Das Rubens-Projekt 71

Technical Report, Universität Siegen 2007

Nils-Peter Skoruppa

Version: $Id: ext72.tex,v f4f3286b0a1b 2013/02/10 22:58:41 nils $

Inhaltsverzeichnis

1 Überblick

Das *Rubens-Projekt 71* beschäftigt sich mit der folgenden Problematik:

> **Systematische Suche nach einem extremalen Gitter vom Rang 72 mit Automorphismus der Ordnung 71. Bei erfolgreichem Abschluss der Rechnungen wird die offene Frage der Existenz oder Nicht-Existenz eines solchen Gitters entschieden sein[1].**

[1] Wir wissen nun am 9. Februar 2013: *Es gibt keine extremalen Gitter vom Rang 72 mit Automorphismus der Ordnung* 71 (siehe Addendum).

2 Extremale Gitter vom Rang 72

Die ganzen, geraden unimodularen Gitter (im Folgenden: GUG) gehören mit zu den interessantesten Gittern und viele der im Hinblick auf Automorphismen-Gruppe oder Dichte bekannesten Gitter sind GUG. Vergleiche hierzu die Gitter-Datenbank in [NS07]. Unter den GUG wiederum sind solche besonders herausragend, die eine möglichst große Minimallänge d haben. Haftet man nämlich an jeden Gitterpunkt eine n-dimensionale Kugel vom Radius $d/2$, so erhält man eine Überdeckung des euklidischen n-dimensionalen Raumes mit nicht-überlappenden Kugeln und der Dichte

$$\frac{\text{vol(Kugel vom Radius } \frac{d}{2})}{\text{vol(Fundamentalmasche des Gitters)}} = \pi^{n/2}\Gamma\left(1+\frac{n}{2}\right)^{-1}\left(\frac{d}{2}\right)^{n/2}.$$

Großes d bedeutet also hohe Dichte.

Die a priori maximale Minimallänge kann man vorhersagen. Ist nämlich L ein GUG, etwa der Dimension r, so ist nach klassischen Resultaten (vgl. etwa [Ser73]) die Thetareihe

$$\Theta_L = \sum_{x\in L} q^{\frac{x^2}{2}}$$

eine Modulform auf der vollen Modulgruppe vom Gewicht $r/2$. Ferner weiß man, daß r ein Vielfaches von 8 ist. Somit ist Θ_L eine Linearkombination der Modulformen

$$E_4^{\frac{r}{8}-3n}\Delta^n = q^n + \ldots \qquad (n = 0, 1, 2, \ldots, \left\lfloor \frac{r}{24} \right\rfloor),$$

wobei

$$E_4 = 1 - 240\sum_{n,l\geq 1} n^3\, q^{nl}, \quad \Delta = \prod_{n\geq 1}(1-q^n).$$

Insbesondere erkennt man hiermit leicht, daß die Minimallänge d von L die Ungleichung

$$\frac{d}{2} \leq \left\lfloor \frac{r}{24} + 1 \right\rfloor$$

erfüllt. Ferner ist Θ_L bekannt, falls in der letzten Ungleichung Gleichheit vorliegt. Dann ist nämlich

$$\Theta_L = E_4^{\frac{r}{8}} -$$

Wir nehmen nun an, dass es ein extremales Gitter L der Dimension 72 gibt. Für die Thetareihe erhalten wir dann

$$\begin{aligned}\Theta_L &= E_4^9 - 2160\,\Delta\,E_4^6 + 965520\,\Delta^2\,E_4^3 - 27302400\,\Delta^3 \\ &= 1 + 6218175600\,q^4 + 15281788354560\,q^5 + \ldots\end{aligned}$$

Wir nehmen weiter an, dass L einen Automorphismus α der Ordnung 71 besitzt.

Ein erster Test für letztere Annahme ist das Folgende. Bezeichnet man mit M das Untergitter von L, welches aus allen Gitterpunkten besteht, die durch α fest gelassen werden, so hat man

$$\Theta_L \equiv \Theta_M \bmod 71.$$

Ferner überlegt man sich leicht, dass M die Determinante -71 besitzt. Aus der Modulformentheorie ist bekannt, dass der Rang r von M die Kongruenz

$$\frac{r}{2} \equiv 36 \bmod \frac{l-1}{2}$$

mit $l = 71$ erfüllen muss. Die einzige Möglichkeit ist daher $r = 2$. Binäre ganze quadratische Formen der Diskriminante -71 gibt es (bis auf $\mathrm{GL}(2,\mathbb{Z})$-Äquivalenz) genau 4, nämlich — in Gauß-Notation —

$$[1,1,8],\ [2,1,9],\ [3,1,6],\ [4,3,5].$$

Man findet tatsächlich ([Sko09])

$$\sum_{r,s\in\mathbb{Z}} q^{4r^2+3rs+5s^2} \equiv \Theta_L \bmod 71.$$

3 Parametrisierung der geraden unimodularen Gitter mit Automorphismen der Ordnung 71

Zur Untersuchung, ob nun tatsächlich ein extremales Gitter vom Rang 72 mit Automorphismus der Ordnung 71 existiert, benutzen wir den folgenden Satz [CS99], hier direkt schon für unseren Fall formuliert:

Satz. *Sei L ein GUG vom Rang 72 mit Minimallänge 8 und mit einem Automorphismus der Ordnung 71. Dann gibt es ein ganzes Ideal $\mathfrak{A}$ im Körper K der 71-ten Einheitzwurzeln und eine total positive Zahl $\lambda \in K$, sodass L (bis auf Isomorphie) folgende Beschreibung hat:*

$$L = \mathfrak{A}(\lambda) \perp \begin{bmatrix} 8 & 3 \\ 3 & 10 \end{bmatrix} + \mathbb{Z}\, x$$

mit einem

$$x \in \mathfrak{A}(\lambda)^{\#} \perp \begin{bmatrix} 8 & 3 \\ 3 & 10 \end{bmatrix}^{\#}, \quad x^2 \in 2\mathbb{Z}.$$

Hierbei bezeichnet $\mathfrak{A}(\lambda)$ das Gitter, welches entsteht, indem man $\mathfrak{A}$ mit folgendem Skalarprodukt versieht:

$$(a, b) \mapsto \mathrm{tr}\,(a\,\lambda\,\overline{b}).$$

Es gilt hierbei

$$\lambda\,\mathfrak{A}\,\overline{\mathfrak{A}} = (1-\zeta)^{-68},$$

wo ζ eine primitive 71-te Einheitswurzel ist.

Wir stellen zunächst fest:

- Das Gitter $\mathfrak{A}(\lambda)$ hat Minimallänge 8.
- Das Ideal $\mathfrak{A}\,\overline{\mathfrak{A}}$ ist ein Hauptideal. Anders ausgedrückt bedeutet dies, dass die Idealklasse von $\mathfrak{A}$ in C^- liegt. Hierbei bezeichnet C^- die Untergruppe der Idealklassen k von K, für die $\overline{k} = k^{-1}$ gilt (-1-Eigenraum bezüglich komplexer Multiplikation).
- Liegen die Gitter $\mathfrak{A}$ und $\mathfrak{B}$ in der gleichen Idealklasse, etwa $\mathfrak{A} = \mu\mathfrak{B}$ für ein $\mu \in K$, so sind die Gitter $\mathfrak{A}(\lambda)$ und $\mathfrak{B}(\mu\lambda\overline{\mu})$ isomorph. Ferner hat man
  $$\mathfrak{A}(\lambda) \cong \mathfrak{A}^\sigma(\lambda^\sigma)$$
  für jede Galoissubstitution σ von K.
- Ist ε eine Einheit in K, so ist $\varepsilon\overline{\varepsilon}$ total positiv und
  $$\mathfrak{A}(\lambda\varepsilon\overline{\varepsilon}) \cong \mathfrak{A}(\lambda).$$
- Es gilt (als Identität zwischen Idealen)
  $$(1-\zeta)^{-68} = \left(4\sin^2(\frac{\pi}{71})\right)^{-34}$$
  und $\sin^2(\pi/71)$ ist ein total positives Element von K. Insbesondere folgt, dass $\mathfrak{A}\,\overline{\mathfrak{A}}$ von einem total positiven Element erzeugt wird.

Die Gesamtheit aller zu untersuchenden Gitter wird demnach schon beschrieben durch die Repräsentanten $\mathfrak{A}(\lambda\varepsilon)$, wobei

$$\mathfrak{A} \in C^-, \quad \varepsilon \in E_{\gg 0}/F, \quad \lambda = \mu^{-1}\left(4\sin^2(\frac{\pi}{71})\right)^{-34}.$$

Hierbei ist μ total positiv gewählt, sodass $\mu = \mathfrak{A}\overline{\mathfrak{A}}$ (stets möglich — s.u.), es ist E die Gruppe der Einheiten in K, es bezeichnet $E_{\gg 0}$ die Untergruppe der total positiven Einheiten, und F ist die Untergruppe aller Einheiten der Gestalt $\varepsilon\overline{\varepsilon}$ mit einer geeigneten Einheit ε von K. Ferner genügt es noch, diese Repräsentanten bis auf Galoiskonjugation zu untersuchen. Bezeichne im Folgenden G die Galoisgruppe von K.

4 Die Einheitengruppe von $\mathbb{Q}(\mu_{71})$

Wir stellen hier einige Fakten über die Einheitengruppe E von $K = \mathbb{Q}(\mu_{71})$ zusammen.

Satz. *Es bezeichnen K^+ den maximalen total reellen Unterkörper von K und und E^+ seine Einheitengruppe. Für zu 71 relativ primes a bezeichne σ_a die Galoissubstitution $\zeta \mapsto \zeta^a$ ($\zeta \in \mu_l$). Dann gilt:*

1. *Es gilt $E = \mu_l \, E_+$ (und daher insbesondere $F = E_+^2$).*
2. *Die Abbildung*
$$\varepsilon \mapsto (\mathrm{sign}(\varepsilon^{\sigma_a}))_{1 \le a \le 35}$$
induziert einen Isomorphismus
$$E_+ / E_{\gg 0} \to \mathbb{F}_2^{35}.$$
Hierbei steht $E_{\gg 0}$ für die Untergruppe der total positiven Einheiten.

Beweis. Wir beweisen die erste Behauptung (siehe auch [Was97], Proposition 1.5). Ist $u \in K$, $u \neq 0$ so hat $z := u/\overline{u}$ den Absolutbetrag 1, und das gleiche gilt für sämtliche Konjugierte von z (denn G ist kommutativ). Da z zudem ganz ist, ist es eine Einheitswurzel. Die Gruppe der Einheitswurzeln in K ist aber gerade $\{\pm 1\}\mu_l$. Wäre $z = -\zeta^a$ für eine $1 \neq \zeta \in \mu_l$ und eine ganze Zahl a, so hätte man also $u = -\zeta^a \, \overline{u} \equiv -\overline{u} \bmod (1-\zeta)$, andererseits gilt aber $u \equiv \overline{u} \bmod (1-\zeta)$ (schreibe u als Polynom in ζ), also $2u \in (1-\zeta)$, also auch $2 \in (1-\zeta)$. Dies ist ein Widerspruch (betrachte Normen).

Wir erhalten damit einen Gruppenhomomorphismus

$$E \to \mu_l, \quad u \mapsto u/\overline{u}.$$

Der Kern ist aber offenbar E_+ (wieder, weil die Galoisgruppe G von K kommutativ ist). Hieraus folgt sofort die erste Behauptung (ist $u \in E$, so gibt es — da l ungerade ist — ein $\eta \in \mu_l$ mit $u/\overline{u} = \eta^2$, d.h. $(u/\eta) \cdot \overline{u/\eta} = 1$, somit $u/\eta \in E^+$).

Zum Nachweis der zweiten Behauptung betrachten wir die zyklotomischen Einheiten

$$\varepsilon(a) = \frac{\sin\left(\frac{2\pi a}{71}\right)}{\sin\left(\frac{2\pi}{71}\right)} = \zeta^{1-a} \, \frac{\zeta^{2a}-1}{\zeta^2-1} \qquad (a \in \mathbb{Z},\ 71 \not| a).$$

Offenbar gilt

$$\varepsilon(ab) = \varepsilon(a)^{\sigma_b} \varepsilon(b),$$

und für $1 \leq a \leq 70$ hat man

$$\varepsilon(a) > 0 \Longleftrightarrow a \leq 35.$$

Zum Nachweis der zweiten Behauptung genügt es zu zeigen, dass die Bilder der 34 Einheiten $\varepsilon(a)$ $(2 \leq a \leq 35)$ und der Vektor $(1, 1, \ldots, 1)$ (d.h. das Bild von -1 unter der in Frage stehenden Abbildung) linear unabhängig über $\mathbb{F}_2$ sind. Das Bild von $\varepsilon(a)$ ist

$$(\operatorname{sign} \varepsilon(a)^{\sigma_b})_b = (\operatorname{sign}(\varepsilon(ab))_b + (\operatorname{sign} \varepsilon(b))_b = (\operatorname{sign} \varepsilon(ab))_b \,,$$

wie leicht mit den angegebenen Eigenschaften der zyklotomischen Einheiten folgt. Eine einfache Rechnung mit GP zeigt nun die Behauptung. □

Korollar. *Es gilt* $E_{\gg 0} = E_+^2$.

Beweis. Es ist ja

$$[E_+ : E_+^2] = [E_+ : E_{\gg 0}] \cdot [E_{\gg 0} : E_+^2].$$

Nach dem Dirichletschen Einheitensatz ist der Rang von E_+ gerade 34, also $[E_+ : E_+^2] = 35$ (die Einheitswurzel -1 von K_+ erhöht den Index). Nach dem Satz ist $[E_+ : E_{\gg 0}] = 35$. Es folgt $[E_{\gg 0} : E_+^2] = 1$. □

Als Folgerung aus dem Beweis des Satzes notieren wir noch

Korollar. *Ist* $\lambda \in K^+$, *so gibt es eine Teilmenge* $T \subset \{2, \ldots, 35\}$, *und ein Vorzeichen* ϵ, *sodass*

$$\lambda \, \epsilon \prod_{a \in \lambda} \varepsilon(a)$$

total positiv ist.

Wir bemerken noch, dass E^+ von den zyklotomischen Einheiten und von ± 1 erzeugt wird. Die folgt aus der Tatsache, dass der Index der von den zyklotomischen Einheiten und ± 1 erzeugten Untergruppe in E^+ nach einem allgemeinen Satz gleich der Klassenzahl von K^+ ist (siehe [Was97], Theorem 8.2), und diese ist gerade 1.

5 Die Klassengruppe von $\mathbb{Q}(\mu_{71})$

Für einen Teiler $d|72$ bezeichnen wir mit K_d den Teilkörper $K_d \subseteq K$ vom Grad $[K_d : \mathbb{Q}] = d$. Die Klassengruppen $\operatorname{Pic}(K_d)$ (und einige andere Invarianten) der Zwischenkörper haben wir in Tabelle 1 zusammengestellt. Die

Tabelle 1: Zwischenkörper und ihre Invarianten

Körper	K_2	K_5	K_7	K_{10}	K_{14}	K_{35}	K_{70}
Klassengruppe	7	1	1	7	49 (zykl.)	1	$7^2 \cdot 79241$ (zykl.)
Diskriminante	-71	71^4	71^6	-71^9	-71^{13}	71^{34}	-71^{69}
inv. Differente	$\sqrt{-71}$					$(\zeta + \zeta^{-1} - 2)^{34}$	$(1-\zeta)^{69}$

Berechnung der Klassengruppen von K_d für $d \neq 71$ geschieht mittels Pari/GP.

Die Klassenzahl h_-, d.h. die Anzahl der Klassen in

$$\mathrm{Pic}(K)^- = \{C \in \mathrm{Pic}(K) \,|\, C\,\overline{C} = 1\}.$$

ist nach der analytischen Klassenzahlformel für K und K_+ und der Tatsache, dass

$$1 \to \mathrm{Pic}(K)^- \to \mathrm{Pic}(K) \to \mathrm{Pic}(K^+) \to 1$$

(gebildet mit Inklusion bzw. Normabbildung) exakt ist, durch folgende Formel gegeben:

$$h_- = \frac{\zeta_K}{\zeta_{K^+}}(1) = \frac{1}{(2l)^{(l-1)/2}} |F(\theta)F(\theta^3)\cdots F(\theta^{l-2})|.$$

Dabei ist θ eine primitive 70-te Einheitswurzel und

$$F(X) = \sum_{s=0}^{69} g_s X^s,$$

wo $g_s = g^s \% 71$ mit einer Primitivwurzel g modulo l.

Eine Rechnung mit GP ergibt

$$h_- = 3,882,809 = 7^2 * 79241.$$

Für unseren Fall ist h_- schon die Klassenzahl h schlechthin, da K^+ ja Klassenzahl 1 hat, und nach obiger exakter Sequenz ja h_- der Quotient der Klassenzahl von K und der von K^+ ist. Die Klassengruppe von K ist dann weiter aber auch zyklisch: sie enthält ja ein Element der Ordnung 49, was wiederum aus der Surjektivität der durch die Norm induzierten Abbildung $\mathrm{Pic}(K) \to \mathrm{Pic}(K_{14})$ folgt. Ferner sehen wir, dass für jedes Ideal $\mathfrak{a}$ von K stets $\mathfrak{a} \cdot \overline{\mathfrak{a}}$ ein Hauptideal ist.

(Die Exaktheit der Sequenz ergibt sich folgendermaßen: Die Surjektivität der Normabbildung folgt aus der Klassenkörpertheorie (vgl. [Was97], Appendix, Theorem 5). Der Kern von $C_k \to \mathrm{Pic}(K^+)$ ist gleich dem Kern der Komposition $C_K \to \mathrm{Pic}(K^+) \to K$ mit der natürlichen Abbildung $\mathrm{Pic}(K^+) \to \mathrm{Pic}(K)$ (und damit offensichtlich $\mathrm{Pic}(K)^-$), da letztere injektiv ist: es sei nämlich $\mathfrak{A}$ Ideal in K^+ und $\mathfrak{A}O_K = (\alpha)$. Jedenfalls ist — wie oben — $\overline{\alpha} = z\alpha$ mit einer Einheitzwurzel z. Setzen wir $\lambda = 1 - \zeta$, so ist $\lambda/\overline{\lambda} = -\zeta$, erzeugt also die Einheitswurzeln in K, somit also $z = (\lambda/\overline{\lambda})^k$ für ein ganzes k, also $\alpha\lambda^k$ reell. es folgt $\mathfrak{A}O_K(\lambda^k O_K) = \alpha\lambda^k O_K$, und daher ist λ^k Ideal in K^+. Da $71 = \lambda^{70}$ muss dann aber k gerade sein (Übungsaufgabe). Es ist dann aber z ein Quadrat in K, und daher ist es im Bild der Abbildung $E \to W$, $u \mapsto u/\overline{u}$, etwa $z =\mapsto u/\overline{u}$. Also ist $\alpha u \in K^+$. Zum Nachweis, dass W^2 das Bild der Abbildung $E \to W$ ist, genügt es zu sehen, dass jedenfalls W^2 im Bild ist, denn $u/\overline{u} = u^2$ für Einheitswurzeln u, und zwar also vom Index 1 oder 2. Aber 2 ist richtig, denn andernfalls gäbe es eine Einheit, sodass $(1-\zeta)u$ in K^+ läge, ein Primelement in K^+ über 71 und $p = (1-\zeta)u$ in K^+, was offenbar ein Widerspruch ist.)

Wir betrachten nun $\mathrm{Pic}(K)$ als $\mathbb{Z}[G]$-Modul. Es bezeichne $\mathfrak{St}$ das Stickelberger-Ideal, d.h.

$$\mathfrak{St} = \theta \cdot \{a - [a] \,|\, a = 1, \ldots, l-1\}, \quad \theta = \frac{1}{l}\sum_{a=1}^{l-1} a\,[a^{-1}]$$

Hierbei bezeichnet $[a]$ die Gaoissubstitution $\mu_l \ni z \mapsto z^a$. Nach dem Satz von Stickelberger vernichtet $\mathfrak{St}$ die Klassengruppe von K.

Wir setzen ferner

$$\mathbb{Z}[G]^- := \{\alpha \in \mathbb{Z}[G] \,|\, \alpha\,[-1] = -\alpha\} = \ker(1 + [-1]) = \mathrm{im}(1 - [-1]).$$

Nach einem Satz von Iwasawa [Was97, p. 103] ist der Index von $\mathfrak{St} \cap \mathbb{Z}[G]^-$ in $\mathbb{Z}[G]^-$ gerade gleich h_-. Da $\mathrm{Pic}(K)$ zyklisch ist und $\mathrm{Pic}(K) = \mathrm{Pic}(K)^{1-[-1]}$ erfüllt, insbesondere also auch zyklisch als $\mathbb{Z}[G]^-$-Modul ist, folgt, dass

$$\mathrm{Pic}(K) \approx \mathbb{Z}[G]^-/\mathfrak{St} \cap \mathbb{Z}[G]^-$$

als $\mathbb{Z}[G]$-Moduln. (Siehe hierzu auch [Was97, p. 107].)

Danach ist aber der Annihilator von $\mathrm{Pic}(K)$ gerade das Ideal

$$\mathfrak{Ann} := \{\alpha \in \mathbb{Z}[G] \,|\, \alpha \cdot (1 - [-1]) \in \mathfrak{St}\} = \mathfrak{St} : (1 - [-1]),$$

wie man mittels der exakten Sequenz von $\mathbb{Z}[G]$-Moduln

$$0 \to \mathfrak{Ann} \to \mathbb{Z}[G] \to Z[G]^-/\mathfrak{St} \cap Z[G]^- \to 0$$

(die dritte Abbildung ist Multiplikation mit $1-[-1]$) aus dem vorstehenden Isomorphismus folgert. Es gilt dann also, dass

$$\mathrm{Pic}(K) \approx \mathbb{Z}[G]/\{\alpha \in \mathbb{Z}[G] \,|\, \alpha \cdot (1-[-1]) \in \mathfrak{St}\}$$

als $\mathbb{Z}[G]$-Moduln.

Insbesondere können wir hiermit den durch die Operation von G auf $\mathrm{Pic}(K)$ gegebenen Homomorphismus

$$G \to \mathrm{Aut}(\mathrm{Pic}(K)) \approx (\mathbb{Z}/h\mathbb{Z})^*$$

berechnen.

Primitivwurzel modulo $l = 71$ ist 7, und wir suchen $([7]-n)([1]-[-1]) \in \mathfrak{St}$ für ein zu h teilerfremdes n. Eine Rechnung mit PARI/GP ergibt $n = 1,137,674$. Insbesondere ist die Abbildung $G \to (\mathbb{Z}/h\mathbb{Z})^*$ injektiv.

6 Rechnungen

Damit ergibt sich zur systematischen Suche nach einem extremalen Gitter vom Rang 72 mit Automorphismus der Ordnung 71 folgendes Vorgehen:

- Für alle rationalen Primzahlen p mit $p \le S$, $p \neq 71$ führe das Folgende aus: Zerlege $\Phi = \Phi_{71} := X^{70} + X^{69} + \cdots + 1$ über dem Körper $\mathbb{F}_p$, etwa

  $$\Phi \equiv f_1 \cdots f_r \bmod p, \qquad (f_j \in \mathbb{Z}[X]).$$

- Betrachte für $f = f_1$ das Primideal

  $$\mathfrak{P} := (p, f(\zeta)).$$

  Entscheide, ob $\mathfrak{P}\overline{\mathfrak{P}}$ ein Hauptideal ist, und wenn ja, ob es in die Klassengruppe $\mathrm{Pic}(K)^-$ erzeugt. Wenn ja, berechne ein total positives $a \in K$, Soda $\mathfrak{P}\overline{\mathfrak{P}} = (a)$ und beende die Suche.

Eine Suche mit Pari/GP ergab $p = 569$. Sei also $\mathfrak{P}$ ein Primideal über p, und $a = \mathfrak{P}\overline{\mathfrak{P}}$. Damit können wir nun alle potentiell extremalen Gitter vom Rang 72 mit einem Automorphismus der Ordnung 71 bestimmen:

- Berechne die Gitter

  $$\Gamma := \mathfrak{P}^n \left(a^{-n}\, 2^{-68}\, \sin^{-68}(\pi/71)\right),$$

  wo $1 \le n \le h$.

- Für jedes Gitter Γ aus der eben beschriebenen Liste bestimme die Klassen $[x]$ wo

$$[x] \in \Gamma^{\#}/\Gamma \oplus \begin{bmatrix} 8 & 3 \\ 3 & 10 \end{bmatrix}^{\#} / \begin{bmatrix} 8 & 3 \\ 3 & 10 \end{bmatrix}, \quad x^2 \in 2\mathbb{Z}, \quad x^2 \geq 8.$$

  Verklebe Γ und $\begin{bmatrix} 8 & 3 \\ 3 & 10 \end{bmatrix}$ wie im Satz beschrieben.

Die Entscheidung, ob die Potenzen eines Primideals die Klassengruppe erzeugen, bedarf einiger zusätzlicher Überlegungen, da die entsprechenden Rechnungen zu aufwendig werden. Die Berechnung der Gitter Γ kann ebenfalls nicht direkt in der angeführten Form durchgeführt werden, da die Berechnung der Potenzen $\mathfrak{P}^n$ zu lange dauern würde. Tatsächlich erzeugen wir Vertreter der Klassengruppe mittels der zusätzlichen Strukture der Klassengruppe als Galois-Modul (siehe den vorangehenden Abschnitt). Details der Rechnungen werden anderswo veröffentlicht.

Literatur

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[NS07] G. Nebe and N. J. A. Sloane. *A Catalogue of Lattices*. Nebe and Sloane, 2007. `http://www2.research.att.com/ njas/lattices/`.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Sko09] Nils-Peter Skoruppa. Reduction mod l of theta series of level l^n. In *Quadratic forms—algebra, arithmetic, and geometry*, volume 493 of *Contemp. Math.*, pages 379–389. Amer. Math. Soc., Providence, RI, 2009.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

7 Addendum. (Hinzugefügt am 9. Feb. 2013)

Wir wissen nun:

Satz. *Es gibt keine extremalen Gitter vom Rang 72 mit einem Automorphismus der Ordnung* 71.

Die Berechnung aller potentiell extremalen Gitter mit Automorphismus der Ordnung 71 wurde in der Tat 2007 abgeschlossen. Zu jenem Zeitpunkt konnten wir allerdings mit den uns zur Verfügung stehenden Mitteln für die meisten Gitter keine kurzen Vektoren finden, sodass wie sie von der Liste der potentiell extremalen Gitter ausschließen hätten können. Mittlerweile konnten wir aber nach Hinweisen von Gabriele Nebe mittels in Magma implementierter Algorithmen zur Gitterreduktion zeigen, dass alle Gitter einen Vektor mit Quadratlänge ≤ 6 besitzen. Ein entsprechende ausführliche Veröffentlichung mit den Details der im vorliegendenden Bericht skizzierten Vorgehensweise ist in Vorbereitung.