(T)$ ist eine normierte alternierende Multilinearform auf der Algebra der Matrizen. Folglich gilt $g(T) = \det T$.

Für ein beliebiges l wählen wir $T \in \mathbb{C}^{3\times 3}$ so, dass $B = A^{(l)}[T] \in \mathbb{C}^{3\times 3}$ eine Diagonalmatrix ist und $\det T = 1$ gilt. Wenn wir $\mathbf{t}^{(l)} = T\mathbf{x}$ in (5.4) substituieren, erhalten wir

$$Z(\mathbf{x})(\operatorname{adj} B)Z(\mathbf{x}) + B[\mathbf{x}]B = B\mathbf{x}\mathbf{x}^T B.$$

Da B diagonal ist, lässt sich (5.4) mithilfe einer kurzen Rechnung folgern.

Wir betrachten nun wieder (5.3). Wegen (5.4) gilt

$$\begin{aligned}
&\Big(A - \frac{\Delta}{2t_0}Z(\mathbf{t})\Big)\Big(2t_0^2 I + t_0(\operatorname{adj} A)Z(\mathbf{t}) + \frac{\Delta}{2}\mathbf{t}\mathbf{t}^T A\Big) \\
&= 2t_0^2 A + \frac{\Delta}{2}A\mathbf{t}\mathbf{t}^T A - \frac{\Delta}{2}Z(\mathbf{t})(\operatorname{adj} A)Z(\mathbf{t}) \\
&= 2t_0^2 A + \frac{\Delta}{2}A[\mathbf{t}]A = 2vA = v\Big(A - \frac{\Delta}{2t_0}Z(\mathbf{t})\Big)(I + U).
\end{aligned}$$

Nach U aufgelöst ergibt dies (5.2).

Fall 2: Es sind $\mathbf{t} \in \mathcal{O}^3$ und $t_0 = 0$ gegeben.
In diesem Fall lässt sich (5.2) zu

$$A[\mathbf{t}]U = -A[\mathbf{t}]I + 2\mathbf{t}\mathbf{t}^T A$$

vereinfachen. Daraus folgt $\operatorname{Tr} U = -1$ und $\operatorname{rk}(I + U) = 1$, sodass 1 ein einfacher und -1 ein doppelter Eigenwert von U ist. Insbesondere gilt $\det U = 1$.

Weiterhin ist

$$A[\mathbf{t}]^2 A[U] = A[\mathbf{t}]^2 A - 4A[\mathbf{t}]A\mathbf{t}\mathbf{t}^2 A + 4A\mathbf{t}\mathbf{t}^T A\mathbf{t}\mathbf{t}^T A = A[\mathbf{t}]^2 A.$$

Zusammen mit $A[\mathbf{t}] = v \neq 0$ folgt daraus $A[U] = A$.

Fall 3: Es ist ein echter Automorphismus U mit $\det(I + U) = 0$ gegeben. Wenn U einen Eigenvektor $\mathbf{v}$ mit Eigenwert $\lambda \neq 1, -1$ besitzt, gilt

$$A\mathbf{v} = U^T AU\mathbf{v} = \lambda U^T A\mathbf{v}$$

und somit ist λ^{-1} ein Eigenwert von U^T und damit auch von U. Da wegen $\det(I + U) = 0$ auch -1 ein Eigenwert von U ist, steht die Existenz eines solchen λ im Widerspruch zu $\det U = 1$.

Also gilt $\operatorname{rk}(I + U) = 1$, sodass zwei Vektoren $\mathbf{t}, \mathbf{s} \in K^3 \setminus \{\mathbf{0}\}$ mit $I + U = \mathbf{t}\mathbf{s}^T A$ existieren. Aus

$$\begin{aligned} A\mathbf{s}\mathbf{t}^T A\mathbf{t}\mathbf{s}^T A &= (I + U)^T A(I + U) = A(I + U) + (I + U)^T A \\ &= A\mathbf{t}\mathbf{s}^T A + A\mathbf{s}\mathbf{t}^T A \end{aligned}$$

folgt

$$\mathbf{s}\mathbf{t}^T Z(\mathbf{s}) = (\mathbf{s}\mathbf{t}^T A - I)\mathbf{t}\mathbf{s}^T Z(\mathbf{s}) = \mathbf{0}$$

und somit auch $\mathbf{t}^T Z(\mathbf{s}) = 0$. Dies impliziert $\mathbf{s} = \mu\mathbf{t}$ für ein $\mu \in K \setminus \{0\}$ und wegen

$$\begin{aligned} A = U^T AU &= (\mu A\mathbf{t}\mathbf{t}^T - I)A(\mu\mathbf{t}\mathbf{t}^T A - I) \\ &= \mu^2 A\mathbf{t}\mathbf{t}^T A\mathbf{t}\mathbf{t}^T A - 2\mu A\mathbf{t}\mathbf{t}^T A + A \\ &= (\mu A[\mathbf{t}] - 2)\mu A\mathbf{t}\mathbf{t}^T A + A \end{aligned}$$

gilt $A[\mathbf{t}] \neq 0$ und $\mu = 2/A[\mathbf{t}]$. Mit $t_0 = 0$ folgt die Behauptung. □

Es ist leicht möglich, eine Schranke für das v aus dem vorherigen Lemma herzuleiten.

Lemma 5.4. *Mit den Bezeichnungen wie im vorherigen Lemma gilt*

$$v \mid \Delta^2 \operatorname{den}(U)(2t_0, \mathbf{t})^2.$$

Beweis. Der Beweis verläuft im Wesentlichen wie der von Lemma 26 von Dietmann [Die03].

Da die Spur des Produkts einer symmetrischen und einer schiefsymmetrischen Matrix verschwindet, gilt

$$\operatorname{Tr}\Big((\operatorname{adj} A)Z(\mathbf{t})\Big) = 0.$$

Deshalb folgt aus

$$v(I+U) = 2t_0^2 I + t_0(\operatorname{adj} A)Z(\mathbf{t}) + \frac{\Delta}{2}\mathbf{t}\mathbf{t}^T A, \tag{5.5}$$

dass

$$3v + v\operatorname{Tr} U = \operatorname{Tr}\Big(v(I+U)\Big) = 6t_0^2 + \frac{\Delta}{2}\operatorname{Tr}(\mathbf{t}^T A\mathbf{t}) = 2v + 4t_0^2.$$

Da das Ideal $v\operatorname{den}(U)^{-1}$ sowohl v als auch $v\operatorname{Tr} U$ teilt, resultiert hieraus

$$v\operatorname{den}(U)^{-1} \mid (2t_0)^2.$$

Wenn wir (5.5) mit $\operatorname{adj} A$ multiplizieren, erhalten wir

$$0 \equiv 2t_0^2 \operatorname{adj} A + t_0(\operatorname{adj} A)Z(\mathbf{t})(\operatorname{adj} A) + \frac{\Delta^2}{2}\mathbf{t}\mathbf{t}^T \quad (v\operatorname{den}(U)^{-1}).$$

Wir addieren das Transponierte und bekommen

$$\Delta^2\mathbf{t}\mathbf{t}^T \equiv 0 \quad (v\operatorname{den}(U)^{-1}).$$

Damit folgt $v\operatorname{den}(U)^{-1} \mid \Delta^2(\mathbf{t})^2$ und insgesamt die Behauptung. □

5.3 Äquivalenz quadratischer Formen

Um unser Lemma über Automorphismen anwenden zu können, müssen wir zunächst einen Automorphismus konstruieren.

Lemma 5.5. *Wenn $A, B \in \mathcal{O}^{3\times 3}$ symmetrische und nichtsinguläre Matrizen sind, die $B = A[R]$ für ein $R \in K^{3\times 3}$ erfüllen, dann existiert eine Matrix $S \in K^{3\times 3}$, sodass*

$$B = A[S] \qquad \operatorname{N}\operatorname{den}(S) + \operatorname{N}\operatorname{den}(S^{-1}) + \langle S\rangle \ll G^{9d/2}$$

mit $G = \langle A\rangle + \langle B\rangle$ gilt.

Beweis. Die Idee des Beweises ist dieselbe wie beim Beweis von Lemma 22 aus Dietmanns Arbeit [Die03]. Sei

$$F = \begin{pmatrix} A & 0 \\ 0 & -B \end{pmatrix} \in \mathcal{O}^{6\times 6}.$$

Da die Form $F[\mathbf{X}]$ wegen $B = A[R]$ auf einem dreidimensionalen Unterraum von K^6 verschwindet, folgt aus Corollary 2 von Vaaler [Vaa87] die Existenz von drei K-linear unabhängigen Vektoren $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \in \mathcal{O}^6$ mit

$$\prod_{i=1}^{3} \left(\prod_{\mathfrak{p}} \mathrm{N}\,\mathfrak{p}^{-\,\mathrm{v}_{\mathfrak{p}}(\mathbf{x}_i)} \prod_{l=1}^{r_1+r_2} |\mathbf{x}_i^{(l)}|_\infty^{c_l/d} \right)$$
$$\ll \left(\prod_{\mathfrak{p}} \max\left\{ \mathrm{N}\,\mathfrak{p}^{-\,\mathrm{v}_{\mathfrak{p}}(A)}, \mathrm{N}\,\mathfrak{p}^{-\,\mathrm{v}_{\mathfrak{p}}(B)} \right\} \prod_{l=1}^{r_1+r_2} \left(\sum_{i,j=1}^{3} |a_{ij}^{(l)}|^2 + |b_{ij}^{(l)}|^2 \right)^{c_l/2d} \right)^{3/2},$$

die einen K-Vektorraum aufspannen, auf dem $F[\mathbf{X}]$ verschwindet. Die rechte Seite dieser Abschätzung ist in $O(G^{3/2})$. Da die linke Seite bei der Skalierung der $\mathbf{x}_i$ mit beliebigen Elementen aus $K \setminus \{0\}$ unverändert bleibt, können wir wegen Lemma 2.1(ii) und (iii) von

$$1 \ll \prod_{\mathfrak{p}} \mathrm{N}\,\mathfrak{p}^{-\,\mathrm{v}_{\mathfrak{p}}(\mathbf{x}_i)},$$
$$\max_l \prod_{i=1}^{3} |\mathbf{x}_i^{(l)}|_\infty \ll \prod_{l=1}^{r_1+r_2} \prod_{i=1}^{3} |\mathbf{x}_i^{(l)}|_\infty^{c_l/d}$$

ausgehen. Folglich gilt

$$\max_l \prod_{i=1}^{3} |\mathbf{x}_i^{(l)}|_\infty \ll G^{3/2}.$$

Um die Notation im Rest des Beweises zu vereinfachen, schreiben wir

$$\mathbf{x}_i = \begin{pmatrix} \mathbf{x}_i' \\ \mathbf{x}_i'' \end{pmatrix}, \qquad X' = (\mathbf{x}_1', \mathbf{x}_2', \mathbf{x}_3'), \qquad X'' = (\mathbf{x}_1'', \mathbf{x}_2'', \mathbf{x}_3'')$$

mit $\mathbf{x}_i', \mathbf{x}_i'' \in \mathcal{O}^3$.

Sei vorerst $\det X'' \neq 0$. Dann erfüllt die Matrix $S = X'X''^{-1}$ stets $B = A[S]$, denn die quadratische Form $(B - A[S])[\mathbf{X}]$ verschwindet auf $K[\mathbf{x}_1'', \mathbf{x}_2'', \mathbf{x}_3''] = K^3$.

Aus $\mathrm{den}(S) \mid \det X''$ folgt

$$\mathrm{N}\,\mathrm{den}(S) \leq |\mathrm{Nm}\,\det X''| \ll \prod_{l=1}^{r_1+r_2} \prod_{i=1}^{3} |\mathbf{x}_i^{(l)}|_\infty^{c_l} \ll G^{3d/2}$$

und $\mathrm{den}(S^{-1}) \mid \det X'$ impliziert analog $\mathrm{N}\,\mathrm{den}(S^{-1}) \ll G^{3d/2}$.

Des Weiteren folgt mithilfe der Cramerschen Regel

$$\langle S\rangle \ll \langle \det X''^{-1}\rangle \max_l \prod_{i=1}^{3} |\mathbf{x}_i^{(l)}|_\infty \ll G^{3d/2},$$

sodass für $\det X'' \neq 0$ bereits alles gezeigt ist.

Wenn dagegen $\det X'' = 0$ gilt, können wir mithilfe generischer Symmetrien neue Vektoren erzeugen, auf die wir das eben verwendete Argument anwenden können. Sei dazu

$$\mathbf{t} = \begin{pmatrix} \mathbf{t}' \\ \mathbf{t}'' \end{pmatrix} \in \mathcal{O}^6$$

ein beliebiger $F[\mathbf{t}] \neq 0$ erfüllender Vektor. Dann ist

$$\sigma_{\mathbf{t}}(\mathbf{x}) = \begin{pmatrix} \sigma_{\mathbf{t}}(\mathbf{x})' \\ \sigma_{\mathbf{t}}(\mathbf{x})'' \end{pmatrix} = F[\mathbf{t}]\mathbf{x} - 2(\mathbf{x}^T F\mathbf{t})\mathbf{t}$$

für alle $\mathbf{x} \in \mathcal{O}^6$ mit $F[\mathbf{x}] = 0$ eine Nullstelle der Form $F[\mathbf{X}]$.

Nun untersuchen wir den Rang von X''. Wenn dieser Rang kleiner als 2 wäre, könnten wir, indem wir Linearkombinationen bilden, von $\mathbf{x}_2'' = \mathbf{x}_3'' = \mathbf{0}$ ausgehen. Dies würde aber implizieren, dass $A[\mathbf{X}]$ auf dem zweidimensionalen Raum $K[\mathbf{x}_2', \mathbf{x}_3']$ verschwindet. Wie im rationalen Fall steht dies allerdings im Widerspruch zur Nichtsingularität von A. Folglich ist der Rang von X'' gleich 2.

Als Nächstes werden wir zeigen, dass für generische $\mathbf{t}$ die Determinante von

$$\left(\sigma_{\mathbf{t}}(\mathbf{x}_1)'', \sigma_{\mathbf{t}}(\mathbf{x}_2)'', \sigma_{\mathbf{t}}(\mathbf{x}_3)''\right) \in K^{3\times 3}$$

nicht verschwindet. Da sowohl die Determinante als auch $\sigma_{\mathbf{t}}$ lineare Funktionen sind, können wir dabei o. B. d. A. von $\mathbf{x}_3'' = \mathbf{0}$ und $\operatorname{rk}(\mathbf{x}_1'', \mathbf{x}_2'') = 2$ ausgehen. Damit gilt

$$\begin{aligned}
&\det\left(\sigma_{\mathbf{t}}(\mathbf{x}_1)'', \sigma_{\mathbf{t}}(\mathbf{x}_2)'', \sigma_{\mathbf{t}}(\mathbf{x}_3)''\right) \\
&= \det\left(F[\mathbf{t}]\mathbf{x}_1'' - 2(\mathbf{x}_1^T F\mathbf{t})\mathbf{t}'', F[\mathbf{t}]\mathbf{x}_2'' - 2(\mathbf{x}_2^T F\mathbf{t})\mathbf{t}'', -2(\mathbf{x}_3^T F\mathbf{t})\mathbf{t}''\right) \\
&= -2(\mathbf{x}_3^T F\mathbf{t})F[\mathbf{t}]^2 \det(\mathbf{x}_1'', \mathbf{x}_2'', \mathbf{t}'') \neq 0
\end{aligned}$$

für generische $\mathbf{t}$ und somit insbesondere auch für ein $\mathbf{t} \in \mathcal{O}^6$ mit $\langle \mathbf{t}\rangle \ll 1$. Es gilt

$$|\sigma_{\mathbf{t}}(\mathbf{x}_i)^{(l)}|_\infty \ll G|\mathbf{x}_i^{(l)}|_\infty, \qquad l = 1, 2, 3$$

und damit auch

$$\max_l \prod_{i=1}^{3} |\sigma_{\mathbf{t}}(\mathbf{x}_i)^{(l)}|_\infty \ll G^{9/2},$$

sodass wir die Behauptung folgern können, indem wir das obige Argument wiederholen. □

Wir sind nun in der Lage, Proposition 4 auf Proposition 1 zurückzuführen.

Beweis von Proposition 4. Der Beweis verläuft im Wesentlichen analog zu dem von Theorem 4 von Dietmann [Die03]. Wir können o. B. d. A. von $\Delta/4 \in \mathcal{O}$ ausgehen. Aus Lemma 5.5 folgt die Existenz einer Matrix $S \in K^{3\times 3}$ mit

$$B = A[S], \qquad \mathrm{N}\,\mathrm{den}(S) + \mathrm{N}\,\mathrm{den}(S^{-1}) + \langle S\rangle \ll G^{9d/2}.$$

Da $-S$ diese Eigenschaften ebenfalls erfüllt, können wir o. B. d. A. davon ausgehen, dass $U = RS^{-1}$ ein echter Automorphismus von A ist. Deshalb können wir Lemma 5.3 anwenden und die Existenz von $t_0 \in \mathcal{O}$ und $\mathbf{t} \in \mathcal{O}^3$ mit

$$\begin{aligned} U &= \frac{1}{v}\left(t_0^2 I - \frac{\Delta}{4}A[\mathbf{t}]I + t_0(\mathrm{adj}\,A)Z(\mathbf{t}) + \frac{\Delta}{2}\mathbf{t}\mathbf{t}^T A\right), \\ v &= t_0^2 + \frac{\Delta}{4}A[\mathbf{t}] \in \mathcal{O}\setminus\{0\} \end{aligned}$$

folgern. Weil wir t_0 und $\mathbf{t}$ beliebig skalieren dürfen, ohne dadurch U zu verändern, können wir wegen Lemma 2.1(ii) von $\mathrm{N}(t_0, \mathbf{t}) \ll 1$ ausgehen. Deshalb folgt

$$|\mathrm{Nm}\, v| \ll \mathrm{N}(\Delta^2\,\mathrm{den}(U)) \ll |\mathrm{Nm}\,\Delta^2| G^{9d/2}$$

aus Lemma 5.4. Wegen Lemma 2.1(i) gibt es ein $\widetilde{\eta} \in \eta v\,\mathrm{den}(S)$ mit

$$|\mathrm{Nm}\,\widetilde{\eta}| \ll \mathrm{N}(\eta v\,\mathrm{den}(S)) \ll |\mathrm{Nm}\,\eta\Delta^2| G^{9d}.$$

Da ΔA genau dann positiv definit ist, wenn A definit ist, können wir Proposition 1 nutzen, um $t_0' \in \mathcal{O}$ und $\mathbf{t}' \in \mathcal{O}^3$ mit

$$t_0'^2 + \frac{\Delta}{4}A[\mathbf{t}'] = v, \qquad t_1' \equiv t_1 \quad (\widetilde{\eta}), \qquad \mathbf{t}' \equiv \mathbf{t} \quad (\widetilde{\eta})$$

zu finden, die für alle l die Abschätzung

$$\begin{aligned}\max\{|t_0'^{(l)}|, |\mathbf{t}'^{(l)}|\} &\ll \frac{|v^{(l)}|^{1/2}\left(\langle A\rangle^{24d}\,|\mathrm{Nm}\,\Delta^{28}\widetilde{\eta}^{6}|\right)^{\gamma(r_0)+\varepsilon}}{\min\{1, |\Delta^{(l)} d_i^{(l)}|\}^{1/2}} \\ &\ll \frac{|v^{(l)}|^{1/2}\left(\langle A\rangle^{24d}\,|\mathrm{Nm}\,\Delta^{40}\eta^{6}|G^{54d}\right)^{\gamma(r_0)+\varepsilon}}{\min\{1, |\Delta^{(l)} d_i^{(l)}|\}^{1/2}}\end{aligned}$$

erfüllen. Die Äquivalenzbedingung impliziert

$$R' = \frac{1}{v}\left(t_0'^2 I - \frac{\Delta}{4}A[\mathbf{t}']I + t_0'(\mathrm{adj}\,A)Z(\mathbf{t}') + \frac{\Delta}{2}\mathbf{t}'\mathbf{t}'^T A\right)S \equiv R \quad (\eta)$$

und damit insbesondere auch $R' \in \mathcal{O}^{3\times 3}$.

Außerdem folgt aus Lemma 5.3, dass $R'S^{-1}$ ein Automorphismus von A ist und somit $A[R'] = A[S] = B$ gilt.

Schließlich ergibt sich die Abschätzung

$$\begin{aligned}\|R'^{(l)}\| &\ll \max\left\{|\Delta^{(l)}|\,\langle A\rangle\,, \langle \mathrm{adj}\,A\rangle\right\}\frac{\max\{|t_0'^{(l)}|, |\mathbf{t}'^{(l)}|\}^2}{|v^{(l)}|}\,\langle S\rangle \\ &\ll \frac{\left(\langle A\rangle^{24d}\,|\mathrm{Nm}\,\Delta^{40}\eta^{6}|G^{54d}\right)^{2\gamma(r_0)+\varepsilon} G^{9d/2}}{\min\{1, |\Delta^{(l)} d_i^{(l)}|\}}.\end{aligned}$$

Damit ist die Behauptung bewiesen. □

Wir haben nun alle Fälle von Proposition 1 abgehandelt und damit den Beweis von Satz 1 vollständig geführt.

Literatur

[BF94] J. Brüdern und E. Fouvry. *Lagrange's four squares theorem with almost prime variables*. In: *J. reine angew. Math.* Bd. 454 (1994), S. 59–96.

[BM95] R.W. Bruggeman und R.J. Miatello. *Estimates of Kloosterman sums for groups of real rank one*. In: *Duke Math. J.* Bd. 80(1) (1995), S. 105–137.

[BV14] T.D. Browning und P. Vishe. *Cubic hypersurfaces and a version of the circle method for number fields*. In: *Duke Math. J.* Bd. 163(10) (2014), S. 1825–1883.

[Cas55] J.W.S. Cassels. *Bounds for the least solutions of homogeneous quadratic equations*. In: *Proc. Cambridge Philos. Soc.* Bd. 51 (1955), S. 262–264.

[Cha80a] J.H.H. Chalk. *Algebraic Lattices*. In: *C. R. Math. Rep. Acad. Sci. Canada*, Bd. 2(1) (1980), S. 5–10.

[Cha80b] J.H.H. Chalk. *Linearly Independent Zeros of Quadratic Forms over Number-Fields*. In: *Mh. Math.* Bd. 90(1) (1980), S. 13–25.

[Coc87] T. Cochrane. *Small solutions of congruences over algebraic number fields*. In: *Illinois J. Math.* Bd. 31 (1987), S. 618–625.

[DFI93] W. Duke, J. Friedlander und H. Iwaniec. *Bounds for automorphic L-functions*. In: *Invent. math.* Bd. 112 (1993), S. 1–8.

[Die03] R. Dietmann. *Small solutions of quadratic diophantine equations*. In: *Proc. London Math. Soc.* Bd. 86(3) (2003), S. 545–582.

[DMR76] M. Davis, J.V. Matijasevič und J. Robinson. *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution*. In: *Mathematical developments arising from Hilbert problems*. Bd. 28. Proc. Sympos. Pure Math. Providence RI: Amer. Math. Soc., 1976, S. 323–378.

[DPR61] M. Davis, H. Putnam und J. Robinson. *The decision problem for exponential diophantine equations*. In: *Ann. of Math. (2)*, Bd. 74 (1961), S. 425–436.

[Est62] T. Estermann. *A new application of the Hardy-Littlewood-Kloosterman Method*. In: *Proc. London Math. Soc.* Bd. 12(3) (1962), S. 425–444.

[GMR81] W.H. Gustafson, M.E. Moore und I. Reiner. *Matrix Completions Over Dedekind Rings*. In: *Linear and Multilinear Algebra*, Bd. 10(2) (1981), S. 141–144.

[Göd31] K. Gödel. *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*. In: *Monatsh. Math. Phys.* Bd. 38 (1931), S. 173–198.

[GS81] F.J. Grunewald und D. Segal. *How to solve a quadratic equation in integers*. In: *Math. Proc. Cambridge Philos. Soc.* Bd. 89(1) (1981), S. 1–5.

[Hea96] D.R. Heath-Brown. *A new form of the circle method, and its application to quadratic forms*. In: *J. reine angew. Math.* Bd. 481 (1996), S. 149–206.

[Hec54] E. Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen*. 2. Aufl. Leipzig: Akademische Verlagsgesellschaft, Geest & Portig, 1954.

[Hel12] L. Helfrich. *Search bounds for zeros of rational cubic forms*. Masterarbeit. Universität Göttingen, 2012.

[Hil00] D. Hilbert. *Mathematische Probleme*. In: *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* (1900), S. 253–297.

[Hum39] P. Humbert. *Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini*. In: *Comment. Math. Helv.* Bd. 12 (1939), S. 263–306.

[Hum49] P. Humbert. *Réduction de formes quadratiques dans un corps algébrique fini*. In: *Comment. Math. Helv.* Bd. 23 (1949), S. 50–63.

[Ica97] M.I. Icaza. *Hermite constant and extreme forms for algebraic number fields*. In: *J. London Math. Soc.* Bd. 55(1) (1997), S. 11–22.

[Iwa97] H. Iwaniec. *Topics in Classical Automorphic Forms*. Bd. 17. Grad. Stud. Math. Providence RI: Amer. Math. Soc., 1997.

[Jon80] J.P. Jones. *Undecidable Diophantine equations*. In: *Bull. Amer. Math. Soc. (N.S.)* Bd. 3 (1980), S. 859–862.

[JW56] B.W. Jones und G.L. Watson. *On indefinite ternary quadratic forms*. In: *Canad. J. Math*, Bd. 8 (1956), S. 592–608.

[Klo26] H.D. Kloosterman. *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$. In: *Acta Math.* Bd. 49(3-4) (1926), S. 407–464.

[Kor90a] D.M. Kornhauser. *On small solutions of the general nonsingular quadratic Diophantine equation in five and more unknowns.* In: *Math. Proc. Cambridge Philos. Soc.* Bd. 107 (1990), S. 197–211.

[Kor90b] D.M. Kornhauser. *On the smallest solution to the general binary quadratic equation.* In: *Acta Arith.* Bd. 55 (1990), S. 83–94.

[Mac33] C.C. MacDuffee. *The theory of matrices.* Bd. 2. Ergeb. Math. Grenzgeb. Berlin: Springer, 1933.

[Mat70] J.V. Matijasevič. *Enumerable sets are diophantine.* In: *Soviet Math. Dokl.* Bd. 11(2) (1970), S. 354–357.

[Mat77] J.V. Matijasevič. *Some purely mathematical results inspired by mathematical logic.* In: *Logic, Foundations of Mathematics, and Computability Theory.* Berlin: Springer, 1977, S. 121–127.

[Maz94] B. Mazur. *Questions of decidability and undecidability in number theory.* In: *J. Symbolic Logic*, Bd. 59 (1994), S. 353–371.

[MF80] C. Müller und W. Freeden. *Multidimensional Euler and Poisson summation formulas.* In: *Results Math.* Bd. 3 (1980), S. 33–63.

[MR10] B. Mazur und K. Rubin. *Ranks of twists of elliptic curves and Hilbert's tenth problem.* In: *Invent. Math.* Bd. 181 (2010), S. 541–575.

[Pom59] C. Pommerenke. *Über die Gleichverteilung von Gitterpunkten auf m-dimensionalen Ellipsoiden.* In: *Acta Arith.* Bd. 5 (1959), S. 227–257.

[PZ00] T. Pheidas und K. Zahidi. *Undecidability of existential theories of rings and fields: a survey.* In: *Hilbert's tenth problem: relations with arithmetic and algebraic geometry.* Bd. 270. Contemp. Math. Providence RI: Amer. Math. Soc., 2000, S. 49–105.

[Rag75] S. Raghavan. *Bounds for minimal solutions of diophantine equations.* In: *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* (1975), S. 109–114.

[Rum86] R.S. Rumely. *Arithmetic over the ring of all algebraic integers.* In: *J. Reine Angew. Math.* Bd. 368 (1986), S. 127–133.

[SB90] J. Stoer und R. Bulirsch. *Numerische Mathematik 2.* 3. Aufl. Berlin: Springer, 1990.

[Sie72] C.L. Siegel. *Zur Theorie der quadratischen Formen*. In: *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* (1972), S. 21–46.

[Ski94] C.M. Skinner. *Rational points on nonsingular cubic hypersurfaces*. In: *Duke Math. J.* Bd. 75(2) (1994), S. 409–466.

[Str99] S. Straumann. *Das Äquivalenzproblem ganzer quadratischer Formen: Einige explizite Resultate*. Diplomarbeit. Universität Basel, 1999.

[Vaa87] J.D. Vaaler. *Small zeros of quadratic forms over number fields*. In: *Trans. Amer. Math. Soc.* Bd. 302(1) (1987), S. 281–296.

[Wat60] G.L. Watson. *Integral quadratic forms*. Cambridge Tracts Math. Math. Phys. 51. New York: Cambridge University Press, 1960.