Gerade unimodulare Gitter in Dimension 24

von Mykhailo Shatokhin

Inhaltsverzeichnis

Diese Ausarbeitung basiert auf Kapitel 3 von Wolfgang Ebelings Lattices and Codes. Das Ziel ist die Klassifikation von geraden unimodularen Gittern in Dimension 24 und die Beschreibung der Codes, die diesen Gittern entsprechen.

3.1 Theta Funktionen mit harmonischen Koeffizienten

Definition 3.0. *Sei $D \subset \mathbb{C}^n$ eine offene Menge. Eine Funktion $f : D \to \mathbb{C}$ heißt harmonisch genau dann, wenn $f \in C^2(D, \mathbb{C})$ und*

$$\forall \boldsymbol{x} \in D : \Delta f(\boldsymbol{x}) = \textstyle\sum_{k=1}^{n} \frac{\partial^2}{\partial x_k^2} f(\boldsymbol{x}) = 0$$

Satz 3.1. *Ein Polynom $P \in \mathbb{C}[x_1, ..., x_n]$ vom Grad $r > 1$ ist harmomisch genau dann, wenn es eine lineare Kombination von $(\boldsymbol{\xi} \cdot \boldsymbol{x})$ mit $\boldsymbol{\xi}^2 = 0$ ist.*

Beweis. Sei $\mathcal{F}_{m,r}$ die Menge aller homogenen Polynome aus $\mathbb{C}[x_1, ..., x_n]$ vom Grad r. Bezeichnen wir den Multiindex $(i_1, ..., i_n)$ als i und $|i| = \sum_{k=1}^{n} i_k$. Sei außerdem

$$c(i) = \left(\begin{array}{c} |i| \\ i_1 \ldots i_n \end{array} \right) = \tfrac{|i|!}{i_1! \ldots i_n!},$$

dann gilt für beliebiges Polynom $f \in \mathcal{F}_{m,r}$

$$f(\boldsymbol{x}) = \textstyle\sum_{|i|=r} c(i) a(i) \boldsymbol{x}^i.$$

Definieren wir ein Skalarprodukt $[\cdot, \cdot] : \mathcal{F}_{n,r} \times \mathcal{F}_{n,r} \to \mathbb{C}$ so

$$\forall f, g \in \mathcal{F}_{n,r}, f(\boldsymbol{x}) = \textstyle\sum_{|i|=r} c(i) a(i) \boldsymbol{x}^i, g(\boldsymbol{x}) = \sum_{|i|=r} c(i) b(i) \boldsymbol{x}^i : [f, g] := \sum_{|i|=r} c(i) a(i) \overline{b(i)}.$$

$[\cdot, \cdot]$ ist Hermitesch und positiv definit, außerdem bilden die Monomen eine orthogonale Basis von $\mathcal{F}_{n,r}$. Bezeichnen wir $\rho_{\boldsymbol{\xi}}^r := (\boldsymbol{\xi} \cdot \boldsymbol{x})^r$, dann

$$\rho_{\boldsymbol{\xi}}^r = \textstyle\sum_{|i|=r} c(i) \boldsymbol{\xi}^i \boldsymbol{x}^i.$$

Man kann merken, dass (für $f(\boldsymbol{x}) = \sum_{|i|=r} c(i) a(i) \boldsymbol{x}^i$)

$$[f, \rho_{\boldsymbol{\xi}}^r] = \textstyle\sum_{|i|=r} c(i) a(i) \overline{\boldsymbol{\xi}^i} = f(\overline{\boldsymbol{\xi}}).$$

Daraus folgt insbesondere, dass $\mathcal{F}_{n,r} = \left\langle \rho_{\boldsymbol{\xi}}^r \,\middle|\, \boldsymbol{\xi} \in \mathbb{C}^n \right\rangle$.

Betrachten wir die Operation $\Delta : \mathcal{F}_{n,r} \to \mathcal{F}_{n,r-2}$. Sie ist surjektiv und lässt sich als $\omega(\nabla)$ darstellen, wo $\omega \in \mathcal{F}_{n,2}, \omega(\boldsymbol{x}) = \sum_{k=1}^n x_k^2$, und $\nabla = \left(\frac{\partial}{\partial x_1}, ..., \frac{\partial}{\partial x_n}\right)$. Die Menge der harmonischen Polynome ist $Harm_{n,r} = Ker(\Delta)$. Merken wir, dass

$$r![f,g] = r! \sum_{|i|=r} c(i)a(i)\overline{b(i)} = \sum_{|i|=r} c(i)^2 a(i)\nabla^i \overline{b(i)}\boldsymbol{x}^i = f(\nabla)\overline{g(\boldsymbol{x})},$$

weil für Multiindexe i, j gilt $\nabla^i \boldsymbol{x}^j = \frac{|i|!}{c(i)}\mathbf{1}_{i=j}$. Daraus folgt, dass

$$\mathcal{F}_{n,r} = Harm_{n,r} \perp \omega\mathcal{F}_{n,r-2} = Ker(\Delta) \perp \omega Bild(\Delta).$$

Um das zu beweisen, betrachten wir $\omega g \in \omega\mathcal{F}_{n,r-2}$ und $f \in Harm_{n,r}$, dann

$$r![wg, f] = (\omega g)(\nabla)\overline{f} = (g\omega)(\nabla)\overline{f} = g(\nabla)\omega(\nabla)\overline{f} = g(\nabla)\big(\Delta\overline{f}\big) = 0.$$

Sei $R = \left\langle \rho_{\boldsymbol{\xi}}^r \,\middle|\, \boldsymbol{\xi} \in \mathbb{C}^n, \boldsymbol{\xi}^2 = 0 \right\rangle$ und $g \in Harm_{n,r} \cap R^\perp$, dann

$$\forall \boldsymbol{\xi} \in \mathbb{C}^n : g(\overline{\boldsymbol{\xi}}) = [g, \rho_{\boldsymbol{\xi}}^r] = 0 \implies \omega | g,$$

also existiert $h \in \mathcal{F}_{n,r-2}$ mit $g = \omega h$, aber

$$r![g,g] = r![\omega h, g] = h(\nabla)(\Delta g) = 0 \implies g = 0,$$

folglich $Harm_{n,r} = R$. □

Lemma 3.1. *Man hat folgende Fourier-Transformationen*

$f(\boldsymbol{x}) = \exp\big(\pi i\big(\frac{-1}{\tau}\big)\boldsymbol{x}^2\big)$,	$\widehat{f}(\boldsymbol{y}) = \big(\sqrt{\frac{\tau}{i}}\big)^n \exp(\pi i\tau\boldsymbol{y}^2)$,	$\tau \in \mathbb{H}, -\frac{\pi}{4} < \arg\sqrt{\frac{\tau}{i}} < \frac{\pi}{4}$
$f(\boldsymbol{x}) = \exp\big(\pi i\big(\frac{-1}{\tau}\big)(\boldsymbol{x}+\boldsymbol{z})^2\big)$,	$\widehat{f}(\boldsymbol{y}) = \big(\sqrt{\frac{\tau}{i}}\big)^n \exp(\pi i\tau\boldsymbol{y}^2)\exp(2\pi i\boldsymbol{z}\cdot\boldsymbol{y})$,	$\tau \in \mathbb{H}, \boldsymbol{z} \in \mathbb{R}^n$
$f(\boldsymbol{x}) = P(\boldsymbol{x})e^{-\pi\boldsymbol{x}^2}$,	$\widehat{f}(\boldsymbol{y}) = P\left(\frac{-1}{2\pi i}\frac{\partial}{\partial x_1}, ..., \frac{-1}{2\pi i}\frac{\partial}{\partial x_1}\right)e^{-\pi\boldsymbol{y}^2}$,	$P \in \mathbb{C}[x_1, ..., x_n]$
$f(\boldsymbol{x}) = (\boldsymbol{\xi}\cdot\boldsymbol{x})^r e^{-\pi\boldsymbol{x}^2}$,	$\widehat{f}(\boldsymbol{y}) = \big(\frac{\boldsymbol{\xi}\cdot\boldsymbol{y}}{i}\big)^r e^{-\pi\boldsymbol{y}^2}$,	$\boldsymbol{\xi} \in \mathbb{C}^n, (\boldsymbol{\xi}^2 = 0) \vee (r = 1)$
$f(\boldsymbol{x}) = (\boldsymbol{\xi}\cdot(\boldsymbol{x}+\boldsymbol{z}))^r e^{\pi i\left(\frac{-1}{\tau}\right)(\boldsymbol{x}+\boldsymbol{z})^2}$,	$\widehat{f}(\boldsymbol{y}) = \big(\sqrt{\frac{\tau}{i}}\big)^{n+2r}\big(\frac{\boldsymbol{\xi}\cdot\boldsymbol{y}}{i}\big)^r e^{2\pi i\boldsymbol{z}\cdot\boldsymbol{y}}e^{\pi i\tau\boldsymbol{y}^2}$	

Beweis. Hier wird Lemma 2.1 benutzt

$$\int_{\mathbb{R}^n} e^{-\pi\boldsymbol{x}^2}e^{-2\pi i\boldsymbol{x}\cdot\boldsymbol{y}}\,d\boldsymbol{x} = e^{-\pi\boldsymbol{y}^2}.$$

Alle Gleichungen folgen daraus mithilfe der Eigenschaften der Fourier-Transformation. □

Definition 3.1. *Sei $\boldsymbol{z} \in \mathbb{R}^n$ und $P \in \mathbb{C}[x_1, ..., x_n]$ harmonisch vom Grad r, dann setze*

$$\vartheta_{\boldsymbol{z}+\Gamma,P}(\tau) = \sum_{\boldsymbol{x}\in\boldsymbol{z}+\Gamma} P(\boldsymbol{x})e^{\pi i\tau\boldsymbol{x}^2}.$$

Behauptung 3.1. *Es gilt*

$$\vartheta_{\boldsymbol{z}+\Gamma,P}\big(-\tfrac{1}{\tau}\big) = \big(\sqrt{\tfrac{\tau}{i}}\big)^{n+2r} i^{-r}\frac{1}{covol(\Gamma)}\sum_{y\in\Gamma^\#} P(\boldsymbol{y})e^{2\pi i\boldsymbol{y}\cdot\boldsymbol{z}}e^{\pi i\tau\boldsymbol{y}^2}.$$

Beweis. Das folgt aus Poissonscher Summenformel (Satz 2.3) und oberen Formeln für Fourier Transformationen. □

Es wird weiter angenommen, dass Γ ein ganzes gerades Gitter ist, n ist gerade, P ist harmonisch vom Grad r, $k = \frac{n}{2} + r$.

Merken wir, dass $\Gamma \subset \Gamma^{\#}$, und für solche $\boldsymbol{y}_1, \boldsymbol{y}_2 \in \Gamma^{\#}$, dass $\boldsymbol{y}_1 \equiv \boldsymbol{y}_2 \,(mod\,\Gamma)$, gilt

$$\forall \boldsymbol{x} \in \Gamma : \boldsymbol{y}_1 \cdot \boldsymbol{x} \equiv \boldsymbol{y}_2 \cdot \boldsymbol{x} \,(mod\,\mathbb{Z}), \quad \boldsymbol{y}_1^2 \equiv \boldsymbol{y}_2^2 \,(mod\,2\mathbb{Z}).$$

Für $\boldsymbol{z} \in \Gamma^{\#}$ folgt daraus

$$\begin{aligned} &\vartheta_{\boldsymbol{z}+\Gamma,P}(\tau+1) = e^{\pi i \boldsymbol{z}^2} \vartheta_{\boldsymbol{z}+\Gamma,P}(\tau), \\ &\vartheta_{\boldsymbol{z}+\Gamma,P}\left(-\tfrac{1}{\tau}\right) = \tfrac{1}{covol(\Gamma)} \left(\tfrac{\tau}{i}\right)^k i^{-r} \textstyle\sum_{\sigma \in \Gamma^{\#}/\Gamma} e^{2\pi i \sigma \boldsymbol{z}} \vartheta_{\sigma+\Gamma,P}(\tau). \end{aligned}$$

Die Gruppe $SL_2(\mathbb{Z})$ operiert auf Funktionen $f : \mathbb{H} \to \mathbb{C}$ durch

$$f(\tau) \overset{A}{\mapsto} (f|_k A)(\tau) = f(A\tau)(c\tau+d)^{-k}.$$

Behauptung 3.2. *Die Menge aller Funktionen* $\left\{\vartheta_{\boldsymbol{z}+\Gamma,P} \,\middle|\, \boldsymbol{z} \in \Gamma^{\#}\right\}$, *ist invariant unter* $SL_2(\mathbb{Z})$. *Genauer, für* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *gilt*

$$\begin{aligned} &\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A = \tfrac{1}{covol(\Gamma) c^{n/2} i^{k+r}} \sum_{\sigma \in \Gamma^{\#}/\Gamma} \left(e^{-\pi i b(d\sigma^2 + 2\sigma \boldsymbol{z})} \sum_{\substack{\lambda \in \Gamma^{\#}/c\Gamma, \\ \lambda \equiv \boldsymbol{z} + d\sigma (mod\,\Gamma)}} e^{\pi i \frac{a}{c}\lambda^2} \right) \vartheta_{\sigma+\Gamma,P}, \quad c \neq 0, \\ &\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A = \tfrac{1}{d^{n/2}} e^{\pi i ab \boldsymbol{z}^2} \vartheta_{a\boldsymbol{z}+\Gamma,P}, \qquad c = 0. \end{aligned}$$

Beweis. Für $c = 0$ gilt $a^2 = 1$, deswegen $a\Gamma = \Gamma$ und

$$\begin{aligned} (\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A)(\tau) &= d^{-k} \vartheta_{\boldsymbol{z}+\Gamma,P}(a^2\tau + ab) = d^{-k} \textstyle\sum_{\boldsymbol{x} \in \boldsymbol{z}+\Gamma} P(\boldsymbol{x}) e^{\pi i (a^2\tau+ab)\boldsymbol{x}^2} \\ &= e^{\pi i ab \boldsymbol{z}^2} d^{-k} a^{-r} \textstyle\sum_{\boldsymbol{x} \in a\boldsymbol{z}+\Gamma} P(\boldsymbol{x}) e^{\pi i \tau \boldsymbol{x}^2} = d^{-n/2} e^{\pi i ab \boldsymbol{z}^2} \vartheta_{a\boldsymbol{z}+\Gamma,P}(\tau) \end{aligned}$$

Merken wir, dass

$$\vartheta_{\boldsymbol{z}+\Gamma,P} = \sum_{\lambda \in \Gamma^{\#}/c\Gamma,\, \lambda \equiv \boldsymbol{z}\,(mod\,\Gamma)} \vartheta_{\lambda+c\Gamma,P}$$

Es gilt

$$\boldsymbol{y}_1, \boldsymbol{y}_2 \in \Gamma^{\#}, \boldsymbol{y}_1 \equiv \boldsymbol{y}_2 \,(mod\,c\Gamma) \implies \boldsymbol{y}_1^2 = \boldsymbol{y}_2^2 \,(mod\,2c\mathbb{Z}),$$

deswegen

$$\begin{aligned} \vartheta_{\lambda+c\Gamma,P}\left(\tfrac{a\tau+b}{c\tau+d}\right) &= \vartheta_{\lambda+c\Gamma,P}\left(\tfrac{a}{c} - \tfrac{1}{c(c\tau+d)}\right) = e^{\pi i \frac{a}{c}\lambda^2} \vartheta_{\lambda+c\Gamma,P}\left(\tfrac{-1}{c(c\tau+d)}\right) \\ &= \tfrac{c^k}{covol(c\Gamma) i^{k+r}} (c\tau+d)^k \sum_{\sigma \in (c\Gamma)^{\#}/c\Gamma} e^{\pi i \left(\frac{a}{c}\lambda^2 + 2\sigma\lambda\right)} \vartheta_{\sigma+c\Gamma,P}(c^2\tau + cd) \\ &= \tfrac{c^k}{covol(c\Gamma) i^{k+r}} (c\tau+d)^k \sum_{\sigma \in (c\Gamma)^{\#}/c\Gamma} e^{\pi i \left(\frac{a}{c}\lambda^2 + 2\sigma\lambda + cd\sigma^2\right)} \vartheta_{\sigma+c\Gamma,P}(c^2\tau) \end{aligned}$$

Weil $(c\Gamma)^{\#} = \frac{1}{c}\Gamma^{\#}$ und $covol(c\Gamma) = c^n covol(\Gamma)$, gilt

$$\begin{aligned}(\vartheta_{\lambda+c\Gamma.P}|_k A)(\tau) &= \frac{c^r}{covol(\Gamma)c^{n/2}i^{k+r}} \sum_{\sigma\in\Gamma^{\#}/c^2\Gamma} e^{\pi i\left(\frac{a}{c}\lambda^2+2\sigma\frac{\lambda}{c}+\frac{d}{c}\sigma^2\right)}\vartheta_{\frac{\sigma}{c}+c\Gamma,P}(c^2\tau)\\ &= \frac{1}{covol(\Gamma)c^{n/2}i^{k+r}} \sum_{\sigma\in\Gamma^{\#}/c^2\Gamma} e^{\pi i\left(\frac{a}{c}\lambda^2+2\sigma\frac{\lambda}{c}+\frac{d}{c}\sigma^2\right)}\vartheta_{\sigma+c^2\Gamma,P}(\tau)\end{aligned}$$

Sei $G(\sigma)$ der Koeffizient bei $\vartheta_{\sigma+c^2\Gamma,P}(\tau)$ in Darstellung von $\vartheta_{\rho+\Gamma,P}|_k A$, dann

$$G(\sigma) = \frac{1}{covol(\Gamma)c^{n/2}i^{k+r}} \sum_{\lambda\in\Gamma^{\#}/c\Gamma,\lambda\equiv\boldsymbol{z}\,(mod\,\Gamma)} e^{\pi i\left(\frac{a}{c}+\frac{2\lambda\sigma}{c}+\frac{d}{c}\sigma^2\right)}$$

Merken wir, dass

$$\frac{a}{c}+\frac{2\lambda\sigma}{c}+\frac{d}{c}\sigma^2 = \frac{a}{c}(\lambda+d\sigma)^2 - 2b\lambda\sigma + db\sigma^2$$

deswegen

$$\begin{aligned}G(\sigma) &= \frac{1}{covol(\Gamma)c^{n/2}i^{k+r}} e^{-\pi ib(d\sigma^2+2\sigma\boldsymbol{z})} \sum_{\lambda\in\Gamma^{\#}/c\Gamma,\lambda\equiv\boldsymbol{z}\,(mod\,\Gamma)} e^{\pi i\frac{a}{c}(\lambda+d\sigma)^2}\\ &= \frac{1}{covol(\Gamma)c^{n/2}i^{k+r}} e^{-\pi ib(d\sigma^2+2\sigma\boldsymbol{z})} \sum_{\lambda\in\Gamma^{\#}/c\Gamma,\lambda\equiv\boldsymbol{z}+d\sigma\,(mod\,\Gamma)} e^{\pi i\frac{a}{c}\lambda^2}\end{aligned}$$

insbesondere ist $G(\sigma)$ nur von Restklasse $[\sigma]\in\Gamma^{\#}/\Gamma$ abhängig, folglich

$$(\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A)(\tau) = \sum_{\sigma\in\Gamma^{\#}/c^2\Gamma} G(\sigma)\vartheta_{\sigma+c^2\Gamma,P}(\tau) = \sum_{\sigma\in\Gamma^{\#}/\Gamma} G(\sigma)\vartheta_{\sigma+\Gamma,P}(\tau)$$

□

Betrachten wir die Summe

$$S = \sum_{\lambda\in\Gamma^{\#}/c\Gamma,\lambda\equiv\boldsymbol{z}+d\sigma\,(mod\,\Gamma)} e^{\pi i\frac{a}{c}\lambda^2}$$

Wenn man λ durch $\lambda + c\mu, \mu\in\Gamma^{\#}, c\mu\in\Gamma$ ersetzt, soll S unverändert bleiben, also

$$\begin{aligned}S &= \sum_{\lambda\in\Gamma^{\#}/c\Gamma,\lambda\equiv\boldsymbol{z}+d\sigma\,(mod\,\Gamma)} e^{\pi i\frac{a}{c}(\lambda+c\mu)^2}\\ &= e^{\pi iac\mu^2}\sum_{\lambda\in\Gamma^{\#}/c\Gamma,\lambda\equiv\boldsymbol{z}+d\sigma\,(mod\,\Gamma)} e^{\pi i\left(\frac{a}{c}\lambda^2+2a\lambda\mu\right)}\\ &= e^{\pi i\left(ac\mu^2+2a(\boldsymbol{z}+d\sigma)\mu\right)}S\end{aligned}$$

deswegen kann S nur dann ungleich 0 sein, wenn für alle $\mu\in\Gamma^{\#}, c\mu\in\Gamma$ gilt $e^{\pi i\left(ac\mu^2+2a(\boldsymbol{z}+d\sigma)\mu\right)} = 1$.

Definition 3.2. *Die natürliche Zahl* $N = \min\left\{x\in\mathbb{N}\,\middle|\,\forall\mu\in\Gamma^{\#} : x\mu^2\in 2\mathbb{Z}\right\}$ *heißt das Level von* Γ.

Lemma 3.2. $N\Gamma^{\#}\subset\Gamma$

Beweis. Die Basiswechselmatrix von Γ nach $N\Gamma^{\#}$ ist $N\mathcal{G}(\Gamma^{\#})$, wo $\mathcal{G}(\Gamma^{\#})$ die Grammatrix der Basis von $\Gamma^{\#}$ ist. Berechnen wir

$$(N\mathcal{G}(\Gamma^{\#}))_{ij} = N(e_i^{\#}\cdot e_j^{\#}) = \frac{1}{2}N\Big((e_i^{\#}+e_j^{\#})^2 - (e_i^{\#})^2 - (e_j^{\#})^2\Big)\in\mathbb{Z},$$

weil N das Level von Γ ist. Daraus folgt die Behauptung. □

Bemerkung 3.1. *Sei $D = (-1)^{n/2} disc(\Gamma)$ und N das Level von Γ, dann $D\mathcal{G}(\Gamma)^{-1}$ und $N\mathcal{G}(\Gamma)^{-1} = N\mathcal{G}(\Gamma^{\#})$ sind ganzzahlige Matrizen mit geraden Zahlen auf der Diagonale. Außerdem $N|D$ und $D|N^n$.*

Beweis. Merken wir, dass $A = \left\{x \in \mathbb{Z} \,\middle|\, \forall \mu \in \Gamma^{\#} : x\mu^2 \in 2\mathbb{Z}\right\} = N\mathbb{Z}$, ansonsten existiert $a \in A \backslash N\mathbb{Z}$ und $N > ggt(a, N) \in A$. Außerdem $D \in A$, weil $D(e_i^{\#})^2 \in 2\mathbb{Z}$ für alle $e_i^{\#}$, deswegen $N|D$. Außerdem $det(N\mathcal{G}(\Gamma)^{-1}) = N^n disc(\Gamma)^{-1} \in \mathbb{Z}$, deswegen $D|N^n$ □

Gelte $N|c$, dann kann S nur dann ungleich 0 sein, wenn $\forall \mu \in \Gamma^{\#} : a(\boldsymbol{z} + d\sigma)\mu \in \mathbb{Z}$, also

$$a(\boldsymbol{z} + d\sigma) \in \Gamma^{\#\#} = \Gamma.$$

Es ist schon bekannt, dass $bc\sigma \in \Gamma$, deswegen soll $a\boldsymbol{z} + \sigma \in \Gamma$ gelten.

Korollar 3.1. *Sei Γ ein gerades ganzes Gitter vom Level N, $\boldsymbol{z} \in \Gamma^{\#}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ und $N|c$, dann*

$$\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A = \varepsilon(A) e^{\pi i ab \boldsymbol{z}^2} \vartheta_{a\boldsymbol{z}+\Gamma,P},$$
$$\varepsilon(A) = \begin{cases} \frac{1}{covol(\Gamma)(ic)^{n/2}} \sum\limits_{\lambda \in \Gamma/c\Gamma} e^{\pi i \frac{a}{c} \lambda^2}, & c \neq 0, \\ d^{-n/2}, & c = 0. \end{cases}$$

Beweis. Aus Behauptung 3.2 sind allgemeine Formeln schon bekannt, und für $c = 0$ ist sie unverändert. Für $c \neq 0$ gilt

$$\vartheta_{a\boldsymbol{z}+\Gamma,P} = (-1)^r \vartheta_{-a\boldsymbol{z}+\Gamma,P} \implies \frac{1}{covol(\Gamma)c^{n/2}i^{k+r}} \vartheta_{\sigma+\Gamma,P} = \frac{1}{covol(\Gamma)c^{n/2}i^{k+r}} \vartheta_{-a\boldsymbol{z}+\Gamma,P} = \frac{1}{covol(\Gamma)c^{n/2}i^{n/2}} \vartheta_{a\boldsymbol{z}+\Gamma,P}.$$

Außerdem merken wir, dass $\boldsymbol{z} + d\sigma \equiv_\Gamma \boldsymbol{z} - ad\boldsymbol{z} \equiv_\Gamma \boldsymbol{z} - (1 - bc)\boldsymbol{z} \equiv_\Gamma 0$, deswegen

$$\sum_{\sigma \in \Gamma^{\#}/\Gamma} \left(e^{-\pi i b \left(d\sigma^2 + \sigma \boldsymbol{z}\right)} \sum_{\substack{\lambda \in \Gamma^{\#}/c\Gamma, \\ \lambda \equiv \boldsymbol{z}+d\sigma (mod\, \Gamma)}} e^{\pi i \frac{a}{c} \lambda^2} \right) = \sum_{\substack{\sigma \in \Gamma^{\#}/\Gamma, \\ \sigma \equiv -a\boldsymbol{z} (mod\, \Gamma)}} \left(e^{-\pi i b \left(d\sigma^2 + \sigma \boldsymbol{z}\right)} \sum_{\lambda \in \Gamma/c\Gamma} e^{\pi i \frac{a}{c} \lambda^2} \right)$$
$$= e^{-\pi i b (da^2 \boldsymbol{z}^2 - a\boldsymbol{z}^2)} \sum_{\lambda \in \Gamma/c\Gamma} e^{\pi i \frac{a}{c} \lambda^2} = e^{\pi i ab \boldsymbol{z}^2 (1-bc)} \sum_{\lambda \in \Gamma/c\Gamma} e^{\pi i \frac{a}{c} \lambda^2} = e^{\pi i ab \boldsymbol{z}^2} \sum_{\lambda \in \Gamma/c\Gamma} e^{\pi i \frac{a}{c} \lambda^2}$$

□

Definieren wir die folgende Untergruppen von $SL_2(\mathbb{Z})$, wobei immer $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ sei

$$\begin{aligned} \Gamma_0 &= \{A \in SL_2(\mathbb{Z}) \,|\, N|c\}, \\ \Gamma_1 &= \{A \in SL_2(\mathbb{Z}) \,|\, a \equiv d \equiv 1 \,(mod\, N), N|c\}, \\ \Gamma\ &= \{A \in SL_2(\mathbb{Z}) \,|\, a \equiv d \equiv 1 \,(mod\, N), N|c, N|b\} \trianglelefteq SL_2(\mathbb{Z}), \end{aligned}$$

Die letzte Folgerung impliziert, dass $\varepsilon : \Gamma_0(N) \to \mathbb{C}^*$ ein Gruppenhomomorphismus ist (ein Charakter von $\Gamma_0(N)$).

Korollar 3.2. *Sei $A \in \Gamma_0(N)$ mit $dc \neq 0$, dann*

$$\varepsilon(A) = d^{-n/2} \sum\nolimits_{\lambda \in \Gamma/d\Gamma} e^{\pi i \frac{b}{d} \lambda^2}.$$

Beweis. Sei $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $B = AC^{-1} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$, dann $\vartheta_{\Gamma,P}|_k A = (\vartheta_{\Gamma,P}|_k B)|_k C$, und aus Behauptung 3.2 folgt

$$\begin{aligned}\vartheta_{\Gamma,P}|_k A &= \frac{1}{covol(\Gamma)d^{n/2}i^{k+r}} \sum_{\sigma\in\Gamma^\#/\Gamma} \left(e^{\pi i a(-c\sigma^2+2\sigma\boldsymbol{z})} \sum_{\substack{\lambda\in\Gamma^\#/d\Gamma,\\ \lambda\equiv\boldsymbol{z}-c\sigma (mod\,\Gamma)}} e^{\pi i\frac{b}{d}\lambda^2} \right) \left(\frac{(-1)^{n/2}}{covol(\Gamma)i^{k+r}} \sum_{\sigma_1\in\Gamma^\#/\Gamma} e^{-2\pi i\sigma\sigma_1}\vartheta_{\sigma_1+\Gamma,P} \right) \\ &= \frac{(-1)^{n/2}}{covol(\Gamma)^2 d^{n/2}(-1)^{k+r}} \left(\sum_{\substack{\lambda\in\Gamma^\#/d\Gamma,\\ \lambda\equiv\boldsymbol{z} (mod\,\Gamma)}} e^{\pi i\frac{b}{d}\lambda^2} \right) \sum_{\sigma,\sigma_1\in\Gamma^\#/\Gamma} e^{2\pi i\sigma(a\boldsymbol{z}-\sigma_1)}\vartheta_{\sigma_1+\Gamma,P}.\end{aligned}$$

Merken wir, dass

$$\forall\mu\in\Gamma^\# : \sum_{\sigma\in\Gamma^\#/\Gamma} e^{2\pi i\sigma(a\boldsymbol{z}-\sigma_1)} = \sum_{\sigma\in\Gamma^\#/\Gamma} e^{2\pi i(\sigma+\mu)(a\boldsymbol{z}-\sigma_1)} = e^{2\pi i\mu(a\boldsymbol{z}-\sigma_1)} \sum_{\sigma\in\Gamma^\#/\Gamma} e^{2\pi i\sigma(a\boldsymbol{z}-\sigma_1)},$$

folglich $a\boldsymbol{z} - \sigma_1 \in \Gamma$ (ansonsten ist die Summe gleich 0), d.h. $\sigma_1 \equiv a\boldsymbol{z}\,(mod\,\Gamma)$. Außerdem

$$\begin{aligned}\sum_{\substack{\lambda\in\Gamma^\#/d\Gamma,\\ \lambda\equiv\boldsymbol{z} (mod\,\Gamma)}} e^{\pi i\frac{b}{d}\lambda^2} &= \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}(\lambda+\boldsymbol{z})^2} = \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}(\lambda+(ad-bc)\boldsymbol{z})^2} = \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\left(\lambda^2+2ad\lambda\boldsymbol{z}+a^2d^2\boldsymbol{z}^2\right)} \\ &= e^{\pi i a^2 bd\boldsymbol{z}} \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2} = e^{\pi i ab(1-bc)\boldsymbol{z}} \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2} = e^{\pi i ab\boldsymbol{z}} \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2}.\end{aligned}$$

Also

$$\begin{aligned}\vartheta_{\Gamma,P}|_k A &= \frac{1}{covol(\Gamma)^2 d^{n/2}} e^{\pi i ab\boldsymbol{z}} \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2} \sum_{\sigma\in\Gamma^\#/\Gamma} \vartheta_{a\boldsymbol{z}+\Gamma,P} \\ &= \frac{|\Gamma^\#/\Gamma|}{covol(\Gamma)^2 d^{n/2}} e^{\pi i ab\boldsymbol{z}} \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2}\vartheta_{a\boldsymbol{z}+\Gamma,P} = \frac{1}{d^{n/2}} e^{\pi i ab\boldsymbol{z}} \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2}\vartheta_{a\boldsymbol{z}+\Gamma,P}.\end{aligned}$$

□

Lemma 3.3. *Sei* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ *und* $l \in \mathbb{Z}$, *dann*

$$\varepsilon\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon\begin{pmatrix} a & b+la \\ c & d+lc \end{pmatrix}.$$

Beweis. Folgt aus dem vorigen Korollar. □

Sei $G(b,d) = \sum_{\lambda\in\Gamma/d\Gamma} e^{\pi i\frac{b}{d}\lambda^2}$.

Lemma 3.4. *Sei* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ *und* $bc \neq 0$, *dann* $G(b,d) \in \mathbb{Q}$ *und* $G(b,d) = G(1,d)$.

Beweis. Γ ist gerade, deswegen $\left(e^{\pi i\frac{b}{d}\lambda^2}\right)^d = 1$ und $G(b,d) \in \mathbb{Q}(\xi_d)$. Außerdem folgt aus vorigen zwei Aussagen

$$\forall l\in\mathbb{Z} : G(b,d) = d^{n/2}\varepsilon(A) = d^{n/2}(d+lc)^{-n/2} \textstyle\sum_{\lambda\in\Gamma/(d+lc)\Gamma} e^{\pi i\frac{b+la}{d+lc}\lambda^2} \in \mathbb{Q}(\xi_{d+lc}).$$

Weil $ggt(d,c)=1$, existiert so ein $l_0 \in \mathbb{Z}$, dass $ggt(d, d+l_0 c)=1$. Dann

$$G(b,d) \in \mathbb{Q}(\xi_d) \cap \mathbb{Q}(\xi_{d+l_0c}) = \mathbb{Q}.$$

$G(b,d)$ ist unter beliebigem Automorphismus von $\mathbb{Q}(\xi_d)$ invariant ($G(b,d) \in \mathbb{Q}$), folglich $G(b,d) = G(1,d)$. □

Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = A \in \Gamma_0(N)$. Weil $\varepsilon(A) = d^{-n/2}G(b,d) = d^{-n/2}G(1,d) = \varepsilon(d)$, gilt

$$\forall B \in \Gamma_0(N), B_{22} = d : \varepsilon(B) = \varepsilon(A).$$

Insbesondere kann man B mit $B_{21} = N$ wählen, woraus lässt sich sehen, dass $\varepsilon(d+N) = \varepsilon(d)$, deswegen hängt $\varepsilon(A)$ nur von der Restklasse $[d] \in \mathbb{Z}/N\mathbb{Z}$. Aus Korollar 3.2 kann man berechnen, dass $\varepsilon(A) = 1$ für $A \in \Gamma_1(N)$, deswegen gilt im Fall $N = 1$

$$\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A = \vartheta_{\boldsymbol{z}+\Gamma,P}.$$

Im allgemeinen Fall hat man den folgenden Satz.

Satz 3.2. *Es gilt*

$$\begin{aligned} &\vartheta_{\boldsymbol{z}+\Gamma,P}|_k A = \vartheta_{\boldsymbol{z}+\Gamma,P}, && A \in \Gamma(N), \\ &\vartheta_{\Gamma,P}|_k A = \left(\frac{(-1)^{n/2}disc(\Gamma)}{d}\right)\vartheta_{\Gamma,P} = \left(\frac{D}{d}\right)\vartheta_{\Gamma,P}, && A \in \Gamma_0(N), \end{aligned}$$

wobei $\left(\frac{a}{b}\right)$ *das Legendre-Symbol ist.*

3.2 Wurzelgitter von geraden unimodularen Gittern

Sei $\Gamma \in \mathbb{R}^n$ gerade und unimodular, dann ist das Level $N = 1$.

Korollar 3.3. *Sei P harmonisch in n Variablen und $Grad(P) = r$, dann $\vartheta_{\Gamma,P}$ ist eine Modulform vom Gewicht $\frac{n}{2} + r$ und Spitzenform falls $r > 0$.*

Beweis. Erste Behauptung folgt aus dem vorigen Satz. Merken wir dazu, dass für $q = e^{2\pi i\tau}$ gilt

$$\begin{aligned} &\vartheta_{\Gamma,P}(\tau) = \textstyle\sum_{s=0}^{\infty} c_s q^s, \\ &c_s = \textstyle\sum_{x\in\Gamma, x^2=2s} P(x), \end{aligned}$$

deswegen $c_0 = P(0) = 0$, wenn $r > 0$.

Sei $\Gamma_2 = \{x \in \Gamma \,|\, x^2 = 2\}$ und $f(x) = (x \cdot y)^2 - \frac{x^2y^2}{n}$. Es wurde schon gezeigt, dass f harmonisch ist, deswegen ist $\vartheta_{\Gamma,f}$ eine Spitzenform vom Gewicht $\frac{n}{2} + 2$. Für $n = 8, 16, 24$ ist das Gewicht entsprechend $6, 10, 14$, woraus folgt, dass $\vartheta_{\Gamma,f} = 0$.

Behauptung 3.3. *Sei $\Gamma \in \mathbb{R}^n$ ein gerades unimodulares Gitter und $n \in \{8, 16, 24\}$. Für $y \in \mathbb{R}^n$ gilt*

$$\textstyle\sum_{x\in\Gamma, x^2=2r}(x\cdot y)^2 - \left(\sum_{x\in\Gamma,x^2=2r} x^2\right)\frac{y^2}{n} = 0,$$

insbesondere gilt für $r = 1$

$$\textstyle\sum_{x\in\Gamma_2}(x\cdot y)^2 = \frac{2|\Gamma_2|y^2}{n}$$

Korollar 3.4. *Entweder* $\Gamma_2 = \emptyset$ *oder* $\langle \Gamma_2 \rangle_{\mathbb{R}} = \mathbb{R}^n$.

Beweis. Falls $\langle \Gamma_2 \rangle_{\mathbb{R}} \neq \mathbb{R}^n$, existiert y, das zu allen Wurzeln orthogonal ist, woraus folgt, dass $|\Gamma_2| = 0$. □

Korollar 3.5. *Alle irreduziblen Komponenten von* $\langle \Gamma \rangle_2$ *haben dieselbe Coxeter-Zahl.*

Beweis. Wählen wir y in irreduzibler Komponente und nutzen die vorige Behauptung erst für das ganze Gitter, und dann für die Komponente. □

Betrachten wir die geraden unimodularen Gittern für $n = 8, 16, 24$. Für $n = 8$ gilt $\langle \Gamma_2 \rangle_{\mathbb{Z}} = E_8$. Für $n = 16$ ist ϑ_Γ eine modulare Forme mit Gewicht 8, deswegen $\vartheta_\Gamma = E_4^2$, $|\Gamma_2| = 480$ und $h = 30$. Dann ist entweder $\langle \Gamma_2 \rangle_{\mathbb{Z}} = E_8 + E_8$ oder $\langle \Gamma_2 \rangle_{\mathbb{Z}} = D_{16}$. Für $n = 24$ hat man folgendes

Behauptung 3.4. *Sei* $\Gamma \subset \mathbb{R}^{24}$ *gerade und unimodular, dann*

$$\begin{aligned} &\langle \Gamma_2 \rangle_{\mathbb{Z}} \in \{\emptyset\} \cup \{\alpha A_\beta \,|\, \alpha\beta = 24\} \cup \{\alpha D_\beta \,|\, \alpha\beta = 24\} \cup \{\alpha E_\beta \,|\, \alpha\beta = 24\} \\ &\cup \{4A_5 + D_4,\, 2A_7 + 2D_5,\, 2A_9 + D_6,\, A_{15} + D_9,\, E_8 + D_{16},\, 2E_7 + D_{10},\, E_7 + A_{17},\, E_6 + D_7 + A_{11}\} \end{aligned}$$

Beweis. Betrachten wir die folgende Tabelle

Γ	$\lvert\Gamma_2\rvert$	h	$det(\Gamma)$	$\Gamma^\#/\Gamma$	$dim(\Gamma)$
A_n	$n(n+1)$	$n+1$	$n+1$	$\mathbb{Z}/(n+1)\mathbb{Z}$	$n \geq 1$
D_n	$2n(n-1)$	$2(n-1)$	4	$\begin{cases} \mathbb{Z}/4\mathbb{Z} & 2 \nmid n \\ (\mathbb{Z}/2\mathbb{Z})^2 & 2 \mid n \end{cases}$	$n \geq 4$
E_6	72	12	3	$\mathbb{Z}/3\mathbb{Z}$	6
E_7	126	18	2	$\mathbb{Z}/2\mathbb{Z}$	7
E_8	240	30	1	1	8

Man kann daraus leicht alle Wurzelgittern finden, dafür gilt $\langle \Gamma_2 \rangle_{\mathbb{R}} = \mathbb{R}^{24}$ und die gleiche Coxeter-Zahl haben. □

Dieselben Argumente kann man auch für $n > 24$ anwenden, aber in diesem Fall gilt nicht, dass $\vartheta_{\Gamma,f} = 0$. Zum Beispiel, sei f wie in Behauptung 3.3 und $n = 32$, dann

$$\vartheta_{\Gamma,f} = \alpha \Delta E_6.$$

Daraus folgt insbesondere, dass

$$-528\Big(\textstyle\sum_{x\in\Gamma, x^2=2} f(x)\Big) = -528 c_1 = c_2 = \Big(\textstyle\sum_{x\in\Gamma, x^2=4} f(x)\Big).$$

Das kann man nutzen, zum Beispiel, um die Anzahl der Elementen $e \in C \subset \mathbb{F}_2^{32}$ mit $e_1 = 1$ zu finden. Dafür betrachten wir $\Gamma = \Gamma_C$ und $y = (\sqrt{2}, 0, ..., 0)$, dann ist

$$\forall x \in \Gamma : x \cdot y = \mathbf{1}_{x_1 = \sqrt{2}^{-1}},$$

deswegen

$$-528\left(\left|\left\{x \in \Gamma_2 \,\middle|\, x_1 = \sqrt{2}^{-1}\right\}\right| - \tfrac{1}{8}|\Gamma_2|\right) = \left|\left\{x \in \Gamma_4 \,\middle|\, x_1 = \sqrt{2}^{-1}\right\}\right| - \tfrac{1}{4}|\Gamma_4|.$$

Falls $|\Gamma_2| = 0$ gilt $\left|\left\{x \in \Gamma_4 \,\middle|\, x_1 = \sqrt{2}^{-1}\right\}\right| = \frac{1}{4}|\Gamma_4|$

3.3 Obergitter und Codes

Sei $\Gamma \in \mathbb{R}^n$ ein gerades Gitter, $\Gamma \hookrightarrow \Gamma^{\#}$ und $G_\Gamma = \Gamma^{\#}/\Gamma$. G_Γ ist eine endliche abelsche Gruppe mit $|G_\Gamma| = disc(\Gamma)$. Definieren wir außerdem die Abbildungen

$$b_\Gamma : G_\Gamma \times G_\Gamma \to \mathbb{Q}/\mathbb{Z}, b_\Gamma(x+\Gamma, y+\Gamma) = x \cdot y + \mathbb{Z}$$
$$q_\Gamma : G_\Gamma \to \mathbb{Q}/2\mathbb{Z}, q_\Gamma(x+\Gamma) = x^2 + 2\mathbb{Z}.$$

b_Γ ist eine endliche symmetrische bilineare Form, q_Γ ist eine endliche quadratische Form, d.h.

$$\forall r \in \mathbb{Z}, x \in G : q_\Gamma(rx) = r^2 q_\Gamma(x),$$
$$q_\Gamma(x+y) - q_\Gamma(x) - q_\Gamma(y) = 2b_\Gamma(x,y) + 2\mathbb{Z}.$$

q_Γ heißt Diskriminantenform von Γ.

Sei Λ ein gerades Gitter in $\mathbb{R}^n$. Die Einbettung in ein gerades Gitter $\Lambda \hookrightarrow \Gamma$ heißt gerades Obergitter von Λ. Betrachten wir $H_\Gamma = \Gamma/\Lambda$, das eine endliche ($|H_\Gamma| = [\Gamma : \Lambda]$) abelsche Gruppe ist. Wir haben eine Kette der Einbettungen

$$\Lambda \hookrightarrow \Gamma \hookrightarrow \Gamma^{\#} \hookrightarrow \Lambda^{\#},$$

deswegen $H_\Gamma \subset \Lambda^{\#}/\Lambda = G_\Lambda$, H_Γ ist isotrop, d.h. $q_\Lambda|_{H_\Gamma} = 0$ (weil Γ gerade ist).

Behauptung 3.5. *Die Abbildung $\Gamma \to H_\Gamma$ ist eine Bijektion zwischen geraden Obergittern von Λ und isotropen Untergruppen von G_Λ. Unimodularen Gittern entsprechen den Untergruppen H mit $|H|^2 = |G_\Lambda|$.*

Beweis. Der erste Teil ist einfach, weil das Gitter zur Vereinigung der Restklassen gleich sein soll, und die Abbildung ist auf diese Weise eindeutig bestimmt. Es lässt sich merken, dass $[\Gamma : \Lambda] = [\Lambda^{\#} : \Gamma^{\#}] = |H_\Gamma|$, woraus man die zweite Behauptung herleiten kann. □

Zwei Gitter Γ, Γ' sind isomorph, wenn ein orthogonaler Automorphismus $u \in O(n, \mathbb{R})$ mit $u(\Gamma) = \Gamma'$ existiert. Analog kann man Automorphismus des Gitters und Isomorphismus der Obergittern definieren. Merken wir außerdem, dass Isomorphismus der Gittern ein Isomorphismus der dualen Gittern und ihren quadratischen Formen induziert. Insbesondere existiert ein Homomorphismus $Aut(\Lambda) \to Aut(G_\Lambda)$.

Behauptung 3.6. *Zwei gerade Obergittern $\Lambda \hookrightarrow \Gamma, \Gamma'$ sind isomorph genau dann, wenn H_Γ, H'_Γ isotrop und unter einem Automorphismus aus Bild vom Homomorphismus $Aut(\Lambda) \to Aut(G_\Lambda)$ konjugiert sind.*

Sei $\Lambda = \langle \Lambda_2 \rangle$. Wir wollen einen Obergitter finden, der keine neuen Wurzeln beinhaltet. Betrachten wir die Abbildung

$$l_\Lambda : G_\Lambda \to \mathbb{Q},\ l_\Lambda(\xi) = \min\{x^2 \,|\, x \in \lambda, x + \Lambda = \xi + \Lambda\},$$

folglich beinhaltet $\Gamma \backslash \Lambda$ genau dann keine Wurzeln, wenn $\forall \xi \in H_\Gamma : l_\Lambda(\xi) \neq 2$.

Korollar 3.6. *Sel $\Lambda = \langle \Lambda_2 \rangle_{\mathbb{Z}}$. Es gibt eine natürliche Bijektion zwischen Isomorphieklassen von geraden Obergittern $\Lambda \hookrightarrow \Gamma$ mit $\Gamma_2 = \Lambda_2$ und Bahnen von isotropen Untergruppen $H \subset G_\Lambda$, die der Bedingung $\forall \xi \in H : l_\Lambda(\xi) \neq 2$ genügen, unter Bild vom Homomorphismus $O(\Lambda) \to O(G_\Lambda)$.*

Beweis. Aus der vorigen Behauptung folgt, das die Abbildung wohldefiniert ist. Die Abbildung $\Gamma \to H_\Gamma$ ist bijektiv, folglich ist die Abbildung zwischen Isomorphieklassen auch bijektiv. □

Ähnliche Ergebnisse kann man für doppelt-gerade Codes bekommen. Sei C so ein Code, definieren wir das tetradsche System

$$C_4 = \{c \in C \,|\, w(c) = 4\}.$$

Code C, den sein tetradsches System erzeugt, ist tetradscher Code genannt. Es ist schon bewiesen, dass solche Codes in irreduzible tetradsche Codes zerfallen, d.h. in die Summe von d_{2k}, $e_7 = H^\perp$ und $e_8 = \tilde{H}$.

Definieren wir analog $G_C = C^\perp / C$ und Gewichtsfunktion

$$w_C : G_C \to \mathbb{Z}, w_C(\eta) = \min\{w(y) \,|\, y + C = \eta + C\}.$$

Zwei Codes C, C' sind äquivalent, falls $\exists \sigma \in S_n : \sigma(C) = C'$, woraus folgt

$$Aut(C) = \{\sigma \in S_n \,|\, \sigma(C) = C\}.$$

Automorphismus von C induziert ein Automorphismus von $C^\perp$ und G_C, deswegen existiert ein kanonisches Homomorphismus $Aut(C) \to Aut(G_C)$.

Behauptung 3.7. *Sei C ein tetradscher Code in $\mathbb{F}_2^n$, dann existiert eine natürliche Bijektion zwischen Equivalenzklassen von doppelt-geraden Codes $C' \in \mathbb{F}_2^n$ mit $C_4' = C_4$ und Bahnen von $H \leq G_C$ mit $\min_{\xi \in H} w(\xi) > 4$ unter dem Bild von $Aut(C)$. C' ist genau dann selbstdual, wenn $|H|^2 = G_C$.*

Beweis. Analog zum Fall der Gitter ist die Abbildung $C' \to H_{C'}$ bijektiv und

$$|H_{C'}| = [C' : C] = [C^\perp : C'^\perp].$$

Es ist dann zu zeigen, dass dem Code C' mit $C_4' = C_4$ eine Gruppe $H_{C'}$ mit $\min_{\xi \in H_{C'}} w(\xi) > 4$ entspricht, was leicht zu sehen ist. □

Erinnert wir uns, das dem Code C ein Gitter Γ_C entspricht, mit $\Gamma_C = \frac{1}{\sqrt{2}} \rho^{-1}(C)$. Merken wir, dass $\sqrt{2}\boldsymbol{e}_i \in \Gamma_C$, wo $\{\boldsymbol{e}_i\}_i$ die Standardbasis von $\mathbb{R}^n$ ist. Diese Wurzeln orthogonal sind, deswegen $nA_1 \subset \Gamma_C$.

Satz 3.3. *Abbildung $C \to \Gamma_C$ induziert eine Bijektion zwischen Äquivalenzklassen von doppelt-geraden Codes und Isomorphieklassen von geraden Gittern, die nA_1 beinhalten. Unimodulare Gitter entsprechen den selbstdualen Codes.*

Beweis. Der zweite Teil des Satzes ist schon bewiesen. Klar, dass die Bilder von zwei isomorphen Codes isomorph sind, weil Permutation der Koordinaten in $O(n, \mathbb{R})$ liegt. Umgekehrt, jede Isomorphieklasse der Gitter hat ein Gitter, darin $nA_1 = \langle \sqrt{2}\boldsymbol{e}_i \rangle$ liegt, und es ist bis auf Permutation der Koordinaten definiert. Es kann in die entsprechende Isomorphieklasse der Codes abgebildet werden, und es lässt sich sehen, das diese zwei Abbildungen Inversen voneinander sind. □

3.4 Klassifikation von geraden unimodularen Gittern in Dimension 24

Satz 3.4. **(Niemeier)** *Bis auf Isomorphismus gibt es genau 24 geraden unimodularen Gitter in $\mathbb{R}^{24}$, die durch ihre Wurzelgitter eindeutig bestimmt sind (sehe Behauptung 3.4).*

Der Beweis des Satzes kann man in "On the classification of integral even unimodular 24-dimensional quadratic forms" von B.B. Venkov finden. Darin werden alle Wurzelgitter betrachtet und für jedes wird es bewiesen, dass die Gruppe $H \leq G_{\Lambda_2}$ mit $|H|^2 = |G_{\Lambda_2}|$ bis zum Isomorphismus aus entsprechender Menge eindeutig definiert ist.

Korollar 3.7. *Es gibt bis auf Isomorphismus 9 Gitter, die dem doppelt-geraden selbstdualen Codes entsprechen. Ihre Wurzelgitter sind*

$$24A_1, 6D_4, 4D_6, 3D_8, 2D_{12}, D_{24}, 3E_8, 2E_7 + D_{10}, E_8 + D_{16}.$$

Beweis. Behauptung 1.5 lässt uns sagen, dass die einzigen Wurzelgitter, die nA_1 beinhalten, als eine Summe von A_1, B_m, E_7 und E_8 dargestellt werden können, und das entsprechende unimodulare Gitter ist in jedem Fall eindeutig definiert. □

Tetradsche Systeme der Codes, die im Korollar 3.7 betrachtet werden, sind

$$\emptyset, 6d_4, 4d_6, 3d_8, 2d_{12}, d_{24}, 3e_8, 2e_7 + d_{10}, e_8 + d_{16}.$$

Zu jedem System existiert genau ein doppelt gerader selbstdualer Code.

Beispiel. Sei $\langle\Gamma_2\rangle_{\mathbb{Z}} = 24A_1$, dann $G_{\Gamma_2} \cong (\mathbb{Z}/2\mathbb{Z})^{24}$ und Bild von $O(\langle\Gamma_2\rangle_{\mathbb{Z}})$ ist $B \cong S_{24}$. Man kann Γ als Teilgitter von $\sqrt{2}\mathbb{Z}^n$ betrachten, dann lässt sich merken, dass die Abbildungen zwischen Γ und entsprechendem Code und zwischen $\Lambda^{\#}$ (wo $\Lambda_2 = \Gamma_2$) und G_{Γ_2} gleich sind, deswegen ist es genug, den Code $C \in G_{\Gamma_2}$ mit nötigen Eigenschaften zu finden. Es gilt

$$\forall a = (a_1, ..., a_{24}) \in G_{\Gamma_2} : l(a) = \tfrac{1}{2} \textstyle\sum_{k=1}^{24} a_i = \tfrac{1}{2}\|a\|,$$

deswegen gilt für C

$$\forall c \in C : \|c\| \in 4\mathbb{Z}, \quad |\{c \in C \mid \|c\| = 4\}| = 0,$$

folglich ist C ein extremaler doppelt-gerader linearer Code in $\mathbb{F}_2^{24}$, also ist er der erweiterte binäre Golay-Code.