Lokale Eigenschaften von Gittern mit einem Automorphismus

Dissertation
zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften (Dr. rer. nat.)

Der Fakultät für Mathematik
der Technischen Universität Dortmund
vorgelegt von

Stefan Höppner
im Januar 2016

Dissertation
Lokale Eigenschaften von Gittern mit einem Automorphismus

Fakultät für Mathematik
Technische Universität Dortmund

Erstgutachter:	Prof. Dr. Rudolf Scharlau
Zweitgutachter:	Prof. Dr. Detlev Hoffmann

Tag der mündlichen Prüfung: 30. März 2016

Inhaltsverzeichnis

Einleitung

Gitter werden seit dem 18. Jahrhundert erforscht. Mit ihrer Hilfe gelang die Lösung wichtiger Probleme aus der Zahlentheorie. Beispiele hierfür sind der Vier-Quadrate-Satz, der 1770 von Lagrange bewiesen wurde, und ein Beweis des quadratischen Reziprozitätsgesetzes, der im frühen 19. Jahrhundert von Gauß veröffentlicht wurde. Seit dieser Zeit traten Gitter in verschiedenen Teilgebieten der Mathematik auf, aber ihr wesentliches Anwendungsgebiet blieb die Zahlentheorie. Seit ungefähr 20 bis 30 Jahren ist das Interesse an Gittern durch die Informationstechnik jedoch angestiegen und sie werden auch in praktischen Anwendungen immer wichtiger. Zum Beispiel findet man auf Gitter basierende fehlerkorrigierende Codes heutzutage in vielen elektronischen Geräten. Ein weiteres aktuelles Anwendungsgebiet, in dem Gitter zunehmend wichtig werden, ist die Kryptographie. Derzeit sind Kryptosysteme wie RSA oder Diffie-Hellman sehr populär, welche auf der Zerlegung von ganzen Zahlen und dem diskreten-Logarithmen-Problem basieren. Falls die Entwicklung von Quantencomputern weiter voranschreitet, werden diese Probleme mit Hilfe von Shors Algorithmus in Zukunft leicht lösbar sein, während die auf Gittern basierenden Kryptosysteme nach derzeitigem Stand auch nicht durch Quantencomputer angegriffen werden können.

Sei (L, b) ein $\mathbb{Z}$-Gitter mit nicht ausgearteter, symmetrischer Bilinearform b. Das Geschlecht $\mathrm{Gen}_{\mathbb{Z}}(L, b)$ besteht aus allen Gittern (M, b), deren Lokalisierungen $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ an allen Stellen $p \in \mathbb{P}(\mathbb{Q})$ isometrisch zu den Lokalisierungen von (L, b) sind. Es kann mit steigendem Rang sehr groß werden und interessante Gitter enthalten. Eine Methode, mit deren Hilfe Geschlechter positiv definiter Gitter klassifiziert werden können, ist die Knesersche Nachbarmethode. Sehr große Geschlechter sind damit in angemessener Zeit aber nicht klassifizierbar. Zum Beispiel kann das Geschlecht der geraden, unimodularen Gitter mit Rang 24 mit der Nachbarschaftsmethode klassifiziert werden (vgl. [Kne02] Seite 116). Das Geschlecht der geraden, unimodularen Gitter mit Rang 32 enthält bereits mehr als eine Milliarde Isometrieklassen (vgl. [Kin03] Seite 853) und ist deswegen nicht mehr in angemessener Zeit klassifizierbar. Alle anderen Methoden konstruieren gezielt ein Gitter mit den gewünschten Eigenschaften. Anhand bekannter Resultate zeigt sich, dass die so konstruierten Gitter Automorphismen mit bestimmten Ordnungen besitzen. Dies ist häufig konstruktionsbedingt, wie man exemplarisch anhand der auch in dieser Arbeit thematisierten Idealgitterkonstruktion von Eva Bayer-Fluckiger (vgl. [BF02]) sieht. Zum Beispiel besitzt das Leech-Gitter eine Struktur von Rang 1 über den Ganzheitsringen des 35., 39., 52., 56. und 84. Kreisteilungskör-

pers. Das Coxeter-Todd-Gitter besitzt eine Struktur von Rang 1 über den Ganzheitsringen des 21., 28. und 42. Kreisteilungskörpers. Damit besitzen diese Gitter auch fixpunktfreie Automorphismen der jeweiligen Ordnungen. In einigen Fällen können auch Automorphismen mit kleinerer Ordnung bei der Konstruktion hilfreich sein. Ein Beispiel hierfür ist das neue extremale, gerade, unimodulare Gitter mit Rang 48, das Gabriele Nebe 2014 mit Hilfe eines Automorphismus der Ordnung 5 gefunden hat (vgl. [Neb14]).

Das Ziel dieser Arbeit ist es, Gitter mit einem Automorphismus zu untersuchen und Kriterien zu finden, mit deren Hilfe man diese Gitter in einem Geschlecht grundsätzlich ausschließen kann. Damit kann ein Erfolg vieler Konstruktionmethoden von vornherein ausgeschlossen werden.

Sei G die zyklische Gruppe, die von einem Gitterautomorphismus der Ordnung m erzeugt wird. Ein Gitter mit einem Automorphismus der Ordnung m besitzt auf kanonische Weise eine hermitesche $\mathbb{Z}G$-Modulstruktur. Umgekehrt kann mit Hilfe der Spur aus einem hermiteschen $\mathbb{Z}G$-Gitter ein $\mathbb{Z}$-Gitter mit einem Automorphismus der Ordnung m konstruiert werden. Das erste Kapitel beginnt daher mit einer Einführung von hermiteschen Gittern über Gruppenringen und dem Zusammenhang zu quadratischen $\mathbb{Z}$-Gittern mit einem Automorphismus. Dabei reicht es die Gruppenringe $\mathbb{Z}G$ und $\mathbb{Z}_pG$ für $p \in \mathbb{P}(\mathbb{Q})$ zu betrachten. Sie sind Ordnungen in den Gruppenalgebren $\mathbb{Q}G$ und $\mathbb{Q}_pG$. Diese Algebren besitzen die maximalen Ordnungen $\bigoplus_{d|m} \mathbb{Z}[\zeta_d]$ und $\bigoplus_{d|m} \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d] \cong \bigoplus_{d|m} \bigoplus_{(\pi)|p\mathbb{Z}[\zeta_d]} \mathbb{Z}[\zeta_d]_\pi$, wobei ζ_d die d-te Einheitswurzel ist. Falls die Gruppenordnung m eine Einheit im Gruppenring $\mathbb{Z}_pG$ ist, dann ist $\mathbb{Z}_pG$ bereits die Maximalordnung. Ihre Zerlegung impliziert eine Zerlegung eines hermiteschen $\mathbb{Z}_pG$-Gitters in hermitesche $\mathbb{Z}[\zeta_d]_\pi$-Gitter, die im Wesentlichen sogar orthogonal ist. Falls die Gruppenordnung m keine Einheit ist, dann kann der Gruppenring in die Maximalordnung eingebettet werden. Diese Einbettung wird für $m = p \in \mathbb{P}(\mathbb{Q})$ ganz konkret angegeben: In diesem Fall ist das $\mathbb{Z}_pG$-Gitter ein Teilgitter von $\Gamma \otimes_{\mathbb{Z}_pG} L$, welches wiederum eine orthogonale Zerlegung in ein $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter L^ζ und ein $\mathbb{Z}_p$-Gitter L^1 besitzt.
Der zweite Abschnitt beginnt mit der lokalen Theorie hermitescher Gitter. Von zentraler Bedeutung sind dabei Arbeiten von Ronald Jacobowitz aus dem Jahr 1962 und von Larry Gerstein aus dem Jahr 1970. Jacobowitz hat in [Jac62] Gitter über einem lokalen Körper K mit einer Involution untersucht. Gerstein hat in [Ger70] basierend auf einer Arbeit von Goro Shimura [Shi64] Gitter über $K \times K$ für einen lokalen Körper K untersucht. Diese Ergebnisse werden für $K = \mathbb{Q}[\zeta_m]_\pi$ beziehungsweise $K \times K \cong \mathbb{Q}[\zeta_m]_\pi \times \mathbb{Q}[\zeta_m]_{\overline{\pi}}$ verwendet, um eine besondere p-modulare Zerlegung von $\mathbb{Z}$-Gittern mit einem Automorphismus zu finden. Eine p-modulare Zerlegung wird üblicherweise wie folgt definiert:

Proposition 1.24. *Sei p eine Primzahl und L ein $\mathbb{Z}_p$-Gitter.*

(a) Dann gibt es (p^i)-modulare Teilgitter $L_i \subseteq L$, sodass:

$$L = \bigsqcup_{i \in \mathbb{Z}} L_i$$

Es können nur endlich viele $L_i \neq \{0\}$ sein. Eine solche Zerlegung heißt ***p-modulare Zerlegung*** *von L.*

(b) Falls $L \cong \bigsqcup_{i\in\mathbb{Z}} L_i \cong \bigsqcup_{i\in\mathbb{Z}} L'_i$ zwei p-modulare Zerlegungen sind, gilt:

(i) $\operatorname{rang}_{\mathbb{Z}_p}(L_i) = \operatorname{rang}_{\mathbb{Z}_p}(L'_i)$ für alle i.
Insbesondere ist $|\{i \in \mathbb{Z} \mid L_i \neq \{0\}\}| = |\{i \in \mathbb{Z} \mid L'_i \neq \{0\}\}|$

(ii) Falls $p \neq 2$ ist, gilt $L_i \cong L'_i$ für alle $i \in \mathbb{Z}$

Das zentrale Resultat des zweiten Abschnitts ist die Konstruktion von p-modularen Zerlegungen für Gitter mit einem Automorphismus g der Ordnung m mit $p \nmid m$, für die zusätzlich $g(L_i) = L_i$ für alle i gilt. Diese Zerlegung ist für $p \neq 2$ bis auf Isometrie eindeutig. Sei $f^+(p)$ der Trägheitsindex des Ideals (p) in der Erweiterung $\mathbb{Q}[\zeta_m+\overline{\zeta_m}]/\mathbb{Q}$. Als eine Folgerung aus der Konstruktion dieser Zerlegung erhält man die Bedingung, dass die Ränge der p-modularen Komponenten für $p \nmid m$ ein Vielfaches von $2f^+(p)$ sind.
Im dritten Abschnitt wird der Fall $p|m$ genauer untersucht. Eine invariante, p-modulare Zerlegung gibt es im Allgemeinen nicht, was man am Beispiel des Gitters A_{p-1} sieht. Mit Hilfe eines modifizierten Modularitätbegriffs (vgl. Definition 1.49) kann aber auch für diesen Fall eine orthogonale Zerlegung in orthogonal unzerlegbare $\mathbb{Z}_pG$-Gitter konstruiert werden:

Satz 1.52. *Sei p eine ungerade Primzahl. Jeder hermitesche $\mathbb{Z}_pG$-Modul (L, h) kann als orthogonale Summe von (i, j, k)-modularen Teilmoduln mit den folgenden Modulstrukturen geschrieben werden: $\mathbb{Z}_p$, $\mathbb{Z}_p[\zeta_p]$, $\mathbb{Z}_pG$, $\mathbb{Z}_pG \oplus \mathbb{Z}_p$, $\mathbb{Z}_p[\zeta_p] \oplus \mathbb{Z}_p[\zeta_p]$, $\mathbb{Z}_pG \oplus \mathbb{Z}_p[\zeta_p]$, $\mathbb{Z}_pG \oplus \mathbb{Z}_pG$, $\mathbb{Z}_pG \oplus \mathbb{Z}_p[\zeta_p] \oplus \mathbb{Z}_p$, $\mathbb{Z}_pG \oplus \mathbb{Z}_pG \oplus \mathbb{Z}_p$ und $\mathbb{Z}_pG \oplus \mathbb{Z}_pG \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Der Beweis verwendet Resultate von Irving Reiner, der die unzerlegbaren $\mathbb{Z}_pG$-Moduln ohne eine hermitesche Form für $|G| = p$ bestimmt hat und zeigen konnte, dass für $\mathbb{Z}_pG$-Moduln ein Krull-Schmidt-Theorem gilt. Des Weiteren wird am Ende des ersten Kapitels gezeigt, dass es für die Fälle $p = 2$ und $p^2|m$ unendlich viele orthogonal unzerlegbare Summanden von beliebig großem Rang gibt und es wird der Spezialfall der unimodularen $\mathbb{Z}_pG$-Gitter genauer untersucht.

In den ersten beiden Abschnitten des zweiten Kapitels werden $\mathbb{Z}$-Gitter mit einem Automorphismus betrachtet, dessen Minimalpolynom das m-te Kreisteilungspolynom ist. In diesem Spezialfall vereinfacht sich die Struktur über dem Gruppenring zu einer Struktur über $\mathbb{Z}[\zeta_m]$ und die Spur des Gruppenrings vereinfacht sich zur gewöhnlichen Spur für Galoiserweiterungen. Im ersten Abschnitt werden einige notwendige Bedingungen für die Existenz von diesen Gittern in einem Geschlecht formuliert. Mit Hilfe der Resultate von Ronald Jacobowitz und Larry Gerstein kann ein Zwischenergebnis aus dem ersten Kapitel verbessert werden: Es wird gezeigt, dass die Ränge der p-modularen Komponenten für $m \neq p^t$ ein Vielfaches von $2f^+(p)$ sind. Des Weiteren sind für $m \neq 2^t$ alle Komponenten der 2-modularen Zerlegung gerade. Für $m = 2^t$ wird genau untersucht, welche hermiteschen Strukturen über die Spurkonstruktion gerade $\mathbb{Z}$-Gitter und welche Strukturen ungerade $\mathbb{Z}$-Gitter liefern.

Der zweite Abschnitt beschäftigt sich mit der Bestimmung der Quadratklasse der Determinanten von den reskalierten, modularen Komponenten von Gittern mit einem Automorphismus. Ihr kann mit Hilfe des Kroneckersymbols $\left(\frac{\det}{p}\right)$ ein Wert aus $\{\pm 1\}$ zugeordnet werden. Dieser Wert wird auch das Vorzeichen der modularen Komponente genannt. Der unterliegende hermitesche $\mathbb{Q}[\zeta_m]$-Vektorraum ist durch die Dimension, die Determinante und die Signatur bis auf Isometrie eindeutig festgelegt. Durch die Spurkonstruktion sind die Dimension, die Determinante und die Signatur des $\mathbb{Q}$-Vektorraums ebenfalls festgelegt. Mit diesen Invarianten gibt es im Wesentlichen zwei quadratische Räume, die durch die Hasse-Invariante unterschieden werden. Also kann nur ein quadratischer Raum die hermitesche Struktur besitzen und es ergeben sich weitere Einschränkungen für die Vorzeichen der modularen Komponenten. Gabriele Nebe hat in ihrer Habilitation [Neb99] in Kapitel 3.3.2 die Invarianten dieser Räume bestimmt. Die dort verwendeten Methoden werden in dieser Arbeit modifiziert, um damit die Vorzeichen zu bestimmen. Der folgende Satz fasst die zentralen Resultate des zweiten Abschnitts zusammen:

Satz 2.39. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Dann besitzt die i-te, p-modulare Komponente L_i eines quadratischen $\mathbb{Z}$-Gitters (L, b) mit einem Automorphismus mit Minimalpolynom Φ_m das Vorzeichen*

$$\epsilon_{p,i} = \begin{cases} (-1)^{\frac{\operatorname{rang}(L_i)}{f(p)}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{\operatorname{rang}(L_i)}{2}} & \text{falls } p \neq 2 \\ (-1)^{\frac{\operatorname{rang}(L_i)}{f(p)}} & \text{falls } p = 2 \end{cases}$$

In dem noch fehlenden Fall, in dem Einschränkungen für p-modulare Zerlegungen für $m = p^t$ gefunden werden sollen, muss man sich darauf beschränken, dass das Gitter als $\mathbb{Z}_p$-Gitter quadratfrei ist oder als hermitesches Gitter den Rang 1 besitzt. Für ungerade Gitter werden damit abschließend Einschränkungen für die sogenannte Oddity einer ungeraden, modularen Komponente bestimmt. Im dritten Abschnitt wird gezeigt, wie man die Ergebnisse der ersten beiden Abschnitte verwenden kann, um in einem beliebigen $\mathbb{Z}$-Geschlecht Gitter mit gewissen Automorphismentypen auszuschließen, ohne das ganze Geschlecht zu klassifizieren. Im letzten Abschnitt werden Gitter mit einem Automorphismus konstruiert, die in einem vorgegebenen Geschlecht liegen. Eva Bayer-Fluckiger hat in [BF02] bereits notwendige und hinreichende Bedingungen formuliert, unter denen $\mathbb{Z}$-Gitter mit einer zusätzlichen hermiteschen Struktur über einem Zahlkörper von Rang 1 existieren. Sie stellt dabei unter anderem eine Bedingung an die Determinante, die die Norm von Idealen sein muss. Durch eine geschickte Wahl der Ideale wird in der vorliegenden Arbeit gezeigt, dass sogar ein Gitter mit einem Automorphismus in einem vorgegebenen Geschlecht konstruiert werden kann:

Satz 2.57. *Seien $n_{p,i}, m, n_+, n_- \in \mathbb{N}$ mit $\varphi(m) = n_+ + n_-$ so gewählt, dass sie die entsprechenden Einträge eines möglichen Geschlechtssymbols sind. In diesem Geschlecht gibt es genau dann ein ganzzahliges $\mathbb{Z}$-Gitter mit einem Automorphismus, der das Minimalpolynom Φ_m besitzt, wenn die folgenden Bedingungen erfüllt sind:*

(i) $n_+ \equiv_2 0$ *und* $n_- \equiv_2 0$

(ii) Falls $m = q^t$ eine Primzahlpotenz ist, gilt für die Ränge der modularen Komponenten:

$$\begin{cases} 2f^+(p)|n_{p,i} & \text{für } p = q = 2 \text{ und für alle } p \in \mathbb{P}(\mathbb{Q}) \setminus \{q, \infty\} \\ n_{p,i} \equiv_2 1 & \text{für } p = q \neq 2 \end{cases}$$

Falls $m \neq q^t$ ist, muss $2f^+(p)|n_{p,i}$ für alle $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ gelten. Zusätzlich muss für alle p mit $p|m$ die Kettenbedingung (vgl. Definition 2.55) erfüllt sein.

(iii) Falls $m \neq q^t$ ist, so gilt mit $a(p) := p^{\nu_p(m)-1}(p\nu_p(m) - \nu_p(m) - 1) + \sum_{i\in\mathbb{Z}} i \cdot \frac{n_{p,i}}{f(p)}$ die Beziehung:

$$4 \cdot \sum_{p\in\mathbb{P}(\mathbb{Q})\setminus\{\infty\}} a(p) \equiv_8 n_+ - n_-$$

Im verbleibenden Teil des Abschnitts wird beschrieben, wie $\mathbb{Z}$-Gitter mit einem Automorphismus und einem größeren Rang konstruiert werden können. Falls m keine Primzahlpotenz ist, kann man solche Gitter leicht aus Gittern mit kleinerem Rang konstruieren. Falls m eine Primzahlpotenz ist, enthalten diese Gitter eine p-Potenz in der Determinante. Deshalb müssen unter Umständen Obergitter gebildet werden. Der Nachweis ihrer Existenz ist im Allgemeinen ein sehr schwieriges Problem, weshalb abschließend einige Spezialfälle betrachtet werden, über die Aussagen getroffen werden können.

Ich möchte mich an dieser Stelle bei Prof. Dr. Rudolf Scharlau für die interessante Themenstellung und die Betreuung dieses Projektes bedanken. Ebenso geht mein Dank an meine Kollegen, die mir in den vergangenen Jahren stets mit Rat und Tat zur Seite standen. Ein besonderer Dank geht an Michael Jürgens für die vielen Diskussionen und bereichernden Tipps.

Kapitel 1

Eine orthogonale Zerlegung von $\mathbb{Z}_pG$-Gittern

Dieses Kapitel beginnt mit einer kurzen Einführung in die Theorie der hermiteschen Gitter über Gruppenringen. Es wird gezeigt, wie $\mathbb{Z}$-Gitter mit einem Automorphismus und hermitesche Gitter über dem Gruppenring zusammenhängen. Des Weiteren wird eine Zerlegung in Teilgitter über Ganzheitsringe von Kreisteilungskörpern konstruiert und es wird gezeigt, unter welchen Bedingungen diese Zerlegung sogar eine Zerlegung des Gitters liefert. Im zweiten Teil wird eine p-modulare Zerlegung von $\mathbb{Z}$-Gittern mit einem Automorphismus g konstruiert, bei der jede Komponente g-invariant ist. Dies ist an allen Primstellen möglich, die nicht die Gruppenordnung teilen. Am Ende des Kapitels wird für $|G| = p$ eine orthogonale Zerlegung eines $\mathbb{Z}_pG$-Gitters in möglichst kleine Teilgitter konstruiert.

1.1 Hermitesche Gitter über Gruppenringen

Definition 1.1. Ein quadratisches $\mathbb{Z}$-Gitter ist ein Paar (L, b), bestehend aus einem endlich erzeugten, torsionsfreien $\mathbb{Z}$-Modul und einer nicht ausgearteten, symmetrischen Bilinearform b. Da $\mathbb{Z}$ ein Hauptidealring ist, ist jedes $\mathbb{Z}$-Gitter frei und man kann stets eine Basis $\{v_1, \dots, v_n\}$ des Gitters wählen. Der Vektorraum $V := \mathbb{Q} \otimes_{\mathbb{Z}} L$ liegt L zugrunde. Die Skalarerweiterung $\mathbb{Q}_p \otimes_{\mathbb{Q}} V$ heißt die **Lokalisierung** von V an der Stelle p. Die Menge $\{1 \otimes v_1, \dots, 1 \otimes v_n\}$ bildet dann eine Basis von $\mathbb{Q}_p \otimes_{\mathbb{Q}} V$. Im Folgenden werden die Elemente $1 \otimes v_i$ wieder mit v_i identifiziert. Der von $\{v_1, \dots, v_n\}$ in $\mathbb{Q}_p \otimes_{\mathbb{Q}} V$ aufgespannte $\mathbb{Z}_p$-Modul heißt **Lokalisierung eines Gitters** L an der Stelle p. Die Bilinearform $b : V \times V \to \mathbb{Q}$ kann eindeutig zu einer Bilinearform $b_p : (\mathbb{Q}_p \otimes_{\mathbb{Q}} V) \times (\mathbb{Q}_p \otimes_{\mathbb{Q}} V) \to \mathbb{Q}_p \otimes_{\mathbb{Q}} V$ geliftet werden. Falls Verwechslungen ausgeschlossen sind, wird die geliftete Form wieder mit b bezeichnet. Die Menge der archimedischen und nicht-archimedischen Stellen sei $\mathbb{P}$. Es wird grundsätzlich angenommen, dass alle Gitter **voll** sind, das heißt, sie enthalten eine Vektorraumbasis.

Mit Hilfe der Lokalisierung definiert man das $\mathbb{Z}$-Geschlecht eines Gitters:

Definition 1.2. Zwei $\mathbb{Z}$-Gitter $(L,b) \subseteq (V,b)$ und $(L',b') \subseteq (V',b')$ heißen **verwandt**, falls es für alle $p \in \mathbb{P}(\mathbb{Q})$ eine Isometrie $\phi_p : (\mathbb{Z}_p \otimes_{\mathbb{Z}} L, b) \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} L', b')$ gibt. Das **Geschlecht** von (L,b) ist

$$\mathrm{Gen}_{\mathbb{Z}}(L,b) := \{(L',b') \subseteq (V',b') \mid (L',b') \text{ ist verwandt zu } (L,b)\}$$

Alle $\mathbb{Q}$-Vektorräume, die den Gittern eines $\mathbb{Z}$-Geschlechts zugrunde liegen, sind nach dem Lokal-Global-Prinzip von Minkowski und Hasse isometrisch. Da dieses Prinzip nicht für Gitter gilt, müssen die Gitter in einem Geschlecht nicht notwendig isometrisch sein und ein Geschlecht zerfällt in endlich viele Isometrieklassen. Sei R ein Ring mit einer Involution. Ein hermitesches Gitter (L,h) ist ein endlich erzeugter, torsionsfreier R-Modul L mit einer hermiteschen Form h. Das bedeutet, dass h in der ersten Komponente linear und in der zweiten Komponente semilinear ist. Sei nun ein $\mathbb{Z}$-Gitter (L,b) mit einem Automorphismus g der Ordnung m fixiert. Es sei $G := \langle g \rangle$. Damit wird ein $\mathbb{Z}$-Gitter (L,b) vermöge $g.x := g(x)$ zu einem Modul über dem Gruppenring $\mathbb{Z}G$, der durch die Abbildung $g \mapsto g^{-1}$ eine Involution erhält. Die Bilinearform b kann zu einer nicht ausgearteten Form h geliftet werden:

$$\begin{array}{rcl} h : L \times L & \longrightarrow & \mathbb{Z}G \\ (v,w) & \mapsto & \displaystyle\sum_{i=0}^{m-1} b(g^{-i}(v),w)g^i \end{array}$$

Damit ist (L,h) ein hermitesches $\mathbb{Z}G$-Gitter. Umgekehrt kann aus jedem hermiteschen $\mathbb{Z}G$-Gitter wieder ein $\mathbb{Z}$-Gitter mit einem Automorphismus g konstruiert werden. Mit Hilfe der Spur

$$\begin{array}{rcl} \mathrm{t} : \quad \mathbb{Z}G & \longrightarrow & \mathbb{Z} \\ \displaystyle\sum_{i=0}^{m-1} a_i g^i & \mapsto & ma_0 \end{array}$$

erhält man eine symmetrische Bilinearform $\frac{1}{m}\,\mathrm{t} \circ h$ auf L als $\mathbb{Z}$-Gitter. Es enthält einen Automorphismus der Ordnung m.

Bemerkung 1.3. Diese Konstruktion liefert eine Äquivalenz von der Kategorie der hermiteschen $\mathbb{Z}G$-Gitter und der Kategorie der quadratischen $\mathbb{Z}$-Gitter mit einem Automorphismus. Diese bekannte Aussage findet man mit weiteren Details und der Konstruktion des Funktors zum Beispiel in [FM69]. Alternativ funktioniert der Beweis in der Ausarbeitung von Björn Hoffmann in [Hof12] auf Seite 15 für den Fall $19 \geq |G| \in \mathbb{P}(\mathbb{Q})$ auch allgemein für endliche zyklische Gruppen.

Weil die Ganzzahligkeit der hermiteschen Gitter für den weiteren Verlauf irrelevant ist, wird der Faktor $1/m$ in die hermitesche Form hineingezogen, sodass sie Werte in $\frac{1}{m}\mathbb{Z}G$ besitzt. Man kann nun auch Geschlechter von hermiteschen $\mathbb{Z}G$-Gittern definieren. Im Gegensatz zu $\mathbb{Z}$-Gittern liegt ihnen im Allgemeinen kein Vektorraum zugrunde, sondern ein Modul M über der Gruppenalgebra $\mathbb{Q}G$.

Definition 1.4. Zwei $\mathbb{Z}G$-Gitter $(L,h) \subseteq (M,h)$ und $(L',h') \subseteq (M',h')$ heißen **verwandt**, falls es für alle $p \in \mathbb{P}(\mathbb{Q})$ eine Isometrie $\phi_p : (\mathbb{Z}_p \otimes_{\mathbb{Z}} L, h_p) \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} L', h'_p)$ gibt. Das $\mathbb{Z}G$-**Geschlecht** von L ist

$$\mathrm{Gen}_{\mathbb{Z}G}(L,h) := \{(L',h') \subseteq (M',h') \mid (L',h') \text{ ist verwandt zu } (L,h)\}$$

Bemerkung 1.5.

(a) Eine $\mathbb{Z}_pG$-Isometrie $\phi_p : (\mathbb{Z}_p \otimes_{\mathbb{Z}} L, h_p) \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} L', h'_p)$ ist insbesondere eine $\mathbb{Z}_p$-Isometrie. Ein $\mathbb{Z}$-Geschlecht kann daher in verschiedene $\mathbb{Z}G$-Geschlechter zerfallen.

(b) Jedes $\mathbb{Z}$-Geschlecht enthält nach [Kne02] Satz 21.3. nur endlich viele Isometrieklassen. Konstruiert man aus einem $\mathbb{Z}$-Gitters mit zwei Automorphismen g, g' zwei $\mathbb{Z}G$-Gitter, so sind sie genau dann isometrisch, wenn g und g' konjugiert sind. Daher zerfällt die Isometrieklasse eines $\mathbb{Z}$-Geschlechts entsprechend der Anzahl der Konjugationsklassen seiner Automorphismengruppe in viele $\mathbb{Z}G$-Isometrieklassen.

Wegen der Äquivalenz der Kategorien erhält man durch die Untersuchung von $\mathbb{Z}$-Gittern mit einem Automorphismus gleichzeitig Informationen über Geschlechter von Gittern über dem Gruppenring. Umgekehrt werden im Laufe der Arbeit Aussagen über hermitesche $\mathbb{Z}G$-Gitter und insbesondere auch über hermitesche $\mathbb{Z}[\zeta_m]$-Gitter verwendet, um Aussagen über $\mathbb{Z}$-Gitter mit einem Automorphismus treffen zu können. Dies geschieht zum Beispiel mit Hilfe von Ordnungen:

Definition 1.6. Sei R ein Dedekindring mit Quotientenkörper K. Des Weiteren sei A eine endlich-dimensionale K-Algebra. Eine R-**Ordnung** ist ein Teilring $\Lambda \subseteq A$, der dasselbe Einselement wie A besitzt und ein endlich erzeugter R-Teilmodul von A ist, sodass $K \otimes_R \Lambda = A$ ist.

Beispiele für Ordnungen sind die Gruppenringe $\mathbb{Z}G$ und $\mathbb{Z}_pG$, die in der Gruppenalgebra $\mathbb{Q}G$ beziehungsweise $\mathbb{Q}_pG$ enthalten sind. Diese Algebren enthalten weitere Ordnungen, die bezüglich der Inklusion geordnet werden können. Die maximalen Ordnungen ergeben sich aus der Zerlegung der Gruppenalgebren:

Proposition 1.7. *Sei $p \in \mathbb{P}(\mathbb{Q})$. Es gilt*

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_m] \cong \prod_{(\pi)|(p)} \mathbb{Q}[\zeta_m]_\pi \quad \textit{sowie} \quad \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m] \cong \prod_{(\pi)|(p)} \mathbb{Z}[\zeta_m]_\pi$$

Einen Beweis der beiden Aussagen findet man in [Ser79] Kapitel II §3. Es ist von Vorteil, wenn man den ersten und zweiten Kreisteilungskörper mit $\mathbb{Q}$ identifiziert, denn viele Behauptungen sind dann auch für $m \in \{1,2\}$ richtig und es werden Fallunterscheidungen eingespart. Die Spur ist in diesen Fällen die Identität und die Involution operiert trivial.

Proposition 1.8. *Die maximalen Ordnungen* Γ *in* $A \in \{\mathbb{Q}G, \mathbb{Q}_pG\}$ *sind*

$$\begin{array}{ll} \bigoplus_{d|m} \mathbb{Z}[\zeta_d] & \text{falls } A = \mathbb{Q}G \\ \bigoplus_{d|m} \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d] \cong \bigoplus_{d|m} \bigoplus_{(\pi)|p\mathbb{Z}[\zeta_d]} \mathbb{Z}[\zeta_d]_\pi & \text{falls } A = \mathbb{Q}_pG \end{array}$$

Beweis. Φ_d das d-te Kreisteilungspolynom. Für die Gruppenalgebra gilt:

$$\begin{aligned} \mathbb{Q}G &\cong \mathbb{Q}[X] \Big/ (X^m - 1) \cong \bigoplus_{d|m} \mathbb{Q}[X] \Big/ (\Phi_d(X)) \cong \bigoplus_{d|m} \mathbb{Q}[\zeta_d] \\ \mathbb{Q}_pG &= \mathbb{Q}_p[X] \Big/ (X^m - 1) \cong \bigoplus_{d|m} \mathbb{Q}_p[X] \Big/ (\Phi_d(X)) \cong \bigoplus_{d|m} \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_d] \\ &\cong \bigoplus_{d|m} \bigoplus_{(\pi)|p\mathbb{Z}[\zeta_d]} \mathbb{Q}[\zeta_d]_\pi \end{aligned}$$

Unmittelbar aus dem Satz von Maschke folgt, dass die Gruppenalgebra in den betrachteten Fällen stets separabel ist, das heißt $L \otimes A$ ist für alle Körpererweiterungen $L/\mathbb{Q}$ bzw. $L/\mathbb{Q}_p$ halbeinfach. Nach [Rei75] Theorem 10.5. auf Seite 128 sind die zugehörigen Maximalordnungen dann die Maximalordnungen der einzelnen Summanden. Weil dies Körper sind, sind ihre Maximalordnungen die Ganzheitsringe. □

Betrachtet man die Lokalisierung an der unendlichen Stelle, so spielen die natürlichen Einbettungen $\sigma : \mathbb{Z}[\zeta_d] \hookrightarrow \mathbb{C}$ eine wichtige Rolle. Weil die Körpererweiterung $\mathbb{Q}[\zeta_d] : \mathbb{Q}$ für $d > 2$ rein imaginär ist, operiert die Konjugation auf den Einbettungen nicht trivial und sie können zu Paaren $(\sigma, \overline{\sigma})$ gruppiert werden. Der erste und zweite Kreisteilungskörper werden mit $\mathbb{Q}$ identifiziert. Daher sind ihre Einbettungen ρ, ρ' reell.

Proposition 1.9. *Sei* V_d *eine Menge, welche aus jedem Paar von Einbettungen* $\sigma, \overline{\sigma} : \mathbb{Z}[\zeta_d] \to \mathbb{C}$ *genau einen Vertreter enthält. Es gilt:*

$$\mathbb{R}G \cong \begin{cases} \mathbb{R}^2 \times \prod_{\substack{d|m \\ d>2}} \prod_{\sigma \in V_d} \mathbb{C} & \text{falls } 2 \mid m \\ \mathbb{R} \times \prod_{\substack{d|m \\ d>2}} \prod_{\sigma \in V_d} \mathbb{C} & \text{falls } 2 \nmid m \end{cases}$$

Beweis. Mit Hilfe des chinesischen Restsatzes folgt:

$$\mathbb{R}G \cong \mathbb{R}[X] \Big/ (X^m - 1) \cong \bigoplus_{d|m} \mathbb{R}[X] \Big/ (\Phi_d(X)) \cong \bigoplus_{d|m} \bigoplus_{(T(X))|(\Phi_d(X))} \mathbb{R}[X] \Big/ (T(X))$$

Weil die Körpererweiterung $\mathbb{Q}[\zeta_m]/\mathbb{Q}$ separabel ist, zerfallen die Kreisteilungspolynome in verschiedene Faktoren. Für $d \in \{1, 2\}$ ist der entsprechende Summand isomorph zu $\mathbb{R}$. Für $d \notin \{1, 2\}$ erhält man $\frac{\varphi(d)}{2}$ Kopien von $\mathbb{C}$. □

Proposition 1.10. *Sei* $\Lambda \in \{\mathbb{Z}G, \mathbb{Z}_pG\}$ *und* Γ *die maximale Ordnung. Es gilt*

$$\Lambda \subseteq \Gamma \subseteq m^{-1}\Lambda$$

Diese Aussage findet man in [Rei75] Theorem 41.1 auf Seite 379.

Korollar 1.11. *Falls die Gruppenordnung eine Einheit ist, ist der Gruppenring bereits die maximale Ordnung.*

Falls die Gruppenordnung keine Einheit ist, kann der Gruppenring in die Maximalordnung eingebettet werden. Dies wird später für Gruppen von Primzahlordnung benötigt. Daher sollen nun die Darstellungen dieser Gruppen betrachtet werden. Eine elementare Rechnung zeigt die folgende Proposition, welche die Einbettung des Gruppenrings mit einer Gruppe von Primzahlordnung in die Maximalordnung beschreibt:

Proposition 1.12. *Seien p eine Primzahl, $R \in \{\mathbb{Z}, \mathbb{Z}_p\}$ und G eine zyklische Gruppe mit $|G| = p$. Der Gruppenring RG kann mittels*

$$\begin{aligned} \iota : RG &\hookrightarrow R[\zeta_p] \times R \\ g &\mapsto (\zeta_p, 1) \end{aligned}$$

diagonal eingebettet werden und es gilt

$$(R[\zeta_p] \times R)/\iota(RG) \cong \mathbb{F}_p \cong \iota(RG)/((1-\zeta_p)R[\zeta_p] \times pR)$$

Man betrachte nun die Modulstruktur eines hermiteschen $\mathbb{Z}G$-Gitters. Für Gruppen von Primzahlordnung haben Diederichsen und Reiner diese Moduln bis auf Isomorphie klassifiziert und eine Zerlegung in Teilmoduln angegeben:

Theorem 1.13. *Es seien G eine Gruppe mit $|G| = p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und M ein $\mathbb{Z}G$-Modul. Dann gibt es eine Modulzerlegung*

$$M = M_g \oplus M_\zeta \oplus M_1 \oplus I \cdot v_I \text{ für ein } v_I \in M,$$

wobei M_g ein freier $\mathbb{Z}G$-Modul, M_ζ ein freier $\mathbb{Z}[\zeta_p]$-Modul, M_1 ein freier $\mathbb{Z}$-Modul und $I \subset \mathbb{Z}[\zeta_p]$ ein Ideal ist. Diese Zerlegung ist bis auf Isomorphie eindeutig, das heißt, zu einer weiteren Zerlegung

$$M = M'_g \oplus M'_\zeta \oplus M'_1 \oplus I' \cdot v'_I \text{ für ein } v'_I \in M$$

gibt es Isomorphismen $M'_g \cong M_g$, $M'_\zeta \cong M_\zeta$, $M'_1 \cong M_1$ und $I' \cong I$ als $\mathbb{Z}G$-Moduln.

Der Gruppenring über endliche abelsche Gruppen ist zwar kein Dedekindring, aber er weist viele Eigenschaften eines Dedekindrings auf und wird in der Literatur auch als "Dedekind-like" bezeichnet. Zum Beispiel kann das Ideal I als Vertreter der Steinitzklasse von M aufgefasst werden. Definiert man $n_1 := \dim(M_1)$, $n_\zeta := \dim(M_\zeta)$ und $n_g := \dim(M_g)$, so wird die Isomorphieklasse von $\mathbb{Z}G$-Moduln durch das Tupel $(n_g, n_\zeta, n_1, [I])$ vollständig beschrieben. Einen Beweis des vorherigen Theorems findet man in [CR62] Theorem 74.3. Dort wird auch ein Erzeugendensystem des Moduls M konstruiert, welches später noch gebraucht wird:

Korollar 1.14. *Seien $|G| \in \mathbb{P}(\mathbb{Q})$. Des Weiteren sei L ein $\mathbb{Z}G$-Gitter. Dann gibt es Vektoren $v_1, \ldots, v_{n_g+n_\zeta+n_1}, v_I$, sodass*

$$M = \bigoplus_{i=1}^{n_g} \mathbb{Z}Gv_i \oplus \bigoplus_{i=n_g+1}^{n_g+n_\zeta} \mathbb{Z}[\zeta_p]v_i \oplus \bigoplus_{i=n_g+n_\zeta+1}^{n_g+n_\zeta+n_1} \mathbb{Z}v_i \quad \oplus I \cdot v_I$$

*Die Menge $\{v_1, \ldots, v_{n_g+n_\zeta+n_1}, v_I\}$ heißt **Pseudobasis** von M.*

Weil Gitter über Maximalordnungen bessere Eigenschaften besitzen, wird im weiteren Verlauf für $R \in \{\mathbb{Z}, \mathbb{Z}_p\}$ anstelle eines RG-Gitters (L, h) das Gitter $((R[\zeta_p] \times R) \otimes_{RG} L, h)$ betrachtet. Es zerfällt in zwei orthogonale Teilgitter:

Proposition 1.15. *Sei $R \in \{\mathbb{Z}, \mathbb{Z}_p\}$ und (L, h) ein hermitesches RG-Gitter. Dann gibt es genau ein $R[\zeta_p]$-Gitter (L^ζ, h^ζ) und genau ein R-Gitter (L^1, b^1), sodass $(R[\zeta_p] \times R) \otimes_{RG} L = L^\zeta \perp L^1$ gilt.*

Beweis. Man erhält mit Hilfe der vollständigen Menge primitiver, orthogonaler Idempotente $(1,0), (0,1) \in R[\zeta_p] \times R$ eine eindeutige Modulzerlegung von $(R[\zeta_p] \times R) \otimes_{RG} L$ in zwei Teilgitter $L^\zeta \oplus L^1$. Dabei ist L^ζ ein $R[\zeta_p]$-Gitter und L^1 ein R-Gitter. Die Zerlegung ist orthogonal, denn für alle $y \in L^\zeta$ und $z \in L^1$ gilt:

$$p \cdot h(y,z) = \sum_{i=0}^{p-1} h(g^i(y), g^i(z)) = \sum_{i=0}^{p-1} h(g^i(y), z) = h(\sum_{i=0}^{p-1} g^i(y), z) = h(0,z) = 0$$

□

Bemerkung 1.16. Erzeugendensysteme der Gitter L^ζ und L^1 lassen sich mit Hilfe der Zerlegung aus Theorem 1.13 bestimmen, denn L_1 kann in L^1 wiedergefunden werden und L_ζ sowie I in L^ζ. Nur L_g wird beim Übergang zur Maximalordnung in zwei zueinander orthogonale Teilgitter aufgespalten. Daher gibt es zu jedem Vektor $x \in L$ ein $y' \in L^\zeta$ und ein $z' \in L^1$, sodass $x = (y', 0) + (0, z')$ ist. Für $x_1, x_2 \in L^\zeta \perp L^1$ gilt wegen der Orthogonalität $h(x_1, x_2) = (h^\zeta(y_1', y_2'), h^1(z_1', z_2'))$.

Als nächstes soll wieder ein $\mathbb{Z}$-Gitter (L, b) mit einem Automorphismus betrachtet werden, der nicht notwendigerweise von Primzahlordnung ist. Für jedes dieser Gitter sollen Teilgitter bestimmt werden, die eng mit der Operation des Automorphismus zusammenhängen. Zunächst wird dafür eine Zerlegung des zugrundeliegenden Vektorraums in g-invariante Teilräume benötigt. Eine solche Zerlegung heißt **Primärzerlegung** :

Proposition 1.17. *Seien V ein hermitescher $\mathbb{Q}G$-Modul und $W_d := \mathrm{Kern}(\Phi_d(g))$. Dann gilt für V als $\mathbb{Q}$-Vektorraum*

(a) $V = \perp_{d|m} W_d$

(b) Jedes W_d ist g-invariant.

(c) Das Minimalpolynom von $g|_{W_d}$ ist Φ_d.

Beweis. Aus der Zerlegung von $\mathbb{Q}G \cong \prod_{d|m} \mathbb{Q}[\zeta_d]$ kann mit Hilfe der entsprechend gewählten, vollständigen Menge primitiver, orthogonaler Idempotente $\{e_d \mid d|m\}$ eine Zerlegung von V als $\mathbb{Q}G$-Modul konstruiert werden:

$$V = \bigoplus_{d|m} e_d V$$

Da die Involution auf den Idempotenten trivial operiert, gilt für $d \neq d'$:

$$h(e_d V, e_{d'} V) = e_d \overline{e_{d'}} h(V, V) = 0$$

Mit $\mathrm{t}(0) = 0$ erhält man eine Zerlegung von V als $\mathbb{Q}$-Vektorraum in g-invariante Teilräume:

$$V = \bigperp_{d|m} W_d$$

□

Definition 1.18. Es sei (L, b) ein Gitter auf dem quadratischen Vektorraum (V, b) mit $V := \mathbb{Q} \otimes_{\mathbb{Z}} L$. Des Weiteren sei $g \in \mathrm{Aut}(L)$ mit Minimalpolynom φ. Da $|G| = m$ ist, ist das Minimalpolynom φ von g ein Teiler von $X^m - 1$, also ein Produkt von verschiedenen Kreisteilungspolynomen Φ_d mit $d|m$. Nach Proposition 1.17 gibt es eine Zerlegung von V in g-invariante Teilräume W_i. Bildet man $L \cap W_i$, so erhält man Teilgitter von L. Im weiteren Verlauf bezeichnet man mit $L_1 := \mathrm{Kern}(g - 1) \cap L$ das **Fixgitter** von L und definiert $L_d := \mathrm{Kern}(\Phi_d(g)) \cap L$. Auf L_d operiert g für $d > 2$ nach Konstruktion fixpunktfrei. Falls $d \notin \{1, 2\}$ ist, kann man L_d demnach im Sinne von Proposition 1.17 als hermitesches Gitter über $\mathbb{Z}[\zeta_d]$ auffassen. Falls $d \in \{1, 2\}$ ist, bleibt L_{ζ_d} ein quadratisches $\mathbb{Z}$-Gitter.

Bildet man die orthogonale Summe $\bigperp_{d|m} L_d$, so erhält man im Allgemeinen nicht das Gitter L, sondern ein weiteres Teilgitter von L. Dessen Index wird im Fall $m = p$ mit der folgenden Proposition beschrieben:

Proposition 1.19. *Sei (L, b) ein Gitter mit einem Automorphismus g der Ordnung p. Des Weiteren sei n_g wie in Theorem 1.13 definiert. Dann gilt:*

$$[L : L_\zeta \perp L_1] = p^{n_g} \leq p^{\min\{\mathrm{rang}_{\mathbb{Z}}(L_1), \mathrm{rang}_{\mathbb{Z}}(L_\zeta)\}}$$

Beweis. Nach Lemma 1.14 gibt es Vektoren $v_i \in L$ und ein Ideal I, sodass

$$L \cong \bigoplus_{i=1}^{n_g} \mathbb{Z}Gv_i \oplus \bigoplus_{i=n_g+1}^{n_g+n_\zeta} \mathbb{Z}[\zeta_p]v_i \oplus \bigoplus_{i=n_g+n_\zeta+1}^{n_g+n_\zeta+n_1} \mathbb{Z}v_i \oplus I \cdot v_I$$

Da $\mathrm{Spann}\{v_I, v_{n_g+1}, \ldots, v_{n_g+n_\zeta}\} \subseteq L_\zeta$ und $\mathrm{Spann}\{v_{n_g+n_\zeta+1}, \ldots, v_{n_g+n_\zeta+n_1}\} \subseteq L_1$ primitive Teilgitter sind, genügt es $M := \bigoplus_{i=1}^{n_g} \mathbb{Z}Gv_i$ zu betrachten. Nach Proposition 1.12 findet man zu jedem $\mathbb{Z}Gv_i$ ein Teilgitter $((1-\zeta_p)\mathbb{Z}[\zeta_p] \times \{0\})v_i \oplus (\{0\} \times p\mathbb{Z})v_i$ von Index p^2. Dabei ist $((1-\zeta_p)\mathbb{Z}[\zeta_p] \times \{0\})v_i \in \mathrm{Kern}(\Phi_p(g))$ und $(\{0\} \times p\mathbb{Z})v_i \in \mathrm{Kern}(1-g)$. □

Bemerkung 1.20.

(a) Die Determinante des Teilgitters $L_\zeta \perp L_1$ ist also um den Faktor p^{2n_g} größer als die Determinante des Gitters. Aus der Konstruktion der Einbettung folgt, dass sich der Faktor gleichmäßig auf L_1 und L_ζ aufteilt.

(b) Für eine beliebige Gruppenordnung m ist es schwer, den Index zu berechnen. Wegen Proposition 1.10 ist aber klar, dass für die Primteiler des Indexes nur die Teiler der Gruppenordnung in Frage kommen.

Um $\mathbb{Z}$-Gitter mit einem Automorphismus zu untersuchen, betrachtet man häufig die Teilgitter L_{ζ_d} eines $\mathbb{Z}$-Gitters, auf dem der Automorphismus wie eine Einheitswurzel operiert. Daher soll im Folgenden die Struktur eines $\mathbb{Z}$-Gitters mit einem solchen Automorphismus der Ordnung m genauer betrachtet werden. Dabei spielt die Spurkonstruktion von zwei Algebren eine wichtige Rolle. Zum einen wird die Gruppenalgebra $\mathbb{Q}G = \bigoplus_{d|m} \mathbb{Q}[\zeta_d]$ wichtig sein. Weil $\mathbb{Z}$-Geschlechter betrachtet werden, wird an Stellen von $\mathbb{Z}$ lokalisiert und man erhält zum anderen eine Ordnung in der $\mathbb{Q}_p$-Algebra $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_d]$. Für die Spur, interpretiert als Spur der Darstellungsmatrix der Linksmultiplikation, folgt dann mit Hilfe von Proposition 1.7 direkt aus ihrer Definition:

Proposition 1.21.

(a) Für alle $x = (x_d)_{d|m} \in \prod_{d|m} \mathbb{Q}[\zeta_d]$ *gilt*

$$\mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}G}(x) = \sum_{d|m} \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_d]}(x_d)$$

(b) Für alle $x = (x_\pi)_{(\pi)|(p)} \in \prod_{(\pi)|(p)} \mathbb{Q}[\zeta_d]_\pi$ *gilt*

$$\mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_d]}(x) = \sum_{(\pi)|(p)} \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_d]_\pi}(x_\pi)$$

Bemerkung 1.22. Sei (L, b) ein $\mathbb{Z}$-Gitter mit einem fixpunktfreien Automorphismus der Ordnung m und Minimalpolynom Φ_m. Fasst man L als Gitter über dem Gruppenring auf, so sind bis auf L_{ζ_m} alle Summanden der Primärzerlegung $\{0\}$. Der Automorphismus g wird in diesem Fall mit ζ_m identifiziert und L wird zu einem $\mathbb{Z}[\zeta_m]$-Modul. Die Bilinearform kann zu der hermiteschen Form über dem Gruppenring geliftet werden. Gemäß Proposition 1.21 entspricht sie in diesem Spezialfall gerade der Körperspur:

$$b(v, w) \quad = \quad \mathrm{t}(h(v, w)) = \sum_{d|m} \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_d]}(h(v, w)_d) = \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}(h(v, w))$$

Im weiteren Verlauf der Arbeit werden Gitter oder Teilgitter betrachtet, die eine zusätzliche Struktur über $\mathbb{Z}[\zeta_m]$ oder $\mathbb{Z}[\zeta_m]_\pi$ besitzen. Weil dabei regelmäßig die Zerlegung von Idealen

benutzt wird, soll die in vielen Lehrbüchern übliche Notation fixiert werden. Der Trägheitsgrad eines Primideals in der Körpererweiterung $\mathbb{Q}[\zeta_m] : \mathbb{Q}$ werde mit f bezeichnet und der Trägheitsgrad einer Zerlegung in $\mathbb{Q}[\zeta_m + \overline{\zeta_m}] : \mathbb{Q}$ mit f^+. Die Verzweigungsindizes seien e und e^+ und die Anzahl der Primteiler wird mit r und r^+ bezeichnet.

1.2 Eine g-invariante modulare Zerlegung

In diesem Abschnitt werden zunächst einige grundlegende Definitionen eingeführt und modulare Zerlegungen eines $\mathbb{Z}$-Gitters vorgestellt. Anschließend wird gezeigt, dass es zu jedem $\mathbb{Z}$-Gitter (L, b) mit einem Automorphismus der Ordnung m und an allen Stellen $p \nmid m$ stets eine p-modulare Zerlegung existiert, für die jede Komponente invariant unter dem Automorphismus ist.

Definition 1.23. Es seien R ein Ring und (L, b) ein quadratisches R-Gitter. Sei

$$\begin{aligned} \hat{b} : L &\longrightarrow \mathrm{Hom}_R(L, R) \\ y &\mapsto b(-, y) \end{aligned}$$

Ein R-Gitter (L, b) heißt **$\mathfrak{A}$-modular** für ein Ideal $\mathfrak{A} \subseteq R$, wenn L von $\hat{b}$ bijektiv auf $\mathrm{Hom}_R(L, \mathfrak{A})$ abbildet. Falls ein Gitter R-modular ist, wird es auch **unimodular** genannt. Das von $\{b(v, w) \mid v, w \in L\}$ erzeugte Ideal $\mathrm{Scale}(L)$ nennt man **Skalenideal** von L. Ist R ein lokaler Ring, so ist $\mathrm{Scale}(L) = \{b(v, w) \mid v, w \in L\}$. Das von $\{b(v_i, v_i) \mid v_i \in L\}$ erzeugte Ideal heißt **Norm** von L. Auf dieselbe Art werden Scale und Norm für hermitesche Gitter definiert.

Proposition 1.24. *Sei p eine Primzahl und L ein $\mathbb{Z}_p$-Gitter.*

(a) Dann gibt es (p^i)-modulare Teilgitter $L_i \subseteq L$, so dass:

$$L \cong \bigperp_{i \in \mathbb{Z}} L_i$$

*Es können nur endlich viele $L_i \neq \{0\}$ sein. Eine solche Zerlegung heißt **p-modulare Zerlegung** von L.*

(b) Falls $L \cong \bigperp_{i \in \mathbb{Z}} L_i \cong \bigperp_{i \in \mathbb{Z}} L'_i$ zwei p-modulare Zerlegungen sind, gilt:

(i) $\mathrm{rang}_{\mathbb{Z}_p}(L_i) = \mathrm{rang}_{\mathbb{Z}_p}(L'_i)$ für alle i.
Insbesondere ist $|\{i \in \mathbb{Z} \mid L_i \neq \{0\}\}| = |\{i \in \mathbb{Z} \mid L'_i \neq \{0\}\}|$

(ii) Falls $p \neq 2$ ist, gilt $L_i \cong L'_i$ für alle $i \in \mathbb{Z}$

Einen Beweis findet man zum Beispiel in [Kit03] auf den Seiten 79ff. Das Ziel dieses Abschnitts ist es, für ein $\mathbb{Z}$-Gitter L mit einem Automorphismus g der Ordnung m an jeder Stelle $p \nmid m$ die Existenz einer p-modularen Zerlegung, für die zusätzlich $g(L_i) = L_i$ gilt, nachzuweisen.

Definition 1.25.

(a) Es sei (L, b) ein $\mathbb{Z}$-Gitter auf dem quadratischen $\mathbb{Q}$-Vektorraum (V, b). Dann heißt $(L, b)^{\#} := \{y \in V \mid b(x, y) \in \mathbb{Z} \text{ für alle } x \in L\}$ das **duale Gitter** von L bezüglich b.

(b) Es sei (L, h) ein $\mathbb{Z}[\zeta_m]$-Gitter auf dem hermiteschen $\mathbb{Q}[\zeta_m]$-Vektorraum (V, h). Dann heißt $(L, h)^{\#} := \{y \in V \mid h(x, y) \in \mathbb{Z}[\zeta_m] \text{ für alle } x \in L\}$ das **duale Gitter** von L bezüglich h.

Wie im ersten Abschnitt beschrieben wurde, gibt es $\mathbb{Z}$-Gitter mit einem fixpunktfreien Automorphismus, die eine zusätzliche hermitesche Struktur über $\mathbb{Z}[\zeta_m]$ besitzen. Zu solchen Gittern gibt also zwei duale Gitter, die sich unterscheiden können. Zum Beschreiben dieses Unterschieds wird die Differente benötigt:

Definition 1.26. Sei $F : E$ eine Körpererweiterung mit Ganzheitsringen $\mathfrak{O}_F$ und $\mathfrak{O}_E$. Das gebrochene Ideal $D := \{x \in F \mid \mathrm{Spur}_E^F(x\mathfrak{O}_F) \subseteq \mathfrak{O}_E\}$ heißt der **Dedekindsche Komplementärmodul**. Das dazu inverse Ideal wird **Differente** $\mathfrak{D}_E^F := D^{-1}$ genannt.

Bemerkung 1.27. In dieser Arbeit werden die Differente für die Erweiterungen $\mathbb{Q}[\zeta_m] : \mathbb{Q}$, $\mathbb{Q}[\zeta_m] : \mathbb{Q}[\zeta_m + \overline{\zeta_m}]$ und $\mathbb{Q}[\zeta_m + \overline{\zeta_m}] : \mathbb{Q}$ sowie für die Erweiterungen, die sich durch die Lokalisierungen ergeben, benötigt. Im Folgenden werden einige Eigenschaften der Differente und der Diskriminante aufgelistet, die im weiteren Verlauf der Arbeit verwendet werden. Man kann sie zum Beispiel in [Lan86] ab Seite 60 finden:

(a) Für einen Körperturm $E \subseteq F \subseteq G$ gilt: $\mathfrak{D}_E^G = \mathfrak{D}_F^G \cdot \mathfrak{D}_E^F$.

(b) Die Primteiler von $\mathfrak{D}_E^F$ sind genau die verzweigten Primelemente.

(c) Sei $(p) \subset E$ ein Primideal. Bezeichnet man mit $\mathfrak{P}_i \subset F$ die Primideale über (p), so gilt: $\mathfrak{D}_E^F = \prod_i (\mathfrak{D}_{E_p}^{F_{\mathfrak{P}_i}} \cap F)$.

(d) Falls $m = p^t$ ist, gilt $\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} = ((1 - \zeta_m)^{p^{(t-1)}(pt-t-1)})$.

(e) Falls $m = m_1 \cdot m_2$ mit $\mathrm{ggT}(m_1, m_2) = 1$ ist, gilt $\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} = (\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_{m_1}]}) \cdot (\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_{m_2}]})$.

(f) Es gilt $\mathrm{Norm}_E^F(\mathfrak{D}_E^F) = |\operatorname{disc}_E^F|$. Daher ist eine analoge Aussage von a) und b) auch für die Diskriminante gültig.

Lemma 1.28. *Es sei $\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}$ die Differente der Körpererweiterung $\mathbb{Q}[\zeta_m] : \mathbb{Q}$. Des Weiteren sei (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]$-Gitter. Dann ist (L, b) mit $b := \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} \circ h$ ein quadratisches $\mathbb{Z}$-Gitter und es gilt:*

$$(L, b)^{\#} = (\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]})^{-1}(L, h)^{\#}$$

Ist $p \in \mathbb{P}(\mathbb{Q})$, so gilt für die Lokalisierung an der Stelle p:

$$(\mathbb{Z}_p \otimes L, b)^{\#} = ((\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]})^{-1} \cdot \mathbb{Z}_p) \cdot (\mathbb{Z}_p \otimes L, h)^{\#}$$

Beweis. Die erste Formel ist wohl bekannt. Man findet sie zum Beispiel in [Sch98] auf Seite 490. Die zweite Formel folgt aus der Tatsache, dass die Gitter global übereinstimmen und damit auch ihre Lokalisierungen. □

Lemma 1.29. *Es seien $p \nmid m$ und π eine über p liegende Stelle in $\mathbb{Z}[\zeta_m]$. Dann wird ein (p^t)-modulares, hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter (L,h) durch $b(x,y) := \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h(x,y))$ zu einem (p^t)-modularen, quadratischen $\mathbb{Z}_p$-Gitter.*

Beweis. Weil $p \nmid m$, ist die Körpererweiterung $\mathbb{Q}[\zeta_m]_\pi : \mathbb{Q}_p$ unverzweigt. Daher ist die Differente $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} = \mathbb{Z}[\zeta_m]_\pi$ und mit Lemma 1.28 folgt, dass (L,b) genau dann unimodular ist, wenn (L,h) unimodular ist. Des Weiteren folgt aus der Tatsache, dass die Körpererweiterung $\mathbb{Q}[\zeta_m]_\pi : \mathbb{Q}_p$ unverzweigt ist, dass man p als uniformisierendes Element für beide Körper wählen kann. Falls (L,h) (p^t)-modular ist, gibt es eine hermitesche Form h', sodass $h = p^t h'$ gilt und (L,h') unimodular ist. Nach obigen Überlegungen muss daher $b' := \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h'$ ebenfalls unimodular sein. Damit folgt für alle $x, y \in L$:

$$\begin{aligned} b(x,y) &= \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h(x,y)) = \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(p^t \cdot h'(x,y)) \\ &= p^t \cdot \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h'(x,y)) = p^t \cdot b'(x,y) \end{aligned}$$

Also ist (L,b) (p^t)-modular. □

Die Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ besitzt den Grad 2. Daher kann ein Primideal aus dem Ring $\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ über $\mathbb{Z}[\zeta_m]$ entweder träge bleiben, zerfallen oder verzweigen. Diese drei Fälle werden im weiteren Verlauf der Arbeit abkürzend mit **der träge Fall**, der **zerfallende Fall** und der **verzweigte Fall** bezeichnet. Die Begriffe werden auch für die Lokalisierungen dieser Erweiterung verwendet. Für hermitesche Gitter über den lokalen Erweiterungen gibt es zu allen drei Fällen bereits Ergebnisse von Ronald Jacobowitz und Larry Gerstein, die im weiteren Verlauf häufig benutzt werden.

Definition 1.30. Sei die träge oder verzweigte Erweiterung $\mathbb{Z}[\zeta_m]_\pi/\mathbb{Z}[\zeta_m + \overline{\zeta_m}]_{\pi'}$ gegeben. Des Weiteren sei (L,h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter. Eine Zerlegung

$$L \cong \bigperp_{i \in \mathbb{Z}} L_i$$

in (π^i)-modulare Komponenten heißt **π-modulare Zerlegung** von L. Eine modulare Komponente heißt **normal**, wenn $\mathrm{Norm}(L_i, h|_{L_i}) = \mathrm{Scale}(L_i, h|_{L_i})$ gilt. Ansonsten heißt L_i **subnormal**. Man sagt, zwei $\mathbb{Z}[\zeta_m]_\pi$-Gitter $\perp_{i\in\mathbb{Z}} L_i$ und $\perp_{i\in\mathbb{Z}} L_i'$ sind vom selben **modularen Typ**, wenn $\mathrm{rang}_{\mathbb{Z}[\zeta_m]_\pi} L_i = \mathrm{rang}_{\mathbb{Z}[\zeta_m]_\pi} L_i$ für alle $i \in \mathbb{Z}$ gilt und L_i genau dann normal ist, wenn L_i' normal ist.

Proposition 1.31. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und $m \in \mathbb{N}$ gegeben. Die über (p) liegenden Primideale von $\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ seien in der Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ träge. Des Weiteren sei π eine über p liegende Stelle in $\mathbb{Z}[\zeta_m]$.*

(a) Dann gibt es zu jedem hermiteschen $\mathbb{Z}[\zeta_m]_\pi$-Gitter (L,h) eine π-modulare Zerlegung

$$L \cong \bigperp_{i\in\mathbb{Z}} L_i$$

Es können nur endlich viele $L_i \neq \{0\}$ sein. Diese modularen Teilgitter L_i besitzen eine Orthogonalbasis.

(b) Zwei $\mathbb{Z}[\zeta_m]_\pi$-Gitter sind genau dann isometrisch, wenn sie vom selben modularen Typ sind.

Einen Beweis dieser Aussage findet man unter Verwendung von [Jac62] Proposition 4.3. in [Jac62] Kapitel 7. Auch der verzweigte Fall wird dort in Proposition 8.1 und 8.2 in Kombination mit Proposition 4.3 behandelt:

Proposition 1.32. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{2,\infty\}$ und $m := p^t$. Die über (p) liegenden Primideale von $\mathbb{Z}[\zeta_m+\overline{\zeta_m}]$ sind in der Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m+\overline{\zeta_m}]$ verzweigt. Sei π eine über p liegende Stelle in $\mathbb{Z}[\zeta_m]$.*

(a) Dann gibt es zu jedem hermiteschen $\mathbb{Z}[\zeta_m]_\pi$-Gitter (L,h) eine π-modulare Zerlegung

$$L \cong \bigperp_{i\in\mathbb{Z}} L_i$$

Es können nur endlich viele $L_i \neq \{0\}$ sein und für $p \neq 2$ gilt:

$$L_i \cong \begin{cases} \langle \pi^{\frac{i}{2}} \rangle \perp \ldots \perp \langle \pi^{\frac{i}{2}} \rangle \perp \langle \pi^{-\frac{i(n-1)}{2}} \det(L_i) \rangle & \text{falls } i \text{ gerade} \\ \mathbb{H}(i) \perp \ldots \perp \mathbb{H}(i) \perp \mathbb{H}(i) & \text{falls } i \text{ ungerade} \end{cases}$$

wobei $\mathbb{H}(i)$ mit π^i skalierte, hyperbolische Ebenen sind.

(b) Zwei $\mathbb{Z}[\zeta_m]_\pi$-Gitter L und L' sind genau dann isometrisch, wenn

(i) sie vom selben modularen Typ sind und

(ii) für π-modulare Zerlegungen $L \cong \bigperp L_i$ und $L' \cong \bigperp L'_i$ gilt $\det(L_i) = \det(L'_i)$ für alle geraden i.

Dyadische Stellen werden in [Jac62] Kapitel 9 bis 11 genauer untersucht. In dieser Arbeit werden die Ergebnisse jedoch nicht benötigt.

Definition 1.33. Sei $\mathfrak{P} \subseteq (p) \subseteq \mathbb{Z}[\zeta_m+\overline{\zeta_m}]$ ein Primideal, dass über $\mathbb{Z}[\zeta_m]$ in zwei Primideale $\mathfrak{Q}_i\overline{\mathfrak{Q}_i}$ zerfällt. Des Weiteren seien π eine über p liegende Stelle und (L,h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$-Gitter. Eine Zerlegung

$$L \cong \bigperp_{i\in\mathbb{Z}} L_i$$

in $(\pi^i \times \overline{\pi}^i)$-modulare Komponenten heißt **π-modulare Zerlegung** von L. Man sagt, zwei $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$-Gitter $\perp_{i\in\mathbb{Z}} L_i$ und $\perp_{i\in\mathbb{Z}} L'_i$ sind vom selben **modularen Typ**, wenn für alle $i \in \mathbb{Z}$ $\operatorname{rang}_{\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}}(L_i) = \operatorname{rang}_{\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}}(L_i)$ gilt.

Die folgende Proposition folgt aus [Ger70] Bemerkung 1.6. und wurde erstmals in [Shi64] bewiesen.

Proposition 1.34. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und $m \in \mathbb{N}$. Die über (p) liegenden Primideale von $\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ seien in der Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ zerfallend. Des Weiteren sei π eine über p liegende Stelle.*

(a) Dann gibt es zu jedem hermiteschen $\mathbb{Z}[\zeta_m]_\pi \times \overline{\mathbb{Z}[\zeta_m]_\pi}$-Gitter (L, h) eine $(\pi^i \times \overline{\pi}^i)$-modulare Zerlegung

$$L \cong \bigperp_{i\in\mathbb{Z}} L_i$$

Es können nur endlich viele $L_i \neq \{0\}$ sein. Diese Teilgitter L_i besitzen eine Orthogonalbasis, und das von jedem Basisvektor aufgespannte Teilgitter, aufgefasst als $\mathbb{Z}[\zeta_m]_\pi$-Gitter von doppeltem Rang, besitzt eine Gram-Matrix der Form

$$\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$$

(b) Zwei $\mathbb{Z}[\zeta_m]_\pi \times \overline{\mathbb{Z}[\zeta_m]_\pi}$-Gitter sind genau dann isometrisch, wenn sie vom selben modularen Typ sind.

Proposition 1.35. *Sei $p \nmid m$ eine endliche Stelle und (L, h) ein hermitesches $\mathbb{Z}G$-Gitter. Dann kann $\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L$ in eine orthogonale Summe von Teilgittern über $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$ mit $d \mid m$ zerlegt werden und jedes solche Teilgitter besitzt eine Orthogonalbasis sowie eine orthogonale Zerlegung in Teilgitter von Rang 1 über $\mathbb{Z}[\zeta_d]_\pi$ oder $\mathbb{Z}[\zeta_d]_\pi \times \mathbb{Z}[\zeta_d]_{\overline{\pi}}$ für über p liegende Stellen π in $\mathbb{Z}[\zeta_d]$.*

Beweis. Nach Korollar 1.11 ist $\mathbb{Z}_pG$ bereits die maximale Ordnung in der Gruppenalgebra und es gilt $\mathbb{Z}_pG \cong \bigoplus_{d|m} \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$. Sei $\{e_d \mid d \text{ teilt } m\}$ die zu dieser Ringzerlegung gehörige vollständige Menge orthogonaler Idempotente. Mit ihrer Hilfe kann $\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L$ zerlegt werden:

$$\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L = \bigoplus_{d|m} e_d(\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L)$$

Diese Summe ist wegen $e_d = \overline{e_d}$ orthogonal, denn für $d \neq d'$ gilt:

$$h(e_d(\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L), e_{d'}(\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L)) = e_d e_{d'} h(\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L, \mathbb{Z}_pG \otimes_{\mathbb{Z}G} L) = 0$$

Jedes $(L_d, h_d) := (e_d(\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L), h|_{e_d(\mathbb{Z}_pG \otimes_{\mathbb{Z}G} L)})$ ist nach Konstruktion ein hermitesches $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$-Gitter. Da nach Proposition 1.7 $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d] \cong \prod_{(\pi)|(p)} \mathbb{Z}[\zeta_d]_\pi$ gilt, kann man

wieder die kanonische, vollständige Menge primitiver Idempotente $\{e'_\pi \mid \pi \text{ teilt } p\}$ wählen und damit eine Modulzerlegung konstruieren:

$$L_d = \bigoplus_{(\pi)|(p)} e'_\pi L_d$$

Die Gitter $e'_\pi L_d$ sind Gitter über dem lokalen Ring $\mathbb{Z}[\zeta_d]_\pi$ und es gilt $\operatorname{rang}_{\mathbb{Z}[\zeta_d]_\pi} e'_\pi L_d = \operatorname{rang}_{\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]} L_d$. Um die Orthogonalität dieser Zerlegung zu untersuchen, müssen zwei Fälle unterschieden werden. Dazu betrachtet man zunächst die Primidealzerlegung von $p\mathbb{Z}[\zeta_d + \overline{\zeta_d}] = P_1 \cdot \ldots \cdot P_{r^+}$. Weil $\mathbb{Q}[\zeta_d] : \mathbb{Q}[\zeta_d + \overline{\zeta_d}]$ eine Galoiserweiterung von Grad 2 ist, gilt für alle P_i entweder $P_i\mathbb{Z}[\zeta_d] = Q_i$ oder $P_i\mathbb{Z}[\zeta_d] = Q_i\overline{Q_i}$ für ein Primideal $Q_i \subseteq \mathbb{Z}[\zeta_d]$. Weil $p \nmid m$ und damit auch kein Teiler der Diskriminante ist, kann der verzweigte Fall nicht eintreten.

1.Fall: $P_i\mathbb{Z}[\zeta_d] = Q_i$

Dann ist $e'_\pi = \overline{e'_\pi}$ und für $\pi \neq \pi'$ folgt $h(e'_\pi L_d, e'_{\pi'} L_d) = e'_\pi e'_{\pi'} h(L_d, L_d) = 0$. Damit gilt sogar

$$L_d = \bigperp_{(\pi)|(p)} e'_\pi L_d$$

Nach Proposition 1.31 besitzen die $\mathbb{Z}[\zeta_d]_\pi$-Gitter $e'_\pi L_d$ eine Orthogonalbasis $v_{\pi,1}, \ldots, v_{\pi,n}$. Dies gilt insbesondere für $p = 2$. Also hat man L in eine orthogonale Summe von Teilgittern von Rang 1 zerlegt. Solche Teilgitter sind stets modular. Die Vektoren $\{(v_{\pi_1,i} \oplus \ldots \oplus v_{\pi_r,i}) \mid i \in \{1, \ldots, \operatorname{rang}(L_d)\}\}$ bilden dann eine Orthogonalbasis von L_d, denn es gilt für $i \neq j$:

$$h((v_{\pi_1,i} \oplus \ldots \oplus v_{\pi_r,i}), (v_{\pi_1,j} \oplus \ldots \oplus v_{\pi_r,j})) = (h(v_{\pi_k,i}, v_{\pi_k,j})_{\pi_k}) = 0$$

2.Fall: $P_i\mathbb{Z}[\zeta_d] = Q_i\overline{Q_i}$

Sei $(p) = Q_1 \cdot \ldots \cdot Q_r$ die Primidealzerlegung in $\mathbb{Z}[\zeta_d]$. In diesem Fall operiert die Konjugation nicht trivial auf den Q_i. Man kann die Ideale also zu Paaren $(Q_i, \overline{Q_i})$ gruppieren. Durch Umnummerierung wird o.B.d.A. angenommen, dass $Q_i = \overline{Q_{i+1}}$ und damit $e_i = \overline{e_{i+1}}$ für alle ungeraden i gilt. Es folgt für alle $i, j \in \{1, \ldots, r^+\}$ mit $i \neq j$:

$$h(e'_{2i-1} L_d, e'_{2j} L_d) = h(\overline{e'_{2j}} e'_{2i-1} L_d, L_d) = h(0, L_d) = 0$$

Daher erhält man die folgende orthogonale Zerlegung:

$$L_d = \bigperp_{i=1}^{r^+} (e'_{2i-1} L_d \oplus e'_{2i} L_d)$$

Jeder orthogonale Summand $e'_{2i-1} L_d \oplus e'_{2i} L_d$ ist ein Gitter über dem Produkt $\mathbb{Z}[\zeta_d]_{Q_i} \times \mathbb{Z}[\zeta_d]_{\overline{Q_i}}$. Mit Hilfe der Konjugation rechnet man leicht nach, dass $\mathbb{Q}[\zeta_d]_{\overline{Q_i}} \cong \mathbb{Q}[\zeta_d]_{Q_i}$ beziehungsweise $\mathbb{Z}[\zeta_d]_{\overline{Q_i}} \cong \mathbb{Z}[\zeta_d]_{Q_i}$ gilt. Gemäß Proposition 1.34 gibt es eine Basis $\{v_{i,1}, \ldots, v_{i,n}\}$ von $e'_{2i-1} L_d$ und eine Basis $\{w_{i,1}, \ldots, w_{i,n}\}$ von $e'_{2i} L_d$, sodass die Gram-Matrix von $e'_{2i-1} L_d \oplus e'_{2i} L_d$ bezüglich der Vektoren

$$\{v_{i,1} \oplus 0,\ \ 0 \oplus w_{i,1},\ \ v_{i,2} \oplus 0,\ \ 0 \oplus w_{i,2},\ \ \ldots\ \ , v_{i,n} \oplus 0,\ \ 0 \oplus w_{i,n}\}$$

von der folgenden Form ist:

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & h(v_{i,1}, w_{i,1}) \\ h(w_{i,1}, v_{i,1}) & 0 \end{matrix}} & & & 0 & \\ & \boxed{\begin{matrix} 0 & h(v_{i,2}, w_{i,2}) \\ h(w_{i,2}, v_{i,2}) & 0 \end{matrix}} & & & \\ & & & \ddots & \\ 0 & & & & \boxed{\begin{matrix} 0 & h(v_{i,n}, w_{i,n}) \\ h(w_{i,n}, v_{i,n}) & 0 \end{matrix}} \end{pmatrix}$$

Damit erhält man eine orthogonale Zerlegung von (L_d, h_d) in Teilgitter der Form $(T_{i,j}, h|_{T_{i,j}})$ mit $T_{i,j} := \text{Spann}_{\mathbb{Z}[\zeta_d]_{Q_i} \times \mathbb{Z}[\zeta_d]_{\overline{Q_i}}}\{v_{i,j} \oplus w_{i,j}\}$. Weil die Erweiterung unverzweigt ist, kann p als uniformisierendes Element für beide Lokalisierungen $\mathbb{Z}[\zeta_d]_{Q_i}$ und $\mathbb{Z}[\zeta_d]_{\overline{Q_i}}$ gleichzeitig verwendet werden. Da $p^t | h(v_{i,j}, w_{i,j})$ genau dann gilt, wenn auch $p^t | h(w_{i,j}, v_{i,j})$, ist $(T_{i,j}, h|_{T_{i,j}})$ ein $(p^t \times p^t)$-modulares Teilgitter. Die Vektoren

$$\{(v_{1,j} \oplus w_{1,j} \oplus \ldots \oplus v_{r^+,j} \oplus w_{r^+,j}) \mid j \in \{1, \ldots, \text{rang}(L_d)\}\}$$

bilden dann eine Orthogonalbasis von L_d, denn für $j \neq k$ gilt:

$$\begin{aligned} & h((v_{1,j} \oplus w_{1,j} \oplus \ldots \oplus v_{r^+,j} \oplus w_{r^+,j}), (v_{1,k} \oplus w_{1,k} \oplus \ldots \oplus v_{r^+,k} \oplus w_{r^+,k})) \\ = \quad & (h(v_{i,j} \oplus w_{i,k}), h(w_{i,j} \oplus v_{i,k}))_{1 \leq k \leq r^+} = 0 \end{aligned}$$

□

Korollar 1.36. *Sei (L, b) ein quadratisches $\mathbb{Z}$-Gitter mit einem Automorphismus g der Ordnung m. Dann zerfällt L in eine orthogonale Summe von g-invarianten Teilgittern $L = \perp_{d|m} L_{\zeta_d}$ und jedes Teilgitter zerfällt in g-invariante, p-modulare Komponenten. Für $d \notin \{1, 2\}$ ist die Dimension jeder Komponente ein ganzzahliges Vielfaches von $2f_d^+$.*

Beweis. Mit Hilfe des Automorphismus kann (L, b) als hermitesches Gitter über dem Gruppenring aufgefasst werden. Nach Proposition 1.35 kann man dieses Gitter in zueinander orthogonale $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$-Teilgitter von Rang 1 zerlegen. Jedes dieser Teilgitter ist eine orthogonale Summe von $\mathbb{Z}[\zeta_d]_\pi$-Gittern oder $\mathbb{Z}[\zeta_d]_\pi \times \mathbb{Z}[\zeta_d]_{\overline{\pi}}$ -Gittern, die ebenfalls Rang 1 besitzen. Durch Anwenden der Spur erhält man nach Lemma 1.29 eine orthogonale Zerlegung von (L, b) in modulare, g-invariante Teilgitter. Falls $d \notin \{1, 2\}$ ist, ist ihr Rang im trägen Fall $f_d = 2f_d^+$ und im zerfallenden Fall $2f_d = 2f_d^+$. □

Proposition 1.37. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und (L, b) ein $\mathbb{Z}$-Gitter mit einem Automorphismus g der Ordnung m mit $p \nmid m$. Des Weiteren seien*

$$L \cong \bigperp_{i\in\mathbb{Z}} L_i \cong \bigperp_{i\in\mathbb{Z}} M_i$$

zwei g-invariante p-modulare Zerlegungen. Dann gilt:

(a) Falls g fixpunktfrei operiert, gibt es eine Isometrie $\varphi : L \to M$ mit $\varphi_i : L_i \to M_i$ und $g \circ \varphi = \varphi \circ g$.

(b) Falls g nicht fixpunktfrei ist, gibt es eine solche Isometrie für $p \neq 2$.

Beweis. (a) Wie in Proposition 1.35 beschrieben wurde, kann man L, aufgefasst als hermitesches $\mathbb{Z}_pG$-Gitter, in eine orthogonale Summe von $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$-Gittern zerlegen:

$$L = \bigperp_{d|m} e_dL$$

Für jedes Gitter $L_d := e_dL$ mit $d > 2$ gibt es dann gegebenenfalls nach einer Umnummerierung eine von zwei möglichen orthogonalen Zerlegungen:

$$L_d = \bigperp_{i=1}^{r^+} e'_iL_d \quad \text{bzw.} \quad L_d = \bigperp_{i=1}^{r^+} (e'_{2i-1}L_d \oplus e'_{2i}L_d)$$

Diese Zerlegung ist eindeutig, weil dies alle nicht-triviale, primitive Idempotente sind, die ein direktes Produkt von Ganzheitsringen von Körpern besitzt. Nach Proposition 1.31 und Proposition 1.34 besitzen die $\mathbb{Z}[\zeta_d]_{\pi_i}$-Gitter und $\mathbb{Z}[\zeta_d]_{\pi_{2i-1}} \times \mathbb{Z}[\zeta_d]_{\pi_{2i}}$-Gitter eine modulare Zerlegung, deren modularer Typ eindeutig ist. Das bedeutet insbesondere, dass die Ränge der modularen Komponenten eindeutig bestimmt sind. Seien

$$L \cong \bigperp_{i\in\mathbb{Z}} L_i \cong \bigperp_{i\in\mathbb{Z}} M_i$$

zwei g-invariante modulare Zerlegungen von (L, b). Man betrachte nun die beiden (p^i)-modularen Komponenten L_i und M_i. Weil die modularen Komponenten g-invariant sind, können sie als hermitesche $\mathbb{Z}_pG$-Gitter aufgefasst und eindeutig zerlegt werden:

$$L_i = \bigperp_{d|m} e_dL_i \quad \text{und} \quad M_i = \bigperp_{d|m} e_dM_i$$

Dabei besitzt jedes $L_{i,d} := e_dL_i$ und jedes $M_{i,d} := e_dM_i$ eine Struktur über $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$. Wenn man diese Gitter für $d > 2$ auf eindeutige Weise weiter zerlegt, erhält man wieder die beiden Fälle

$$\textbf{(1)} \quad L_i = \bigperp_{j=1}^{r^+} e'_j L_{i,d} \qquad \text{und} \qquad M_i = \bigperp_{j=1}^{r^+} e'_j M_{i,d}$$

$$\textbf{(2)} \quad L_i = \bigperp_{j=1}^{r^+} (e'_{2j-1} L_{i,d} \oplus e'_{2j} L_{i,d}) \quad \text{und} \quad M_i = \bigperp_{j=1}^{r^+} (e'_{2j-1} M_{i,d} \oplus e'_{2j} M_{i,d})$$

1. Fall: Da L_i und M_i (p^i)-modular sind, sind die $\mathbb{Z}[\zeta_d]_{\pi_j}$-Gitter $e'_j L_{i,d}$ und $e'_j M_{i,d}$ gemäß Lemma 1.29 ebenfalls (p^i)-modular. Durch

$$\bigperp_{i\in\mathbb{Z}} e'_j L_{i,d} \quad \text{und} \quad \bigperp_{i\in\mathbb{Z}} e'_j M_{i,d}$$

erhält man zwei modulare Zerlegungen des $\mathbb{Z}[\zeta_d]_{\pi_j}$-Gitters $e'_j e_d L$, das nach obigen Überlegungen eindeutig bestimmt ist. Daher sind beide Zerlegungen vom selben modularen Typ. Also ist gemäß Proposition 1.31 $e'_j L_{i,d} \cong e'_j M_{i,d}$ und damit ist $L_{i,d} \cong M_{i,d}$ für $d > 2$.
2. Fall: Weil L_i und M_i (p^i)-modular sind, sind die Gitter $e'_{2j-1} L_{i,d} \oplus e'_{2j} L_{i,d}$ und $e'_{2j-1} M_{i,d} \oplus e'_{2j} M_{i,d}$ gemäß Lemma 1.29 ebenfalls modular. Wie im ersten Fall erhält man durch

$$\bigperp_{i\in\mathbb{Z}} (e'_{2j-1} L_{i,d} \oplus e'_{2j} L_{i,d}) \text{ und } \bigperp_{i\in\mathbb{Z}} (e'_{2j-1} M_{i,d} \oplus e'_{2j} M_{i,d})$$

zwei modulare Zerlegungen des $\mathbb{Z}[\zeta_d]_{\pi_{2j-1}} \times \mathbb{Z}[\zeta_d]_{\pi_{2j}}$-Gitters $e'_{2j-1} e_d L \oplus e'_{2j} e_d L$. Also sind beide Zerlegungen gemäß Proposition 1.34 vom selben modularen Typ. Daher folgt für $d > 2$

$$(e'_{2j-1} L_{i,d} \oplus e'_{2j} L_{i,d}) \cong (e'_{2j-1} M_{i,d} \oplus e'_{2j} M_{i,d})$$

Damit ist auch in diesem Fall $L_{i,d} \cong M_{i,d}$ für $d > 2$.

Da g fixpunktfrei operiert, sind die Teilgitter $L_{i,1} \cong M_{i,1} \cong \{0\}$. Die $\mathbb{Z}_p$-Gitter $L_{i,2}$ und $M_{i,2}$ sind ebenfalls trivial, wenn m ungerade ist. Falls m gerade ist, folgt aus $p \nmid m$ aber $p \neq 2$. Daher gibt es nach Proposition 1.24 eine Isometrie $\varphi_{i,2} : L_{i,2} \to M_{i,2}$. Der Automorphismus g operiert auf $L_{i,2}$ und $M_{i,2}$ mit dem Minimalpolynom $\Phi_2(x) = x + 1$. Für ein $v \in L_{i,2}$ gilt deshalb:

$$\varphi_{i,2}(g(v)) = -\varphi_{i,2}(v) = g(\varphi_{i,2}(v))$$

Insgesamt hat man also $L_{i,d} \cong M_{i,d}$ für alle $d|m$ gezeigt. Damit ist auch $L_i \cong M_i$ als hermitesche $\mathbb{Z}_p G$-Gitter. Fasst man die Gitter wieder als $\mathbb{Z}_p$-Gitter auf, so besitzt der Isomorphismus die angegebene Eigenschaft.
(b) Weil $p \nmid m$ gilt, gibt es nach Korollar 1.11 einen Isomorphismus $\mathbb{Z}_p G \cong \prod_{d|m} \mathbb{Z}[\zeta_d]$ und das Gitter (L, b), aufgefasst als hermitesches $\mathbb{Z}_p G$-Gitter (L, h), kann zerlegt werden:

$$L \cong e_1 L \perp \bigperp_{\substack{d|m \\ d\neq 1}} e_d L$$

Auf $\bigperp e_d L$ operiert g fixpunktfrei. Daher gibt es auf diesem Teilgitter nach (a) eine eindeu-

tige, g-invariante, p-modulare Zerlegung. Der Grundring des Fixgitters e_1L ist $\mathbb{Z}_p$. Weil g auf e_1L trivial operiert, ist jede p-modulare Zerlegung g-invariant. Jedoch ist eine modulare Zerlegung für $\mathbb{Z}_p$-Gitter nach Proposition 1.24 nur im Fall $p \neq 2$ eindeutig. □

Proposition 1.38.

(a) Jedes hermitesche $\mathbb{R}G$-Gitter (L,h) ist eine orthogonale Summe von Teilräumen über $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$ mit $d|m$ und jedes solche Teilgitter besitzt eine orthogonale Zerlegung in G-invariante Teilräume über $\mathbb{R}$ von Rang 1, falls $d \in \{1,2\}$ ist, oder von Rang 2, falls $d \notin \{1,2\}$ ist. Dabei ist jeder Teilraum entweder positiv oder negativ definit.

(b) Diese Zerlegung ist bis auf Isometrie eindeutig.

Beweis. Die Einbettungen $\mathbb{Z}[\zeta_d] \hookrightarrow \mathbb{C}$ gruppieren sich für $d \notin \{1,2\}$ zu Paaren $\{\sigma, \overline{\sigma}\}$. Sei V_d ein Vertretersystem, welches aus jedem Paar genau eine Einbettung enthält. Nach Proposition 1.9 ist

$$\mathbb{R}G \cong \begin{cases} \mathbb{R}^2 \times \prod\limits_{\substack{d|m \\ d\notin\{1,2\}}} \prod\limits_{\sigma\in V_d} \mathbb{C} & \text{falls } 2 \mid m \\ \mathbb{R} \times \prod\limits_{\substack{d|m \\ d\neq 1}} \prod\limits_{\sigma\in V_d} \mathbb{C} & \text{falls } 2 \nmid m \end{cases}$$

und man kann sich mit Hilfe der kanonischen, vollständigen Menge primitiver orthogonaler Idempotente $\{e_\sigma \mid \sigma \in \{\rho\} \cup V_d\}$ beziehungsweise $\{e_\sigma \mid \sigma \in \{\rho, \rho'\} \cup V_d\}$ eine Modulzerlegung von $L' := \mathbb{R} \otimes_{\mathbb{Z}} L$ konstruieren:

$$L' \cong \begin{cases} e_\rho L' \oplus e_{\rho'} L' \oplus \bigoplus\limits_{d|m} \bigoplus\limits_{\sigma\in V_d} e_\sigma L' & \text{falls } 2 \mid m \\ e_\rho L' \oplus \bigoplus\limits_{d|m} \bigoplus\limits_{\sigma\in V_d} e_\sigma L' & \text{falls } 2 \nmid m \end{cases}$$

Diese Modulzerlegung ist eindeutig, da die e_ρ, $e_{\rho'}$ und e_σ alle primitiven Idempotente sind. Aufgrund der Wahl von V_d und den Eigenschaften der reellen Einbettungen ρ und ρ' erhält man $e_\sigma = e_{\overline{\sigma}} = \overline{e_\sigma}$ sowie $e_\rho = \overline{e_\rho}$ und $e'_\rho = \overline{e'_\rho}$. Damit sind die Zerlegungen sogar orthogonal. Jedes $e_\sigma L'$ ist ein hermitescher $\mathbb{C}$-Vektorraum. Er ist damit diagonalisierbar und zerfällt in eine orthogonale Summe von eindimensionalen Teilräumen $(T, h|_T)$. Die Eindeutigkeit dieser Zerlegung folgt daher aus dem Trägheitssatz von Sylvester für $\mathbb{R}$ und $\mathbb{C}$. Für die Spur auf $\mathbb{R}G$ gilt nach Proposition 1.9 und Proposition 1.21 für alle $x \in \mathbb{R}G$.

$$\mathrm{Spur}_{\mathbb{R}}^{\mathbb{R}G}(x) = \begin{cases} (x)_\rho + (x)_{\rho'} + \sum\limits_{d|m} \sum\limits_{\sigma\in V_d} \mathrm{Spur}_{\mathbb{R}}^{\mathbb{C}}(x)_\sigma & \text{falls } 2 \mid m \\ (x)_\rho + \sum\limits_{d|m} \sum\limits_{\sigma\in V_d} \mathrm{Spur}_{\mathbb{R}}^{\mathbb{C}}(x)_\sigma & \text{falls } 2 \nmid m \end{cases}$$

Die Spurabbildung der Algebra $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$, eingeschränkt auf diese Teilräume, ist gerade die gewöhnliche Spur der Körpererweiterung $\mathbb{C}/\mathbb{R}$. Daher können sie als zweidimensionale reelle Vektorräume mit der Bilinearform $\mathrm{Spur}_{\mathbb{R}}^{\mathbb{C}} \circ h|_T$ aufgefasst werden. Je nachdem, ob $h|_T$

positiv oder negativ definit ist, ist dann auch der reelle Raum positiv oder negativ definit. Die reellen Räume $e_\rho L$ und $e_{\rho'} L$ sind nach dem Trägheitssatz von Sylvester ebenfalls (eindeutig) diagonalisierbar. □

Wie man sieht, ergeben sich Einschränkungen für den Teil des Gitters, auf dem g wie eine Einheitswurzel ζ_d mit $d > 2$ operiert, denn dieser Teil lässt sich nur in zweidimensionale, modulare Komponenten zerlegen.

Korollar 1.39. *Sei (L, b) ein Gitter mit der Signatur (n_+, n_-) und mit einem fixpunktfreien Automorphismus ungerader Ordnung. Dann gilt: $2|n_+$ und $2|n_-$.*

Ausblick: In diesem Kapitel wurde gezeigt, dass die modulare Zerlegung eines $\mathbb{Z}$-Gitters mit einem Automorphismus der Ordnung m im Wesentlichen von den enthaltenen Idealen über $\mathbb{Z}[\zeta_d]$ abhängt. In Kapitel 2 wird mit ihrer Hilfe das Geschlechtssymbol bestimmt. Durch Multiplikation von Primidealen bei der sogenannten Idealgitterkonstruktion werden später in Abschnitt 2.4 Gitter konstruiert, die einen Automorphismus von vorgegebener Ordnung sowie vorgegebene Dimensionen der modularen Komponenten besitzen.

1.3 Eine orthogonale Zerlegung im Fall $p \mid m$

In diesem Abschnitt soll der noch fehlende Fall $p \mid m$ untersucht werden. Als erstes wird für $p = m \neq 2$ eine orthogonale Zerlegung von Λ-Gitter konstruiert und eine Liste mit möglichen Strukturen der orthogonal unzerlegbaren Summanden angegeben. Anschließend wird gezeigt, dass es für $p = 2$ und $p^2|m$ unendlich viele verschiedene, orthogonal unzerlegbare Modulstrukturen mit beliebig großem Rang gibt. Für den gesamten Abschnitt wird $\Lambda := \mathbb{Z}_p G$ und $\Gamma := \mathbb{Z}[\zeta_p]_{1-\zeta_p} \times \mathbb{Z}_p$ definiert.

Als erstes soll die Struktur von Λ-Moduln geklärt werden. Es gilt hier ein Krull-Schmidt Theorem, welches in [Rei61] bewiesen wurde:

Proposition 1.40. *Seien G eine beliebige Gruppe und $M_1, \ldots, M_r, N_1, \ldots, N_s$ unzerlegbare Λ-Moduln mit*

$$M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_s$$

Dann gilt $r = s$ und gegebenenfalls nach Umnummerierung $M_i \cong N_i$.

Damit zerfällt ein Λ-Modul stets in unzerlegbare Teilmoduln und diese Teilmoduln sind eindeutig bestimmt. Die unzerlegbaren Darstellungen sind aber nur für einige bestimmte Gruppen bekannt. Für $|G| \in \{p, p^2\}$ hat Irving Reiner diese bestimmt:

Proposition 1.41. *Sei $|G| = p$. Die unzerlegbaren Λ-Moduln sind bis auf Isomorphie $\mathbb{Z}_p$, $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$ und Λ.*

Einen Beweis dieser Aussage findet man zum Beispiel in [HR62] Proposition 2.6. Damit besitzt jeder Λ-Modul M eine Pseudobasis. Das bedeutet, es existieren Vektoren x_i, y_j und

z_k, sodass

$$M = \bigoplus_i \underbrace{\Lambda\, x_i}_{\cong\Lambda} \bigoplus_j \underbrace{\Lambda\, y_j}_{\cong\mathbb{Z}_p[\zeta_p]} \bigoplus_k \underbrace{\Lambda\, z_k}_{\cong\mathbb{Z}_p}$$

Die unzerlegbaren Darstellungen der zyklischen Gruppe mit Ordnung p^2 über $\mathbb{Z}$ sind in [Rei76] konstruiert worden. Mit dieser Konstruktion können unzerlegbare Darstellungen dieser Gruppe über den die p-adischen ganzen Zahlen gefunden werden. Im weiteren Verlauf werden davon aber nur die beiden unzerlegbaren Teilmoduln $\mathbb{Z}_p[\zeta_p] \cong \mathbb{Z}[\zeta_p]_{1-\zeta_p}$ und $\mathbb{Z}_p[\zeta_{p^2}] \cong \mathbb{Z}[\zeta_{p^2}]_{1-\zeta_{p^2}}$ benötigt. Zunächst soll für $p = m \neq 2$ eine orthogonale Zerlegung in orthogonal unzerlegbare Summanden konstruiert werden. Ein einfaches Beispiel zeigt, dass es im Allgemeinen nicht möglich ist, eine Zerlegung zu finden, die gleichzeitig eine modulare Zerlegung des unterliegenden $\mathbb{Z}_p$-Moduls ist.

Beispiel 1.42. Das Gitter A_{p-1} besitzt einen Automorphismus g der Ordnung p. Es ist als $\mathbb{Z}[\zeta_p]$-Modul von Rang 1 irreduzibel. Seine p-modulare Zerlegung enthält aber eine unimodulare Komponente vom Rang $p-2$ und eine (p)-modulare Komponente vom Rang 1. Es kann also keine g-invariante, p-modulare Zerlegung geben.

Das folgende Lemma beschreibt das orthogonale Abspalten von Teilgittern mit Rang 2. Man kann es zum Beispiel in [Jac62] Proposition 4.2 finden und elementar nachrechnen:

Lemma 1.43. *Es sei (L,h) ein hermitesches Gitter mit Basis $B := \{v_1,\dots,v_n\}$, $n > 2$. Seien $v_i, v_j, v_k \in B$ verschieden. Sind*

$$c(v_i,v_j,v_k) := \frac{h(v_k,v_i)\cdot h(v_j,v_j) - h(v_k,v_j)\cdot h(v_j,v_i)}{h(v_j,v_i)\cdot h(v_i,v_j) - h(v_i,v_i)\cdot h(v_j,v_j)}$$

und

$$d(v_i,v_j,v_k) := \frac{h(v_k,v_j)\cdot h(v_i,v_i) - h(v_k,v_i)\cdot h(v_i,v_j)}{h(v_j,v_i)\cdot h(v_i,v_j) - h(v_i,v_i)\cdot h(v_j,v_j)}$$

für alle $k \notin \{i,j\}$ ganzzahlig, so ist

$$\begin{aligned} & v_i \perp (v_k + c(v_i,v_j,v_k)v_i + d(v_i,v_j,v_k)v_j) \\ \textit{und} \quad & v_j \perp (v_k + c(v_i,v_j,v_k)v_i + d(v_i,v_j,v_k)v_j) \end{aligned}$$

Eine analoge Aussage gilt für quadratische Gitter.

Nun sollen die Darstellungen von Gruppen mit Primzahlordnung betrachtet werden. Die folgende Proposition beschreibt die Einbettung des Gruppenrings in die Maximalordnung (vgl. [Que81] S. 161):

Proposition 1.44. *Für die Einbettung*

$$\begin{aligned} \iota : \Lambda &\hookrightarrow \Gamma \\ g &\mapsto (\zeta_p, 1) \end{aligned}$$

des Gruppenrings Λ in die Maximalordnung Γ gilt:

(a) $I := (1-g)\cdot\Lambda + p\cdot\Lambda \cong (1-\zeta_p)\mathbb{Z}[\zeta_p]_{1-\zeta_p} \times p\mathbb{Z}_p$ *ist das maximale* Γ*-Ideal in* Λ

(b) $\iota(\Lambda)/I \cong \mathbb{F}_p$ *und kann mit der Diagonale in* $\Gamma/I \cong \mathbb{F}_p \times \mathbb{F}_p$ *identifiziert werden.*

Beweis.

(a) ι bildet $1-g$ auf $(1-\zeta_p, 0)$ und $\sum_{i=0}^{p-1} g^i$ auf $\sum_{i=0}^{p-1}(\zeta_p^i, 1) = (0, p)$ ab. Damit ist $\iota|_I$ der gesuchte Isomorphismus. Sei J ein beliebiges Ideal in Γ. Es kann mittels

$$J = (1,0)\cdot J + (0,1)\cdot J$$

in ein Produkt von Idealen zerlegt werden. Weil $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$ und $\mathbb{Z}_p$ lokale Ringe sind, ist J von der Form $(1-\zeta_p)^i \times (p)^j$. Zu prüfen ist nun, welche Ideale in Λ liegen. Falls $i = 0$ ist, ist $J = ((1, p^j))$, aber der Erzeuger liegt nicht in Bild(ι). Ebenso liegt für $j = 0$ der Erzeuger von $J = (((1-\zeta_p)^i, 1))$ nicht in Bild(ι). Da $(1-\zeta_p, p) = \iota(1-g) + \sum_{i=0}^{p-1} \iota(g^i)$ im Bild liegt, ist J für $i = j = 1$, also $J = I$, in Λ. Für alle weiteren $i, j \in \mathbb{N}$ erhält man dann Ideale $J \subsetneqq I \subsetneqq \Lambda$. Damit ist I maximal in Λ.

(b) Die Isomorphie $(\mathbb{Z}[\zeta_p]_{1-\zeta_p} \times \mathbb{Z}_p)/I \cong \mathbb{F}_p \times \mathbb{F}_p$ kann mit Hilfe der Restklassenkörper elementar nachgerechnet werden. Da $\iota(\Lambda)/I \subset \Gamma/I$ ist und I ein maximales Ideal in $\iota(\Lambda)$ ist, muss $\iota(\Lambda)/I$ isomorph zu einem echt in $\mathbb{F}_p \times \mathbb{F}_p$ enthaltenen Körper sein. Dafür kommt nur $\mathbb{F}_p$ in Frage. □

Zur besseren Übersicht wird im weiteren Verlauf Λ als Teilmenge von Γ aufgefasst.

Lemma 1.45. *Sei* $x \in \Gamma$*. Dann gilt:*

$$x \in \Lambda \Leftrightarrow x + I \in \Lambda/I$$

Beweis. "⇒" ist klar. Sei $x+I \in \Lambda/I$ vorgegeben. Dann gibt es ein $y \in \Lambda$ mit $x+I = y+I$. Also ist $x - y \in I$ und aus $I \subseteq \Lambda$ folgt $x \in \Lambda$. □

Lemma 1.46. *Seien* $x, y \in \Lambda \subseteq \Gamma$ *so, dass* $\frac{x}{y} \in \Gamma$ *ist. Dann gilt sogar* $\frac{x}{y} \in \Lambda$*.*

Beweis. Γ ist ein Produkt von lokalen Ringen. Da es für jeden Ring eine Bewertung gibt, kann für alle $c := (c_\zeta, c_1) \in \Gamma$ das Tupel $(\nu_{1-\zeta_p}(c_\zeta), \nu_p(c_1))$ definiert werden. Dies ist keine Bewertung. Sei $(z_\zeta, z_1) := \frac{(x_\zeta, x_1)}{(y_\zeta, y_1)} \in \Gamma$. Dann folgt $\nu_{1-\zeta_p}(x_\zeta) \leq \nu_{1-\zeta_p}(y_\zeta)$ und $\nu_p(x_1) \leq \nu_p(y_1)$. Man schreibt $x_\zeta = \delta_x(1-\zeta_p)^{a_x}$ und $x_1 = \epsilon_x p^{b_x}$. Mit y verfährt man analog. Dann ist $(z_\zeta, z_1) = (\frac{\delta_x}{\delta_y}(1-\zeta_p)^{a_x - a_y}, \frac{\epsilon_x}{\epsilon_y} p^{b_x - b_y})$. Aus Proposition 1.44 folgt:

$$\Lambda/I \cong \mathbb{F}_p \cong \{(\lambda, \lambda) \in \mathbb{F}_p \times \mathbb{F}_p \mid \lambda \in \mathbb{F}_p\} \hookrightarrow \Gamma/I$$

Also ist

$$\overline{x_1} = \overline{\epsilon_x} = \overline{\delta_x} = \overline{x_\zeta}$$
$$\overline{y_1} = \overline{\epsilon_y} = \overline{\delta_y} = \overline{y_\zeta}$$

Da die Projektion auf die Restklasse ein Ringhomomorphismus ist, folgt daher:

$$\overline{z_1} = \overline{(\frac{\epsilon_x}{\epsilon_y})} = (\frac{\overline{\epsilon_x}}{\overline{\epsilon_y}}) = (\frac{\overline{\delta_x}}{\overline{\delta_y}}) = \overline{z_\zeta}$$

Damit ist $(z_\zeta, z_1) + I \in \Lambda + I$ und gemäß Lemma 1.45 ist dann $(z_\zeta, z_1) \in \Lambda$. □

Lemma 1.47. *Es sei ein Λ-Modul M mit der oben angegebenen Pseudobasis x_i, y_j und z_k gegeben. Dann können einzelne Vektoren durch Linearkombinationen so ersetzt werden, dass die neue Menge von Vektoren wieder eine Pseudobasis bildet:*

(a) Man ersetzt x_i durch $x_i'' := x_i + (\lambda_\zeta, \lambda_1)x_j$ für ein $(\lambda_\zeta, \lambda_1) \in \Lambda$. Es gilt $\Lambda x_i'' \cong \Lambda$.

(b) Man ersetzt x_i durch $x_i'' := x_i + (\lambda_\zeta, \lambda_1)y_j$ für ein $(\lambda_\zeta, \lambda_1) \in \Lambda$. Es gilt $\Lambda x_i'' \cong \Lambda$.

(c) Man ersetzt x_i durch $x_i'' := x_i + (\lambda_\zeta, \lambda_1)z_j$ für ein $(\lambda_\zeta, \lambda_1) \in \Lambda$. Es gilt $\Lambda x_i'' \cong \Lambda$.

(d) Man ersetzt y_i durch $y_i'' := y_i + (\lambda_\zeta, 0)x_j$ für ein $(\lambda_\zeta, 0) \in \Lambda \cap (\mathbb{Z}_p[\zeta_p] \times \{0\})$. Es gilt $\Lambda y_i'' \cong \mathbb{Z}_p[\zeta_p]$.

(e) Man ersetzt y_i durch $y_i'' := y_i + (\lambda_\zeta, \lambda_1)y_j$ für ein $(\lambda_\zeta, \lambda_1) \in \Lambda$. Es gilt $\Lambda y_i'' \cong \mathbb{Z}_p[\zeta_p]$.

(f) Man ersetzt z_i durch $z_i'' := z_i + (0, \lambda_1)x_j$ für ein $(0, \lambda_1) \in \Lambda \cap (\{0\} \times \mathbb{Z}_p)$. Es gilt $\Lambda z_k'' \cong \mathbb{Z}_p$.

(g) Man ersetzt z_i durch $z_i'' := z_i + (\lambda_\zeta, \lambda_1)z_j$ für ein $(\lambda_\zeta, \lambda_1) \in \Lambda$. Es gilt $\Lambda z_i'' \cong \mathbb{Z}_p$.

Beweis. Man kann in allen Fällen leicht zeigen, dass die neue Menge wieder ein Erzeugendensystem ist, denn die Vektoren liegen in M und die ursprüngliche Pseudobasis kann mit ihnen erzeugt werden. Zu zeigen ist also noch, dass man nach dem Ersetzen eines Vektors wieder eine Pseudobasis erhält. Dazu bestimmt man den Isomorphietyp mit Hilfe der drei möglichen Annullatoren (0), $(\Phi_p(g))$ und $(g-1)$:

(a) Zu jedem x_i gibt es ein y_i' und ein z_i', sodass $x_i = (y_i', 0) + (0, z_i')$. Ebenso kann $x_j = (y_j', 0) + (0, z_j')$ geschrieben werden. Da x_i und x_j Teil einer Pseudobasis sind, müssen y_i' und y_j' sowie z_i' und z_j' linear unabhängig sein, weil ansonsten $\Lambda x_i \cap \Lambda x_j \neq \{0\}$ wäre. Damit können zwei Annullatoren ausgeschlossen werden:

$$\Phi_p(g)(x_i'') \quad = \quad \sum_{i=0}^{p-1} g^k(x_i + (\lambda_\zeta, \lambda_1)x_j) = (0, p(z_i' + \lambda_1 z_j'))$$

Weil z_i' und z_j' linear unabhängig sind, ist $(0, p(z_i' + \lambda_1 z_j')) \neq (0,0)$ und $(\Phi_p(g))$ kann nicht der Annullator sein.

$$(g-1)(x_i'') \quad = \quad (g-1)(x_i + (\lambda_\zeta, \lambda_1)x_j) = ((g-1)(y_i' + \lambda_\zeta y_j'), 0)$$

Weil g auf y_i' und y_j' nicht-trivial operiert, ist $((g-1)(y_i' + \lambda_\zeta y_j'), 0) \neq (0,0)$. Der Annullator kann also auch nicht $(g-1)$ sein. Daher muss es (0) sein und $\Lambda x_i'' \cong \Lambda$ gelten.

(d) Es gilt:

$$\begin{aligned}\Phi_p(g)(y_i'') &= \sum_{i=1}^{p-1} g^i(y_i'') = \sum_{i=1}^{p-1} g^i(y_i + (\lambda_\zeta, 0)x_j) = (\sum_{i=1}^{p-1}(g^i(y_i)) + \lambda_\zeta \sum_{i=1}^{p-1}(g^i(y_j'), 0) \\ &= (0,0)\end{aligned}$$

Also ist $\mathrm{Ann}_\Lambda(y_i'') = (\Phi_p(g))$ und das neue Erzeugendensystem eine Pseudobasis. Des Weiteren gilt $\Lambda y_j'' \cong \mathbb{Z}[\zeta_p]_{1-\zeta_p}$.

Die Fälle (b) und (c) können analog zu (a) bewiesen werden und die Fälle (e), (f) und (g) analog zu (d). Weil sich in keinem Fall der Isomorphietyp durch das Modifizieren eines Vektors ändert, bilden die neuen Vektoren eine Pseudobasis. □

Lemma 1.48. *Sei (L,h) ein Λ-Gitter. Für Vektoren $y,z \in L$ mit $\Lambda y \cong \mathbb{Z}[\zeta_p]_{1-\zeta_p}$ und $\Lambda z \cong \mathbb{Z}_p$ gilt: $\Lambda(y+z) \cong \Lambda$.*

Beweis. $\Lambda(y+z)$ hat den Λ-Rang 1 und muss nach Proposition 1.41 eine der folgenden Modulstrukturen besitzen:

$$\Lambda, \quad \mathbb{Z}[\zeta_p]_{1-\zeta_p} \quad \mathbb{Z}_p$$

Da die $g^i(y)$ verschieden sind, kann die Modulstruktur nicht $\mathbb{Z}_p$ sein. Weil $\sum_{i=0}^{p-1} g^i(y+z) = \sum_{i=0}^{p-1} g^i(y) + \sum_{i=0}^{p-1} g^i(z) = pz \neq 0$ ist, kann die Modulstruktur nicht $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$ sein. Also muss $\Lambda(y+z) \cong \Lambda$ sein. □

Lemma 1.48 liefert eine Methode, mit der man Λ-Moduln mit vorgegebener Modulstruktur konstruieren kann. Damit sollen nun Moduln konstruiert werden, die eine weitere Eigenschaft besitzen:

Definition 1.49. Seien $i,j,k \in \mathbb{N}_0 \cup \{-1\}$, sodass entweder $i<j$ oder $i=j=-1$ gilt. Ein Λ-Gitter L heißt (i,j,k)**-modular**, wenn für $\Gamma \otimes_\Lambda L = L^\zeta \perp L^1$ die folgenden Bedingungen erfüllt sind:

(i)
- Falls $k \neq -1$ ist, ist L^ζ $((1-\zeta_p)^k)$-modular.
- Falls $k=-1$ ist, ist $L^\zeta = \{0\}$.

(ii)
- Falls $i=j=-1$ ist, ist $L^1 = \{0\}$.
- Falls $-1=i<j$ ist, ist L^1 (p^j)-modular.
- Falls $-1<i<j$ ist, gibt es ein (p^i)-modulares $\mathbb{Z}_p$-Gitter L_1^1 und ein (p^j)-modulares $\mathbb{Z}_p$-Gitter L_2^1 mit $L^1 = L_1^1 \perp L_2^1$.

Definition 1.50.

(1) $U_1(j)$ sei das $\mathbb{Z}_p$-Gitter mit der Gram-Matrix

$$\begin{pmatrix} p^j \end{pmatrix}$$

Es kann insbesondere als $(-1,j,-1)$-modulares Λ-Gitter aufgefasst werden und besitzt die Modulstruktur $\mathbb{Z}_p$.

(2) $U_2(k)$ sei das $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter mit der Gram-Matrix

$$\left((1-\zeta_p)^k\right)$$

Es kann insbesondere als $(-1,-1,k)$-modulares Λ-Gitter aufgefasst werden und besitzt die Modulstruktur $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$.

(3) Es seien $U_3^1(j) := U_1(j)$ und $U_3^\zeta(k) := U_2(k)$ definiert. Des Weiteren seien z' eine Basis von $U_3^1(j)$ und $\{y'\}$ eine Basis von $U_3^\zeta(k)$. Dann besitzt das $(-1,j,k)$-modulare Gitter $U_3(j,k) := \mathrm{Spann}_\Lambda\{y' \oplus z'\}$ nach Lemma 1.48 die Λ-Modulstruktur Λ.

(4) $U_4^1(j)$ sei das $\mathbb{Z}_p$-Gitter, das durch die folgende Gram-Matrix definiert ist:

$$\begin{pmatrix} 0 & p^j \\ p^j & 0 \end{pmatrix}$$

Die Basis des Gitters sei $\{z, z'\}$. Des Weiteren sei $U_4^\zeta(k) := U_2(k)$ mit Basis $\{y'\}$ gegeben. Damit besitzt das $(-1,j,k)$-modulare Gitter $U_4(j,k) := \mathrm{Spann}_\Lambda\{y' \oplus z', 0 \oplus z\}$ nach Lemma 1.48 die Λ-Modulstruktur $\Lambda \oplus \mathbb{Z}_p$.

(5) Sei $U_5(k)$ das $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter mit der folgenden Gram-Matrix:

$$\begin{pmatrix} 0 & (1-\zeta_p)^k \\ \overline{(1-\zeta_p)^k} & 0 \end{pmatrix}$$

Es kann insbesondere als $(-1,-1,k)$-modulares Λ-Gitter aufgefasst werden und besitzt die Modulstruktur $\mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}$.

(6) Seien $U_6^1(j) := U_1(j)$ mit Basis $\{z'\}$ und $U_6^\zeta(k) := U_5(k)$ mit Basis $\{y, y'\}$. Dann besitzt das $(-1,j,k)$-modulare Gitter $U_6(j,k) := \mathrm{Spann}_\Lambda\{y' \oplus z', y \oplus 0\}$ nach Lemma 1.48 die Λ-Modulstruktur $\Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}$.

(7) Seien $U_1(i)$ und $U_1(j)$ mit Basen $\{z\}$ beziehungsweise $\{z'\}$ gegeben. Des Weiteren sei $U_7^\zeta(k) := U_5(k)$ mit Basis $\{y, y'\}$. Dann besitzt $U_7(i,j,k) := \mathrm{Spann}_\Lambda\{y' \oplus z', y \oplus 0, 0 \oplus z\}$ nach Lemma 1.48 die Λ-Modulstruktur $\Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}_p$. Falls $i \neq j$ ist, ist das Gitter (i,j,k)-modular. Andernfalls ist es $(-1,j,k)$-modular.

(8) Seien $\mathbb{Z}_p$-Gitter $U_1(i)$ und $U_1(j)$ mit Basen $\{z_1'\}$ beziehungsweise $\{z_2'\}$ gegeben. Man definiert $U_8^1(i) := U_1(i) \perp U_1(j)$ sowie $U_8^\zeta(k) := U_5(k)$ mit Basis $\{y_1', y_2'\}$ Dann besitzt das Gitter $U_8(i,j,k) := \mathrm{Spann}_\Lambda\{y_1' \oplus z_1', y_2' \oplus z_2'\}$ nach Lemma 1.48 die Λ-Modulstruktur $\Lambda \oplus \Lambda$. Es ist (i,j,k)-modular oder $(-1,j,k)$-modular.

(9) Seien $U_4^1(i)$ mit Basis $\{z_1, z_1'\}$ und $U_1(j)$ mit Basis $\{z_2'\}$ gegeben. Des Weiteren seien $U_9^\zeta(k) := U_5(k)$ mit Basis $\{y_1', y_2'\}$ und $U_9^1(i) := U_4^1(i) \perp U_1^1(j)$. Dann besitzt das Gitter $U_9(i,j,k) := \mathrm{Spann}_\Lambda\{y_1' \oplus z_1', y_2' \oplus z_2', 0 \oplus z_1\}$ nach Lemma 1.48 die Λ-Modulstruktur $\Lambda \oplus \Lambda \oplus \mathbb{Z}_p$. Es ist (i,j,k)-modular oder $(-1,j,k)$-modular.

(10) Seien $U_4^1(i)$ mit Basis $\{z_1, z_1'\}$ und $U_4^1(j)$ mit Basis $\{z_2, z_2'\}$ sowie $U_{10}^\zeta(k) := U_5(k)$ mit Basis $\{y_1', y_2'\}$ und $U_{10}^1(i) := U_4^1(i) \perp U_4^1(j)$ gegeben. Dann besitzt das Gitter $U_{10}(i,j,k) := \mathrm{Spann}_\Lambda\{y_1' \oplus z_1', y_2' \oplus z_2', 0 \oplus z_1, 0 \oplus z_2\}$ nach Lemma 1.48 die Λ-Modulstruktur $\Lambda \oplus \Lambda \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Es ist (i,j,k)-modular oder $(-1,j,k)$-modular.

Proposition 1.51.

(a) Die Λ-Gitter $U_1(j)$, $U_2(k)$, $U_3(j,k)$ und $U_4(j,k)$ sind für alle $j,k \in \mathbb{N}_0$ orthogonal unzerlegbar.

(b) Die Λ-Gitter $U_5(k)$, $U_6(j,k)$, $U_7(j,k)$, $U_8(i,j,k)$, $U_9(i,j,k)$ und $U_{10}(i,j,k)$ sind für alle $i,j,k \in \mathbb{N}$ mit $2 \nmid k$ orthogonal unzerlegbar.

Beweis.

(a) Nach Proposition 1.41 sind die Gitter $U_1(j)$, $U_2(k)$ und $U_3(j,k)$ unzerlegbar und damit auch orthogonal unzerlegbar. Seien M_1 und M_2 Λ-Moduln mit $U_4(j,k) = M_1 \perp M_2$. Dann ist $\Gamma \otimes_\Lambda U_4(j,k) = (M_1^1 \perp M_2^1) \perp (M_1^\zeta \perp M_2^\zeta)$. Da $U_4^\zeta(k) = U_2(k)$ orthogonal unzerlegbar ist, muss o.B.d.A. $M_1^\zeta = \{0\}$ sein. Damit muss aber $M_1^1 = \{0\}$ oder $M_1^1 = \mathrm{Spann}_\Lambda\{z\}$ sein, denn ansonsten erhielte man eine orthogonale Zerlegung von $\mathrm{Spann}_\Lambda\{y' \oplus z'\} \cong \Lambda$. Wenn $M_1^1 = \{0\}$ ist, folgt $M_1 = \{0\}$ und damit die Behauptung. Angenommen es wäre $M_1^1 = \mathrm{Spann}_\Lambda\{z\}$. Dann würde man von $U_4^1(i)$ eine Orthogonalbasis der Form $B := \{z, \mu z + \mu' z'\}$ erhalten und es folgte:

$$0 = b(z, \mu z + \mu' z') = \mu b(z,z) + \mu' b(z,z') = \mu' p^i$$

Damit wäre $\mu' = 0$, was einen Widerspruch zur Orthogonalbasis B liefert. Also muss $M_1^1 = \{0\}$ sein und damit ist auch $M_1 = \{0\}$.

(b) Der Beweis der orthogonalen Unzerlegbarkeit verläuft bei U_5 bis U_{10} ähnlich. Daher wird dies nur für U_{10} mit der oben angegebenen Basis gezeigt. Seien M_1 und M_2 Λ-Moduln mit $U_{10}(i,j,k) = M_1 \perp M_2$. Dann gilt $\Gamma \otimes_\Lambda U_{10}(i,j,k) = (M_1^1 \perp M_2^1) \perp (M_1^\zeta \perp M_2^\zeta)$. Wegen $2 \nmid k$ ist $U_{10}^\zeta(k)$ nach 1.32 orthogonal unzerlegbar. Sei also o.B.d.A. $M_1^\zeta = \{0\}$. Dann müssen $z_1', z_2' \in M_2^1$ liegen, weil $z_1' \in M_1^1$ oder $z_2' \in M_1^1$ eine orthogonale Zerlegung von $\mathrm{Spann}_\Lambda\{y_1' \oplus z_1'\} \cong \Lambda$ oder $\mathrm{Spann}_\Lambda\{y_2' \oplus z_2'\} \cong \Lambda$ implizieren würde. Analog zu (a) kann man dann zeigen, dass auch $z_1, z_2 \in M_2^1$ sein müssen. Damit ist $M_1 = \{0\}$. □

Satz 1.52. *Sei p eine ungerade Primzahl. Jeder hermitesche Λ-Modul (L,h) kann als orthogonale Summe von (i,j,k)-modularen Teilmoduln mit den folgenden Modulstrukturen geschrieben werden: $\mathbb{Z}_p$, $\mathbb{Z}_p[\zeta_p]$, Λ, $\Lambda \oplus \mathbb{Z}_p$, $\mathbb{Z}_p[\zeta_p] \oplus \mathbb{Z}_p[\zeta_p]$, $\Lambda \oplus \mathbb{Z}_p[\zeta_p]$, $\Lambda \oplus \Lambda$, $\Lambda \oplus \mathbb{Z}_p[\zeta_p] \oplus \mathbb{Z}_p$, $\Lambda \oplus \Lambda \oplus \mathbb{Z}_p$ und $\Lambda \oplus \Lambda \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$*

Beweis. (i) Man wählt sich gemäß Proposition 1.41 eine Pseudobasis:

$$L = \bigoplus \underbrace{\Lambda x_i}_{\cong \Lambda} \oplus \bigoplus \underbrace{\Lambda y_i}_{\cong \mathbb{Z}_p[\zeta_p]} \oplus \bigoplus \underbrace{\Lambda z_i}_{\cong \mathbb{Z}_p}$$

Erweitert man nun den Grundring des Gitters zu Γ, so zerfällt gemäß Lemma 1.15 das Gitter $(\Gamma \otimes_\Lambda L, h) = (L^\zeta, h^\zeta) \perp (L^1, b^1)$. Des Weiteren gibt es zu jedem x_i ein $y_i' \in L^\zeta$ und $z_i' \in L^1$, sodass $x_i = (y_i', 0) + (0, z_i')$. Man definiert

$$\begin{aligned} X &:= \{x_1, \ldots, x_{n_g}\} \\ Y &:= \{y_1, \ldots, y_{n_\zeta}\} \qquad Y' := \{y_1', \ldots, y_{n_g}'\} \\ Z &:= \{z_1, \ldots, z_{n_1}\} \qquad Z' := \{z_1', \ldots, z_{n_g}'\} \end{aligned}$$

$Y \cup Y'$ ist eine Basis von L^ζ und $Z \cup Z'$ ist eine Basis von L^1. Durch Übergang zur Maximalordnung erhält man eine Zerlegung in Gitter über lokalen Ringen. Die Teilgitter besitzen zwar eine modulare Zerlegung, aber die orthogonale Zerlegung der Teilgitter lässt nur unter bestimmten Umständen Rückschlüsse auf eine orthogonale Zerlegung von L zu. Daher wird es das Ziel sein, die Pseudobasis von L so zu verändern, dass beim Übergang zu $\Gamma \otimes_\Lambda L$ möglichst viele Basisvektoren in L^1 und L^ζ orthogonal zueinander sind. Damit erhält man dann sofort eine orthogonale Zerlegung von L.

(ii) Falls $Y' = \emptyset$ ist und damit auch $Z' = \emptyset$ gilt, folgt $L \cong L^1 \perp L^\zeta$. Wegen $p \neq 2$ kann man sich eine Orthogonalbasis von L^1 wählen und erhält damit Summanden der Form $\mathbb{Z}_p$. Für L^ζ kann nach Proposition 1.32 eine modulare Zerlegung gefunden werden. Demnach zerfallen hermitesche $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter wie (L^ζ, h^ζ) stets in eine orthogonale Summe von modularen Teilgittern von Rang 1 oder Rang 2. Da solche Gitter im Allgemeinen keine Orthogonalbasis besitzen, können orthogonale Summanden der Form $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$ und $\mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}$ auftreten. Im Folgenden wird also angenommen, dass $Y' \neq \emptyset$ und $Z' \neq \emptyset$ ist.

(iii) Man betrachte zunächst die minimalen Elemente der Menge

$$H_1 := \{\nu_p(b^1(v, w)) \mid v, w \in Z \cup Z'\}$$

Die Pseudobasis von L soll so verändert werden, dass in H_1, gebildet mit Hilfe der neuen Pseudobasis, Elemente einer bestimmten Form nicht auftreten. Falls es etwa ein Element der Form $\nu_p(b^1(z_j, z_k)) < \min\{\nu_p(b^1(z_j, z_j)), \nu_p(b^1(z_k, z_k))\}$ gibt, so ersetzt man die Vektoren z_j und z_k schrittweise durch $z_j'' := z_j + z_k$ und $z_k'' := z_j - z_k$. Diese Vektoren liegen offensichtlich in L. Weil $p \neq 2$ ist, kann man mit ihnen die ursprüngliche Pseudobasis durch $z_j = \frac{1}{2}(z_j'' + z_k'')$ und $z_k = \frac{1}{2}(z_j'' - z_k'')$ erzeugen. Nach Lemma 1.47 (g) bilden auch die neuen Vektoren eine Pseudobasis. Bildet man bezüglich diesem die Menge H_1, so enthält sie wegen $\nu_p(b^1(z_j + z_k, z_j + z_k)) = \nu_p(b^1(z_j, z_k))$ und $\nu_p(b^1(z_j - z_k, z_j - z_k)) = \nu_p(b^1(z_j, z_k))$ ein minimales Element mit der obigen Eigenschaft weniger. Wenn in H_1 ein Element mit der Eigenschaft $\nu_p(b^1(z_j', z_k')) < \min\{\nu_p(b^1(z_j', z_j')), \nu_p(b^1(z_k', z_k'))\}$ existiert, so ersetzt man die Vektoren x_j und x_k schrittweise durch $x_j'' := x_j + x_k$ und $x_k'' := x_j - x_k$. Auch diese Vektoren liegen offensichtlich in L. Weil $p \neq 2$ ist, kann man mit ihnen die ursprüngliche Pseudobasis durch $x_j = \frac{1}{2}(x_j'' + x_k'')$ und $x_k = \frac{1}{2}(x_j'' - x_k'')$ erzeugen. Also bilden gemäß Lemma 1.47 (a) auch die neuen Vektoren eine Pseudobasis. Weil $\nu_p(b^1(z_j' + z_k', z_j' + z_k')) = \nu_p(b^1(z_j', z_k'))$ und $\nu_p(b^1(z_j' - z_k', z_j' - z_k')) = \nu_p(b^1(z_j', z_k'))$ ist, enthält die Menge H_1, gebildet mit der neuen

Pseudobasis, ein minimales Element mit der obigen Eigenschaft weniger. Elemente der Form $\nu_p(b^1(z'_j, z_k)) < \min\{\nu_p(b^1(z'_j, z'_j)), \nu_p(b^1(z_k, z_k))\}$ können nicht entfernt werden und führen zu orthogonal unzerlegbaren Teilgittern, wie in Proposition 1.51 bereits erläutert wurde.
(iv) Es wird im weiteren Verlauf des Beweises davon ausgegangen, dass es in H_1 durch wiederholtes Anwenden von Schritt (iii) keine Elemente mit den unerwünschten Eigenschaften gibt. Die Pseudobasis von L soll jetzt schrittweise so verändert werden, dass sie eine orthogonale Zerlegung von L^1 in Teilgitter mit Rang 1 oder 2 induziert. Sollte es in H_1 ein minimales Element der Form $\nu_p(b^1(z_j, z_j))$ geben, definiert man

$$\begin{aligned} x''_i &:= x_i - \tfrac{h(x_i,z_j)}{h(z_j,z_j)+(1-\zeta_p,0)}\ z_j \quad \text{für } 1 \le i \le n_g \\ y''_i &:= y_i \qquad\qquad\qquad\qquad\quad \text{für } 1 \le i \le n_\zeta \\ z''_i &:= z_i - \tfrac{h(z_i,z_j)}{h(z_j,z_j)+(1-\zeta_p,0)}\ z_j \quad \text{für } 1 \le i \le n_1, i \ne j \end{aligned}$$

Weil $h(z_j, z_j) \in \{0\} \times \mathbb{Z}_p$ ist, muss der Nenner so modifiziert werden, dass er kein Nullteiler ist, aber im Gruppenring liegt. Nach Voraussetzung liegt $h(z_j, z_j)$ im Gruppenring und es gilt $(1 - \zeta_p, 0) \in I \subseteq \Lambda$. Die Brüche $\frac{b^1(z'_i,z_j)}{b^1(z_j,z_j)}$ besitzen aufgrund der Wahl von z_j Werte in $\mathbb{Z}_p$. Damit sind $\frac{h(x_i,z_j)}{h(z_j,z_j)+(1-\zeta_p,0)} = (0, \frac{b^1(z'_i,z_j)}{b^1(z_j,z_j)}) \in \Gamma$. Nach Lemma 1.46 muss der Bruch sogar in Λ liegen. Für den zweiten Bruch kann dies ähnlich nachgerechnet werden. Damit kann durch mehrmaliges Anwenden von Lemma 1.47 (c) und (g) gezeigt werden, dass die neuen Vektoren wieder eine Pseudobasis bilden. Des Weiteren gilt:

$$\begin{aligned} h(x''_i, z_j) &= h(x_i - \frac{h(x_i, z_j)}{h(z_j, z_j) + (1 - \zeta_p, 0)}\ z_j, z_j) \\ &= h(x_i, z_j) - \frac{h(x_i, z_j)}{h(z_j, z_j) + (1 - \zeta_p, 0)}\ h(z_j, z_j) \\ &= (0, b^1(z'_i, z_j)) - \frac{(0, b^1(z'_i, z_j))}{(1 - \zeta_p, b^1(z_j, z_j))}\ (0, b^1(z_j, z_j)) = (0, 0) \\ h(y''_i, z_j) &= (0, 0) \quad \text{nach Lemma 1.15} \\ h(z''_i, z_j) &= h(z_i - \frac{h(z_i, z_j)}{h(z_j, z_j) + (1 - \zeta_p, 0)}\ z_j, z_j) \\ &= h(z_i, z_j) - \frac{h(z_i, z_j)}{h(z_j, z_j) + (1 - \zeta_p, 0)}\ h(z_j, z_j) \\ &= (0, b^1(z_i, z_j)) - \frac{(0, b^1(z_i, z_j))}{(1 - \zeta_p, b^1(z_j, z_j))}\ (0, b^1(z_j, z_j)) = (0, 0) \end{aligned}$$

Damit steht z_j senkrecht auf den anderen Vektoren der Pseudobasis und man erhält einen orthogonalen $(-1, \nu_p(b^1(z_j, z_j)), -1)$-modularen Summanden $\mathrm{Spann}_\Lambda\{z_j\} \cong \mathbb{Z}_p$, der sofort abgespalten werden kann.
(v) Es werde nun angenommen, dass es ein minimales Element der Form $\nu_p(b^1(z'_j, z'_j))$ gibt. Da es möglich ist, dass das zugehörige y'_j isotrop ist, muss sichergestellt werden, dass nicht durch einen Nullteiler geteilt wird. Dafür wird ein Element benötigt, das in der zweiten Komponente Null ist, damit die orthogonale Projektion nicht verändert wird, und gleichzeitig in Λ liegt. Ein solches Element ist zum Beispiel:

$$\delta_j := \begin{cases} (1-\zeta_p,0)^2 & \text{falls } \nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)+(1-\zeta_p)) > \nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)) \\ (1-\zeta_p,0) & \text{sonst} \end{cases}$$

Damit kann nun die modifizierte orthogonale Projektion der Vektoren definiert werden:

$$\begin{array}{lll} x''_i & := x_i - \frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j & \text{für } 1 \le i \le n_g, i \ne j \\ y''_i & := y_i & \text{für } 1 \le i \le n_\zeta \\ z''_i & := z_i - \frac{h(z_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j & \text{für } 1 \le i \le n_1 \end{array}$$

Die Nenner sind als Summe von Elementen des Gruppenrings selbst wieder im Gruppenring. Falls $h(x_j,x_j) \in I$ ist, muss $b^1(z'_j,z'_j) \in p\cdot\mathbb{Z}_p$ sein. Nach Wahl von x_j folgt damit auch $b^1(z'_i,z'_j) \in p\cdot\mathbb{Z}_p$. Weil $h(x_i,x_j) \in \Lambda$ ist, muss die Restklasse in Λ/I gerade $(\overline{0},\overline{0})$ sein. Also muss auch $h(x_i,x_j) \in I$ sein und $\nu_{1-\zeta_p}(h^\zeta(y'_i,y'_j)) \ge 1$ gelten. Wegen $\nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)) \ge 1$ folgt aus der Wahl von δ, dass $\nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)+(1-\zeta_p)) = 1$ beziehungsweise $\nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)+(1-\zeta_p)^2) = 1$ ist. Also besitzt der erste Bruch Werte in Γ. Falls $h(x_j,x_j) \notin I$ ist, muss $h(x_j,x_j)+I$ von der Form $(\overline{a},\overline{a})$ für $a \in \mathbb{F}_p^*$ sein und damit gilt $\nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)) = \nu_p(b^1(z'_j.z'_j)) = 0$. Also ist $\nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)) = 0 \le \nu_{1-\zeta_p}(h^\zeta(y'_i,y'_j))$ und nach Wahl von x_j auch $\nu_p(b^1(z'_j,z'_j)) \le \nu_p(b^1(z'_i,z'_j))$. Damit ist auch in diesem Fall der erste Bruch in Γ. Analog kann dies auch für den zweiten Bruch nachgewiesen werden. Wegen $h(z_i,x_j) \in \{0\}\times\mathbb{Z}_p$ kann der Beweis jedoch abgekürzt werden. Mit Lemma 1.46 folgt, dass die Brüche sogar in Λ liegen. Durch mehrmaliges Anwenden von Lemma 1.47 (c) und (g) kann damit gezeigt werden, dass die neuen Vektoren wieder eine Pseudobasis bilden. Des Weiteren gilt für die neue Pseudobasis:

$$\begin{aligned} h(x''_i,x_j) &= h(x_i - \frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j, x_j) = h(x_i,x_j) - \frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j}\, h(x_j,x_j) \\ &= (h^\zeta(y'_i,y'_j), b^1(z'_i,z'_j)) - \frac{(h^\zeta(y'_i,y'_j), b^1(z'_i,z'_j))}{(h^\zeta(y'_i,y'_j), b^1(z'_j,z'_j))+\delta_j}\, (h^\zeta(y'_i,y'_j), b^1(z'_j,z'_j)) \\ &= (h^\zeta(y'_i,y'_j) - \frac{h^\zeta(y'_i,y'_j)}{h^\zeta(y'_i,y'_j)+\delta_j^\zeta}\, h^\zeta(y'_i,y'_j), 0) \\ h(y''_i,x_j) &= (h^\zeta(y_i,y'_j),0) \\ h(z''_i,x_j) &= h(z_i - \frac{h(z_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j, x_j) = h(z_i,x_j) - \frac{h(z_i,x_j)}{h(x_j,x_j)+\delta_j}\, h(x_j,x_j) \\ &= (0, b^1(z_i,z'_j)) - \frac{(0,b^1(z_i,z'_j))}{(h^\zeta(y'_j,y'_j), b^1(z'_j,z'_j))+\delta_j}\, (h^\zeta(y'_j,y'_j), b^1(z'_j,z'_j)) \\ &= (0,0) \end{aligned}$$

Damit ist x_j ein Vektor, dessen L^1-Anteil z'_j orthogonal zu den L^1-Anteilen der übrigen Vektoren des neuen Erzeugendensystems ist. Um eine Zerlegung in möglichst kleine Komponenten zu erhalten, wiederholt man die Schritte (iv) und (v) schrittweise für die übrigen Vektoren der Pseudobasis, bis es keine minimalen Elemente der jeweiligen Form gibt.

(vi) Sollte es ein minimales Element der Form $\nu_p(b^1(z_j, z_k'))$ geben, definiert man für Vektoren v_i, v_j, v_k, angelehnt an die Notation aus Lemma 1.43:

$$\begin{array}{rll} N(v_i,v_j) & := (N^\zeta(v_i,v_j), N^1(v_i,v_j)) & := h(v_j,v_i)\cdot h(v_i,v_j) - h(v_i,v_i)\cdot h(v_j,v_j) \\ c'(v_i,v_j,v_k) & := (c^\zeta(v_i,v_j,v_k), c^1(v_i,v_j,v_k)) & := h(v_k,v_i)\cdot h(v_j,v_j) - h(v_k,v_j)\cdot h(v_j,v_i) \\ d'(v_i,v_j,v_k) & := (d^\zeta(v_i,v_j,v_k), d^1(v_i,v_j,v_k)) & := h(v_k,v_j)\cdot h(v_i,v_i) - h(v_k,v_i)\cdot h(v_i,v_j) \end{array}$$

Der gemeinsame Nenner N ist in diesem Fall stets ein Nullteiler. Daher muss er mit einem Element des Gruppenrings modifiziert werden. Weil $c'(z_j,x_k,x_i), d'(z_j,x_k,x_i), N(z_j,x_k) \in \{0\}\times\mathbb{Z}_p$ sind, kann dies in diesem Fall leicht erreicht werden:

$$\begin{array}{lll} x_i'' & := x_i + \frac{c'(z_j,x_k,x_i)}{N(z_j,x_k)+(1-\zeta_p,0)}\ z_j + \frac{d'(z_j,x_k,x_i)}{N(z_j,x_k)+(1-\zeta_p,0)}\ x_k & \text{für } 1\le i\le n_g, i\neq k \\ y_i'' & := y_i & \text{für } 1\le i\le n_\zeta \\ z_i'' & := z_i + \frac{c'(z_j,x_k,z_i)}{N(z_j,x_k)+(1-\zeta_p,0)}\ z_j + \frac{d'(z_j,x_k,z_i)}{N(z_j,x_k)+(1-\zeta_p,0)}\ x_k & \text{für } 1\le i\le n_1, i\neq j \end{array}$$

Man betrachte nun den Bruch $\frac{c'(z_j,x_k,x_i)}{N(z_j,x_k)+(1-\zeta_p,0)}$. Der Nenner ist als Summe von Elementen des Gruppenrings selbst wieder im Gruppenring. Nach Wahl von z_j, x_k ist die zweite Komponente stets in $\mathbb{Z}_p$ enthalten. Daher ist $\frac{c'(z_j,x_k,x_i)}{N(z_j,x_k)+(1-\zeta_p,0)} \in \{0\}\times\mathbb{Z}_p \subseteq \Gamma$ und aus Lemma 1.46 folgt, dass der Bruch sogar in Λ liegen muss. Dies kann analog auch für die anderen Brüche gezeigt werden. Nach mehrmaligem Anwenden von Lemma 1.47 (c) und (g) folgt, dass die neuen Vektoren wieder eine Pseudobasis bilden. Des Weiteren folgt aus Lemma 1.43, angewendet auf die zweite Komponente:

$$\begin{array}{lll} h(z_j,x_i'') & = h(\frac{0}{1-\zeta_p},0) = (0,0) & \text{für } 1\le i\le n_g, i\neq j \\ h(x_k,x_i'') & = h(\frac{0}{1-\zeta_p},0) = (0,0) & \text{für } 1\le i\le n_g, i\neq k \\ h(z_j,y_i'') & = (0,0) & \text{nach Lemma 1.15} \\ h(x_k,y_i'') & \in (\mathbb{Z}[\zeta_p]_{1-\zeta_p}\times\{0\})\cap\Lambda & \text{nach Lemma 1.15} \\ h(z_j,z_i'') & = h(\frac{0}{1-\zeta_p},0) = (0,0) & \text{für } 1\le i\le n_1, i\neq j \\ h(x_k,z_i'') & = h(\frac{0}{1-\zeta_p},0) = (0,0) & \text{für } 1\le i\le n_1, i\neq k \end{array}$$

Damit ist der L^1-Anteil von $\mathrm{Spann}_\Lambda\{z_j,x_k\} \cong \Lambda\oplus\mathbb{Z}_p$ orthogonal zu den L^1-Anteilen der anderen Vektoren der neuen Pseudobasis.

(vii) Durch wiederholtes Anwenden der Schritte (iv), (v) und (vi) kann die Pseudobasis von L so abgeändert werden, dass sie eine orthogonale Zerlegung von L^1 in Teilgitter der Form $\mathrm{Spann}_{\mathbb{Z}_p}\{z_j\}$, $\mathrm{Spann}_{\mathbb{Z}_p}\{z_j'\}$ und $\mathrm{Spann}_{\mathbb{Z}_p}\{z_j,z_k'\}$ induziert. Im weiteren Verlauf soll dies für die Pseudobasis vorausgesetzt werden. Dabei kann man, wie in (iv) beschrieben wurde, $(-1,\nu_p(b^1(z_j,z_j)),-1)$-modulare Teilgitter des Typs $\mathrm{Spann}_\Lambda\{z_j\}\cong\mathbb{Z}_p$ unmittelbar orthogonal abspalten. Die verbleibenden Vektoren der Pseudobasis spannen dann das orthogonale Komplement auf. Sei

$$H_\zeta := \{\nu_{1-\zeta_p}(h^\zeta(v,w)) \mid v,w\in Y\cup Y'\}$$

Man betrachtet wieder die minimalen Elemente dieser Menge. Falls es ein minimales Element der Form $\nu_{1-\zeta_p}(h^\zeta(y_j,y_j))$ gibt, wird die Pseudobasis wie folgt modifiziert:

$$\begin{array}{lll} x_i'' & := x_i - \frac{h(x_i,y_j)}{h(y_j,y_j)+(0,p)}\ y_j & \text{für } 1 \le i \le n_g \\ y_i'' & := y_i - \frac{h(y_i,y_j)}{h(y_j,y_j)+(0,p)}\ y_j & \text{für } 1 \le i \le n_\zeta, i \ne j \\ z_i'' & := z_i & \text{für } 1 \le i \le n_1 \end{array}$$

Aufgrund der Wahl von y_j gilt:

$$\frac{h(x_i,y_j)}{h(y_j,y_j)+(0,p)} = \frac{(h^\zeta(y_i',y_j),0)}{(h^\zeta(y_j,y_j),p)} = (\frac{h^\zeta(y_i',y_j)}{h^\zeta(y_j,y_j)},0) \in \Gamma$$

Damit liegt der Bruch nach Lemma 1.46 in Λ. Für den zweiten Bruch gilt dies analog. Also bilden die neuen Vektoren nach schrittweiser Anwendung von Lemma 1.47 (b) und (e) wieder eine Pseudobasis, für die gilt:

$$\begin{array}{lll} h(x_i'',y_j) & = h(x_i,y_j) - \frac{h(x_i,y_j)}{h(y_j,y_j)+(0,p)}\ h(y_j,y_j) = (h^\zeta(y_i',y_j) - \frac{h^\zeta(y_i',y_j)}{h^\zeta(y_j,y_j)}\ h^\zeta(y_j,y_j),0) \\ & = (0,0) & \\ h(y_i'',y_j) & = h(y_i,y_j) - \frac{h(y_i,y_j)}{h(y_j,y_j)+(0,p)}\ h(y_j,y_j) = (h^\zeta(y_i,y_j) - \frac{h^\zeta(y_i,y_j)}{h^\zeta(y_j,y_j)}\ h^\zeta(y_j,y_j),0) \\ & = (0,0) & \\ h(z_i'',y_j) & = (0,0) \quad \text{nach Lemma 1.15} & \end{array}$$

Damit erhält man einen $(-1,-1,\nu_{1-\zeta_p}(h^\zeta(y_j,y_j)))$-modularen, orthogonalen Summanden $\text{Spann}_\Lambda\{y_j\} \cong \mathbb{Z}[\zeta_p]_{1-\zeta_p}$. Das orthogonale Komplement wird von den übrigen Basisvektoren aufgespannt. Damit man möglichst viele Summanden mit einem kleinen Rang erhält, wiederholt man diesen Schritt, bis es in H_ζ keine minimalen Elemente der Form $\nu_{1-\zeta_p}(h^\zeta(y_i,y_i))$ mit $y_i \in Y$ gibt.

(viii) Sollte es ein minimales Element der Form $\nu_{1-\zeta_p}(h^\zeta(y_j,y_k))$ geben, definiert man mit Hilfe der Definitionen aus Schritt (vi):

$$\begin{array}{lll} x_i'' & := x_i + \frac{c'(y_j,y_k,x_i)}{N(y_j,y_k)+(0,p)}\ y_j + \frac{d'(y_j,y_k,x_i)}{N(y_j,y_k)+(0,p)}\ y_k & \text{für } 1 \le i \le n_g \\ y_i'' & := y_i + \frac{c'(y_j,y_k,y_i)}{N(y_j,y_k)+(0,p)}\ y_j + \frac{d'(y_j,y_k,y_i)}{N(y_j,y_k)+(0,p)}\ y_k & \text{für } 1 \le i \le n_\zeta, i \notin \{j,k\} \\ z_i'' & := z_i & \text{für } 1 \le i \le n_1 \end{array}$$

Weil $c'(y_j,y_k,x_i), d'(y_j,y_k,x_i), N(y_j,y_k) \in \mathbb{Z}[\zeta_p]_{1-\zeta_p} \times \{0\}$ liegen und y_j, y_k passend gewählt wurden, liegen die Brüche in Γ und mit Lemma 1.46 sogar in Λ. Daher bilden die neuen Vektoren nach wiederholter Anwendung von Lemma 1.47 (b) und (e) wieder eine Pseudobasis. Des Weiteren folgt aus Lemma 1.43, angewendet auf die erste Komponente:

$$\begin{array}{lll} h(y_j,x_i'') & = (0,0) & \text{für } 1 \le i \le n_g \\ h(y_j,y_i'') & = (0,0) & \text{für } 1 \le i \le n_\zeta, i \notin \{j,k\} \\ h(y_j,z_i'') & = (0,0) & \text{für } 1 \le i \le n_1, \text{nach Lemma 1.15} \end{array}$$

Damit ist $\text{Spann}_\Lambda\{y_j,y_k\}$ ein $(-1,-1,\nu_{1-\zeta_p}(h^\zeta(y_j,y_k)))$-modularer, orthogonaler Summand mit der Struktur $\mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}$. Proposition 1.32 zeigt, dass diese Teilgitter auch für $p \ne 2$ keine Orthogonalbasis besitzen müssen. Falls das Teilgitter eine Orthogonalbasis

besitzt, kann man es in zwei orthogonale Summanden der Form $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$ zerlegen. Falls in diesem Schritt ein Teilgitter abgespalten wurde, fährt man erneut mit (vii) fort.

(ix) Wenn es ein minimales Element der Form $\nu_{1-\zeta_p}(h^\zeta(y'_j, y'_j))$ gibt, wird zum Ändern der Pseudobasis wieder ein zusätzliches Element aus Λ benötigt. Denn es ist denkbar, dass $h(x_j, x_j) \in \mathbb{Z}[\zeta_p]_{1-\zeta_p} \times \{0\}$ ist, wenn das zugehörige z'_j zu einer Komponente von L^1 gehört, die den Rang 2 besitzt.

$$\delta_j := \begin{cases} (0,p)^2 & \text{falls } \nu_p(b^1(z'_j, z'_j) + p) > \nu_p(b^1(z'_j, z'_j)) \\ (0,p) & \text{sonst} \end{cases}$$

Damit kann die Pseudobasis wie folgt verändert werden:

$$\begin{array}{lll} x''_i & := x_i - \frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j & \text{für } 1 \le i \le n_g, i \neq j \\ y''_i & := y_i - \frac{h(y_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j & \text{für } 1 \le i \le n_\zeta \\ z''_i & := z_i & \text{für } 1 \le i \le n_1 \end{array}$$

Da die $x_i \in X$ in den Schritten (iii),(iv),(v) und (vi) so gewählt wurden, dass die zugehörigen z'_i orthogonal zueinander sind, gilt:

$$\frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j} = \frac{(h^\zeta(y'_i,y'_j),0)}{(h^\zeta(y'_j,y'_j), b^1(z'_j,z'_j)) + \delta_j} = (\frac{h^\zeta(y'_i,y'_j)}{h^\zeta(y'_j,y'_j)}, 0)$$

Damit liegt der erste Bruch in Γ und nach Lemma 1.46 sogar in Λ. Mit einer ähnlichen Rechnung kann dies auch für den zweiten Bruch nachgewiesen werden. Aus Lemma 1.47 (a) und (d) folgt, dass die neuen Vektoren wieder eine Pseudobasis bilden.

$$\begin{array}{rcl} h(x''_i, x_j) := & h(x_i - \frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j, x_j) = h(x_i,x_j) - \frac{h(x_i,x_j)}{h(x_j,x_j)+\delta_j}\, h(x_j,x_j) \\ = & (h^\zeta(y'_i,y'_j) - \frac{h^\zeta(y'_i,y'_j)}{h^\zeta(y'_j,y'_j)}\, h^\zeta(y'_j,y'_j), 0) = (0,0) \\ h(y''_i, x_j) := & h(y_i - \frac{h(y_i,x_j)}{h(x_j,x_j)+\delta_j}\, x_j, x_j) = h(y_i,x_j) - \frac{h(y_i,x_j)}{h(x_j,x_j)+\delta_j}\, h(x_j,x_j) \\ = & (h^\zeta(y_i,y'_j) - \frac{h^\zeta(y_i,y'_j)}{h^\zeta(y'_j,y'_j)}\, h^\zeta(y'_j,y'_j), 0) = (0,0) \end{array}$$

Für die $z_i = z''_i$ können zwei Fälle eintreten: Entweder sind alle z_i orthogonal zu z'_j oder es gibt genau ein $z_l \in Z$, das nicht orthogonal zu z'_j ist. Falls alle z_i orthogonal zu z'_j sind, kann man einen $(-1, \nu_p(b^1(z'_j,z'_j)), \nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)))$-modularen, orthogonalen Summanden der Form $\mathrm{Spann}_\Lambda\{x_j\} \cong \Lambda$ abspalten. Falls es ein z_l gibt, das nicht orthogonal zu z'_j ist, kann man einen $(-1, \nu_p(b^1(z'_j,z_l)), \nu_{1-\zeta_p}(h^\zeta(y'_j,y'_j)))$-modularen Summanden $\mathrm{Spann}_\Lambda\{x_j, z_l\} \cong \Lambda \oplus \mathbb{Z}_p$ orthogonal abspalten. Um möglichst kleine orthogonale Summanden zu erhalten, muss dieser Schritt so oft wie möglich wiederholt werden.

(x) Falls es ein minimales Element der Form $\nu_{1-\zeta_p}(h^\zeta(y'_j, y_k))$ gibt, definiert man mit Hilfe der Definitionen aus Schritt (vi):

$$\begin{aligned} x_i'' &:= x_i + \tfrac{c'(x_j,y_k,x_i)}{N(x_j,y_k)+(0,p)}\ x_j + \tfrac{d'(x_j,y_k,x_i)}{N(x_j,y_k)+(0,p)}\ y_k && \text{für } 1 \le i \le n_g, i \ne j \\ y_i'' &:= y_i + \tfrac{c'(x_j,y_k,y_i)}{N(x_j,y_k)+(0,p)}\ x_j + \tfrac{d'(x_j,y_k,y_i)}{N(x_j,y_k)+(0,p)}\ y_k && \text{für } 1 \le i \le n_\zeta, i \ne k \\ z_i'' &:= z_i && \text{für } 1 \le i \le n_1 \end{aligned}$$

Weil $c'(x_j, y_k, x_i), d'(x_j, y_k, x_i), N(x_j, y_k) \in \mathbb{Z}[\zeta_p]_{1-\zeta_p} \times \{0\}$ liegen und y_j', y_k passend gewählt wurden, liegen die beiden oberen Brüche in Γ und mit Lemma 1.46 sogar in Λ. Man kann auf diese Art ebenfalls zeigen, dass die beiden verbleibenden Brüche auch in Λ liegen müssen. Also bilden diese neuen Vektoren gemäß Lemma 1.47 (a),(b),(d) und (e) eine Pseudobasis von L. Des Weiteren folgt aus Lemma 1.43, angewendet auf die erste Komponente, sowie der konstruktionsbedingten Eigenschaft $b^1(v, w) = 0$ für alle $v, w \in Z'$:

$$\begin{aligned} h(x_j, x_i'') &= (0,0) && \text{für } 1 \le i \le n_g, i \ne j \\ h(y_k, x_i'') &= (0,0) && \text{für } 1 \le i \le n_g \\ h(x_j, y_i'') &= (0,0) && \text{für } 1 \le i \le n_\zeta \\ h(y_k, y_i'') &= (0,0) && \text{für } 1 \le i \le n_\zeta, i \ne k \\ h(y_k, z_i'') &= (0,0) && \text{für } 1 \le i \le n_\zeta, \text{ nach Lemma 1.15} \end{aligned}$$

Für $h(x_j, z_i'')$ gibt es nun wieder zwei Möglichkeiten. Falls alle z_i orthogonal zu z_j' sind, kann ein $(-1, \nu_p(b^1(z_j', z_j')), \nu_{1-\zeta_p}(h^\zeta(y_j', y_k)))$-modularer Summand der Form $\mathrm{Spann}_\Lambda\{x_j, y_k\} \cong \Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}$ orthogonal abgespalten werden. Sollte es genau ein z_l geben, das nicht orthogonal zu z_j' ist, kann ein $(-1, \nu_p(b^1(z_j', z_l)), \nu_{1-\zeta_p}(h^\zeta(y_j', y_k)))$-modularer Summand der Form $\mathrm{Spann}_\Lambda\{x_j, y_k, z_l\} \cong \Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}_p$ orthogonal abgespalten werden.

(xi) Falls es ein minimales Element der Form $\nu_{1-\zeta_p}(h^\zeta(y_j', y_k'))$ gibt, kann die Pseudobasis folgendermaßen verändert werden:

$$\begin{aligned} x_i'' &:= x_i + \tfrac{c'(x_j,x_k,x_i)}{N(x_j,x_k)+(0,p)}\ x_j + \tfrac{d'(x_j,x_k,x_i)}{N(x_j,x_k)+(0,p)}\ x_k && \text{für } 1 \le i \le n_g, i \notin \{j,k\} \\ y_i'' &:= y_i + \tfrac{c'(x_j,x_k,y_i)}{N(x_j,x_k)+(0,p)}\ x_j + \tfrac{d'(x_j,x_k,y_i)}{N(x_j,x_k)+(0,p)}\ x_k && \text{für } 1 \le i \le n_\zeta \\ z_i'' &:= z_i && \text{für } 1 \le i \le n_1 \end{aligned}$$

Hierbei gilt: $c'(x_j, x_k, x_i), d'(x_j, x_k, x_i), N(x_j, x_k) \in \mathbb{Z}[\zeta_p]_{1-\zeta_p} \times \{0\}$. Daher kann das Teilen durch einen Nullteiler mittels Addition von $(0, p)$ leicht verhindert werden, ohne dass die Orthogonalprojektion beeinflusst wird. Bei den anderen Brüchen verhält es sich ebenso. Des Weiteren kann leicht nachgerechnet werden, dass die Brüche aufgrund der Wahl von y_j' und y_k' in Γ liegen. Weil sowohl Zähler als auch Nenner in Λ sind, folgt mit Lemma 1.46, dass die Brüche Werte in Λ besitzen. Daher bilden diese Vektoren gemäß Lemma 1.47 (a) und (d) zusammen mit x_j und x_k eine neue Pseudobasis von L, für die aus Lemma 1.43, angewendet auf die erste Komponente, sowie der konstruktionsbedingten Eigenschaft $b^1(v, w) = 0$ für alle $v, w \in Z'$ gilt:

$$\begin{aligned} h(x_j, x_i'') &= h(x_k, x_i'') &&= (0,0) && \text{für } 1 \le i \le n_g, i \notin \{j,k\} \\ h(x_j, y_i'') &= h(x_k, y_i'') &&= (0,0) && \text{für } 1 \le i \le n_\zeta \end{aligned}$$

Für die zu y'_j und y'_k gehörenden z'_j und z'_k gibt es drei Möglichkeiten. Beide Vektoren könnten etwa zu Komponenten in L^1 von Rang 1 gehören und man erhält damit einen $(\nu_p(b^1(z'_j, z'_j)), \nu_p(b^1(z'_k, z'_k)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$ -modularen, orthogonalen Summanden $\mathrm{Spann}_\Lambda\{x_j, x_k\}$ mit der Struktur $\Lambda \oplus \Lambda$. Sollte $\nu_p(b^1(z'_j, z'_j)) = \nu_p(b^1(z'_k, z'_k))$ sein, so ist die abgespaltene Komponente $(-1, \nu_p(b^1(z'_k, z'_k)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$-modular. Falls ein Vektor in einer Komponente von Rang 1 und ein Vektor in einer Komponente mit Rang 2 liegt, kann ein orthogonaler Summand der Form $\mathrm{Spann}_\Lambda\{x_j, x_k, z_s\} \cong \Lambda \oplus \Lambda \oplus \mathbb{Z}_p$ abgespalten werden. Er kann $(\nu_p(b^1(z'_j, z_s)), \nu_p(b^1(z'_k, z'_k)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$-modular beziehungsweise $(-1, \nu_p(b^1(z'_k, z'_k)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$-modular sein. Des Weiteren ist es denkbar, dass der Summand $(\nu_p(b^1(z'_j, z'_j)), \nu_p(b^1(z'_k, z_s)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$-modular beziehungsweise $(-1, \nu_p(b^1(z'_k, z_s)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$-modular ist. Sollten sowohl z'_j als auch z'_k in Komponenten mit Rang 2 liegen, ist es möglich, einen $(\nu_p(b^1(z'_j, z_s)), \nu_p(b^1(z'_k, z_t)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$ -modularen oder $(-1, \nu_p(b^1(z'_k, z_t)), \nu_{1-\zeta_p}(h^\zeta(y'_j, y'_k)))$-modularen orthogonalen Summanden der Form $\mathrm{Spann}_\Lambda\{x_j, x_k, z'_s, z'_t\} \cong \Lambda \oplus \Lambda \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ abzuspalten.

(xii) Wenn in (vii) - (xi) ein Teilgitter abgespalten worden ist, wiederholt man die gesamte Konstruktion solange für das orthogonale Komplement, bis $X = \emptyset$ ist. Mit Hilfe von (ii) ist die Konstruktion dann abgeschlossen. □

Bemerkung 1.53. Proposition 1.51 hat bereits gezeigt, dass es zu jeder Struktur aus der Liste von Satz 1.52 ein (i, j, k)-modulares, orthogonal unzerlegbares Gitter mit dieser Struktur gibt. Damit kann die Liste nicht weiter verkleinert werden.

Es wäre wünschenswert, wenn jedes modulare Teilgitter aus dem vorherigen Satz isometrisch zu einem U_i aus Definition 1.50 wäre. Das folgende Beispiel zeigt aber, dass dies nicht immer der Fall ist.

Beispiel 1.54. Gegeben seien ein $\mathbb{Z}_p$-Gitter L^1 und ein $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter L^ζ mit den Gram-Matrizen

$$L^1: \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad L^\zeta: \quad \begin{pmatrix} 0 & 1 \\ 1 & (1-\zeta_p)\overline{(1-\zeta_p)} \end{pmatrix}$$

Die Basen seien $\{z'_1, z'_2\}$ und $\{y'_1, y'_2\}$. Des Weiteren seien $x_i := y'_i \oplus z'_i$. Damit ist $L := \mathrm{Spann}_\Lambda\{x_1, x_2\}$ nach Lemma 1.48 ein Λ-Gitter mit der Struktur $\Lambda \oplus \Lambda$. Daher kann dieses Gitter mit Ausnahme von U_8 zu keinem anderen U_i isometrisch sein. Wenn L zu U_8 isometrisch wäre, dann müsste es eine Basis von L geben, die eine Orthogonalbasis von L^1 und gleichzeitig eine Basis aus isotropen Vektoren in L^ζ induziert. Angenommen es gäbe eine solche Basis $\{(v^1, v^\zeta), (w^1, w^\zeta)\}$. Dann gibt es $(\lambda_i^1, \lambda_i^\zeta), (\mu_i^1, \mu_i^\zeta) \in \Lambda$, sodass

$$(v^1, v^\zeta) = (\lambda_1^1, \lambda_1^\zeta)x_1 + (\lambda_2^1, \lambda_2^\zeta)x_2$$
$$(w^1, w^\zeta) = (\mu_1^1, \mu_1^\zeta)x_1 + (\mu_2^1, \mu_2^\zeta)x_2$$

Da $\{v^1, w^1\}$ eine Orthogonalbasis von L^1 bilden und L unimodular ist, gilt:

$$\begin{aligned} b^1(v^1,v^1) &= b^1(\lambda_1^1 z_1' + \lambda_2^1 z_2', \lambda_1^1 z_1' + \lambda_2^1 z_2') \\ &= (\lambda_1^1)^2 b^1(z_1',z_1') + (\lambda_2^1)^2 b^1(z_2',z_2') + 2\lambda_1^1\lambda_2^1 b^1(z_1',z_2') \\ &= 2\lambda_1^1\lambda_2^1 \end{aligned}$$

Da $b^1(v^1,v^1) \in \mathbb{Z}_p^*$ sein muss, folgt damit, dass auch $\lambda_i^1 \in \mathbb{Z}_p^*$ sein müssen. Weil $\{v^\zeta, w^\zeta\}$ eine Basis von L^ζ ist, die aus isotropen Vektoren besteht, gilt:

$$\begin{aligned} 0 &= h^\zeta(v^\zeta,v^\zeta) = h^\zeta(\lambda_1^\zeta y_1' + \lambda_2^\zeta y_2', \lambda_1^\zeta y_1' + \lambda_2^\zeta y_2') \\ &= \lambda_1^\zeta\overline{\lambda_1^\zeta} h^\zeta(y_1',y_1') + \lambda_2^\zeta\overline{\lambda_2^\zeta} h^\zeta(y_2',y_2') + \lambda_1^\zeta\overline{\lambda_2^\zeta} h^\zeta(y_1',y_2') + \overline{\lambda_1^\zeta}\lambda_2^\zeta h^\zeta(y_2',z_1') \\ &= \lambda_2^\zeta\overline{\lambda_2^\zeta}(1-\zeta_p)\overline{(1-\zeta_p)} + \lambda_1^\zeta\overline{\lambda_2^\zeta} + \overline{\lambda_1^\zeta}\lambda_2^\zeta \end{aligned}$$

Weil $\lambda_i^1 \in \mathbb{Z}_p^*$ sind, liegen sie in von $\overline{0}$ verschiedenen Restklassen von Γ/I. Dann müssen aber auch die λ_i^ζ in von $\overline{0}$ verschiedenen Restklassen liegen und damit aus $\mathbb{Z}[\zeta_p]_{1-\zeta_p}^*$ sein. Dies liefert einen Widerspruch zur letzten Gleichung. Also kann w^ζ nicht isotrop sein.

Im Allgemeinen ist die Zerlegung aus Satz 1.52 nicht eindeutig, was das folgende Beispiel zeigt:

Beispiel 1.55. Man betrachte das $\mathbb{Z}_p$-Gitter (L^1,h^1) und das $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter (L^ζ,h^ζ) mit den Gram-Matrizen

$$L^1: \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \qquad L^\zeta: \begin{pmatrix} 0 & 1-\zeta_p & 1-\zeta_p & 1-\zeta_p \\ 1-\zeta_p & 0 & 1-\zeta_p & 1-\zeta_p \\ 1-\zeta_p & 1-\zeta_p & 0 & 1-\zeta_p \\ 1-\zeta_p & 1-\zeta_p & 1-\zeta_p & 0 \end{pmatrix}$$

Sind $\{z_1', z_2'\}$ und $\{y_1, y_2, y_1', y_2'\}$ Basen von L^1 und L^ζ, so erhält man nach Lemma 1.48 ein Gitter $L := \mathrm{Spann}_\Lambda\{z_1' \oplus y_1', z_2' \oplus y_2', y_1, y_2\}$ mit der Struktur $\Lambda \oplus \Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}$. Der Beweis von Satz 1.52 würde eine Zerlegung des Typs $(\Lambda \oplus \Lambda) \perp (\mathbb{Z}[\zeta_p]_{1-\zeta_p} \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p})$ liefern. Es wäre in diesem Fall aber auch möglich, das Teilgitter $\mathrm{Spann}_\Lambda\{y_1' \oplus z_1', y_1\}$ analog zu Schritt (x) orthogonal abzuspalten. Man erhielte dann die Zerlegung $(\Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p}) \perp (\Lambda \oplus \mathbb{Z}[\zeta_p]_{1-\zeta_p})$.

Damit ist der Fall, dass die Gruppe G von ungerader Primzahlordnung ist, abgeschlossen. Für $p = 2$ gibt es kein vergleichbares Resultat, denn das folgende Beispiel zeigt, dass es unendlich viele orthogonal unzerlegbare Summanden mit beliebig großem Rang gibt. Der entscheidende Unterschied zum Fall $p \neq 2$ liegt darin, dass es in L^1 Teilgitter der Form $\mathrm{Spann}\{z_j', z_k'\}$ geben kann, die nicht diagonalisierbar sind. Das bedeutet, dass der Schritt (iii) im Beweis von Satz 1.52 nicht funktioniert. Weil auch L^ζ unzerlegbare Komponenten mit Rang 2 enthalten kann, können diese Komponenten mit Hilfe der Diagonaleinbettung miteinander verbunden werden.

Beispiel 1.56. Es seien $\mathbb{Z}_2$-Gitter L_i^1 und L_i^ζ durch die Gram-Matrizen

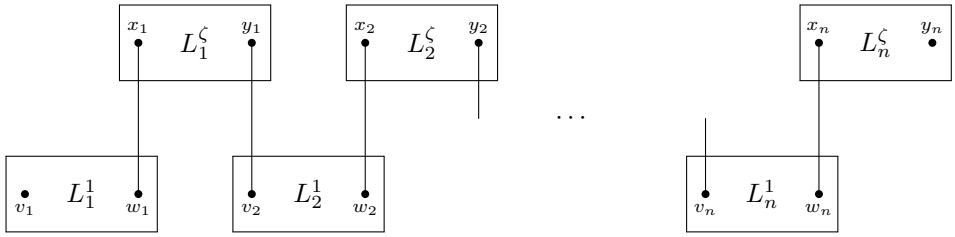
$$\begin{pmatrix} 0 & 2^i \\ 2^i & 0 \end{pmatrix}$$

gegeben. Diese Gitter sind (2^i)-modular, besitzen keine Orthogonalbasis und sind daher orthogonal unzerlegbar. Die Basisvektoren von L_i^1 werden mit $\{v_i, w_i\}$ und die Basisvektoren von L_i^ζ mit $\{x_i, y_i\}$ bezeichnet. Man definiert $L^1 := \perp_{i=1}^n L_i^1$ und $L^\zeta := \perp_{i=1}^n L_i^\zeta$ und bildet mit Hilfe von Lemma 1.48 das Teilgitter

$$L := \text{Spann}\{\{v_1 \oplus 0\} \cup \{w_i \oplus x_i, v_{i+1} \oplus y_i \mid i \in 1, \dots n-1\} \cup \{0 \oplus y_n\}\} \subseteq L^1 \perp L^\zeta$$

Angenommen es gäbe eine orthogonale Zerlegung von diesem Gitter. Dann würde dies eine orthogonale Zerlegung von einem L_i^1 oder einem L_i^ζ implizieren. Da diese Teilgitter aber orthogonal unzerlegbar sind, erhält man einen Widerspruch. Somit erhält man orthogonal unzerlegbare Gitter von beliebig großem Rang.

Das Konstruktionsprinzip kann durch folgende Skizze veranschaulicht werden:



Nach demselben Prinzip kann für Gruppen mit nicht-quadratfreier Ordnung m gezeigt werden, dass es unendlich viele orthogonal unzerlegbare Summanden mit beliebig großem Rang gibt:

Beispiel 1.57. Es sei p eine Primzahl mit $p^2 \mid m$. Damit sind die Ringe $\mathbb{Z}[\zeta_p]$ und $\mathbb{Z}[\zeta_{p^2}]$ als direkte Faktoren in der Maximalordnung enthalten. Gemäß Proposition 1.32 gibt es zu beiden Ringen orthogonal unzerlegbare Gitter von Rang 2, wie zum Beispiel die $((1-\zeta_p)^{2i-1})$-modularen Gitter $L_i^{\zeta_p}$ und die $((1-\zeta_{p^2})^{2i-1})$-modularen Gitter $L_i^{\zeta_{p^2}}$ mit den Gram-Matrizen:

$$L_i^{\zeta_p} : \begin{pmatrix} 0 & (1-\zeta_p)^{2i-1} \\ (1-\zeta_p)^{2i-1} & 0 \end{pmatrix} \qquad L_i^{\zeta_{p^2}} : \begin{pmatrix} 0 & (1-\zeta_{p^2})^{2i-1} \\ (1-\zeta_{p^2})^{2i-1} & 0 \end{pmatrix}$$

Die Basisvektoren von $L_i^{\zeta_p}$ werden mit $\{v_i, w_i\}$ und die Basisvektoren von $L_i^{\zeta_{p^2}}$ mit $\{x_i, y_i\}$ bezeichnet. Man definiert $L^{\zeta_p} := \perp_{i=1}^n L_i^{\zeta_p}$ und $L^{\zeta_{p^2}} := \perp_{i=1}^{n-1} L_i^{\zeta_{p^2}}$ und bildet mit Hilfe von Lemma 1.48 das Teilgitter

$$\text{Spann}\{\{v_1 \oplus 0\} \cup \{w_i \oplus x_i, v_{i+1} \oplus y_i \mid i \in 1, \dots n-2\} \cup \{0 \oplus y_n\}\} \subseteq L^{\zeta_p} \perp L^{\zeta_{p^2}}$$

Wie im Fall $m = p = 2$ kann gezeigt werden, dass dieses Gitter orthogonal unzerlegbar ist.

Als letzte verbleibende Möglichkeit soll nun m Produkt von verschiedenen ungeraden Primzahlen sein. Die Erweiterung $\mathbb{Z}[\zeta_d] : \mathbb{Z}[\zeta_d+\zeta_d^{-1}]$ ist gemäß [Was82] Kapitel 2 (an den endlichen Stellen) unverzweigt, falls d keine Primzahl ist. Für Primzahlen $d \neq p$ ist die Lokalisierung ebenfalls unverzweigt, da die Diskriminante nur den Primteiler d besitzt. Daher gibt es in diesen Fällen nach Proposition 1.31 stets eine Orthogonalbasis. Also kann es keine zwei verschiedenen Teilgitter L_d mit orthogonal unzerlegbaren Komponenten von Rang 2 geben. Somit kann in diesem Fall mit der obigen Methode auch kein Beispiel für unendlich viele, orthogonal unzerlegbare Gitter gefunden werden. Es ist jedoch auch nicht zu erwarten, dass man eine ähnliche Liste mit orthogonalen Summanden wie im Fall $m = p$ findet. Weil die Gruppe zyklisch und damit abelsch ist, besitzt sie nur eine p-Sylowgruppe, die isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist. Also gibt es, gemäß [Jon63] Theorem 8, nur endlich viele unzerlegbare Moduln. Ihre Anzahl und auch ihr Isomorphietyp sind anscheinend noch nicht genau bekannt, sodass dies geklärt werden müsste. Klar ist aber, dass die Anzahl wesentlich höher ist als im Fall $|G| = p$, denn nur durch die verschiedenen Möglichkeiten, die man durch die höhere Anzahl an möglichen Minimalpolynomen erhält, bekommt man schon für kleine m zusätzliche unzerlegbare Moduln. Nimmt man anschließend noch die hermitesche Form hinzu, erhält man vermutlich, wie im Fall $|G| = p$, durch Kombinationen viele zusätzliche orthogonal unzerlegbare Moduln. Um dies zu beweisen, kann die oben entwickelte Methode in der Form nicht ohne Weiteres verwendet werden, da die Voraussetzung $|G| = p$ an einigen Stellen die Verwendung bekannter Ergebnisse erlaubte, die für $|G| = m$ anscheinend (noch) nicht existieren.
Abschließend soll ein Blick auf den Spezialfall der unimodularen Λ-Gitter für $p \neq 2$ geworfen werden. Es zeigt sich, dass sich die Liste mit den Modulstrukturen orthogonal unzerlegbarer Summanden unter dieser zusätzlichen Voraussetzung weiter verkleinern lässt und man kann ihre Isometrieklassen bestimmen.

Proposition 1.58. *Sei (L, h) ein hermitesches, unimodulares Λ-Gitter. Dann gibt es ein freies Λ-Gitter L_g, ein freies $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter L_ζ und ein freies $\mathbb{Z}_p$-Gitter L_1 mit*

$$L \cong L_g \perp L_\zeta \perp L_1$$

Diese Zerlegung ist bis auf Isometrie eindeutig.

Beweis. Diese Aussage folgt aus Proposition 1.41 sowie [QSSS76] Satz 3.2 und Satz 3.4. Zu prüfen sind zwei Voraussetzungen für diese Sätze. Zum einen muss der Endomorphismenring $A := \mathrm{End}_\Lambda(M)$ für alle Λ-Moduln M $\mathrm{Rad}(A)$-adisch vollständig sein und zum anderen muss der Endomorphismenring unzerlegbarer Λ-Moduln M lokal sein. Der Endomorphismenring A ist eine $\mathbb{Z}_p$-Algebra und besitzt zwei Topologien. Die erste Topologie auf A wird durch die p-adische Topologie von $\mathbb{Z}_p$ induziert (vgl. [Rei75] S. 83). Bezüglich dieser Topologie ist A vollständig und hausdorff'sch (vgl. [Rei75] Korollar 6.17). Die zweite Topologie ist die $\mathrm{Rad}(A)$-adische Topologie. Mit Hilfe von [Rei75] Seite 85 folgt, dass A bezüglich dieser Topologie ebenfalls vollständig und hausdorff'sch ist, womit die erste Voraussetzung gezeigt ist. Sei A von nun an nicht lokal. Dann ist $\overline{A} := A/\mathrm{Rad}(A)$ nach [Rei75] Theorem 6.14 kein

Schiefkörper und enthält deshalb ein nicht-triviales Linksideal I. Die Algebra $A/\operatorname{Rad}(A)$ ist nach [Rei75] Theorem 6.15 eine endlich-dimensionale $\mathbb{F}_p$-Algebra und ein links-artinscher Ring (vgl. [Rei75] S. 83). Weil $\operatorname{Rad}(\overline{A}) = 0$ ist, kann I gemäß [Rei75] Theorem 6.9 nicht nilpotent sein. Also enthält I gemäß [Rei75] Korollar 6.8 ein Idempotent $\overline{e} \in I \subsetneq \overline{A}$ mit $\overline{e} \notin \{\overline{0}, \overline{1}\}$. Dieses Element kann nach [Rei75] Theorem 6.18 zu einem nicht-trivialen Idempotent $e \in A$ geliftet werden. Damit erhält man eine Zerlegung $A = eA + (1-e)A$. Also ist M zerlegbar. □

Lemma 1.59. *Seien L_1 ein $\mathbb{Z}_p$-Gitter und L_ζ ein $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter, die als Λ-Gitter unimodular sind. Dann gilt:*

(a) $\operatorname{Hom}_\Lambda(L_\zeta, \Lambda) \cong \operatorname{Hom}_{\mathbb{Z}[\zeta_p]_{1-\zeta_p}}(L_\zeta, (1-\zeta_p)\mathbb{Z}[\zeta_p]_{1-\zeta_p})$

(b) $\operatorname{Hom}_\Lambda(L_1, \Lambda) \cong \operatorname{Hom}_{\mathbb{Z}_p}(L_1, p\mathbb{Z}_p)$

Beweis. Die Abbildung

$$\begin{array}{rccc} f: & \operatorname{Hom}_{\mathbb{Z}[\zeta_p]_{1-\zeta_p}}(L_\zeta, (1-\zeta_p)\mathbb{Z}[\zeta_p]_{1-\zeta_p}) & \longrightarrow & \operatorname{Hom}_\Lambda(L_\zeta, \Lambda) \\ & \varphi & \mapsto & (\varphi, 0) \end{array}$$

ist offensichtlich ein injektiver Gruppenhomomorphismus. Sei $\psi \in \operatorname{Hom}_\Lambda(L_\zeta, \Lambda)$. Dann ist $\psi = (\psi_\zeta, 0)$. Also gilt $\psi(L_\zeta) = (\psi_\zeta(L_\zeta), 0) \subseteq \Lambda$. Damit folgt nach Lemma 1.44 $\overline{\psi_\zeta(L_\zeta)} = \overline{0}$. Das bedeutet $\psi_\zeta(L_\zeta) \subseteq (1-\zeta_p)\mathbb{Z}[\zeta_p]_{1-\zeta_p}$. Also ist ψ_ζ ein Urbild von ψ und f ist ein Isomorphismus. Teil (b) wird analog bewiesen. □

Lemma 1.60. *Seien (L_1, h_1) und (L_2, h_2) Λ-Gitter mit der Modulstruktur Λ. Dann gilt:*

$$(L_1, h_1) \cong (L_2, h_2) \Leftrightarrow (\Gamma \otimes L_1, h_1) \cong (\Gamma \otimes L_2, h_2)$$

Beweis. "⇒" ist klar. Es gelte nun $(\Gamma \otimes L_1, h_1) \cong (\Gamma \otimes L_2, h_2)$. Zu $(\Gamma \otimes L_i, h_i)$ gibt es ein $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter (L_i^ζ, h_i^ζ) und ein $\mathbb{Z}_p$-Gitter (L_i^1, b_i^1) mit $(\Gamma \otimes L_i, h_i) = (L_i^\zeta, h_i^\zeta) \perp (L_i^1, b_i^1)$. Wie zuvor wird mit x_i die Basis von (L_i, h_i), mit y_i' die Basis von (L_i^ζ, h_i^ζ) und mit z_i' die Basis von (L_i^1, b_i^1) bezeichnet, sodass $x_i = (y_i', z_i')$ ist. Aus der Voraussetzung folgt nun $(L_1^\zeta, h_1^\zeta) \cong (L_2^\zeta, h_2^\zeta)$ und $(L_1^1, b_1^1) \cong (L_2^1, b_2^1)$. Weil L_1^1 und L_1^ζ jeweils den Rang 1 besitzen, gibt es Isometrien

$$\begin{array}{rccc} \varphi_\zeta: L_1^\zeta & \longrightarrow & L_2^\zeta \\ y_1' & \mapsto & y_2' \end{array} \qquad\qquad \begin{array}{rccc} \varphi_1: L_1^1 & \longrightarrow & L_2^1 \\ z_1' & \mapsto & z_2' \end{array}$$

Dann ist die Abbildung $\varphi: (L_1, h_1) \longrightarrow (L_2, h_2)$ mit $\varphi(x_1) := (\varphi_\zeta(y_1'), \varphi_1(z_1')) = (y_2', z_2') = x_2$ ein Λ-Modulisomorphismus und für alle $\lambda, \mu \in \Lambda$ gilt:

$$\begin{aligned} h_1(\lambda x_1, \mu x_1) &= \lambda\overline{\mu}(h_1^\zeta(y_1', y_1'), b_1^1(z_1', z_1')) = \lambda\overline{\mu}(h_2^\zeta(\varphi_\zeta(y_1'), \varphi_\zeta(y_1')), b_2^1(\varphi_1(z_1'), \varphi_1(z_1')) \\ &= \lambda\overline{\mu}(h_2^\zeta(y_2', y_2'), b_2^1(z_2', z_2')) = h_2(\lambda x_2, \mu x_2) \end{aligned}$$

Damit ist φ eine Isometrie. □

Seien $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter L_i^ζ und $\mathbb{Z}_p$-Gitter L_i^1 durch die folgenden Gram-Matrizen gegeben.

$$L_1^\zeta : \begin{pmatrix} 1 \end{pmatrix} \qquad L_2^\zeta : \begin{pmatrix} \delta_\zeta \end{pmatrix} \qquad L_1^1 : \begin{pmatrix} 1 \end{pmatrix} \qquad L_2^1 : \begin{pmatrix} \delta_1 \end{pmatrix},$$

wobei $\delta_1 \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$ ist und $\delta_\zeta \in \mathbb{Z}[\zeta_p + \overline{\zeta_p}]$ keine Norm eines Elementes aus $\mathbb{Z}[\zeta_p]$ ist. Die Basen seien wie oben $\{y_i'\}$ und $\{z_i'\}$. Dann folgt $L_1^\zeta \ncong L_2^\zeta$ und $L_1^1 \ncong L_2^1$. Also werden die Isometrieklassen von Γ-Gittern, deren Komponenten Rang 1 besitzen, von den Gittern $L_i^\zeta \perp L_j^1$ mit $i, j \in \{1, 2\}$ vertreten. Aus dem vorangegangenen Lemma und aus Lemma 1.48 folgt damit unmittelbar:

Korollar 1.61. *Die Isometrieklassen von Λ-Gittern mit der Modulstruktur Λ werden von den Gittern $L_{i,j} := \mathrm{Spann}_\Lambda\{y_i' \oplus z_j'\}$ mit $i, j \in \{1, 2\}$ vertreten.*

Jetzt können die Ergebnisse zusammengefasst werden:

Proposition 1.62. *Sei p eine ungerade Primzahl. Jedes unimodulare, hermitesche Λ-Gitter (L, h) ist eine orthogonale Summe der folgenden orthogonal unzerlegbaren Teilgitter:*

$\mathbb{Z}_p$-Gitter:	$\langle p \rangle, \langle \delta p \rangle$	*für ein $\delta \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$*
$\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter:	$\mathbb{H}(1)$	
Λ-Gitter:	$L_{1,1}, L_{1,2}, L_{2,1}, L_{2,2}$	

Beweis. Das Gitter (L, h) zerfällt gemäß Proposition 1.58 in eine orthogonale Summe

$$L \cong L_g \perp L_\zeta \perp L_1$$

Damit kann man nun jeden Summanden einzeln betrachten. Das Gitter L_1, das als Λ-Gitter unimodular ist, ist nach Lemma 1.59 als $\mathbb{Z}_p$-Gitter (p)-modular. Es besitzt nach Proposition 1.24 außerdem eine Orthogonalbasis. Daher zerfällt es in Komponenten von Rang 1, von denen es die beiden angegebenen Isometrieklassen gibt. Das Gitter L_ζ ist als $\mathbb{Z}[\zeta_p]_{1-\zeta_p}$-Gitter gemäß Lemma 1.59 $(1-\zeta_p)$-modular. Daher folgt aus Proposition 1.32, dass L_ζ eine orthogonale Summe von hyperbolischen Ebenen $\mathbb{H}(1)$ ist. Das Teilgitter L_g besitzt über der Maximalordnung unimodulare Komponenten. Es soll nun gezeigt werden, dass L_g stets eine Orthogonalbasis besitzt. Nach Satz 1.52 ist L_g orthogonale Summe von Teilgittern mit der Modulstruktur Λ oder $\Lambda \oplus \Lambda$. Sei nun ein Gitter L' mit der Struktur $\Lambda \oplus \Lambda$ und Basis $\{x_1, x_2\}$ gegeben. Nach Proposition 1.32 besitzt L'^ζ eine Orthogonalbasis $\{y_3', y_4'\}$. Dann gibt es $\lambda_i^\zeta, \mu_i^\zeta$ mit

$$\begin{aligned} y_3' &= \lambda_1^\zeta y_1' + \lambda_2^\zeta y_2' \\ y_4' &= \mu_1^\zeta y_1' + \mu_2^\zeta y_2' \end{aligned}$$

Mindestens ein Element der Menge $\{\lambda_1^\zeta, \mu_1^\zeta\}$ und ein Element der Menge $\{\lambda_2^\zeta, \mu_2^\zeta\}$ ist eine Einheit. Man kann nach Multiplikation mit Einheiten ohne Einschränkung annehmen, dass $\lambda_1^\zeta = 1$ und $\mu_2^\zeta = 1$ ist. Ausserdem gibt es λ_i^1, μ_i^1 mit $\lambda_i := (\lambda_i^\zeta, \lambda_i^1), \mu_i := (\mu_i^1, \mu_i^1) \in \Lambda$. Also

können auch $\lambda_1^1 = 1$ und $\mu_2^1 = 1$ gewählt werden. Damit erhält man eine Basis von Λ, die eine Orthogonalbasis von L^ζ induziert:

$$x_3 = x_1 + \lambda_2 x_2$$
$$x_4 = \mu_1 x_1 + x_2$$

$h^\zeta(y_3', y_3')$ und $h^\zeta(y_4', y_4')$ müssen minimale Bewertungen besitzen. Falls $b(z_3', z_3')$ oder $b(z_4', z_4')$ ebenfalls eine minimale Bewertung besitzt, kann man das Gram-Schmidt-Verfahren durchführen und erhält eine Orthogonalbasis. Ansonsten setzt man

$$\epsilon := \begin{cases} 1 & \text{falls } \nu_{1-\zeta_p}(h^\zeta(y_3', y_3') + (\epsilon^\zeta)^2 h^\zeta(y_4', y_4')) = 1 \\ 2 & \text{sonst} \end{cases}$$

Dann besitzt $x_3 + \epsilon x_4$ in beiden Komponenten niedrigste Bewertungen:

$$h^\zeta(y_3' + \epsilon^\zeta y_4', y_3' + \epsilon^\zeta y_4') \quad = \quad h^\zeta(y_3', y_3') + (\epsilon^\zeta)^2 h^\zeta(y_4', y_4')$$

Die Bewertung der ersten Komponente ist nach Definition von ϵ minimal. Für die zweite Komponente gilt:

$$b^1(z_3' + \epsilon^1 z_4', z_3' + \epsilon^1 z_4') \quad = \quad b^1(z_3', z_3') + (\epsilon^1)^2 b^1(z_4', z_4') + 2\epsilon^1 b^1(z_3', z_4')$$

Die Bewertung der zweiten Komponente ist minimal, weil die ersten beiden Summanden nach Voraussetzung durch eine höhere p-Potenz teilbar sind und damit auch ihre Summe. Der dritte Summand hat die Bewertung 1, also die gesamte Summe die Bewertung 1. Damit kann man nun das Gram-Schmidt-Verfahren zum Beispiel mit der Basis $\{x_3 + \epsilon x_4, x_3\}$ durchführen und erhält eine Orthogonalbasis. Damit wurde L_g in eine orthogonale Summe von Teilgittern mit Rang 1 zerlegt. Nach Korollar 1.61 ist jedes Teilgitter isometrisch zu einem $L_{i,j}$. □

Hieraus ergeben sich Auswirkungen auf unimodulare $\mathbb{Z}G$-Gitter, die nach Theorem 1.13 durch das Tupel $(n_g, n_\zeta, n_1, [I])$ beschrieben werden können. Da ihre Lokalisierung und insbesondere das Teilgitter L_ζ die oben angegebene Form besitzen müssen, kommt nicht jede denkbare Struktur tatsächlich vor. Sei

$$n_\zeta' := \begin{cases} n_\zeta & \text{falls } [I] = \mathbb{Z}[\zeta_p] \\ n_\zeta + 1 & \text{sonst} \end{cases}$$

Korollar 1.63. *Sei (L, h) ein unimodulares $\mathbb{Z}G$-Gitter mit $|G| = p$. Dann gilt $2 | n_\zeta'$.*

Kapitel 2

Rationale Invarianten hermitescher $\mathbb{Z}G$-Gitter

In diesem Abschnitt sollen die möglichen $\mathbb{Z}G$-Modulstrukturen, die Gitter in einem vorgegeben $\mathbb{Z}$-Geschlecht besitzen können, untersucht werden. Es zeigt sich, dass im Allgemeinen nicht alle Strukturen, die den entsprechenden $\mathbb{Z}$-Rang aufweisen, auch tatsächlich auftreten. In einigen Fällen gibt es sogar nur die triviale Struktur, das heißt, in dem gesamten $\mathbb{Z}$-Geschlecht es gibt kein Gitter mit einer gewissen Automorphismenordnung m. Dies wird durch die Berechnung der Invarianten eines Geschlechts gezeigt, das einen fixpunktfreien Automorphismus mit Minimalpolynom Φ_m enthält. Im ersten Abschnitt wird zunächst ein kurzer Überblick über die Invarianten eines $\mathbb{Z}$-Geschlechts gegeben. Für ein $\mathbb{Z}$-Gitter, das einen Automorphismus mit Minimalpolynom Φ_m besitzt, werden im Anschluss notwendige Bedingungen für die Ränge des Gitters und der modularen Komponenten bestimmt. Im zweiten Abschnitt werden weitere Invarianten berechnet, indem der unterliegende Raum für jede modulare Komponente mit gegebenem Rang bestimmt wird. Im dritten Teil wird beschrieben, wie diese Resultate verwendet werden können, um in einem vorgegebenen Geschlecht Gitter mit einem Automorphismus auszuschließen. Im letzten Abschnitt sollen in möglichst vielen Fällen, die nicht ausgeschlossen wurden, solche Gitter konstruiert werden. Weil jedes Gitter mit $-\mathrm{id}$ einen fixpunktfreien Automorphismus der Ordnung 2 besitzt, der zudem keine zusätzliche hermitesche Struktur induziert, wird im gesamten Kapitel $m \neq 2$ vorausgesetzt.

2.1 Rationale Invarianten hermitescher $\mathbb{Z}[\zeta_m]$-Gitter I

In diesem Teil wird als erstes ein kurzer Überblick über das Geschlechtssymbol von $\mathbb{Z}$-Geschlechtern gegeben. Anschließend werden einige Invarianten von Geschlechtern von $\mathbb{Z}$-Gittern berechnet, die eine zusätzliche hermitesche Struktur über $\mathbb{Z}[\zeta_m]$ von Rang 1 besitzen. Es werden Einschränkungen für die Ränge der Komponenten einer p-modularen Zerlegung

und die Parität der Komponenten einer 2-modularen Zerlegung bestimmt. Dabei zeigt sich, dass die Möglichkeiten durch die hermitesche Struktur für einige Klassen von Gittern stark eingeschränkt sind.

Gitter, die in einem Geschlecht liegen, besitzen nach Definition an jeder Stelle isometrische Lokalisierungen. Das bedeutet, dass die modularen Zerlegungen von den Gittern eines Geschlechts im Wesentlichen gleich sind. Daher kann man mit ihrer Hilfe ein Symbol definieren, durch das ein Geschlecht vollständig beschrieben wird. In [CS99] Kapitel 15 findet man eine ausführliche Beschreibung dieses Symbols. Weil im weiteren Verlauf damit gearbeitet wird, folgt ein kurzer stichpunktartiger Überblick. Seien ein beliebiges Geschlecht und ein Gitter L aus diesem Geschlecht vorgegeben. Nach Proposition 1.24 gibt es an der Stelle $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ eine modulare Zerlegung

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} L \cong \bigperp_{i\in\mathbb{Z}} L_i$$

Das lokale Geschlechtssymbol an der Stelle $p \notin \{2, \infty\}$ besteht aus einer Folge, bei der in jedem Folgenglied die folgenden charakteristischen Informationen für die von $\{0\}$ verschiedenen Komponenten der modulare Zerlegung eingetragen werden:

- Einen Erzeuger des Skalenideals in Form einer p-Potenz p^i.
- Den Rang der Komponente $n_{p,i}$.
- Das Legendre-Symbol $\epsilon_{p,i} := \left(\frac{\det({}^{p^{-i}}L_i)}{p}\right) \in \{\pm 1\}$, das die Quadratklasse der Determinante der unskalierten Komponente angibt.

Diese Informationen für die i-te Komponente werden nun wie folgt notiert: $(p^i)^{\epsilon_{p,i} n_{p,i}}$. Das lokale Symbol an der Stelle p besteht nun aus einer Aufzählung der Symbole für die einzelnen Komponenten. Die Komponenten, die $\{0\}$ sind, werden nicht notiert. Das Symbol für die unimodularen Komponenten kann mit Hilfe des vollständigen Geschlechtssymbols rekonstruiert werden und muss daher ebenfalls nicht notiert werden. Für $p = 2$ benötigt man etwas andere Informationen, um das Geschlecht vollständig zu beschreiben:

- Einen Erzeuger des Skalenideals in Form einer 2-Potenz 2^i.
- Den Rang der Komponente $n_{2,i}$.
- Das Kronecker-Symbol $\epsilon_{2,i} := \left(\frac{\det({}^{2^{-i}}L_i)}{2}\right)$ der Determinante der reskalierten Komponente, wobei das Kronecker-Symbol an der Stelle 2 definiert ist als

$$\left(\frac{u}{2}\right) := \left\{ \begin{array}{rl} 1 & \text{falls } u \equiv_8 \pm 1 \\ -1 & \text{falls } u \equiv_8 \pm 3 \end{array} \right\}$$

- Die Parität von ${}^{2^{-i}}L_j$, das heißt, es muss notiert werden, ob die reskalierte Komponente gerade oder ungerade ist. Ein Gitter (M, b) heißt **gerade**, wenn $b(v, v) \in 2\mathbb{Z}_2$ für alle $v \in M$ ist.

- Falls ${}^{2^{-i}}L_i$ ungerade ist, muss zusätzlich die Oddity von L_i angegeben werden. Sie ist definiert als Invariante des unterliegenden Raums $\mathbb{Q}_2 \otimes_{\mathbb{Z}_2} {}^{2^{-i}}L_i$. Ist $\langle 2^{\alpha_1}a_1, 2^{\alpha_2}a_2, \ldots, 2^{\alpha_{n_{2,i}}}a_{n_{2,i}}\rangle$ mit $a_i \in \mathbb{Z}_2^*$ eine Diagonalisierung einer Form, dann ist die Oddity definiert als $4k + \sum_{i=1}^{n_{2,i}} a_i \mod 8$, wobei k die Anzahl der Diagonaleinträge mit $2 \nmid \alpha_i$ und $a_i \equiv_8 \pm 3$ ist.

Des Weiteren ist das 2-adische Symbol nicht eindeutig. Man kann jedoch stets eine einheitliche Form finden. Zusätzlich benötigt man für die Stelle ∞ noch die Signatur (r, s) des reellen Raums $\mathbb{R} \otimes_{\mathbb{Z}} L$. Diese Informationen reiht man wie folgt aneinander. Falls das Gitter gerade ist, beginnt das Symbol mit II. Sollte L ungerade sein, beginnt es mit I. Es folgt ein Index mit der Signatur (r, s). Anschließend werden die lokalen Symbole für $p \neq \infty$ nacheinander angehängt.
Wie in Definition 1.18 bereits thematisiert wurde, besitzt ein $\mathbb{Z}$-Gitter mit einem Automorphismus g für alle Teiler d der Ordnung m Teilgitter $L_d := \mathrm{Kern}(\Phi_d(g)) \cap L$. Bildet man $\perp_{d|m} L_d$ erhält man ein volles Teilgitter, aber im Allgemeinen nicht das gesamte Gitter. Diese Zerlegung enthält wichtige Eigenschaften des Automorphismus und liefert später notwendige Bedingungen an die Existenz eines Gitters mit einem Automorphismus einer bestimmten Ordnung.

Definition 2.1. Sei (L, b) ein beliebiges $\mathbb{Z}$-Gitter mit einem Automorphismus g der Ordnung m. Des Weiteren sei $L_d := \mathrm{Kern}(\Phi_d(g))$ für alle $d|m$. Das Tupel $(\mathrm{rang}_{\mathbb{Z}}(L_m), \ldots, \mathrm{rang}_{\mathbb{Z}}(L_1))$, wobei die Einträge über alle Teiler d von m laufen und absteigend sortiert sind, heißt der **Zerlegungstyp** von g. Ein Automorphismus heißt **fixpunktfrei**, wenn $\mathrm{rang}_{\mathbb{Z}}(L_1) = 0$ ist.

Bemerkung 2.2. Nicht jedes Tupel, dass zu einem Zerlegungstyp mit dem passenden $\mathbb{Z}$-Rang gehört, kann auch tatsächlich auftreten. Sei M die Menge der Teiler d, für die der entsprechende Eintrag im Tupel größer als 0 ist. Dann ist $m | \mathrm{kgV}(M)$ eine notwendige Voraussetzung für die Existenz eines Gitters mit Automorphismus der Ordnung m.

Die $\mathbb{Z}$-Gitter L_d besitzen für $d > 2$ konstruktionsbedingt eine hermitesche Struktur über dem d-ten Kreisteilungskörper. Deshalb werden in den nächsten Abschnitten die Invarianten von Gittern berechnet, die eine solche hermitesche Struktur besitzen. Die Gitter L_1 und L_2 besitzen keine zusätzliche Struktur. Deshalb liefern diese Gitter keine Einschränkungen. Da $\mathbb{Z}[\zeta_m]$ im Allgemeinen kein Hauptidealring ist, müssen $\mathbb{Z}[\zeta_m]$-Gitter nicht frei sein. Daher werden zunächst einige grundlegende Begriffe benötigt. Sei $R \in \{\mathbb{Z}[\zeta_m], \mathbb{Z}[\zeta_m]_\pi\}$. Zu jedem hermiteschen R-Gitter (L, h) gibt es stets Vektoren des unterliegenden Raums $v_1, \ldots, v_n$ und Ideale $A_1, \ldots, A_n \subseteq R$ mit

$$L = A_1 v_1 + A_2 v_2 + \ldots + A_n v_n$$

Die Menge $\{v_1, \ldots, v_n\}$ nennt man **Pseudobasis** von (L, h). Das Ideal $\prod A_i$ heißt die **Steinitzklasse** von (L, h) und $\mathfrak{d}(L) := \prod_{i=1}^{n}(A_i\overline{A_i}) \det((h(v_i, v_j)_{1\leq i,j\leq n})$ ist das **Diskriminantenideal** von (L, h). Falls der Grundring ein Hauptidealring ist, dann sind hermitesche Gitter frei. Das heißt, man kann annehmen, dass es Vektoren $v_1, \ldots, v_n$ gibt, sodass $A_i = R$

gilt. Zwischen der Determinante von (L, b) als quadratisches $\mathbb{Z}$-Gitter und dem Diskriminantenideal von (L, h) als hermitesches $\mathbb{Z}[\zeta_m]$-Gitter gibt es den folgenden, wohl bekannten Zusammenhang:

Lemma 2.3.

(a) Sei (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]$-Gitter mit Rang n. Dann gilt für $b := \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} \circ h$:

$$|\det(L, b)| = |\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}|^n \cdot \mathrm{Norm}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}(\mathfrak{d}(L, h))$$

(b) Sei (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter mit Rang n. Dann gilt für $b := \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h$:

$$\nu_p(\det(L, b)) = \nu_p(|\operatorname{disc}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}|) \cdot n + \nu_p(\mathrm{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\det(L, h)))$$

Beweis. Einen Beweis von (a) für positiv definite Gitter findet man in [Jür15] 3.1.4. Falls (L, b) nicht positiv definit ist, beweist man die Aussage analog. Im lokalen Fall ist die Diskriminantengruppe $(L, b)^\#/(L, b)$ eine p-Gruppe, deren Mächtigkeit dieselbe Bewertung wie die Determinante besitzt. Weil $\mathbb{Z}[\zeta_m]_\pi$ Hauptidealringe sind, kann man zusätzlich annehmen, dass die Gitter (L, h) frei sind. Damit verläuft der verbleibende Teil des Beweises analog zu (a). □

Bemerkung 2.4. Für freie Gitter oder für die unterliegenden Räume kann anstatt einer Pseudobasis eine echte Basis gewählt werden. Dann vereinfacht sich die Formel aus Lemma 2.3 (a) zu:

$$|\det(L, b)| = |\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}|^n \cdot \mathrm{Norm}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}(\det(L, h))$$

Bemerkung 2.5. Die erste offensichtliche Einschränkung für die Invarianten von $\mathbb{Z}$-Gittern L mit einem Automorphismus, der das Minimalpolynom Φ_m besitzt, gibt es für den $\mathbb{Z}$-Rang. Sei $\{v_1, \ldots, v_n\}$ eine Pseudobasis von (L, h). Weil nach [Neu92] Satz 2.10 auf Seite 13 jedes Ideal A_i ein freier $\mathbb{Z}$-Modul mit $\varphi(m)$-Elementen ist, besitzt (L, b) den Rang $n \cdot \varphi(m)$. Also können nur $\mathbb{Z}$-Gitter, deren Rang ein Vielfaches von $\varphi(m)$ ist, einen solchen Automorphismus besitzen.

Bemerkung 2.6. Eine weitere Einschränkung für ein Gitter L mit einer zusätzlichen $\mathbb{Z}[\zeta_m]$-Struktur ergibt sich aus dem unterliegenden $\mathbb{Q}[\zeta_m]$-Vektorraum. Er ist eine orthogonale Summe eindimensionaler Unterräume. Die Quadratklassen ihrer Determinanten wurden in [Neb99] Satz 3.3.14 (ii) bereits berechnet. Sei $n := \mathrm{rang}_{\mathbb{Z}[\zeta_m]}(L, h)$. Dann gilt:

$$\det(L, b) \in \begin{cases} m^n \cdot (\mathbb{Q}^*)^2 & \text{falls } m \text{ eine ungerade Primzahlpotenz ist} \\ (\mathbb{Q}^*)^2 & \text{sonst} \end{cases}$$

Als nächstes werden Eigenschaften der lokalen Spurkonstruktion genauer untersucht. Dafür wird zunächst die Differente $\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]_\pi}$ benötigt.

Bemerkung 2.7. Sei π eine über p liegende Stelle in $\mathbb{Q}[\zeta_m]$. Man schreibt $m = p^t \cdot m'$ mit $(p, m') = 1$. Für die Differente $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}$ gilt dann nach Bemerkung 1.27

$$\begin{aligned}\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} &= \mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} \cdot \mathbb{Z}[\zeta_m]_\pi = \mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_{p^t}]} \cdot \mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_{m'}]} \cdot \mathbb{Z}[\zeta_m]_\pi = \mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_{p^t}]} \cdot \mathbb{Z}[\zeta_m]_\pi \\ &= (1-\zeta_{p^t})^{p^{(t-1)}(pt-t-1)} \cdot \mathbb{Z}[\zeta_m]_\pi\end{aligned}$$

Weil $\mathbb{Z}[\zeta_m]_\pi$ stets ein Hauptidealring ist, muss $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}$ ein Hauptideal der Form (π^a) sein, wobei $a := p^{(t-1)}(pt - t - 1)$ ist.

Lemma 2.8. *Seien (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter, $p := \pi^e \in \mathbb{P}(\mathbb{Q})$, $b := \operatorname{Spur} \circ h$ und $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} = (\pi^a)$. Dann folgt:*

(a) Falls (L, h) (π^{ie-a})-modular für ein $i \in \mathbb{N}_0$ ist, dann ist das quadratische $\mathbb{Z}$-Gitter (L, b) (p^i)-modular.

(b) Falls (L, h) (π^j)-modular für ein $j \in \mathbb{Z}$ mit $j \geq -a$ ist und $i, r \in \mathbb{N}_0$ mit $j + a = ie + r$ und $0 \leq r < e$ sind, dann besitzt eine (p)-modulare Zerlegung von (L, b) höchstens zwei nicht-triviale Komponenten mit den Skalenidealen (p^i) und gegebenenfalls (p^{i+1}).

Beweis. (a) Man betrachte zunächst den Fall $i = 0$. Unmittelbar aus der Definition der Differente folgt, dass (L, b) ganzzahlig ist. Sei $n := \operatorname{rang}_{\mathbb{Z}[\zeta_m]_\pi}(L, h)$. Weil (L, h) $(\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^{-1}$-modular ist, muss $\nu_p(\operatorname{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\det(L, h))) = -\nu_p(|\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}|^n)$ sein. Damit folgt aus Lemma 2.3, dass (L, b) unimodular ist.
Für beliebiges i betrachtet man die (π^{-a})-modulare Form $h' := \pi^{-ie}h$. Es gilt:

$$b(L, L) = \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h(L, L)) = \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\pi^{ie}h'(L, L)) = p^i \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h'(L, L))$$

Aus dem ersten Teil des Beweises folgt, dass $(L, \operatorname{Spur} \circ h')$ unimodular ist. Damit ist b (p^i)-modular und Teil (a) ist bewiesen.
(b) Sei (L, h) nun (π^j)-modular, wobei zunächst $j \in \{-a, \ldots, -a + e - 1\}$ sei. Das bedeutet $i = 0$. Dann ist $p(\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^{-1} = (\pi^{-a+e}) \subsetneq (\pi^j) \subseteq (\pi^{-a}) = (\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^{-1}$. Mit Teil a) folgt $\operatorname{Scale}(L, b) \subseteq (p^0)$. Weil die nicht-triviale Komponente von (L, b) mit dem kleinsten Skalenideal der nicht-trivialen Komponente von $(L, b)^\#$ mit dem größten Skalenideal entspricht, kann man analog zeigen, dass $(L, b)^\#$ keine nicht-triviale Komponente mit einem größeren Skalenideal als (p^{-1}) besitzt. Sei j nun beliebig. Dann gilt für $h' := \pi^{-ie}h$:

$$b(L, L) = \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h(L, L)) = \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\pi^{ie}h'(L, L)) = p^i \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(h'(L, L))$$

Weil $(L, \operatorname{Spur} \circ h')$ nach obigen Überlegungen höchstens zwei nicht-triviale, modulare Komponenten mit den Skalierungen (p^0) und möglicherweise (p^1) besitzt, kann $(L, \operatorname{Spur} \circ h)$ höchstens zwei nicht-triviale, modulare Komponenten mit den Skalierungen (p^i) und möglicherweise (p^{i+1}) besitzen. □

Bemerkung 2.9. Ein $(\pi^i, \overline{\pi}^i)$-modulares, hermitesches $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ -Gitter kann im Sinne von Proposition 1.34 als (π^i)-modulares $\mathbb{Z}[\zeta_m]_\pi$-Gitter mit doppeltem Rang aufgefasst werden. Daher gilt die obige Behauptung auch für modulare $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ -Gitter.

An dieser Stelle soll an die drei Fälle erinnert werden, wie ein Primideal in der Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m+\overline{\zeta_m}]$ zerfallen kann (vgl. Seite 17). Bei der Untersuchung von $\mathbb{Z}$-Gittern mit einer hermiteschen $\mathbb{Z}[\zeta_m]$-Struktur spielen diese Fälle eine zentrale Rolle. Dabei ähneln sich der träge Fall und der zerfallende Fall, während der verzweigte Fall ein völlig anderes Verhalten zeigt.

Proposition 2.10. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Die über (p) liegenden Primideale in $\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ seien in der Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ träge. Des Weiteren seien π eine über p liegende Stelle und (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter. Dann ist der Rang von jeder Komponente einer modularen Zerlegung des $\mathbb{Z}_p$-Gitters $(L, \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h)$ ein Vielfaches von $f = 2f^+$.*

Beweis. Das $\mathbb{Z}[\zeta_m]_\pi$-Gitter (L, h) besitzt nach Proposition 1.31 eine Orthogonalbasis, also eine orthogonale Zerlegung in modulare Komponenten von Rang 1. Sei $(L', h') \subseteq (L, h)$ mit $h' := h|_{L'}$ ein solches Teilgitter mit $\mathrm{rang}(L', h') = 1$. Des Weiteren seien $b := \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h$ und $b' := \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h'$. Die Spurkonstruktion liefert dann gemäß Lemma 2.8 ein $\mathbb{Z}_p$-Gitter (L', b') mit höchstens zwei aufeinanderfolgenden modularen Komponenten. Ihre Ränge können mit Hilfe der Determinante bestimmt werden. Nach Lemma 2.3 gilt

$$\nu_p(\det(L', b')) = \nu_p((\mathrm{disc}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^1) + \nu_p(\mathrm{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\det(L', h')))$$

Die Differente $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}$ ist ein Ideal der Form (π^a). Die Diskriminante ist nach Bemerkung 1.27 die Norm der Differente, also $\mathrm{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\pi^a) = p^{fa}$. Damit gilt: $f \mid \nu_p((\mathrm{disc}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^1)$. Die Determinante von (L', h') ist ebenfalls von der Form $u\pi^i$ für ein $u \in \mathbb{Z}[\zeta_m]_\pi^*$ und ein $i \in \mathbb{N}$. Ihre Norm ist dann von der Form $u' p^{fi}$ für ein $u' \in \mathbb{Z}_p^*$. Also muss $\nu_p(\det_{\mathbb{Z}_p}(L', b'))$ ein Vielfaches von f sein. Weil die Differente $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} = (\pi^a)$ nach Bemerkung 1.27 einen reellen Erzeuger besitzt, gibt es ein (π^{-a})-modulares Gitter. Man kann zum Beispiel das skalierte, hermitesche $\mathbb{Z}[\zeta_m]_\pi$- Standardgitter mit Rang 1 wählen. Sein Spurgitter ist gemäß Lemma 2.8 unimodular. Mit jeder größeren π-Potenz vergrößert sich die Determinante als $\mathbb{Z}_p$-Gitter in Schritten von p^{2f^+}. Weil (L', b') aber höchstens zwei aufeinanderfolgende (p)-modulare Komponenten besitzt, muss der Rang der größeren Komponente in $2f^+$-Schritten steigen und der Rang der kleineren Komponente entsprechend kleiner werden. Insgesamt muss aber der Rang beider Komponenten stets ein Vielfaches von $2f^+$ sein. □

Proposition 2.11. *Seien $p \in \mathbb{P}(\mathbb{Q})\setminus\{\infty\}$ und $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Die über (p) liegenden Primideale in $\mathbb{Z}[\zeta_m+\overline{\zeta_m}]$ seien in der Erweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m+\overline{\zeta_m}]$ zerfallend. Des Weiteren seien π eine über p liegende Stelle und (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$-Gitter. Dann ist der Rang von jeder Komponente einer modularen Zerlegung des $\mathbb{Z}_p$-Gitters $(L, (\mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \times \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_{\overline{\pi}}}) \circ h)$ ein Vielfaches von $2f = 2f^+$.*

Beweis. Das hermitesche $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$-Gitter (L,h) besitzt nach Proposition 1.34 stets eine Orthogonalbasis und damit eine orthogonale Zerlegung in $(\pi^i, \overline{\pi}^i)$- modulare Komponenten von Rang 1. Sei $(L',h') \subseteq (L,h)$ mit $h' := h|_{L'}$ ein solches Teilgitter mit $\operatorname{rang}(L',h') = 1$. Weil $\mathbb{Z}[\zeta_m]_\pi \cong \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ ist, kann es als modulares, hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter von Rang 2 aufgefasst werden. Seine Gram-Matrix ist von der Form

$$\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$$

Die Spurkonstruktion liefert gemäß Lemma 2.8 ein $\mathbb{Z}_p$-Gitter $(L', \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h')$ mit höchstens zwei aufeinanderfolgenden modularen Komponenten. Ihre Ränge können mit Hilfe der Determinante bestimmt werden. Nach Lemma 2.3 gilt

$$\nu_p(\det_{\mathbb{Z}_p}(L', \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h')) = \nu_p((\operatorname{disc}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^2) + \nu_p(\operatorname{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\det_{\mathbb{Z}[\zeta_m]_\pi}(L',h')))$$

Die Differente ist ein Ideal der Form (π^a). Die Diskriminante ist nach Bemerkung 1.27 die Norm der Differente, also $\operatorname{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\pi^a) = p^{fa}$. Damit gilt: $2f \mid \nu_p((\operatorname{disc}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^2)$. Aufgrund der Gram-Matrix ist die Determinante von (L',h') von der Form $u\pi^{2i}$ für ein $u \in \mathbb{Z}[\zeta_m]_\pi^*$ und ein $i \in \mathbb{N}$. Deshalb ist ihre Norm ebenfalls von der Form $u'p^{2fi}$ für ein $u' \in \mathbb{Z}_p^*$. Also muss $\nu_p(\det_{\mathbb{Z}_p}(L', \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h'))$ ein Vielfaches von $2f$ sein. Das $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$-Gitter mit der Gram-Matrix $(\pi^{-a}, \overline{\pi^{-a}})$ besitzt ein unimodulares Spurgitter. Mit jeder größeren π-Potenz vergrößert sich die Determinante als $\mathbb{Z}_p$-Gitter in Schritten von p^{2f^+}. Weil es aber nach Lemma 2.8 höchstens zwei aufeinanderfolgende, (p)-modulare Komponenten gibt, muss der Rang der größeren Komponente in $2f^+$-Schritten steigen und der Rang der kleineren Komponente entsprechend kleiner werden. Insgesamt muss aber der Rang jeder Komponente stets ein Vielfaches von $2f^+$ sein. □

Proposition 2.12. *Sei $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$. Des Weiteren seien $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$ und (L,b) ein $\mathbb{Z}$-Gitter, das einen Automorphismus mit Minimalpolynom Φ_m besitzt. Dann sind die Ränge der Komponenten einer p-modularen Zerlegung ein Vielfaches von $2f^+$.*

Beweis. Das Gitter (L,b) kann als hermitesches $\mathbb{Z}[\zeta_m]$-Gitter (L,h) aufgefasst werden. Die Lokalisierung liefert ein Gitter über dem Ring $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m] \cong \prod_{(\pi)|(p)} \mathbb{Z}[\zeta_m]_\pi$. Falls m keine Primzahlpotenz ist, ist die Körpererweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ stets unverzweigt. Seien π' eine über p liegende Stelle von $\mathbb{Z}[\zeta_m+\zeta_m^{-1}]$ und π eine über π' liegende Stelle von $\mathbb{Z}[\zeta_m]$. Dann ist auch die Erweiterung $\mathbb{Z}[\zeta_m]_\pi/\mathbb{Z}[\zeta_m+\zeta_m^{-1}]_{\pi'}$ unverzweigt. Falls $m = q^t$ ist, betrachtet man wegen $m' > 2$ nur Stellen $p \neq q$. Auch in diesem Fall ist die Erweiterung $\mathbb{Z}[\zeta_m]_\pi/\mathbb{Z}[\zeta_m+\zeta_m^{-1}]_{\pi'}$ unverzweigt. Mit Hilfe der entsprechenden vollständigen Menge primitiver Idempotente kann das Gitter $\mathbb{Z}_p \otimes_{\mathbb{Z}} (L,h)$ analog zu Proposition 1.35 orthogonal zerlegt werden. Es gibt zwei Möglichkeiten:

$$\textbf{(i)}\mathbb{Z}_p \otimes_{\mathbb{Z}} (L,h) \cong \perp e_\pi(L,h) \qquad \textbf{(ii)}\mathbb{Z}_p \otimes_{\mathbb{Z}} (L,h) \cong \perp e_\pi(L,h) \oplus e_{\overline{\pi}}(L,h)$$

Im ersten Fall folgt die Behauptung aus Proposition 2.10 und im zweiten Fall aus Proposition 2.11. □

Bemerkung 2.13. Für $m = p^t$ ist die Erweiterung $\mathbb{Q}[\zeta_m]_{1-\zeta_m}/\mathbb{Q}_p$ rein verzweigt und es gilt $f = f^+ = 1$. Damit ist der Rang jeder modularen Komponente ein Vielfaches von f oder f^+. Im Allgemeinen ist sie aber kein Vielfaches von $2 = 2f^+$. Ein einfaches Beispiel hierfür ist das Gitter $A_2 \in \mathrm{II}_2(3^{-1})$. Es besitzt eine hermitesche Struktur von Rang 1 über $\mathbb{Z}[\zeta_3]$ und die Determinante 3. Damit muss es in einer 3-modularen Zerlegung eine unimodulare Komponente von Rang 1 und eine (3)-modulare Komponente von Rang 1 geben.
Für Gitter, die eine hermitesche Struktur von Rang 1 besitzen, kann trotzdem eine Aussage getroffen werden. Weil die Quadratklasse ihrer Determinante nach Bemerkung 2.6 für $p \neq 2$ gleich $p \cdot (\mathbb{Q}^*)^2$ ist und diese Gitter nach Lemma 2.8 nur zwei nicht-triviale, aufeinanderfolgende, p-modulare Komponenten besitzen, muss die Komponente, deren Skalenideal eine ungerade Potenz besitzt, einen ungeraden Rang besitzen. Weil der Rang des gesamten Gitters gerade ist, muss auch die andere nicht-triviale Komponente einen ungeraden Rang besitzen. Die Ränge können aber nicht weiter eingeschränkt werden, wie man mit Hilfe der Gitter A_{p-1} sieht. Sie besitzen eine hermitesche $\mathbb{Z}[\zeta_m]$-Struktur von Rang 1. Durch Multiplikation mit $(1-\zeta_m)^i\overline{(1-\zeta_m)^i}$ kann man zu jeder p-modularen Zerlegung der obigen Form ein Gitter finden, das diese Zerlegung realisiert. Für $p = 2$ ist die Quadratklasse $(\mathbb{Q}^*)^2$. Man folgert analog, dass die Ränge der modularen Komponenten in diesem Fall stets gerade sind, also ein Vielfaches von $2f^+$.

Um die Einschränkungen der Ränge der modularen Komponenten zu erhalten, reicht die Existenz einer hermiteschen Struktur aus. Ihre konkrete Form war irrelevant. Als nächstes werden die Paritäten im 2-adischen Geschlechtssymbol von $\mathbb{Z}$-Gittern mit einer zusätzlichen hermiteschen Struktur über $\mathbb{Z}[\zeta_m]$ untersucht. Hierbei ist die genaue hermitesche Struktur des Gitters entscheidend, was das folgende Beispiel zeigen soll:

Beispiel 2.14. Seien $\mathbb{Z}$-Gitter mit folgenden Gram-Matrizen gegeben:

$$D_4: \begin{pmatrix} 2 & -1 & 0 & 1 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 1 & 0 & -1 & 2 \end{pmatrix} \quad \text{und} \quad I_4: \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Die Gitter $D_4 \perp D_4$ und $I_4 \perp {}^2I_4$ besitzen eine Struktur über $\mathbb{Z}[\zeta_8]$ von Rang 2. Das Gitter $D_4 \perp D_4$ besitzt das 2-adische Geschlechtssymbol $(2^0)_{\mathrm{II}}^{+4}(2^1)_{\mathrm{II}}^{+4}$ und das Gitter $I_4 \perp {}^2I_4$ das Symbol $(2^0)_4^{+4}(2^1)_4^{+4}$. In beiden Fällen stimmen die Ränge und die Vorzeichen der modularen Komponenten überein, aber nicht ihre Paritäten und Oddities. Daher wird im weiteren Verlauf die Parität der modularen Komponenten von Spurgittern mit einer gegebenen hermiteschen Struktur bestimmt.

Definition 2.15. Sei $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und E/F eine Erweiterung von nicht-archimedischen lokalen Körpern mit $[E : \mathbb{Q}_p] < \infty$. Für die maximalen Ideale $\mathfrak{P}_E$ und $\mathfrak{P}_F$ gilt dann $\mathfrak{P}_F\mathfrak{O}_E = \mathfrak{P}_E^e$. Falls $(e, p) = 1$ ist, heißt E/F **zahm verzweigt**. Andernfalls **wild verzweigt**.

Die folgende Proposition findet man in [Frö83] auf Seite 26:

Proposition 2.16. *Sei E/F eine Erweiterung von nicht-archimedischen lokalen Körpern mit $[E : \mathbb{Q}_p] < \infty$. Dann ist E/F genau dann zahm verzweigt, wenn $\mathrm{Spur}_F^E(\mathfrak{O}_E) = \mathfrak{O}_F$ ist.*

Damit kann die Parität im Fall $m \neq 2^t$ bestimmt werden:

Proposition 2.17. *Sei (L, b) ein $\mathbb{Z}$-Gitter mit einem Automorphismus der Ordnung $m \neq 2^t$ und Minimalpolynom Φ_m. Dann ist die Parität von jeder nicht-trivialen Komponente in der 2-modularen Zerlegung gerade.*

Beweis. Das Gitter (L, b) kann auch als hermitesches $\mathbb{Z}[\zeta_m]$-Gitter (L, h) aufgefasst werden. Weil $m \neq 2^t$ ist, ist die Körpererweiterung $\mathbb{Q}_2[\zeta_m] : \mathbb{Q}_2[\zeta_m + \overline{\zeta_m}]$ zahm verzweigt. Aus Proposition 2.16 folgt, dass die Spur surjektiv auf den Ganzheitsringen ist. Damit gibt es ein Element $c \in \mathbb{Z}_2[\zeta_m]$ mit $1 = \mathrm{Spur}_{\mathbb{Q}_2[\zeta_m+\overline{\zeta_m}]}^{\mathbb{Q}_2[\zeta_m]}(c) = c + \overline{c}$. Sei nun eine beliebige 2-modulare Zerlegung gegeben:

$$\mathbb{Z}_2 \otimes_{\mathbb{Z}} L \cong \bigperp_{i\in\mathbb{Z}} L_i$$

Dann ist die reskalierte i-te Komponente ${}^{2^{-i}}L_i$ unimodular und für jedes $v \in {}^{2^{-i}}L_i$ folgt

$$\begin{aligned} b(v,v) &= \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h(v,v)) = \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(c+\overline{c})(h(v,v)) \\ &= \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(ch(v,v))) + \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\overline{ch(v,v)}) \\ &= 2 \cdot \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(c \cdot h(v,v)) \end{aligned}$$

Weil $h(v, v) \in (\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^{-1}$ und $c \in \mathbb{Z}_2$ ist, muss auch $c \cdot h(v, v) \in (\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi})^{-1}$ sein. Also ist $2 \cdot \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(c \cdot h(v, v)) \in 2\mathbb{Z}_2$. □

Beispiel 2.18. Falls $m = 2^t$ ist, gibt es ungerade Gitter mit einer hermiteschen Struktur über dem Ganzheitsring des m-ten Kreisteilungskörpers. So besitzt zum Beispiel das Standardgitter I_2 eine hermitesche Struktur von Rang 1 über $\mathbb{Z}[i]$.

Als nächstes wird genauer untersucht, wann ungerade Gitter auftreten können. Hermitesche $\mathbb{Z}[\zeta_m]$-Gitter können im verzweigten Fall nach [Jac62] Proposition 4.3 als orthogonale Summe von modularen Teilgittern von Rang 1 oder 2 geschrieben werden, wobei die Diagonaleinträge der Gram-Matrix der Gitter mit Rang 2 eine größere Bewertung besitzen als die beiden anderen Einträge. Deshalb reicht es zu prüfen, welche Skalenideale von diesen Gittertypen ungerade $\mathbb{Z}_2$-Gitter liefern.

Lemma 2.19. *Seien $m := p^t$ und die Erweiterung $\mathbb{Q}_p[\zeta_m]/\mathbb{Q}_p$ gegeben. Dann ist $B := \{\zeta_m^i \mid i \in \{0, 1, \ldots \varphi(m) - 1\}\}$ eine Ganzheitsbasis.*

Beweis. Das m-te Kreisteilungspolynom ist über $\mathbb{Z}_p$ irreduzibel. Dies kann analog zu der Irreduzibilität in $\mathbb{Z}$ mit Hilfe des Eisensteinkriteriums bewiesen werden. Damit folgt, dass die Galoisgruppe der Erweiterung $\mathbb{Q}_p[\zeta_m]/\mathbb{Q}_p$ transitiv auf den Einheitswurzeln operiert und die Galoisautomorphismen ebenfalls von der Form $\sigma_k : \zeta_m \mapsto \zeta_m^k$ für $0 \leq k \leq m$ mit $(k, m) = 1$ sind. Nach [Neu92] Satz 10.2 auf Seite 63 ist B eine Ganzheitsbasis der Erweiterung $\mathbb{Q}[\zeta_m]/\mathbb{Q}$. Die Diskriminante $\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]}$ kann mit ihrer Hilfe als die Determinante der Matrix $(\sigma_k(\zeta_m^i))$ berechnet werden. Weil die Galoisautomorphismen die Einheitswurzeln in beiden Erweiterungen auf dieselbe Art abbilden, besitzt die Matrix $(\sigma_k(\zeta_m^i))$ über $\mathbb{Z}_p$ dieselben Einträge und damit auch dieselbe Determinante. Da (p) in der Erweiterung $\mathbb{Q}_p[\zeta_m]/\mathbb{Q}_p$ rein verzweigt ist, folgt andererseits nach Bemerkung 1.27, dass $\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} \mathbb{Z}_p[\zeta_m] = \operatorname{disc}_{\mathbb{Q}_p}^{\mathbb{Q}_p[\zeta_m]}$ ist. Damit besitzt der von B erzeugte Modul dieselbe Diskriminante wie der von einer Ganzheitsbasis erzeugte Modul. Also ist B nach [Lan86] Proposition 10 auf Seite 65 eine Ganzheitsbasis. □

Proposition 2.20. *Es seien $m = 2^t$ und die Körpererweiterung $\mathbb{Q}_2[\zeta_m] : \mathbb{Q}_2$ gegeben. Sei a so, dass die Differente $\mathfrak{D}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]} = (\pi^a)$ mit $\pi := 1 - \zeta_m$ ist. Des Weiteren seien (L, h) ein (π^j)-modulares $\mathbb{Z}[\zeta_m]$-Gitter von Rang 1 und $b := \operatorname{Spur} \circ h$. Dann ist (L, b) genau dann ungerade, wenn $j = -a + ie$ für ein $i \in \mathbb{N}_0$ ist.*

Beweis. " $\Leftarrow$ " Sei ohne Einschränkung $i = 0$ angenommen. Weil der $\operatorname{rang}_{\mathbb{Z}[\zeta_m]}(L, h) = 1$ ist und $\mathbb{Z}_2[\zeta_m]$ ein lokaler Ring ist, besitzt (L, h) eine Basis $\{v\}$. Nach Lemma 2.19 ist $\{\zeta_m^i \cdot v \mid i \in \{0, 1, \ldots \varphi(m) - 1\}\}$ eine $\mathbb{Z}_2$-Basis. Fasst man L als $\mathbb{Z}_2$-Gitter mit Bilinearform b und Automorphismus g auf, dann bildet $\{g^i(v) \mid i \in \{0, 1, \ldots, \varphi(m) - 1\}\}$ eine Basis von (L, b) und es gilt:

$$b(g^i(v), g^i(v)) = b(v, v) = \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h(v, v))$$

Weil h (π^{-a})-modular ist, folgt aus der Definition der Differente, dass (L, b) ganzzahlig ist und dass a maximal mit dieser Eigenschaft ist. Angenommen, $\operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h(v, v))$ wäre in $2\mathbb{Z}_2$. Dann wäre $b(g^i(v), g^j(v)) = \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\zeta_m^{i-j} h(v, v))$. Weil ζ_m^{i-j} eine Einheit ist, liegt $\operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\zeta_m^{i-j} h(v, v))$ ebenfalls in $2\mathbb{Z}_2$. Das bedeutet aber, dass a nicht maximal wäre und man erhält einen Widerspruch. Damit sind die (π^{-a})-modularen Gitter ungerade.
" $\Rightarrow$ " Weil $\mathbb{Q}_2[\zeta_m]/\mathbb{Q}_2$ rein verzweigt ist, gilt bis auf Multiplikation mit Einheiten $\pi^j \in \mathbb{Q}_2[\zeta_m + \overline{\zeta_m}] \Leftrightarrow 2|j$. Sei (L, h) nun (π^{-a+2j})-modular für ein $j \in \{1, \ldots, e-1\}$. Dann ist $h' := (\pi\overline{\pi})^{-1} h$ eine $(\pi^{-a+2(j-1)})$-modulare Form und nach obigen Überlegungen ist (L, h') ganzzahlig. Sei $L \cong \perp L_k$ eine (2)-modulare Zerlegung von (L, b). Für alle $w \in {}^{2^{-k}}L_k$ gilt:

$$\begin{aligned}
b(w, w) &= \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h(w, w)) = \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\pi\overline{\pi} h'(w, w)) \\
&= \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}((2 - \zeta_m - \overline{\zeta_m}) h'(w, w)) \\
&= 2 \cdot \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h'(w, w)) - \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\zeta_m h'(w, w)) - \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\overline{\zeta_m h'(w, w)}) \\
&= 2 \cdot (\operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h'(w, w)) - \operatorname{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\zeta_m h'(w, w))) \in 2\mathbb{Z}_2
\end{aligned}$$ □

Man kann nun zu dem Beispiel 2.14 zurückkehren und die hermiteschen Strukturen der Gitter betrachten.

Beispiel 2.21. Sei $\pi := 1 - \zeta_8$. Die hermiteschen Gram-Matrizen der Gitter sind:

$$D_4 \perp D_4: \quad \frac{1}{4}\begin{pmatrix} \pi\overline{\pi} & 0 \\ 0 & \pi\overline{\pi} \end{pmatrix} \qquad \text{und} \qquad I_4 \perp {}^2I_4: \quad \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Mit $\mathfrak{D}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_8]} = (4)$ sieht man, dass I_4 als hermitesches Gitter $(\mathfrak{D}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_8]})^{-1}$-modular ist und D_4 $\pi\overline{\pi}(\mathfrak{D}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_8]})^{-1}$-modular. Damit besitzen die Gitter $I_4 \perp {}^2I_4$ und $D_4 \perp D_4$ als hermitesche Gitter verschiedene Strukturen. Durch die Spurkonstruktion werden sie auf $\mathbb{Z}$-Gitter abgebildet die sich nur durch die Parität und Oddity unterscheiden.

Abschließend wird die Parität im letzten Fall geprüft.

Proposition 2.22. *Es seien $m = 2^t$ und die Körpererweiterung $\mathbb{Q}_2[\zeta_m] : \mathbb{Q}_2$ gegeben. Sei a so, dass die Differente $\mathfrak{D}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]} = (\pi^a)$ mit $\pi := 1 - \zeta_m$ ist. Sei (L, h) ein modulares $\mathbb{Z}_2[\zeta_m]$-Gitter mit der Gram-Matrix*

$$\begin{pmatrix} c_{1,1} & c_{1,2} \\ \overline{c_{1,2}} & c_{2,2} \end{pmatrix}$$

wobei $\nu_\pi(c_{1,1}) > \nu_\pi(c_{1,2})$ und $\nu_\pi(c_{2,2}) > \nu_\pi(c_{1,2})$ gelte. Dann ist jede modulare Komponente von $(L, \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]} \circ h)$ gerade.

Beweis. Sei (L, h) zunächst $(\mathfrak{D}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]})^{-1}$-modular. Nach Lemma 2.8 ist $(L, \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]} \circ h)$ unimodular. Des Weiteren sei $\{v_1, v_2\}$ eine Basis von (L, h). Zu einem beliebigen $w \in L$ gibt es also $\lambda_i \in \mathbb{Z}_2[\zeta_m]$ mit $w = \lambda_1 v_1 + \lambda_2 v_2$ und es gilt:

$$\begin{aligned} b(w,w) &= \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(h(\lambda_1 v_1 + \lambda_2 v_2, \lambda_1 v_1 + \lambda_2 v_2)) \\ &= \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_1\overline{\lambda_1}h(v_1,v_1)) + \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_2\overline{\lambda_2}h(v_2,v_2)) \\ &\quad + \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_1\overline{\lambda_2}h(v_1,v_2)) + \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_2\overline{\lambda_1}h(v_2,v_1)) \end{aligned}$$

Es gilt: $\mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_1\overline{\lambda_2}h(v_1,v_2)) = \mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_2\overline{\lambda_1}h(v_2,v_1))$. Analog zur Rechnung am Ende des Beweises von Proposition 2.20 zeigt man, dass $\mathrm{Spur}_{\mathbb{Q}_2}^{\mathbb{Q}_2[\zeta_m]}(\lambda_j\overline{\lambda_j}h(v_j,v_j)) \in 2\mathbb{Z}_2$ ist. Damit folgt $b(w,w) \in 2\mathbb{Z}_2$. Die Rechnung zeigt des Weiteren, dass (L, h) gerade, modulare Komponenten besitzen muss, falls es (π^{2i-a})-modular für ein $i > 0$ ist. □

2.2 Rationale Invarianten hermitescher $\mathbb{Z}[\zeta_m]$-Gitter II

Auch in diesem Abschnitt werden $\mathbb{Z}$-Gitter mit einer zusätzlichen $\mathbb{Z}[\zeta_m]$-Struktur untersucht. Zunächst wird ein Zusammenhang zwischen den Vorzeichen im Geschlechtssymbol und den Hasse-Invarianten des unterliegenden Raums hergeleitet. Anschließend werden die Ränge der modularen Komponenten eines $\mathbb{Z}$-Geschlechts, für die im vorherigen Abschnitt notwendige Bedingungen gefunden wurden, als gegeben angesehen und die verbleibenden Invarianten berechnet.

Definition 2.23. Sei K ein lokaler Körper mit Stelle p. Mit $(a_i, a_j)_p$ wird das Hilbert-Symbol bezeichnet. Es besitzt Werte in der Brauergruppe. Weil sie über lokalen Körpern nur zwei Elemente besitzt, kann sie wie üblich mit $\{\pm 1\}$ identifiziert werden. Ist $\langle a_1, a_2, \ldots, a_n\rangle$ eine Diagonalisierung einer quadratischen Form über einem lokalen Körper, so bezeichnet $s_p(\langle a_1, a_2, \ldots, a_n\rangle) := \prod_{i<j}(a_i, a_j)_p$ die **Hasse-Invariante**.

Bemerkung 2.24. Einige Autoren wie zum Beispiel O'Meara bilden das Produkt über alle $i \leq j$. Dies kann zwar andere Werte für die Hasse-Invariante liefern, aber sie erfüllt in beiden Fällen ihren Zweck und kann die beiden möglichen quadratischen Vektorräume mit derselben Dimension und derselben Determinante unterscheiden. Auch wenn einige konkrete Formeln etwas anders aussehen, stimmen praktisch alle Sätze, die für eine Definition gelten, modifiziert ebenfalls für die andere Definition. Weitere Details zu den Unterschieden und zur Umrechnung findet man in [Ger08] auf Seite 87.

Proposition 2.25.

(a) Sei K ein lokaler Körper mit nicht-archimedischer Stelle p. Dann sind zwei (reguläre) quadratische K-Vektorräume $(V, b), (V', b')$ genau dann isometrisch, wenn die folgenden Bedingungen erfüllt sind:

- $\dim(V, b) = \dim(V', b')$,
- $\det(V, b) = \det(V', b')$ *und*
- $s_p(V, b) = s_p(V', b')$

(b) Sei $L : K$ eine quadratische Körpererweiterung lokaler Körper über nicht-archimedischen Stellen und L besitze eine Involution mit Fixkörper K. Zwei hermitesche L-Vektorräume $(V, h), (V', h')$ sind genau dann isometrisch, wenn die folgenden Bedingungen erfüllt sind:

- $\dim(V, h) = \dim(V', h')$ *und*
- $\det(V, h)/\operatorname{Norm}_K^L(L^*) = \det(V', h')/\operatorname{Norm}_K^L(L^*)$

Beweis. Teil (a) wird in [O'M63] Theorem 63:20 bewiesen. Weil K ein lokaler Körper mit nicht-archimedischer Stelle ist, ist jede 5-dimensionale quadratische Form über K isotrop (vgl. [O'M63] 63:19). Damit folgt Teil (b) aus [Sch85] Seite 351 Beispiel 1.6 (ii). □

Man sieht, dass ein hermitescher Raum über lokalen Körpern nur durch die Dimension und die Determinante bis auf Isometrie eindeutig festgelegt wird. Durch die Spurkonstruktion sind die Dimension und die Determinante des $\mathbb{Q}_p$-Vektorraums ebenfalls festgelegt. Mit diesen Invarianten gibt es im Wesentlichen zwei verschiedene quadratische Räume, die durch die Hasse-Invariante unterschieden werden (vgl. [O'M63] 63:22). Weil es unter gewissen Voraussetzungen einen Zusammenhang zwischen den Hasse-Invariante und den Vorzeichen im Geschlechtssymbol gibt, liefert dieses Prinzip Einschränkungen für die Vorzeichen und die Oddity im Geschlechtssymbol von $\mathbb{Z}$-Gittern mit einer $\mathbb{Z}[\zeta_m]$-Struktur. Diese Voraussetzungen sollen zunächst genauer untersucht werden.

Proposition 2.26. *Sei (L, b) ein ganzzahliges Gitter auf dem quadratischen Raum (V, b) und $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty, 2\}$ mit $p \nmid \det(L, b)$. Dann gilt*

$$s_p(L, b) = 1$$

Beweis. Sei $\langle a_1 p^{b_1}, a_2 p^{b_2}, \ldots, a_n p^{b_n} \rangle$ eine Diagonalisierung über $\mathbb{Z}_p$ mit $p \nmid a_i$. Da L ganzzahlig ist, muss $b_i \geq 0$ sein, und weil $p \nmid \det(L)$, folgt $b_i = 0$. Damit ist

$$s_p(L) = \prod_{i<j} (a_i, a_j)_p = 1$$

□

Die Hasse-Invariante an den Stellen 2 und ∞ kann man nicht auf diese Art bestimmen, denn in beiden Fällen gibt es Räume mit derselben ungeraden Determinante und verschiedenen Invarianten.

Beispiel 2.27.

$$\begin{aligned} s_2(\langle 3,3,3\rangle) = -1 &\neq 1 = s_2(\langle 27,1,1\rangle) \\ s_\infty(\langle 3,3,3\rangle) = 1 &\neq -1 = s_\infty(\langle -3,-3,3\rangle) \end{aligned}$$

Definition 2.28. Ein $\mathbb{Z}$-Gitter heißt **lokal quadratfrei**, wenn in seiner modularen Zerlegung alle Komponenten mit den Skalenidealen (p^i) für $i \notin \{0, 1\}$ trivial sind. Ein $\mathbb{Z}_p$-Gitter mit dieser Eigenschaft nennt man **quadratfrei**. Ein $\mathbb{Z}$-Gitter heißt **quadratfrei**, wenn es an jeder Stelle lokal quadratfrei ist. Ein Gitter (L, b) mit $p(L, b)^\# \subseteq (L, b)$ heißt **p-elementar**.

Die folgende Proposition stellt einen Zusammenhang zwischen dem Vorzeichen der (p)-modularen Komponente eines quadratfreien Gitters und der Hasse-Invariante des unterliegenden Raums her.

Proposition 2.29.

(a) Es sei p eine ungerade Primzahl. Dann ist die Hasse-Invariante eines $\mathbb{Z}$-Gitters (L, b) mit dem lokalen Geschlechtssymbol $(p^0)^{\epsilon_{p,0} n_{p,0}} (p^1)^{\epsilon_{p,1} n_{p,1}}$ und $n_{p,1} > 0$ gleich

$$s_p(L, b) = \begin{cases} \epsilon_{p,1} (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,1}(n_{p,1}-1)}{2}} \left(\frac{c}{p}\right)^{n_{p,1}} & \text{falls } n_{p,1} \neq n \\ \epsilon_{p,1}^{n_{p,1}-1} (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,1}(n_{p,1}-1)}{2}} & \text{falls } n_{p,1} = n \end{cases}$$

wobei $n := \operatorname{rang}_{\mathbb{Z}}(L)$ und $c := \frac{\det(L,b)}{p^{n_{p,1}}}$ sind.

(b) Besitzt (L, b) die Signatur (t, u), dann ist

$$s_\infty = (-1)^{\frac{u(u-1)}{2}}$$

Beweis. Sei $n_{p,1} \neq n$. Zur Berechnung von s_p für $p < \infty$ bestimmt man eine p-adische Diagonalisierung der Form mit Hilfe des Geschlechtssymbols:

$$\langle \delta_1 \underbrace{p, p, \ldots, p}_{n_{p,1} \text{ - mal}}, \delta_0, 1, \ldots, 1 \rangle$$

wobei δ_1 gemäß der Definition des Geschlechtssymbols für $p \neq 2$ genau dann ein Quadrat ist, wenn $\epsilon_{p,1} = +1$ ist. Die Quadratklasse von δ_0 ist $c\delta_1 \cdot (\mathbb{Q}^*)^2$. Damit kann nun die Hasse-Invariante berechnet werden:

$$\begin{aligned} s_p &= (p,p)_p^{\frac{n_{p,1}(n_{p,1}-1)}{2}} \cdot (\delta_1, p)_p^{n_{p,1}-1} \cdot (p, \delta_0)_p^{n_{p,1}} \cdot (\delta_1, \delta_0)_p \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,1}(n_{p,1}-1)}{2}} \cdot \left(\frac{\delta_1}{p}\right)^{n_{p,1}-1} \cdot \left(\frac{\delta_0}{p}\right)^{n_{p,1}} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,1}(n_{p,1}-1)}{2}} \cdot \left(\frac{\delta_1}{p}\right) \cdot \left(\frac{c}{p}\right)^{n_{p,1}} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,1}(n_{p,1}-1)}{2}} \cdot \epsilon_{p,1} \cdot \left(\frac{c}{p}\right)^{n_{p,1}} \end{aligned}$$

Falls $n_{p,1} = n$ ist, so ist die Diagonalisierung der Form

$$\langle \delta_1 p, p, \ldots, p \rangle$$

wobei δ_1 wie oben definiert ist. Die Berechnung von s_p verläuft analog. Die Hasse-Invariante Stelle -1 berechnet man mit Hilfe der Diagonalisierung, die man direkt aus der Signatur (t, u) ablesen kann:

$$\langle \underbrace{1, \ldots, 1}_{t}, \underbrace{-1, \ldots, -1}_{u} \rangle$$

Damit folgt $s_\infty = (-1)^{\frac{u(u-1)}{2}}$. □

An der Stelle 2 gibt es im Allgemeinen keinen solchen Zusammenhang. Man kann jedoch die Ergebnisse über die Parität des Spurgitters anwenden, um Aussagen über später relevante Spezialfälle treffen zu können.

Bemerkung 2.30. Sei π eine dyadische Stelle. Ein $\mathbb{Z}[\zeta_m]_\pi$-Gitter (L, h), das für $m \neq 2^t$ nicht (π^{a+ei})-modular ist, muss gemäß Proposition 2.20 gerade modulare Komponenten besitzen. Des Weiteren ist der Rang jeder modularen Komponente ein Vielfaches von $2f^+$. Für den trägen und zerfallenden Fall folgt dies aus den Propositionen 2.10 und 2.11. Im verzweigten Fall sei (L, h) ein Gitter über dem Ring $\mathbb{Z}_2 \otimes \mathbb{Z}[\zeta_m]$ von Rang 1. Es ist also die Lokalisierung eines globalen $\mathbb{Z}$-Gitters. Daher besitzt es dieselbe Determinante wie das $\mathbb{Z}$-Gitter, also nach Bemerkung 2.6 ein Quadrat. Weil (L, h) nach Lemma 2.8 nur zwei aufeinanderfolgende modulare Komponenten besitzt und der $\mathbb{Z}$-Rang von L gleich $\varphi(m) \equiv_2 0$ ist, müssen beide modularen Komponenten einen geraden Rang haben. Also ist jede modulare Komponente von $(L, \mathrm{Spur} \circ h)$ orthogonale Summe von hyperbolischen Ebenen und

möglicherweise einem geraden, anisotropen Gitter von Rang 2.

Für die relevanten Fälle kann man damit einen Zusammenhang zwischen den Vorzeichen im dyadischen Geschlechtssymbol quadratfreier Gitter und der Hasse-Invariante des unterliegenden $\mathbb{Q}_2$-Vektorraums herstellen. Zunächst benötigt man das folgende Lemma, das mit vollständiger Induktion direkt aus der Definition hergeleitet werden kann.

Lemma 2.31. *Seien (V_i, b_i) quadratische $\mathbb{Q}_p$-Vektorräume. Dann gilt:*

$$s_p(\bigperp_{i=1}^{n} V_i) = \prod_{i=1}^{n} s_p(V_i) \cdot \prod_{i<j} (\det(V_i), \det(V_j))_p$$

Proposition 2.32. *Die Hasse-Invariante eines $\mathbb{Z}_2$-Gitters (L, b) mit dem Geschlechtssymbol $1_{\mathrm{II}}^{\epsilon_{2,0} n_{2,0}} 2_{\mathrm{II}}^{\epsilon_{2,1} n_{2,1}}$, wobei $n_{2,1} > 0$ ist, lautet*

$$s_2(L) = \begin{cases} \epsilon_{2,0} \cdot (-1)^{\frac{n^2-2n}{8}} & \text{falls } n_{2,1} < n \\ (-1)^{\frac{n(n-2)}{8}} & \text{falls } n_{2,1} = n \end{cases}$$

Beweis. Sei $\mathbb{A}$ das $\mathbb{Z}_2$-Gitter mit der Gram-Matrix:

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

Weil die modularen Komponenten skalierte, gerade, unimodulare $\mathbb{Z}_2$-Gitter sind, ist jede zu einem der folgenden Gitter isometrisch (vgl. [Kit03] Theorem 5.2.5):

$$\mathbb{A} \perp \mathbb{H} \perp \ldots \perp \mathbb{H}$$
$$\mathbb{H} \perp \mathbb{H} \perp \ldots \perp \mathbb{H}$$

Im ersten Fall ist das Vorzeichen -1 und im zweiten Fall entsprechend $+1$. Insbesondere sind die Ränge der modularen Komponenten gerade. Die Hasse-Invariante der modularen Komponenten kann mit Hilfe von Lemma 2.31 unter Verwendung von $s_2(\mathbb{H}) = 1 = s_2({}^2\mathbb{H})$ und $s_2(\mathbb{A}) = -1 = -s_2({}^2\mathbb{A})$ berechnet werden. Sei m der halbe Rang der modularen Komponente. Dann gilt:

$$\begin{aligned} s_2(\mathbb{H} \perp \mathbb{H} \perp \ldots \perp \mathbb{H}) &= (-1)^{\frac{m(m-1)}{2}} \\ s_2(\mathbb{A} \perp \mathbb{H} \perp \ldots \perp \mathbb{H}) &= -(-1)^{\frac{m(m-1)}{2}} \\ s_2({}^2\mathbb{H} \perp {}^2\mathbb{H} \perp \ldots \perp {}^2\mathbb{H}) &= (-1)^{\frac{m(m-1)}{2}} \\ s_2({}^2\mathbb{A} \perp {}^2\mathbb{H} \perp \ldots \perp {}^2\mathbb{H}) &= (-1)^{\frac{m(m-1)}{2}} \end{aligned}$$

Damit folgt die Behauptung für $n = n_{2,1}$. Für $n_{2,1} < n$ wendet man anschließend noch einmal Lemma 2.31 an. □

Um Fallunterscheidungen zu vermeiden, wird für $n_{2,0} = 0$ im Folgenden $\epsilon_{2,0} = 1$ gesetzt.

Lemma 2.33. *Seien $(L,b) \subseteq (L',b)$ zwei quadratfreie $\mathbb{Z}_p$-Gitter auf dem $\mathbb{Q}_p$-Vektorraum (V,b) mit $\det(L,b) = \det(L',b) \cdot p^i$ für $i \equiv_4 0$. Dann besitzen die Geschlechtssymbole beider Gitter dieselben Vorzeichen.*

Beweis. Seien $(p^0)^{\epsilon_{p,0} n_{p,0}} (p^1)^{\epsilon_{p,1} n_{p,1}}$ und $(p^0)^{\epsilon'_{p,0} n'_{p,0}} (p^1)^{\epsilon'_{p,1} n'_{p,1}}$ die lokalen Geschlechtssymbole von (L,b) und (L',b) und $n := \operatorname{rang}(L,b)$. Dann gilt nach Proposition 2.29 und Proposition 2.32 die folgende Beziehung:

$$\begin{aligned}
\epsilon_{p,1} = &\quad s_p(L,b) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,1}(n_{p,1}-1)}{2}} \left(\tfrac{c}{p}\right)^{n_{p,1}} \\
= &\quad s_p(L',b) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{n'_{p,1}(n'_{p,1}-1)}{2}} \left(\tfrac{c}{p}\right)^{n'_{p,1}} = \epsilon'_{p,1} \quad \text{falls } p \neq 2 \\
\epsilon_{2,0} = &\quad s_2(L,b) \cdot (-1)^{\frac{n^2-2n}{8}} = \epsilon'_{2,0} \qquad\qquad\qquad\qquad \text{falls } p = 2
\end{aligned}$$

Die übrigen Vorzeichen erhält man mit dem gleichen Schluss für die reskalierten Dualgitter ${}^{p}(L',b)^{\#} \subseteq {}^{p}(L,b)^{\#}$. □

Bemerkung 2.34. Als Konsequenz aus dem Lemma ergibt sich, dass sich die modularen Komponenten der beiden Gitter um eine gerade Anzahl hyperbolischer Ebenen unterscheiden müssen.

Proposition 2.35. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$, $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Des Weiteren seien $(\pi') \subseteq \mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ ein Primideal über (p), sodass $(\pi) := (\pi')\mathbb{Z}[\zeta_m]$ ebenfalls ein Primideal ist, und (L,h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi$-Gitter mit Rang 1. Das lokale Geschlechtssymbol von $(L, \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h)$ sei $(p^i)^{\epsilon_{p,i} n_{p,i}} (p^{i+1})^{\epsilon_{p,i+1} n_{p,i+1}}$. Dann sind die Vorzeichen:*

$$\begin{aligned}
\epsilon_{p,i} &= \begin{cases} (-(-1)^{\frac{p-1}{2} \cdot f^+})^{\frac{n_{p,i}}{f}} & \text{falls } p \neq 2 \\ (-1)^{\frac{n_{p,i}}{f}} & \text{falls } p = 2 \end{cases} \\
\epsilon_{p,i+1} &= \begin{cases} (-(-1)^{\frac{p-1}{2} \cdot f^+})^{\frac{n_{p,i+1}}{f}} & \text{falls } p \neq 2 \\ (-1)^{\frac{n_{p,i+1}}{f}} & \text{falls } p = 2 \end{cases}
\end{aligned}$$

Beweis. Aus Lemma 2.8 folgt mit $b := \operatorname{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h$, dass (L,b) höchstens zwei nichttriviale, aufeinanderfolgende (p)-modulare Komponenten mit den Skalenidealen (p^i) und (p^{i+1}) besitzt. Man kann ohne Einschränkung $i = 0$ annehmen. Um für $p = 2$ Aussagen mit Hilfe der Diskriminantengruppe treffen zu können, ist es nötig, anstelle der Bilinearform b die quadratische Form $q(x) := \frac{1}{2} b(x,x)$ zu betrachten. Weil nach Lemma 2.17 jede Komponente einer (2)-modularen Zerlegung gerade ist, besitzt q Werte in $\mathbb{Z}_p$. Da $\operatorname{rang}(L,h) = 1$ ist, muss (L,h) modular sein. Sei $\operatorname{Scale}(L,h) = (\pi^k)$ für ein k und $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} = (\pi^a)$ für ein a. Dann muss $-a \leq k < -a + e$ gelten. Falls sogar $-a + 2 \leq k < -a + e$ gilt, betrachtet man das skalierte Gitter $(L',h) := (\pi^{-1}L, h)$. Für dieses Gitter gilt:

$$(L',q) = (L',h) \supseteq (L,h) = (L,q)$$

Die quadratischen Gitter sind nach Konstruktion quadratfrei und ihre Determinanten un-

terscheiden sich nach Lemma 2.3 um $\mathrm{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\pi^2) = p^{2f}$, wobei $f = 2f^+$ gerade ist. Damit folgt aus Lemma 2.33, dass beide Gitter dieselben Vorzeichen besitzen. Daher kann man ohne Einschränkung annehmen, dass $k - a \in \{0, 1\}$ ist. Falls $k - a = 0$ gilt, ist das Spurgitter (L, q) nach Lemma 2.8 ein unimodulares $\mathbb{Z}_p$-Gitter, dessen unterliegender Raum nach [Neb99] Seite 59 hyperbolisch ist. Deshalb ist auch (L, q) hyperbolisch. Für gerade $k - a$ ist die (p)-modulare Komponente nicht-trivial, aber stets hyperbolisch, weil sich die modularen Komponenten der Gitter nur um eine gerade Anzahl an hyperbolischen Ebenen unterscheiden. Daraus folgt, dass die Vorzeichen der nicht-trivialen Komponenten an der Stelle 2 stets + sind. Für $p \neq 2$ besitzen die nicht-trivialen Komponenten die Determinante $(-1)^{fj} = 1$ für ein j. Die Vorzeichen sind daher stets $+1$. Falls $k - a = 1$ ist, besitzt das Gitter (L, q) eine nicht-triviale, (p)-modulare Komponente. Seine Diskriminantengruppe $(L, q)^\#/(L, q)$ ist ein f-dimensionaler $\mathbb{F}_p$-Vektorraum, der nach [Neb99] Seite 59 von der Form $(\mathbb{F}_p[\zeta_{m'}], \mathrm{Spur}_{\mathbb{F}_p}^{\mathbb{F}_p[\zeta_{m'}+\overline{\zeta_{m'}}]}(\alpha x\overline{x}))$ für ein $\alpha \in \mathbb{F}_p[\zeta_{m'} + \overline{\zeta_{m'}}]$ ist. Dieser Raum ist nach [Neb99] Satz 3.3.4 nicht hyperbolisch. Aus dem Henselschen Lemma (vgl. [Kne02] Satz 15.6) folgt, dass die (p)-modulare Komponente von (L, q) ebenfalls nicht hyperbolisch ist. Also ist das Vorzeichen $\epsilon_{2,1}$ stets -1. Für $p \neq 2$ besitzt die (p)-modulare Komponente die Determinante $\delta(-1)^{\frac{f}{2}}$ für ein $\delta \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$. Sie ist genau dann kein Quadrat, wenn (-1) ein Quadrat ist oder $f^+ = \frac{f}{2}$ gerade ist. Für $p \neq 2$ ist das Vorzeichen also $\epsilon_{p,1} = -(-1)^{\frac{p-1}{2} \cdot f^+}$. Ob der erste oder der zweite Fall eintritt, hängt davon ab, ob der Bruch $\frac{n_{p,1}}{f}$ gerade oder ungerade ist. Daher decken die Ausdrücke $\epsilon_{p,1} = (-(-1)^{\frac{p-1}{2} \cdot f^+})^{\frac{n_{p,1}}{f}}$ und $\epsilon_{2,1} = (-1)^{\frac{n_{2,1}}{f}}$ beide Fälle ab. Das Vorzeichen der anderen Komponente erhält man, indem man den Beweis für das reskalierte Dualgitter ${}^p(L, b)^\#$ wiederholt. □

Gitter mit einer hermiteschen Struktur mit beliebigem Rang besitzen im trägen Fall nach Proposition 1.31 für alle $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ eine Orthogonalbasis. Damit kann dieser Fall auf Proposition 2.35 zurückgeführt werden und man erhält das folgende Korollar.

Korollar 2.36. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$, $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Des Weiteren seien $(\pi') \subseteq \mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ ein Primideal über (p), sodass $(\pi')\mathbb{Z}[\zeta_m]$ ebenfalls ein Primideal ist. Dann besitzt ein quadratisches $\mathbb{Z}$-Gitter (L, b) mit einem Automorphismus mit Minimalpolynom Φ_m das lokale Geschlechtssymbol $(p^0)^{\epsilon_{p,0} n_{p,0}} (p^1)^{\epsilon_{p,1} n_{p,1}} \dots (p^j)^{\epsilon_{p,j} n_{p,j}}$. Die Vorzeichen sind:*

$$\epsilon_{p,i} \quad = \quad \begin{cases} (-(-1)^{\frac{p-1}{2} \cdot f^+})^{\frac{n_{p,i}}{f}} & \text{falls } p \neq 2 \\ (-1)^{\frac{n_{p,i}}{f}} & \text{falls } p = 2 \end{cases}$$

Proposition 2.37. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$, $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Des Weiteren seien $(\pi') \subseteq \mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ ein Primideal über (p), sodass $(\pi')\mathbb{Z}[\zeta_m] = (\pi)(\overline{\pi})$ für ein Primideal (π) ist, und (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$-Gitter mit Rang 1. Dann besitzt $(L, (\mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \times \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_{\overline{\pi}}}) \circ h)$ das lokale Geschlechtssymbol $(p^i)^{\epsilon_{p,i} n_{p,i}} (p^{i+1})^{\epsilon_{p,i+1} n_{p,i+1}}$. Dabei sind beide Komponenten stets hyperbolisch und die Vorzeichen sind:*

$$\epsilon_{p,i} = \begin{cases} (-1)^{\frac{p-1}{2}\cdot\frac{n_{p,i}}{2}} & \textit{falls } p \neq 2 \\ +1 & \textit{falls } p = 2 \end{cases}$$
$$\epsilon_{p,i+1} = \begin{cases} (-1)^{\frac{p-1}{2}\cdot\frac{n_{p,i+1}}{2}} & \textit{falls } p \neq 2 \\ +1 & \textit{falls } p = 2 \end{cases}$$

Beweis. Man kann (L,h) auch als $\mathbb{Z}[\zeta_m]_\pi$-Gitter mit Rang 2 auffassen. Aus Lemma 2.8 folgt mit $b := \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \circ h$, dass (L,b) höchstens zwei nicht-triviale, aufeinanderfolgende (p)-modulare Komponenten mit den Skalenidealen (p^i) und (p^{i+1}) besitzt. Man kann ohne Einschränkung $i = 0$ annehmen. Um für $p = 2$ Aussagen mit Hilfe der Diskriminantengruppe treffen zu können, ist es nötig, anstelle der Bilinearform b die quadratische Form $q(x) := \frac{1}{2}b(x,x)$ zu betrachten, die nach Lemma 2.17 Werte in $\mathbb{Z}_p$ besitzt. Da $\mathrm{rang}(L,h) = 1$ ist, muss (L,h) modular sein. Sei $\mathrm{Scale}(L,h) = (\pi^k, \overline{\pi^k})$ für ein k und $\mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \times \mathfrak{D}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_{\overline{\pi}}} = (\pi^a, \overline{\pi^a})$ für ein a. Dann muss $-a \leq k < -a + e$ gelten. Falls sogar $-a + 2 \leq k < -a + e$ gilt, betrachtet man das skalierte Gitter $(L',h) := ((\pi^{-1}, \overline{\pi^{-1}})L, h)$. Für dieses Gitter gilt:

$$(L',q) = (L',h) \supseteq (L,h) = (L,q)$$

Die quadratischen Gitter sind nach Konstruktion quadratfrei und ihre Determinanten unterscheiden sich nach Lemma 2.3 um $\mathrm{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi}(\pi^2) \cdot \mathrm{Norm}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_{\overline{\pi}}}(\overline{\pi^2}) = p^{4f}$. Damit folgt aus Lemma 2.33, dass beide Gitter dieselben Vorzeichen besitzen. Daher kann man ohne Einschränkung annehmen, dass $k - a \in \{0,1\}$ ist. Falls $k - a = 0$ gilt, ist das Spurgitter (L,q) nach Lemma 2.8 ein unimodulares $\mathbb{Z}_p$-Gitter auf dem hyperbolischen Raum (vgl. [Neb99] Seite 59). Deshalb ist auch (L,q) hyperbolisch. Für gerade $k - a$ ist die (p)-modulare Komponente nicht-trivial, aber stets hyperbolisch, denn die modularen Komponenten beider Gitter unterscheiden sich durch eine gerade Anzahl an hyperbolischen Ebenen. Damit sind die Vorzeichen der nicht-trivialen Komponenten an der Stelle 2 stets $+1$. Für $p \neq 2$ besitzen die nicht-trivialen Komponenten die Determinante $(-1)^{2fj} = 1$ für ein j. Die Vorzeichen sind daher stets $+1$. Falls $k - a = 1$ ist, besitzt das Gitter (L,q) eine nicht-triviale, (p)-modulare Komponente. Seine Diskriminantengruppe $(L,q)^\#/(L,q)$ ist ein $2f$-dimensionaler $\mathbb{F}_p$-Vektorraum, der nach Konstruktion hyperbolisch sein muss. Also folgt aus dem Henselschen Lemma (vgl. [Kne02] Satz 15.6), dass die (p)-modulare Komponente von (L,q) ebenfalls hyperbolisch ist. Für $p = 2$ ist $\epsilon_{2,1} = 1$. Für $p \neq 2$ ist die Determinante $(-1)^{\frac{n_{p,1}}{2}}$. Sie ist genau dann ein Quadrat, wenn (-1) ein Quadrat oder $n_{p,1} \equiv_4 0$ ist. Also ist $\epsilon_{p,1} = (-1)^{\frac{p-1}{2}\cdot\frac{n_{p,i}}{2}}$. Das Vorzeichen der anderen Komponente erhält man, indem man den Beweis für das reskalierte Dualgitter ${}^p(L,b)^\#$ wiederholt. □

Gitter mit einer hermiteschen Struktur mit beliebigem Rang besitzen auch im zerfallenden Fall nach Proposition 1.34 für alle $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ eine Orthogonalbasis. Damit kann dieser Fall auf Proposition 2.37 zurückgeführt werden.

Korollar 2.38. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$, $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Des Weiteren seien $(\pi') \subseteq \mathbb{Z}[\zeta_m + \overline{\zeta_m}]$ ein Primideal über (p), sodass $(\pi')\mathbb{Z}[\zeta_m] = (\pi)(\overline{\pi})$ für ein Primideal (π) ist, und (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ Gitter. Dann besitzt $(L, (\mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_\pi} \times \mathrm{Spur}_{\mathbb{Q}_p}^{\mathbb{Q}[\zeta_m]_{\overline{\pi}}}) \circ h)$ das lokale Geschlechtssymbol $(p^0)^{\epsilon_{p,0} n_{p,0}} (p^1)^{\epsilon_{p,1} n_{p,1}} \ldots (p^j)^{\epsilon_{p,j} n_{p,j}}$. Dabei sind beide Komponenten stets hyperbolisch und die Vorzeichen sind:*

$$\epsilon_{p,i} \quad = \quad \begin{cases} (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,i}}{2}} & \text{falls } p \neq 2 \\ +1 & \text{falls } p = 2 \end{cases}$$

Die Ergebnisse für $\mathbb{Z}_p$-Gitter mit einer zusätzlichen $\mathbb{Z}[\zeta_m]_\pi$ oder $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ -Struktur kann man nun in dem folgenden Satz zusammenführen, um eine Aussage über die Vorzeichen im Geschlechtssymbol von $\mathbb{Z}_p$-Gittern mit einer zusätzlichen $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m]$ -Struktur treffen zu können. Diese Gitter treten als Lokalisierungen von $\mathbb{Z}$-Gittern mit einem Automorphismus mit Minimalpolynom Φ_m auf.

Satz 2.39. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und $m \in \mathbb{N}$ mit $m = p^t m'$ für ein $m' > 2$. Dann besitzt ein quadratisches $\mathbb{Z}$-Gitter (L, b) mit einem Automorphismus mit Minimalpolynom Φ_m das lokale Geschlechtssymbol $(p^0)^{\epsilon_{p,0} n_{p,0}} (p^1)^{\epsilon_{p,1} n_{p,1}} \ldots (p^j)^{\epsilon_{p,j} n_{p,j}}$. Die Vorzeichen sind:*

$$\epsilon_{p,i} \quad = \quad \begin{cases} (-1)^{\frac{n_{p,i}}{f}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{n_{p,i}}{2}} & \text{falls } p \neq 2 \\ (-1)^{\frac{n_{p,i}}{f}} & \text{falls } p = 2 \end{cases}$$

Beweis. Das Gitter (L, b) kann als hermitesches $\mathbb{Z}[\zeta_m]$-Gitter (L, h) aufgefasst werden. Die Lokalisierung liefert ein Gitter über dem Ring $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m] \cong \prod_{(\pi)|(p)} \mathbb{Z}[\zeta_m]_\pi$. Falls m keine Primzahlpotenz ist, ist die Körpererweiterung $\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ stets unverzweigt. Damit ist auch die Erweiterung $\mathbb{Z}[\zeta_m]_\pi / \mathbb{Z}[\zeta_m + \zeta_m^{-1}]_{\pi'}$ unverzweigt. Falls $m = q^t$ ist, betrachtet man wegen $m' > 2$ nur Stellen $p \neq q$. Auch in diesem Fall ist die Erweiterung $\mathbb{Z}[\zeta_m]_\pi / \mathbb{Z}[\zeta_m + \zeta_m^{-1}]_{\pi'}$ unverzweigt. Mit Hilfe der entsprechenden, vollständigen Menge primitiver Idempotente kann das Gitter $\mathbb{Z}_p \otimes_{\mathbb{Z}} L$ wie im Beweis zu Proposition 1.36 orthogonal zerlegt werden. Es gibt zwei Möglichkeiten:

$$\textbf{(i)} \mathbb{Z}_p \otimes_{\mathbb{Z}} L \cong \perp e_\pi L \qquad \textbf{(ii)} \mathbb{Z}_p \otimes_{\mathbb{Z}} L \cong \perp e_\pi L \oplus e_{\overline{\pi}} L$$

Im trägen Fall folgt die Behauptung aus Korollar 2.36. Im zerfallenden Fall folgt die Behauptung aus Korollar 2.38. □

Im trägen und zerfallenden Fall ist das Vorzeichen einer p-modularen Komponente demnach unabhängig von allen anderen Stellen. Der verzweigte Fall verhält sich anders. Dort kann es zu festem Rang und fester Determinante zwei verschiedene hermitesche Formen geben, deren Spurformen zu quadratischen Formen führen, die sich nur durch die Hasse-Invariante unterscheiden.

Beispiel 2.40. Man betrachte das $\mathbb{Z}$-Gitter A_6, welches die Gram-Matrix

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

besitzt. Es liegt im Geschlecht $\mathrm{II}_6(7^{-1})$ und besitzt einen Automorphismus der Ordnung 7. Das Gitter ${}^3A_6$ liegt wegen $\left(\frac{3}{7}\right) = -1$ und $\left(\frac{7}{3}\right) = 1$ in dem Geschlecht $\mathrm{II}_6(3^{+6}7^{+1})$, das Gitter ${}^7A_6$ in $\mathrm{II}_6(7^{-5}49^{-1})$ und das Gitter ${}^{21}A_6$ in $\mathrm{II}_6(3^{+6}7^{+5}49^{+1})$. Damit folgt:

$$ {}^3A_6 \perp {}^7A_6 \in \mathrm{II}_{12}(3^{+6}7^{-6}49^{-1}) \quad \text{und} \quad A_6 \perp {}^{21}A_6 \in \mathrm{II}_{12}(3^{+6}7^{-6}49^{+1}) $$

Offensichtlich besitzen beide Gitter einen fixpunktfreien Automorphismus der Ordnung 7 und ihre modularen Komponenten besitzen dieselben Ränge, aber im Gegensatz zum trägen und zerfallenden Fall sind die Vorzeichen nicht eindeutig festgelegt.

Das Gitter in obigem Beispiel besitzt zwei entscheidende Eigenschaften. Es ist nicht quadratfrei und sein Rang als hermitesches Gitter ist größer als 1. Betrachtet man aber Gitter, die Rang 1 besitzen oder quadratfrei sind, kann man die Vorzeichen mit Hilfe der Hasse-Invarianten bestimmen. Dafür muss zunächst die Hasse-Invariante an allen von p verschiedenen Stellen berechnet werden:

Lemma 2.41. *Seien $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ und (L,b) ein $\mathbb{Z}$-Gitter, das einen Automorphismus g mit Minimalpolynom Φ_{p^t} besitzt. Falls $p = 2$ ist, sei $t > 1$. Des Weiteren sei (d^+, d^-) die Signatur von (L,b) und $n := \mathrm{rang}_{\mathbb{Z}}(L,b)$. Dann gilt:*

$$ s_p(L,b) = \begin{cases} (-1)^{\frac{n(n-2)}{8} + \frac{n}{f(2)} + \frac{d_-}{2}} \prod_{l \in \mathbb{P}(\mathbb{Q}) \setminus \{p,\infty\}} (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} & \text{falls } p \neq 2 \\ (-1)^{\frac{d_-}{2}} \prod_{l \in \mathbb{P}(\mathbb{Q}) \setminus \{2,\infty\}} (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} & \text{falls } p = 2 \end{cases} $$

Beweis. Sei $l \in \mathbb{P}(\mathbb{Q}) \setminus \{2, p, \infty\}$. Des Weiteren sei $(l^0)^{\epsilon_{l,0} n_{l,0}} (l^1)^{\epsilon_{l,1} n_{l,1}} \ldots$ das lokale Geschlechtssymbol von (L,b). Mit seiner Hilfe kann man unmittelbar eine Diagonalisierung der Form ablesen. Durch Skalieren der Basisvektoren von modularen Komponenten erhält man ein quadratfreies Gitter. Seine (p)-modulare Komponente besitzt den Rang $n'_{l,1} := \sum_{i \in \mathbb{Z}} n_{l,2i+1}$ und das Vorzeichen $\epsilon'_{l,1} := \prod_{i \in \mathbb{Z}} \epsilon_{l,2i+1}$. Mit Hilfe von Proposition 2.29 und Satz 2.39 kann man damit die Hasse-Invariante $s_l(L,b)$ berechnen.

$$ \begin{aligned} s_l(L,b) &= (-1)^{\frac{l-1}{2} \cdot \frac{n'_{l,1}(n'_{l,1}-1)}{2}} \cdot \epsilon'_{l,1} = (-1)^{\frac{l-1}{2} \cdot \frac{n'_{l,1}(n'_{l,1}-1)}{2}} \cdot (-1)^{\frac{n'_{l,1}}{f(l)}} \cdot (-1)^{\frac{l-1}{2} \cdot \frac{n'_{l,1}}{2}} \\ &= (-1)^{\frac{n'_{l,1}}{f(l)}} = (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} \end{aligned} $$

Für $l = \infty$ gilt nach Proposition 2.29 $s_\infty(L,b) = (-1)^{\frac{d_-}{2}}$. Damit folgt die Behauptung für

$p = 2$ aus der Produktformel für die Hasse-Invariante (vgl. [O'M63] Theorem 72:1).
Zuletzt wird $s_2(L,b)$ für $p \neq 2$ berechnet. In diesem Fall sind nach Proposition 2.17 alle Komponenten einer 2-modularen Zerlegung von (L,b) gerade. Wie zuvor kann das 2-adische Geschlecht $(2^0)_{\mathrm{II}}^{\epsilon_{2,0}n_{2,0}}(2^1)_{\mathrm{II}}^{\epsilon_{2,1}n_{2,1}}\ldots$ von (L,b) durch Skalieren der höheren modularen Komponenten zu einem quadratfreien Geschlecht auf demselben Raum reduziert werden. Man definiert $n'_{2,0} := \sum_{i\in\mathbb{Z}} n_{l,2i}$ und $\epsilon'_{2,0} := \prod_{i\in\mathbb{Z}} \epsilon_{l,2i}$. Dann ist die Hasse-Invariante $s_2(L,b)$ nach Proposition 2.32 und Satz 2.39

$$\begin{aligned} s_2(L,b) &= \epsilon'_{2,0}\cdot(-1)^{\frac{n(n-2)}{8}} = (-1)^{\frac{n'_{2,0}}{f(2)}}\cdot(-1)^{\frac{n(n-2)}{8}} \\ &= (-1)^{\frac{\nu_2(\det(L,b))+n}{f(2)}}\cdot(-1)^{\frac{n(n-2)}{8}} \end{aligned}$$

Aus der Produktformel für die Hasse-Invariante folgt die Behauptung. □

Bemerkung 2.42. Das obige Resultat kann man auch mit etwas mehr Aufwand unter Verwendung von [Neb99] Satz 3.3.14 (iii) erhalten.

Damit kann man nun im verzweigten Fall die Vorzeichen für Gitter berechnen, die an der Stelle p lokal quadratfrei sind:

Proposition 2.43. *Seien $p \in \mathbb{P}(\mathbb{Q})\setminus\{\infty\}$ und (L,b) ein $\mathbb{Z}$-Gitter, das einen Automorphismus g mit Minimalpolynom Φ_{p^t} und das lokale Geschlechtssymbol $(p^0)^{\epsilon_{p,0}n_{p,0}}(p^1)^{\epsilon_{p,1}n_{p,1}}$ besitzt. Falls $p = 2$ ist, sei $t > 1$. Des Weiteren sei (d^+,d^-) die Signatur von (L,b) und $n := \mathrm{rang}_{\mathbb{Z}}(L,b)$. Mit $c := \frac{\det(L,b)}{p^{\nu_p(\det(L,b))}}$ gilt für $p \neq 2$:*

$$\begin{aligned} \epsilon_{p,1} &= (-1)^{\frac{p-1}{2}\cdot\frac{n_{p,1}-1}{2}+\frac{n(n-2)}{8}+\frac{n}{f(2)}+\frac{d_-}{2}} \prod_{l\in\mathbb{P}(\mathbb{Q})\setminus\{p,\infty\}} (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} \\ \epsilon_{p,0} &= \epsilon_{p,1}\left(\frac{c}{p}\right) \end{aligned}$$

Für $p = 2$ und $n_{2,0} = 0$ oder $n_{2,1} = 0$ gilt für das Vorzeichen der nicht-trivialen Komponente:

$$\epsilon_{2,i} = \left(\frac{c}{2}\right)$$

Falls $n_{2,0} > 0$ und $n_{2,1} > 0$ ist, gilt:

$$\begin{aligned} \epsilon_{2,0} &= (-1)^{\frac{d_-}{2}+\frac{n(n-2)}{8}} \prod_{l\in\mathbb{P}(\mathbb{Q})\setminus\{2,\infty\}} (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} \\ \epsilon_{2,1} &= \epsilon_{2,0}\left(\frac{c}{2}\right) \end{aligned}$$

Beweis. Die Berechnung von $\epsilon_{p,1}$ folgt für $p \neq 2$ aus Lemma 2.41 und Proposition 2.29.

$$\begin{aligned} \epsilon_{p,1} &= s_p(L,b)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{n_{p,1}(n_{p,1}-1)}{2}} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{n_{p,1}-1}{2}+\frac{n(n-2)}{8}+\frac{n}{f(2)}+\frac{d_-}{2}} \prod_{l\in\mathbb{P}(\mathbb{Q})\setminus\{p,\infty\}} (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} \end{aligned}$$

Aus der Definition des Geschlechtssymbols folgt damit die Behauptung für $\epsilon_{p,0}$. Aus der Definition folgt auch das Vorzeichen im Fall $p = 2$ und $n_{2,0} = 0$ oder $n_{2,1} = 0$. Falls $n_{2,0} > 0$ und $n_{2,1} > 0$ ist, kann man das Vorzeichen mit Hilfe von Proposition 2.32 berechnen.

$$\begin{aligned}
\epsilon_{2,0} &= s_2(L,b) \cdot (-1)^{\frac{n(n-2)}{8}} \\
&= (-1)^{\frac{d_-}{2}+\frac{n(n-2)}{8}} \prod_{l \in \mathbb{P}(\mathbb{Q})\setminus\{2,\infty\}} (-1)^{\frac{\nu_l(\det(L,b))}{f(l)}} \\
\epsilon_{2,1} &= \epsilon_{2,0} \left(\frac{c}{2}\right)
\end{aligned}$$

□

Bemerkung 2.44. Falls (L, h) den Rang 1 besitzt, kann man damit die Vorzeichen nicht quadratfreier Gitter bestimmen. Denn das zugehörige $\mathbb{Z}[\zeta_m]$-Gitter besitzt nach Lemma 2.8 nur zwei aufeinanderfolgende, nicht-triviale, modulare Komponenten. Damit kann dieser Fall auf den quadratfreien Fall zurückgeführt werden.

Also sind nun die Vorzeichen im Geschlechtssymbol von Gittern mit einem Automorphismus mit Minimalpolynom Φ_m in Abhängigkeit von den Rängen der modularen Komponenten bestimmt. Abschließend soll die Oddity für ungerade Gitter im dyadischen lokalen Symbol bestimmt werden. Gerade modulare Komponenten besitzen stets die Oddity 0. Daher spielt sie nur bei ungeraden modularen Komponenten eine Rolle. Wann diese auftreten können, wurde bereits in Abschnitt 2.1 untersucht. Nach Proposition 2.17 können solche Gitter höchstens für $m = 2^t$ auftreten und auch dort nur für einige hermitesche Strukturen.

Bemerkung 2.45. Seien $m := 2^t$ und (L, h) ein hermitesches $\mathbb{Z}[\zeta_m]$-Gitter. Die Lokalisierung ist ein Gitter über $\mathbb{Z}_2 \otimes \mathbb{Z}[\zeta_m] \cong \mathbb{Z}[\zeta_m]_{1-\zeta_m}$. Nach [Jac62] Proposition 4.3 kann man diese hermiteschen Gitter in eine orthogonale Summe von modularen Gittern von Rang 1 oder Rang 2 schreiben. Ungerade Gitter können nach Proposition 2.20 und Proposition 2.22 mit $\pi := 1 - \zeta_m$ nur bei (π^{-a+ie})-modularen, hermiteschen Gittern von Rang 1 auftreten. Deshalb kann man sich bei der Berechnung der Oddity auf diesen Fall beschränken.

Proposition 2.46. *Sei (L, b) ein ungerades, unimodulares $\mathbb{Z}_2$-Gitter von Rang 2 mit Determinante d und Hasse-Invariante s. Dann ist (L, b) isometrisch zu $\langle s, sd\rangle$.*

Beweis. Ungerade Gitter besitzen eine Orthogonalbasis, die um Einheiten abgeändert werden kann. Daher kann man annehmen, das (L, b) von der Form $\langle a_1, a_2\rangle$, wobei a_1 und a_2 aus einer der vier Quadratklassen stammen, die durch $1, 3, 5, 7$ oder $-7, -5, -3, -1$ repräsentiert werden. Von den 16 Gittern besitzen einige dasselbe Vorzeichen und dieselbe Oddity. Daher sind sie isometrisch.

$$\begin{aligned}
s = +1: \quad & \langle 1,1\rangle \cong \langle 5,5\rangle \\
& \langle 1,3\rangle \cong \langle 3,1\rangle \cong \langle 5,7\rangle \cong \langle 7,5\rangle \\
& \langle 1,5\rangle \cong \langle 5,1\rangle \\
& \langle 1,7\rangle \cong \langle 7,1\rangle \cong \langle 3,5\rangle \cong \langle 5,3\rangle \\
s = -1: \quad & \langle 3,3\rangle \cong \langle 7,7\rangle \\
& \langle 3,7\rangle \cong \langle 7,3\rangle
\end{aligned}$$

Man sieht, dass jede Isometrieklasse durch $\langle s, sd\rangle$ vertreten wird. □

Proposition 2.47. *Sei $m = 2^t$ für ein $t > 1$. Sei (L, h) ein (π^{a+ie})-modulares $\mathbb{Z}[\zeta_m]$-Gitter mit Rang 1. Sein (2^i)-modulares Spurgitter $(L, \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} \circ h)$ besitze die Determinante d und die Hasse-Invariante S. Dann ist seine Oddity*

$$\begin{cases} 2 & \text{falls } t = 2 \text{ und } S = 1 \\ 6 & \text{falls } t = 2 \text{ und } S = -1 \\ 4 & \text{falls } t = 3 \text{ und } S = 1 \\ 0 & \text{falls } t = 3 \text{ und } S = -1 \\ 0 & \text{falls } t > 3 \text{ und } S = 1 \\ 4 & \text{falls } t > 3 \text{ und } S = -1 \end{cases}$$

Beweis. Man kann ohne Einschränkung $i = 0$ annehmen. Man setzt $b := \mathrm{Spur}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} \circ h$. Für $t = 2$ folgt die Behauptung aus Proposition 2.46. Falls $t = 3$ ist, muss $\mathrm{rang}_{\mathbb{Z}_2}(L, b) = 4$ sein. Die Determinante d muss nach Bemerkung 2.6 ein Quadrat sein. Deshalb ist die unterliegende Form nach [Ger08] Proposition 4.24 genau dann anisotrop, wenn $S = 1$ ist. Weil ungerade unimodulare $\mathbb{Z}_2$-Gitter eine Orthogonalbasis besitzen, kann man nach [Kit03] Proposition 5.2.3. für $S = 1$ das gerade Gitter $\mathbb{A}$ und für $S = -1$ eine hyperbolische Ebene $\mathbb{H}$ abspalten. Also gibt es ein Gitter (L', b') von Rang 2 mit $b' := b|_{L'}$ mit

$$\begin{aligned} (L, b) &= \mathbb{A} \perp (L', b') \quad \text{falls } S = 1 \\ (L, b) &= \mathbb{H} \perp (L', b') \quad \text{falls } S = -1 \end{aligned}$$

Falls $S = 1$ ist, muss $\det(L', b') = 3$ gelten und damit folgt $s_2(L', b') = s_2(\mathbb{A}) \cdot S \cdot (3, 3)_2 = 1$. Aus Proposition 2.46 folgt dann, dass (L', b') isometrisch zum Gitter $\langle 1, 3\rangle$ ist. Seine Oddity ist 4. Weil $\mathbb{A}$ als gerades, unimodulares $\mathbb{Z}_2$-Gitter die Oddity 0 besitzt, muss auch (L, b) die Oddity 4 besitzen. Falls $S = -1$ ist, muss $\det(L', b') = -1$ gelten und damit folgt $s_2(L', b') = s_2(\mathbb{H}) \cdot S \cdot (-1, -1)_2 = 1$. Also muss (L', b') nach Proposition 2.46 isometrisch zu $\langle 1, -1\rangle$ sein und damit die Oddity 0 besitzen. Weil auch $\mathbb{H}$ als gerades, unimodulares $\mathbb{Z}_2$-Gitter die Oddity 0 besitzt, muss (L, b) die Oddity 0 besitzen. Falls $t > 3$ ist, kann man (L, b) nach [Kit03] Proposition 5.2.3. als Summe $(L'', b'') \perp \bigperp \mathbb{H}$ schreiben, wobei $b'' := b|_{L''}$ und $\mathrm{rang}_{\mathbb{Z}_2}(L'', b'') = 4$ ist. Die Anzahl der hyperbolischen Ebenen ist $\frac{\varphi(2^t)-4}{2} = 2^{t-2} - 2$. Weil $t > 3$ ist, ist die Anzahl also stets kongruent zu 2 mod 4. Damit folgt wie im Beweis von Proposition 2.32, dass $s_2(\bigperp \mathbb{H}) = -1$ ist. Außerdem ist $\det(\bigperp \mathbb{H}) = 1$. Damit folgt $s(L'', b'') = -s(L, b)$, $\det(L'', b'') = \det(L, b)$ und $\mathrm{oddity}(L'', b'') = \mathrm{oddity}(L, b)$. Damit kann dieser Fall auf den Fall $t = 3$ zurückgeführt werden. □

2.3 Mögliche $\mathbb{Z}G$-Strukturen in $\mathbb{Z}$-Geschlechtern

In diesem Abschnitt wird anhand von Beispielen gezeigt, wie man die Ergebnisse von Kapitel 2.1 und 2.2 verwenden kann, um Automorphismen mit gewissen Zerlegungstypen oder sogar ganze Automorphismenordnungen in $\mathbb{Z}$-Geschlechtern auszuschließen.

Beispiel 2.48. Das Geschlecht $\mathrm{II}_{14}(7^{+7})$ enthält keine Gitter mit einem Automorphismus der Ordnung 11 oder 13.

Beweis. Angenommen, es gäbe in diesem Geschlecht ein Gitter (L, b) mit einem Automorphismus der Ordnung 11. Dann müsste sein Zerlegungstyp $(1, 4)$ sein. Weil der Trägheitsindex $f^+(7) = 5$ ist, müsste L_{11} nach Proposition 2.12 und Bemerkung 2.6 das Geschlechtssymbol $\mathrm{II}_{14}(11^{-1})$ besitzen. Dann würde aber das Fixgitter L_1 den Rang 4 und eine (7)-modulare Komponente von Rang 7 besitzen. ↯ Ebenso zeigt man, dass es in diesem Geschlecht kein Gitter mit einem Automorphismus der Ordnung 13 geben kann. □

Beispiel 2.49. Das Geschlecht $\mathrm{II}_{12}(11^{+6})$ enthält keine Gitter mit einem Automorphismus der Ordnung 7 oder 13.

Beweis. Angenommen, es gäbe in diesem Geschlecht ein Gitter (L, b) mit einem Automorphismus der Ordnung 13. Dann müsste sein Zerlegungstyp $(1, 0)$ sein, das heißt, es gilt $L = L_{13}$. Nach Bemerkung 2.6 müsste die Quadratklasse der Determinante 13 sein.↯
Angenommen, es gäbe in diesem Geschlecht ein Gitter (L, b) mit einem Automorphismus der Ordnung 7. Dann muss der Zerlegungstyp $(2, 0)$ oder $(1, 6)$ sein. Der Typ $(2, 0)$ liefert nach Satz 2.39 einen Widerspruch zum Vorzeichen. Falls der Automorphismus den Typ $(1, 6)$ besitzt, ist L_7 wegen $f^+(11) = 3$ aus dem Geschlecht $\mathrm{II}_6(7^{-1})$ oder $\mathrm{II}_6(7^{-1}11^{-6})$. Die Vorzeichen ergeben sich aus Satz 2.39 und Proposition 2.43. Damit muss das Fixgitter aus $\mathrm{II}_6(7^{\epsilon 1}11^{-6})$ oder $\mathrm{II}_6(7^{\epsilon 1})$ sein. Weil man mit $L_7 \perp L_1$ dann aber ein Teilgitter mit Index 7^2 erhält, muss anschließend noch das entsprechende Obergitter gebildet werden. Die Obergitter entsprechen den total isotropen Untergruppen der Diskriminantengruppe. In diesem Fall gibt es genau dann ein Obergitter, wenn die Form $\langle -7, \delta 7\rangle$ isotrop ist, wobei δ genau dann ein Quadrat ist, wenn $\epsilon = +1$ ist. Weil $7 \cong_4 3$ ist, ist die Form genau dann isotrop, wenn δ ein Quadrat und $\epsilon = 1$ ist. Weil es aber nur ein Geschlecht (p)-elementarer Gitter gibt und diese aber nach [CS99] Seite 386 das Symbol $\mathrm{II}_6(7^{-1})$ besitzen, kann es kein Gitter mit dem Symbol $\mathrm{II}_6(7^{+1})$ geben. Das andere denkbare Symbol ist ein mit 11 skaliertes, elementares Gitter. Weil $\left(\frac{11}{7}\right) = 1$ ist, gibt es auch kein Gitter, das dieses Symbol besitzt, und man erhält einen Widerspruch. ↯ □

Bemerkung 2.50. Die Geschlechter in den beiden vorangegangenen Beispielen wurden von Rudolf Scharlau mit Hilfe des Programms TN, welches von Rudolf Scharlau und Boris Hemkemeier entwickelt worden war (vgl. [HS04]), vollständig klassifiziert. Mit diesem Resultat können die Beispiele nachgeprüft werden.

An dieser Stelle soll auch ein Beispiel für ein Geschlecht gegeben werden, bei dem es kein Gitter gibt, das einen Automorphismus mit einer gewissen Ordnung $m \notin \mathbb{P}(\mathbb{Q})$ besitzt.

Beispiel 2.51. Das Geschlecht des Gitters E_6 besitzt keinen Automorphismus der Ordnung 15.

Beweis. Das Geschlecht von E_6 besitzt nur eine Isometrieklasse (vgl. [Kne02] 28.13). Angenommen, E_6 besitzt einen Automorphismus der Ordnung 15.

Dann muss dieser wegen des Ranges den Typ $(0, 1, 1, 0)$ haben. Also existiert eine Zerlegung von E_6 in zwei Teilgitter $L_5 \perp L_3$, die jeweils den Rang 1 besitzen. Nach Bemerkung 2.6 sind die Quadratklassen ihrer Determinanten $5 \cdot (\mathbb{Q}^*)^2$ und $3 \cdot (\mathbb{Q}^*)^2$. Nach der Determinanten-Indexformel kann $(L_5 \perp L_3)$ dann aber kein Teilgitter von E_6 sein. □

In der Praxis zeigt sich, dass es für $m \notin \mathbb{P}(\mathbb{Q})$ häufig nicht möglich ist, alle Zerlegungstypen auszuschließen. Daher wird im folgenden Beispiel eine Struktur über $\mathbb{Z}[\zeta_m]$ ausgeschlossen.

Beispiel 2.52. Das Geschlecht $\mathrm{II}_{24}(3^{+6}5^{-6}7^{+4})$ ist das einzige Geschlecht quadratfreier Gitter mit Determinante $3^6 \cdot 5^6 \cdot 7^4$, das einen Automorphismus mit Minimalpolynom Φ_{21} enthält.

Beweis. Zu der gegebenen Determinante existieren acht mögliche Geschlechtssymbole, die sich nur durch die Vorzeichenkombinationen unterscheiden. Schließt man von den Vorzeichen auf die Hasseinvariante, so verstoßen vier Geschlechtssymbole gegen die Produktformel und können deshalb keine Gitter enthalten. Satz 2.39 besagt nun, dass von den verbleibenden vier Geschlechtern nur eines ein Gitter mit einem Automorphismus mit Minimalpolynom Φ_{21} besitzen kann. Mit Hilfe von $f(3) = 6$, $f(5) = 6$ und $f(7) = 1$ berechnet man das Symbol $\mathrm{II}_{24}(3^{+6}5^{-6}7^{+4})$. □

Mit den Methoden aus den Abschnitten 2.1 und 2.2 erhält man Bedingungen an das Teilgitter $\perp_{d|m,d\neq 1} L_d$, auf dem der Automorphismus operiert. Dies erlaubt dann Rückschlüsse auf das Fixgitter, sofern es denn überhaupt existiert. Diese Rückschlüsse können einen Widerspruch liefern, weil es kein Gitter mit den berechneten Eigenschaften gibt. Dies hängt aber vom Einzelfall ab. Allgemeine Aussagen kann man hierbei nicht treffen.

Bemerkung 2.53. Sei (L, b) ein Gitter mit einem Automorphismus der Ordnung $m \in \mathbb{N}$. Die folgenden Faktoren begünstigen den Ausschluss von Gittern mit gewissen Automorphismenordnungen in dem Geschlecht von (L, b).

- Das Fixgitter hat einen kleinen Rang. Die aufgestellten Bedingungen an das Fixgitter liefern dann eher einen Widerspruch (vgl. Beispiel 2.48).
- Der reelle Trägheitsindex f^+ ist für möglichst viele Primteiler der Determinante groß. Dies schränkt die Möglichkeiten für die Ränge der entsprechenden modularen Komponenten ein (vgl. Beispiel 2.48 und Beispiel 2.49).
- Die Automorphismenordnung m besitzt wenige Teiler. Dies reduziert zu Beginn die Anzahl der möglichen Zerlegungstypen. (vgl. Beispiel 2.48 und Beispiel 2.49).
- Der Rang des Gitters ist im Vergleich zur Automorphismenordnung klein. Auch dies reduziert die Anzahl der möglichen Zerlegungstypen (vgl. Beispiel 2.51)
- Die Determinante enthält viele Teiler. Von allen denkbaren Vorzeichenkombinationen kann für jeden Zerlegungstyp höchstens eine Kombination zu einem Geschlecht mit einem Gitter mit $\mathbb{Z}[\zeta]$-Struktur gehören (vgl. Beispiel2.52).

2.4 Konstruktion von Gittern mit einem Automorphismus

In diesem Abschnitt wird eine Methode zur Konstruktion von Gittern mit vorgegebenen Zerlegungstypen vorgestellt. Zusammen mit den bisherigen Ergebnissen des Kapitels werden in Spezialfällen exakte Aussagen zur Existenz von Gittern mit einem Automorphismus in einem vorgegebenen Geschlecht getroffen.

Klar ist, dass der Rang eines $\mathbb{Z}$-Gitters (L, b) mit einem Automorphismus mit Minimalpolynom Φ_m nicht kleiner als $\varphi(m)$ sein kann. Also ist der erste Schritt die Konstruktion von solchen Gittern mit Rang $\varphi(m)$. Eva Bayer-Fluckiger hat in [BF02] unter allgemeineren Voraussetzungen notwendige und hinreichende Bedingungen für ihre Existenz gefunden.

Theorem 2.54. *Seien K ein algebraischer Zahlkörper mit einer Involution und F der Fixkörper. Die Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \subseteq \mathcal{O}_K$ seien die Teiler der Differente $\mathfrak{D}_{\mathbb{Q}}^K$ mit ungeradem Exponenten. Sei s die Anzahl der reellen Einbettungen von F, die zu komplexen Einbettungen von K fortgesetzt werden. Des Weiteren seien $n := [F : Q]$, $n_+, n_- \in \mathbb{N} \setminus \{0\}$ mit $n_+ + n_- = 2n$ und $d \in \mathbb{Z} \setminus \{0\}$ mit $d/|d| = (-1)^{n_-}$.*
Es gibt genau dann ein ganzzahliges Gitter über K mit der Determinante d und der Signatur (n_+, n_-), wenn die folgenden Bedingungen erfüllt sind:

(I) $(n_+, n_-) \geq (n - s, n - s)$ *und* $(n_+, n_-) \equiv_2 (n - s, n - s)$

(II) $|d| = N(\mathfrak{P}_1 \ldots \mathfrak{P}_r) N(\mathfrak{Q}_1 \ldots \mathfrak{Q}_a) N(J)^2$ *, wobei $\mathfrak{Q}_1 \ldots \mathfrak{Q}_a$ gebrochene Ideale in $\mathcal{O}_K$ sind, die träge in der Erweiterung K/F sind, und J ein beliebiges gebrochenes Ideal in $\mathcal{O}_K$ ist.*

(III) Falls in der Erweiterung K/F kein Ideal verzweigt, gilt: $4a \equiv_8 n_+ - n_-$

Dieses Theorem kann für Gitter mit einer hermiteschen $\mathbb{Z}[\zeta_m]$-Struktur modifiziert werden, sodass man entsprechende Gitter mit einem vorgegebenen Geschlechtssymbol findet. Weil $\mathbb{Z}$-Geschlechter betrachtet werden, benötigt man eine zusätzliche Definition:

Definition 2.55. Sei (L, b) ein $\mathbb{Z}$-Gitter, das einen Automorphismus mit Minimalpolynom Φ_m besitzt. Außerdem seien $\mathrm{Scale}(\mathbb{Z}_p \otimes L, b) = (p^k)$, $R_{k-1} := 0$ sowie $c_i \geq 0$ und $R_i \in \{0, \ldots, e-1\}$, sodass $\frac{n_{p,i}}{2f^+} - R_{i-1} = c_i e + R_i$. Man sagt, dass (L, b) die **Kettenbedingung** an der Stelle p erfüllt, wenn $\frac{n_{p,i}}{2f^+} \geq e - R_{i-1}$ für alle $i > k$ gilt.

Bemerkung 2.56. Für $p \nmid m$ ist $e = 1$. Damit ist die Kettenbedingung in diesem Fall stets erfüllt. Sie ist jedoch wichtig, wenn m keine Primzahlpotenz ist und eine Stelle p mit $p|m$ betrachtet wird, denn nach Lemma 2.8 und Bemerkung 2.9 kann das Spurgitter eines modularen $\mathbb{Z}[\zeta_m]_\pi$-Gitters oder eines $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ -Gitters zwei aufeinanderfolgende, modulare Komponenten besitzen.

Satz 2.57. *Seien $n_{p,i}, m, n_+, n_- \in \mathbb{N}$ mit $\varphi(m) = n_+ + n_-$ so gewählt, dass sie die entsprechenden Einträge eines möglichen Geschlechtssymbols sind. In diesem Geschlecht gibt es*

genau dann ein ganzzahliges $\mathbb{Z}$-Gitter mit einem Automorphismus, der das Minimalpolynom Φ_m besitzt, wenn die folgenden Bedingungen erfüllt sind:

(i) $n_+ \equiv_2 0$ *und* $n_- \equiv_2 0$

(ii) Falls $m = q^t$ eine Primzahlpotenz ist, gilt für die Ränge der modularen Komponenten:

$$\begin{cases} 2f^+(p)|n_{p,i} & \text{für } p = q = 2 \text{ und für alle } p \in \mathbb{P}(\mathbb{Q}) \setminus \{q, \infty\} \\ n_{p,i} \equiv_2 1 & \text{für } p = q \neq 2 \end{cases}$$

Falls $m \neq q^t$ ist, muss $2f^+(p)|n_{p,i}$ für alle $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ gelten. Zusätzlich muss für alle p mit $p|m$ die Kettenbedingung erfüllt sein.

(iii) Falls $m \neq q^t$ ist, so gilt mit $a(p) := p^{\nu_p(m)-1}(p\nu_p(m) - \nu_p(m) - 1) + \sum_{i\in\mathbb{Z}} i \cdot \frac{n_{p,i}}{f(p)}$ die Beziehung:

$$4 \cdot \sum_{p\in\mathbb{P}(\mathbb{Q})\setminus\{\infty\}} a(p) \equiv_8 n_+ - n_-$$

Beweis. Seien die Bedingungen (i),(ii) und (iii) erfüllt. Zu zeigen ist, dass die Bedingungen (I),(II) und (III) mit $K = \mathbb{Q}[\zeta_m]$ erfüllt sind. In der Erweiterung $\mathbb{Q}[\zeta_m]/\mathbb{Q}[\zeta_m + \overline{\zeta_m}]$ wird jede reelle Einbettung von $\mathbb{Q}[\zeta_m + \overline{\zeta_m}]$ komplex fortgesetzt. Deshalb folgt (I). Um (II) zu zeigen, muss man die Ideale $\mathfrak{P}_i$, $\mathfrak{Q}_i$ und J geschickt wählen. Die Erweiterung $\mathbb{Q}[\zeta_m]/\mathbb{Q}[\zeta_m + \overline{\zeta_m}]$ ist genau dann verzweigt, wenn m eine Primzahlpotenz ist. Daher sind für $m \neq q^t$ die Ideale in der Differente $\mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m]} = \mathfrak{D}_{\mathbb{Q}[\zeta_m+\overline{\zeta_m}]}^{\mathbb{Q}[\zeta_m]} \cdot \mathfrak{D}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_m+\overline{\zeta_m}]} \cdot \mathbb{Z}[\zeta_m]$ vom zerfallenden Typ $\mathfrak{P}\overline{\mathfrak{P}}$ oder vom trägen Typ $\mathfrak{P}$. Im verzweigten Fall ist die Differente stets die Potenz von $(1-\zeta_m)$. Der Exponent ist für $p = 2$ gerade und für $p \neq 2$ ungerade. Wie zuvor müssen der verzweigte Fall und der unverzweigte Fall getrennt behandelt werden. Sei nun $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$ so, dass die über (p) liegenden Ideale in der Erweiterung $\mathbb{Q}[\zeta_m]/\mathbb{Q}[\zeta_m + \overline{\zeta_m}]$ unverzweigt sind. Falls die Primideale der Differente vom zerfallenden Typ $\mathfrak{P}\overline{\mathfrak{P}}$ sind, definiert man zunächst eine Menge von Idealen $J_{p,0}$, welche das Inverse von genau einem Vertreter von jedem Paar $\mathfrak{P}, \overline{\mathfrak{P}}$ enthält. Falls die Primideale der Differente vom trägen Typ sind, definiert man eine Menge von Idealen $Q_{p,0}$, die aus den Inversen dieser Ideale besteht. Führt man nun mit der Menge dieser Ideale die Idealgitterkonstruktion nach Bayer-Fluckiger durch, erhält man ein $\mathbb{Z}$-Gitter, das an der Stelle p unimodular ist. Seien nun p so, dass der träge Fall eintritt, sowie k der kleinste Index mit $n_{p,k} > 0$ und $r_{p,k} := n_{p,i} - \lfloor \frac{n_{p,i}}{e(p)f(p)} \rfloor \cdot e(p)f(p)$. Dann wählt man über (p) liegende Ideale $Q'_{p,k} := \{\mathfrak{Q}_{p,i}^{ek} \mid i \in \{1, \ldots, \lfloor \frac{n_{p,i}}{e(p)f(p)} \rfloor\}\}$. Der Exponent legt die modulare Komponente des Spurgitters fest, die hiermit konstruiert wird. Falls $p|m$, kann $e(p) > 1$ sein und man benötigt gegebenenfalls ein weiteres Ideal $\mathfrak{Q}_{p,\lceil \frac{n_{p,i}}{e(p)f(p)} \rceil}^{e(p)(k+1)-\frac{r_{p,k}}{f(p)}}$. Zusammen mit $Q'_{p,k}$ sei die Menge dieser Ideale $Q_{p,k}$. Bildet man mit den Idealen aus den Mengen $Q_{p,0}$ und $Q_{p,k}$ das Idealgitter und identifiziert die Stellen mit den Primidealen $\mathbb{Q}_{p,i}$, so zerfällt seine Lokalisierung $(\mathbb{Z}_p \otimes_{\mathbb{Z}} L, h) \cong \bigperp (e_{Q_{p,i}}L, h|_{e_{Q_{p,i}}L})$ konstruktionsbedingt in modulare, hermitesche $\mathbb{Z}[\zeta_m]_{Q_{p,i}}$-Gitter. Ihre Spurgitter sind nach Lemma 2.8 für $i \leq \lfloor \frac{n_{p,i}}{e(p)f(p)} \rfloor$ (p^k)-modular und für $i > \lceil \frac{n_{p,i}}{e(p)f(p)} \rceil$ unimodular. Falls $r_{p,i} > 0$ ist, muss das zu $i = \lceil \frac{n_{p,i}}{e(p)f(p)} \rceil$ gehörige Spurgitter eine (p^k)-modulare Komponente vom Rang $r_{p,k}$ und

eine (p^{k+1})-modulare Komponente vom Rang $e(p)f(p) - r_{p,k}$ besitzen, welche es nach der Voraussetzung (ii) auch gibt. Damit wurden die ersten Ideale so gewählt, dass der Rang der modularen Komponente mit dem größten Skalenideal genau $n_{p,k}$ ist und der Rang der folgenden Komponente $e(p)f(p) - r_{p,k}$. Nach diesem Prinzip wählt man die weiteren Ideale so aus, dass die modularen Komponenten des Spurgitters die angegebenen Ränge besitzen. Sei $Q_p := \bigcup_i Q_{p,i}$. Im zerfallenden Fall nehmen Ideale der Form $\mathfrak{R}_{p,i} \cdot \overline{\mathfrak{R}_{p,i}}$ den Platz der $\mathfrak{Q}_{p,i}$ ein. Ihre Wahl erfolgt nach demselben Prinzip. Wählt man für jedes entsprechende p und i aus jedem Paar $\mathfrak{R}_{p,i} \cdot \overline{\mathfrak{R}_{p,i}}$ genau ein Ideal aus und multipliziert diese, so erhält man das Ideal J aus der Idealgitterkonstruktion. Falls $m = q^t$ ist, kann das Spurgitter an der Stelle q nur zwei aufeinanderfolgende, modulare Komponenten besitzen. Man kann dies durch Multiplikation mit einem geeigneten Ideal der Form $(1-\zeta_q)^j\overline{(1-\zeta_q)}^j$ erreichen, wovon ein Faktor zu J hinzugefügt werden kann. Damit besitzen die gewählten Ideale nicht nur die richtige Norm. Sofern auch die Bedingung (III) erfüllt ist, besitzen die modularen Komponenten des Spurgitters von dem zugehörigen Idealgitter die vorgegebenen Ränge und erfüllen die Kettenbedingung. Also ist die Bedingung (II) erfüllt. Die Bedingung (III) ergibt sich aus (iii) durch das Zählen der gewählten Ideale. Für festes p gibt der Bruch $i \cdot \frac{n_{p,i}}{f(p)}$ die Anzahl der benötigten Ideale an, um eine modulare Komponente mit dem Skalenideal (p^i) und dem Rang $n_{p,i}$ zu konstruieren. Hinzu kommen $p^{\nu_p(m)-1}(p\nu_p(m) - \nu_p(m) - 1)$ Ideale, um die Differente auszugleichen.
Sei nun umgekehrt ein Gitter (L, b) mit einem Automorphismus mit Minimalpolynom Φ_m gegeben. Dann folgt (i) aus Korollar 1.39 und der erste Teil von (ii) aus Proposition 2.12 und Bemerkung 2.13. Man kann das Gitter (L, b) als hermitesches Gitter (L, h) auffassen. Wie in Proposition 1.36 beschrieben, zerfällt $(\mathbb{Z}_p \otimes_{\mathbb{Z}} L, h)$ in eine orthogonale Summe. Es gibt die beiden Fälle:

$$\textbf{(i)}\mathbb{Z}_p \otimes_{\mathbb{Z}} L \cong \perp e_\pi L \qquad \textbf{(ii)}\mathbb{Z}_p \otimes_{\mathbb{Z}} L \cong \perp e_\pi L \oplus e_{\overline{\pi}} L$$

Jedes $\mathbb{Z}[\zeta_m]_\pi$ und jedes $\mathbb{Z}[\zeta_m]_\pi \times \mathbb{Z}[\zeta_m]_{\overline{\pi}}$ - Gitter besitzt nach den Propositionen 1.31 und 1.34 eine orthogonale Zerlegung in modulare Komponenten. Gemäß Lemma 2.8 besitzen ihre Spurgitter wiederum höchstens zwei aufeinanderfolgende, modulare Komponenten. Des Weiteren erfüllt es konstruktionsbedingt die Kettenbedingung. Deshalb erfüllt auch $(\mathbb{Z}_p \otimes L, b)$ als orthogonale Summe solcher Gitter die Kettenbedingung. Zu dem Gitter (L, h) gibt es nach Theorem 2.54 Ideale, die die Bedingung (III) erfüllen. Analog zu obigen Überlegungen kann man über die Parität ihrer Anzahl die Bedingung (iii) verifizieren. □

Bemerkung 2.58. Im vorherigen Satz werden nur Bedingungen an die Ränge formuliert. In den Abschnitten 2.1 und 2.2 wurde bereits gezeigt, dass die übrigen Invarianten durch die Ränge und die Existenz eines Automorphismus bereits festgelegt sind. Die Vorzeichen sind in Satz 2.39 und Proposition 2.43 bestimmt worden. Weil der Rang des hermiteschen Gitters 1 ist, ist damit auch die Parität gemäß den Propositionen 2.17 und 2.20 bestimmt. Die Oddity für die ungeraden Gitter wurde in Proposition 2.47 bestimmt.

Damit kann nun der Fall, in dem die Automorphismenordnung m keine Primzahlpotenz

ist, genauer behandelt werden. Falls das Minimalpolynom zusätzlich Φ_m ist, dann besitzt der Automorphismus eine Struktur über dem Ganzheitsring des m-ten Kreisteilungskörpers. Dieser Fall kann auf den vorherigen Satz zurückgeführt werden.

Satz 2.59. *Seien $m \in \mathbb{N} \setminus \mathbb{P}(\mathbb{Q})$, $n_{p,i}$ die Ränge der Komponenten einer p-modularen Zerlegung und (n_+, n_-) die Signatur. In einem Geschlecht mit diesen Invarianten gibt es ein ganzzahliges $\mathbb{Z}$-Gitter mit einer Struktur über $\mathbb{Z}[\zeta_m]$ von Rang N, wenn die folgenden Bedingungen erfüllt sind:*

(i) $n_+ \equiv_2 0$ *und* $n_- \equiv_2 0$

(ii) Es gilt $2f^+(p) | n_{p,i}$ *für alle* $p \in \mathbb{P}(\mathbb{Q}) \setminus \{\infty\}$. *Zusätzlich muss für alle* p *mit* $p|m$ *die Kettenbedingung erfüllt sein.*

(iii) Mit $a(p) := N \cdot p^{\nu_p(m)-1}(p\nu_p(m) - \nu_p(m) - 1) + \sum_{i\in\mathbb{Z}} i \cdot \frac{n_{p,i}}{f(p)}$ *gilt die Beziehung:*

$$4 \cdot \sum_{p\in\mathbb{P}(\mathbb{Q})\setminus\{\infty\}} a(p) \equiv_8 n_+ - n_-$$

Beweis. Ein Gitter aus dem Geschlecht mit den gegebenen Bedingungen kann als orthogonale Summe von Gittern in kleineren Geschlechtern mit dem Rang $\varphi(m)$ aufgeteilt werden, die die Bedingungen von Satz 2.57 erfüllen. Damit existiert ein $\mathbb{Z}$-Gitter mit einer Struktur über $\mathbb{Z}[\zeta_m]$. □

Falls die Automorphismenordnung $m = q^t$ eine ungerade Primzahlpotenz ist, dann kann man Gitter mit einer $\mathbb{Z}[\zeta_m]$-Struktur nicht zwangsläufig auf diese Art konstruieren:

Beispiel 2.60. Das gerade, unimodulare und positiv definite Gitter E_8 besitzt eine Struktur über $\mathbb{Z}[\zeta_5]$ von Rang 2. In jeder orthogonalen Summe von zwei Idealgittern aus Satz 2.57 muss aber 5^2 ein Teiler der Determinante sein.

Durch das Bilden von Obergittern kann man auch andere Gitter erhalten. Sie entsprechen bijektiv den total isotropen Untergruppen der Diskriminantengruppe. In dem vorherigen Beispiel zeigt sich, dass das Gitter E_8 ein Obergitter von $A_4 \perp A_4$ ist. In der allgemeinen Situation gibt es zwei Probleme. Zum einen können die Diskriminantengruppen sehr groß werden. Die total isotropen Untergruppen sind dann auch nicht mit Hilfe von Computern zu bestimmen. Zum anderen muss ein Obergitter keinen Automorphismus von diesem Typ besitzen. Deshalb werden nun die beiden interessantesten Spezialfälle betrachtet und es wird versucht allgemeine Aussagen herzuleiten. Der erste Spezialfall sind die positiv definiten, geraden, unimodularen Gitter. Ihr Rang n ist bekanntermaßen durch 8 teilbar (vgl. [Kne02] Satz 26.7).

Proposition 2.61. *Sei $n = 2(q-1)$ für eine Primzahl q mit $q \equiv_4 1$. Dann gibt es im Geschlecht der geraden, unimodularen, positiv definiten Gitter von Rang n mindestens ein Gitter mit einem fixpunktfreien Automorphismus der Ordnung q und mindestens ein Gitter mit einem Automorphismus, der die Ordnung q und Fixpunkte besitzt.*

Beweis. Um ein Gitter mit einem fixpunktfreien Automorphismus der Ordnung q zu konstruieren, wählt man sich zwei beliebige Gitter L_1, L_2 aus dem Geschlecht $\mathrm{Gen}(A_{q-1})$ mit jeweils einem Automorphismus g_1, g_2 der Ordnung q. Das Geschlechtssymbol dieses Geschlechts elementarer Gitter ist nach [CS99] Seite 386 Theorem 13 stets $\mathrm{II}_{q-1}(q^{+1})$. Also ist die Diskriminantengruppe von $L_1 \perp L_2$ ein quadratischer $\mathbb{F}_q$-Vektorraum von der Form $\langle 1, 1\rangle$. Weil $q \equiv_4 1$ ist, muss dieser Raum stets hyperbolisch sein und eine total isotrope, selbst-orthogonale Untergruppe U besitzen. Also besitzt $L_1 \perp L_2$ ein Obergitter M. Es muss konstruktionsbedingt gerade und unimodular sein. Der fixpunktfreie Automorphismus $h := g_1 \perp g_2$ von $L_1 \perp L_2$ kann zu einem Automorphismus des Dualgitters $(L_1 \perp L_2)^{\#}$ fortgesetzt werden. Er operiert damit auf der Diskriminantengruppe und seine Ordnung ist ein Teiler von q. Weil q aber die Ordnung der orthogonale Gruppe des hyperbolischen, zweidimensionalen $\mathbb{F}_q$-Vektorraums nicht teilt (vgl. [Kne02] (13.3) 1)) operiert h trivial auf der Diskriminantengruppe. Damit gilt $h(M) = M$ und $h|_M$ ist ein fixpunktfreier Automorphismus von M.
Seien L_1, L_2 nun Gitter aus dem Geschlecht $\mathrm{Gen}(A_{q-1})$, sodass L_1 einen Automorphismus der Ordnung q und L_2 keinen solchen Automorphismus besitzt. Dann beweist man analog zu obigen Überlegungen, dass es ein Obergitter von $L_1 \perp L_2$ mit einem Automorphismus desselben Typs gibt. □

Bemerkung 2.62. Man kann häufig viele weitere Gitter mit einem Automorphismus der Ordnung q konstruieren, indem L_1 und L_2 die Isometrieklassen des Geschlechts $\mathrm{Gen}(A_{q-1})$ durchlaufen, wobei mindestens ein L_i einen Automorphismus der Ordnung q besitzt. Zum Beispiel besitzt das Geschlecht $\mathrm{II}_{12}(13^{+1})$ insgesamt 6 Isometrieklassen von Gittern, von denen aber nur das Gitter A_{12} einen Automorphismus der Ordnung 13 enthält. Falls L alle Isometrieklassen des Geschlechts durchläuft, dann erhält man durch Bilden von Obergittern von $A_{12} \perp L$ insgesamt 6 gerade, unimodulare Gitter mit dem Rang 24 und einem Automorphismus der Ordnung 13. Dabei ist das Obergitter von $A_{12} \perp A_{12}$ das einzige mit einem fixpunktfreien Automorphismus. Es kann aber grundsätzlich weitere Gitter mit einem Automorphismus des gesuchten Typs geben, die mit dieser Methode nicht konstruiert werden können. In diesem Beispiel wäre dies das Leech-Gitter.

Bemerkung 2.63. Die konstruierten Gitter mit einem fixpunktfreien Automorphismus besitzen die Automorphismen $g_1 \oplus \mathrm{id}$ und $\mathrm{id} \oplus g_2$. Deshalb enthält die Ordnung der Automorphismengruppe den Faktor q^2. Das Leech-Gitter zum Beispiel enthält nur den Faktor 13, aber nicht 13^2.

Proposition 2.64. *Sei $n = 4(q-1)$ für eine ungerade Primzahl q. Dann gibt es im Geschlecht der geraden, unimodularen, positiv definiten Gitter von Rang n mindestens ein Gitter mit einem Automorphismus der Ordnung q.*

Beweis. Analog zum vorherigen Beweis wählt man sich Gitter L_1, L_2, L_3, L_4 aus dem Geschlecht $\mathrm{Gen}(A_{q-1}) \in \mathrm{II}_{q-1}(q^{\epsilon 1})$ mit $\epsilon = (-1)^{\frac{q-1}{2}}$. Jedes L_i besitze einen Automorphismus g_i der Ordnung q. Dann ist die Diskriminantengruppe ein quadratischer, vierdimensionaler $\mathbb{F}_q$-Vektorraum. Weil seine Determinante konstruktionsbedingt ein Quadrat ist,

muss er hyperbolisch sein und deshalb einen zweidimensionalen, total isotropen und selbstdualen Unterraum enthalten. Deshalb gibt es ein gerades, unimodulares Obergitter M. Mit $\{h_1 \oplus h_2 \oplus h_3 \oplus h_4 \mid h_i \in \{\mathrm{id}, g_i\}\}$ gibt es mindestens q^4 verschiedene Automorphismen. Weil q^2 ein exakter Teiler der Ordnung der orthogonalen Gruppe von der Diskriminantengruppe ist (vgl. [Kne02] (13.3) 1)), müssen einige Automorphismen trivial auf der Diskriminantengruppe operieren. Diese Automorphismen lassen sich zu Automorphismen von M mit der Ordnung q fortsetzen. □

An dieser Stelle wird ein weiterer Modularitätsbegriff eingeführt, welcher auf Heinz-Georg Quebbemann zurückgeht. Er sollte nicht mit dem in Definition 1.23 eingeführten Begriff der $\mathfrak{A}$-modularen Gitter und insbesondere der (p)-modularen $\mathbb{Z}$-Gitter verwechselt werden.

Definition 2.65. Ein $\mathbb{Z}$-Gitter (L, b) heißt **p-modular**, wenn ${}^p(L, b)^{\#} = (L, b)$ ist.

Der zweite interessante Spezialfall sind die positiv definiten, p-modularen Gitter mit einem Automorphismus, welche als nächstes untersucht werden.

Proposition 2.66. *Sei $n = 2(q-1)$ für eine ungerade Primzahl q. Des Weiteren sei $p \in \mathbb{P}(\mathbb{Q}) \setminus \{2, q, \infty\}$. Dann gibt es im Geschlecht der geraden, p-modularen, positiv definiten Gitter von Rang n genau dann mindestens ein Gitter mit einem fixpunktfreien Automorphismus der Ordnung q und mindestens ein Gitter mit einem Automorphismus, der die Ordnung q und Fixpunkte besitzt, wenn $\left(\frac{-p}{q}\right) = 1$ ist.*

Beweis. Man wählt sich ein beliebiges Gitter L_1 aus dem Geschlecht des Gitters $A_{q-1} \in \mathrm{II}_{q-1}(q^{\epsilon_{q,1}}1)$ mit $\epsilon_{q,1} = (-1)^{\frac{q-1}{2}}$ und ein beliebiges Gitter L_2 aus dem Geschlecht des skalierten Gitters ${}^pA_{q-1} \in \mathrm{II}_{q-1}(q^{\epsilon_{q,1}}1 p^{\epsilon_{p,1}}1)$ mit $\epsilon_{q,1} = (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{-p}{q}\right)$ und $\epsilon_{p,1} = \left(\frac{q}{p}\right)$, wobei L_1 oder L_2 einen Automorphismus der Ordnung q besitzt. Analog zum Beweis von Proposition 2.61 kann man zeigen, dass jedes Obergitter mit Index q^2 p-modular ist und ebenfalls einen Automorphismus der Ordnung q besitzt. Daher ist die Existenz eines Obergitters äquivalent zu der Existenz eines p-modularen Gitters mit einem Automorphismus. Die Diskriminantengruppe von $L_1 \perp L_2$ ist eine orthogonale Summe eines quadratischen $\mathbb{F}_p$-Vektorraums und eines quadratischen $\mathbb{F}_q$-Vektorraums von der Form $\langle \delta p, \delta \rangle$, wobei $\delta = (-1)^{\frac{q-1}{2}}$ ist. Es gibt genau dann ein Obergitter mit dem Index q^2, wenn $\langle \delta p, \delta \rangle$ isotrop ist. Dies wiederum ist genau dann der Fall, wenn die Determinante $\delta^2 p$ in derselben Quadratklasse wie (-1) liegt. Dies ist äquivalent zu der Bedingung $\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}}$. Dieser Ausdruck kann mit Hilfe des Ergänzungssatzes zum quadratischen Reziprozitätsgesetz zu $\left(\frac{-p}{q}\right) = 1$ vereinfacht werden. □

Proposition 2.67. *Sei $n = 4(q-1)$ für eine ungerade Primzahl q. Dann gibt es im Geschlecht der geraden, p-modularen, positiv definiten Gitter von Rang n mindestens ein Gitter mit einem Automorphismus der Ordnung q.*

Beweis. Man wählt sich $L_1, L_2 \in \mathrm{Gen}(A_{q-1})$ und $L_3, L_4 \in \mathrm{Gen}({}^pA_{q-1})$. Mit dieser Wahl der Gitter verläuft der Beweis analog zum Beweis von Proposition 2.64. □

Bemerkung 2.68. Wenn man in den obigen Beweisen die Gitter A_{q-1} durch ein Gitter, das in Satz 2.57 konstruiert wurde, ersetzt oder Fixgitter aus einem beliebigen Geschlecht wählt, kann man in Einzelfällen auch Gitter mit einem Automorphismus von Primzahlordnung konstruieren, die nicht unimodular oder p-modular sind. Entscheidend ist, dass der entsprechende Teil der Diskriminantengruppe eine total isotrope Untergruppe der passenden Ordnung besitzt und ein Automorphismus mit der passenden Ordnung auf dem Obergitter fortgesetzt werden kann.

Fazit und Ausblick

Im ersten Kapitel konnte gezeigt werden, dass jedes Gitter mit einem Automorphismus der Ordnung m an allen Stellen mit $p \nmid m$ eine besondere p-modulare Zerlegung besitzt, bei der jede Komponente invariant unter dem Automorphismus ist. Für $p = m$ gibt es im Allgemeinen keine solche Zerlegung. Es konnte jedoch gezeigt werden, dass es für jedes solche Gitter eine orthogonale Zerlegung in orthogonal unzerlegbare Teilgitter mit insgesamt zehn möglichen Strukturen gibt. Diese Zerlegung ist zwar nicht eindeutig, aber der angegebene, konstruktive Beweis liefert stets eine Zerlegung in dieselben Isomorphietypen. Für die Fälle $p^2|m$ und $p = 2$ wurde darüber hinaus dargelegt, dass es unendlich viele orthogonal unzerlegbare Gitter mit beliebig großem Rang gibt. Man kann mit Hilfe des angegebenen Verfahrens auch noch viele weitere Familien von orthogonal unzerlegbaren Summanden finden. Daher ist es in diesen Fällen wohl nicht möglich, eine übersichtliche Liste der möglichen Strukturen von orthogonalen Summanden anzugeben. Für den verbleibenden Fall, bei dem m eine quadratfreie natürliche Zahl, aber keine Primzahl ist und $p|m$ gilt, konnte keine Aussage getroffen werden. Einige Beispielrechnungen für den Fall $m = p \cdot q$ für eine Primzahl q legen die folgende Vermutung nahe:

Vermutung. Die Anzahl der möglichen orthogonalen Summanden ist endlich, aber sehr viel größer als im Fall $p = m$.

Falls m eine Primzahl ist, dann setzen sich die zehn bereits erwähnten mögliche Strukturen von orthogonal unzerlegbaren Gittern aus orthogonal unzerlegbaren $\mathbb{Z}_p$- und $\mathbb{Z}_p[\zeta_p]$-Gittern zusammen. Das größte Gitter besitzt eine Pseudobasis mit Rang 4 über dem Gruppenring. Falls m nun zusammengesetzt ist, dann besitzt die Maximalordnung $\bigoplus \mathbb{Z}[\zeta_d]_\pi$ mehr Faktoren. Damit können durch Kombination von orthogonal unzerlegbaren $\mathbb{Z}[\zeta_d]_\pi$-Gittern weit mehr als zehn orthogonal unzerlegbare Gitter gefunden werden, sodass in diesem Fall kein praktikables Ergebnis zu erwarten ist.
In den ersten beiden Abschnitten des zweiten Kapitels wurden die möglichen Invarianten eines Geschlechts berechnet, das einen Automorphismus mit irreduziblem Minimalpolynom besitzt. Dabei wurden im ersten Abschnitt Einschränkungen an den Rang und die Parität der modularen Komponenten bestimmt. Im zweiten Abschnitt wurden die Ränge der modularen Komponenten als gegeben vorausgesetzt. Damit konnten die Vorzeichen und die Oddity bestimmt werden. Es zeigte sich dabei, dass die Invarianten durch die Ränge der modularen

Komponenten und die Existenz von einem Gitter mit einem solchen Automorphismus bereits vollständig festgelegt sind. Anhand von Beispielen wurde im Anschluss gezeigt, wie man in vorgegebenen Geschlechtern bestimmte Zerlegungstypen oder ganze Automorphismenordnungen ausschließen kann. Im letzten Abschnitt wurden dann Gitter mit einem irreduziblen Minimalpolynom mit Hilfe der Idealgitterkonstruktion konstruiert. Falls der Rang des Gitters $\varphi(m)$ ist, konnten notwendige und hinreichende Bedingungen für die Existenz eines Gitters mit einem Automorphismus mit Minimalpolynom Φ_m angegeben werden. Für Gitter mit einem größeren Rang ist das Kriterium dann nicht mehr exakt. Eine Aufgabe für die Zukunft wäre es, sich in Proposition 1.35 von der Bedingung $p|m$ für zusammengesetzte m loszulösen und eine Basis mit ähnlichen Eigenschaften zu finden. Sofern dies gelingt, liegt die folgende Vermutung nahe:

Vermutung. In Satz 2.59 gilt ebenfalls die Umkehrung.

Index

Literaturverzeichnis

[BF02] Eva Bayer-Fluckiger, *Determinants of integral ideal lattices and automorphisms of given characteristic polynomial*, Journal of Algebra **257** (2002), 215 – 221.

[CR62] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and applied mathematics, vol. XI, Interscience Publishers, New York [u.a.], 1962.

[CS99] John Horton Conway and Neil J. A. Sloane, *Sphere packings, lattices and groups*, 3. ed., Grundlehren der mathematischen Wissenschaften, vol. 290, Springer, New York [u.a.], 1999.

[FM69] Albrecht Fröhlich and Allan McEvett, *The representation of groups by automorphisms of forms*, Journal of Algebra **12** (1969), 114 – 133.

[Frö83] Albrecht Fröhlich, *Galois module structure of algebraic integers*, Springer, Berlin, 1983.

[Ger70] Larry J. Gerstein, *Integral decomposition of hermitian forms*, American Journal of Mathematics **92** (1970), 398–418.

[Ger08] ———, *Basic quadratic forms*, Graduate studies in mathematics, vol. 90, American Mathematical Society, 2008.

[Hof12] Björn Hoffmann, *Eine Massformel für hermitesche $\mathbb{Z}G$-Gitter*, Dissertation, TU-Dortmund, 2012.

[HR62] Alex Heller and Irving Reiner, *Representations of cyclic groups in rings of integers, I*, Annals of Mathematics **76** (1962), 73–92.

[HS04] Boris Hemkemeier and Rudolf Scharlau, *Algorithmische Konstruktionen von Gittern*, Dissertation, TU-Dortmund, 2004.

[Jac62] Ronald Jacobowitz, *Hermitian forms over local fields*, American Journal of Mathematics **84** (1962), 441–465.

[Jon63] Alfredo Jones, *Groups with a finite number of indecomposable integral representations*, Michigan Mathematical Journal **10** (1963), 257–261.

[Jür15] Michael Jürgens, *Nicht-Existenz und Konstruktion extremaler Gitter*, Dissertation, TU-Dortmund, 2015.

[Kin03] Oliver D. King, *A mass formula for unimodular lattices with no roots*, Mathematics of Computation **72** (2003), 839–863.

[Kit03] Yoshiyuki Kitaoka, *Arithmetic of quadratic forms*, 1. paperback ed. (with corr.), digital print. ed., Cambridge tracts in mathematics, vol. 106, Cambridge University Press, Cambridge [u.a.], 2003.

[Kne02] Martin Kneser, *Quadratische Formen*, Springer, Berlin [u.a.], 2002.

[Lan86] Serge Lang, *Algebraic number theory*, corr. repr. ed., Graduate texts in mathematics, Springer, New York [u.a.], 1986.

[Neb99] Gabriele Nebe, *Orthogonale Darstellungen endlicher Gruppen und Gruppenringe*, Habilitation, RWTH Aachen, 1999.

[Neb14] ———, *A fourth extremal even unimodular lattice of dimension 48*, Discrete mathematics **331** (2014), 133–136.

[Neu92] Jürgen Neukirch, *Algebraische Zahlentheorie* , Springer-Verlag, Berlin, Heidelberg, 1992.

[O'M63] Onorato T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. 117, Springer, Berlin u.a., 1963.

[QSSS76] Heinz-Georg Quebbemann, Rudolf Scharlau, Winfried Scharlau, and M. Schulte, *Quadratische Formen in additiven Kategorien* .

[Que81] Heinz-Georg Quebbemann, *Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung*, Journal für die reine und angewandte Mathematik **326** (1981), 158 – 170.

[Rei61] Irving Reiner, *The Krull-Schmidt theorem for integral group representations*, Bulletin of the American Mathematical Society **67** (1961), 365–367.

[Rei75] ———, *Maximal orders*, L.M.S. monographs, vol. 5, Academic Press, London u.a., 1975.

[Rei76] ———, *Integral representations of cyclic groups of order p^2*, Proceedings of the American Mathematical Society **58** (1976).

[Sch85] Winfried Scharlau, *Quadratic and hermitian forms*, Grundlehren der mathematischen Wissenschaften, vol. 270, Springer, Berlin u.a., 1985.

[Sch98] Alexander Schiemann, *Classification of hermitian forms with the neighbour method*, Journal of Symbolic Computation **26** (1998), 487â508.

[Ser79] Jean Pierre Serre, *Local fields*, Graduate texts in mathematics, vol. 67, Springer, New York u.a., 1979.

[Shi64] Goro Shimura, *Arithmetic of unitary groups*, Annals of Mathematics (1964).

[Was82] Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate texts in mathematics, vol. 83, Springer, New York u.a., 1982.