Extremale Gitter mit großen Automorphismen

Masterarbeit

von Simon Berger

Vorgelegt am Lehrstuhl D für Mathematik der RWTH-Aachen University

bei Prof. Dr. Gabriele Nebe (1. Prüferin)
und Prof. Dr. Markus Kirschmer (2. Prüfer)

26. August 2018

Inhaltsverzeichnis

1 Einleitung

2 Grundbegriffe

§ 2.1 Quadratische Vektorräume

Wir wiederholen zunächst einige wichtige Begriffe aus der Gittertheorie, welche wir in der Arbeit häufig benötigen werden. Zunächst führen wir das Konzept eines quadratischen Vektorraumes ein. Die nun angeführten Definitionen sind [Kne02, Def. (2.1)] entnommen.

(2.1.1) Definition

(i) Sei A ein Ring und E ein A-Modul. Für eine symmetrische Bilinearform $b : E \times E \to A$ heißt das Paar (E, b) ein *bilinearer A-Modul* (bzw. falls A Körper ein *bilinearer A-Vektorraum*).

(ii) Eine Abbildung $q : E \to A$ mit den Eigenschaften

$$q(ax) = a^2 q(x) \quad \text{für } a \in A, x \in E$$
$$q(x + y) = q(x) + q(y) + b_q(x, y)$$

mit einer symmetrischen Bilinearform b_q heißt *quadratische Form*. Ein solches Paar (E, q) heißt *quadratischer A-Modul* (bzw. falls A Körper ein *quadratischer A-Vektorraum*).

(iii) Eine *isometrische Abbildung* (oder kurz *Isometrie*) zwischen zwei bilinearen Moduln (E, b) und (E', b') ist ein Modulisomorphismus $f : E \to E'$ mit $b(x, y) = b'(f(x), f(y))$.

(iv) Analog ist eine Isometrie zwischen zwei quadratischen Moduln (E, q) und (E', q') ist ein Modulisomorphismus $f : E \to E'$ mit $q(x) = q'(f(x))$ für alle $x \in E$.

(2.1.2) Bemerkung

Auf einem quadratischen A-Modul (E, q) ist $b_q : E \times E \to A, (x, y) \mapsto q(x+y) - q(x) - q(y)$ eine symmetrische Bilinearform. Andersherum erhält man aus jeder symmetrischen Bilinearform b auf E eine quadratische Form $q_b : E \to A, x \mapsto b(x, x)$. Es ist dabei $b_{q_b} = 2b$ und $q_{b_q} = 2q$. Ist $2 \in A^*$, so kann man daher stattdessen $q_b : E \to A, x \mapsto \frac{1}{2}b(x, x)$ wählen, womit die Konzepte der quadratischen Formen und der symmetrischen Bilinearformen auf E vertauschbar sind.

Nun folgen Definitionen zum Gitterbegriff, zu finden in [Kne02, Def. (14.1), (14.2)].

(2.1.3) Definition

(i) Sei K ein Körper, V ein endlich-dimensionaler K-Vektorraum mit Basis $(b_1, \ldots, b_n)$. Ein R-Gitter in V ist ein R-Untermodul L von V, zu dem Elemente $a, b \in K^*$ existieren mit $a \sum_{i=1}^n Rb_i \subseteq L \subseteq b \sum_{i=1}^n Rb_i$.

(ii) Sei b eine nicht-ausgeartete symmetrische Bilinearform auf V und L ein Gitter in V. Dann ist auch $L^\# := \{x \in V \mid b(x, y) \in R \text{ für alle } y \in L\}$ ein R-Gitter und heißt *das zu L duale Gitter* (bzgl. b).

(iii) Für $m \in \mathbb{N}$ heißt das Gitter $L^{\#,m} := \frac{1}{m}L \cap L^\#$ *partielles Dualgitter* von L.

(iv) Sei (V, b) ein bilinearer K-Vektorraum und L ein Gitter in V. Die Gruppe $\mathrm{Aut}(L) := \{\sigma : V \to V \mid \sigma \text{ ist Isometrie und } \sigma(L) = L\}$ heißt die *Automorphismengruppe* von L.

(2.1.4) Bemerkung

Falls R ein Hauptidealbereich ist, vereinfacht sich die Definition erheblich, da Teilmoduln von endlich erzeugten freien Moduln über Hauptidealbereichen wieder frei sind. Ein R-Gitter ist per Definition zwischen zwei freien Moduln eingespannt, also sind die R-Gitter in diesem Fall genau die freien R-Moduln von Rang n.

Insbesondere interessieren uns $\mathbb{Z}$-Gitter in $\mathbb{R}^n$. Für eben solche folgen nun ein paar weitere Definitionen, abgeleitet aus [Kne02, Def. (1.7), (1.13), (14.7), (26.1)].

(2.1.5) Definition

Sei L ein $\mathbb{Z}$-Gitter mit Basis $B = (e_1, \ldots, e_n)$ in $(\mathbb{R}^n, b)$, für eine symmetrische Bilinearform b.

(i) Die Matrix $G := \mathrm{Gram}(B) = (b(e_i, e_j))_{i,j=1}^n$ heißt *Gram-Matrix* von L, $\mathrm{Det}(L) := \mathrm{Det}(G)$ heißt die *Determinante* von L.

(ii) Das Gitter L heißt *ganz*, falls $b(L, L) \subseteq \mathbb{Z}$ gilt.

(iii) Das Gitter L heißt *gerade*, falls $b(x, x) \in 2\mathbb{Z}$ für alle $x \in L$ gilt.

(iv) Die *Stufe* von L ist die kleinste Zahl $\ell \in \mathbb{N}$, sodass $\sqrt{\ell}L^{\#}$ ein gerades Gitter ist.

(v) Das *Minimum* von L ist definiert als $\mathrm{Min}(L) := \min\{b(x, x) \mid 0 \neq x \in L\}$.

(2.1.6) Bemerkung

(i) Nach [Kne02, Satz (14.7)] gilt $\mathrm{Det}(L) = |L^{\#}/L|$. Insbesondere ist die Determinante für $\mathbb{Z}$-Gitter unabhängig von der Wahl der Basis. Allgemeiner ist die Determinante von R-Gittern modulo $(R^*)^2$ eindeutig bestimmt [Kne02, (1.13)].

(ii) Direkt aus der Definition des dualen Gitters folgt: L ist ganz genau dann, wenn $L \subseteq L^{\#}$.

(iii) Ein gerades Gitter L ist notwendigerweise ganz, denn seien $x, y \in L$, dann ist

$$b(x,y) = \frac{b(x+y,x+y) - b(x,x) - b(y,y)}{2} \in \mathbb{Z}.$$

(iv) Ist $B = (e_1, \ldots, e_n)$ eine Basis von L, dann ist $B^* := (e_1^*, \ldots, e_n^*)$, wobei $b(e_i, e_j^*) = \delta_{ij}$, eine Basis von $L^{\#}$. Es gilt $\mathrm{Gram}(B^*) = \mathrm{Gram}(B)^{-1}$ [Kne02, (1.14)].

Da wir uns im Zuge dieser Arbeit in der Regel mit geraden Gittern quadratfreier Stufe beschäftigen, ist das folgende Lemma aus [Jü15, Lemma 1.1.1] von großer Bedeutung.

(2.1.7) Lemma

Sei L ein gerades Gitter der Stufe ℓ, wobei ℓ quadratfrei. Dann ist ℓ gleichzeitig die kleinste natürliche Zahl a, sodass $aL^{\#} \subseteq L$ (also der Exponent der Diskriminantengruppe $L^{\#}/L$).

§ 2.2 Modulare Gitter

Wir kommen nun zum ursprünglich von Quebbemann eingeführten Konzept *modularer Gitter* [Que95]. Die hier verwendete Definition ist in [BFS05] zu finden.

(2.2.1) Definition

Sei L ein gerades Gitter und $\ell \in \mathbb{N}$.

(i) L heißt *ℓ-modular*, falls $L \cong \sqrt{\ell} L^{\#}$.

(ii) L heißt *stark ℓ-modular*, falls $L \cong \sqrt{m} L^{\#,m}$ für alle $m|l$, sodass $\mathrm{ggT}(m, \frac{\ell}{m}) = 1$.

(2.2.2) Lemma

Ist L ein gerades Gitter der Dimension n.

(i) Ist L ℓ-modular, dann ist $\mathrm{Det}(L) = \ell^{\frac{n}{2}}$. Insbesondere muss daher n gerade sein.

(ii) Ist L ℓ-modular und ℓ quadratfrei, dann hat L die Stufe ℓ.

(iii) Ist L stark ℓ-modular, von Stufe ℓ und ℓ quadratfrei, dann ist L auch ℓ-modular.

Beweis:

(i) Nach Bem. (2.1.6) ist $\mathrm{Det}(L^{\#}) = \mathrm{Det}(L)^{-1}$. Somit

$$\mathrm{Det}(L) = \mathrm{Det}(\sqrt{\ell} L^{\#}) = \ell^n \mathrm{Det}(L^{\#}) = \frac{\ell^n}{\mathrm{Det}(L)}.$$

Also folgt die Behauptung.

(ii) Sei a die Stufe von L, dann ist $\sqrt{a} L^{\#}$ gerade und hat insbesondere eine ganzzahlige Determinante. Nach (i) erhalten wir $\mathrm{Det}(\sqrt{a} L^{\#}) = \left(\frac{a^2}{\ell}\right)^{\frac{n}{2}} \overset{!}{\in} \mathbb{Z}$. Da ℓ quadratfrei sieht man also $\ell|a$. Andersherum ist $L \cong \sqrt{\ell} L^{\#}$, also selbstverständlich auch $\sqrt{\ell} L^{\#}$ gerade, somit $a|\ell$.

ℓ	1	2	3	5	6	7	11	14	15	23
k_1	24	16	12	8	8	6	4	4	4	2

Tabelle 2.1: k_1 Werte nach ℓ.

(iii) L hat quadratfreie Stufe ℓ, also ist $\ell L^{\#} \subseteq L$ nach Lemma (2.1.7). Wir erhalten

$$L \cong \sqrt{l}L^{\#,\ell} = \sqrt{\ell}\left(\frac{1}{\ell}L \cap L^{\#}\right) = \sqrt{\ell}L^{\#}. \qquad \square$$

Quebbemann zeigte in [Que95], dass die Theta-Reihen eines modularen Gitters Modulform einer bestimmten Gruppe ist. Außerdem hat die Algebra der Modulformen eine besonders einfache Gestalt, wenn die Summe der Teiler von ℓ selbst ein Teiler von 24 ist. Konkret ist diese Eigenschaft für $\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$ erfüllt. In der Literatur sind diese Stufen also besonders interessant. Es lässt sich zeigen (vgl. z.B. [Jü15, 1.2.2]), dass der Raum der Modulformen der erwähnten Gruppe in diesem Fällen ein eindeutiges Element θ der Form $1 + O(q^d)$ mit möglichst großem d und ganzzahligen Koeffizienten hat. Wir wollen den Begriff eines *extremalen Gitters* definieren als ein Gitter, welches ein möglichst großes Minimum besitzt, also ein Gitter mit Thetareihe θ. In unseren Spezialfällen gilt $d = 1 + \lfloor \frac{n}{k_1} \rfloor$, wobei k_1 Tabelle (2.1) zu entnehmen ist.

Wir können also definieren:

(2.2.3) Definition

Sei L ein ℓ-modulares Gitter der Dimension n und $\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$. Erfüllt L die Schranke

$$\mathrm{Min}(L) \geq 2\left(1 + \lfloor \frac{n}{k_1} \rfloor\right)$$

wobei k_1 gewählt ist wie in Tabelle (2.1), so nennen wir L ein *extremales Gitter*.

Die Dimensionen, welche jeweils echt von k_1 geteilt werden bezeichnet man häufig auch als *Sprungdimensionen*, da in diesen Fällen das Minimum im Vergleich zur nächst kleineren Dimension um 2 nach oben "springt".
Da die Determinante für ℓ-modulare Gitter in fester Dimension nach Lemma (2.2.2) eindeutig bestimmt ist, liefern modulare Gitter mit möglichst großem Minimum die dichtesten Kugelpackungen. In diesem Sinne ist die Klassifikation extremaler Gitter besonders interessant.

(2.2.4) Definition

Die Funktion

$$\gamma : \{L \mid L \text{ ist } n\text{-dimensionales } \mathbb{Z}\text{-Gitter}\} \to \mathbb{R}, L \mapsto \frac{\mathrm{Min}(L)}{\mathrm{Det}(L)^{\frac{1}{n}}} \tag{2.1}$$

heißt *Hermite-Funktion*. Der Wert

$$\gamma_n := \max\{\gamma(L) \mid L \text{ ist } n\text{-dimensionales } \mathbb{Z}\text{-Gitter}\}$$

heißt *Hermite-Konstante* zur Dimension n.

Ein höherer Wert bezüglich der Funktion γ bedeutet dabei ein dichteres Gitter im Hinblick auf die dazugehörige Kugelpackung. In der Literatur wird häufig alternativ mit der sogenannten *Zentrumsdichte* $\delta(L) = \frac{\mathrm{Min}(L)^{\frac{n}{2}}}{2^n\sqrt{\mathrm{Det}(L)}}$ gearbeitet (vgl. [CS93, (1.5)]). Cohn und Elkies haben in [CE03] obere Schranken für die Zentrumsdichte ermittelt. Mithilfe der Identität $\gamma(L) = 4\delta(L)^{\frac{2}{n}}$ lassen sich daraus obere Schranken für die Hermite-Konstante herleiten. Zusätzlich sind für die Dimensionen 1 bis 8 und 24 die Werte von γ_n explizit bekannt. Hierfür können wir also die Hermite-Funktionen der dichtesten bekannten Gitter als Schranken festhalten (vgl. [NS]). Die sich ergebenden oberen Schranken in Dimensionen 1 bis 36 sind in Tabelle (2.2) festgehalten.

n	$\gamma_n \leq$	n	$\gamma_n \leq$	n	$\gamma_n \leq$	n	$\gamma_n \leq$
1	1	10	$2,2636$	19	3.3975	28	4.4887
2	1.1547	11	2.3934	20	3.5201	29	4.6087
3	1.2599	12	2.3934	21	3.6423	30	4.7286
4	1.4142	13	2.6494	22	3.7641	31	4.8484
5	1.5157	14	2.7759	23	3.8855	32	4.9681
6	1.6654	15	2.9015	24	4.0000	33	5.0877
7	1.8115	16	3.0264	25	4.1275	34	5.2072
8	2.0000	17	3.1507	26	4.2481	35	5.3267
9	2.1327	18	3.2744	27	4.3685	36	5.4462

Tabelle 2.2: Obere Schranken für γ_n bei $1 \leq n \leq 36$.

Diese Schranken sind sehr nützlich, da sie in vielen Fällen die Existenz von bestimmten Gittern von vorneherein ausschließt. Beispielsweise hätte ein hypothetisches extremales 23-modulares Gitter L in Dimension 6 bereits Minimum ≥ 8 und Determinante 23^3, also $\gamma(L) \geq \frac{8}{\sqrt{23}} \approx 1.6681 > 1.6654$ und kann somit nicht existieren. Genauer schließen die Schranken die folgenden extremalen Gitter aus:

(2.2.5) Lemma

Erfüllen $\ell \in \mathbb{N}$ und $n \in \underline{36}$ eine der Bedingungen

- $\ell = 1$ und $n \in \{2, 4, 6\}$.
- $\ell = 2$ und $n = 2$.
- $\ell = 11$ und $n \in \{20, 24, 28, 30, 32, 34, 36\}$.
- $\ell = 23$ und $n \in \{6, 8, 10, \ldots, 34, 36\}$,

so existiert kein extremales ℓ-modulares Gitter in Dimension n.

Beweis:

Tabelle (2.2). □

Vergleicht man die hypothetischen Zentrumsdichten extremaler Gitter (deren Existenz bisher nach [Jü15] noch offen ist) mit denen der dichtesten bisher bekannten Gitter (zu finden in [NS]), so fällt auf, dass die Entdeckung extremaler Gitter in den folgenden Stufen ℓ und Dimensionen $1 \leq n \leq 48$ jeweils neue dichteste Kugelpackungen liefern würden:

- $\ell = 3$ und $n \in \{36, 38\}$.
- $\ell = 5$ und $n \in \{32, 36, 40, 44, 48\}$.
- $\ell = 6$ und $n = 40$.
- $\ell = 7$ und $n \in \{32, 34, 38, 40, 36\}$.
- $\ell = 11$ und $n \in \{18, 22\}$.
- $\ell = 14$ und $n = 28$.
- $\ell = 15$ und $n = 28$.

Wie man sieht, ist die Erforschung extremaler modularer Gitter also von großem Interesse für die Gittertheorie. Im nächsten Kapitel beschreiben wir nun eine Vorgehensweise, modulare Gitter zu klassifizieren, welche zusätzlich eine Struktur als gebrochenes Ideal eines Zahlkörpers aufweisen, sogenannte *Ideal-Gitter*.

3 Ideal-Gitter

§ 3.1 Definitionen

Wir geben nun die Definition eines Ideal-Gitter abgeleitet aus [BFS05] an.

(3.1.1) Definition

(i) Ein *(algebraischer) Zahlkörper* ist eine endliche Erweiterung des Körpers $\mathbb{Q}$.

(ii) Der *Ring der ganzen Zahlen* eines Zahlkörpers K ist der Ring

$$\mathbb{Z}_K := \{a \in K \mid \mu_{a,\mathbb{Q}}(X) \in \mathbb{Z}[X]\}.$$

(iii) Die *Norm* eines Ideals $\mathcal{I}$ von $\mathbb{Z}_K$ ist definiert als

$$\mathcal{N}(\mathcal{I}) := |\mathbb{Z}_K/\mathcal{I}|.$$

(iv) Ein Zahlkörper K heißt *CM-Körper*, falls K total-imaginär ist und ein total-reeller Teilkörper $K^+ \leq K$ existiert mit $[K : K^+] = 2$.

(v) Sei K ein CM-Körper und $\mathbb{Z}_K$ der Ring der ganzen Zahlen in K. Ein *Ideal-Gitter* ist ein Gitter $(\mathcal{I}, b)$, sodass $\mathcal{I}$ ein gebrochenes $\mathbb{Z}_K$-Ideal ist und $b : \mathcal{I} \times \mathcal{I} \to \mathbb{R}$ eine symmetrische positiv-definite Bilinearform mit $b(\lambda x, y) = b(x, \overline{\lambda} y)$ für $x, y \in \mathcal{I}$ und $\lambda \in \mathbb{Z}_K$. Die Abbildung $\bar{}$ bezeichnet dabei die herkömmliche komplexe Konjugation.

(vi) Ein Element $\alpha \in K^+$ heißt *total-positiv*, wenn $\iota(\alpha) > 0$ für alle Einbettungen $\iota : K^+ \hookrightarrow \mathbb{R}$. Wir schreiben dann auch $\alpha \gg 0$. Die Menge aller total-positiven Elemente in K^+ wird mit $K^+_{\gg 0}$ bezeichnet.

Bis auf weiteres sei im Folgenden stets K ein CM-Körper, $\mathbb{Z}_K$ der Ring der ganzen Zahlen in K und K^+ der maximale total-reelle Teilkörper von K.

(3.1.2) Bemerkung

Die Eigenschaften der Bilinearform in der obrigen Definition sind nach [BFS05] äquivalent dazu, dass ein total-positives Element $\alpha \in K^+$ existiert mit $b(x, y) = \mathrm{Spur}_{K/\mathbb{Q}}(\alpha x \overline{y})$. Wir können Ideal-Gitter daher auch durch die Notation $(\mathcal{I}, \alpha)$ beschreiben.

Ein Ideal-Gitter $\mathcal{I}$ kann immer auch als $\mathbb{Z}$-Gitter betrachtet werden, indem man $\mathbb{Z}_K$-Erzeuger von $\mathcal{I}$ und eine $\mathbb{Z}$-Basis von $\mathbb{Z}_K$ zu $\mathbb{Z}$-Erzeugern von $\mathcal{I}$ kombiniert. Im Folgenden bezeichnen wir daher $\mathcal{I}$ als gerade, ganz, modular, etc., falls $\mathcal{I}$ als $\mathbb{Z}$-Gitter diese Eigenschaften erfüllt und $\mathcal{I}^\#$ als das Dualgitter von $\mathcal{I}$ als $\mathbb{Z}$-Gitter.

Wir beschäftigen uns in dieser Arbeit mit Ideal-Gittern über zyklotomischen Zahlkörpern, also Körpern der Form $\mathbb{Q}(\zeta_m)$ für primitive m-te Einheitswurzeln ζ_m. Solche Körper sind CM-Körper mit maximalem total-reellem Teilkörper $K^+ = \mathbb{Q}(\zeta_m + \overline{\zeta_m})$. Wir erhalten Körper dieser Form, indem wir Automorphismen von $\mathbb{Z}$-Gittern betrachten, die wie primitive Einheitswurzeln operieren. Diese Aussagen wollen wir nun ein wenig präzisieren. Dazu eine kurze Definition:

(3.1.3) Definition

Sei K ein Körper und $m \in \mathbb{N}$.

1. Ein Element $\zeta \in K$ heißt primitive m-te Einheitswurzel, falls $|\langle\zeta\rangle| = m$ ist.

2. Gilt $\mathrm{char}(K) \nmid m$ und sind $\zeta_1, \ldots, \zeta_n$ die primitiven m-ten Einheitswurzeln in einem Zerfällungskörper von $X^m - 1$, dann heißt das Polynom

$$\Phi_m(X) := \prod_{i=1}^{n} (X - \zeta_i)$$

das *m-te Kreisteilungspolynom*.

Einige wichtige bekannte Fakten zu Kreisteilungspolynomen (z.B. zu finden in [Mol11, Kap. 1]), sind die folgenden:

(3.1.4) Satz

(i) Gilt $\mathrm{char}(K) \nmid m$, so enthält der Zerfällungskörper von $X^m - 1$ genau $\varphi(m)$ primitive m-te Einheitswurzeln. Dabei ist $\varphi(m) = |\,(\mathbb{Z}/m\mathbb{Z})^*\,|$ die *Eulersche φ-Funktion*.

(ii) Ist $\mathrm{char}(K) = 0$, dann ist $\Phi_m \in \mathbb{Z}[X]$ und $X^m - 1 = \prod_{d|m} \Phi_d$.

(iii) Speziell für $K = \mathbb{Q}$ gilt $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ und $\Phi(m) \in \mathbb{Q}[X]$ ist irreduzibel.

(iv) Gilt $\mathrm{char}(K) \nmid m$, so ist $K(\zeta_m)/K$ ist eine Galoiserweiterung.

Wir sehen also, dass ζ_m genau dann eine primitive m-te Einheitswurzel ist, wenn sie

das Minimalpolynom Φ_m hat. Wir können $\mathbb{Z}$-Gitter somit auf die folgende Weise als Ideal-Gitter auffassen (vgl. [Neb13, Abschnitt (5.2)]):

(3.1.5) Lemma
Sei L ein $\mathbb{Z}$-Gitter in einem n-dimensionalen bilinearen Vektorraum (V, b) und $\sigma \in \mathrm{Aut}(L)$ mit $\mu_\sigma = \Phi_m$ für ein $m \in \mathbb{N}$ mit $\varphi(m) = n$. Dann ist L isomorph zu einem Ideal-Gitter in $\mathbb{Q}(\zeta_m)$.

Beweis:
Durch die Operation von σ wird $\mathbb{Q}L$ mittels $\zeta_m \cdot x := \sigma(x)$ für $x \in \mathbb{Q}L$ zu einem eindimensionalen $\mathbb{Q}(\zeta_m)$-Vektorraum und L zu einem ein $\mathbb{Z}[\zeta_m]$-Modul. Wegen $\mathbb{Z}[\zeta_m] = \mathbb{Z}_{\mathbb{Q}[\zeta_m]}$ ist L also ein gebrochenes Ideal in $\mathbb{Q}(\zeta_m)$.
Da σ ein Automorphismus ist, ist die Bilinearform $b : L \times L \to \mathbb{Q}$ des Vektorraums ζ_m-invariant. Sei nun $\lambda \in \mathbb{Z}[\zeta_m]$ beliebig. Wir können $\lambda = \sum_{i=0}^{m-1} a_i \zeta_m^i$ für Koeffizienten $a_i \in \mathbb{Z}$ schreiben und sehen

$$b(\lambda x, y) = \sum_{i=0}^{m-1} a_i b(\zeta_m^i x, y) = \sum_{i=0}^{m-1} a_i b(x, \zeta_m^{-i} y) = \sum_{i=0}^{m-1} a_i b(x, \overline{\zeta_m^i} y) = b(x, \overline{\lambda} y),$$

womit die Eigenschaften eines Ideal-Gitters erfüllt sind. □

Mittels der Klassifikation der Ideal-Gitter über $\mathbb{Q}(\zeta_m)$ erhalten wir also zugleich alle $\mathbb{Z}$-Gitter mit Minimalpolynom Φ_m. Wie diese Klassifikation durchgeführt werden kann, erläutern wir in den nächsten Abschnitten.

§ 3.2 Strategie zur Klassifikation

Die in den nächsten Abschnitten beschriebenen Aussagen und Vorgehensweisen zur Klassifikation von Ideal-Gittern sind an [Jü15, Abschnitt (3.2)] und [Neb13, Abschnitt (5.2)] angelehnt.

(3.2.1) Definition

Das $\mathbb{Z}_K$-ideal

$$\Delta := \{x \in K \mid \mathrm{Spur}_{K/\mathbb{Q}}(x\overline{y}) \in \mathbb{Z} \text{ für alle } y \in \mathbb{Z}_K\}$$

bezeichnet die *inverse Differente* von $\mathbb{Z}_K$.

Wir können nun das Dual eines Idealgitters mithilfe der inversen Differente ausdrücken.

(3.2.2) Lemma

Sei $(\mathcal{I}, \alpha)$ ein Ideal-Gitter. Dann ist $\mathcal{I}^{\#} = \overline{\mathcal{I}}^{-1}\Delta\alpha^{-1}$ das Dualgitter von $\mathcal{I}$ als $\mathbb{Z}$-Gitter.

Beweis:

$$\begin{aligned}
\mathcal{I}^{\#} &= \{x \in K \mid b(x, \mathcal{I}) \subseteq \mathbb{Z}\} \\
&= \{x \in K \mid \mathrm{Spur}_{K/\mathbb{Q}}(\alpha x\overline{\mathcal{I}}) \subseteq \mathbb{Z}\} \\
&= \alpha^{-1}\{x \in K \mid \mathrm{Spur}_{K/\mathbb{Q}}(x\overline{\mathcal{I}}) \subseteq \mathbb{Z}\} \\
&= \alpha^{-1}\overline{\mathcal{I}}^{-1}\{x \in K \mid \mathrm{Spur}_{K/\mathbb{Q}}(x\overline{\mathbb{Z}_K}) \subseteq \mathbb{Z}\} \\
&= \overline{\mathcal{I}}^{-1}\Delta\alpha^{-1}.
\end{aligned}$$

□

Mit Blick auf modulare Gitter kann man damit die nächste Folgerung ziehen:

(3.2.3) Korollar

Sei ℓ quadratfrei und $(\mathcal{I}, \alpha)$ ein gerades Ideal-Gitter der Stufe ℓ. Die Menge $\mathcal{B} := \alpha\mathcal{I}\overline{\mathcal{I}}\Delta^{-1}$ ist ein $\mathbb{Z}_K$-Ideal mit $\ell\mathbb{Z}_K \subseteq \mathcal{B}$ und Norm $\mathcal{N}(\mathcal{B}) = \det(\mathcal{I})$.

Beweis:

Da ℓ quadratfrei ist, gilt $\ell\mathcal{I}^{\#} \subseteq \mathcal{I}$ nach Lemma (2.1.7). Mit Lemma (3.2.2) bedeutet dies:

$$\begin{aligned} & \ell\mathcal{I}^{\#} \subseteq \mathcal{I} \subseteq \mathcal{I}^{\#} \\ \Leftrightarrow \quad & \ell\overline{\mathcal{I}}^{-1}\Delta\alpha^{-1} \subseteq \mathcal{I} \subseteq \overline{\mathcal{I}}^{-1}\Delta\alpha^{-1} \\ \Leftrightarrow \quad & \ell\mathbb{Z}_K \subseteq \alpha\mathcal{I}\overline{\mathcal{I}}\Delta^{-1} \subseteq \mathbb{Z}_K. \end{aligned}$$

Für die Norm gilt

$$\det(\mathcal{I}) = |\mathcal{I}^{\#}/\mathcal{I}| = |\mathbb{Z}_K / \left(\mathcal{I}\left(\mathcal{I}^{\#}\right)^{-1}\right)| = |\mathbb{Z}_K/\mathcal{B}| = \mathcal{N}(\mathcal{B}). \qquad \square$$

Da es jeweils nur endlich viele $\mathbb{Z}_K$-Ideale mit bestimmter Norm gibt, existieren bei der Konstruktion von Idealgittern mit fester Determinante nur endlich viele Möglichkeiten für $\mathcal{B}$. Mithilfe der Primidealzerlegung lässt sich ein rekursiver Algorithmus (Algorithmus (1)) konstruieren, welcher alle Teiler eines Ideals $\mathcal{J}$ mit bestimmter Norm n berechnen kann.

Konkret wird unsere Strategie im groben daraus bestehen, alle (relevanten) Möglichkeiten für $\mathcal{I}$ und $\mathcal{B}$ durchzugehen und zu testen, für welche davon das Ideal $\left(\mathcal{I}\overline{\mathcal{I}}\right)^{-1}\Delta\mathcal{B}$ ein Hauptideal mit total-positivem Erzeuger $\alpha \in K^{+}$ ist. Dazu machen wir zunächst einige Einschränkungen, um den Suchraum zu verkleinern.

Algorithmus 1 Berechnung aller Teiler mit fester Norm

1: **Eingabe**: $\mathbb{Z}_K$-Ideal $\mathcal{J}$, Norm n.

2: **Ausgabe**: Liste aller Teiler von $\mathcal{J}$ mit Norm n.

3:

4: **if** $n = 1$ **then return** $[\mathbb{Z}_K]$

5: **if** $n \nmid \mathcal{N}(\mathcal{J}))$ **then return** [ ]

6: **if** $\mathcal{N}(\mathcal{J}) = n$ **then return** $[\mathcal{J}]$

7: Zerlege $\mathcal{J}$ in Primideale $\mathcal{J} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_k^{s_k}$

8: $n_\mathfrak{p} \leftarrow \mathcal{N}(\mathfrak{p}_1)$

9: $A \leftarrow [\,]$

10: **for** $j \in \{0, \dots s_1\}$ **do**

11: **if** $n_\mathfrak{p}^j \mid n$ **then**

12: $B \leftarrow$ Teiler von $\mathfrak{p}_2^{s_2} \dots \mathfrak{p}_k^{s_k}$ mit Norm $\frac{n}{n_\mathfrak{p}^j}$ (rekursiv)

13: **for** $X \in B$ **do**

14: $A \leftarrow A \cup \left[\mathfrak{p}_1^j X\right]$

15: **return** A

§ 3.3 Die Klassengruppe

(3.3.1) Definition

Die *Klassengruppe*

$$\mathrm{Cl}_K := \{J \mid J \text{ ist gebrochenes } \mathbb{Z}_K\text{-Ideal}\}/\{(c)_{\mathbb{Z}_K} \mid c \in K^*\}.$$

(3.3.2) Lemma

Seien $\mathcal{I}$ ein gebrochenes $\mathbb{Z}_K$-Ideal und $\alpha \in K^+_{\gg 0}$. Für $\lambda \in K^*$ gilt $(\lambda\mathcal{I}, \alpha) \cong (\mathcal{I}, \lambda\overline{\lambda}\alpha)$.

Beweis:

Sei $b_\alpha : K \times K \to \mathbb{R}, (x, y) \mapsto \mathrm{Spur}_{K/\mathbb{Q}}(\alpha x \overline{y})$ die zu α gehörige Bilinearform. Dann ist

$$b_\alpha(\lambda x, \lambda y) = \mathrm{Spur}_{K/\mathbb{Q}}(\lambda\overline{\lambda}\alpha x\overline{y}) = b_{\lambda\overline{\lambda}\alpha}(x, y).$$

Folglich ist $\psi : (K, b_{\lambda\overline{\lambda}\alpha}) \to (K, b_\alpha), x \mapsto \lambda x$ eine Isometrie mit $\psi(\mathcal{I}) = (\lambda\mathcal{I})$. □

Mit dieser Aussage genügt es also, aus jeder Klasse der jeweils nur einen Vertreter zu betrachten. Wählt man $\lambda \in \mathbb{Z}_K^*$, so zeigt das Lemma, dass $(\mathcal{I}, \alpha) \cong (\mathcal{I}, \lambda\overline{\lambda}\alpha)$. Für α reichen also Vertreter modulo $\{\lambda\overline{\lambda} \mid \lambda \in \mathbb{Z}_K^*\}$.

Wir wollen nun die zu untersuchenden Möglichkeiten für $\mathcal{I}$ noch weiter einschränken: Ist $K/\mathbb{Q}$ galoissch (wie es für zyklotomische Zahlkörper der Fall ist), so genügt ein Repräsentant modulo der Operation der Galosgruppe.

(3.3.3) Lemma

Sei $K/\mathbb{Q}$ eine Galoiserweiterung, $\mathcal{I}$ ein gebrochenes $\mathbb{Z}_K$-Ideal und $\alpha \in K^+_{\gg 0}$. Für $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ ist $(\mathcal{I}, \alpha) \cong (\sigma(\mathcal{I}), \sigma(\alpha))$.

Beweis:

Da die Spur invariant unter der Galoisgruppe ist, erhält man die folgende Gleichungskette.

$$\begin{aligned} b_{\sigma(\alpha)}(\sigma(x), \sigma(y)) &= \mathrm{Spur}_{K/\mathbb{Q}}\left(\sigma(\alpha)\sigma(x)\overline{\sigma(y)}\right) \\ &= \mathrm{Spur}_{K/\mathbb{Q}}\left(\sigma\left(\alpha x \overline{y}\right)\right) = \mathrm{Spur}_{K/\mathbb{Q}}\left(\alpha x \overline{y}\right) = b_\alpha(x, y) \end{aligned}$$

Also induziert σ eine Isometrie $\sigma : (K, b_\alpha) \to (K, b_{\sigma(\alpha)})$. □

§ 3.4 Total-positive Erzeuger

Wir benötigen nun einen Test, welcher für ein gegebenes gebrochenes $\mathbb{Z}_K$-Ideal $\mathcal{I}$ überprüft, dieses von einem total-positiven Element $\alpha \in K^+_{\gg 0}$ erzeugt wird. Dazu untersuchen wir zuerst, ob $\mathcal{I}$ überhaupt von einem Element aus K^+ erzeugt ist und anschließend, wann ein Ideal $\alpha'\mathbb{Z}_K$ für $\alpha' \in K^+$ einen total-positiven Erzeuger hat.

(3.4.1) Satz

Sei $\mathcal{I}$ ein gebrochenes $\mathbb{Z}_K$-Ideal. Es existiert genau dann ein $\alpha' \in K^+$ mit $\mathcal{I} = \alpha'\mathbb{Z}_K$, wenn $\mathcal{I} \cap K^+ = \alpha'\mathbb{Z}_{K^+}$ und für jeden Primteiler $\mathfrak{p}$ von $\mathcal{I}$ gilt

- Ist $\mathfrak{p}$ verzweigt in K/K^+, so ist $\nu_\mathfrak{p}(\mathcal{I}) \in 2\mathbb{Z}$.
- Ist $\mathfrak{p}$ unverzweigt in K/K^+, so ist $\nu_\mathfrak{p}(\mathcal{I}) = \nu_{\overline{\mathfrak{p}}}(\mathcal{I})$.

Beweis:

Wir zeigen zunächst, dass die Bedingungen an die Primteiler äquivalent dazu sind, dass $\mathcal{I} = (\mathcal{I} \cap K^+)\mathbb{Z}_K$.

Sei dazu zuerst $\mathcal{I} = (\mathcal{I} \cap K^+)\mathbb{Z}_K$ erfüllt. Seien

$$\mathcal{I}' := \mathcal{I} \cap K^+ = \prod_{\mathfrak{a}} \mathfrak{a}^{\nu_{\mathfrak{a}}(\mathcal{I} \cap K^+)}, \quad \mathcal{I} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathcal{I})}$$

die Primidealzerlegungen. Dann folgt

$$\prod_{\mathfrak{a}} \mathfrak{a}^{\nu_{\mathfrak{a}}(\mathcal{I}')}\mathbb{Z}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathcal{I})}.$$

Aufgrund der Eindeutigkeit der Primidealzerlegung bedeutet dies

$$\mathfrak{a}^{\nu_{\mathfrak{a}}(\mathcal{I}')}\mathbb{Z}_K = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathcal{I})}$$

für jedes Primideal $\mathfrak{a}$ von $\mathbb{Z}_{K^+}$. Es ist $[K : K^+] = 2$, also kann $\mathfrak{a}\mathbb{Z}_K$ nur eine der Formen $\mathfrak{p}$, $\mathfrak{p}^2$, oder $\mathfrak{p}\overline{\mathfrak{p}}$ für ein Primideal $\mathfrak{p}$ in $\mathbb{Z}_K$ annehmen.

- Falls $\mathfrak{a}\mathbb{Z}_K = \mathfrak{p}^2$ (also falls $\mathfrak{p}$ verzweigt ist), so folgt $\nu_{\mathfrak{p}}(\mathcal{I}) = 2\nu_a(\mathcal{I}') \in 2\mathbb{Z}$.
- In den anderen beiden Fällen (also falls $\mathfrak{p}$ unverzweigt ist) gilt $\nu_{\mathfrak{p}}(\mathcal{I}) = \nu_{\mathfrak{a}}(\mathcal{I}') = \nu_{\mathfrak{p}}(\overline{\mathcal{I}})$.

Seien nun andersherum die Primideal-Bedingungen erfüllt. Definiert man

$$\mathcal{I}' := \prod_{\mathfrak{a}} \mathfrak{a}^{\nu_{\mathfrak{a}}(\mathcal{I}')}, \quad \nu_{\mathfrak{a}}(\mathcal{I}') = \begin{cases} \nu_{\mathfrak{p}}(\mathcal{I}) & \mathfrak{a}\mathbb{Z}_K \in \{\mathfrak{p}, \mathfrak{p}\overline{\mathfrak{p}}\} \\ \frac{1}{2}\nu_{\mathfrak{p}}(\mathcal{I}) & \mathfrak{a}\mathbb{Z}_K = \mathfrak{p}^2 \end{cases}$$

so gilt

$$\mathcal{I} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathcal{I})} = \prod_{\mathfrak{a}} (\mathfrak{a}\mathbb{Z}_K)^{\nu_{\mathfrak{a}}(\mathcal{I}')} = \mathcal{I}'\mathbb{Z}_K.$$

Also folgt $(\mathcal{I} \cap K^+)\mathbb{Z}_K = (\mathcal{I}'\mathbb{Z}_K \cap K^+)\mathbb{Z}_K = \mathcal{I}'\mathbb{Z}_K = \mathcal{I}$ und es gilt die behauptete Äquivalenz.

Die Behauptung des Satzes wurde somit darauf reduziert, dass genau dann $\mathcal{I} = \alpha'\mathbb{Z}_K$, wenn $\mathcal{I} \cap K^+ = \alpha'\mathbb{Z}_{K^+}$ und $\mathcal{I} = (\mathcal{I} \cap K^+)\mathbb{Z}_K$ für $\alpha' \in K^+$. Dies folgt allerdings leicht mithilfe von $(\alpha'\mathbb{Z}_K) \cap K^+ = \alpha'\mathbb{Z}_{K^+}$. □

Mithilfe dieses Satzes können wir nun Algorithmus (2) formulieren, welcher zu einem gegebenen Ideal $\mathcal{I}$ testet, ob dieses einen Erzeuger in K^+ hat und - falls ja - einen solchen zurückgibt. Ein Primideal $\mathfrak{a}$ wie im Beweis unseres Satzes erhalten wir, indem wir eine Primzahl p finden, sodass $\mathfrak{p} | (p\mathbb{Z}_K)$, dann muss $\mathfrak{a}$ eines der Primideale aus der Faktorisierung von $p\mathbb{Z}_{K^+}$ teilen.

(3.4.2) Lemma
Sei $\alpha' \in K^+$. Ein total-positives Element $\alpha \in K^+_{\gg 0}$ ist genau dann ein Erzeuger des Ideals $\alpha'\mathbb{Z}_K$, wenn eine Einheit $\epsilon \in \mathbb{Z}^*_{K^+}$ existiert mit $\alpha = \alpha'\epsilon$ und $\operatorname{sign}((\iota(\epsilon)) = \operatorname{sign}(\iota(\alpha'))$ für alle Einbettungen $\iota : K^+ \hookrightarrow \mathbb{R}$.

Beweis:
Ein weiterer Erzeuger hat immer die Gestalt $\alpha = \alpha'\epsilon$ für eine Einheit $\epsilon \in (\mathbb{Z}_{K^+})^*$. Damit α total-positiv wird muss für alle Einbettungen $\iota : K^+ \hookrightarrow \mathbb{R}$ gelten:

$$1 \overset{!}{=} \operatorname{sign}(\iota(\alpha)) = \operatorname{sign}\Big(\iota(\alpha')\iota(\epsilon)\Big) = \operatorname{sign}\Big(\iota(\alpha')\Big)\operatorname{sign}(\iota(\epsilon))$$

Also müssen die Vorzeichen jeweils identisch sein. □

Elemente aus $\left(\mathbb{Z}^*_{K^+}\right)^2$ haben immerzu positives Signum bezüglich allen Einbettungen. Außerdem liefern total-positive Elemente, die in der gleichen Klasse modulo Quadraten liegen nach Lemma (3.3.2) isomorphe Idealgitter. Es genügt also, sich bei der Suche nach einer Einheit wie im vorherigen Lemma auf Vertreter modulo Quadraten zu beschränken.

Algorithmus 2 Berechnung total-reelles Erzeugers

Eingabe: $\mathbb{Z}_K$-Ideal $\mathcal{I}$

Ausgabe: Element $\alpha' \in K^+$ mit $\alpha'\mathbb{Z}_K = \mathcal{I}$, oder *false*, falls ein solches Element nicht existiert.

$\mathcal{I}' \leftarrow 1\mathbb{Z}_{K^+}$

split $\leftarrow [\,]$

Zerlege $\mathcal{I} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_k^{s_k}$ in Primideale.

for $i \in \{1 \dots k\}$ **do**

    if $i \in$ split **then continue**

    $p \leftarrow$ minimale natürliche Zahl $p \in \mathbb{N}$ mit $\mathfrak{p}_i | (p\mathbb{Z}_K)$

    Zerlege $p\mathbb{Z}_{K^+}$ in Primideale: $p\mathbb{Z}_{K^+} = \mathfrak{q}_1^{t_1} \dots \mathfrak{q}_l^{t_l}$

    $\mathfrak{a} \leftarrow \mathfrak{q}_j$ mit $\mathfrak{p}_i | (\mathfrak{q}_j\mathbb{Z}_K)$

    if $\mathfrak{a}\mathbb{Z}_K = \mathfrak{p}_i^2$ **then**

        if $2 \nmid s_i$ **then return** *false*

        $\mathcal{I}' \leftarrow \mathcal{I}'\mathfrak{a}^{\frac{s_i}{2}}$

    else if $\mathfrak{a}\mathbb{Z}_K = \mathfrak{p}_i$ **then**

        $\mathcal{I}' \leftarrow \mathcal{I}'\mathfrak{a}^{s_i}$

    else if $\mathfrak{a}\mathbb{Z}_K = \mathfrak{p}_i\overline{\mathfrak{p}_i}$ **then**

        if $\nu_{\mathfrak{p}_i}(\mathcal{I}) \neq \nu_{\overline{\mathfrak{p}_i}}(\mathcal{I})$ **then return** *false*

        $\mathcal{I}' \leftarrow \mathcal{I}'\mathfrak{a}^{s_i}$

        $j \leftarrow j'$ mit $\mathfrak{p}_{j'} = \overline{\mathfrak{p}_i}$

        split $\leftarrow$ split $\cup\, [j]$

if $\mathcal{I}'$ kein Hauptideal **then**

    return *false*

else

    return Erzeuger von $\mathcal{I}'$

Nach dem Dirichletschen Einheitensatz [Neu92, Theorem (7.4)] hat die Einheitengruppe die Struktur

$$\mathbb{Z}_{K^+}^* = \{\pm 1\} \times \mathbb{Z}^{t-1}.$$

mit $t := [K^+ : \mathbb{Q}]$. Die Erzeuger $(\epsilon_1, \dots \epsilon_t)$ der Gruppe heißen *Grundeinheiten*. Jede Einheit ϵ lässt sich also darstellen in der Form $\epsilon = \epsilon_1^{\nu_1} \dots \epsilon_t^{\nu_t}$. Das folgende Korollar liefert uns nun die Lösung auf unsere Frage nach den total-positiven Erzeugern.

Dann lässt sich folgendes Korollar ziehen:

(3.4.3) Korollar

Sei $\alpha' \in K^+$, seien die Einbettungen von K^+ in $\mathbb{R}$ gegeben durch $\iota_1, \dots, \iota_t$ und seien $\epsilon_1, \dots, \epsilon_t$ die Grundeinheiten von $\mathbb{Z}_{K^+}^*$. Definiere die Matrix

$$M \in \mathbb{F}_2^{t \times t}, \quad M_{ij} = \begin{cases} 1 & , \text{sign}(\iota_i(\epsilon_j) = -1 \\ 0 & , \text{sign}(\iota_i(\epsilon_j) = 1 \end{cases}$$

und den Vektor

$$V \in \mathbb{F}_2^{1 \times t}, \quad V_i = \begin{cases} 1 & , \text{sign}(\iota_i(\alpha') = -1 \\ 0 & , \text{sign}(\iota_i(\alpha') = 1 \end{cases}.$$

Dann sind die total-positiven Erzeuger des Ideals $\alpha' \mathbb{Z}_K$ genau die Elemente der Menge $\{\alpha' \epsilon_1^{x_1} \dots \epsilon_t^{x_t} \epsilon^2 \mid x \in \mathbb{F}_2^{1 \times t}, xM = V, \epsilon \in (\mathbb{Z}_{K^+}^*)\}$.

Beweis:

Nach Lemma (3.4.2) und da Quadrate immerzu positives Signum haben, sind die total-positiven Erzeuger gegeben durch die Elemente $u = \alpha' \epsilon_1^{x_1} \dots \epsilon_t^{x_t} \epsilon^2$, wobei $x \in \mathbb{F}_2^{1 \times t}$, $\epsilon \in \mathbb{Z}_{K^+}^*$ und $\epsilon_1^{x_1} \dots \epsilon_t^{x_t}$ bezüglich allen Einbettungen dasselbe Signum wie α' hat. Das

Signum bezüglich einem ι_i ist genau dann gleich, wenn

$$|\{j \mid \text{sign}(\iota_i(\epsilon_j)) = -1 \text{ und } x_j = 1\}| \equiv \begin{cases} 1 \pmod 2 & , \text{sign}(\iota_i(\alpha')) = -1 \\ 0 \pmod 2 & , \text{sign}(\iota_i(\alpha')) = 1 \end{cases}.$$

Diese Kongruenz ist aber genau dann erfüllt, wenn x Lösung des linearen Gleichungssystems $xM = V$ ist. □

(3.4.4) Bemerkung

Um später in der Implementierung Zeit zu sparen, kann man bemerken, dass sich verschiedene total-positive Erzeuger des gleichen Ideals jeweils lediglich um eine total-positive Einheit unterscheiden. Es lohnt sich also, zu Beginn des Algorithmus die Menge aller total-positiven Einheiten (diese korrespondieren zum Kern von M) zu berechnen, sodass man später pro Ideal jeweils nur eine spezielle Lösung des Gleichungssystems finden muss und die Menge aller total-positiven Erzeuger durch Multiplikation mit den vorher berechneten total-positiven Einheiten erstellt.

Eine weitere Anmerkung zur Implementierung: `MAGMA` kann mit der Funktion `pFundamentalUnits` eine Untergruppe von $\mathbb{Z}_{K^+}^*$ mit ungeradem Index berechnen. Wie das folgende Lemma zeigt, reicht dies für unser Vorhaben bereits aus, da wir nur ein Vertretersystem der Einheiten modulo Quadraten benötigen.

(3.4.5) Lemma

Sei G eine abelsche Gruppe und $U \leq G$ mit $[G : U]$ ungerade. Dann ist

$$G/G^2 \cong U/U^2.$$

Beweis:

Betrachte den Epimorphismus $\pi : G \to G/G^2$. Es ist bereits $\pi|_U$ surjektiv, denn sei $gG^2 \in G/G^2$, dann ist $g^{[G:U]} \in U$, da $(gU)^{[G:U]} = U$ und weil der Index ungerade ist auch $\pi\left(g^{[G:U]}\right) = gG^2$. Zudem ist $\text{Kern}(\pi|_U) = U \cap G^2 = U^2$, denn für $g^2 \in U \cap G^2$

muss $|gU| \leq 2$ gelten, die Ordnung kann aber wegen des ungeraden Index nicht 2 sein, also folgt bereits $g \in U$ und somit $g^2 \in U^2$. Mit dem Homomorphiesatz folgt die Behauptung. $\square$

Anhand der gewonnenen Erkenntnisse erstellen wir nun einen Algorithmus (3), der zu einem Ideal $\mathcal{I} = \alpha'\mathbb{Z}_K$ für $\alpha' \in K^+$ ein Vertretersystem aller total-positiven Erzeuger $\alpha \in K^+_{\gg 0}$ modulo $\lambda\overline{\lambda}$ für $\lambda \in \mathbb{Z}_K^*$ zurückgibt. Die Ergebnisse der Zeilen $6 - 14$ können in der Implementierung nach einmaliger Durchführung abgespeichert werden, sodass die Resultate anschließend für jedes zu prüfende α' wiederverwertet werden können.

Algorithmus 3 Berechnung total-positiver Erzeuger

Eingabe: Erzeuger $\alpha' \in K^+$ von $\mathcal{I}$.

Ausgabe: Liste von Vertretern der Menge aller total-positiven Erzeuger $\alpha \in K^+_{\gg 0}$ von $\mathcal{I}$ modulo $\{\lambda\overline{\lambda} \mid \lambda \in \mathbb{Z}_K^*\}$ zurückgibt.

$\iota_1, \ldots, \iota_t \leftarrow$ Einbettungen $K^+ \hookrightarrow \mathbb{R}$

$\epsilon_1, \ldots \epsilon_t \leftarrow$ Erzeuger einer Untergruppe von $\mathbb{Z}_{K^+}^*$ mit ungeradem Index

$M \leftarrow 0 \in \mathbb{F}_2^{t \times t}$

for $(i, j) \in \underline{t} \times \underline{t}$ **do**

    if $\iota_i(\epsilon_j) < 0$ **then**

        $M_{ij} \leftarrow 1$

$U' \leftarrow [\epsilon_1^{a_1} \ldots \epsilon_t^{a_t} \mid a \in \mathrm{Kern}(M)]$

$U \leftarrow [\,]$

for $u' \in U'$ **do**

    if $u' \neq u\lambda\overline{\lambda}$ für alle $u \in U, \lambda \in \mathbb{Z}_K^*$ **then**

        $U \leftarrow U \cup [u']$

$V \leftarrow 0 \in \mathbb{F}_2^{1 \times t}$

for $i \in \{1, \ldots, t\}$ **do**

    if $\iota_i(\alpha') < 0$ **then**

        $V_i \leftarrow 1$

$x \leftarrow$ Lösung von $xM = V$

return xU

§ 3.5 Finaler Algorithmus und Ergebnisse

Alle bisherigen Bestandteile können nun zu einem Algorithmus zusammengesetzt werden, der zu einem quadratfreien $\ell \in \mathbb{N}$, einer vorgegebenen Determinante d und einem

CM-Körper K mit total-reellem Teilkörper K^+ alle Ideal-Gitter berechnet.

Algorithmus 4 Berechnung von Ideal-Gittern

1: **Eingabe:** Quadratfreies $\ell \in \mathbb{N}$, $d \in \mathbb{N}$, CM-Körper K, maximaler total-reeller Teilkörper K^+ von K
2: **Ausgabe:** Per Isomorphie reduzierte Liste aller geraden Ideal-Gitter $(\mathcal{I}, \alpha)$ in K von Stufe ℓ und mit Determinante d
3:
4: $\mathfrak{A} \leftarrow$ Vertretersystem von $Cl_K/\mathrm{Gal}(K/\mathbb{Q})$
5: $\mathfrak{B} \leftarrow [\mathcal{B} \mid \mathcal{B}$ ist $\mathbb{Z}_K$-Ideal mit $\ell\mathbb{Z}_K \subseteq \mathcal{B} \subseteq \mathbb{Z}_K$ und $\mathcal{N}(\mathcal{B}) = d]$ (nach Algorithmus (1))
6: List $\leftarrow [\ ]$
7: **for** $(\mathcal{I}, \mathcal{B}) \in (\mathfrak{A}, \mathfrak{B})$ **do**
8: $\quad \mathcal{J} \leftarrow \left(\mathcal{I}\overline{\mathcal{I}}\right)^{-1} \Delta\mathcal{B}$
9: $\quad$ **if** $\exists \alpha' \in K^+$ mit $\mathcal{J} = \alpha'\mathbb{Z}_K$ (nach Algorithmus (2)) **then**
10: $\quad\quad X \leftarrow \left[\alpha \in K^+_{\gg 0} \mid \mathcal{J} = \alpha\mathbb{Z}_K\right]$ (nach Algorithmus (3))
11: $\quad\quad$ **for** $\alpha \in X$ **do**
12: $\quad\quad\quad$ **if** $(\mathcal{I}, \alpha)$ ist gerades Gitter der Stufe ℓ **then**
13: $\quad\quad\quad\quad$ **if** $(\mathcal{I}, \alpha) \ncong (\tilde{\mathcal{I}}, \tilde{\alpha})$ für alle $(\tilde{\mathcal{I}}, \tilde{\alpha}) \in$ List **then**
14: $\quad\quad\quad\quad\quad$ List $\leftarrow$ List $\cup\, [(\mathcal{I}, \alpha)]$

Mit diesem Algorithmus kann man nun alle ℓ-modularen Gitter in Dimension n klassifizieren, welche einen Automorphismus σ besitzen mit $\mu_\sigma = \Phi_m$ und $\varphi(m) = n$. Dazu wendet man Algorithmus (4) wie in Lemma (2.2.2) und Lemma (3.1.5) besprochen mit $d = l^{\frac{n}{2}}$ und $K = \mathbb{Q}(\zeta_m)$ an. Eine weitere kleine Erleichterung bringt in diesem Spezialfall die Tatsache, dass $\mathbb{Q}(\zeta_m) \cong \mathbb{Q}(\zeta_{2m})$, falls $m \equiv 1 \pmod 2$. Insbesondere sind die Ideal-Gitter über $\mathbb{Q}(\zeta_m)$ und $\mathbb{Q}(\zeta_{2m})$ dieselben. Man kann also für eine vollständige Aufzählung alle m mit $m \equiv 2 \pmod 4$ weglassen. Eine Implementierung in `MAGMA` liefert nun alle ℓ-modularen Ideal-Gitter mit Dimension $n \leq 36$ (eine Steigerung der Dimension

n \ ℓ	1	2	3	5	6	7	11	14	15	23
4	–	1(1)	1(1)	–	–	–	1(1)	1(1)	–	1(1)
6	–	–	1(1)	–	–	1(1)	–	–	–	–
8	1(1)	1(1)	1(1)	1(1)	1(1)	1(1)	2(1)	2(1)	1(1)	3(–)
10	–	–	–	–	–	–	1(1)	–	–	–
12	–	1(1)	2(1)	1(1)	1(1)	1(–)	1(–)	1(1)	–	1(–)
16	1(1)	2(1)	3(2)	1(–)	2(1)	4(3)	5(–)	5(–)	3(1)	5(–)
18	–	–	1(–)	–	–	–	–	–	–	–
20	–	1(1)	–	–	1(1)	1(–)	2(–)	–	–	–
22	–	–	–	–	–	–	–	–	–	2(–)
24	4(1)	2(1)	7(1)	5(1)	5(2)	8(–)	7(–)	8(–)	5(–)	–
32	7(5)	13(4)	13(7)	10(–)	12(–)	19(–)	42(–)	21(–)	23(–)	–
36	–	6(3)	8(–)	8(–)	–	–	2(–)	36(–)	4(–)	–

Tabelle 3.1: Anzahl der ℓ-modularen Ideal-Gitter in Dimension $n \leq 36$, sowie der Anzahl der extremalen Gitter darunter

beansprucht exponentiell höheren Zeitaufwand) und $\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$. In Tabelle (3.5) sind die Gesamtzahlen der Ideal-Gitter zu finden, außerdem befindet sich in Anhang A eine ausführlichere Zusammenfassung der Klassifikationsergebnisse mit zusätzlicher Angabe der zugrundeliegenden zyklotomischen Zahlkörpern und Anzahl der Gitter aufgeteilt nach Minimum.

4 Sub-Ideal-Gitter

§ 4.1 Einführung

Im letzten Kapitel haben wir gesehen, wie Gitter in Dimension n mit einem Automorphismus σ klassifiziert werden können, falls $\mu_\sigma = \Phi_m$ und $\varphi(m) = n$ erfüllt sind. In diesem Kapitel wollen wir versuchen, Aussagen über Gitter zu treffen, welche lediglich ein Ideal-Gitter enthalten. Gilt $\Phi_m | \mu_\sigma$ für ein $\sigma \in \mathrm{Aut}(L)$, so können wir den zugrundeliegenden Vektorraum V in σ-invariante Teilräume aufspalten:

$$V = \mathrm{Kern}(\Phi_m(\sigma)) \oplus \mathrm{Kern}\left(\frac{\mu_\sigma}{\Phi_m}(\sigma)\right).$$

Für $\frac{n}{2} < \varphi(m) \leq n$ muss $\mathrm{Kern}(\Phi_m(\sigma))$ die Dimension $\varphi(m)$ haben, wird also zu einem eindimensionalen $\mathbb{Q}(\zeta_m)$-Vektorraum und $L \cap \mathrm{Kern}(\Phi_m(\sigma))$ hat eine Struktur als Ideal-Gitter über diesem zyklotomischen Körper. Vergleiche dazu [Neb13, Abs. (5.3)]

(4.1.1) Definition

Sei L ein $\mathbb{Z}$-Gitter der Dimension n.

(i) Ein *großer Automorphismus* von L ist ein $\sigma \in \mathrm{Aut}(L)$ mit $\Phi_m | \mu_\sigma$ für ein $m \in \mathbb{N}$, sodass $\frac{n}{2} < \varphi(m) \leq n$.

(ii) Ist $\sigma \in \mathrm{Aut}(L)$ ein großer Automorphismus, so bezeichnet man das Ideal-Gitter $L \cap \mathrm{Kern}(\Phi_m(\sigma))$ über $\mathbb{Q}(\zeta_m)$ als *Sub-Ideal-Gitter* von L.

Für Gitter mit großen Automorphismen verstehen wir die Ideal-Gitter-Komponente mit der Theorie des letzten Kapitels sehr gut. Probleme bereitet uns allerdings der andere Teil $\mathrm{Kern}\left(\frac{\mu_\sigma}{\Phi_m}(\sigma)\right)$ des Vektorraums, über welchen wir a priori nicht viel aussagen können. Abhilfe schaffen uns unter gewissen Umständen die Automorphismen von Primzahlordnung.

§ 4.2 Automorphismen von Primzahlordnung

Der folgende Abschnitt ist an [Jü15, Kap. 4] und [Neb13, Kap. 4] angelehnt.

Sei L in diesem Abschnitt ein $\mathbb{Z}$-Gitter in einem n-dimensionalen bilinearen $\mathbb{Q}$-Vektorraum (V, b) und $\sigma \in \mathrm{Aut}(L)$ von Primzahlordnung p. Dann ist $\mu_\sigma \in \{\Phi_p, \Phi_1\Phi_p\}$. Man erhält eine σ-invariante Zerlegung

$$V = \mathrm{Kern}(\Phi_1(\sigma)) \oplus \mathrm{Kern}(\Phi_p(\sigma)) =: V_1 \oplus V_p$$

Es ist $\Phi_1(X) = X - 1$, also $V_p = \mathrm{Bild}(\sigma - 1)$, $V_1 = \mathrm{Kern}(\sigma - 1)$. Seien n_p die Dimension von V_p und n_1 die Dimension von V_1 über $\mathbb{Q}$. Da V_p eine Struktur als $\mathbb{Q}(\zeta_p)$-Vektorraum hat und $\mathrm{Dim}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) = p - 1$, muss n_p von $p - 1$ geteilt werden.

Wie das folgende Lemma zeigt, ist die Summe sogar orthogonal.

(4.2.1) Lemma

Sei $\sigma \in O(V, b)$ von Primzahlordnung p, dann ist

$$V = \mathrm{Kern}(\Phi_p(\sigma)) \perp \mathrm{Kern}(\Phi_1(\sigma)).$$

Beweis:

Sei $x_p \in \mathrm{Kern}(\Phi_p(\sigma))$ und $x_1 \in \mathrm{Kern}(\Phi_1(\sigma))$. Dann gilt $\sigma(x_1) = x_1$ und es existiert ein $y \in V$ mit $(\sigma - 1)(y) = x_p$. Zusammen mit der Tatsache, dass die Bilinearform b invariant unter σ ist, folgt:

$$b(x_1, x_p) = b(x_1, (\sigma - 1)(y)) = b(\sigma(x_1), \sigma(y)) - b(x_1, y) = b(x_1, y) - b(x_1, y) = 0. \quad \square$$

Damit induziert σ ein Teilgitter von L. Definiert man nämlich $L_p := L \cap V_p$ und $L_1 := L \cap V_1$, so ist offensichtlich $M := L_p \perp L_1 \leq L$. Im Folgenden wollen wir die Struktur von M näher untersuchen.

(4.2.2) Lemma

Seien σ, L_1 und L_p wie oben.

(i) Es existiert ein Polynom $v \in \mathbb{Z}[X]$ mit $1 = \frac{1}{p} v \cdot \Phi_1 + \frac{1}{p} \Phi_p$.

(ii) Es gilt $pL \subseteq L_p \perp L_1 \subseteq L$.

Beweis:

(i) Nach (3.1.4) ist $\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$, also ist $\Phi_p(1) = p$ und somit 1 eine Nullstelle von $p - \Phi_p \in \mathbb{Z}[X]$. Da $\Phi_1(X) = X - 1$ folgt daher

$$p - \Phi_p = v \cdot \Phi_1 \text{ für ein } v \in \mathbb{Q}[X]. \tag{4.1}$$

Mit dem Lemma von Gauß muss $v \in \mathbb{Z}[X]$ gelten. Umstellen der Gleichung (4.1) liefert die Behauptung.

(ii) Zu zeigen ist $px \in L_p \perp L_1$ für alle $x \in L$. Wegen $(\Phi_1\Phi_p)(\sigma) = 0$ und der σ-Invarianz von L ist

$$\begin{aligned} px = (v \cdot \Phi_1)(\sigma)(x) + \Phi_p(\sigma)(x) &\in \mathrm{Kern}(\Phi_p(\sigma)) \cap L + \mathrm{Kern}(\Phi_1(\sigma))(\sigma) \cap L \\ &= (V_p \cap L) \perp (V_1 \cap L) = L_p \perp L_1 \end{aligned}$$ □

Mit diesem Lemma muss M ein Gitter der Dimension n sein, also gilt $\mathrm{Dim}(L_p) = n_p$ und $\mathrm{Dim}(L_1) = n_1$. Ist L gerade und von quadratfreier Stufe ℓ, so gilt $\ell L^\# \subseteq L$. Lemma (4.2.2)(ii) ist äquivalent zu $pM^\# \subseteq L^\#$. Zusammen erhält man folglich

$$\ell p M^\# \subseteq \ell L^\# \subseteq L$$

Schneidet man mit V_p, so folgt

$$\ell p(M^\# \cap V_p) \subseteq (L \cap V_p) \Leftrightarrow \ell p L_p^\# \subseteq L_p$$

und analog $\ell p L_1^\# \subseteq L_1$.

Im Spezialfall $\mathrm{ggT}(\ell, p) = 1$ bedeutet dies, dass die Stufe der Gitter L_p und L_1 das Produkt ℓp teilt.
Als nächstes wollen wir die Determinanten von L_p und L_1 untersuchen. Dazu werden die partiellen Dualgitter betrachtet.

(4.2.3) Lemma
Sei L ein gerades Gitter der quadratfreien Stufe ℓ und $\sigma \in \mathrm{Aut}(L)$ von Primzahlordnung p mit $\mathrm{ggT}(p, \ell) = 1$.

(i) $pL_1^{\#,p} \subseteq L_1$.

(ii) $(1 - \sigma)L_p^{\#,p} \subseteq L_p$.

Beweis:

Teil (i) folgt bereits aus der Definition des partiellen Duals, denn es gilt

$$pL_1^{\#,p} = p\left(\frac{1}{p}L_1 \cap L_1^{\#}\right) = L_1 \cap pL_1^{\#} \subseteq L_1.$$

Kommen wir nun zu Teil (ii). Definiere dazu die Projektionen $\pi_1 := \frac{1}{p}\Phi_p(\sigma)$ und $\pi_p := 1 - \pi_1$ auf V_1 bzw. V_p (vgl. Lemma (4.2.2)). Es zeigt sich:

$$\begin{aligned}(1-\sigma)\pi_p &= (1-\sigma)(1-\pi_1)\\ &= 1-\sigma-\pi_1+\sigma\pi_1\\ &= 1-\sigma-\pi_1+\frac{1}{p}(\sigma^p+\sigma^{p-1}+\cdots+\sigma)\\ &= 1-\sigma-\pi_1+\frac{1}{p}(1+\sigma^{p-1}+\cdots+\sigma)\\ &= 1-\sigma-\pi_1+\pi_1\\ &= 1-\sigma.\end{aligned}$$

Sei nun $(b_1,\ldots,b_n)$ eine Basis von L mit zugehöriger Dualbasis $(b_1^{\#},\ldots,b_n^{\#})$, sodass $(b_1,\ldots,b_{n_p})$ Basis von L_p ist. Dann gilt

$$\pi_p(L^{\#}) = \pi_p(\langle b_1^{\#},\ldots,b_n^{\#}\rangle) = \langle b_1^{\#},\ldots,b_{n_p}^{\#}\rangle = L_p^{\#}.$$

Setzt man diese beiden Fakten zusammen, so erhält man

$$(1-\sigma)L_p^{\#} = (1-\sigma)\pi_p(L^{\#}) = (1-\sigma)L^{\#} \overset{\text{Stufe } \ell}{\subseteq} (1-\sigma)\frac{1}{\ell}L \overset{L\ \sigma\text{-invariant}}{\subseteq} \frac{1}{\ell}L.$$

Außerdem ist $(1-\sigma)L_p^{\#} \subseteq V_p$, also zusammen

$$(1-\sigma)L_p^{\#} \subseteq \frac{1}{\ell}L \cap V_p = \frac{1}{\ell}L_p$$

Für das partielle Dual ergibt sich hiermit

$$(1-\sigma)L_p^{\#,p} = (1-\sigma)\left(\frac{1}{p}L_p \cap L_p^{\#}\right) \subseteq \frac{1}{p}L_p \cap \frac{1}{\ell}L_p = \frac{1}{\mathrm{ggT}(p,\ell)}L_p = L_p \qquad \square$$

Wir benötigen noch ein weiteres Hilfslemma.

(4.2.4) Lemma

Sei Λ ein gerades Gitter, dessen Stufe $p\ell$ teilt, wobei p prim und ℓ quadratfrei mit $\mathrm{ggT}(p,\ell)=1$. Dann ist $\Lambda^{\#,p}/\Lambda \cong \Lambda^{\#}/\Lambda^{\#,\ell}$.

Beweis:

Sei $\psi : \Lambda^{\#,p} \to \Lambda^{\#}/\Lambda^{\#,\ell}, x \mapsto x + \Lambda^{\#,\ell}$.

Surjektivität: Sei $x \in \Lambda^{\#}$. Wegen $p\ell\Lambda^{\#} \subseteq \Lambda$ ist $p\Lambda^{\#} \subseteq \Lambda^{\#,\ell}$ und $\ell\Lambda^{\#} \subseteq \Lambda^{\#,p}$. Nach Euklid existieren Zahlen $s,t \in \mathbb{Z}$ mit $sp + t\ell = 1$. Dann ist $x = spx + t\ell x \subseteq \Lambda^{\#,\ell} + \Lambda^{\#,p}$ und somit $\psi(t\ell x) = x + \Lambda^{\#,\ell}$.

Kern: Der Kern der Abbildung ist $\Lambda^{\#,p} \cap \Lambda^{\#,\ell}$. Es ist einerseits

$$\Lambda^{\#,p} \cap \Lambda^{\#,\ell} \subseteq \frac{1}{p}\Lambda \cap \frac{1}{\ell}\Lambda = \frac{1}{\mathrm{ggT}(p,\ell)}\Lambda = \Lambda$$

und andersherum per Definition $\Lambda \subseteq \Lambda^{\#,p}$ und $\Lambda \subseteq \Lambda^{\#,\ell}$. Insgesamt ist $\mathrm{Kern}(\psi) = \Lambda$.

Die Behauptung folgt nun mit dem Homomorphiesatz. □

Nun ein wichtiger Satz zur Bestimmung der Determinanten:

(4.2.5) Satz

Sei L wie vorher von Stufe quadratfreien Stufe ℓ und $\sigma \in \mathrm{Aut}(L)$ mit $|\sigma| = p$, $\mathrm{ggT}(p,\ell) = 1$. Seien außerdem L_1 und L_p definiert wie zuvor mit Dimensionen n_1 und n_p. Dann gilt:

$$L_1^{\#,p}/L_1 \cong \mathbb{F}_p^s \cong L_p^{\#,p}/L_p$$

für ein $s \in \{0,\ldots,\min(n_1, \frac{n_p}{p-1})\}$.

Beweis:

Wir zeigen zunächst$L_1^{\#,p}/L_1 \cong L_p^{\#,p}/L_p$. Dies ist nach Lemma (4.2.4) äquivalent zu $L_1^{\#}/L_1^{\#,\ell} \cong L_p^{\#}/L_p^{\#,\ell}$.

Sei $y \in L_1^{\#}$ beliebig. Die Abbildung $L_1 \to \mathbb{Z}, x \mapsto b(x,y)$ ist eine Linearform. Da L_1 der Schnitt von L mit dem Untervektorraum V_1 ist, lässt sich diese Linearform sich eindeutig fortsetzen zu einer Linearform auf ganz L. Unter Ausnutzung der Isomorphie $\mathrm{Hom}_{\mathbb{Z}}(L,\mathbb{Z}) \cong L^{\#}$ existiert ein Element $\hat{y} \in L^{\#}$, welches diese Linearform darstellt, insbesondere gilt also $b(x,y) = b(x,\hat{y})$ für alle $x \in L_1$. Zunächst zeigt sich für das Element $\hat{y} - y$:

$$b(x, \hat{y} - y) = 0 \quad \text{für alle } x \in L_1$$

und somit $\hat{y} - y \in V_1^{\perp} = V_p$. Außerdem ist

$$b(x, \hat{y} - y) = b(x,\hat{y}) - b(x,y) = b(x,\hat{y}) \in \mathbb{Z} \quad \text{für alle } x \in L_p.$$

Insgesamt gilt damit $\hat{y} - y \in L_p^{\#}$. Wir können somit die folgende Abbildung definieren:

$$\psi : L_1^{\#} \to L_p^{\#}/L_p^{\#,\ell}, y \mapsto (\hat{y} - y) + L_p^{\#,\ell}.$$

Wir zeigen nun, dass ψ ein wohldefinierter Epimomorphismus mit Kern $L_1^{\#,\ell}$ ist und folgern dann die Behauptung erneut mit dem Homomorphiesatz.

Wohldefiniert: Es definiere $\tilde{y} \in L^{\#}$ eine weitere Fortsetzung. Da L von Stufe ℓ ist, gilt $\hat{y} - \tilde{y} \in L^{\#} \subseteq \frac{1}{\ell}L$. Wir schlussfolgern für $y \in L_1^{\#}$:

$$(\hat{y} - y) - (\tilde{y} - y) = \hat{y} - \tilde{y} \in \frac{1}{\ell}L \cap L_p^{\#} = \frac{1}{\ell}L_p \cap L_p^{\#} = L_p^{\#,\ell}.$$

Das Bild unter ψ hängt daher nicht von der gewählten Fortsetzung ab.

Linearität: Seien $y_1, y_2 \in L_1^{\#}$ mit Elementen $\hat{y_1}, \hat{y_2} \in L^{\#}$, welche die zugehörigen fortgesetzten Linearformen darstellen. Für $s,t \in \mathbb{Z}$ definiert dann $s\hat{y_1} + t\hat{y_2}$ eine Fortsetzung der Linearform $x \mapsto b(x, sy_1 + ty_2)$.

Surjektivität: Sei $y' \in L_p^{\#}$. Es korrespondiere $\hat{y} \in L^{\#}$ zu einer Fortsetzung von $x \mapsto b(x,y) \in \mathrm{Hom}_{\mathbb{Z}}(L_p, \mathbb{Z})$ auf L. Wie zuvor liegt dann das Element $y := \hat{y} - y'$ in $L_1^{\#}$. Durch $\hat{y}$ wird zudem eine Fortsetzung der Linearform $L_1 \to \mathbb{Z}, x \mapsto b(x,y)$ dargestellt, denn für alle $x \in L_1$ ist

$$b(x,y) = b(x, \hat{y} - y') = b(x,\hat{y}) - b(x,y') = b(x,\hat{y})$$

Somit ist $\psi(y) = (\hat{y} - y) + L_1^{\#,\ell} = y' + L_1^{\#,\ell}$.

Kern: Es ist $\mathrm{Kern}(\psi) \subseteq L_1^{\#,\ell}$, denn sei $y \in \mathrm{Kern}(\psi)$, so gilt $\hat{y} - y \in \frac{1}{\ell} L_p^{\#,\ell} \subseteq \frac{1}{\ell} L_p \subseteq \frac{1}{\ell} L$. Da zudem $\hat{y} \in L^{\#} \subseteq \frac{1}{\ell} L$ ist, folgt $y = \hat{y} - (\hat{y} - y) \in \frac{1}{\ell}$. Insgesamt gilt daher $y \in \frac{1}{\ell} L \cap L_1^{\#} = \frac{1}{\ell} L_1 \cap L_1^{\#} = L_1^{\#,\ell}$

Andersherum ist $L_1^{\#,\ell} \subseteq \mathrm{Kern}(\psi)$, denn sei $y \in L_1^{\#,\ell}$, so ist $y \in \frac{1}{\ell} L_1 \subseteq \frac{1}{\ell} L$. Somit gilt $\hat{y} - y \in \frac{1}{\ell} L \cap L_p^{\#} = \frac{1}{\ell} L_p \cap L_p^{\#} = L_p^{\#,\ell}$ und damit $y \in \mathrm{Kern}(\psi)$.

Die erste Behauptung folgt nun aus dem Homomorphiesatz.

Verwendet man nun Lemma (4.2.3), so zeigt sich, dass $L_1^{\#,p} / L_1$ ein Quotient der Gruppe $L_1^{\#,p} / p L_1^{\#,p} \cong \mathbb{F}_p^{n_1}$ ist und somit die Gestalt $\mathbb{F}_p^s$ für ein $s \in \{0, \ldots, n_1\}$ besitzt.
Analog zeigt dasselbe Lemma, dass $L_p^{\#,p} / L_p$ ein Quotient der Gruppe $L_p^{\#,p} / (1-\sigma) L_p^{\#,p} \cong (\mathbb{Z}[\zeta_p] / (1-\zeta_p)\mathbb{Z}[\zeta_p])^{\frac{n_p}{p-1}}$. In letzterer Gruppe ist

$$\begin{aligned} p + (1-\zeta_p)\mathbb{Z}[\zeta_p] &= \underbrace{1 + \cdots + 1}_{p \text{ mal}} + (1-\zeta_p)\mathbb{Z}[\zeta_p] \\ &= 1^{p-1} + \cdots + 1^0 + (1-\zeta_p)\mathbb{Z}[\zeta_p] \\ &= \zeta_p^{p-1} + \cdots + \zeta_p^0 + (1-\zeta_p)\mathbb{Z}[\zeta_p] \\ &= 0 + (1-\zeta_p)\mathbb{Z}[\zeta_p], \end{aligned}$$

diese enthält also genau p Elemente und wir erhalten finalerweise, dass $L_p^{\#,p} / L_p$ ein Quotient von $(\mathbb{F}_p)^{\frac{n_p}{p-1}}$ ist. Damit folgt $s \leq \frac{n_p}{p-1}$. □

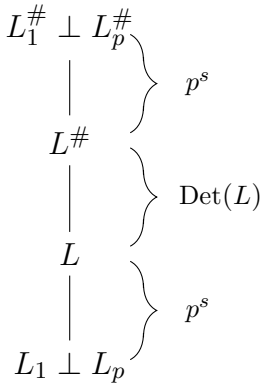

Abbildung 4.1: Inklusionsverband

Nach Lemma (4.2.4) ist

$$\mathrm{Det}(L_p) = \left[L_p^\# : L_p\right] = \left[L_p^\# : L_p^{\#,\ell}\right] \cdot \left[L_p^{\#,\ell} : L_p\right] = \left[L_p^{\#,p} : L_p\right] \cdot \left[L_p^{\#,\ell} : L_p\right].$$

Außerdem teilt p den Index $\left[L_p^{\#,\ell} : L_p\right]$ nicht, da der Exponent der Faktorgruppe $L_p^{\#,\ell}/L_p$ wegen $\ell L_p^{\#,\ell} \subseteq L_p$ ein Teiler von ℓ sein muss und $\mathrm{ggT}(\ell, p) = 1$. Ist also s wie im vorigen Satz, so ist s bereits die p-Bewertung der Determinante von L_p. Die Überlegungen funktionieren selbstverständlich analog für L_1. Der Satz sagt uns also, dass $\mathrm{Det}(L_1) = p^s c$ und $\mathrm{Det}(L_p) = p^s d$ für gewisse $c, d \in \mathbb{N}$ teilerfremd zu p. Nach Lemma (4.2.2) ist der Index $[L : M]$ allerdings eine p-Potenz, während die Determinante von L teilerfremd zu p ist. Daher muss $c \cdot d = \mathrm{Det}(L)$ gelten und sich der in Abbildung (4.1) dargestellte Inklusionsverband ergeben.

Diese Überlegungen erlauben uns folgende Definition:

(4.2.6) Definition

Sei L ein gerades Gitter der quadratfreien Stufe ℓ. Sei weiterhin $\sigma \in \mathrm{Aut}(L)$ von Ordnung p und L_1 und L_p mit Dimensionen n_1 und n_p wie zuvor die von σ induzierten Teilgitter. Die Primfaktorzerlegung von ℓ sei gegeben durch $\ell = q_1 \dots q_m$. Ist

$\mathrm{Det}(L_1) = p^s q_1^{k_{1,1}} \dots q_m^{k_{1,m}}$ und $\mathrm{Det}(L_p) = p^s q_1^{k_{p,1}} \dots q_m^{k_{p,m}}$, so nennen wir das Tupel

$$p - (n_1, n_p) - s - q_1 - (k_{1,1}, k_{p,1}) - q_2 - (k_{1,2}, k_{p,2}) - \dots - q_m - (k_{1,m}, k_{p,m})$$

den *Typen* von σ.

Ist $m = 1$, also ℓ prim, so können wir die Schreibweise verkürzen zu

$$p - (n_1, n_p) - s - (k_1, k_p).$$

Wir können nun einige Einschränkungen an den Typen eines solchen Automorphismus machen.

(4.2.7) Satz

Sei L ein gerades, n-dimensionales Gitter der quadratfreien Stufe ℓ mit Determinante $\mathrm{Det}(L) = \ell^k$. Sei zudem $\sigma \in \mathrm{Aut}(L)$ von Typ $p - (n_1, n_p) - s - q_1 - (k_{1,1}, k_{p,1}) - \dots - q_m - (k_{1,m}, k_{p,m})$, wobei $\mathrm{ggT}(p, \ell) = 1$. Dann gelten folgende Einschränkungen (für alle $i \in \underline{m}$):

(i) $n_1 + n_p = n$.

(ii) $s \in \{0, \dots, \min(n_1, \frac{n_p}{p-1})\}$.

(iii) $s \equiv_2 (p-2)\frac{n_p}{p-1}$.

(iv) $k_{1,i} \in \{0, \dots, \min(n_1, k)\}$.

(v) $k_{1,i} \equiv_2 k$.

(vi) $k_{p,i} \in \{0, \dots, \min(n_p, k)\}$.

(vii) $k_{p,i} \equiv_2 0$.

(viii) $(2f(\ell))\,|k_{p,i}$, wobei $f(\ell)$ den Trägheitsgrad von $\ell\mathbb{Z}_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})}$ bezeichne.

(ix) $k_{1,i} + k_{p,i} = k$.

Beweis:

Eigenschaft (i) ist klar, (ii) ist Satz (4.2.5), Nummer (iv), (vi) und (ix) ergeben sich daraus, dass die Stufen von L_p und L_1 Teiler von $p\ell$ sind und der Tatsache, dass $\frac{\mathrm{Det}(L_1)\mathrm{Det}(L_p)}{p^{2s}} = \mathrm{Det}(L)$.

Nach [Jü15, Satz (3.1.4)(d) und Lemma (3.1.1)] existiert ein $\mathbb{Z}_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})}$-Ideal $\mathfrak{a}$ mit

$$\mathrm{Det}(L_p) = p^s q_1^{k_{p,1}} \dots q_m^{k_{p,m}} = p^{(p-2)\frac{n_p}{p-1}} \cdot \mathcal{N}(\mathfrak{a})^2.$$

Daraus folgt sofort Eigenschaft (iii) und mit $\mathrm{ggT}(p,\ell) = 1$ auch (vii). Zuletzt ergibt sich (v) aus (vii) und (ix). Teil (viii) ist [Jü15, Korollar (4.1.9)]. □

Im Spezialfall $p = 2$ hat die Gruppe $M^{\#,2}/M$ Exponent 2, mit einer Verallgemeinerung von [Neb13, Lemma (4.9)] können wir eine weitere Einschränkung machen.

(4.2.8) Lemma

Sei M ein gerades Gitter in einem bilinearen Vektorraum (V, b) und $M^{\#,2}/M$ habe Exponent 2. Dann enthält M ein Teilgitter isometrisch zu $\sqrt{2}U$, wobei U ein Gitter mit $U = U^{\#,2}$ ist und der Index $\left[M : \sqrt{2}U\right]$ eine Zweierpotenz.

Beweis:

Wir betrachten die 2-adische Jordanzerlegung (vgl. [CS93, Kapitel 7]

$$\mathbb{Z}_2 \otimes M \cong f_1 \oplus \sqrt{2} f_2$$

mit einem geraden Gitter f_1 und einem ganzen Gitter f_2, sodass $\mathrm{Det}(f_1)$ und $\mathrm{Det}(f_2)$ teilerfremd zu 2 sind. Da f_1 ein regulärer $\mathbb{Z}_2$-Modul ist, erlaubt uns [Kne02, Satz (4.1)] eine Zerlegung

$$f_1 = E_1 \perp E_2 \perp \cdots \perp E_m$$

mit regulären Teilmoduln E_i von Dimension ≤ 2. Da jedes E_i ein gerades Gitter sein muss, folgt $\mathrm{Dim}(E_i) = 2$ für alle $i = 1, \ldots, m$. Insbesondere hat f_1 die gerade Dimension $2m$.

Ist $m = 0$, so sind wir fertig mit $U := f_2$. Sei also nun $m > 0$.
Wir zeigen nun, f_1 enthält ein Element v mit $b(v, v) \in 2\mathbb{Z}_2^*$. Dazu schreiben wir $E_1 = \langle x, y\rangle$ und definieren s, t durch $b(x, x) \in 2^s\mathbb{Z}_2^*$ und $b(y, y) \in 2^t\mathbb{Z}_2^*$. Ist $s = 1$ oder $t = 1$, so haben wir mit $v := x$ bzw. $v := y$ ein solches Element gefunden. Seien also nun $s, t \geq 2$. Dann folgt

$$b(x - y, x - y) = b(x, x) + b(y, y) - 2b(x, y).$$

Nun muss $b(x, y)$ in $\mathbb{Z}_2^*$ liegen, da sonst die Gram-Matrix von E_1 nur gerade Einträge und somit auch eine gerade Determinante hätte. Somit erhalten wir

$$b(x - y, x - y) \in 2^s\mathbb{Z}_2^* + 2^t\mathbb{Z}_2^* + 2\mathbb{Z}_2^* = 2(\underbrace{2^{s-1}\mathbb{Z}_2^* + 2^{t-1}\mathbb{Z}_2^*}_{\subseteq 2\mathbb{Z}_2} + \mathbb{Z}_2^*) \subseteq 2\mathbb{Z}_2^*.$$

Damit ist $v := x - y$ ein Element wie gesucht.
Nach den obrigen Überlegungen können ohne Einschränkung annehmen, dass $E_1 = \langle x, v\rangle$, sonst vertausche x und y. Setze nun $w := b(v, v)x - b(v, x)v$, dann ist $b(v, w) = b(v, v)b(v, x) - b(v, x)b(v, v) = 0$ und mit $b(x, v) \in \mathbb{Z}_2^*$ außerdem

$$b(w, w) = b(v, v)^2 b(x, x) - b(v, v)b(x, v)^2 \in 2^{2+s}\mathbb{Z}_2^* + 2\mathbb{Z}_2^* = 2\mathbb{Z}_2^*.$$

Nun folgt: $\langle v\rangle \perp \langle w\rangle \perp E_2 \perp \cdots \perp E_m$ ist ein Teilgitter von f_1 vom Index 2 und $\langle v\rangle \perp \langle w\rangle = \sqrt{2}g$ für ein reguläres, ganzes Gitter g. Insgesamt ist somit

$$U' := \langle v\rangle \perp \langle w\rangle \perp E_2 \perp \cdots \perp E_m \perp \sqrt{2}f_2$$

ein Teilgitter von M vom Index 2 und mit Jordanzerlegung $(E_2 \perp \cdots \perp E_m) \perp \sqrt{2}\,(g \perp f_2)$. Induktion liefert nun die Behauptung. $\square$

Ist M wie im obigen Lemma mit Determinante $2^s a$ für ein ungerades $a \in \mathbb{N}$, dann hat das Gitter U somit Determinante a und Minimum $\mathrm{Min}(U) \geq \frac{\mathrm{Min}(M)}{2}$. Wir können nun mithilfe der Einschränkungen aus Satz (4.2.7), Lemma (4.2.8) und der Hermite-Schranken aus (2.2) den Algorithmus (5) entwerfen, welcher die möglichen Automorphismentypen gerader Gitter mit quadratfreier Stufe zurückgibt.

Algorithmus 5 Aufzählung von Automorphismen-Typen

Eingabe: Quadratfreies $\ell \in \mathbb{N}$, $k \in \mathbb{N}$, $n \in \mathbb{N}$, $m \in \mathbb{N}$.

Ausgabe: Liste aller Typen von Automorphismen mit Primzahlordnung p von geraden Gittern der Stufe ℓ, Determinante ℓ^k, Dimension n, und Minimum $\geq m$, wobei $\mathrm{ggT}(p, \ell) = 1$.

Res $\leftarrow$ [ ]

$b \leftarrow$ Liste von Schranken für die Hermite-Konstante γ_i für $1 \leq i \leq n$

$q_1, \ldots, q_m \leftarrow$ Primfaktoren von ℓ

for $p \in \mathbb{P}_{\leq n} - \{q_1, \ldots, q_m\}$ **do**

  $f :=$ Trägheitsgrad von $\ell\mathbb{Z}_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})}$

  for $n_p \in \{i(p-1) \mid 1 \leq i \leq \lfloor \frac{n}{p-1} \rfloor\}$ **do**

    $n_1 \leftarrow n - n_p$

    for $(k_{p,1}, k_{p,2}, \ldots, k_{p,m}) \in \{(2f)i \mid i \in \{0, \ldots, \lfloor \frac{\min(n_p,k)}{2f} \rfloor\}\}^m$ **do**

      $k_{1,i} \leftarrow k - k_{p,i}, \quad i \in \underline{m}$

      if $\exists i \in \underline{m} : (k_{1,i} > \min(n_1, k)) \vee (k_{1,i} \not\equiv_2 k) \vee (k_{p,i} \not\equiv_2 0)$ **then**

        continue

      for $s \in \{0, \ldots, \min(n_1, \frac{n_p}{p-1})\}$ **do**

        if $s \not\equiv_2 (p-2)\frac{n_p}{p-1}$ **then continue**

        $\gamma_1 \leftarrow \frac{m}{\left(p^s q_1^{k_{1,1}} \ldots q_m^{k_{1,m}}\right)^{1/n_1}}$

        $\gamma_p \leftarrow \frac{m}{\left(p^s q_1^{k_{p,1}} \ldots q_m^{k_{p,m}}\right)^{1/n_p}}$

        if $\gamma_1 > b_{n_1}$ oder $\gamma_p > b_{n_p}$ **then continue**

        if $p = 2$ **then**

          $\gamma_1' \leftarrow \frac{m/2}{\left(q_1^{k_{1,1}} \ldots q_m^{k_{1,m}}\right)^{1/n_1}}$

          $\gamma_p' \leftarrow \frac{m/2}{\left(q_1^{k_{p,1}} \ldots q_m^{k_{p,m}}\right)^{1/n_p}}$

          if $\gamma_1' > b_{n_1}$ oder $\gamma_p' > b_{n_p}$ **then continue**

        Res $\leftarrow$ Res $\cup\, [p - (n_1, n_p) - s - q_1 - (k_{1,1}, k_{p,1}) - \cdots - (k_{1,m}, k_{p,m})]$

return Res

Wir haben in diesem Kapitel die möglichen Typen von Automorphismen mit Primzahlordnung studiert und Aussagen über die Determinanten der induzierten Teilgitter getroffen. Als nächstes beschreiben wir, wie wir mithilfe der Kneser'schen Nachbarschaftsmethode alle Gitter in fester (kleiner) Dimension und Determinante klassifizieren können.

§ 4.3 Kneser-Nachbarschaftsmethode

5 Anhang

Anhang A: Ergebnisse der Ideal-Gitter-Klassifikation

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
1	8	1(1)	$\mathbb{Q}(\zeta_{15})$	1	–	–	–	–	–	–	–	–
	16	1(1)	$\mathbb{Q}(\zeta_{40})$	1	–	–	–	–	–	–	–	–
	24	4(1)	$\mathbb{Q}(\zeta_{35})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{45})$	1	–	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{54})$	1	–	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{75})$	1	–	–	–	–	–	–	–	–
	32	7(5)	$\mathbb{Q}(\zeta_{51})$	–	2	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{68})$	1	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{80})$	1	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{120})$	–	1	–	–	–	–	–	–	–
2	4	1(1)	$\mathbb{Q}(\zeta_{8})$	1	–	–	–	–	–	–	–	–
	8	1(1)	$\mathbb{Q}(\zeta_{16})$	1	–	–	–	–	–	–	–	–
	12	1(1)	$\mathbb{Q}(\zeta_{36})$	1	–	–	–	–	–	–	–	–

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
2	16	2(1)	$\mathbb{Q}(\zeta_{32})$	1	–	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{40})$	–	1	–	–	–	–	–	–	–
	20	1(1)	$\mathbb{Q}(\zeta_{33})$	–	1	–	–	–	–	–	–	–
	24	2(1)	$\mathbb{Q}(\zeta_{56})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{72})$	1	–	–	–	–	–	–	–	–
	32	13(4)	$\mathbb{Q}(\zeta_{51})$	–	–	3	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{64})$	1	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{68})$	–	3	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{80})$	–	1	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{96})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{120})$	–	2	–	–	–	–	–	–	–
	36	6(3)	$\mathbb{Q}(\zeta_{57})$	–	–	3	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{76})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{108})$	1	1	–	–	–	–	–	–	–
3	4	1(1)	$\mathbb{Q}(\zeta_{12})$	1	–	–	–	–	–	–	–	–
	6	1(1)	$\mathbb{Q}(\zeta_{9})$	1	–	–	–	–	–	–	–	–
	8	1(1)	$\mathbb{Q}(\zeta_{24})$	1	–	–	–	–	–	–	–	–
	12	2(1)	$\mathbb{Q}(\zeta_{21})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{36})$	1	–	–	–	–	–	–	–	–
	16	3(2)	$\mathbb{Q}(\zeta_{40})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{48})$	1	–	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{60})$	–	1	–	–	–	–	–	–	–
	18	1(−)	$\mathbb{Q}(\zeta_{27})$	1	–	–	–	–	–	–	–	–
	24	7(1)	$\mathbb{Q}(\zeta_{39})$	–	–	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{52})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{56})$	–	2	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{72})$	1	1	–	–	–	–	–	–	–

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
3	32	13(7)	$\mathbb{Q}(\zeta_{80})$	–	2	4	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{96})$	1	–	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{120})$	–	3	2	–	–	–	–	–	–
	36	8(−)	$\mathbb{Q}(\zeta_{57})$	–	1	2	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{63})$	–	1	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{76})$	–	–	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{108})$	1	–	1	–	–	–	–	–	–
5	8	1(1)	$\mathbb{Q}(\zeta_{15})$	–	1	–	–	–	–	–	–	–
	12	1(1)	$\mathbb{Q}(\zeta_{21})$	–	1	–	–	–	–	–	–	–
	16	1(−)	$\mathbb{Q}(\zeta_{40})$	–	1	–	–	–	–	–	–	–
	24	5(1)	$\mathbb{Q}(\zeta_{35})$	–	–	–	1	–	–	–	–	–
			$\mathbb{Q}(\zeta_{45})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{56})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{72})$	–	–	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{84})$	–	1	–	–	–	–	–	–	–
	32	10(−)	$\mathbb{Q}(\zeta_{80})$	–	1	–	1	–	–	–	–	–
			$\mathbb{Q}(\zeta_{96})$	–	1	–	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{120})$	–	–	2	5	–	–	–	–	–
	36	8(−)	$\mathbb{Q}(\zeta_{63})$	–	1	–	7	–	–	–	–	–
6	8	1(1)	$\mathbb{Q}(\zeta_{24})$	–	1	–	–	–	–	–	–	–
	12	1(1)	$\mathbb{Q}(\zeta_{28})$	–	1	–	–	–	–	–	–	–
	16	2(1)	$\mathbb{Q}(\zeta_{40})$	–	–	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{48})$	–	1	–	–	–	–	–	–	–
	20	1(1)	$\mathbb{Q}(\zeta_{33})$	–	–	1	–	–	–	–	–	–
	24	5(2)	$\mathbb{Q}(\zeta_{56})$	–	1	–	1	–	–	–	–	–
			$\mathbb{Q}(\zeta_{72})$	–	1	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{84})$	–	–	–	1	–	–	–	–	–

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
6	32	12(−)	$\mathbb{Q}(\zeta_{80})$	−	−	1	5	−	−	−	−	−
			$\mathbb{Q}(\zeta_{96})$	−	1	−	1	−	−	−	−	−
			$\mathbb{Q}(\zeta_{120})$	−	−	−	4	−	−	−	−	−
7	6	1(1)	$\mathbb{Q}(\zeta_{7})$	−	1	−	−	−	−	−	−	−
	8	1(1)	$\mathbb{Q}(\zeta_{24})$	−	1	−	−	−	−	−	−	−
	12	1(−)	$\mathbb{Q}(\zeta_{28})$	−	1	−	−	−	−	−	−	−
	16	4(3)	$\mathbb{Q}(\zeta_{40})$	−	−	1	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{48})$	−	1	1	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{60})$	−	−	1	−	−	−	−	−	−
	20	1(−)	$\mathbb{Q}(\zeta_{44})$	−	−	1	−	−	−	−	−	−
	24	8(−)	$\mathbb{Q}(\zeta_{56})$	−	1	2	2	−	−	−	−	−
			$\mathbb{Q}(\zeta_{72})$	−	1	1	−	−	−	−	−	−
	32	19(−)	$\mathbb{Q}(\zeta_{80})$	−	−	1	1	2	−	−	−	−
			$\mathbb{Q}(\zeta_{96})$	−	1	2	3	−	−	−	−	−
			$\mathbb{Q}(\zeta_{120})$	−	−	2	7	−	−	−	−	−
11	4	1(1)	$\mathbb{Q}(\zeta_{12})$	−	1	−	−	−	−	−	−	−
	8	2(1)	$\mathbb{Q}(\zeta_{15})$	−	−	1	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{24})$	−	1	−	−	−	−	−	−	−
	10	1(1)	$\mathbb{Q}(\zeta_{11})$	−	−	1	−	−	−	−	−	−
	12	1(−)	$\mathbb{Q}(\zeta_{36})$	−	1	−	−	−	−	−	−	−
	16	5(−)	$\mathbb{Q}(\zeta_{40})$	−	−	1	1	−	−	−	−	−
			$\mathbb{Q}(\zeta_{48})$	−	1	−	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{60})$	−	−	−	2	−	−	−	−	−
	20	2(−)	$\mathbb{Q}(\zeta_{33})$	−	−	−	1	−	−	−	−	−
			$\mathbb{Q}(\zeta_{44})$	−	−	1	−	−	−	−	−	−

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
11	24	7(−)	$\mathbb{Q}(\zeta_{35})$	−	−	−	1	−	1	−	−	−
			$\mathbb{Q}(\zeta_{45})$	−	−	1	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{56})$	−	−	−	1	−	−	−	−	−
			$\mathbb{Q}(\zeta_{72})$	−	1	−	1	−	−	−	−	−
			$\mathbb{Q}(\zeta_{84})$	−	−	1	−	−	−	−	−	−
	32	42(−)	$\mathbb{Q}(\zeta_{80})$	−	−	1	1	1	1	−	−	−
			$\mathbb{Q}(\zeta_{96})$	−	1	−	−	1	−	−	−	−
			$\mathbb{Q}(\zeta_{120})$	−	−	1	13	18	4	−	−	−
	36	2(−)	$\mathbb{Q}(\zeta_{108})$	−	1	−	−	1	−	−	−	−
14	4	1(1)	$\mathbb{Q}(\zeta_{8})$	−	1	−	−	−	−	−	−	−
	8	2(1)	$\mathbb{Q}(\zeta_{16})$	−	1	−	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{24})$	−	−	1	−	−	−	−	−	−
	12	1(1)	$\mathbb{Q}(\zeta_{28})$	−	−	−	1	−	−	−	−	−
	16	5(−)	$\mathbb{Q}(\zeta_{32})$	−	1	−	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{40})$	−	−	1	−	−	−	−	−	−
			$\mathbb{Q}(\zeta_{48})$	−	−	1	1	−	−	−	−	−
			$\mathbb{Q}(\zeta_{60})$	−	−	1	−	−	−	−	−	−
	24	8(−)	$\mathbb{Q}(\zeta_{56})$	−	−	−	4	−	2	−	−	−
			$\mathbb{Q}(\zeta_{72})$	−	−	1	1	−	−	−	−	−
	32	21(−)	$\mathbb{Q}(\zeta_{64})$	−	1	−	−	2	−	−	−	−
			$\mathbb{Q}(\zeta_{80})$	−	−	−	−	−	2	1	−	−
			$\mathbb{Q}(\zeta_{96})$	−	−	1	1	2	2	−	−	−
			$\mathbb{Q}(\zeta_{120})$	−	−	−	4	−	5	−	−	−
	36	36(−)	$\mathbb{Q}(\zeta_{57})$	−	−	−	−	3	25	8	−	−

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
15	8	1(1)	$\mathbb{Q}(\zeta_{24})$	–	–	1	–	–	–	–	–	–
	16	3(1)	$\mathbb{Q}(\zeta_{40})$	–	–	–	–	1	–	–	–	–
			$\mathbb{Q}(\zeta_{48})$	–	–	1	–	–	–	–	–	–
			$\mathbb{Q}(\zeta_{60})$	–	–	–	1	–	–	–	–	–
	24	5(−)	$\mathbb{Q}(\zeta_{56})$	–	–	–	1	–	–	–	–	–
			$\mathbb{Q}(\zeta_{72})$	–	–	1	–	–	1	–	–	–
			$\mathbb{Q}(\zeta_{84})$	–	–	–	–	–	2	–	–	–
	32	23(−)	$\mathbb{Q}(\zeta_{80})$	–	–	–	–	2	3	1	–	–
			$\mathbb{Q}(\zeta_{96})$	–	–	1	–	1	–	–	–	–
			$\mathbb{Q}(\zeta_{120})$	–	–	–	4	1	9	1	–	–
	36	4(−)	$\mathbb{Q}(\zeta_{76})$	–	–	–	–	2	1	–	1	–
23	4	1(1)	$\mathbb{Q}(\zeta_{12})$	–	–	1	–	–	–	–	–	–
	8	3(−)	$\mathbb{Q}(\zeta_{24})$	–	–	1	2	–	–	–	–	–
	12	1(−)	$\mathbb{Q}(\zeta_{36})$	–	–	1	–	–	–	–	–	–
	16	5(−)	$\mathbb{Q}(\zeta_{40})$	–	–	–	–	1	–	–	–	–
			$\mathbb{Q}(\zeta_{48})$	–	–	1	2	–	–	–	–	–
			$\mathbb{Q}(\zeta_{60})$	–	–	–	–	–	1	–	–	–
	22	2(−)	$\mathbb{Q}(\zeta_{23})$	–	–	–	–	–	2	–	–	–

ℓ	Dim	Gesamtzahl(extremal)	K	Minimum								
				2	4	6	8	10	12	14	16	18
23	24	14(−)	$\mathbb{Q}(\zeta_{39})$	−	−	−	−	1	1	−	1	−
			$\mathbb{Q}(\zeta_{52})$	−	−	−	−	1	2	−	−	−
			$\mathbb{Q}(\zeta_{56})$	−	−	−	−	−	−	−	1	−
			$\mathbb{Q}(\zeta_{72})$	−	−	1	2	1	2	−	−	−
			$\mathbb{Q}(\zeta_{84})$	−	−	−	−	−	1	−	−	−
	32	20(−)	$\mathbb{Q}(\zeta_{80})$	−	−	−	−	1	−	1	1	1
			$\mathbb{Q}(\zeta_{96})$	−	−	1	2	−	−	2	2	−
			$\mathbb{Q}(\zeta_{120})$	−	−	−	−	1	3	1	4	−
	36	2(−)	$\mathbb{Q}(\zeta_{108})$	−	−	1	−	−	−	1	−	−

Tabelle 5.1: Anzahlen der Ideal-Gitter der Stufen $\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$ und Determinante $\ell^{\frac{n}{2}}$ mit Dimensionen ≤ 36 nach zugehörigem Kreisteilungskörper K und Minimum.

6 Literaturverzeichnis

[BFS05] Eva Bayer Fluckiger and Ivan Suarez. Modular lattices over cyclotomic fields. *Journal of Number Theory*, 114:394–411, 2005.

[CE03] Henry Cohn and Noam Elkies. New upper bounds on sphere packings I. *Annals of Mathematics*, 157:689–714, 2003.

[CS93] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der mathematischen Wissenschaften*. Springer, 3rd edition, 1993.

[Jü15] Michael Jürgens. *Nicht-Existenz und Konstruktion extremaler Gitter*. PhD thesis, Technische Universität Dortmund, März 2015.

[Kne02] M. Kneser. *Quadratische Formen*. Springer, 2002.

[Mol11] Richard A. Mollin. *Algebraic number theory*. CRC Press, 2nd edition, 2011.

[Neb13] Gabriele Nebe. On automorphisms of extremal even unimodular lattices. *International Journal of Number Theory*, 09:1933–1959, 2013.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[NS] Gabriele Nebe and N. J. A. Sloane. A Catalogue of Lattices. `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/`. Aufgerufen: 10.08.2018.

[Que95] H. G. Quebbemann. Modular Lattices in Euclidean Spaces. *Journal of Number Theory*, 54:190–202, 1995.