Perfekte Gitter über imaginärquadratischen Zahlkörpern

Oliver Braun

Bachelorarbeit im Fach Mathematik

RWTH Aachen
Lehrstuhl D für Mathematik
Prof. Dr. Gabriele Nebe

Inhaltsverzeichnis

1. Einleitung **5**
1.1. Notationen und Konventionen 6
1.2. Gitter 10

2. Der Satz von Voronoi **15**
2.1. Grundlagen 15
2.2. Perfektion und Eutaxie 16

3. Der Voronoi-Algorithmus für Körper mit Klassenzahl 1 **20**
3.1. Grundlagen 20
3.2. Ergebnisse in Dimension 2 21

4. Größere Klassenzahlen **22**
4.1. Definitionen 22
4.2. Spurform und Abschätzungen 26
4.3. Perfektion und Eutaxie 29
4.4. Charakterisierung extremer Formen 33
4.5. Der Voronoi-Algorithmus 39
4.5.1. Voronoi-Bereiche 39
4.5.2. Implementierung 43

A. Rechnerische Ergebnisse in Dimension 2 **45**
A.1. $\mathbb{Q}(\sqrt{-5})$ 45
A.2. $\mathbb{Q}(\sqrt{-6})$ 47
A.3. $\mathbb{Q}(\sqrt{-10})$ 48
A.4. $\mathbb{Q}(\sqrt{-15})$ 50
A.5. $\mathbb{Q}(\sqrt{-21})$ 51
A.6. $\mathbb{Q}(\sqrt{-23})$ 55

B. Rechnerische Ergebnisse in Dimension 3 **56**
B.1. $h_K = 2$ 56
B.2. $h_K = 3$ 57

C. Quellcode der Implementierung **59**

D. Eigenständigkeitserklärung **74**

Literaturverzeichnis **75**

1. Einleitung

Die klassische Gittertheorie über dem Ring der ganzen Zahlen befasst sich, neben weiteren vielfältigen Problemstellungen, mit der Suche nach solchen Gittern, die eine möglichst dichte Kugelpackung in einem n-dimensionalen Euklidischen Vektorraum liefern. Um dieses Problem zu behandeln, interpretiert man die Gitterpunkte eines $\mathbb{Z}$-Gitters L als Mittelpunkte von Kugeln, deren Radien jeweils identisch und gerade so groß gewählt werden, dass je zwei Kugeln sich nicht überlappen. Proportional zur Dichte der auf diese Weise konstruierten Kugelpackung ist die Hermite-Invariante

$$\gamma(L) = \frac{\min(L)}{(\det(L))^{1/n}}$$

Dabei bezeichnet $\min(L)$ die minimale Länge eines von Null verschiedenen Gittervektors, $\det(L)$ ist die Determinante einer Gram-Matrix des Gitters.
Die gestellte Aufgabe besteht also darin, lokale Maxima von γ auf der Menge aller n-dimensionalen Gitter aufzufinden. Dieser Aufgabe nehmen sich am Ende des neunzehnten Jahrhunderts zuerst die Mathematiker Korkine und Zolotareff an, die in ihren Veröffentlichungen „Sur les formes quadratiques“ (1873) und „Sur les formes quadratiques positives“ (1877) erstmals von „extremen“ Gittern beziehungsweise quadratischen Formen sprechen und damit gerade die lokalen Maxima von γ meinen. Nach dieser Vorarbeit erscheint im Jahre 1908 die Arbeit „Nouvelles applications des paramètres continus à la théorie des formes quadratiques : 1 Sur quelques propriétés des formes quadratiques positives parfaites“ von Grigori Voronoi, die das Problem der Suche nach extremen Gittern auf der theoretischen Ebene löst. Voronoi definiert zwei Eigenschaften, nämlich Perfektion und Eutaxie (wobei die zweite Bezeichnung auf Coxeter (1951) zurückgeht) und beweist, dass die extremen Gitter gerade diejenigen sind, die perfekt und eutaktisch sind. Ferner legt er dar, dass es - bei Festlegung einer geeigneten Äquivalenzrelation - nur endlich viele Klassen perfekter Gitter gibt. Zur Suche nach extremen Gittern bestimmt man also zunächst die perfekten Gittern und testet diese auf Eutaxie. Diese Tatsache ist vor allem deswegen interessant, weil Voronois Arbeit überdies einen Algorithmus von geometrischer Natur enthält, der alle perfekten Gitter in einer gegebenen Dimension auflistet. Jedoch wächst die Komplexität dieses Algorithmus mit der Dimension so rasant, dass er sich nur bis zur Dimension 7 effektiv durchführen lässt. In Dimension 8 lässt sich der Algorithmus nicht mehr in seiner ursprünglichen Form durchführen. So sorgt etwa

das achtdimensionale Gitter $\mathbb{E}_8$ dafür, dass man zur Durchführung des Algorithmus ein Polytop mit 25075566937584 Seitenflächen zu untersuchen hat. In diesem Fall muss man theoretische Resultate über die Struktur von $\mathbb{E}_8$ zum Einsatz bringen, um Rechenzeit einzusparen.
Nichtsdestoweniger war Voronois Arbeit maßgeblich für die weitere Entwicklung der Gittertheorie und der vorgestellte Algorithmus hat, trotz des Rechenaufwands, zur Entdeckung aller perfekten Gitter in den Dimensionen 1 bis 8 geführt.

Die vorliegende Arbeit hat das Ziel, die von Voronoi entwickelte Theorie auf Gitter über den Ganzheitsringen imaginärquadratischer Zahlkörper mit Klassenzahl größer 1 zu übertragen. Es wird dazu auf Definitionen von R. Coulangeon zurückgegriffen, die sich in [Cou04] finden. Aufbauend auf diesen Definitionen werden ähnliche Resultate wie in der klassischen Gittertheorie bewiesen: unter Festlegung einer geeigneten Äquivalenzrelation existieren nur endlich viele Klassen perfekter Hermitescher Formen, die extremen Hermiteschen Formen sind wiederum diejenigen, die perfekt und eutaktisch sind und schließlich wird der Voronoische Algorithmus verwendet, um perfekte Hermitesche Formen über imaginärquadratischen Zahlkörpern aufzulisten.
Eine Schwierigkeit besteht darin, dass der Ganzheitsring eines Zahlkörpers mit mindestens zwei Idealklassen kein Hauptidealbereich mehr ist, sodass auch nichtfreie Gitter existieren. So kann nicht in jeder Situation eine Gitterbasis gewählt werden. Jedoch gestattet die Interpretation der Gitter des Ganzheitsrings als $\mathbb{Z}$-Gitter den Rückgriff auf Voronois wegweisende Arbeit. Ein zentrales Hilfsmittel beim Verfassen dieser Arbeit war zudem die Dissertation [Mey08] von B. Meyer, die den Voronoi-Algorithmus für imaginärquadratische Zahlkörper mit Klassenzahl 1 enthält.
Das erste Kapitel präsentiert die benötigten Grundlagen aus der algebraischen Zahlentheorie und der Modultheorie für Dedekindringe. Die zwei darauffolgenden Kapitel wiederholen die klassische Voronoi-Theorie über den ganzen Zahlen und über Ganzheitsringen imaginärquadratischer Zahlkörper mit Klassenzahl 1. Das vierte Kapitel, in welchem die Theorie für Körper mit mehreren Idealklassen entwickelt wird, bildet das Herzstück der Arbeit.

Mein Dank gilt meiner Betreuerin Frau Prof. Dr. Gabriele Nebe, die auf meine Fragen stets eine Antwort wusste. Ich bin zudem B. Meyer zu Dank verpflichtet, der mir den Quellcode seines Voronoi-Algorithmus in Magma [BCP97] zur Verfügung gestellt hat.

1.1. Notationen und Konventionen

Wir verwenden in dieser Arbeit die folgenden Bezeichnungen.

$\mathscr{S}_n$ für die Menge aller symmetrischen $n \times n$-Matrizen mit Einträgen aus $\mathbb{R}$. Darin $\mathscr{S}_n^+$ die Menge aller postiv definiten symmetrischen Matrizen.
Für ein $A \in \mathbb{R}^{n\times n}$ bezeichne A^T die transponierte Matrix. Analog verwenden wir diese Bezeichnung für Zeilen- und Spaltenvektoren.

$\mathcal{H}_n$ soll für die Menge aller Hermiteschen $n \times n$-Matrizen mit Einträgen aus $\mathbb{C}$ stehen, $\mathcal{H}_n^+$ bezeichne die Teilmenge aller positiv definiten Hermiteschen $n \times n$-Matrizen.
Für $A \in \mathbb{C}^{n\times n}$ sei A^* die adjungierte Matrix, d.h. die transponierte und eintragsweise komplex-konjugierte Matrix. Auch diese Bezeichnung weiten wir auf Vektoren mit komplexen Einträgen aus.

Ist $\mathcal{A} \in \mathscr{S}_n$ oder $\mathcal{A} \in \mathcal{H}_n$ und x ein Zeilenvektor der Länge n, so definieren wir $\mathcal{A}[x] := x\mathcal{A}x^T$ im reellen Fall und $\mathcal{A}[x] := x\mathcal{A}x^*$ im komplexen Fall.
Gleichsam schreiben wir $\mathcal{A}[B] := B\mathcal{A}B^T$ beziehungsweise $\mathcal{A}[B] := B\mathcal{A}B^*$ für $B \in \mathbb{R}^{n\times n}$ beziehungsweise $B \in \mathbb{C}^{n\times n}$.

Mengen der Gestalt K^n, $\mathbb{R}^n$, $\mathbb{C}^n$, $\mathbb{Z}^n$ etc. sollen stets als Mengen von Zeilen mit n Einträgen verstanden werden.

Definition 1.1.1 *Sei R ein Ring mit 1 und P ein R-Modul. Dann heißt P ein projektiver R-Modul, falls eine der folgenden äquivalenten Bedingungen erfüllt ist.*

1. *Jede kurze exakte Sequenz von R-Moduln*

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

   spaltet.

2. *Für jeden surjektiven Homomorphismus $f : M \to N$ von R-Moduln und jeden Homomorphismus $g : P \to N$ von R-Moduln gibt es einen R-Modulhomomorphismus $\varphi : P \to M$, sodass $g = f \circ \varphi$.*

Es sei auch angemerkt, dass ein R-Modul genau dann projektiv ist, wenn er ein direkter Summand eines freien R-Moduls ist.

Definition 1.1.2 *Sei $K/\mathbb{Q}$ eine Körpererweiterung vom Grad 2 und $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ die Menge der Einbettungen von K in $\overline{\mathbb{Q}} \subset \mathbb{C}$. Nehmen diese Einbettungen nur Werte in $\mathbb{R}$ an, so nennt man K einen reellquadratischen Zahlkörper, anderenfalls heißt K imaginärquadratischer Zahlkörper.*

Die Menge $\mathbb{Z}_K := \{x \in K \mid x \text{ ganz über } \mathbb{Z}\}$ ist ein Teilring von K, der Ganzheitsring (vgl. [Neu07]). Dieser Ring ist ein Dedekindring, was bedeutet, dass jedes Ideal

$\{0\} \neq \mathfrak{I} \trianglelefteq \mathbb{Z}_K$ *eine eindeutige Zerlegung in ein Produkt von Primidealen besitzt.*
Dazu äquivalent ist, dass $\mathbb{Z}_K$ *ein höchstens eindimensionaler Noetherscher ganzabgeschlossener Integritätsring ist.*

Definition 1.1.3 *Sei* $K/\mathbb{Q}$ *ein algebraischer Zahlkörper mit Ganzheitsring* $\mathbb{Z}_K$*. Ein endlich erzeugter* $\mathbb{Z}_K$*-Teilmodul von* K*, der nicht der Nullmodul ist, heißt ein gebrochenes Ideal von* K*. Die gebrochenen Ideale bilden bezüglich der Multiplikation*

$$\mathfrak{ab} := \{\sum_i a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\}$$

eine abelsche Gruppe I_K*. Die Menge* J_K *der gebrochenen Hauptideale bildet in* I_K *eine Untergruppe.*

Die Faktorgruppe $I_K/J_K =: \mathcal{C}\ell_K$ *heißt die Idealklassengruppe von* K*.* $h_K := [I_K : J_K]$ *nennen wir die Klassenzahl des Zahlkörpers* K*.*

Satz 1.1.4 *Die Klassenzahl eines Zahlkörpers ist endlich.*

Beweis: [Neu07, I, (6.3) Theorem]. □

Genauer haben wir stets die folgende exakte Sequenz.

$$1 \longrightarrow \mathbb{Z}_K^* \longrightarrow K^* \longrightarrow I_K \longrightarrow \mathcal{C}\ell_K \longrightarrow 1$$

Zudem verwenden wir noch die folgende übliche Definition.

Definition 1.1.5 *Sei* $\mathfrak{a} \trianglelefteq \mathbb{Z}_K$ *ein ganzes Ideal, also ein Ideal in* $\mathbb{Z}_K$ *im üblichen Sinne. Dann definieren wir die Idealnorm von* $\mathfrak{a}$ *als* $N(\mathfrak{a}) := |\mathbb{Z}_K/\mathfrak{a}|$*.*
Die Idealnorm ist multiplikativ auf den ganzen Idealen (siehe [Neu07]). Da die eindeutige Primfaktorzerlegung ganzer Ideale auf alle gebrochenen Ideale eines Zahlkörpers ausgedehnt werden kann, lässt sich auch die Idealnorm entsprechend multiplikativ fortsetzen (vgl. [Neu07]).

Genauere Einsichten in die Struktur der Einheitengruppe $\mathbb{Z}_K^*$ liefert der folgende Satz von Dirichlet.

Satz 1.1.6 (Dirichletscher Einheitensatz) *Sei* $K/\mathbb{Q}$ *ein algebraischer Zahlkörper und es sei ferner* $[K : \mathbb{Q}] = n = r + 2s$*, wobei* r *die Anzahl der reellwertigen Einettungen von* K *in* $\overline{\mathbb{Q}}$ *bezeichne;* s *stehe für die Anzahl der Paare zueinander konjugierter komplexer Einbettungen. In dieser Sitution ist die Gruppe* $\mathbb{Z}_K^*$ *endlich erzeugt. Ihr freier Anteil*

hat den Rang $r+s-1$, ihr Torsionsanteil ist die Gruppe $\mu(K)$ der in K enthaltenen Einheitswurzeln, sodass

$$\mathbb{Z}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

Beweis: [Neu07, I, (7.4) Theorem] □

Wir werden nun einige wichtige Strukturaussagen über gebrochene Ideale eines Zahlkörpers notieren.

Lemma 1.1.7 *Ist $K/\mathbb{Q}$ ein algebraischer Zahlkörper und sind $\mathfrak{a}$, $\mathfrak{b}$ gebrochene Ideale in K, so existieren $x, y \in K$ mit der Eigenschaft, dass $x\mathfrak{a}$ und $y\mathfrak{b}$ ganz und teilerfremd sind.*

Beweis: Geeignete $x, y \in K$ erhält man aus dem chinesischen Restsatz. □

Korollar 1.1.8 *Sei $K/\mathbb{Q}$ ein algebraischer Zahlkörper und $\mathfrak{a}$, $\mathfrak{b}$ gebrochene Ideale in K, so ist $\mathfrak{a} \oplus \mathfrak{b} \cong \mathbb{Z}_K \oplus \mathfrak{ab}$. Insbesondere ist $\mathfrak{a}$ ein projektiver $\mathbb{Z}_K$-Modul.*

Beweis: Das letzte Lemma gestattet es uns, $\mathfrak{a}$ und $\mathfrak{b}$ ohne Einschränkung als ganz und teilerfremd anzunehmen, da Multiplikation von gebrochenen Idealen mit Elementen von K sicherlich einen $\mathbb{Z}_K$-Modulisomorphismus definiert.

Der Homomorphismus $\mathfrak{a} \oplus \mathfrak{b} \to \mathbb{Z}_K,\ (a,b) \mapsto a+b$ ist also surjektiv;
sein Kern ist $\{(a,b) \in \mathfrak{a} \oplus \mathfrak{b} \mid a = -b\} = \{(a,-a) \in \mathfrak{a} \oplus \mathfrak{b} \mid a \in \mathfrak{a} \cap \mathfrak{b}\} \cong \mathfrak{a} \cap \mathfrak{b}$.
Die folgende Sequenz von Moduln ist also exakt.

$$0 \longrightarrow \mathfrak{a} \cap \mathfrak{b} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \longrightarrow \mathbb{Z}_k \longrightarrow 0$$

Da $\mathbb{Z}_K$ frei, also insbesondere projektiv ist, spaltet die obige Sequenz, sodass $\mathfrak{a} \oplus \mathfrak{b} \cong \mathbb{Z}_K \oplus (\mathfrak{a} \cap \mathfrak{b})$. Da $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind, gilt $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$; dies zeigt die Behauptung.

Hieraus ergibt sich sofort $\mathbb{Z}_K^2 \cong \mathbb{Z}_K \oplus \mathfrak{a}\mathfrak{a}^{-1} \cong \mathfrak{a} \oplus \mathfrak{a}^{-1}$, $\mathfrak{a}$ ist also direkter Summand eines freien Moduls und somit projektiv. □

Interessant ist für uns später noch, gebrochene Ideale eines Zahlkörpers als Moduln über dem Ring $\mathbb{Z}$ der ganzen Zahlen zu betrachten. Dazu formulieren wir das folgende

Lemma 1.1.9 *Ist $n := [K : \mathbb{Q}] < \infty$, so ist jedes gebrochene Ideal $\mathfrak{a}$ von K ein freier $\mathbb{Z}$-Modul vom Rang n.*

Beweis: Sicherlich ist $\mathbb{Z}_K$ ein freier, da torsionsfreier, $\mathbb{Z}$-Modul vom Rang n. Nun gilt für beliebiges $0 \neq a \in \mathfrak{a}$:

$$a\mathbb{Z}_K \subseteq \mathfrak{a} \subseteq \mathbb{Z}_K$$

Die Behauptung folgt, da $a\mathbb{Z}_K \cong \mathbb{Z}_K$. □

1.2. Gitter

In diesem Abschnitt sei stets $K/\mathbb{Q}$ ein imaginärquadratischer Zahlkörper und n eine natürliche Zahl.

Definition 1.2.1 *Ein Gitter L in K^n ist ein endlich erzeugter $\mathbb{Z}_K$-Teilmodul von K^n mit der Eigenschaft $K \otimes L \cong K^n$. Als torsionsfreier Modul über einem Dedekindring ist ein Gitter insbesondere ein projektiver Modul.*

Da die gebrochenen Ideale eines Zahlkörpers projektive Moduln über dem Ganzheitsring sind, sind die eindimensionalen Gitter über einem imaginärquadratischen Zahlkörper gerade die gebrochenen Ideale.

Satz 1.2.2 *Sei L ein Gitter in K^n. Dann gibt es eine Basis $(v_1, ..., v_n)$ von K^n und gebrochene Ideale $\mathfrak{a}_1, ..., \mathfrak{a}_n$ von K, sodass $L \cong \mathfrak{a}_1 v_1 \oplus ... \oplus \mathfrak{a}_n v_n$. Ebenso gibt es eine Basis $(u_1, ..., u_n)$ von K^n und ein gebrochenes Ideal $\mathfrak{a}$ in K, sodass $L \cong \mathbb{Z}_K u_1 \oplus ... \oplus \mathbb{Z}_K u_{n-1} + \mathfrak{a} u_n$.*

Beweis: Der Beweis der ersten Aussage findet sich in [O'M00, 81:3 Theorem].

Hat man $L \cong \bigoplus_{i=1}^{n} \mathfrak{a}_i$, so erhält man $L \cong \mathbb{Z}_K^{n-1} \oplus (\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_n)$ durch vollständige Induktion aus 1.1.7. □

Mit den obigen Bezeichnungen nennen wir $[\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_n] = [\mathfrak{a}] \in \mathcal{C}\ell_K$ die Steinitzklasse von L, kurz $\mathrm{St}(L)$.

Satz 1.2.3 (Steinitz) *Zwei $\mathbb{Z}_K$-Moduln $L = I_1 \oplus ... \oplus I_n$, $L' = I'_1 \oplus ... \oplus I'_m$ sind genau dann isomorph, wenn $m = n$ und wenn sie der gleichen Steinitzklasse angehören.*

Beweis: Ist $\varphi : M \to N$ ein $\mathbb{Z}_K$-Modulisomorphismus, so erhält man sofort

$$n = \dim_K(K \otimes (I_1 \oplus ... \oplus I_n)) = \dim_K(K \otimes (I_1' \oplus ... \oplus I_m')) = m$$

Durch Multiplikation mit geeigneten Elementen in K^* dürfen wir ohne Einschränkung annehmen, dass $I_i \supseteq \mathbb{Z}_K^*$ und $I_i' \supseteq \mathbb{Z}_K^*$ für alle $1 \leq i \leq n$ gilt, denn sicherlich ist die Multiplikation mit einem Element aus K^* ein $\mathbb{Z}_K$-Modulisomorphismus.
Die Bilder der $1 \in I_i$ unter φ seien mit $(a_{i,1}, ..., a_{i,n})$ bezeichnet, die Bilder der $1 \in I_i'$ unter der Umkehrabbildung mit $(b_{i,1}, ..., b_{i,n})$. Fasst man diese Zeilen jeweils zu Matrizen A und B zusammen, so erhält man, dass das Produkt AB gerade I_n, die $n \times n$-Einheitsmtrix, ergibt. Dies lässt sich leicht einsehen, indem man abermals durch Tensorieren mit K zu $K \otimes L \cong K^n$ übergeht. Dort beschreiben A und B offensichtlich zueinander inverse Automorphismen.
Folglich ist $\det A = (\det B)^{-1}$.

Wir behaupten nun $a_{i,j} I_i \subseteq I_j'$ für alle Kombinationen von i und j. Sei dazu $x_i \in I_i$ und es sei ferner $\tau \in \mathbb{Z}_K$ sodass $\tau x_i \in \mathbb{Z}_K$. Das Bild von x_i unter φ sei $(\ell_1, ..., \ell_n)$. Dann gilt einerseits

$$\varphi(\tau \cdot (0, ..., 0, x_i, 0, ..., 0)) = \tau \cdot (\ell_1, ..., \ell_n),$$

andererseits haben wir

$$\varphi((\tau \cdot x_i) \cdot (0, ..., 0, 1, 0, ..., 0)) = (\tau \cdot x_i) \cdot (a_{i,1}, ..., a_{i,n}).$$

Wir erhalten daraus sofort $\tau x_i a_{i,j} = \tau \ell_j$, also $x_i a_{i,j} = \ell_j \in I_j'$, wie behauptet.
Analog erhält man $b_{i,j} I_i' \subseteq I_j$.

Aus der obigen Behauptung folgt

$$\prod_{i=1}^{n} I_i' \supseteq a_{1,\pi(1)} \cdot ... \cdot a_{n,\pi(n)} \prod_{i=1}^{n} I_i$$

für alle $\pi \in S_n$. Also insbesondere

$$\prod_{i=1}^{n} I_i' \supseteq \det(A) \prod_{i=1}^{n} I_i \supseteq \det(A)\det(B) \prod_{i=1}^{n} I_i' = \prod_{i=1}^{n} I_i'$$

Also $\mathrm{St}(L) = \mathrm{St}(L')$.

Ist umgekehrt $m = n$ und $\mathrm{St}(L) = \mathrm{St}(L')$, so erhält man die Isomorphie von L und L' durch Anwendung von 1.1.7. □

Bemerkung 1.2.4 *Sind $I_1, ..., I_n$ gebrochene Ideale, so hat jeder Isomorphismus zwischen $L := I_1 \oplus ... \oplus I_n$ und $\mathbb{Z}_K^{n-1} \oplus I_1 \cdot ... \cdot I_n$ eine Determinante in $\mathbb{Z}_K^*$.*

Beweis: Wir verwenden 1.2.5 und ohne Einschränkung sei $n = 2$. Die Behauptung für beliebiges n erhalten wir dann durch Hintereinanderausführung solcher Isomorphismen, die jeweils zwei der direkten Summanden von $I_i \oplus I_{i+1}$ in $\mathbb{Z}_K \oplus I_i I_{i+1}$ überführen.
Sei φ der angegebene Isomorphismus mit Umkehrabbildung φ^{-1}. Indem wir diese Abbildungen sofort in ihrer Matrixschreibweise auffassen, erhalten wir

$$\varphi \in \begin{pmatrix} I_1^{-1} & I_2 \\ I_2^{-1} & I_1 \end{pmatrix}, \quad \varphi^{-1} \in \begin{pmatrix} I_1 & I_2 \\ I_2^{-1} & I_1^{-1} \end{pmatrix}$$

Für die Determinanten erhalten wir sofort

$$\det(\varphi) \in I_1^{-1} I_1 + I_2^{-1} I_2 \subseteq \mathbb{Z}_K, \ \det(\varphi^{-1}) \in I_1 I_1^{-1} + I_2^{-1} I_2 \subseteq \mathbb{Z}_K$$

Wegen $\det(\varphi) \cdot \det(\varphi^{-1}) = 1$ muss $\det(\varphi)$ eine Einheit sein. □

Im Folgenden werden wir Endomorphismenringe und Automorphismengruppen von $\mathbb{Z}_K$-Gittern untersuchen. Aufschluss über die Endomorphismen gibt uns die folgende Aussage.

Lemma 1.2.5 *Sind $M = I_1 \oplus ... \oplus I_n$ und $N = J_1 \oplus ... \oplus J_n$ $\mathbb{Z}_K$-Gitter in K^n, wobei die I_i und J_i gebrochene Ideale seien, so gilt*

1. $\mathrm{Hom}_{\mathbb{Z}_K}(I_i, J_j) \cong J_j \cdot I_i^{-1}$

2. $\mathrm{Hom}_{\mathbb{Z}_K}(M, N) \cong \{(\varphi_{ij})_{i,j=1}^n \mid \varphi_{ij} \in \mathrm{Hom}_{\mathbb{Z}_K}(I_i, J_j)\}$, *wenn wir mit Zeilen von links multiplizieren.*

Beweis:

1. Jedes $\varphi \in \mathrm{Hom}_{\mathbb{Z}_K}(I_i, J_j)$ liefert einen eindeutigen K-linearen Homomorphismus $K \to K$, sodass ein $\alpha \in K$ existiert mit $\varphi(x) = \alpha x$ für alle $x \in I_i$. Damit $\varphi(I_i) \subseteq J_j$ gilt, muss $\alpha \in J_j \cdot I_i^{-1}$ gelten.

2. Dies ist klar aufgrund der direkten Summenzerlegung von M und N.

□

Korollar 1.2.6 *Ist $L = \mathbb{Z}_K^{n-1} \oplus \mathfrak{a}$, so ist*

$$\mathrm{End}_{\mathbb{Z}_K}(L) \cong \left(\begin{array}{ccc|c} & \mathbb{Z}_K^{(n-1)\times(n-1)} & & \mathfrak{a} \\ & & & \vdots \\ & & & \mathfrak{a} \\ \hline \mathfrak{a}^{-1} & ... & \mathfrak{a}^{-1} & \mathbb{Z}_K \end{array}\right)$$

Wir halten in dieser Situation noch eine Aussage über die Determinante eines Endomorphismus von $L = \mathbb{Z}_K^{n-1} \oplus \mathfrak{a}$ fest.

Lemma 1.2.7 *Ist $A \in \mathrm{End}_{\mathbb{Z}_K}(L)$, so ist $\det(A) \in \mathbb{Z}_K$.*

Beweis: $\mathrm{End}_{\mathbb{Z}_K}(L)$ ist eine $\mathbb{Z}_K$-Ordnung und besteht somit aus ganzen Elementen. Insbesondere ist die Determinante jeweils ganz. □

Nun möchten wir feststellen, was $(\mathrm{End}_{\mathbb{Z}_K}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a}))^* = \mathrm{Aut}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a})$ ist. Aus dem letzten Lemma erhalten wir eine Antwort.

Satz 1.2.8 *Es ist*

$$\mathrm{Aut}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a}) \cong \left\{ A \in \mathrm{End}_{\mathbb{Z}_K}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a}) \mid \det A \in \mathbb{Z}_K^* \right\}$$

Beweis: Sei $A \in \mathrm{End}_{\mathbb{Z}_K}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a})$, sodass A^{-1} ebenfalls in dieser Menge liege. Dann haben sowohl A als auch A^{-1} in $\mathbb{Z}_K$ gelegene Determinanten, die sich gegenseitig invertieren. Also $\det A \in \mathbb{Z}_K^*$.
Umgekehrt sei $A \in \mathrm{End}_{\mathbb{Z}_K}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a})$ und $\det(A) \in \mathbb{Z}_K^*$. Da $\mathrm{End}_{\mathbb{Z}_K}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a})$ eine $\mathbb{Z}_K$-Ordnung in $K^{n\times n}$ ist, hat A ein Minimalpolynom mit Koeffizienten in $\mathbb{Z}_K$. Wegen $\det(A) \in \mathbb{Z}_K^*$ erhalten wir also A^{-1} als Polynom A, multipliziert mit einer Einheit von $\mathbb{Z}_K$, sodass $A^{-1} \in \mathrm{End}_{\mathbb{Z}_K}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a})$. □

Schließlich werden wir noch eine Aussage über die Endlichkeit gewisser Mengen in Gittern zeigen. Es seien dazu Einbettungen $K \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ fixiert.

Lemma 1.2.9 *Ist $K/\mathbb{Q}$ imaginärquadratisch, so ist $\mathbb{Z}_K$ diskret in $\mathbb{C}$. Somit ist auch jedes ganze Ideal $\mathfrak{a} \subseteq \mathbb{Z}_K$ diskret in $\mathbb{C}$.*

Beweis: Es ist $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega \in \mathbb{C} - \mathbb{R}$. Da $(1, \omega)$ linear unabhängig ist, ist $\mathbb{Z}_K$ ein Gitter im Sinne von [Mar03], sodass die Behauptung aus [Neu07, I, (4.2) Satz] folgt. □

Bemerkung 1.2.10 *Diese Aussage bleibt richtig, falls $\mathfrak{a}$ ein beliebiges gebrochenes Ideal von K ist. Zu jedem gebrochenen Ideal $\mathfrak{a}$ existiert nämlich ein ganzes Ideal $\tilde{\mathfrak{a}}$, sodass $\mathfrak{a} = \kappa\tilde{\mathfrak{a}}$ für ein $\kappa \in K^*$. Der $\mathbb{Z}_K$-Modulisomorphismus $\mathfrak{a} \to \tilde{\mathfrak{a}}$, $x \mapsto \kappa x$ ist ein Homöomorphismus, sodass $\mathfrak{a}$ genau wie $\tilde{\mathfrak{a}}$ diskret in $\mathbb{C}$ ist.*

Die folgende Bemerkung ist klar ob der Äquivalenz der Normen auf $\mathbb{C}^n$.

Bemerkung 1.2.11 *Ist $\mathcal{A} \in \mathcal{H}_n^+$, so ist für jedes $\mu \in \mathbb{R}_{>0}$ die Menge*

$$\{x \in \mathbb{C}^n \mid \mathcal{A}[x] \leq \mu\}$$

kompakt.

Korollar 1.2.12 *Ist $L = \mathbb{Z}_K^{n-1} \oplus \mathfrak{a}$ mit einem $\mathfrak{a} \trianglelefteq \mathbb{Z}_K$, so ist für jedes $\mu \in \mathbb{R}_{>0}$ die Menge*

$$\{x \in L \mid \mathcal{A}[x] \leq \mu\} = L \cap \{x \in \mathbb{C}^n \mid \mathcal{A}[x] \leq \mu\}$$

endlich.

2. Der Satz von Voronoi

2.1. Grundlagen

Die klassische Gittertheorie über dem Körper $\mathbb{Q}$ der rationalen Zahlen ist eng verbunden mit der Suche nach dichten Kugelpackungen in einem Euklidischen Raum. Hat man ein $\mathbb{Z}$-Gitter im Euklidischen Raum $(\mathbb{R}^n,\ (\ ,\ ))$ vorliegen, so kann man jeden Gitterpunkt als Mittelpunkt einer Kugel auffassen. Ein wichtiger Bestandteil der Gittertheorie ist die Suche nach solchen Gittern, die auf diese Weise eine möglichst dichte regelmäßige Kugelpackung liefern.
Wir zitieren im Folgenden einige wichtige Resultate, welche die Suche nach solchen Gittern ermöglichen. Zuvor beginnen wir mit einigen Definitionen und Begriffen.

Bemerkung 2.1.1 *Da $\mathbb{Z}$ ein Hauptidealbereich ist, ist jeder projektive Modul frei. Mit anderen Worten ist jedes $\mathbb{Z}$-Gitter ein freier Modul, also das $\mathbb{Z}$-lineare Erzeugnis einer Basis des $\mathbb{R}^n$.*

Es sei im Folgenden L ein $\mathbb{Z}$-Gitter im $\mathbb{R}^n$ mit Gitterbasis $(b_1, ..., b_n)$. Dann nennen wir

$$\mathrm{Gram}(L)_{i,j} := (b_i, b_j)$$

die Gram-Matrix von L. Im vorliegenden Fall ist L eindeutig durch $\mathrm{Gram}(L) \in \mathscr{S}_n^+$ festgelegt, sodass wir im Folgenden nur noch mit Matrizen arbeiten werden. Diese können wir auch als Darstellungsmatrizen quadratischer Formen verstehen.

Von nun an sei also $\mathcal{A} \in \mathscr{S}_n$. Dann definieren wir

$$\min(\mathcal{A}) := \min\{\mathcal{A}[x] \mid x \in \mathbb{Z}^n - \{0\}\}$$

als das Minimum von $\mathcal{A}$ und

$$S(\mathcal{A}) := \{x \in \mathbb{Z}^n \mid \mathcal{A}[x] = \min \mathcal{A}\}$$

Wir nennen zwei quadratische Formen, also zwei Matrizen $\mathcal{A}, \mathcal{B} \in \mathscr{S}_n^+$, ähnlich, falls es ein $a \in \mathbb{R}_{>0}$ und ein $T \in \mathrm{GL}_n(\mathbb{Z})$ gibt, sodass

$$\mathcal{A} = aT\mathcal{B}T^T$$

Die Menge der Ähnlichkeitsklassen positiv definiter quadratischer Formen ist also die Menge der Doppelnebenklassen $\mathbb{R}_{>0} \setminus \mathscr{S}_n^+ / \mathrm{GL}_n(\mathbb{Z})$.

Auf der Menge der positiv definiten quadratischen Formen definieren wir die Hermite-Funktion

$$\gamma \ : \ \mathscr{S}_n^+ \to \mathbb{R}_{>0}, \ \mathcal{A} \mapsto \frac{\min \mathcal{A}}{(\det \mathcal{A})^{1/n}}$$

Diese ist sicherlich auch vertreterweise eine Funktion auf $\mathbb{R}_{>0} \setminus \mathscr{S}_n^+ / \mathrm{GL}_n(\mathbb{Z})$.

Die Hermite-Konstante in Dimension n definieren wir als

$$\gamma_n := \sup_{\mathcal{A} \in \mathscr{S}_n^+} \gamma(\mathcal{A})$$

2.2. Perfektion und Eutaxie

Die Beweise der Sätze und Lemmata in diesem Abschnitt werden nicht ausgeführt. Sie finden sich in [Mar03].

Bemerkung 2.2.1 *$\mathscr{S}_n$ wird durch*

$$\mathscr{S}_n \times \mathscr{S}_n \to \mathbb{R}, \ (\mathcal{A}, \mathcal{B}) \mapsto \mathrm{Spur}(\mathcal{A}\mathcal{B})$$

zu einem Euklidischen Vektorraum. Insbesondere haben wir dadurch also eine Topologie auf $\mathscr{S}_n$.

Definition 2.2.2 *Wir nennen $\mathcal{A} \in \mathscr{S}_n$ extrem, falls $\mathcal{A}$ ein lokales Maximum der Hermite-Funktion γ ist.*

Gemäß [Mar03] taucht der Begriff der extremen quadratischen Form zuerst im Jahr 1873 bei Korkine und Zolotareff auf. 1908 stellte dann Voronoi eine Charakterisierung extremer Gitter und einen Algorithmus vor, der die Berechnung der Ähnlichkeitsklassen solcher Formen gestattet. Diese Resultate werden wir im Folgenden darlegen.

Definition 2.2.3 *Wir nennen $\mathcal{A}$ perfekt, falls die Menge*

$$\{x^T x \mid x \in S(\mathcal{A})\}$$

den Raum $\mathscr{S}_n$ erzeugt.
$\mathcal{A}$ soll eutaktisch heißen, falls es zu jedem $x \in S(\mathcal{A})$ Koeffizienten $\lambda_x \in \mathbb{R}_{>0}$ gibt

$$\mathcal{A}^{-1} = \sum_{x \in S(\mathcal{A})} \lambda_x x^T x$$

Diese zwei Definitionen offenbaren ihre Sinnhaftigkeit im folgenden Satz.

Satz 2.2.4 (Voronoi) *Eine Form $\mathcal{A} \in \mathscr{S}_n^+$ ist genau dann extrem, wenn sie perfekt und eutaktisch ist.*

Voronoi stellte außerdem fest, dass es nur endlich viele Ähnlichkeitsklassen perfekter Formen in jeder gegebenen Dimension gibt. Durch das Studium der folgenden Mengen, der heute nach ihm benannten Voronoi-Bereiche, konnte er einen Algorithmus angeben, welcher diese endlich vielen Klassen auflistet.

Definition 2.2.5 *Sei $\mathcal{A} \in \mathscr{S}_n^+$. Dann heißt*

$$\mathcal{V}(\mathcal{A}) := \{ \sum_{x \in S(\mathcal{A})} a_x \cdot x^T x \mid a_x \in \mathbb{R}_{\geq 0}\}$$

der Voronoi-Bereich von $\mathcal{A}$.
Ist $\mathcal{A}$ perfekt, so ist $\dim(\langle \mathcal{V}(\mathcal{A}) \rangle) = \dim(\mathscr{S}_n)$.

Zu untersuchen sind nun insbesondere die Seitenflächen und Seitenvektoren.

Definition 2.2.6 *Sei $\mathcal{A} \in \mathscr{S}_n^+$. Dann nennen wir $\mathcal{S} \subseteq \mathcal{V}(\mathcal{A})$ eine Seitenfläche des Voronoi-Bereichs, wenn $\mathcal{S}$ eine Hyperebene in $\mathscr{S}_n$ ist, die* $\dim(\langle \mathcal{S} \cap \mathcal{V}(\mathcal{A}) \rangle) = \dim(\langle \mathcal{V}(\mathcal{A}) \rangle) - 1$ *so erfüllt, dass $\mathcal{V}(\mathcal{A})$ in genau einem der durch $\mathcal{S}$ definierten Halbräume liegt.*
Ein Seitenvektor zu $\mathcal{S}$ ist ein $R \in \mathscr{S}_n - \{0\}$ mit $\mathrm{Spur}(RS) = 0$ *für jedes $S \in \mathcal{S}$ und* $\mathrm{Spur}(RX) \geq 0$ *für jedes $X \in \mathcal{V}(\mathcal{A})$.*

Hauptbestandteil des von Voronoi vorgestellten Algorithmus ist der folgende Satz, der uns aufzeigt, warum das Studium von Voronoi-Bereichen sinnvoll ist.

Satz 2.2.7 *Es sei $\mathcal{A} \in \mathscr{S}_n^+$ perfekt und $\mathcal{S}$ eine Seite von $\mathcal{V}(\mathcal{A})$ mit einem Seitenvektor R. Ist $t \in \mathbb{R}$, so sei*

$$\mathcal{A}_t := \mathcal{A} + tR \in \mathscr{S}_n$$

Dann gilt

1. *Es gibt ein eindeutig bestimmtes $\rho > 0$ sodass für $0 < t < \rho$ die Form $\mathcal{A}_t$ nicht perfekt ist und $\min(\mathcal{A}_t) = \min(\mathcal{A})$ gilt. Ist jedoch $t > \rho$, so ist $\min(\mathcal{A}_t) < \min(\mathcal{A})$ oder $\mathcal{A}_t$ ist nicht positiv definit.*

2. *Die Form $\mathcal{A}_\rho$ ist perfekt und ihr Minimum stimmt mit dem von $\mathcal{A}$ überein. $\mathcal{A}_\rho$ heißt dann direkter perfekter Nachbar von $\mathcal{A}$.*

Es sei noch angemerkt, dass die Voronoi-Bereiche der perfekten Formen eine Face-To-Face-Pflasterung des Raumes bilden. Die Voronoi-Bereiche zweier verschidener perfekter Formen schneiden sich genau in einer Seitenfläche.

Als symbolische Darstellung der endlich vielen Ähnlichkeitsklassen perfekter quadratischer Formen kann ein Graph verwendet werden, den wir nun definieren.

Definition 2.2.8 *Sei $n \in \mathbb{N}$. Der Voronoi-Graph in Dimension n ist derjenige Graph, dessen Ecken die Ähnlichkeitsklassen perfekter n-dimensionaler Formen sind. Zwei Ecken seien durch eine Kante verbunden, wenn es in ihnen Vertreter gibt, welche direkte perfekte Nachbarn sind.*

Satz 2.2.9 *Der Voronoi-Graph in Dimension n ist zusammenhängend.*

Aufgrund dieses Satzes wissen wir nun, dass wir von einer perfekten Form $\mathcal{A}$ in gegebener Dimension ausgehen können und durch das Studium von $\mathcal{V}(\mathcal{A})$ und der Voronoi-Bereiche der direkten perfekten Nachbarn alle Ähnlichkeitsklassen perfekter Formen auflisten können.

Kennen wir in einer Dimension n noch keine perfekte Form, so können wir wie folgt eine geeignete Form finden, die dann als Ausgangspunkt des Voronoi-Algorithmus fungieren kann.

Lemma 2.2.10 *Sei $\mathcal{A} \in \mathscr{S}_n^+$ nicht perfekt und sei $R \in \mathcal{V}(\mathcal{A})^\perp$. Dann gibt es ein $\rho > 0$, sodass $\mathcal{A} + \rho R$ das selbe Minimum hat wie $\mathcal{A}$, jedoch $\dim(\langle \mathcal{V}(\mathcal{A}_\rho) \rangle) > \dim(\langle \mathcal{V}(\mathcal{A}) \rangle)$.*

Wir beenden diesen Abschnitt mit einem Beispiel, in welchem wir den Voronoi-Graphen in Dimension 2 bestimmen.

Wir gehen zu diesem Zweck von der perfekten quadratischen Form

$$\mathbb{A}_2 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

aus. Diese hat Minimum 2 und besitzt, bis auf Vorzeichen, 3 Vektoren, die dieses Minimum realisieren, nämlich $(1,0)$, $(0,1)$, $(1,1)$. Die Matrizen der Projektionen auf die kürzesten Vektoren sind $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

Der Voronoi-Bereich $\mathcal{V}(\mathbb{A}_2)$ hat also drei Seitenflächen. Die zugehörigen Seitenvektoren sind

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 2 \end{pmatrix}$$

Diese liefern als direkte perfekte Nachbarn

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 6 & -3 \\ -3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & -3 \\ -3 & 6 \end{pmatrix}$$

Diese sind allesamt zu $\mathbb{A}_2$ ähnlich, sodass in Dimension 2 $\mathbb{A}_2$ die einzige perfekte Form ist. Mithin besteht der Voronoi-Graph nur aus einem Punkt.

3. Der Voronoi-Algorithmus für Körper mit Klassenzahl 1

3.1. Grundlagen

Hat der imaginärquadratische Zahlkörper K, über welchem wir alle perfekten Formen auflisten möchten, Klassenzahl 1, so ist jeder projektive Modul über dem Ganzheitsring $\mathbb{Z}_K$ bereits frei. Anders gesagt bedeutet dies, dass jedes Gitter von der Steinitzklasse $[\mathbb{Z}_K]$ ist. In diesem Fall lässt sich die Voronoi-Theorie für K in Analogie zur klassischen Voronoi-Theorie für $\mathbb{Q}$ aufbauen, wie man in [Mey08] nachlesen kann.

Bemerkung 3.1.1 *Wir bezeichnen im Folgenden mit $\mathcal{H}_n$ den $\mathbb{R}$-Vektorraum der Hermiteschen Matrizen. Dabei handelt es sich um einen Raum von Dimension n^2, der vermöge*

$$\mathcal{H}_n \times \mathcal{H}_n \to \mathbb{R},\ (A, B) \mapsto \mathrm{Spur}(AB)$$

ein Euklidischer Vektorraum ist.

Definition 3.1.2 *Eine Hermitesche Form $\mathcal{A}$ in K^n heißt perfekt, falls die Menge $\{s^*s \mid s \in S(\mathcal{A})\}$ den $\mathbb{R}$-Vektorraum $\mathcal{H}_n$ der Hermiteschen Matrizen vom Format $n \times n$ erzeugt. $\mathcal{A}$ heißt eutaktisch, falls es $\lambda_x \in \mathbb{R}_{>0}$ gibt, sodass*

$$\mathcal{A}^{-1} = \sum_{x \in S(\mathcal{A})} \lambda_x \cdot x^*x$$

Definition 3.1.3 *Wie zuvor definieren wir für $\mathcal{A} \in \mathcal{H}_n$:*

$$\min \mathcal{A} := \min_{0 \neq x \in \mathbb{Z}_K^n} \mathcal{A}[x]$$

$$\gamma(\mathcal{A}) := \frac{\min \mathcal{A}}{(\det \mathcal{A})^{\frac{1}{n}}}$$

Wie im vorigen Kapitel gilt auch hier der folgende wichtige Satz.

Satz 3.1.4 *Eine Hermitesche Form $\mathcal{A}$ über dem imaginärquadratischen Zahlkörper ist genau dann extrem, d.h. ein lokales Maximum der Hermite-Funktion γ, wenn $\mathcal{A}$ perfekt und eutaktisch ist.*

Beweis: [Cou01, Theorem 3.5] enthält die vorliegende Situation als Spezialfall. □

3.2. Ergebnisse in Dimension 2

Mit dem von B. Meyer in [Mey08] beschriebenen und in Magma [BCP97] unter Zuhilfenahme von [BDH96] implementierten Algorithmus erhalten wir, dass jede zweidimensionale perfekte Form ähnlich zu einem der folgenden Vertreter ist.

Körper	**Perfekte Formen**
$\mathbb{Q}(i)$	$P_1 := \begin{pmatrix} 1 & \frac{1}{2}(1+i) \\ \frac{1}{2}(1-i) & 1 \end{pmatrix}$
$\mathbb{Q}(\sqrt{-2})$	$P_1 := \begin{pmatrix} 1 & \frac{1}{2}(1+\sqrt{-2}) \\ \frac{1}{2}(1-\sqrt{-2}) & 1 \end{pmatrix}$
$\mathbb{Q}(\sqrt{-3})$	$P_1 := \begin{pmatrix} 1 & \frac{1}{6}(3+\sqrt{-3}) \\ \frac{1}{6}(3-\sqrt{-3}) & 1 \end{pmatrix}$
$\mathbb{Q}(\sqrt{-7})$	$P_1 := \begin{pmatrix} 1 & \frac{1}{14}(7+3\sqrt{-7}) \\ \frac{1}{14}(7-3\sqrt{-7}) & 1 \end{pmatrix}$
$\mathbb{Q}(\sqrt{-11})$	$P_1 := \begin{pmatrix} 1 & \frac{1}{22}(11+5\sqrt{-11}) \\ \frac{1}{22}(11-5\sqrt{-11}) & 1 \end{pmatrix}$
$\mathbb{Q}(\sqrt{-19})$	$P_1 := \begin{pmatrix} 1 & \frac{1}{38}(19+7\sqrt{-19}) \\ \frac{1}{38}(19-7\sqrt{-19}) & 1 \end{pmatrix}$ $P_2 := \begin{pmatrix} 4 & \frac{1}{19}(38+15\sqrt{-19}) \\ \frac{1}{19}(38-15\sqrt{-19}) & 4 \end{pmatrix}$
$\mathbb{Q}(\sqrt{-43})$	$P_1 := \begin{pmatrix} 1 & \frac{1}{86}(43+11\sqrt{-43}) \\ \frac{1}{86}(43-11\sqrt{-43}) & 1 \end{pmatrix}$ $P_2 := \begin{pmatrix} \frac{7}{3} & \frac{1}{258}(301+79\sqrt{-43}) \\ \frac{1}{258}(301-79\sqrt{-43}) & \frac{7}{3} \end{pmatrix}$ $P_3 := \begin{pmatrix} 28 & \frac{1}{43}(602+159\sqrt{-43}) \\ \frac{1}{43}(602-159\sqrt{-43}) & 28 \end{pmatrix}$ $P_4 := \begin{pmatrix} \frac{17}{3} & \frac{1}{258}(731+177\sqrt{-43}) \\ \frac{1}{258}(731-177\sqrt{-43}) & 5 \end{pmatrix}$

4. Größere Klassenzahlen

In diesem Kapitel widmen wir uns der Situation, in welcher der zugrundeliegende imaginärquadratische Zahlkörper mehr als nur eine Ideaklasse besitzt. Zwar könnte man die Definitionen aus dem vorangegangenen Kapitel unverändert auf diesen Fall übertragen, dies gestattet jedoch nur Einblick in einen Teil der vorhandenen Struktur. Die Tatsache, dass der Zahlkörper eine Klassenzahl größer als Eins hat, impliziert nämlich, dass nicht mehr jeder torsionsfreie Modul über dem Ganzheitsring frei ist. Wir stellen daher nun Definitionen vor, die in [Cou04] für diesen Fall vorgeschlagen werden.

In diesem Kapitel seien stets Einbettungen $K \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ fixiert.

4.1. Definitionen

Sei $L = I_1 \oplus ... \oplus I_n$ und $\mathcal{A} \in \mathcal{H}_n$. Zu $x = (x_1, ..., x_n) \in L$ definieren wir das ganze Ideal $\mathfrak{a}_x := x_1 I_1^{-1} + ... + x_n I_n^{-1}$.

Dann setzen wir

$$\min_L(\mathcal{A}) := \min_{x \in L - \{0\}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)}$$

und

$$\det_L(\mathcal{A}) := N(I_1 \cdot ... \cdot I_n) \det \mathcal{A}$$

Damit setzen wir dann

$$\gamma_L(\mathcal{A}) = \frac{\min_L(\mathcal{A})}{(\det_L(\mathcal{A}))^{1/n}}$$

und

$$\gamma_L := \sup_{\mathcal{A} \in \mathcal{H}_n} \gamma_L(\mathcal{A})$$

Es erscheint sofort angebracht, eine Eigenschaft der Minimumsdefinition zu notieren.

Bemerkung 4.1.1 *Es sei $\tilde{x} \in L$ ein kürzester Vektor zu $\mathcal{A}$, also*

$$\frac{\mathcal{A}[\tilde{x}]}{N(\mathfrak{a}_{\tilde{x}})} = \min_L(\mathcal{A})$$

Ist $\alpha \in \mathbb{Z}_K$, so ist $\alpha\tilde{x} \in L$ ebenfalls ein kürzester Vektor.

Beweis:

$$\frac{\mathcal{A}[\alpha\tilde{x}]}{N(\mathfrak{a}_{\alpha\tilde{x}})} = \frac{(\alpha\tilde{x})\mathcal{A}(\alpha\tilde{x})^*}{N(\alpha\tilde{x}_1 I_1^{-1} + ... + \alpha\tilde{x}_n I_n^{-1})} = \frac{\alpha\overline{\alpha}\mathcal{A}[\tilde{x}]}{N_{K/\mathbb{Q}}(\alpha)N(\mathfrak{a}_{\tilde{x}})}$$

Da im Fall eines imaginärquadratischen Zahlkörpers $\alpha\overline{\alpha} = N_{K/\mathbb{Q}}(\alpha)$ gilt, folgt die Behauptung. □

Die obige Rechnung bleibt offensichtlich auch für beliebiges $\alpha \in K$ richtig, dann ist jedoch $\alpha\tilde{x}$ nicht mehr unbedingt ein Gittervektor in L.

Die folgende Aussage ist von zentraler Bedeutung.

Lemma 4.1.2 *Seien L, L' zwei n-dimensionale $\mathbb{Z}_K$-Gitter mit $\mathrm{St}(L) = \mathrm{St}(L')$. Dann gilt $\gamma_L = \gamma_{L'}$.*

Beweis Seien $L = I_1 \oplus ... \oplus I_n$, $L' = J_1 \oplus ... \oplus J_n$ und sei $\alpha \in K^*$ mit der Eigenschaft $I_1 \cdot ... \cdot I_n = \alpha J_1 \cdot ... \cdot J_n$. Es sei ferner ein $\mathcal{A} \in \mathcal{H}_n$ gegeben. Wir werden im Folgenden ein $\tilde{\mathcal{A}} \in \mathcal{H}_n$ angeben, sodass $\gamma_L(\mathcal{A}) = \gamma_{L'}(\tilde{\mathcal{A}})$.
Dazu konstruieren wir zunächst einen Isomorphismus $\varphi : L \to L'$ mit Determinante α^{-1}.

$$L \xrightarrow{\tau} \mathbb{Z}_K^{n-1} \oplus I_1 \cdot ... \cdot I_n \xrightarrow{\psi} \mathbb{Z}_K^{n-1} \oplus J_1 \cdot ... \cdot J_n \xrightarrow{\mu} L'$$

Dabei sei ψ gegeben durch die Diagonalmatrix $\mathrm{diag}(1, 1, ..., \alpha^{-1})$; μ und τ seien geeignete Isomorphismen wie in 1.2.3; ihre Determinante ist mithin eine Einheit in $\mathbb{Z}_K^*$. Nun setzen wir $\varphi := \mu \circ \psi \circ \tau$. Der Isomorphismus φ habe ferner eine Matrixdarstellung sodass $\varphi(x) = xU$ für alle $x \in L$.
Wir stellen jetzt fest, dass

$$\mathfrak{a}_x = \mathfrak{a}'_{\varphi(x)}$$

Dabei sei $\mathfrak{a}_x$ für $x \in L$ wie zuvor definiert. $\mathfrak{a}'_y$ sei für $y \in L'$ definiert als $y_1 J_1^{-1} + ... + y_n J_n^{-1}$. Für $L \ni x = (x_1, ..., x_n)$ haben wir

$$\varphi(x) = xU = \left(\sum_{i=1}^{n} x_i U_{i,1}, ..., \sum_{i=1}^{n} x_i U_{i,n} \right)$$

und es gilt

$$\mathfrak{a}_x = x_1 I_1^{-1} + ... + x_n I_n^{-1} \supseteq \sum_{i=1}^{n} x_i U_{i,1} J_1^{-1} + ... + \sum_{i=1}^{n} x_i U_{i,n} J_n^{-1},$$

denn sei $1 \leq \ell \leq n$ und es sei $\tilde{j} \in J_\ell^{-1}$. Dann haben wir

$$\left(\sum_{i=1}^{n} x_i U_{i,\ell} \right) \tilde{j} = \sum_{i=1}^{n} x_i \underbrace{\left(U_{i,\ell} \tilde{j} \right)}_{\in I_i^{-1}} \in x_1 I_1^{-1} + ... + x_n I_n^{-1}$$

Also haben wir in der Tat $\mathfrak{a}_x \supseteq \mathfrak{a}'_{\varphi(x)}$. Daraus folgt jedoch sofort

$$\mathfrak{a}_x \supseteq \mathfrak{a}'_{\varphi(x)} \supseteq \mathfrak{a}_{\varphi^{-1}(\varphi(x))} = \mathfrak{a}_x$$

Nun sind wir bereit, $\tilde{A}$ als $\mathcal{A}[U^{-1}]$ anzugeben. Die Überlegung $\mathfrak{a}_x = \mathfrak{a}'_{\varphi(x)}$ gestattet uns sofortigen Aufschluss über das L'-Minimum von $\tilde{\mathcal{A}}$:

$$\min_{L'}(\mathcal{A}[U^{-1}]) = \min_{x \in L' - \{0\}} \frac{(\mathcal{A}[U^{-1}])[x]}{N(\mathfrak{a}'_x)} = \min_{x \in L' - \{0\}} \frac{\mathcal{A}[\varphi^{-1}(x)]}{N(\mathfrak{a}_{\varphi^{-1}(x)})} = \min_{x \in L - \{0\}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} = \min_L(\mathcal{A})$$

Es gilt ferner

$$\begin{aligned} \det_{L'}(\mathcal{A}[U^{-1}]) &= N(J_1 \cdot ... \cdot J_n) N_{K/\mathbb{Q}}(\det(U^{-1})) \det(\mathcal{A}) \\ &= N_{K/\mathbb{Q}}(\alpha) N(I_1 \cdot ... \cdot I_n) N_{K/\mathbb{Q}}(\alpha^{-1}) \det(\mathcal{A}) \\ &= \det_L(\mathcal{A}) \end{aligned}$$

Es folgt $\gamma_{L'}(\mathcal{A}[U^{-1}]) = \gamma_L(\mathcal{A})$ und damit die Behauptung. □

Daher und aufgrund der Tatsache, dass jedes Gitter isomorph zu einem Gitter der Form $\mathbb{Z}_K^{n-1} \oplus \mathfrak{a}$ mit $\mathfrak{a} = I_1 \cdot ... \cdot I_n$ ist, genügt es, die Konstanten γ_L für diese Gitter zu bestimmen. Wir setzen also $\gamma_i := \gamma_{L_i}$ für die Gitter $L_i := \mathbb{Z}_K^{n-1} \oplus \mathfrak{a}_i$, wobei $\mathfrak{a}_i$ ein Vertretersystem der Idealklassengruppe durchläuft. Wir wählen die Vertreter so, dass sie ganz sind und minimale Idealnorm haben. Außerdem sei $\mathfrak{a}_1 := \mathbb{Z}_K$.
Wir können daher die Hermite-Konstante in Dimension n für den Körper K definieren als

$$\gamma_{n,K} := \max_{1 \leq i \leq h_K} \gamma_{L_i}$$

In Abschnitt 4.3 werden wir noch einige weitere Einschränkungen an die zu betrachtenden Gitter kennenlernen.

Es erscheint wünschenswert, dass die hier vorgeschlagenen Definitionen bei der Einschränkung auf Körper mit Klassenzahl 1 mit den Definitionen des letzten Kapitels übereinstimmen.

Bemerkung 4.1.3 *Ist $h_K = 1$, so ist jedes Gitter L isomorph zu $\mathbb{Z}_K^n$ und wir haben*

$$\gamma_L(\mathcal{A}) = \gamma(\mathcal{A})$$

für jedes $\mathcal{A} \in \mathcal{H}_n$ gemäß der Definition im vorigen Kapitel.

Beweis: Ohne Einschränkung ist $L = \mathbb{Z}_K^n$, sodass sicherlich

$$\det_L(\mathcal{A}) = \det(\mathcal{A})$$

Die Tatsache, dass $h_K = 1$ ist, impliziert unter Anderem, dass $\mathbb{Z}_K$ ein Hauptidealbereich ist. Sei $L \ni x = (x_1, ..., x_n)$. Dann ist

$$N(\mathfrak{a}_x) = N(x_1\mathbb{Z}_K^{-1} + ... + x_n\mathbb{Z}_K^{-1}) = N(\langle \mathrm{ggT}(x_1, ..., x_n)\rangle) = N_{K/\mathbb{Q}}(\mathrm{ggT}(x_1, ..., x_n))$$

Wegen 4.1.1 kann ein Gittervektor, der $\min_L(\mathcal{A})$ annimmt, ohne Einschränkung mit teilerfremden Einträgen gewählt werden. Dann fällt die Norm $N(\mathfrak{a}_x)$ aber nicht mehr ins Gewicht, sodass in der Tat

$$\min_L(\mathcal{A}) = \min(\mathcal{A})$$

Folglich $\gamma_L(\mathcal{A}) = \gamma(\mathcal{A})$. □

Bei der Bestimmung des Minimums ist die folgende Aussage hilfreich.

Lemma 4.1.4

$$\min_{L_i}(\mathcal{A}) = \min_{1\le j\le h} \min_{\substack{x\in L_i-\{0\} \\ [\mathfrak{a}_x]=[\mathfrak{a}_j]}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} = \min_{1\le j\le h} \min_{\substack{x\in L_i-\{0\} \\ \mathfrak{a}_x=\mathfrak{a}_j}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_j)}$$

Beweis: Die erste Gleichheit folgt sofort aus der Tatsache, dass wir für die Idealgruppe I_K eine Nebenklassenzerlegung

$$I_K = \bigcup_{j=1}^{h_K} \mathfrak{a}_j J_K$$

haben.

Sei $x \in L_i - \{0\}$. Dann gibt es ein $1 \le j \le h_K$ und ein $\alpha \in K^*$ sodass $\alpha\mathfrak{a}_x = \mathfrak{a}_j$. $\alpha\mathfrak{a}_x$ entspricht jedoch auch gerade $\mathfrak{a}_{\alpha x}$.
Wir behaupten nun, dass $\alpha x \in L_i$. Da $\mathfrak{a}_{\alpha x} = \mathfrak{a}_j$ ganz ist, gilt

$$\alpha x_j\mathbb{Z}_K^{-1} \subseteq \mathbb{Z}_K,\ \alpha x_n\mathfrak{a}_i^{-1} \subseteq \mathbb{Z}_K$$

für alle $1 \leq j \leq n-1$. Daraus folgt $\alpha x_j \in \mathbb{Z}_K,\ \alpha x_n \in \mathfrak{a}$. Also liegt αx in der Tat in L_i. Da nach 4.1.1

$$\frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} = \frac{\mathcal{A}[\alpha x]}{N(\mathfrak{a}_{\alpha x})} = \frac{\mathcal{A}[\alpha x]}{N(\mathfrak{a}_j)}$$

gilt, können wir also zu jedem $x \in L_i$ ein $\tilde{x} \in L_i$ angeben, sodass die obigen Werte übereinstimmen. Folglich stimmen auch die Minima überein. □

Lemma 4.1.5 *Ist $a \in \mathbb{R}_{>0}$ und $U \in \mathrm{Aut}(L)$ (aufgefasst als Matrixgruppe), so ist*

$$\gamma_L(\mathcal{A}) = \gamma_L(a\mathcal{A}[U]).$$

Insbesondere stimmen L-Minimum und L-Determinante von $\mathcal{A}$ und $\mathcal{A}[U]$ überein.

Beweis: Wie im Beweis von 4.1.2 erkennt man

$$\mathfrak{a}_{xU} = \sum_{i=1}^{n} x_i U_{i,1} I_1^{-1} + ... + \sum_{i=1}^{n} x_i U_{i,n} I_n^{-1} \subseteq x_1 I_1^{-1} + ... + x_n I_n^{-1} = \mathfrak{a}_x$$

und folglich $\mathfrak{a}_{xU} = \mathfrak{a}_x$. Für das Minimum haben wir also

$$\min_L(\mathcal{A}[U]) = \min_{x \in L - \{0\}} \frac{\mathcal{A}[xU]}{N(\mathfrak{a}_x)} = \min_{x \in L - \{0\}} \frac{\mathcal{A}[xU]}{N(\mathfrak{a}_{xU})} = \min_L(\mathcal{A})$$

Da für $U \in \mathrm{Aut}(L)$ die Eigenschaft $\det U \in \mathbb{Z}_K^*$ gilt, ist die Aussage über die Determinante klar. Die Invarianz von γ_L unter Multiplikation mit a ist trivial. □

Offenbar haben wir durch obige Operation eine Doppelnebenklassenzerlegung von $\mathcal{H}_n$ gegeben. Eine Klasse in $\mathbb{R}_{>0} \backslash \mathcal{H}_n / \mathrm{Aut}(L)$ nennen wir Ähnlichkeitsklasse von $\mathcal{A}$ bezüglich L.

4.2. Spurform und Abschätzungen

Dieser Abschnitt, welcher sich mit der Spurform befasst, wird maßgeblich für die Implementierung des Voronoi-Algorithmus sein.

In diesem Abschnitt sei weiterhin $K = \mathbb{Q}(\sqrt{d})$ ein imaginärquadratischer Zahlkörper und $\omega \in K$, sodass $\mathbb{Z}_K = \mathbb{Z}[\omega]$. Also beispielsweise

$$\omega = \begin{cases} \sqrt{d} & d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \end{cases}$$

Definition 4.2.1 *Sei $\mathcal{A} \in \mathcal{H}_n$ mit Einträgen in K und sei $L = \mathbb{Z}_K^{n-1} \oplus \mathfrak{a}$ ein $\mathbb{Z}_K$-Gitter. Man wähle eine $\mathbb{Z}$-Basis $B = (b_1, b_2, ..., b_{2n})$ von L (vgl. dazu 1.1.9). Dann heißt*

$$\mathrm{Tr}_B(\mathcal{A}) := \frac{1}{2}(S_{K/\mathbb{Q}}(b_i \mathcal{A} b_j^*))_{i,j} \in \mathbb{Q}^{2n \times 2n}$$

die Spurform von $\mathcal{A}$.

Lemma 4.2.2 *Die Werte $\mathcal{A}[\ell]$ mit $\ell \in L$ stimmen mit den Werten $\mathrm{Tr}_B(\mathcal{A})[\tilde{\ell}]$ überein, wenn $\tilde{\ell} \in \mathbb{Z}^{2n}$ die Darstellung von ℓ in der Basis B ist.*

Beweis: Sei B wie in der Definition der Spurform gewählt. Es sei weiter ein $x \in L$ gegeben. Wir schreiben $x = \sum_{i=1}^{2n} x_i b_i$ mit $x_i \in \mathbb{Z}$.
Sei dann $\tilde{x} = (x_1, ..., x_{2n}) \in \mathbb{Z}^{1 \times 2n}$. Damit gilt:

$$\begin{aligned}
\tilde{x}\mathrm{Tr}_B(\mathcal{A})\tilde{x}^T &= \sum_{i=1}^{2n} \tilde{x}_i \cdot \left(\mathrm{Tr}_B(\mathcal{A})\tilde{x}^T\right)_i = \sum_{i=1}^{2n} x_i \sum_{k=1}^{2n} \mathrm{Tr}_B(\mathcal{A})_{i,k} x_k \\
&= \sum_{i=1}^{2n}\sum_{k=1}^{2n} \frac{1}{2} S_{K/\mathbb{Q}}\left(b_i \mathcal{A} b_k^*\right) x_i x_k = \sum_{i=1}^{2n}\sum_{k=1}^{2n} \frac{1}{2} S_{K/\mathbb{Q}}\left(x_i b_i \mathcal{A} x_k b_k^*\right) \\
&= \frac{1}{2} S_{K/\mathbb{Q}}\left(\sum_{i=1}^{2n}\sum_{k=1}^{2n} x_i b_i \mathcal{A} x_k b_k^*\right) = \frac{1}{2} S_{K/\mathbb{Q}}\left(x \mathcal{A} x^*\right) = x \mathcal{A} x^*,
\end{aligned}$$

da stets $x\mathcal{A}x^*$ in $\mathbb{R}$ liegt. □

Insbesondere sei noch angemerkt, dass stets die Gleichheit

$$\min_{0 \neq x \in L} \mathcal{A}[x] = \min_{0 \neq x \in \mathbb{Z}^{2n}} \mathrm{Tr}_B(\mathcal{A})[x]$$

herrscht.

Der folgende Satz wird später bei der Implementierung des Voronoischen Algorithmus hilfreich sein, um zwei gegebene Hermitesche Formen auf Äquivalenz zu überprüfen.

Satz 4.2.3 *Es seien $a,\ b\ :\ K^n \times K^n \to K$ zwei nicht ausgeartete Hermitesche Formen auf K^n. Für ein $\varphi\ :\ K^n \to K^n$ gilt dann für alle $v, u \in K^n$*

$$\begin{aligned}
\varphi \in \mathrm{End}_{\mathbb{Q}}(K^n) \text{ mit } & S_{K/\mathbb{Q}}(a(\varphi(v), \varphi(u))) = S_{K/\mathbb{Q}}(b(v,u)) \\
\text{und } & S_{K/\mathbb{Q}}(\omega a(\varphi(v), \varphi(u))) = S_{K/\mathbb{Q}}(\omega b(v,u))
\end{aligned}$$

genau dann, wenn

$$\varphi \in \mathrm{End}_K(K^n),\ a(\varphi(v), \varphi(u)) = b(v,u)$$

Beweis: Sei zunächst φ $\mathbb{Q}$-linear und es gelten die Gleichungen für die Spuren. Da $\mathbb{Q}$ vollkommen ist, ist die Spurbilinearform nicht ausgeartet, sodass die Gleichungen

$$\begin{aligned} &S_{K/\mathbb{Q}}(a(\varphi(v),\varphi(u))) = S_{K/\mathbb{Q}}(b(v,u)),\\ &S_{K/\mathbb{Q}}(\omega a(\varphi(v),\varphi(u))) = S_{K/\mathbb{Q}}(\omega b(v,u)) \quad \forall\ v,u \in K^n \end{aligned}$$

implizieren, dass $a(\varphi(v),\varphi(u)) = b(v,u)$ für alle $v,u \in K^n$ gilt.
Wir zeigen nun, dass φ K-linear ist. Dazu nehmen wir an, dass es ein $0 \neq v \in K^n$ mit der Eigenschaft $\omega\varphi(v) \neq \varphi(\omega v)$ gibt. Da a nicht ausgeartet ist, existiert dann ein $u \in K^n$ mit

$$\omega b(v,u) = b(\omega v,u) = a(\varphi(\omega v),\varphi(u)) \neq a(\omega\varphi(v),\varphi(u)) = \omega a(\varphi(v),\varphi(u)) = \omega b(v,u)$$

Dies ist ein Widerspruch.

Umgekehrt ist klar, dass ein K-linearer Endomorphismus ebenfalls $\mathbb{Q}$-linear mit den gewünschten Eigenschaften ist. □

Wir erhalten aus diesem Satz in der Sprache der Matrizen die folgende Aussage.

Korollar 4.2.4 *Seien $\mathcal{A},\ \mathcal{B} \in \mathcal{H}_n$. Es existiert genau dann ein $U \in \mathrm{Aut}(\mathbb{Z}_K^{n-1} \oplus \mathfrak{a})$ mit $\mathcal{B} = U\mathcal{A}U^*$, wenn ein $T \in \mathrm{GL}_{2n}(\mathbb{Z})$ existiert, welches $T\mathrm{Tr}_B(\mathcal{A})T^T = \mathrm{Tr}(\mathcal{B})$ und $T\mathrm{Tr}_B(\omega\mathcal{A})T^T = \mathrm{Tr}_B(\omega\mathcal{B})$ erfüllt.*

Im Folgenden benötigen wir noch zwei bekannte Resultate aus der Theorie der $\mathbb{Z}$-Gitter, welche wir ohne Beweis zitieren werden.
Sei dazu Λ ein $\mathbb{Z}$-Gitter in einem n-dimensionalen Euklidischen Vektorraum $(V,\ (\ ,\ ))$.

Satz 4.2.5 (Hadamard) *Sei $(b_1,...,b_n)$ eine Gitterbasis von Λ. Dann gilt*

$$\det(\Lambda) \leq \prod_{j=1}^{n}(b_j,b_j)$$

Beweis: [Mar03, Theorem 2.1.1] □

Satz 4.2.6 (Hermite) *Λ besitzt eine Gitterbasis $(b_1,...,b_n)$ mit der Eigenschaft*

$$\prod_{j=1}^{n}(b_j,b_j) \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} \det(\Lambda)$$

Beweis: [Mar03, Theorem 2.2.1] □

Eine Gitterbasis mit dieser Eigenschaft nennen wir Hermite-reduziert.

4.3. Perfektion und Eutaxie

Das Ziel dieses Abschnitts soll es sein, die Begriffe Perfektion und Eutaxie auf die vorliegende Situation zu übertragen und, [Mar03] folgend, ähnliche Eigenschaften wie in der klassischen Voronoi-Theorie nachzuweisen.

In [Cou01] arbeitet R. Coulangeon mit endlichen Mengen kürzester Vektoren, indem er die Klassen der kürzesten modulo $\mathbb{Z}_K^*$ betrachtet. Die Bemerkung 4.1.1 macht hier jedoch eine andere Vorgehensweise nötig.

Bemerkung 4.3.1 *Die Menge*

$$\left\{ x \in L_i - \{0\} \mid \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} = \min_{L_i}(\mathcal{A}) \right\} / \mathbb{Z}_K^*$$

ist nicht endlich.

Jedoch ist

$$S_i(\mathcal{A}) := \left\{ x \in L_i - \{0\} \mid \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} = \min_{L_i}(\mathcal{A}) \right\} / \sim$$

endlich, wenn wir die Äquivalenzrelation $\sim$ auf L_i durch

$$v \sim w \ :\Longleftrightarrow\ \exists\ \kappa \in K^* \ :\ v = \kappa w$$

definieren.

Beweis: Die erste Behauptung folgt sofort aus 4.1.1 und dem Einheitensatz von Dirichlet, welcher impliziert, dass der Ganzheitsring eines imaginärquadratischen Zahlkörpers unendlich viele Assoziiertenklassen von Elementen besitzt.

Zum Beweis der Tatsache, dass $S_i(\mathcal{A})$ endlich ist, werden wir eine injektive Abbildung ι in die nach 1.2.12 endliche Menge

$$\{x \in L_i \mid \mathcal{A}[x] \leq \mu \tilde{m}\} =: \tilde{L}_i$$

angeben. Dabei sei $\mu := \min_{L_i}(\mathcal{A})$ und $\tilde{m} := \max_{1 \leq j \leq h_K} N(\mathfrak{a}_j)$.

Dem Beweis von 4.1.4 entnehmen wir, dass es zu jedem $x \in L_i$ ein $\alpha_x \in K^*$ gibt, sodass $\hat{x} := \alpha_x x \in L_i$ mit $\mathfrak{a}_{\hat{x}} = \mathfrak{a}_j$ für ein $1 \leq j \leq h_K$. Wir definieren nun ι wie folgt.

$$\iota \ :\ S_i(\mathcal{A}) \to \tilde{L}_i,\ [v] \mapsto \hat{v}$$

Seien $v_1,\ v_2 \in [v]$ für ein $v \in L_i$. Dann existiert ein $k \in K^*$ mit $kv_1 = v_2$. Ferner existieren eindeutige $\alpha,\ \beta \in K^*$ sodass $\alpha v_1 = \tilde{v_1}$ und $\beta v_2 = \tilde{v_2}$. Wegen der Eindeutigkeit ist $\beta k = \alpha$ und es gilt

$$\hat{v_1} = \alpha v_1 = \alpha k^{-1} v_2 = \alpha k^{-1} \beta^{-1} \hat{v_2} = \hat{v_2}$$

Also ist ι wohldefiniert, denn die Bilder liegen sicherlich in $\tilde{L_i}$.
Die Injektivität von ι ist offensichtlich. □

Definition 4.3.2 *Sei $\mathcal{A} \in \mathcal{H}_n$. Dann nennen wir $\mathcal{A}$ γ_i-perfekt, falls*

$$\langle x^* x \mid x \in S_i(\mathcal{A}) \rangle_{\mathbb{R}} = \mathcal{H}_n.$$

Wir nennen $\mathcal{A}$ γ_i-eutaktisch, falls es zu jedem $x \in S_i(\mathcal{A})$ ein $\lambda_x \in \mathbb{R}_{>0}$ gibt mit

$$\mathcal{A}^{-1} = \sum_{x \in S_i(\mathcal{A})} \lambda_x \cdot x^* x$$

Satz 4.3.3 *Ist $\mathcal{A} \in \mathcal{H}_n$ γ_i-perfekt, so ist $\mathcal{A}$ durch $\min_{L_i}(\mathcal{A})$ und $S_i(\mathcal{A})$ eindeutig bestimmt.*

Beweis: Es sei $\mathfrak{B}$ eine weitere Lösung des inhomogenen linearen Gleichungssystems

$$\frac{\mathfrak{B}[x]}{N(\mathfrak{a}_x)} = \min_{L_i}(\mathcal{A}) \ \forall\ x \in S_i(\mathcal{A})$$

Dann gilt für all diese x:

$$0 = \frac{(\mathcal{A} - \mathfrak{B})[x]}{N(\mathfrak{a}_x)} = \mathrm{Spur}\left(\frac{(\mathcal{A} - \mathfrak{B})[x]}{N(\mathfrak{a}_x)}\right) = \frac{1}{N(\mathfrak{a}_x)} \mathrm{Spur}(x^* x(\mathcal{A} - \mathfrak{B}))$$

Dann liegt aber $\mathcal{A} - \mathfrak{B}$ bezüglich dem durch die Spur erklärten Skalarprodukt im Raum $\langle x^* x \mid x \in S_i(\mathcal{A}) \rangle^{\perp} = \{0\}$. □

Bemerkung 4.3.4 *Ist $\mathcal{A}$ γ_i-perfekt, so ist $|S_i(\mathcal{A})| \geq \dim_{\mathbb{R}} \mathcal{H}_n = n^2$.*

Bemerkung 4.3.5 *Ist $\mathcal{A}$ γ_i-perfekt, so ist $\langle S_i(\mathcal{A}) \rangle_{\mathbb{R}} = \mathbb{C}^n$.*

Beweis: Ist die Aussage falsch, so existiert ein $0 \neq y \in \mathbb{C}^n$ mit der Eigenschaft $(x, y)^2 = 0$ für alle $x \in S_i(\mathcal{A})$, wobei $(\ ,\ )$ das Standardskalarprodukt des $\mathbb{C}^n$ bezeichne. Dann haben wir für alle $x \in S_i(\mathcal{A})$

$$0 = (x, y)^2 = (xy^*)^2 = (xy^*)(yx^*) = \mathrm{Spur}(xy^* yx^*) = \mathrm{Spur}((x^* x)(y^* y))$$

Dann liegt $y^* y$ in $\langle x^* x \mid x \in S_i(\mathcal{A}) \rangle^{\perp} = \{0\}$. Dies ist ein Widerspruch. □

Bemerkung 4.3.6 *γ_i-Perfektion ist eine Eigenschaft der Ähnlichkeitsklasse (bezüglich L_i) von $\mathcal{A}$.*

Lemma 4.3.7 *Ist $\mathcal{A}$ γ_i-perfekt, so existiert ein $a \in \mathbb{R}_{>0}$ mit $a\mathcal{A} \in \mathbb{Z}_K^{n\times n}$.*

Beweis: Sei ohne Einschränkung $\min_{L_i}(\mathcal{A}) = 1$ (durch Multiplikation vom $\mathcal{A}$ mit $(\min_{L_i}(\mathcal{A}))^{-1}$). $\mathcal{A}$ ist wie zuvor die eindeutige Lösung des linearen Gleichungssystems

$$\mathfrak{B}[x] = N(\mathfrak{a}_x) \ \forall \ x \in S_i(\mathcal{A}) \subseteq L_i \subseteq \mathbb{Z}_K^n$$

mit in $\mathbb{Z}_K$ gelegenen Koeffizienten. Nach Cramer ist die Lösung $\mathcal{A}$ also in $K^{n\times n}$ enthalten. Multiplizieren wir diese Lösung mit dem Produkt aller auftretenden Nenner, so liegt sie in $\mathbb{Z}_K^{n\times n}$. □

Satz 4.3.8 *Die Menge*

$$\{[\mathcal{A}] \in \mathbb{R}_{>0} \setminus \mathcal{H}_n/\mathrm{Aut}(L) \mid \mathcal{A} \ \gamma_i\text{-perfekt}\}$$

ist endlich.

Beweis: Es sei $\mathcal{A}$ γ_i-perfekt und ohne Einschränkung sei $\min_{L_i}(\mathcal{A}) = 1$. Wir bezeichnen weiterhin $\tilde{m} := \max_{1\leq j\leq h_K} N(\mathfrak{a}_j)$ und $\mathbb{Z}_K = \mathbb{Z}[\omega]$.
Das $\mathbb{Z}_K$-Gitter L_i mit der Hermiteschen Form $\mathcal{A}$ liefert ein $\mathbb{Z}$-Gitter (Λ, q) vom Rang $2n$, wobei die quadratische Form q gegeben ist durch $q(v) := \mathcal{A}[v] \ \forall \ v \in \Lambda$.
Man wähle nun $\{v_1, ..., v_n\} \subseteq S_i(\mathcal{A})$ K-linear unabhängig. Dann ist die Menge $\{v_1, \omega v_1, v_2, \omega v_2, ..., \omega v_n\} \subseteq \Lambda$ $\mathbb{Q}$-linear unabhängig. Nach Hadamard ist dann

$$\det(\Lambda) \leq \det(\langle v_1, \omega v_1, ..., \omega v_n\rangle_{\mathbb{Z}}) \leq \prod_{j=1}^{n} q(v_j) \prod_{j=1}^{n} q(\omega v_j) \leq \tilde{m}^{2n} N_{K/\mathbb{Q}}(\omega)^n$$

denn für jeden kürzesten Vektor gilt $\mathcal{A}[x] \leq \tilde{m}$.

Es sei nun $(b_1, ..., b_{2n})$ eine Hermite-reduzierte $\mathbb{Z}$-Basis von Λ, also

$$\prod_{j=1}^{2n} q(b_j) \leq \left(\frac{4}{3}\right)^{\frac{2n(2n-1)}{2}} \det(\Lambda) \leq \left(\frac{4}{3}\right)^{n(2n-1)} \tilde{m}^{2n} N_{K/\mathbb{Q}}(\omega)^n =: C_{n,K}$$

Dann gilt insbesondere für jedes $1 \leq j \leq 2n$ die Ungleichung

$$q(b_j) \leq \frac{C_{n,K}}{\prod_{k\neq j} q(b_j)} \leq C_{n,K}$$

Es sei nun $x \in S_i(\mathcal{A})$, wir schreiben $x = \sum_{j=1}^{2n} a_j b_j$. Nach Cramer gilt dann

$$\begin{aligned} a_\ell^2 &= \frac{\det(\langle b_1, ..., b_{\ell-1}, x, b_\ell, ..., b_{2n}\rangle_{\mathbb{Z}})}{\det(\Lambda)} \leq C_{n,K} \frac{q(x) \prod_{j \neq \ell} q(b_j)}{\prod_{j=1}^{2n} q(b_j)} \\ &= C_{n,K} \frac{q(x)}{q(b_\ell)} \leq C_{n,K} q(x) = C_{n,K} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} N(\mathfrak{a}_x) \leq C_{n,K} \tilde{m} \end{aligned}$$

Jeder kürzeste Vektor einer γ_i-perfekten Form $\mathcal{A}$ liegt also in der endlichen Menge

$$\left\{ (a_1, ..., a_{2n}) \in \mathbb{Z}^{2n} \;\middle|\; |a_j| \leq \sqrt{C_{n,K} \tilde{m}} \right\}$$

Da das Minimum und die Menge der kürzesten Vektoren eine γ_i-perfekte Form eindeutig festlegen und obige Menge nur endlich viele Teilmengen besitzt, existieren also nur endlich viele Ähnlichkeitsklassen γ_i-perfekter Formen. □

Die folgenden Aussagen können verwendet werden, um einige Berechnungen zur Bestimmung der Hermite-Konstante auszusparen.

Satz 4.3.9 *Ist* $L = \bigoplus_{j=1}^{n} I_j$ *ein* $\mathbb{Z}_K$*-Gitter und* $\mathfrak{p}$ *ein gebrochenes Ideal von* K*, so stimmen die Mengen der Ähnlichkeitsklassen der perfekten Hermiteschen Formen auf* L *und* $\mathfrak{p}L$ *überein.*

Beweis: Ist $x = \sum_{j=1}^{n} x_j e_j \in \mathfrak{p}L$, so ist

$$\frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} = \frac{\mathcal{A}[x]}{N(x_1(\mathfrak{p}I_1)^{-1} + ... + x_n(\mathfrak{p}I_n)^{-1})} = N(\mathfrak{p}) \frac{\mathcal{A}[x]}{N(x_1 I_1^{-1} + ... + x_n I_n^{-1})}$$

Folglich haben wir

$$\min_{\mathfrak{p}L}(\mathcal{A}) = N(\mathfrak{p}) \min_L(\mathcal{A})$$

Der Wert $\dfrac{\mathcal{A}[x]}{N(x_1 I_1^{-1} + ... + x_n I_n^{-1})}$ hängt zudem nur von der „Richtung“ $\langle x \rangle_K$ ab. Es ist jedoch sicherlich in jedem Gitter Λ jede vorkommende Richtung vertreten: ausgehend von einem Gittervektor x in einem beliebigen Gitter L' gelangt man durch Multiplikation mit gegebenenfalls vorkommenden Nennern in das Gitter $\mathbb{Z}_K^n$. Multipliziert man diesen Vektor dann noch mit Elementen aus den Idealen, deren direkte Summe Λ ist, so hat man einen Gittervektor von Λ erhalten, der die selbe Richtung wie x hat.

Es gilt ferner

$$\det_{\mathfrak{p}L}(\mathcal{A}) = N(\mathfrak{p})^n \det_L(\mathcal{A})$$

sodass schließlich

$$\gamma_{\mathfrak{p}L}(\mathcal{A}) = \frac{\min_{\mathfrak{p}L}(\mathcal{A})}{(\det_{\mathfrak{p}L}(\mathcal{A}))^{1/n}} = \frac{\min_L(\mathcal{A})}{(\det_L(\mathcal{A}))^{1/n}} = \gamma_L(\mathcal{A})$$

Damit ist die Behauptung gezeigt. □

Aus dieser Bemerkung erhalten wir sofort eine wichtige Folgerung.

Korollar 4.3.10 *Für die Steinitzklassen von L und $\mathfrak{p}L$ gilt*

$$\mathrm{St}(\mathfrak{p}L) = [\mathfrak{p}]^n \mathrm{St}(L),$$

sodass zur Bestimmung der Hermite-Konstante $\gamma_{n,K}$ nur die Gitter $\mathbb{Z}_K^{n-1} \oplus \mathfrak{I}$ betrachtet werden müssen, wobei $\mathfrak{I}$ ein Vertretersystem von $\mathcal{C}\ell_K/\mathcal{C}\ell_K^n$ durchläuft. Dabei bezeichne $\mathcal{C}\ell_K^n \leq \mathcal{C}\ell_K$ die Untergruppe der n-ten Potenzen in $\mathcal{C}\ell_K$.

Die folgende leicht einzusehende Bemerkung reduziert ebenfalls den Aufwand zur Bestimmung von $\gamma_{n,K}$.

Bemerkung 4.3.11 *Es bezeichne $\bar{\ }$ den Galoisautomorphismus von K. Dann gilt, dass die perfekten Formen auf dem Gitter L durch Anwenden des Galoisautomorphismus zu den perfekten Formen auf dem Gitter $\overline{L}$ in Bijektion stehen.*
Insbesondere gilt dies also für die Gitter $\mathbb{Z}_K^{n-1} \oplus \mathfrak{a}$ und $\mathbb{Z}_K^{n-1} \oplus \overline{\mathfrak{a}}$.

4.4. Charakterisierung extremer Formen

Definition 4.4.1 *$\mathcal{A} \in \mathcal{H}_n$ heiße γ_i-extrem, wenn $\mathcal{A}$ ein lokales Maximum der Funktion γ_{L_i} ist.*

Das Ziel dieses Abschnitts soll sein, in Analogie zum klassischen Satz von Voronoi zu beweisen, dass γ_i-extreme Formen genau diejenigen sind, die γ_i-perfekt und γ_i-eutaktisch sind. Dazu folgen wir Abschnitt 3.4 aus [Mar03] und übernehmen einige Resultate unverändert und ohne Beweis.

Wir fixieren weiterhin eine Einbettung $K \hookrightarrow \mathbb{C}$. Dadurch können wir die Gitter L_i im unitären Vektorraum $\mathbb{C}^n$ (mit dem Standardskalarprodukt) betrachten.

Bemerkung 4.4.2 *Es sei* $\mathrm{End}_h(\mathbb{C}^n)$ *der Raum der Hermiteschen Endomorphismen von* $\mathbb{C}^n$*. Dieser ist mit der Spurbilinearform ein unitärer Vektorraum, den wir durch*

$$\mathrm{Spur}^* \ : \ \mathrm{End}_h(\mathbb{C}^n) \to \mathrm{End}_h(\mathbb{C}^n)^*, \ f \mapsto (g \mapsto \mathrm{Spur}(gf))$$

mit seinem Dualraum identifizieren können.

Zu jedem $0 \neq x \in \mathbb{C}^n$ *haben wir* $p_x \ : \ v \mapsto \frac{(v,x)}{(x,x)}x$ *als Hermiteschen Endomorphismus, der bezüglich einer Orthonormalbasis die Darstellungsmatrix* $\frac{1}{(x,x)}x^*x$ *hat.*
Wir schreiben $\varphi_x := (x,x)\mathrm{Spur}^*(p_x)$ *und es gilt* $\varphi_x(f) = (xf, x)$*.*

Mit dieser Bemerkung können wir jetzt die zuvor definierten Begriffe übertragen.

Bemerkung 4.4.3 *Dass ein* $\mathcal{A} \in \mathcal{H}_n$ γ_i*-perfekt ist, bedeutet, dass die Menge*

$$\{\varphi_x \mid x \in S_i(\mathcal{A})\}$$

den Raum $\mathrm{End}_h(\mathbb{C}^n)^*$ *erzeugt.*

Die Bedingung, dass $\mathcal{A}$ *eutaktisch ist, also*

$$\mathcal{A}^{-1} = \sum_{x \in S_i(\mathcal{A})} \lambda_x x^* x$$

mit strikt positiven λ_x *überträgt sich zu*

$$\mathrm{id} = \sum_{x \in S_i(\mathcal{A})} \lambda_x (x,x) p_x$$

Durch Anwenden von Spur^* *erhält man daraus*

$$\mathrm{Spur} = \sum_{x \in S_i(\mathcal{A})} \lambda_x \varphi_x$$

Satz 4.4.4 (Stiemke) *Sei* V *ein* $\mathbb{R}$*-Vektorraum und* $\varphi_1, ..., \varphi_t \in V^*$*. Dann sind äquivalent*

1. $\{x \in V \mid \varphi_j(x) \geq 0 \ \forall \ 1 \leq j \leq t\} = \bigcap_{i=1}^{t} \ker(\varphi_i)$
2. *Es existieren* $a_1, ...a_t \in \mathbb{R}_{>0}$ *mit* $\sum_{i=1}^t a_i \varphi_i = 0$*.*

Beweis: [Mar03, Theorem 3.3.1]. □

Satz 4.4.5 *Sei* $0 \neq h \in \mathrm{End}_h(\mathbb{C}^n)$ *und* $J := [-\varepsilon, \varepsilon]$ *ein Intervall, sodass* $h_t := th + \mathrm{id}$ *für* $t \in J$ *nur positive Eigenwerte hat. Dann ist die Funktion*

$$f \ : \ J \to \mathbb{R}, \ t \mapsto \det(h_t)$$

strikt logarithmisch konkav und $\frac{1}{f}$ *ist strikt konvex.*

Beweis: [Mar03, Proposition 3.1.14]. □

Ab hier bezeichne $\alpha \in \mathrm{End}_h(\mathbb{C}^n)$ den Endomorphismus, den $\mathcal{A} \in \mathcal{H}_n$ bezüglich der Standardbasis auf $\mathbb{C}^n$ induziert.

Lemma 4.4.6 *1. Es existiert eine Umgebung* U *von* 0 *in* $\mathrm{End}_h(\mathbb{C}^n)$*, sodass für jedes* $h \in U$ *mit* $\mathrm{Spur}(h) \leq 0$ *und jedes* $g \in \mathrm{End}(\mathbb{C}^n)$ *mit* $g \circ \alpha \circ g^* = \alpha + h$ *gilt:* $g \in U(\mathbb{C}^n, \alpha)$ *- das heißt die Hermitesche Konjugation mit* g *lässt* α *fest und somit ist* $h = 0$ *- oder* $|\det(g)| < 1$*.*

2. Sei K *ein abgeschlossener Kegel in* $\mathrm{End}_h(\mathbb{C}^n)$ *mit* $\mathrm{Spur}(h) > 0$ *für alle* $0 \neq h \in K$*. Dann gibt es ein* $\delta > 0$*, sodass für alle* $h \in K$ *mit* $0 < \mathrm{Spur}(h^2) < \delta$ *gilt* $\det(\mathrm{id} + h) > 1$*.*

Beweis:

1. Wir wählen ein $\tau \in \mathrm{GL}(\mathbb{C}^n)$, welches $\tau \circ \alpha \circ \tau^* = \mathrm{id}$ erfüllt (dies ist möglich, da α eine positiv definite Hermitesche Form definiert) und erhalten somit

   $$\tau \circ g^* \circ \alpha \circ g \circ \tau^* = \mathrm{id} + \tau \circ h \circ \tau^*$$

   Sind $\lambda_1, ..., \lambda_n$ die Eigenwerte von $\tau \circ h \circ \tau^*$, so sind $1 + \lambda_1, ..., 1 + \lambda_n$ die Eigenwerte von $\mathrm{id} + \tau \circ h \circ \tau^*$.
   Durch eine geeignete Wahl von U können wir sicherstellen, dass die $1 + \lambda_i$ für jedes $1 \leq i \leq n$ und für alle $g \in U$ positiv sind. Nun betrachte man $f_1 := \log(f_h)$ mit

   $$f_h \ : \ [0, 1] \to \mathbb{R}, \ t \mapsto \det(\mathrm{id} + t \cdot \tau \circ h \circ \tau^*) = \prod_{i=1}^{n} (1 + t\lambda_i)$$

   Wir haben dann $f_1'(t) = \sum_{i=1}^{n} \frac{\lambda_i}{1 + t\lambda_i}$; insbesondere $f_1'(0) = \mathrm{Spur}(h) \leq 0$. Ist nun $h = 0$, so liegt g in $U(\mathbb{C}^n, \alpha)$.

Ist $h \neq 0$, so ist f_1 nach 4.4.5 strikt konkav, wodurch f_1' streng monoton fallend ist und für alle $t \in [0,1]$ gilt, dass $f_1'(t) \leq 0$. Insbesondere ist dann $f_1(1) < f_1(0) = 0$, woraus

$$\det(\mathrm{id} + \tau \circ h \circ \tau^*) = \exp(f_1(1)) = \exp(f_1(0)) = 1$$

folgt. Wegen $|\det(\tau)|^2 \cdot \det(\alpha) = 1$ erhalten wir daraus sofort $|\det(g)| < 1$.

2. [Mar03, Lemma 3.4.4 (2)]

□

Bemerkung 4.4.7 (Polarzerlegung) *Es sei $(V, \mathcal{A})$ ein unitärer Vetkorraum. Dann besitzt jedes $g \in \mathrm{GL}(V)$ eine eindeutige Faktorisierung in $g = g_h \circ g_u$ mit g_h Hermitesch und $\mathcal{A}[g_u] = \mathcal{A}$.*

Lemma 4.4.8 *Sei $\mathcal{A} \in \mathcal{H}_n$. Dann gibt es eine Umgebung U von $\mathrm{id} \in \mathrm{End}(\mathbb{C}^n)$, sodass*

$$S_i(\mathcal{A}[g]) \subseteq S_i(\mathcal{A})g \ \forall \ g \in U$$

Beweis: Setze $m_1 := \min_{L_i}(\mathcal{A})$, $m_2 := \min\left\{ \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} \mid x \in L_i,\ \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} > m_1 \right\}$ und schreibe $g = g_h \circ g_u$ mit $\mathcal{A}[g_u] = \mathcal{A}$ und g_h Hermitesch. Wähle U nun so klein, dass für jedes $g \in U$ alle Eigenwerte von g_h positiv sind und $\left(\frac{\lambda_{\max}}{\lambda_{\min}}\right)^2 < \frac{m_2}{m_1}$ für den größten und kleinsten Eigenwert von g_h gilt.
Nun wähle man $x \in L_i$ mit $\frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} > m_1$ - also $\frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} \geq m_2$ - und $y \in L_i$ mit $\frac{\mathcal{A}[y]}{N(\mathfrak{a}_y)} = m_1$. Dann gilt

$$\frac{\mathcal{A}[yg]}{N(\mathfrak{a}_y)} = \frac{\mathcal{A}[yg_h]}{N(\mathfrak{a}_y)} \leq \lambda_{\max}^2 \frac{\mathcal{A}[y]}{N(\mathfrak{a}_y)} = \lambda_{\max}^2 m_1$$

und daher

$$\frac{\mathcal{A}[xg]}{N(\mathfrak{a}_x)} = \frac{\mathcal{A}[xg_h]}{N(\mathfrak{a}_x)} \geq \lambda_{\min}^2 \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)} \geq \lambda_{\min}^2 m_2 > \frac{\mathcal{A}[yg]}{N(\mathfrak{a}_y)}$$

Dies zeigt die Behauptung. □

Lemma 4.4.9 *Es existiert eine Umgebung U von $\mathrm{id} \in \mathrm{End}(\mathbb{C}^n)$, so dass für alle $g \in U$ genau dann $\min_{L_i}(\mathcal{A}[g]) = \min_{L_i}(\mathcal{A})$ gilt, wenn $\min\left\{ \frac{\varphi_x(h_g)}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A}) \right\} = 0$ gilt, wobei $h_g \in \mathrm{End}_h(\mathbb{C}^n)$ definiert sei als die Abbildung, die von $\mathcal{A}[g] - \mathcal{A}$ bezüglich der Standardbasis induziert wird.*

Beweis: Man wähle U so klein, dass $S_i(\mathcal{A}[g]) \subseteq S_i(\mathcal{A})g$ für alle $g \in U$ gilt. Für $x \in S_i(\mathcal{A})$ erhalten wir dann

$$\begin{aligned}\frac{\mathcal{A}[xg]}{N(\mathfrak{a}_x)} &= \frac{\mathcal{A}[xg_h]}{N(\mathfrak{a}_x)} = \frac{1}{N(\mathfrak{a}_x)}(x\mathcal{A}[g_h], x) \\ &= \frac{1}{N(\mathfrak{a}_x)}\left(\varphi_x(\mathcal{A}) + \varphi_x(h_g)\right)\end{aligned}$$

Also haben wir $\min_{L_i}(\mathcal{A}[g]) = \min_{L_i}(\mathcal{A}) + \min\left\{\frac{\varphi_x(h_g)}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A})\right\}$, damit ist die Behauptung bewiesen. □

Satz 4.4.10 *Sei $\mathcal{A} \in \mathcal{H}_n$. Dann ist $\mathcal{A}$ genau dann γ_i-extrem, wenn für jedes $h \in \mathrm{End}_h(\mathbb{C}^n)$ mit $\mathrm{Spur}(h) \leq 0$ und $\min\left\{\frac{\varphi_x(h)}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A})\right\} = 0$ gilt, dass $h = 0$.*

Beweis: $\mathcal{A}$ ist γ_i-extrem, falls eine Umgebung U von $\mathrm{id} \in \mathrm{End}(\mathbb{C}^n)$ existiert, sodass für alle $g \in U$ gilt

$$\gamma_i(\mathcal{A}[g]) \geq \gamma_i(\mathcal{A}) \Longrightarrow g \in \mathbb{R}^* U(\mathbb{C}^n, \mathcal{A})$$

Dabei sei die unitäre Gruppe bezüglich $\mathcal{A}$. Es gilt dann natürlich auch $\gamma_i(\mathcal{A}[g]) = \gamma_i(\mathcal{A})$. Da wir mit $\mathbb{R}^*$ skalieren dürfen, müssen wir nur solche $g \in U$ betrachten, die $\min_{L_i}(\mathcal{A}[g]) = \min_{L_i}(\mathcal{A})$ erfüllen. Für $h_g := g\circ\alpha\circ g^* - \alpha \in \mathrm{End}_h(\mathbb{C}^n)$ gilt dann $\min\left\{\frac{\varphi_x(h_g)}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A})\right\} = 0$; die Abbildungen h_g liegen also im abgeschlossenen Kegel

$$\mathcal{K} := \left\{h \in \mathrm{End}_h(\mathbb{C}^n) \mid \frac{\varphi_x(h)}{N(\mathfrak{a}_x)} \geq 0 \ \forall\ x \in S_i(\mathcal{A})\right\}$$

Sei nun $\mathcal{A}$ extrem und $h_g \in \mathcal{K}$ mit $\mathrm{Spur}(h_g) \leq 0$. Dann ist nach 4.4.6 entweder $\mathcal{A}[g] = \mathcal{A}$ oder $|\det(g)| < 1$. Im letzteren Fall ist $\det(\mathcal{A}[g]) < \det(\mathcal{A})$. Weil jedoch die L_i-Minima von $\mathcal{A}[g]$ und $\mathcal{A}$ übereinstimmen, ist dann $\gamma_i(\mathcal{A}[g]) > \gamma_i(\mathcal{A})$, was ob der γ_i-Extremalität von $\mathcal{A}$ nicht möglich ist. Es tritt also der erste Fall ein, was $h_g = 0$ impliziert.

Nun gelte umgekehrt die Implikation

$$\forall\ h \in \mathrm{End}_h(\mathbb{C}^n),\ \mathrm{Spur}(h) \leq 0,\ \min\left\{\frac{\varphi_x(h)}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A})\right\} = 0 \Longrightarrow h = 0$$

und wir nehmen an, dass $\mathcal{A}$ nicht γ_i-extrem ist. Dann existiert in jeder Umgebung U von $\mathrm{id} \in \mathrm{End}(\mathbb{C}^n)$ ein $g \in U$ mit $\min_{L_i}(\mathcal{A}) = \min_{L_i}(\mathcal{A}[g])$ (also $h_g = g \circ \alpha \circ g^* - \alpha \in \mathcal{K}$) und $\gamma_i(\mathcal{A}[g]) \geq \gamma_i(\mathcal{A})$, aber $g \notin U(\mathbb{C}^n, \mathcal{A})$.
Es ist dann $|\det(g)| \leq 1$, woraus wir

$$\det(h_g + \alpha) = \det(\mathcal{A}[g]) \leq \det(\mathcal{A})$$

erhalten. Indem wir g hinreichend nah bei id wählen, erreichen wir, dass h_g beliebig nah an 0 liegt. Wegen 4.4.6 kann dann nicht für jedes $g \in U$ $\mathrm{Spur}(h_g) > 0$ sein; es existiert folglich ein $0 \neq h \in \mathcal{K}$ mit $\mathrm{Spur}(h_g) < 0$. Dies ist ein Widerspruch. □

Satz 4.4.11 *Ist $\mathcal{A} \in \mathcal{H}_n$, so ist $\mathcal{A}$ genau dann γ_i-extrem, wenn es γ_i-perfekt und γ_i-eutaktisch ist.*

Beweis: Sei $\mathcal{A}$ zunächst γ_i-eutaktisch und γ_i-perfekt. Wir betrachten $h \in \mathrm{End}_h(\mathbb{C}^n)$ mit $\min\left\{\frac{\varphi_x(h)}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A})\right\} = 0$ und $\mathrm{Spur}(h) \leq 0$. Weil $\mathcal{A}$ γ_i-eutaktisch ist, haben wir

$$\mathrm{Spur}(h) = \sum_{x \in S_i(\mathcal{A})} \eta_x \varphi_x(h)$$

mit strikt positiven η_x.
Es gilt nun $\varphi_x(h) \geq 0$ und $\mathrm{Spur}(h) \leq 0$, also $\varphi_x(h) = 0$ für jedes $x \in S_i(\mathcal{A})$. Daraus folgt $h = 0$, da die γ_i-Perfektion von $\mathcal{A}$ impliziert, dass die φ_x den Raum $\mathrm{End}_h(\mathbb{C}^n)^*$ erzeugen. $\mathcal{A}$ ist also γ_i-extrem nach 4.4.10.

Es sei nun umgekehrt $\mathcal{A}$ γ_i-extrem. Wir möchten zeigen, dass $\mathcal{A}$ γ_i-extrem und γ_i-eutaktisch ist.
γ_i-Perfektion: Es sei $h \in \mathrm{End}_h(\mathbb{C}^n)$ mit $\varphi_x(h) = 0$ für jedes $x \in S_i(\mathcal{A})$. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $\mathrm{Spur}(h) \leq 0$, indem wir sonst h durch $-h$ ersetzen. Weil $\mathcal{A}$ γ_i-extrem ist, liefert 4.4.10, dass dann $h = 0$ ist. Somit haben wir aber $\langle \varphi_x \mid x \in S_i(\mathcal{A})\rangle = \mathrm{End}_h(\mathbb{C}^n)^*$; $\mathcal{A}$ ist also γ_i-extrem.
γ_i-Eutaxie: Man wende den Satz von Stiemke (4.4.4) auf die Linearformen φ_x für $x \in S_i(\mathcal{A})$ sowie $-\mathrm{Spur}$ an. Dazu ist zu zeigen, dass die Ungleichungen $\varphi_x(h) \geq 0$ für alle $x \in S_i(\mathcal{A})$ und $\mathrm{Spur}(h) \leq 0$ die Gleichheiten $0 = \varphi_x(h) = \mathrm{Spur}(h)$ implizieren.
Sei $k \in \mathbb{R}$, setze $h' := h - k\alpha$. Dann haben wir $\mathrm{Spur}(h') = \mathrm{Spur}(h) - kn$ sowie für jedes $x \in S_i(\mathcal{A})$

$$\begin{aligned}\varphi_x(h') &= \varphi_x(h) - k\varphi_x(\alpha) \\ &= \varphi_x(h) - kN(\mathfrak{a}_x)\min_{L_i}(\mathcal{A})\end{aligned}$$

Nun wählen wir k so, dass $\min\left\{\frac{\varphi_x(h')}{N(\mathfrak{a}_x)} \mid x \in S_i(\mathcal{A})\right\} = 0$. Sicherlich ist dann $k \geq 0$ und somit $\mathrm{Spur}(h') \leq \mathrm{Spur}(h) \leq 0$. 4.4.10 impliziert dann, dass $h' = 0$, also $h = k\alpha$. Wir haben aber $0 \geq \mathrm{Spur}(h) = k\mathrm{Spur}(\alpha)$. Es folgt $k = 0$ und somit $h = 0$. Der Satz von Stiemke liefert nun die γ_i-Eutaxiebedingung für $\mathcal{A}$. □

Korollar 4.4.12 *Die Hermite-Konstante $\gamma_{n,K}$ ist algebraisch über $\mathbb{Q}$; ihre n-te Potenz ist eine rationale Zahl.*

Beweis: Die Hermite-Konstante wird von einer γ_i-extremen Form $\mathcal{A}$ realisiert. Diese ist also insbesondere γ_i-perfekt und somit nach 4.3.7 in $K^{n\times n}$ enthalten. $\square$

4.5. Der Voronoi-Algorithmus

4.5.1. Voronoi-Bereiche

Definition 4.5.1 *Sei $\mathcal{A} \in \mathcal{H}_n$ positiv definit. Dann nennen wir die Menge*

$$\mathcal{V}_i(\mathcal{A}) := \left\{ \sum_{x \in S_i(\mathcal{A})} \lambda_x \cdot x^* x \mid \lambda_x \in \mathbb{R}_{\geq 0} \right\}$$

den Voronoi-Bereich (genauer den γ_i-Voronoi-Bereich) von $\mathcal{A}$.

Aufgrund der Definition von γ_i-Perfektion ist die folgende Bemerkung sofort klar.

Bemerkung 4.5.2 *$\mathcal{V}_i(\mathcal{A})$ ist ein konvexer abgeschlossener Kegel, der im konvexen abgeschlossenen Kegel der positiv definiten Hermiteschen Matrizen enthalten ist.*
$\mathcal{A}$ ist genau dann γ_i-perfekt, wenn $\mathcal{V}_i(\mathcal{A})$ nichtleeres Inneres hat und genau dann, wenn $\mathcal{V}_i(\mathcal{A})$ in keiner Hyperebene von $\mathcal{H}_n$ enthalten ist.

Bemerkung 4.5.3 *Das relative Innere von $\mathcal{V}_i(\mathcal{A})$ ist*

$$\left\{ \sum_{x \in S_i(\mathcal{A})} \lambda_x \cdot x^* x \mid \lambda_x \in \mathbb{R}_{>0} \right\}$$

Definition 4.5.4 *Sei $\mathcal{A} \in \mathcal{H}_n$ positiv definit. Eine Seite von $\mathcal{V}_i(\mathcal{A})$ ist eine Hyperebene $\mathcal{S}$ in $\mathcal{H}_n$, mit $\dim(\langle \mathcal{S} \cap V_i(\mathcal{A}) \rangle) = \dim(\langle \mathcal{V}_i(\mathcal{A}) \rangle) - 1$, sodass $\mathcal{V}_i(\mathcal{A})$ in genau einem der durch $\mathcal{S}$ erklärten Halbräume liegt.*

Ist $\mathcal{A}$ überdies γ_i-perfekt, so definieren wir einen Seitenvektor von $\mathcal{A}$ zur Seite $\mathcal{S}$ als ein $0 \neq R \in \mathcal{H}_n$ mit den Eigenschaften

$$\mathrm{Spur}(RS) = 0 \ \forall \ S \in \mathcal{S}, \quad \mathrm{Spur}(RT) \geq 0 \ \forall \ T \in \mathcal{V}_i(\mathcal{A}).$$

Wir merken sofort an, dass $R \in \mathcal{H}_n$ genau dann ein Seitenvektor zur Seite $\mathcal{S}$ von $\mathcal{V}_i(\mathcal{A})$ ist, wenn

1. Für alle $x \in S_i(\mathcal{A})$ mit $x^*x \in \mathcal{S}$ gilt $\mathrm{Spur}(x^*xR) = R[x] = 0$

2. Für alle $x \in S_i(\mathcal{A})$ mit $x^*x \notin \mathcal{S}$ gilt $\mathrm{Spur}(x^*xR) = R[x] > 0$.

Folglich kann der Seitenvektor als Erzeuger der Lösungsmenge eines homogenen linearen Gleichungssystems mit Koeffizienten in K in $K^{n\times n}$ gewählt werden.

Satz 4.5.5 *Ist $n \geq 2$ und $\mathcal{A} \in \mathcal{H}_n$ γ_i-perfekt und $\mathcal{S}$ eine Seite von $\mathcal{V}_i(\mathcal{A})$ mit Seitenvektor R, so ist R indefinit und es existiert ein $x \in L_i$ mit $R[x] < 0$.*

Beweis: Angenommen R ist nicht indefinit, dann stimmen das Radikal von R, $\{v \in \mathbb{C}^n \mid vR = 0\}$, und die Menge der isotropen Vektoren von R, $\{v \in \mathbb{C}^n \mid R[v] = 0\}$ überein, da $R[x] \geq 0$ für alle $x \in \mathbb{C}^n$ gilt. Die Menge der isotropen Vektoren von R ist also ein Teilraum von $\mathbb{C}^n$ von Dimension $d < n$. Somit ist $\langle v^*v \mid \mathrm{Spur}(v^*vR) = 0\rangle \leq \mathcal{H}_n$ ein Teilraum von Dimension höchstens

$$d^2 \leq (n-1)^2 = n^2 - 2n + 1 \leq n^2 - 3 < n^2 - 1 = \dim \mathcal{H}_n - 1$$

Jedoch ist $\mathcal{S}$ ein Teilraum von Dimension $n^2 - 1$, der von v^*v mit isotropen Vektoren v erzeugt wird. Also ist R indefinit.

Es gibt also ein $x \in \mathbb{C}^n$ mit $R[x] < 0$. Die Abbildung $x \mapsto R[x]$ ist als Polynom stetig und K^n liegt dicht in $\mathbb{C}^n$. Also gibt es ein $y \in K^n$ mit $R[y] < 0$. Multipliziert man y mit allen vorkommenden Nennern, so liegt das Ergebnis in $\mathbb{Z}_K^n$. Multipliziert man diesen Vektor noch mit einem Element in $\mathfrak{a}_i$, so ist der so entstandene Vektor in L_i enthalten. □

Satz 4.5.6 *Seien $\mathcal{A}_1,\ \mathcal{A}_2 \in \mathcal{H}_n$ positiv definit.*

1. *Ist $T \in \mathcal{V}_i(\mathcal{A}_2)$ im relativen Inneren von $\mathcal{V}_i(\mathcal{A}_1)$ enthalten, so gilt $\mathcal{V}_i(\mathcal{A}_1) \subseteq \mathcal{V}_i(\mathcal{A}_2)$.*

2. *Keine Hermitesche Form im Inneren des γ_i-Voronoi-Bereichs einer perfekten Form liegt in irgendeinem anderen γ_i-Voronoi-Bereich.*

Beweis: Es sei ohne Einschränkung $\min_{L_i}(\mathcal{A}_1) = \min_{L_i}(\mathcal{A}_2) =: m$. Ist $T \in \mathcal{V}_i(\mathcal{A}_1) \cap \mathcal{V}_i(\mathcal{A}_2)$, so gibt es $\lambda_x \geq 0$ sodass

$$T = \sum_{x \in S_i(\mathcal{A}_1)} \lambda_x \frac{x^*x}{N(\mathfrak{a}_x)}$$

Daraus erhalten wir sofort

$$\mathrm{Spur}(T\mathcal{A}_1) = \sum_{x \in S_i(\mathcal{A}_1)} \lambda_x \mathrm{Spur}\left(\frac{x^* x \mathcal{A}_1}{N(\mathfrak{a}_x)}\right) = m \sum_{x \in S_i(\mathcal{A}_1)} \lambda_x$$

und

$$\mathrm{Spur}(T\mathcal{A}_2) = \sum_{x \in S_i(\mathcal{A}_1)} \lambda_x \frac{\mathcal{A}_2[x]}{N(\mathfrak{a}_x)} \geq m \sum_{x \in S_i(\mathcal{A}_1)} \lambda_x = \mathrm{Spur}(T\mathcal{A}_1)$$

Analog erhalten wir $\mathrm{Spur}(T\mathcal{A}_2) \leq \mathrm{Spur}(T\mathcal{A}_1)$, also die Gleichheit.
Da T im relativen Inneren von $\mathcal{V}_i(\mathcal{A}_1)$ liegt, sind alle $\lambda_x > 0$. Aus $\mathrm{Spur}(T\mathcal{A}_1) = \mathrm{Spur}(T\mathcal{A}_2)$ folgt nun, dass für alle $x \in S_i(\mathcal{A}_1)$ gilt: $\frac{\mathcal{A}_2[x]}{N(\mathfrak{a}_x)}$.
Es folgt $S_i(\mathcal{A}_1) \subseteq S_i(\mathcal{A}_2)$ und somit auch $\mathcal{V}_i(\mathcal{A}_1) \subseteq \mathcal{V}_i(\mathcal{A}_2)$.

Ist $\mathcal{A}_1$ überdies γ_i-perfekt, so ist es durch die Gleichungen $\frac{\mathcal{A}_1[x]}{N(\mathfrak{a}_x)} = \min_{L_i}(\mathcal{A}_1)$ für alle $x \in S_i(\mathcal{A}_1)$ eindeutig bestimmt. Da in obiger Situation $\mathcal{A}_2$ diese Gleichungen ebenfalls erfüllt, gilt $\mathcal{A}_1 = \mathcal{A}_2$. □

Der folgende Satz ist einer der wichtigsten Bestandteile des Voronoi-Algorithmus.

Satz 4.5.7 *Sei $\mathcal{A}$ γ_i-perfekt und R ein Seitenvektor zur Seite $\mathcal{S}$ von $\mathcal{V}_i(\mathcal{A})$. Setze $S := \{x \in S_i(\mathcal{A}) \mid x^* x \in \mathcal{S}\}$, $m := \min_{L_i}(\mathcal{A})$.*
Für $t \in \mathbb{R}$ definieren wir

$$\mathcal{A}_t := \mathcal{A} + t \cdot R \in \mathcal{H}_n$$

Dann existiert genau ein $\rho \in \mathbb{R}_{>0}$ mit den folgenden Eigenschaften.

1. *Für $0 < t < \rho$ ist $\mathcal{A}_t$ nicht perfekt und $\min_{L_i}(\mathcal{A}_t) = m$.*
   Für $t > \rho$ ist $\mathcal{A}_t$ entweder nicht positiv definit oder $\min_{L_i}(\mathcal{A}_t) < m$.

2. *Für $0 < t < \rho$ ist $S_i(\mathcal{A}_t) = S$.*

3. *Ist $t < 0$, so ist $\mathcal{A}_t$ nicht positiv definit oder $\min_{L_i}(\mathcal{A}_t) < m$.*

4. *$\mathcal{A}_\rho$ ist perfekt mit $\min_{L_i}(\mathcal{A}_\rho) = m$.*
   $\mathcal{S} = \mathcal{V}_i(\mathcal{A}) \cap \mathcal{V}_i(\mathcal{A}_\rho)$; $\mathcal{A}$ und $\mathcal{A}_\rho$ sind die einzigen perfekten Formen, deren γ_i-Voronoi-Bereich $\mathcal{S}$ enthält.

Beweis: Nach 4.5.5 existiert ein $x \in L_i$ mit $R[x] < 0$. Also ist für $\mathcal{A}_t$ indefinit, sobald t hinreichend groß ist. Wir setzen

$$\rho := \inf\{t > 0 \mid \min_{L_i}(\mathcal{A}_t) < m \text{ oder } \mathcal{A}_t \text{ nicht positiv definit}\}$$

ρ ist dann größer als Null.

Sei nun $0 < t < \rho$. Dann ist $\min_{L_i}(\mathcal{A}_t) \geq m$ und wegen $R[x] = 0$ für alle $x \in S$ herrscht Gleichheit. Daher gilt auch die Teilmengenbeziehung $S \subseteq S_i(\mathcal{A}_t)$.
Sei nun $y \in S_i(\mathcal{A}_t)$. Wäre $R[y] < 0$, so wäre für alle $t' > t$

$$\frac{\mathcal{A}_{t'}[y]}{N(\mathfrak{a}_y)} < \min_{L_i}(\mathcal{A}_t) = \min_{L_i}(\mathcal{A})$$

Ebenso erhielte man dies für alle $t' < t$, wenn $R[y] > 0$ wäre. Somit ist $R[y] = 0$ und folglich $y \in S$.
Da $\{x^*x \mid x \in S\}$ in $\mathcal{H}_n$ eine Hyperebene erzeugt, ist $\mathcal{A}_t$ nicht perfekt. Damit sind 1. und 2. bewiesen.

Um 3. einzusehen betrachte man für $t < 0$ ein $y \in S_i(\mathcal{A}) - S$. Dieses erfüllt dann $R[y] > 0$ und somit

$$\frac{\mathcal{A}_t[y]}{N(\mathfrak{a}_y)} = \frac{\mathcal{A}[y]}{N(\mathfrak{a}_y)} + \frac{tR[y]}{N(\mathfrak{a}_y)} < m$$

Ad 4.: Da $\min_{L_i}(\mathcal{A}_t) < \min_{L_i}(\mathcal{A})$ für alle $t > \rho$ gilt, finden wir ein $y \in S_i(\mathcal{A}_\rho)$, welches $R[y] < 0$ erfüllt. Folglich ist $\langle x^*x \mid x \in S \cup \{y\}\rangle = \mathcal{H}_n$ und $\mathcal{A}_\rho$ ist γ_i-perfekt.
Ist nun $\mathcal{A}'$ eine weitere γ_i-perfekte Form, deren γ_i-Voronoi-Bereich $\mathcal{S}$ enthält. Sicherlich schneiden sich $\mathcal{V}_i(\mathcal{A})$ und $\mathcal{V}_i(\mathcal{A}_\rho)$ nur in $\mathcal{S}$. Wegen $\mathcal{V}_i(\mathcal{A}') \supsetneq \mathcal{S}$ gibt es dann einen gemeinsamen inneren Punkt von $\mathcal{V}_i(\mathcal{A}')$ und $\mathcal{V}_i(\mathcal{A})$ oder $\mathcal{V}_i(\mathcal{A}_\rho)$. Aus 4.5.6 folgt dann $\mathcal{A}' = \mathcal{A}$ oder $\mathcal{A}' = \mathcal{A}_\rho$. □

Definition 4.5.8 *Die Hermitesche Form $\mathcal{A}_\rho$ aus dem vorangegangenen Satz heißt direkter perfekter Nachbar von $\mathcal{A}$ zur Seite $\mathcal{S}$.*

Bemerkung 4.5.9 *Ist $\min_{L_i}(\mathcal{A})$ rational, so liegt $\mathcal{A}$ in $K^{n\times n}$. Wählt man den Seitenvektor dann ebenfalls aus $K^{n\times n}$, so ist ρ rational.*

Analog zu 4.5.7 sieht man das folgende Lemma ein.

Lemma 4.5.10 *Sei $\mathcal{A} \in \mathcal{H}_n$ nicht perfekt und $R \in \langle \mathcal{V}_i(\mathcal{A})\rangle^\perp$. Schreibe wieder $\mathcal{A}_t := \mathcal{A} + tR$. Dann existiert genau ein $\rho \in (0, \infty]$ mit der Eigenschaft, dass $\min_{L_i}(\mathcal{A}_t) = \min_{L_i}(\mathcal{A})$ für alle $0 \leq t \leq \rho$ gilt. Ferner ist $\dim(\langle \mathcal{V}_i(\mathcal{A}_\rho)\rangle) > \dim(\langle \mathcal{V}_i(\mathcal{A})$.
Für $t > \rho$ ist das Minimum von $\mathcal{A}_t$ kleiner als das von $\mathcal{A}$ oder $\mathcal{A}_t$ ist nicht positiv definit.*

Definition 4.5.11 *Für das Gitter L_i in Dimension n definieren wir den Voronoi-Graphen als einen Graphen, dessen Ecken die Ähnlichkeitsklassen γ_i-perfekter Hermitescher Formen sind. Die Kanten verbinden gerade diejenigen Klassen, die Vertreter enthalten, die direkte perfekte Nachbarn sind.*

Satz 4.5.12 *Der Voronoi-Graph eines fest gewählten Gitters in Dimension n ist ein endlicher zusammenhängender Graph.*

Beweis: Die Endlichkeit haben wir bereits in 4.3.8 gesehen. Wir zeigen, dass der Graph zusammenhängend ist.
Seien $\mathcal{A}$ und $\mathfrak{B}$ zwei γ_i-perfekte Hermitesche Formen gleichen Minimums. Wir möchten zeigen, dass eine endliche Folge

$$\mathcal{A} = \mathcal{A}_0,\ \mathcal{A}_1,\ \ldots\ \mathcal{A}_r = \mathfrak{B}$$

γ_i-perfekter Formen existiert, sodass für $1 \leq i \leq r$ $\mathcal{A}_{i-1}$ und $\mathcal{A}_i$ direkte perfekte Nachbarn sind.

Zu diesem Zweck wählen wir einen inneren Punkt $T \in \mathcal{V}_i(\mathfrak{B})$. Ist $T \in \mathcal{V}_i(\mathcal{A})$, so gilt $\mathcal{A} = \mathfrak{B}$ nach 4.5.6.
Sonst gibt es einen Seitenvektor R von $\mathcal{A}$ mit $\mathrm{Spur}(TR) < 0$. Definiere nun $\mathcal{A}_1$ als die zu $\mathcal{A}$ über R direkt benachbarte perfekte Form, $\mathcal{A}_1 := \mathcal{A} + \rho R$. Es gilt dann

$$\mathrm{Spur}(\mathcal{A}_1 T) = \mathrm{Spur}((\mathcal{A} + \rho R)T) = \mathrm{Spur}(\mathcal{A}T) + \rho\mathrm{Spur}(RT) < \mathrm{Spur}(\mathcal{A}T)$$

Nun ist $T \in \mathcal{V}_i(\mathcal{A}_1)$ oder wir können $\mathrm{Spur}(\mathcal{A}_i T)$ in jedem weiteren Schritt strikt verkleinern. Dieser Prozess ist endlich nach [Mar03, Theorem 7.3.2] □

Somit führt die Untersuchung der Voronoi-Bereiche einer ersten perfekten Form sowie der Voronoi-Bereiche aller auf diese Weise neu gefundenen perfekten Formen in einem terminierenden Algorithmus zu einer vollständigen Liste aller perfekten Formen in einer festen Dimension.

4.5.2. Implementierung

Es ist, neben der Darstellung der Theorie, ein Ziel dieser Arbeit, den Voronoi-Algorithmus für imaginärquadratische Zahlkörper mit mindestens zwei Idealklassen in Magma [BCP97] zu implementieren. Dazu adaptieren wir den Algorithmus von B. Meyer aus [Mey08], welcher über Körpern mit Klassenzahl 1 alle perfekten Formen auflistet. Die Implementierung greift auf das Programm QHull [BDH96] zurück, um die Seitenflächen der Voronoi-Bereiche zu bestimmen.
Wir werden im Folgenden kurz darlegen, wie der Voronoi-Algorithmus implementiert wurde.

Der implementierte Algorithmus besteht aus zwei Hauptbestandteilen. Der erste Programmteil, **FirstPerfect**, bestimmt mit Hilfe von 4.5.10 eine erste γ_i-perfekte Form über dem Gitter $\mathbb{Z}_K^{n-1} \oplus \mathfrak{a}_i$. Magma stellt Prozeduren bereit, um den zugrundeliegenden Körper K sowie seine Idealklassengruppe $\mathcal{C}\ell_K$ zu bestimmen und mit ihnen zu arbeiten.

Der zweite Bestandteil, **PerfectNeighbours**, bestimmt ausgehend von einer ersten γ_i-perfekten Form alle weiteren γ_i-perfekten Formen. Dazu werden die Seitenflächen des zugehörigen Voronoi-Bereichs bestimmt und zu jeder dieser Seitenflächen der direkte perfekte Nachbar bestimmt (vgl. 4.5.7). Neue perfekte Formen werden der Liste der perfekten Formen hinzugefügt und ebenfalls untersucht, sodass alle perfekten Formen bekannt sind, sobald die Durchführung des Algorithmus beendet ist.

Neben dem Zusatzprogramm QHull ist vor Allem die Spurform 4.2.1 ein unverzichtbares Hilfsmittel, da sie die für $\mathbb{Z}$-Gitter in Magma hinterlegten Funktionen in der vorliegenden Situation nutzbar macht. So verwenden wir sowohl die Prozeduren zur Bestimmung kürzester Vektoren in $\mathbb{Z}$-Gittern als auch die Algorithmen, die Isometrien und Automorphismengruppen von $\mathbb{Z}$-Gittern berechnen (siehe dazu [PS97]).

Da bei der Untersuchung der perfekten Formen von Dimension n $\mathbb{Z}$-Gitter der Dimension $2n$ zu untersuchen sind, wird ab Dimension 4 das Gitter $\mathbb{E}_8$ zu untersuchen sein [HKN11]. Dies ist jedoch mit dem konventionellen Voronoi-Algorithmus nicht in zufriedenstellender Zeit zu bewerkstelligen. Es sei daher darauf hingewiesen, dass der vorliegende Algorithmus in aller Regel nur in den Dimensionen 2 und 3 funktionieren kann.

A. Rechnerische Ergebnisse in Dimension 2

In diesem Abschnitt stellen wir die Ergebnisse des implementierten Algorithmus in Dimension 2 vor.

A.1. $\mathbb{Q}(\sqrt{-5})$

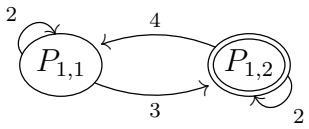
Die Vertreter der Ähnlichkeitsklassen perfekter Formen über dem Gitter $L_i := \mathbb{Z}_K \oplus \mathfrak{a}_i$ notieren wir im Folgenden stets als $P_{i,j}$.
Darauffolgend listen wir wichtige Invarianten auf und stellen den Voronoi-Graphen im Bild oder durch seine Adjazenzmatrix dar. Im letzteren Fall beschreibt der Eintrag (k, ℓ) der Adjazenzmatrix die Anzahl der Seitenflächen des Voronoi-Bereichs von $P_{i,k}$, die $P_{i,\ell}$ als direkten perfekten Nachbarn liefern.

Die angegebenen Hermiteschen Formen P sind jeweils so skaliert, dass ihr Minimum stets $\min_L(P) = 1$ erfüllt.

$\mathcal{C}\ell_K = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2]\} \cong C_2$, $\mathfrak{a}_1 := \mathbb{Z}_K$, $\mathfrak{a}_2 := \langle 2,\ 1 + \sqrt{-5} \rangle$

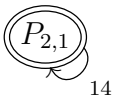
$$P_{1,1} := \begin{pmatrix} 1 & \frac{1}{10}(5 + 3\sqrt{-5}) \\ \frac{1}{10}(5 - 3\sqrt{-5}) & 1 \end{pmatrix}$$
$$P_{1,2} := \begin{pmatrix} 1 & \frac{1}{5}(5 + 2\sqrt{-5}) \\ \frac{1}{5}(5 - 2\sqrt{-5}) & 2 \end{pmatrix}$$

P	$\det_{L_1}(P)$	$\lvert S_{L_1}(P)\rvert$	Seiten	$\mathrm{Aut}(L_1, P)$
$(1,1)$	$\frac{3}{10}$	6	5	C_6
$(1,2)$	$\frac{1}{5}$	8	6	Q_8



$$P_{2,1} := \begin{pmatrix} 1 & \frac{1}{10}(5+2\sqrt{-5}) \\ \frac{1}{10}(5-2\sqrt{-5}) & \frac{1}{2} \end{pmatrix}$$

P	$\det_{L_2}(P)$	$\lvert S_{L_2}(P)\rvert$	Seiten	$\mathrm{Aut}(L_2, P)$
$(2,1)$	$\frac{1}{10}$	24	14	$\mathrm{SL}(2,3)$



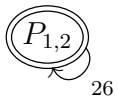
Für die Hermite-Konstante gilt also auf den betrachteten Gittern
$\gamma^{(1)}_{2,\mathbb{Q}(\sqrt{-5})} = \sqrt{5}$
$\gamma^{(2)}_{2,\mathbb{Q}(\sqrt{-5})} = \sqrt{10}$
Der Bestwert $\gamma_{2,\mathbb{Q}(\sqrt{-5})} = \sqrt{10}$ wird von der Hermiteschen Form $(2,1)$ angenommen.

A.2. $\mathbb{Q}(\sqrt{-6})$

$\mathcal{C}\ell_K = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2]\} \cong C_2,\ \mathfrak{a}_1 := \mathbb{Z}_K,\ \mathfrak{a}_2 := \langle 2,\ \sqrt{-6}\rangle$

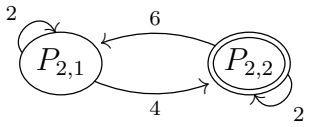
$$P_{1,1} := \begin{pmatrix} 1 & \frac{1}{6}(3+2\sqrt{-6}) \\ \frac{1}{6}(3-2\sqrt{-6}) & 1 \end{pmatrix}$$

P	$\det_{L_1}(P)$	$\lvert S_{L_1}(P)\rvert$	Seiten	$\mathrm{Aut}(L_1, P)$
$(1,1)$	$\frac{1}{12}$	24	26	$\mathrm{SL}(2,3)$



$$P_{2,1} := \begin{pmatrix} 1 & \frac{1}{6}(3+\sqrt{-6}) \\ \frac{1}{6}(3-\sqrt{-6}) & \frac{1}{2} \end{pmatrix}$$
$$P_{2,2} := \begin{pmatrix} 1 & \frac{1}{4}(3+\sqrt{-6}) \\ \frac{1}{4}(3-\sqrt{-6}) & 1 \end{pmatrix}$$

P	$\det_{L_2}(\mathcal{A})$	$\lvert S_{L_2}(\mathcal{A})\rvert$	Seiten	$\mathrm{Aut}(L_2, \mathcal{A})$
$(2,1)$	$\frac{1}{6}$	8	6	Q_8
(2,2)	$\frac{1}{8}$	12	8	$C_3 \rtimes C_4$



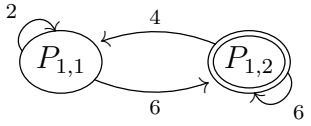
Für die Hermite-Konstante gilt also auf den betrachteten Gittern
$\gamma^{(1)}_{2,\mathbb{Q}(\sqrt{-6})} = \sqrt{12}$
$\gamma^{(2)}_{2,\mathbb{Q}(\sqrt{-6})} = \sqrt{8}$
Der Bestwert $\gamma_{2,\mathbb{Q}(\sqrt{-6})} = \sqrt{12}$ wird von der Hermiteschen Form $(1,1)$ angenommen.

A.3. $\mathbb{Q}(\sqrt{-10})$

$\mathcal{C}\ell_K = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2]\} \cong C_2$, $\mathfrak{a}_1 := \mathbb{Z}_K$, $\mathfrak{a}_2 := \left\langle 2,\ \sqrt{-10} \right\rangle$

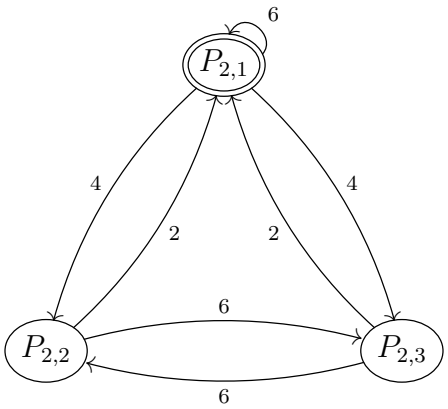
$$P_{1,1} := \begin{pmatrix} 1 & \frac{1}{4}(2+\sqrt{-10}) \\ \frac{1}{4}(2-\sqrt{-10}) & 1 \end{pmatrix}$$
$$P_{1,2} := \begin{pmatrix} 1 & \frac{1}{30}(15+11\sqrt{-10}) \\ \frac{1}{30}(15-11\sqrt{-10}) & \frac{5}{3} \end{pmatrix}$$

P	$\det_{L_1}(P)$	$\lvert S_{L_1}(P)\rvert$	Seiten	$\mathrm{Aut}(L_1, P)$
$(1,1)$	$\frac{1}{8}$	6	8	C_6
$(1,2)$	$\frac{13}{180}$	12	10	C_4



$$P_{2,1} := \begin{pmatrix} 1 & \frac{1}{20}(10+3\sqrt{-10}) \\ \frac{1}{20}(10-3\sqrt{-10}) & \frac{1}{2} \end{pmatrix}$$
$$P_{2,2} := \begin{pmatrix} 4 & \frac{1}{20}(45+14\sqrt{-10}) \\ \frac{1}{20}(45-14\sqrt{-10}) & \frac{5}{2} \end{pmatrix}$$
$$P_{2,3} := \begin{pmatrix} 5 & \frac{1}{20}(55+14\sqrt{-10}) \\ \frac{1}{20}(55-14\sqrt{-10}) & \frac{5}{2} \end{pmatrix}$$

P	$\det_{L_2}(P)$	$\lvert S_{L_2}(P)\rvert$	Seiten	$\mathrm{Aut}(L_2, P)$
$(2,1)$	$\frac{1}{20}$	24	14	$\mathrm{SL}(2,3)$
$(2,2)$	$\frac{3}{40}$	12	8	$C_3 \rtimes C_4$
$(2,3)$	$\frac{3}{40}$	12	8	$C_3 \rtimes C_4$



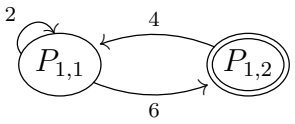
Für die Hermite-Konstante gilt also auf den betrachteten Gittern
$\gamma^{(1)}_{2,\mathbb{Q}(\sqrt{-10})} = \sqrt{\frac{180}{13}}$
$\gamma^{(2)}_{2,\mathbb{Q}(\sqrt{-10})} = \sqrt{20}$
Der Bestwert $\gamma_{2,\mathbb{Q}(\sqrt{-10})} = \sqrt{20}$ wird von der Hermiteschen Form $(2,1)$ angenommen.

A.4. $\mathbb{Q}(\sqrt{-15})$

$\mathcal{C}\ell_K = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2]\} \cong C_2$, $\mathfrak{a}_1 := \mathbb{Z}_K$, $\mathfrak{a}_2 := \left\langle 2,\ \frac{\sqrt{-15}+1}{2} - 1 \right\rangle$

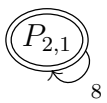
$$P_{1,1} := \begin{pmatrix} 1 & \frac{1}{6}(3+\sqrt{-15}) \\ \frac{1}{6}(3-\sqrt{-15}) & 1 \end{pmatrix}$$
$$P_{1,2} := \begin{pmatrix} 2 & \frac{1}{10}(15+3\sqrt{-15}) \\ \frac{1}{10}(15-3\sqrt{-15}) & 2 \end{pmatrix}$$

P	$\det_{L_1}(P)$	$\lvert S_{L_1}(P)\rvert$	Seiten	$\mathrm{Aut}(L_1, P)$
$(1,1)$	$\frac{1}{3}$	6	8	C_6
$(1,2)$	$\frac{2}{5}$	4	4	C_4



$$\begin{pmatrix} 1 & \frac{1}{10}(5+\sqrt{-15}) \\ \frac{1}{10}(5-\sqrt{-15}) & \frac{1}{2} \end{pmatrix}$$

P	$\det_{L_2}(P)$	$\lvert S_{L_2}(P)\rvert$	Seiten	$\mathrm{Aut}(L_2, P)$
$(2,1)$	$\frac{1}{5}$	12	8	$C_3 \rtimes C_4$



Für die Hermite-Konstante gilt also auf den betrachteten Gittern
$\gamma^{(1)}_{2,\mathbb{Q}(\sqrt{-15})} = \sqrt{3}$
$\gamma^{(2)}_{2,\mathbb{Q}(\sqrt{-15})} = \sqrt{5}$
Der Bestwert $\gamma_{2,\mathbb{Q}(\sqrt{-15})} = \sqrt{5}$ wird von der Hermiteschen Form $(2,1)$ angenommen.

A.5. $\mathbb{Q}(\sqrt{-21})$

$\mathcal{C}\ell_K = \{[\mathfrak{a}_i] \mid 1 \leq i \leq 4\} \cong C_2 \times C_2$,
$\mathfrak{a}_1 := \mathbb{Z}_K$, $\mathfrak{a}_2 := \langle 2,\ \sqrt{-21} - 1\rangle$, $\mathfrak{a}_3 := \langle 5,\ \sqrt{-21} - 2\rangle$, $\mathfrak{a}_4 := \langle 3,\ \sqrt{-21}\rangle$

$$P_{1,1} := \begin{pmatrix} 1 & \frac{1}{6}(3+\sqrt{-21}) \\ \frac{1}{6}(3-\sqrt{-21}) & 1 \end{pmatrix}$$
$$P_{1,2} := \begin{pmatrix} 1 & \frac{1}{14}(7+4\sqrt{-21}) \\ \frac{1}{14}(7-4\sqrt{-21}) & 2 \end{pmatrix}$$
$$P_{1,3} := \begin{pmatrix} 1 & \frac{1}{14}(14+3\sqrt{-21}) \\ \frac{1}{14}(14-3\sqrt{-21}) & 2 \end{pmatrix}$$
$$P_{1,4} := \begin{pmatrix} 13 & \frac{1}{6}(39+23\sqrt{-21}) \\ \frac{1}{6}(39-23\sqrt{-21}) & 27 \end{pmatrix}$$
$$P_{1,5} := \begin{pmatrix} 5 & \frac{1}{14}(35+19\sqrt{-21}) \\ \frac{1}{14}(35-19\sqrt{-21}) & 9 \end{pmatrix}$$
$$P_{1,6} := \begin{pmatrix} 23 & \frac{1}{7}(84+45\sqrt{-21}) \\ \frac{1}{7}(84-45\sqrt{-21}) & 44 \end{pmatrix}$$

P	$\det_{L_1}(P)$	$\lvert S_{L_1}(P)\rvert$	Seiten	$\mathrm{Aut}(L_1, P)$
$(1,1)$	$\frac{1}{6}$	6	8	C_6
$(1,2)$	$\frac{1}{28}$	24	26	$C_3 \rtimes C_4$
$(1,3)$	$\frac{1}{28}$	24	26	$C_3 \rtimes C_4$
$(1,4)$	$\frac{1}{6}$	6	8	C_6
$(1,5)$	$\frac{1}{14}$	12	8	C_6
$(1,6)$	$\frac{1}{7}$	8	6	C_4

Adjazenzmatrix des Voronoi-Graphen:

$$\begin{pmatrix} 2 & 3 & 3 & 0 & 0 & 0 \\ 6 & 0 & 12 & 6 & 2 & 0 \\ 6 & 12 & 0 & 6 & 2 & 0 \\ 0 & 3 & 3 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 4 & 2 \end{pmatrix}$$

$$P_{2,1} := \begin{pmatrix} 1 & \frac{1}{42}(21+4\sqrt{-21}) \\ \frac{1}{42}(21-4\sqrt{-21}) & \frac{1}{2} \end{pmatrix}$$
$$P_{2,2} := \begin{pmatrix} 2 & \frac{1}{14}(14+3\sqrt{-21}) \\ \frac{1}{14}(14-3\sqrt{-21}) & 1 \end{pmatrix}$$
$$P_{2,3} := \begin{pmatrix} \frac{7}{3} & \frac{1}{42}(35+6\sqrt{-21}) \\ \frac{1}{42}(35-6\sqrt{-21}) & \frac{1}{2} \end{pmatrix}$$
$$P_{2,4} := \begin{pmatrix} \frac{7}{3} & \frac{1}{14}(21+2\sqrt{-21}) \\ \frac{1}{14}(21-2\sqrt{-21}) & \frac{7}{6} \end{pmatrix}$$
$$P_{2,5} := \begin{pmatrix} 7 & \frac{1}{42}(147+32\sqrt{-21}) \\ \frac{1}{42}(147-32\sqrt{-21}) & \frac{7}{2} \end{pmatrix}$$

P	$\det_{L_2}(P)$	$\lvert S_{L_2}(P)\rvert$	Seiten	$\mathrm{Aut}(L_2, P)$
$(2,1)$	$\frac{5}{42}$	8	6	C_4
$(2,2)$	$\frac{1}{14}$	8	6	C_4
$(2,3)$	$\frac{11}{126}$	8	6	C_2
$(2,4)$	$\frac{11}{126}$	8	6	C_2
$(2,5)$	$\frac{5}{42}$	8	6	C_4

Adjazenzmatrix des Voronoi-Graphen:

$$\begin{pmatrix} 1 & 1 & 2 & 2 & 0 \\ 1 & 0 & 2 & 2 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 2 & 1 \end{pmatrix}$$

$$P_{3,1} := \begin{pmatrix} 1 & \frac{1}{105}(42+4\sqrt{-21}) \\ \frac{1}{105}(42-4\sqrt{-21}) & \frac{1}{5} \end{pmatrix}$$
$$P_{3,2} := \begin{pmatrix} 25 & \frac{1}{105}(1092+94\sqrt{-21}) \\ \frac{1}{105}(1092-94\sqrt{-21}) & 5 \end{pmatrix}$$
$$P_{3,3} := \begin{pmatrix} 10 & \frac{1}{30}(129+8\sqrt{-21}) \\ \frac{1}{30}(129-8\sqrt{-21}) & 2 \end{pmatrix}$$
$$P_{3,4} := \begin{pmatrix} 13 & \frac{1}{30}(156+17\sqrt{-21}) \\ \frac{1}{30}(156-17\sqrt{-21}) & \frac{13}{5} \end{pmatrix}$$
$$P_{3,5} := \begin{pmatrix} \frac{4}{3} & \frac{1}{45}(21+2\sqrt{-21}) \\ \frac{1}{45}(21-2\sqrt{-21}) & \frac{1}{5} \end{pmatrix}$$

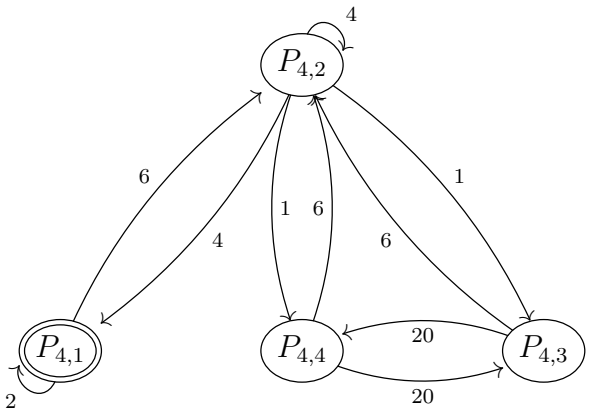
P	$\det_{L_3}(P)$	$\lvert S_{L_3}(P)\rvert$	Seiten	$\mathrm{Aut}(L_3, P)$
$(3,1)$	$\frac{1}{21}$	16	10	Q_8
$(3,2)$	$\frac{1}{21}$	16	10	Q_8
$(3,3)$	$\frac{1}{12}$	8	6	C_4
$(3,4)$	$\frac{1}{12}$	8	6	C_4
$(3,5)$	$\frac{1}{27}$	16	10	C_4

Adjazenzmatrix des Voronoi-Graphen:

$$\begin{pmatrix} 0 & 4 & 2 & 2 & 2 \\ 4 & 0 & 2 & 2 & 2 \\ 1 & 1 & 0 & 2 & 2 \\ 1 & 1 & 2 & 0 & 2 \\ 1 & 1 & 2 & 2 & 4 \end{pmatrix}$$

$$P_{4,1} := \begin{pmatrix} 1 & \frac{1}{18}(9+\sqrt{-21}) \\ \frac{1}{18}(9-\sqrt{-21}) & \frac{1}{3} \end{pmatrix}$$
$$P_{4,2} := \begin{pmatrix} 2 & \frac{1}{12}(11+\sqrt{-21}) \\ \frac{1}{12}(11-\sqrt{-21}) & \frac{1}{2} \end{pmatrix}$$
$$P_{4,3} := \begin{pmatrix} 11 & \frac{1}{42}(217+23\sqrt{-21}) \\ \frac{1}{42}(217-23\sqrt{-21}) & 3 \end{pmatrix}$$
$$P_{4,4} := \begin{pmatrix} 5 & \sqrt{1}42(91+5\sqrt{-21}) \\ \frac{1}{42}(91-5\sqrt{-21}) & 1 \end{pmatrix}$$

P	$\det_{L_4}(P)$	$\lvert S_{L_4}(P)\rvert$	Seiten	$\mathrm{Aut}(L_4, P)$
$(4,1)$	$\frac{1}{18}$	12	8	C_6
$(4,2)$	$\frac{1}{24}$	16	10	C_4
$(4,3)$	$\frac{1}{42}$	48	26	$\mathrm{SL}(2,3)$
$(4,4)$	$\frac{1}{42}$	48	26	$\mathrm{SL}(2,3)$



Für die Hermite-Konstante gilt also auf den betrachteten Gittern
$\gamma^{(1)}_{2,\mathbb{Q}(\sqrt{-21})} = \sqrt{28}$
$\gamma^{(2)}_{2,\mathbb{Q}(\sqrt{-21})} = \sqrt{14}$
$\gamma^{(3)}_{2,\mathbb{Q}(\sqrt{-21})} = \sqrt{27}$
$\gamma^{(4)}_{2,\mathbb{Q}(\sqrt{-21})} = \sqrt{42}$
Der Bestwert $\gamma_{2,\mathbb{Q}(\sqrt{-21})} = \sqrt{42}$ wird von den Hermiteschen Formen $(4,3)$ und $(4,4)$ angenommen.

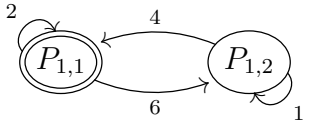
A.6. $\mathbb{Q}(\sqrt{-23})$

$\mathcal{C}\ell_K = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2],\ [\mathfrak{a}_3]\} \cong C_3$, $\mathfrak{a}_1 := \mathbb{Z}_K$, $\mathfrak{a}_2 := \left\langle 2,\ \frac{\sqrt{-23}+1}{2} - 1 \right\rangle$, $\mathfrak{a}_3 := \left\langle 2,\ \frac{\sqrt{-23}+1}{2} \right\rangle$

Es ist $\mathcal{C}\ell_K/\mathcal{C}\ell_K^2 \cong \{1\}$, sodass wir uns wegen 4.3.10 auf die Betrachtung des freien Gitters $\mathbb{Z}_K \oplus \mathbb{Z}_K$ beschränken.

$$P_{1,1} := \begin{pmatrix} 1 & \frac{1}{46}(23 + 7\sqrt{-23}) \\ \frac{1}{46}(23 - 7\sqrt{-23}) & 1 \end{pmatrix}$$
$$P_{1,2} := \begin{pmatrix} 3 & \frac{1}{46}(115 + 15\sqrt{-23}) \\ \frac{1}{46}(115 - 15\sqrt{-23}) & 3 \end{pmatrix}$$

P	$\det_{L_1}(P)$	$\lvert S_{L_1}(P)\rvert$	Seiten	$\mathrm{Aut}(L_1, P)$
$(1,1)$	$\frac{5}{23}$	9	8	C_6
$(1,2)$	$\frac{7}{23}$	6	5	C_4



Die Hermite-Konstante ist also $\gamma_{2,\mathbb{Q}(\sqrt{-23})} = \sqrt{\frac{23}{5}}$.

B. Rechnerische Ergebnisse in Dimension 3

B.1. $h_K = 2$

Ist $\mathcal{C}\ell_K \cong C_2$, so ist $\mathcal{C}\ell_K/\mathcal{C}\ell_K^3 \cong \{1\}$, sodass wir im Fall eines Körpers mit Klassenzahl 2 in dieser Dimension stets bloß das freie Gitter $\mathbb{Z}_K^3$ betrachten.

Wir geben zunächst über den Körpern $\mathbb{Q}(\sqrt{d})$ die Anzahlen der gefundenen perfekten Hermiteschen Formen sowie die Hermite-Konstante an.

d	-5	-6	-15	-10	-13
Anzahl perfekter Formen	92	271	11	≥ 3159	≥ 2746
$\gamma_{3,\mathbb{Q}(\sqrt{d})}$	$\sqrt[3]{20}$	$\sqrt[3]{24}$	$\sqrt[3]{15}$	$\geq \sqrt[3]{\frac{121670}{911}}$	$\geq \sqrt[3]{\frac{632684}{6749}}$

Über dem Körper $\mathbb{Q}(\sqrt{-5})$ wird das globale Maximum der Hermite-Funktion realisiert durch die zwei Hermiteschen Formen

$$\begin{pmatrix} 1 & \frac{1}{10}(5+3\sqrt{-5}) & \frac{1}{2} \\ \frac{1}{10}(5-3\sqrt{-5}) & 1 & 0 \\ \frac{1}{2} & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & \frac{1}{10}(10+7\sqrt{-5}) & \frac{1}{10}(5-2\sqrt{-5}) \\ \frac{1}{10}(10-7\sqrt{-5}) & 2 & \frac{1}{10}(-5-2\sqrt{-5}) \\ \frac{1}{10}(5+2\sqrt{-5}) & \frac{1}{10}(-5+2\sqrt{-5}) & 1 \end{pmatrix}.$$

Über dem Körper $\mathbb{Q}(\sqrt{-6})$ existieren 7 nicht zueinander ähnliche perfekte Hermitesche Formen, die das globale Maximum der Hermite-Funktion realisieren. Es handelt sich um

$$\begin{pmatrix} 1 & \frac{1}{6}(3+2\sqrt{-6}) & \frac{1}{12}(6-\sqrt{-6}) \\ \frac{1}{6}(3-2\sqrt{-6}) & 1 & -\frac{1}{6}\sqrt{-6} \\ \frac{1}{12}(6+\sqrt{-6}) & \frac{1}{6}\sqrt{-6} & 1 \end{pmatrix}, \quad \begin{pmatrix} 3 & \frac{1}{12}(21+10\sqrt{-6}) & \frac{1}{24}(36-5\sqrt{-6}) \\ \frac{1}{12}(21-10\sqrt{-6}) & \frac{5}{2} & \frac{1}{24}(12-13\sqrt{-6}) \\ \frac{1}{24}(36+5\sqrt{-6}) & \frac{1}{24}(12+13\sqrt{-6}) & 1 \end{pmatrix},$$

$$\begin{pmatrix} \frac{5}{2} & \frac{1}{12}(21+10\sqrt{-6}) & \frac{1}{24}(30-7\sqrt{-6}) \\ \frac{1}{12}(21-10\sqrt{-6}) & 3 & \frac{1}{8}(2-5\sqrt{-6}) \\ \frac{1}{24}(30+7\sqrt{-6}) & \frac{1}{8}(2+5\sqrt{-6}) & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & \frac{1}{2}(3+\sqrt{-6}) & \frac{1}{4}(6+\sqrt{-6}) \\ \frac{1}{2}(3-\sqrt{-6}) & 2 & \frac{1}{12}(18-\sqrt{-6}) \\ \frac{1}{4}(6-\sqrt{-6}) & \frac{1}{12}(18+\sqrt{-6}) & 2 \end{pmatrix},$$

$$\begin{pmatrix} 2 & \frac{1}{4}(6+3\sqrt{-6}) & \frac{1}{12}(12-\sqrt{-6}) \\ \frac{1}{4}(6-3\sqrt{-6}) & 3 & \frac{1}{6}(3-2\sqrt{-6}) \\ \frac{1}{12}(12+\sqrt{-6}) & \frac{1}{6}(3+2\sqrt{-6}) & 1 \end{pmatrix}, \quad \begin{pmatrix} 5 & \frac{1}{8}(23+11\sqrt{-6}) & \frac{1}{16}(36-5\sqrt{-6}) \\ \frac{1}{8}(23-11\sqrt{-6}) & 4 & \frac{1}{24}(18-19\sqrt{-6}) \\ \frac{1}{16}(36+5\sqrt{-6}) & \frac{1}{24}(18+19\sqrt{-6}) & \frac{5}{4} \end{pmatrix},$$

$$\begin{pmatrix} \frac{13}{4} & \frac{1}{8}(18+9\sqrt{-6}) & \frac{1}{48}(60-17\sqrt{-6}) \\ \frac{1}{8}(18-9\sqrt{-6}) & 4 & -\frac{2}{3}\sqrt{-6} \\ \frac{1}{48}(60+17\sqrt{-6}) & \frac{2}{3}\sqrt{-6} & 1 \end{pmatrix}.$$

Über dem Körper $\mathbb{Q}(\sqrt{-15})$ wird das globale Maximum der Hermite-Funktion nur von

$$\begin{pmatrix} 1 & \frac{1}{6}(3+\sqrt{-15}) & \frac{1}{30}(15+\sqrt{-15}) \\ \frac{1}{6}(3-\sqrt{-15}) & 1 & 0 \\ \frac{1}{30}(15-\sqrt{-15}) & 0 & 1 \end{pmatrix}$$

angenommen.

B.2. $h_K = 3$

Hier betrachten wir die Körper $\mathbb{Q}(\sqrt{-23})$ und $\mathbb{Q}(\sqrt{-31})$ mit den folgenden Idealklassengruppen:

$$\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-23})} = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2],\ [\mathfrak{a}_3]\} \cong C_3, \mathfrak{a}_1 := \mathbb{Z}_K, \mathfrak{a}_2 := \left\langle 2,\ \tfrac{\sqrt{-23}+1}{2} - 1 \right\rangle, \mathfrak{a}_3 := \left\langle 2,\ \tfrac{\sqrt{-23}+1}{2} \right\rangle$$

$$\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-31})} = \{[\mathfrak{a}_1],\ [\mathfrak{a}_2],\ [\mathfrak{a}_3]\} \cong C_3, \mathfrak{a}_1 := \mathbb{Z}_K, \mathfrak{a}_2 := \left\langle 2,\ \tfrac{\sqrt{-31}+1}{2} \right\rangle, \mathfrak{a}_3 := \left\langle 2,\ \tfrac{\sqrt{-31}+1}{2} - 1 \right\rangle$$

Da über beiden Körpern jeweils $\mathfrak{a}_2 = \overline{\mathfrak{a}_3}$ gilt, können wir unsere Untersuchungen auf die Gitter $\mathbb{Z}_K^3$ und $\mathbb{Z}_K^2 \oplus \mathfrak{a}_2$ beschränken (vgl. 4.3.11).

K	L	Anzahl perfekter Formen	Anzahl perfekter Formen, die das globale Maximum realisieren
$\mathbb{Q}(\sqrt{-23})$			
	$\mathbb{Z}_K^3$	55	1
	$\mathbb{Z}_K^2 \oplus \mathfrak{a}_2$	62	1
$\mathbb{Q}(\sqrt{-31})$			
	$\mathbb{Z}_K^3$	440	1
	$\mathbb{Z}_K^2 \oplus \mathfrak{a}_2$	727	5

Die Hermite-Konstanten bestimmen sich zu $\gamma^{(1)}_{3,\mathbb{Q}(\sqrt{-23})} = \sqrt[3]{\frac{30613}{1029}}$, $\gamma^{(2)}_{3,\mathbb{Q}(\sqrt{-23})} = \sqrt[3]{46}$ sowie $\gamma^{(1)}_{3,\mathbb{Q}(\sqrt{-31})} = \sqrt[3]{\frac{1984}{59}}$, $\gamma^{(2)}_{3,\mathbb{Q}(\sqrt{-31})} = \sqrt[3]{62}$.

C. Quellcode der Implementierung

Dieser Abschnitt stellt den Quellcode des in Magma [BCP97] implementierten Algorithmus vor. Verwendet wird zusätzlich das Programm QHull [BDH96].
Der vorliegende Algorithmus basiert auf dem Programm von B. Meyer aus [Mey08].

```
1  //Perfect Neighbours
2  clear;
3
4  //n beliebig, K imaginaerquad., a beliebig
5
6  n:=3;
7
8  d:=-1;
9  K<w>:=QuadraticField(d);
10 if d mod 4 eq 1 then
11   tau:=(1+w)/2;
12 else
13   tau:=w;
14 end if;
15 C,f:=ClassGroup(K);
16 Idealvertreter:=[];
17 for c in C do Append(~Idealvertreter,f(c)); end for;
18
19 mmax:=Maximum([Norm(p) : p in Idealvertreter]);
20
21 if d ne -1 then
22   F<sqrtd>:=QuadraticField(-d);
23   Injec:=hom<F -> RealField() | Sqrt(-d)>;
24 else
25   F:=Rationals();
26   sqrtd:=1;
27   Injec:=hom<F -> RealField() |>;
28 end if;
```

```
29
30 //Geeigneten Vertreter fuer a aus Idealvertreter fuer p2 waehlen!
31 p1:=Idealvertreter[1];
32 p2:=Idealvertreter[1];
33
34 //Z-Basis von a:
35 if p2 eq p1 then ZB:=[1,tau]; else ZB:=Generators(p2); end if;
36
37 //Z-Basis von L bestimmen
38
39 B:=[];
40 for k in [1..(n-1)] do
41  v:=KMatrixSpace(K,1,n)!0;
42  for i in [1..2] do
43   if i eq 1 then
44    v[1][k]:=K!1;
45   else
46    v[1][k]:=tau;
47   end if;
48   Append(~B,v);
49  end for;
50 end for;
51
52 for i in [1..2] do
53  v:=KMatrixSpace(K,1,n)!0;
54  if i eq 1 then
55   v[1][n]:=ZB[1];
56  else
57   v[1][n]:=ZB[2];
58  end if;
59  Append(~B,v);
60 end for;
61
62 //Normierte R-Basis der Hermiteschen Formen konstruieren:
63
64 BasHermNorm:=[];
65 for i in [1..n] do
66  res:=MatrixRing(K,n)!0;
67  res[i][i]:=1;
68  Append(~BasHermNorm,res);
69  for j in [i+1..n] do
```

```
70    for k in [1..2] do
71     res:=MatrixRing(K,n)!0;
72     if k eq 1 then
73      res[i][j]:=1/2;
74      res[j][i]:=1/2;
75      Append(~BasHermNorm,res);
76     else
77      res[i][j]:=w/2;
78      res[j][i]:=-w/2;
79      Append(~BasHermNorm,res);
80     end if;
81    end for;
82   end for;
83 end for;
84
85 //Hilfsfunktionen
86
87 spurform:=function(A);
88  res:=MatrixRing(Rationals(),2*n) ! 0;
89  for i in [1..2*n] do
90   for j in [1..2*n] do
91    res[i][j]:=Rationals()!
92               Trace(K!(B[i]*A*HermitianTranspose(B[j]))[1][1]);
93   end for;
94  end for;
95  res:=(1/2)*res;
96  return res;
97 end function;
98
99 auswerten:=function(A,x);
100  x:=KMatrixSpace(K,1,n)!x;
101  z:=K!0; N:=K!0; I:=ideal<Integers(K)|0>;
102  z:=K!((x*A*HermitianTranspose(x))[1][1]);
103  for i in [1..n-1] do
104   I:=I+x[1][i]*p1;
105  end for;
106  I:=I+x[1][n]*(p1/p2);
107  N:=Norm(I);
108  return z/N;
109 end function;
110
```

```
kuerzen:=function(A,m,S);
 res:=[];
 for i in [1..#S] do
  x:=Vector(S[i][1]);
  xk:=KMatrixSpace(K,1,n)!0;
  for j in [1..2*n] do
   xk:=xk+x[j]*B[j];
  end for;
  if auswerten(A,xk) eq m then
   Append(~res,xk);
  end if;
 end for;
 return res;
end function;

vektorkuerzen:=function(x);
 res:=KMatrixSpace(K,1,n)!0;
 for j in [1..2*n] do
  res:=res+x[j]*B[j];
 end for;
 return res;
end function;

idealnorm:=function(x);
 N:=0;
 I:=ideal<Integers(K) | 0>;
 for i in [1..n-1] do
  I:=I+x[1][i]*(p1);
 end for;
 I:=I+x[1][n]*(p1/p2);
 N:=Norm(I);
 return N;
end function;

hermitianmin:=function(A);
 L:=LatticeWithGram(spurform(A));
 minL:=Minimum(L);
 S:=ShortVectors(L,minL/mmax,minL*mmax);
 m:=Min([auswerten(A,vektorkuerzen(s[1])) : s in S]);
 return m;
end function;
```

```
152
153 function perfrank(M);
154  VV:=[];
155  for m in M do s:=Matrix(m[1]);
156   v:=HermitianTranspose(s)*Matrix(s);
157   Append(~VV, ElementToSequence(v));
158  end for;
159  return Rank(Matrix(VV)) ;
160 end function;
161
162 RemoveMultiples:=function(M);
163  V:=VectorSpace(K,n);
164  out:=[];
165  Append(~out,M[1]);
166  for m in M do;
167  ismultiple:=false;
168   for v in out do;
169    if Vector(m) in sub<V|[Vector(v)]> then;
170     ismultiple:=true;
171    end if;
172   end for;
173   if not ismultiple then;
174    Append(~out,m);
175   end if;
176  end for;
177  return out;
178 end function;
179
180 isisom:=function(M,N);
181  Me:=spurform(M);
182  Ne:=spurform(N);
183  mul1:=Lcm([Denominator(x) : x in Eltseq(Me)]);
184  mul2:=Lcm([Denominator(x) : x in Eltseq(Ne)]);
185  Me:=ChangeRing(mul1*mul2*Me,Integers());
186  Ne:=ChangeRing(mul1*mul2*Ne,Integers());
187  LM:=LatticeWithGram(Me);
188  LN:=LatticeWithGram(Ne);
189
190  Me2:=spurform(tau*M);
191  Ne2:=spurform(tau*N);
192
```

```
193  mul1:=Lcm([Denominator(x) : x in Eltseq(Me2)]);
194  mul2:=Lcm([Denominator(x) : x in Eltseq(Ne2)]);
195  Me2:=ChangeRing(mul1*Me2,Integers());
196  Ne2:=ChangeRing(mul2*Ne2,Integers());
197
198  if IsIsometric(LM,[Me2],LN,[Ne2]) then
199   return true;
200  else
201   return false;
202  end if;
203 end function;
204
205 function projzeileNorm(v);
206  p:=HermitianTranspose(v)*Matrix(v);
207  liste:=[];
208  for i in [1..n] do
209   Append(~liste,F!(p[i][i]));
210   for j in [i+1..n] do
211    Append(~liste, F!(( p[i][j]+Conjugate(p[i][j]) )/2));
212    Append(~liste, sqrtd*(F!
213           ((p[i][j]-Conjugate(p[i][j]))/(2*w))) );
214   end for;
215  end for;
216  return liste;
217 end function;
218
219 function ListToSmallMatrixNorm(list);
220  L:=list;
221  change:=false;
222  if n eq 2 then
223   if not (L[1] in Rationals() and L[2] in Rationals() and
224           L[4] in Rationals()) then
225    change:=true;
226   end if;
227  end if;
228  if n eq 3 then
229   if not (L[1] in Rationals() and L[2] in Rationals() and
230           L[4] in Rationals() and L[6] in Rationals() and
231           L[7] in Rationals() and L[9] in Rationals()) then
232    change:=true;
233   end if;
```

```
234  end if;
235  if change then
236   L:=sqrtd*L;
237  end if;
238  res:=MatrixRing(K,n)!0;
239  for i in [1..n^2] do
240   if L[i] in Rationals() then
241    res:=res+L[i]*BasHermNorm[i];
242   else
243    res:=res+(K!(L[i]/sqrtd))*BasHermNorm[i];
244   end if;
245  end for;
246  return res;
247 end function;
248
249 findperp1 := function(L)
250  Cond:=[projzeileNorm(l) : l in L];
251  Cond:=Transpose(Matrix(Cond));
252
253  if Dimension(Kernel(Cond)) ne 1 then return false; end if;
254
255  dirlist:=Kernel(Cond).1;
256
257  dir:=MatrixRing(K,n)!ListToSmallMatrixNorm(dirlist);
258
259  return MatrixRing(K,n)!dir;
260 end function;
261
262 findperp := function(L)
263  Cond:=[projzeileNorm(l) : l in L];
264  Cond:=Transpose(Matrix(Cond));
265
266  dirlist:=Kernel(Cond).1;
267
268  dir:=MatrixRing(K,n)!ListToSmallMatrixNorm(dirlist);
269
270  return MatrixRing(K,n)!dir;
271 end function;
272
273 RealToString := function(r)
274    if Sign(r) eq -1 then
```

```
275         str := "-";
276     else
277         str := "";
278     end if;
279     r:=Abs(r);
280     p := Integers()! Floor(r) ;
281     str := str cat IntegerToString(p) cat ".";
282     for i := 1 to 15 do
283         r:=10*(r-p);
284         p := Integers()! Floor(r) ;
285         str := str cat IntegerToString(p);
286     end for;
287 return str;
288 end function;
289
290 aut := function(A);
291  Ae:=spurform(A);
292  mul:=Lcm([Denominator(x) : x in Eltseq(Ae)]);
293  Ae:=ChangeRing(mul*Ae,Integers());
294
295  Ae2:=spurform(tau*A);
296  mul:=Lcm([Denominator(x) : x in Eltseq(Ae2)]);
297  Ae2:=ChangeRing(mul*Ae2,Integers());
298
299  L:=LatticeWithGram(Ae);
300
301  G:=AutomorphismGroup(L,[Ae2]);
302
303  return G;
304 end function;
305
306 //FirstPerfect
307
308 Pini:=MatrixRing(K,n)!1;
309 Pini[n][n]:=1/Norm(p2);
310 Pinie:=spurform(Pini);
311 Pinie2:=spurform(w*Pini);
312
313 Lini:=LatticeWithGram(Pinie);
314 Sini:=RemoveMultiples(kuerzen(Pini,1,
315         ShortVectors(Lini,1,mmax)));
```

```
316 Rini:=perfrank(Sini);
317
318 count:=1;
319
320 while Rini lt n^2 and count lt 100 do
321  count:=count+1;
322  dir:=findperp(Sini);
323
324  tsup:=1000;
325  tinf:=0;
326  t:=(tsup+tinf)/2;
327
328  bool:=false;
329  count2:=1;
330
331  while not bool and count2 lt 100 do
332
333   count2:=count2+1;
334   M:=1;
335   Pt:=Pini+t*dir;
336   while M eq 1 do
337    if IsPositiveDefinite(spurform(Pt)) then
338     Lt:=LatticeWithGram(spurform(Pt));
339     M:=hermitianmin(Pt);
340     if M eq 1 then
341      tinf:=t;
342      t:=(tinf+tsup)/2;
343      Pt:=Pini+t*dir;
344     end if;
345    else
346     tsup:=t;
347     t:=(tinf+tsup)/2;
348     Pt:=Pini+t*dir;
349    end if;
350   end while;
351
352   St:=RemoveMultiples(kuerzen(Pt,M,
353         ShortVectors(Lt,M/mmax,M*mmax)));
354
355   tt:=Rationals()!Min([(idealnorm(v)-K!
356     ((v*Pini*HermitianTranspose(v))[1,1]))/
```

```
357      (K!((v*dir*HermitianTranspose(v))[1,1])) : v in St]);
358    bool:=false;
359    if tt lt t and tt gt 0 then
360     Pc:=Pini+tt*dir;
361     Pce:=spurform(Pc);
362     Lc:=LatticeWithGram(Pce);
363     M:=hermitianmin(Pc);
364     if M eq 1 then
365      bool:=true;
366     else
367      tsup:=tt;
368      t:=(tinf+tsup)/2;
369      Pt:=Pini+t*dir;
370     end if;
371    else
372     tsup:=t;
373     t:=(tsup+tinf)/2;
374     Pt:=Pini+t*dir;
375    end if;
376   end while;
377
378   Pini:=Pc;
379   Pinie:=spurform(Pini);
380   Pinie2:=spurform(w*Pini);
381
382   Lini:=LatticeWithGram(Pinie);
383   Sini:=RemoveMultiples(kuerzen(Pini,1,
384         ShortVectors(Lini,1,mmax)));
385   Rini:=perfrank(Sini);
386 end while;
387
388 if Rini ne n^2 then
389  print "Fehler";
390 end if;
391
392 //Perfekte Nachbarn auflisten
393
394 perfectlist:=[Pini];
395
396 numberoffaces:=[];
397 Nachbarn:=[];
```

```
E:={**};
Todo:=[Pini];

while(#Todo gt 0) do

P:=Todo[1];
Pe:=spurform(P);
L:=LatticeWithGram(Pe);
m:=hermitianmin(P);
S:=ShortVectors(L,m/mmax,m*mmax);
Sk:=RemoveMultiples(kuerzen(P,m,S));
Sproj:=[projzeileNorm(v) : v in Sk];

Exclude(~Todo,Todo[1]);

if perfrank(Sk) ne n^2 then print "FEHLER"; end if;

G:=aut(P);
G:=ChangeRing(G,Rationals());

DonQhull:=Open("DonneePourQhull","w");
Puts(DonQhull, IntegerToString(n^2) cat " RBOX c");
Puts(DonQhull, IntegerToString(#Sproj+1) );
Puts(DonQhull, &cat ["0 " : i in [1..n^2] ] );
for st in [ &cat [RealToString(Injec(n)) cat " "
            : n in Eltseq(X)] : X in Sproj] do
 Puts(DonQhull,st);
end for;
delete DonQhull;

System("/home3/castor/tmp/kirschme/qhull/bin/
qhull -Fv <DonneePourQhull >SommetsParFace");

Faces:=[];
SomFac:=Open("SommetsParFace","r");
nbface := StringToInteger(Gets(SomFac));
for i in [1..nbface] do
 Faces:=Append(Faces, Remove([StringToInteger(n)
        : n in Split(Gets(SomFac)," ")],1));
end for;
delete SomFac;
```

```
439 Faces:=[ Exclude(F,0) : F in Faces | 0 in F];
440 Faces:=[ {n : n in F} : F in Faces];
441 Append(~numberoffaces,#Faces);
442
443 count:=0;
444
445 while(#Faces gt 0) do
446  count:=count+1;
447  if count mod 100 eq 0 then print count; end if;
448  F1:=findperp1([Sk[n] : n in Faces[1]]);
449  Exclude(~Faces,Faces[1]);
450
451  sgn:=Sign(&+ [Rationals()!auswerten(F1,x) : x in Sk]);
452  F1:=sgn*F1;
453
454  tsup:=10000;
455  tinf:=0;
456  t:=(tinf+tsup)/2;
457  minimcont:=0;
458  while minimcont ne 1 do
459   coherent:=false;
460   while not coherent do
461    Pt:=P+t*F1;
462    M:=1;
463    while M eq 1 do
464     if IsPositiveDefinite(spurform(Pt)) then
465      M:=hermitianmin(Pt);
466      if M eq 1 then
467       tinf:=t;
468       t:=(tinf+tsup)/2;
469       Pt:=P+t*F1;
470      end if;
471     else
472      tsup:=t;
473      t:=(tinf+tsup)/2;
474      Pt:=P+t*F1;
475     end if;
476    end while;
477    St:=RemoveMultiples(kuerzen(Pt,hermitianmin(Pt),
478        ShortVectors(LatticeWithGram(spurform(Pt)),
479        hermitianmin(Pt)/mmax , hermitianmin(Pt)*mmax)));
```

```
480     SFace:=[ s : s in Sk | auswerten(F1,s) eq 0];
481
482     Cond:=[projzeileNorm(s) : s in SFace] cat
483           [projzeileNorm(s) : s in St];
484     Uns:=Vector( #Cond , [ F!(idealnorm(v))
485                   : v in SFace ] cat
486                    [F!(idealnorm(v)) : v in St] );
487     Cond:=Transpose(Matrix(Cond));
488
489     coherent:=IsConsistent(Cond,Uns);
490     if not coherent then
491      tsup:=t;
492      t:=(tinf+tsup)/2;
493      Pt:=P+t*F1;
494     end if;
495   end while;
496   Pcont:=ListToSmallMatrixNorm(Solution(Cond,Uns));
497   Pconte:=spurform(Pcont);
498   Lcont:=LatticeWithGram(Pconte);
499   Scont:=ShortVectors(Lcont,hermitianmin(Pcont)/mmax,
500           hermitianmin(Pcont)*mmax);
501   Scontk:=RemoveMultiples(kuerzen(Pcont,
502           hermitianmin(Pcont),Scont));
503
504   minimcont:=hermitianmin(Pcont);
505
506   tsup:=t;
507   t:=(tinf+tsup)/2;
508   Pt:=P+t*F1;
509 end while;
510
511 iso:=false;
512 for i in [1..#perfectlist] do
513   if isisom(Pcont,perfectlist[i]) then
514     iso:=true;
515     Include(~E,<Position(perfectlist,P),i>);
516   end if;
517 end for;
518 if not iso then
519   Append(~perfectlist,Pcont);
520   Append(~Todo,Pcont);
```

```
521   Include(~E,<Position(perfectlist,P),
522         Position(perfectlist,Pcont)>);
523  end if;
524 end while;
525 end while;
526
527 print "Formen:";
528 print perfectlist;
529 print "Determinanten:";
530 print [Norm(p2)*Determinant(P) : P in perfectlist];
531 print "#kuerzeste Vektoren:";
532 print [#RemoveMultiples(kuerzen(p,1,ShortVectors(LatticeWithGram
533       (spurform(p)),1,mmax))) : p in perfectlist];
534 print "#Seiten";
535 print numberoffaces;
536 print "Automorphismengruppen:";
537 autlist:=[#aut(p) : p in perfectlist];
538 print autlist;
539 //Listen schreiben fuer Gruppenidentifikation
540 if Maximum(autlist) lt 2000 then
541  L1:=Open("Liste1","w");
542  Puts(L1, "Liste1:=[");
543  for i in [1..#perfectlist] do
544   if i ne #perfectlist then
545    Puts(L1, IntegerToString(IdentifyGroup
546         (aut(perfectlist[i]))[1]) cat " , ");
547   else
548    Puts(L1, IntegerToString(IdentifyGroup
549         (aut(perfectlist[i]))[1]));
550   end if;
551  end for;
552  Puts(L1, " ];");
553  delete L1;
554
555  L2:=Open("Liste2","w");
556  Puts(L2, "Liste2:=[");
557  for i in [1..#perfectlist] do
558   if i ne #perfectlist then
559    Puts(L2, IntegerToString(IdentifyGroup
560         (aut(perfectlist[i]))[2]) cat " , ");
561   else
```

```
562     Puts(L2, IntegerToString(IdentifyGroup
563           (aut(perfectlist[i]))[2]));
564    end if;
565   end for;
566   Puts(L2, " ];");
567   delete L2;
568
569   print "Listen geschrieben.";
570 end if;
```

D. Eigenständigkeitserklärung

Hiermit versichere ich, die Arbeit selbstständig verfasst zu haben und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt zu haben.

Aachen, im März 2012 _____

Literaturverzeichnis

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust: *The Magma algebra system. I. The user language.* J. Symbolic Comput., 24(3-4):235-265, 1997

[BDH96] Barber, C.B., Dobkin, D.P., and Huhdanpaa, H.T., „The Quickhull algorithm for convex hulls," ACM Trans. on Mathematical Software, 22(4):469-483, Dec 1996, http://www.qhull.org.

[Cou01] Renaud Coulangeon: *Voronoï theory over algebraic number fields*, in *Réseaux euclidiens, designs sphériques et formes modulaires*, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001

[Cou04] Renaud Coulangeon: *Invariants d'Hermite, théorie de Voronoï et designs sphériques*, Habilitationsschrift, Universität Bordeaux, 2004

[HKN11] Michael Hentschel, Aloys Krieg, Gabriele Nebe: *On the classification of even unimodular lattices with a complex structure*, 2011, Int. J. Number Theory, noch nicht veröffentlicht

[Mar03] Jacques Martinet: *Perfect Lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften, Vol. 327, Springer-Verlag, 2003

[Mey08] Bertrand Meyer: *Constantes d'Hermite et théorie de Voronoï*, Dissertation, Universität Bordeaux, 2008

[Neu07] Jürgen Neukirch: *Algebraische Zahlentheorie*, Springer-Verlag, 2007

[O'M00] O. Timothy O'Meara: *Introduction to Quadratic Forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition

[PS97] Wilhelm Plesken, Bernd Souvignier: *Computing Isometries of Lattices*, Journal of Symbolic Computation 24 (1997), S. 327-334