Commun. Math. Phys. 126, 25–48 (1989)

Communications in
Mathematical
Physics

Classification of Lattices with Z_m Symmetry

Mizuki Ono
Department of Physics, University of Tokyo, Bunkyo-ku, Tokyo 113, Japan

Abstract. We consider the n-dimensional Euclidean lattices with Z_m symmetries. It is shown that such lattices can be considered as ideals of some cyclotomic fields. Therefore we can translate problems about the above lattices into those about number theory. For all n ($n \leqq 22$), we have obtained the classification of such lattices.

1. Introduction

In recent years superstring theory has been actively investigated. Since superstring theory has the critical dimension 10, we must consider compactification problems. Recently, many compactification schemes have been studied intensively [1–4]. Especially, since orbifold models [1] are phenomenologically interesting and easy to handle, many orbifold models have been constructed [5–7]. Therefore, not only phenomenological considerations, but also systematic classifications of orbifold models are needed [7].

An orbifold is a torus divided by its automorphisms, and the torus is an Euclidean space divided by some lattice. Therefore, in order to classify orbifold models, we have to classify lattices, at first. So in this paper, we consider lattices which have Z_m symmetries.

This paper is organized as follows. In Sect. 2, we clarify the problem by considering it form the viewpoint of eigenvalues of automorphism transformations. In Sect. 3, we study cases in which lattices have special symmetries. We show that in these cases, lattices can be considered as ideals of some cyclotomic field. Furthermore, we classify such special lattices. In Sect. 4, we classify general lattices by making use of the results which are obtained in Sect. 2 and 3. Section 5 is devoted to a conclusion.

Throughout this paper, we assume some knowledge of number theory. About number theory, we refer to [8–11]. Especially about cyclotomic fields, we refer to [11].

2. Consideration from Eigenvalues of Transformation

Let us denote the lattice as Γ and the transformation as X. Here $X \in O(n)$ and $X^m = 1$. Since the order of X is m, all its eigenvalues are m^{th} roots of 1. Therefore there exist some orthonormal basis $\{u_j\}_{1 \leqq j \leqq n}$ with which X has a form

$$X = \begin{pmatrix} X_1 & & & \\ & X_2 & & \\ & & \ddots & \\ & & & X_k \end{pmatrix} \tag{2.1}$$

where for all j, X_j is some element of $O(d_j)$ (d_j is some natural number and they satisfy that $\sum_{j=1}^{k} d_j = n$) and all its eigenvalues are primitive $m_j{}^{\text{th}}$ roots of 1 (m_j is some divisor of m). Note that if $i \neq j$, then $m_i \neq m_j$.

From now on, elements (or blocks) of a matrix which are not explicitly written should be understood to be zero (or zero matrix).

We show in what follows that Γ is embedded in an orthogonal sum of some special lattices.

Let some basis of Γ be $\{\lambda_j\}_{1 \leqq j \leqq n}$, and let us denote the matrix whose j^{th} column vector is $\lambda_j (1 \leqq j \leqq n)$ as Λ. Then, $\Lambda^{-1} X \Lambda \in GL(n, Z)$.

Generally, minimal polynomials of the primitive l^{th} root of 1 are called the cyclotomic polynomials, and are denoted by $\Phi_l(x)$. It is known from number theory that they have the following characters:

1. Degree of $\Phi_l(x)$ is $\varphi(l)$. ($\varphi(x)$ is the Euler's function.)
2. $\Phi_l(x) \in Z[x]$, i.e., all coefficients of $\Phi_l(x)$ are integers.
3. Coefficient of $x^{\varphi(l)}$ is 1.
4. $\Phi_l(x) = 0$, if and only if x is a primitive l^{th} root of 1.
5. $\Phi_l(x)$ has no multiple roots.

Suppose we pick up arbitrary $j (1 \leqq j \leqq k)$. Then, we have

$$\Phi_{m_j}(X) = \begin{pmatrix} \Phi_{m_j}(X_1) & & & & & & \\ & \ddots & & & & & \\ & & \Phi_{m_j}(X_{j-1}) & & & & \\ & & & O & & & \\ & & & & \Phi_{m_j}(X_{j+1}) & & \\ & & & & & \ddots & \\ & & & & & & \Phi_{m_j}(X_k) \end{pmatrix}.$$

Since $i \neq j \Rightarrow m_i \neq m_j$, for all i $(i \neq j)$, $\det \Phi_{m_j}(X_i) \neq 0$. Therefore, $\dim U_j = n - d_j$, where $U_j = \{x \in R^n \mid \exists y \in R^n, x = \Phi_{m_j}(X) y\}$. Clearly U_j is a subspace of R^n, which is spanned by $\{u_i\}_{1 \leqq i \leqq \sum_{l=1}^{j-1} d_l}$ and $\{u_i\}_{\sum_{l=1}^{j} d_l < i \leqq n}$. Since $\Phi_{m_j}(x) \in Z[x]$, and $\Lambda^{-1} X \Lambda \in GL(n, Z)$, we get

$$\Lambda^{-1} \Phi_{m_j}(X) \Lambda = \Phi_{m_j}(\Lambda^{-1} X \Lambda) \in M_n(Z).$$

(Here $M_n(Z)$ implies $n \times n$-dimensional integral matrices.)

Therefore, $\Gamma \cap U_j$ is an $(n-d_j)$-dimensional sublattice of Γ. Let some basis of this sublattice be $\{\gamma_i\}_{1 \leqq i \leqq n-d_j}$, and filling these, let another basis of Γ be $\{\gamma_i\}_{1 \leqq i \leqq n}$.

Now let the subspace of R^n which is spanned by $\{u_i\}_{\sum_{l=1}^{j-1} d_l < i \leqq \sum_{l=1}^{j} d_l}$ be V_j. Then $R^n = U_j \perp \dot{V}_j$("$\perp$" means "orthogonal sum"). And let projections of arbitrary vectors x on V_j be $x^{(j)}$. Then we get the following:

$$\Gamma^{(j)} = [\gamma_1^{(j)}, \ldots, \gamma_n^{(j)}] = [\gamma_{n-d_j+1}^{(j)}, \ldots, \gamma_n^{(j)}].$$

(Here $\Gamma^{(j)} = \{x^{(j)} | x \in \Gamma\}$, and $[\gamma_1^{(j)}, \ldots, \gamma_n^{(j)}]$ implies a lattice spanned by $\{\gamma_i^{(j)}\}_{1 \leqq i \leqq n}$.)

Notice d_j-vectors $\{\gamma_i^{(j)}\}_{n-d_j+1 \leqq i \leqq n}$ are linearly independent.

Therefore $\Gamma^{(j)}$ is a d_j-dimensional lattice contained in V_j. Clearly, $\Gamma^{(j)}$ is invariant under the operation of X, and within the subspace V_j, the operation of X is equivalent to that of X_j. Therefore $\Gamma^{(j)}$ is a d_j-dimensional X_j-invariant lattice which is contained in V_j.

In the above consideration, j is arbitrary, and by definition of $V_j, R^n = V_1 \perp \cdots \perp V_k$. Therefore we get the following result.

"Choose proper d_j-dimensional X_j-invariant lattices Γ_j for $1 \leqq j \leqq k$, and let the orthogonal sum of $\Gamma_j (1 \leqq j \leqq k)$ be Γ'. Then Γ is embedded in Γ'."

3. Lattices with Special Symmetry

Next, let us consider Γ_j, which is a d_j-dimensional X_j-invariant lattice. Here $X_j \in O(d_j)$, and its eigenvalues are primitive m_jth roots of 1 only.

Here d_j must be a multiple of $\varphi(m)$. This statement can be proven as follows. Let us denote some basis of Γ_j as $\{\lambda_i^j\}_{1 \leqq i \leqq d_j}$, and the matrix whose ith column vector is $\lambda_i^j (1 \leqq i \leqq d_j)$ as Λ_j. Then $\Lambda_j^{-1} X_j \Lambda_j \in GL(d_j, Z)$. Therefore $f_j(x) \in Z[x]$. Here $f_j(x)$ is the characteristic polynomial of X_j. And solutions of $f_j(x) = 0$ are primitive m_jth roots of 1 only. Hence there exists some natural number n_j, which satisfies $f_j(x) = \{\Phi_{m_j}(x)\}^{n_j}$. Therefore d_j must satisfy $d_j = \varphi(m_j) \cdot n_j$.

From now on we denote $\Gamma_j, X_j, d_j, m_j, n_j$ as Γ, X, d, m, n in this section.

3.1 The Minimal Lattice. First, let us consider special cases, $n = 1$. Let us denote $\exp(2\pi i/m)$ as ζ_m, and mth cyclotomic field as $Q(\zeta_m)$. In these cases, we show in this subsection that there is a correspondence between Γ's and ideals of $Q(\zeta_m)$.

If $m = 1$ or, 2, then $\varphi(m) = 1$. Therefore these cases are trivial. Suppose $m \geqq 3$.

First, we transform Γ to a form easy to handle. With proper orthonormal basis, X has a form

$$X = \begin{pmatrix} R_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ & & & & R_{\varphi(m)/2} \end{pmatrix}.$$

Here for all j,

$$R_j = \begin{pmatrix} \cos\theta_j & -\sin\theta_j \\ \sin\theta_j & \cos\theta_j \end{pmatrix}.$$

(For all $l, e^{i\theta_l}$ is a primitive mth root of 1, and let $e^{i\theta_1}$ be ζ_m.)

Let some basis of Γ be $\{\lambda_j\}_{1 \leqq j \leqq \varphi(m)}$ with $\lambda_j = (\lambda_{1j}, \ldots, \lambda_{\varphi(m)j})^T$ ("T" means "transposed"). Then there exists some A ($A \in GL(\varphi(m), Z)$) which satisfies

$$X\begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1\varphi(m)} \\ \vdots & & \vdots \\ \lambda_{\varphi(m)1} & \cdots & \lambda_{\varphi(m)\varphi(m)} \end{pmatrix} = \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1\varphi(m)} \\ \vdots & & \vdots \\ \lambda_{\varphi(m)1} & \cdots & \lambda_{\varphi(m)\varphi(m)} \end{pmatrix} A.$$

Multiplying

$$\Xi \overset{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & & & \\ 1 & -i & & & \\ & & \ddots & & \\ & & & 1 & i \\ & & & 1 & -i \end{pmatrix}$$

from the left, we get

$$\begin{pmatrix} R'_1 & & \\ & \ddots & \\ & & R'_{\varphi(m)/2} \end{pmatrix} \Omega = \Omega A.$$

Here

$$\text{for all } j, \quad R'_j = \begin{pmatrix} e^{i\theta_j} & 0 \\ 0 & e^{-i\theta_j} \end{pmatrix}, \quad \text{and} \quad \Omega = \Xi \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1\varphi(m)} \\ \vdots & & \vdots \\ \lambda_{\varphi(m)1} & \cdots & \lambda_{\varphi(m)\varphi(m)} \end{pmatrix}.$$

This means that all row vectors of Ω are eigenvectors of A.

Since all eigenvalues of A are primitive m^{th} roots of 1, they are all contained in $Q(\zeta_m)$. Therefore we can choose vectors-on-$Q(\zeta_m)$ as eigenvectors of A, and all eigenspaces of A are 1-dimensional spaces (since $\Phi_m(x)$ has no multiple roots). Hence we can write Ω as follows.

$$\Omega = \begin{pmatrix} c_1 & & & & \\ & c_1^* & & & \\ & & \ddots & & \\ & & & c_{\varphi(m)/2} & \\ & & & & c^*_{\varphi(m)/2} \end{pmatrix} \Omega', \quad \text{where} \quad \begin{cases} \Omega' \in GL(\varphi(m), Q(\zeta_m)) \\ c_j \in C - \{0\} \quad (\text{for all } j) \end{cases}$$

Notice that for all j, the $(2j-1)^{\text{th}}$ and the $(2j)^{\text{th}}$ row vectors of Ω' are mutually complex conjugate.

Let the first row vector of Ω' be $(\alpha_1, \ldots, \alpha_{\varphi(m)})$. Then this satisfies

$$\zeta_m(\alpha_1, \ldots, \alpha_{\varphi(m)}) = (\alpha_1, \ldots, \alpha_{\varphi(m)})A.$$

Transforming both sides of this equation by some element of $G(Q(\zeta_m)/Q)$ (group of automorphisms of $Q(\zeta_m)$, which fix Q pointwise) that transforms ζ_m to

$e^{i\theta_j}(1 \leqq j \leqq \varphi(m)/2)$, we get

$$e^{i\theta_j}(\beta_1, \ldots, \beta_{\varphi(m)}) = (\beta_1, \ldots, \beta_{\varphi(m)})A$$

(where for all l, β_l is the image of α_l by this transformation).

Since all eigenspaces of A are 1-dimensional spaces, this equation implies

$$(\beta_1, \ldots, \beta_{\varphi(m)}) \propto \{\text{the } (2j-1)^{\text{th}} \text{ row vector of } \Omega'\}.$$

Therefore, by choosing the above $c_l(1 \leqq l \leqq \varphi(m)/2)$ properly, we can assume

$$(\beta_1, \ldots, \beta_{\varphi(m)}) = \{\text{the } (2j-1)^{\text{th}} \text{ row vector of } \Omega'\}.$$

Hence Ω' is totally determined by its first row vector.

With this Ω', we consider the correspondence between lattices and ideals of $Q(\zeta_m)$.

Now let us consider $(\alpha_1, \ldots, \alpha_{\varphi(m)})$. We define next two sets:

$$\mathfrak{a} = \left\{ \sum_{i=1}^{\varphi(m)} n_i \alpha_i \,|\, \forall i, n_i \in Z \right\},$$

$$\mathfrak{o}_m = \left\{ \sum_{i=0}^{\varphi(m)-1} n_i (\zeta_m)^i \,|\, \forall i, n_i \in Z \right\}.$$

It is known from number theory that $\mathfrak{o}_m$ is the principal order of $Q(\zeta_m)$, and clearly $\mathfrak{a}$ is a submodule of $Q(\zeta_m)$.

By definition of $(\alpha_1, \ldots, \alpha_{\varphi(m)})$ for arbitrary j $(j \geqq 0)$, the next relation is satisfied,

$$(\zeta_m)^j(\alpha_1, \ldots, \alpha_{\varphi(m)}) = (\alpha_1, \ldots, \alpha_{\varphi(m)})A^j.$$

This means

$$(\zeta_m)^j \alpha_i \in \mathfrak{a} \quad (j \geqq 0, 1 \leqq i \leqq \varphi(m)).$$

Therefore $\mathfrak{a}$ is an $\mathfrak{o}_m$-submodule of $Q(\zeta_m)$. And it is known from number theory that for each α_i $(1 \leqq i \leqq \varphi(m))$, there exists some natural number l_i which satisfies $l_i \alpha_i \in \mathfrak{o}_m$. Therefore $N\mathfrak{a} \subset \mathfrak{o}_m$, where $N = \prod_{i=1}^{\varphi(m)} l_i$.

To summarize

1. $\mathfrak{a}$ is an $\mathfrak{o}_m$-submodule of $Q(\zeta_m)$.
2. There exists some natural number N which satisfies $N\mathfrak{a} \subset \mathfrak{o}_m$.

Hence $\mathfrak{a}$ is some (fractional) ideal of $Q(\zeta_m)$, and $\{\alpha_i\}_{1 \leqq i \leqq \varphi(m)}$ are its integral basis.

Conversely, if some ideal of $Q(\zeta_m)$, say $\mathfrak{a}'$, is given, we can get a $\varphi(m)$-dimensional X-invariant lattice by tracing the above process backward. Therefore we have a correspondence between lattices and ideals of $Q(\zeta_m)$.

Next, we consider how many kinds of lattices exist.

First, we define some equivalence classes of lattices, then we show that number of those equivalence classes is given by the class number of $Q(\zeta_m)$.

We say "two lattices are equivalent," if and only if (considering with proper basis) they have same transformation matrix A. Clearly this defines equivalence classes. Let us consider how many these equivalence classes exist.

In the process of obtaining lattices from ideals of $Q(\zeta_m)$, we have to choose some integral basis of $\mathfrak{a}'$, say $\{\alpha_i'\}_{1\leqq i\leqq\varphi(m)}$. Suppose we choose another integral basis, say $\{\alpha_i''\}_{1\leqq i\leqq\varphi(m)}$. Let the lattices which we get from these bases be Γ' and Γ'' for each. Since both $\{\alpha_i'\}_{1\leqq i\leqq\varphi(m)}$ and $\{\alpha_i''\}_{1\leqq i\leqq\varphi(m)}$ are integral bases of $\mathfrak{a}'$, there exists some $B(B\in GL(\varphi(m),Z))$ which satisfies

$$(\alpha_1'',\dots,\alpha_{\varphi(m)}'')=(\alpha_1',\dots,\alpha_{\varphi(m)}')B.$$

Remembering the above correspondence between lattices and ideals, this relation implies that Γ' and Γ'' are equivalent. Therefore, all lattices which are got from one ideal, belong to one equivalence class. Let us denote the equivalence class which we get from an ideal $\mathfrak{a}$ as $\Gamma(\mathfrak{a})$.

Here it can be shown as follows that "$\Gamma(\mathfrak{a})=\Gamma(\mathfrak{b})\Leftrightarrow\mathfrak{b}/\mathfrak{a}$ is a principal ideal."

Suppose for some two ideals $\mathfrak{a}$ and $\mathfrak{b}$ that $\Gamma(\mathfrak{a})=\Gamma(\mathfrak{b})$ is satisfied. This means these two lattices have some transformation matrix A. Therefore, remembering that all eigenspaces of A are 1-dimensional spaces, we get the following. Let some integral basis of $\mathfrak{a}$ be $\{\alpha_i\}_{1\leqq i\leqq\varphi(m)}$ and some integral basis of $\mathfrak{b}$ be $\{\beta_i\}_{1\leqq i\leqq\varphi(m)}$. Then there exists some $\xi\in Q(\zeta_m)$ which satisfies

$$(\beta_1,\dots,\beta_{\varphi(m)})=\xi(\alpha_1,\dots,\alpha_{\varphi(m)}).$$

This means $\mathfrak{b}=(\xi)\mathfrak{a}$, where (ξ) is the principal ideal generated by ξ.

Conversely, suppose for two ideals $\mathfrak{a}$ and $\mathfrak{b}$ that $\mathfrak{b}=(\xi)\mathfrak{a}$ is satisfied ((ξ) is the principal ideal generated by ξ). This means the following. Let some integral basis of $\mathfrak{a}$ be $\{\alpha_i\}_{1\leqq i\leqq\varphi(m)}$. Then, we can take $\{\xi\alpha_i\}_{1\leqq i\leqq\varphi(m)}$ as an integral basis of $\mathfrak{b}$. This implies $\Gamma(\mathfrak{a})$ and $\Gamma(\mathfrak{b})$ have some transformation matrix. Therefore $\Gamma(\mathfrak{a})=\Gamma(\mathfrak{b})$ is satisfied.

Hence there is one-to-one correspondence between equivalence classes of lattices and ideal classes of $Q(\zeta_m)$. Therefore the number of equivalence classes of lattices is given by the class number of $Q(\zeta_m)$, which we denote as h_m. It is known from number theory that for all m, h_m is finite.

3.2. General Lattices. Next let us consider general cases, $n\geqq 2$. In these cases, we show in this subsection that Γ is embedded in a direct sum of minimal lattices, which we considered in Sect. 3.1.

Let some basis of Γ be $\{\gamma_j\}_{1\leqq j\leqq d}$. Take an arbitrary non-zero vector of Γ, say γ. For all j $(j\geqq 0)$, it is satisfied that $X^j\gamma\in\Gamma$. Here it can be shown that $\{X^j\gamma\}_{0\leqq j\leqq\varphi(m)-1}$ are linearly independent.

Remembering that $\Phi_m(X)=0$, and that $\Phi_m(x)\in Z[x]$, there exist some integers $\{n_i\}_{0\leqq i\leqq\varphi(m)-1}$ which satisfy

$$X^{\varphi(m)}\gamma=\sum_{i=0}^{\varphi(m)-1}n_i(X^i\gamma).$$

Therefore the $\varphi(m)$-dimensional subspace spanned by $\{X^j\gamma\}_{0\leqq j\leqq\varphi(m)-1}$ is an X-invariant subspace. Let us call this subspace V_1'. Then $\Gamma_1'\overset{\text{def}}{=}\Gamma\cap V_1'$ is a $\varphi(m)$-dimensional X-invariant sublattice of Γ. Let some basis of Γ_1' be $\{\gamma_{1j}'\}_{1\leqq j\leqq\varphi(m)}$.

Next, we take an arbitrary vector γ' which satisfies $\gamma'\in\Gamma$, $\gamma'\notin V_1'$, and with γ', make V'_2 and Γ'_2 as we did above, and let some basis of Γ'_2 be $\{\gamma'_{2j}\}_{1\leqq j\leqq\varphi(m)}$. Again it can be shown that $2\varphi(m)$-vectors $\{\gamma'_{1j},\gamma'_{2j}\}_{1\leqq j\leqq\varphi(m)}$ are linearly independent.

Next, we take an arbitrary vector γ'' which satisfies $\gamma''\in\Gamma$, $\gamma''\notin V'_1\oplus V'_2$ ("$\oplus$" means "direct sum"), and make V'_3 and Γ'_3 as we did above. We repeat this process again and again.

Finally, we get $\{\Gamma'_j\}_{1\leqq j\leqq n}$. For all j,Γ'_j is a $\varphi(m)$-dimensional X-invariant sublattice contained in V'_j, and $\Gamma'_1\oplus\cdots\oplus\Gamma'_n$ is a d-dimensional X-invariant sublattice of Γ. Let some basis of Γ'_j be $\{\gamma'_{ji}\}_{1\leqq i\leqq\varphi(m)}$ for $1\leqq j\leqq n$. Then some matrix M ($M\in M_d(Z)$, $\det M\neq 0$) exists, which satisfies

$$(\gamma'_{11},\dots,\gamma'_{1\varphi(m)};\dots;\gamma'_{n1},\dots,\gamma'_{n\varphi(m)})=(\gamma_1,\dots,\gamma_d)M.$$

Thus we obtain the following.

$$(\gamma_1,\dots,\gamma_d)=(\gamma''_{11},\dots,\gamma''_{1\varphi(m)};\dots;\gamma''_{n1},\dots,\gamma''_{n\varphi(m)})(\det M\cdot M^{-1}),$$

where

$$\gamma''_{ji}=\frac{\gamma'_{ji}}{\det M}\quad(1\leqq j\leqq n,1\leqq i\leqq\varphi(m)).$$

Since $\det M\cdot M^{-1}\in M_d(Z)$, this means that Γ is a d-dimensional sublattice of $\Gamma''_1\oplus\cdots\oplus\Gamma''_n$. Here for all $j,\Gamma''_j=\Gamma'_j/\det M$, which is a $\varphi(m)$-dimensional X-invariant lattice, and $\Gamma''_j\subset V'_j$.

Now let us transform Γ, X and A to forms easy to handle. We define sublattices $\Gamma^{(j)}$ $(1\leqq j\leqq n)$ as follows:

$$\Gamma^{(j)}\overset{\text{def}}{=}\Gamma\cap(V'_1\oplus\cdots\oplus V'_j).$$

Especially $\Gamma^{(1)}=\Gamma'_1,\Gamma^{(n)}=\Gamma$, and they satisfy $\Gamma^{(1)}\subset\Gamma^{(2)}\subset\cdots\subset\Gamma^{(n)}$. For all j, since V'_j is an X-invariant subspace of R^d, $\Gamma^{(j)}$ is a $j\cdot\varphi(m)$-dimensional, X-invariant sublattice of Γ.

Let some basis of $\Gamma^{(1)}$ be $\{\gamma^j\}_{1\leqq j\leqq\varphi(m)}$. By completing these, let some basis of $\Gamma^{(2)}$ be $\{\gamma^j\}_{1\leqq j\leqq 2\varphi(m)}$, and so on.

Finally, we get $\{\gamma^j\}_{1\leqq j\leqq n\cdot\varphi(m)=d}$ as a basis of $\Gamma^{(n)}=\Gamma$.

Let us denote the matrix whose j^{th} column vector is γ^j $(1\leqq j\leqq d)$ also as Γ. Then, there exists some A ($A\in GL(d,Z)$) which satisfies $X\Gamma=\Gamma A$. Since for all j, $\{\gamma^i\}_{1\leqq i\leqq j\cdot\varphi(m)}$ are bases of an X-invariant sublattice $\Gamma^{(j)}, A$ is a matrix of form

$$A=\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n}\\ & A_{22} & \cdots & A_{2n}\\ & & \ddots & \vdots\\ & & & A_{nn}\end{pmatrix}$$

(where for all i,j,A_{ij} is a $\varphi(m)\times\varphi(m)$-matrix).

Now, let us take $\{\gamma''_{ij}\}_{1\leqq i\leqq n,1\leqq j\leqq\varphi(m)}$ as a basis of R^d. Since Γ is a sublattice of $(\Gamma''_1\oplus\cdots\oplus\Gamma''_n)$, with this basis, $\Gamma\in M_d(Z)$, and by definition of $\{\gamma^j\}_{1\leqq j\leqq d},\Gamma$ is a matrix of form

$$\Gamma = \begin{pmatrix} \Gamma_{11} & \Gamma_{12} & \cdots & \Gamma_{1n} \\ & \Gamma_{22} & \cdots & \Gamma_{2n} \\ & & \ddots & \vdots \\ & & & \Gamma_{nn} \end{pmatrix}$$

(where for all i, j, Γ_{ij} is a $\varphi(m) \times \varphi(m)$-matrix).

Since Γ''_j $(1 \leqq j \leqq n)$ are X-invariant lattices, X is a matrix of form

$$X = \begin{pmatrix} X_{11} & & & \\ & X_{22} & & \\ & & \ddots & \\ & & & X_{nn} \end{pmatrix}$$

(where for all j, X_{jj} is a $\varphi(m) \times \varphi(m)$-matrix).

Next let us consider if we can eliminate off diagonal blocks of A, i.e., if Γ is a direct sum of Γ''_j $(1 \leqq j \leqq n)$. For general cases, we cannot answer this question. But for special cases, $h_m = 1$, we show in the following that the answer for this question is *yes*. (Notice that for all n which satisfies $\varphi(n) \leqq 22$, it is satisfied that $h_n = 1$, except for $n = 23, 46$. For these values of $n, \varphi(23) = \varphi(46) = 22$, and $h_{23} = h_{46} = 3$ [12].)

In these cases, since all ideals of $Q(\zeta_m)$ are principal ideals, say (ξ), we can take $\{\xi(\zeta_m)^j\}_{0 \leqq j \leqq \varphi(m)-1}$ as an integral basis of it. Therefore we can take some basis of Γ with which

$$X_{jj} = A_{jj} = Y \quad (1 \leqq j \leqq n).$$

Here

$$Y = \begin{pmatrix} 0 & \cdots & 0 & -\delta_0 \\ 1 & & & -\delta_1 \\ & \ddots & & \vdots \\ & & 1 & -\delta_{\varphi(m)-1} \end{pmatrix},$$

where δ_j $(0 \leqq j \leqq \varphi(m) - 1)$ are defined by

$$\Phi_m(x) = x^{\varphi(m)} + \sum_{j=0}^{\varphi(m)-1} \delta_j x^j.$$

From the relation $X\Gamma = \Gamma A$, we get

$$Y\Gamma_{11} = \Gamma_{11} Y, \tag{3.1}$$

$$Y\Gamma_{12} = \Gamma_{11} A_{12} + \Gamma_{12} Y. \tag{3.2}$$

Now let us change the basis of this $\varphi(m)$-dimensional space so that with this basis, the first row vector of Γ_{11} is $(1, \zeta_m, (\zeta_m)^2, \ldots, (\zeta_m)^{\varphi(m-1)-1})$ and others of Γ_{11} are obtained from this by $G(Q(\zeta_m)/Q)$-transformations. Let us also denote the matrix which represents this transformation as B. This B satisfies

$$B^{-1}YB=\begin{pmatrix} e^{i\theta_1} & & & \\ & \cdot & & \\ & & \cdot & \\ & & & e^{i\theta_{\varphi(m)}} \end{pmatrix}.$$

Then from (3.2), we get

$$(B^{-1}YB)(B^{-1}\Gamma_{12})=(B^{-1}\Gamma_{11})A_{12}+(B^{-1}\Gamma_{12})Y.$$

Let the first row vector of $B^{-1}\Gamma_{12}$ be $(\alpha_1,\dots,\alpha_{\varphi(m)})$. Then we get

$$\zeta_m(\alpha_1,\dots,\alpha_{\varphi(m)})=(1,\zeta_m,\dots,(\zeta_m)^{\varphi(m-1)-1})A_{12}+(\alpha_1,\dots,\alpha_{\varphi(m)})Y. \tag{3.3}$$

Notice that the following relation is satisfied:

$$\zeta_m(\alpha_1,\alpha_1\zeta_m,\dots,\alpha_1(\zeta_m)^{\varphi(m)-1})=(\alpha_1,\alpha_1\zeta_m,\dots,\alpha_1(\zeta_m)^{\varphi(m)-1})Y. \tag{3.4}$$

Therefore, if we write

$$(\alpha_1,\dots,\alpha_{\varphi(m)})-(\alpha_1,\alpha_1\zeta_m,\dots,\alpha_1(\zeta_m)^{\varphi(m)-1})=(0,\beta_2,\dots,\beta_{\varphi(m)}),$$

then from (3.3) and (3.4), we get

$$\zeta_m(0,\beta_2,\dots,\beta_{\varphi(m)})=(1,\zeta_m,\dots,(\zeta_m)^{\varphi(m)-1})A_{12}+(0,\beta_2,\dots,\beta_{\varphi(m)})Y. \tag{3.5}$$

By using the explicit form of Y, this relation is written as

$$(0,\zeta_m\beta_2,\dots,\zeta_m\beta_{\varphi(m)})=(\xi_1,\dots,\xi_{\varphi(m)})+\left(\beta_2,\dots,\beta_{\varphi(m)}-\sum_{i=1}^{\varphi(m)-1}\delta_i\beta_{i+1}\right),$$

with $(\xi_1,\dots,\xi_{\varphi(m)})=(1,\zeta_m,\dots,(\zeta_m)^{\varphi(m)-1})A_{12}$. Notice $\xi_j\in\mathfrak{o}_m$ $(1\leqq j\leqq\varphi(m))$, since $A_{12}\in M_{\varphi(m)}(Z)$.

Then by comparing the first component of both-hand sides, we get $\beta_2\in\mathfrak{o}_m$, then by comparing the second component of both-hand sides, we get $\beta_3\in\mathfrak{o}_m$, and so on.

Finally, we get $\beta_j\in\mathfrak{o}_m$ $(|\leqq j\leqq\varphi(m))$. Therefore there exists some integral matrix Z_{12} which satisfies

$$(0,\beta_2,\dots,\beta_{\varphi(m)})=(1,\zeta_m,\dots,(\zeta_m)^{\varphi(m)-1})Z_{12}. \tag{3.6}$$

Now let us define a matrix B' as follows. The row first vector of B' is $(0,\beta_2,\dots,\beta_{\varphi(m)})$, and others of B' are got from this by $G(Q(\zeta_m)/Q)$-transformations. Then from (3.6), we get

$$B'=(B^{-1}\Gamma_{11})Z_{12}, \tag{3.7}$$

and from (3.5), we have

$$(B^{-1}U\,B)B'=(B^{-1}\Gamma_{11})A_{12}+B'Y.$$

Then, using (3.7), we get

$$B^{-1}Y\Gamma_{11}Z_{12}=B^{-1}\Gamma_{11}A_{12}+B^{-1}\Gamma_{11}Z_{12}Y.$$

Finally, using (3.1), we obtain

$$YZ_{12}=A_{12}+Z_{12}Y. \tag{3.8}$$

Now, let us change the basis of Γ by the following $GL(d,Z)$ transformation

$$C=\begin{pmatrix} I-Z_{12} & & & \\ & I & & \\ & & I & \\ & & & \ddots \end{pmatrix}.$$

Then, A is transformed to

$$C^{-1}AC=\begin{pmatrix} Y & A_{12}+Z_{12}Y-YZ_{12} & \cdots & \cdots \\ & Y & \cdots & \cdots \\ & & Y & \cdots \\ & & & \ddots \end{pmatrix}=\begin{pmatrix} Y & O & \cdots & \cdots \\ & Y & \cdots & \cdots \\ & & Y & \cdots \\ & & & \ddots \end{pmatrix}.$$

(At the last step we used (3.8).) Therefore we can eliminate A_{12}.

Now, this form of A means that $\Gamma^{(2)}$ is a direct sum of two $\varphi(m)$-dimensional X-invariant lattices. Therefore we lose no generality if we suppose $\{\gamma^j\}_{\varphi(m)<j\leqq 2\varphi(m)}$ are contained in Γ_2'', i,e., $\Gamma_{12}=O$. Then the relation $X\Gamma=\Gamma A$ becomes as follows:

$$\begin{pmatrix} Y & & \\ & \ddots & \\ & & Y \end{pmatrix}\begin{pmatrix} \Gamma_{11} & O & \Gamma_{13} & \cdots \\ & \Gamma_{22} & \Gamma_{23} & \cdots \\ & & \Gamma_{33} & \cdots \\ & & & \ddots \end{pmatrix}=\begin{pmatrix} \Gamma_{11} & O & \Gamma_{13} & \cdots \\ & \Gamma_{22} & \Gamma_{23} & \cdots \\ & & \Gamma_{33} & \cdots \\ & & & \ddots \end{pmatrix}\begin{pmatrix} Y & O & A_{13} & \cdots \\ & Y & A_{23} & \cdots \\ & & Y & \cdots \\ & & & \ddots \end{pmatrix}.$$

From this relation, we get

$$Y\Gamma_{11}=\Gamma_{11}Y,\quad Y\Gamma_{13}=\Gamma_{11}A_{13}+\Gamma_{13}Y,$$
$$Y\Gamma_{22}=\Gamma_{22}Y,\quad Y\Gamma_{23}=\Gamma_{22}A_{23}+\Gamma_{23}Y.$$

Therefore, repeating the same process as we did above, we can eliminate A_{13}, A_{23}, Γ_{13}, Γ_{23}.

Repeating this process again and again, finally we obtain the following form of A and Γ:

$$A=\begin{pmatrix} Y & & \\ & \ddots & \\ & & Y \end{pmatrix},\quad \Gamma=\begin{pmatrix} \Gamma_{11} & & \\ & \ddots & \\ & & \Gamma_{nn} \end{pmatrix}.$$

Therefore we can eliminate off diagonal blocks of A, i.e., Γ is a direct sum of n-sublattices, each of which is a $\varphi(m)$-dimensional, X-invariant lattices.

4. General Lattices

Let us consider again the result of Sect. 2. In this section we suppose that $h_{m_j}=1$ for all j.

First, let us transform Γ, X and A to forms easy to handle. Let some basis of Γ' be $\{\gamma_i'\}_{1\leqq i\leqq n}$, and take these vectors as the basis of R^n. Then X has a form of

(2.1), where for all j, $X_j \in GL(d_j, Z)$, and all elements of vectors which are contained in Γ are integers. Let some basis of Γ be $\{\lambda^{(i)}\}_{1\leqq i\leqq n}$, which satisfies that for all j, $\{\lambda^{(i)}\}_{1\leqq i\leqq \sum_{i=1}^{j} d_l}$ are a basis of $\Gamma \cap (V_1 \oplus \cdots \oplus V_j)$, and let us denote the matrix whose ith column vector is $\lambda^{(i)} (1 \leqq i \leqq n)$ also as Γ. Then there exists some integral matrix A which satisfies $X\Gamma = \Gamma A$. Here

$$\Gamma = \begin{pmatrix} \Gamma_{11} & \Gamma_{12} & \cdots & \Gamma_{1k} \\ & \Gamma_{22} & \cdots & \Gamma_{2k} \\ & & \ddots & \vdots \\ & & & \Gamma_{kk} \end{pmatrix}, \quad A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ & A_{22} & \cdots & A_{2k} \\ & & \ddots & \vdots \\ & & & A_{kk} \end{pmatrix},$$

where for all i, j, Γ_{ij} and A_{ij} are $d_i \times d_j$-matrices. (These Γ_{ij}'s and A_{ij}'s have nothing to do with those Sect. 3.2.)

From this relation, we get

$$X_j \Gamma_{jj} = \Gamma_{jj} A_{jj} \quad (1 \leqq j \leqq k).$$

This means that Γ_{jj} is a lattice like Γ_j in Sect. 3.2. Therefore we can assume that for all j

$$X_j = A_{jj} = \begin{pmatrix} Y_j & & \\ & \cdot & \\ & & Y_j \end{pmatrix}, \quad \Gamma_{jj} = \begin{pmatrix} \Gamma_{jj}^{(1)} & & \\ & \cdot & \\ & & \Gamma_{jj}^{(n_j)} \end{pmatrix},$$

where Y_j is defined as Y was done in Sect. 3.2, and let us define for all i, j,

$$\Gamma_{ij} = \begin{pmatrix} \Gamma_{ij}^{(11)} & \cdots & \Gamma_{ij}^{(1n_j)} \\ \vdots & & \vdots \\ \Gamma_{ij}^{(n_i 1)} & \cdots & \Gamma_{ij}^{(n_i n_j)} \end{pmatrix}, \quad A_{ij} = \begin{pmatrix} A_{ij}^{(11)} & \cdots & A_{ij}^{(1n_j)} \\ \vdots & & \vdots \\ A_{ij}^{(n_i 1)} & \cdots & A_{ij}^{(n_i n_j)} \end{pmatrix},$$

where for all i, j, k, l, $\Gamma_{ij}^{(kl)}$ and $A_{ij}^{(kl)}$ are $\varphi(m_i) \times \varphi(m_j)$-matrices.

4.1. Is Γ a Direct Sum of Small Lattices? Let us consider if we can eliminate off diagonal blocks of A, i.e., if Γ is a direct sum of Γ_{jj}'s. As we will see below, it is easier to consider if we can eliminate off diagonal blocks of Γ. Actually, it is not always possible to eliminate them. Let us consider this problem.

From the relation $X\Gamma = \Gamma A$, we get

$$X_1 \Gamma_{12} = \Gamma_{11} A_{12} + \Gamma_{12} A_{22}.$$

And the ith row $(1 \leqq i \leqq \varphi(m_1))$ and the jth column $(1 \leqq j \leqq \varphi(m_2))$ of this equation mean

$$Y_1 \Gamma_{12}^{(11)} = \Gamma_{11}^{(1)} A_{12}^{(11)} + \Gamma_{12}^{(11)} Y_2. \tag{4.1}$$

Let us change basis of this $\varphi(m_1)$-dimensional space so that with this basis, the first row vector of $\Gamma_{11}^{(1)}$ is $(1, \zeta_{m_1}, \ldots, (\zeta_{m_1})^{\varphi(m_1)-1})$, and others of $\Gamma_{11}^{(1)}$ are obtained from this by $G(Q(\zeta_{m_1})/Q)$-transformations. Let us denote the matrix which represent this transformation as $B_1^{(1)}$. This $B_1^{(1)}$ satisfies

$$B_1^{(1)-1}Y_1B_1^{(1)} = \begin{pmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_{\varphi(m_1)}} \end{pmatrix} \quad (e^{i\theta_1} = \zeta_{m_1}),$$

then from (4.1), we have

$$(B_1^{(1)-1}Y_1B_1^{(1)})(B_1^{(1)-1}\Gamma_{12}^{(11)}) = (B_1^{(1)-1}\Gamma_{11}^{(1)})A_{12}^{(11)} + (B_1^{(1)-1} - \Gamma_{12}^{(11)})Y_2. \tag{4.2}$$

Let us denote the jth row vector of $B_1^{(1)-1}\Gamma_{12}^{(11)}$ as $(\alpha_1^{(j)}, \dots, \alpha_{\varphi(m_1)}^{(j)})$. Then from (4.2), we get for all j,

$$\begin{aligned} e^{i\theta_j}(\alpha_1^{(j)}, \dots, \alpha_{\varphi(m_1)}^{(j)}) &= (1, g_j(\zeta_{m_1}), \dots, g_j((\zeta_{m_1})^{\varphi(m_1)-1}))A_{12}^{(11)} \\ &\quad + (\alpha_1^{(j)}, \dots, \alpha_{\varphi(m_1)}^{(j)})Y_2, \end{aligned} \tag{4.3}$$

where $g_j \in G(Q(\zeta_{m_1})/Q)$, which satisfies $g_j(\zeta_{m_1}) = e^{i\theta_j}$.

Therefore

$$\begin{aligned} (\alpha_1^{(j)}, \dots, \alpha_{\varphi(m_1)}^{(j)}) &= (1, g_j(\zeta_{m_1}), \dots, g_j((\zeta_{m_1})^{\varphi(m_1)-1}))A_{12}^{(11)}(e^{i\theta_j} - Y_2)^{-1} \\ &= g_j\{(1, \zeta_{m_1}, \dots, (\zeta_{m_1})^{\varphi(m_1)-1})A_{12}^{(11)}(e^{i\theta_1} - Y_2)^{-1}\} \\ &= g_j\{(\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_1)}^{(1)})\}. \end{aligned} \tag{4.4}$$

(Notice by the supposition $m_1 \neq m_2$, for all j, $\det(e^{i\theta_j} - Y_2) = \Phi_{m_2}(e^{i\theta_j}) \neq 0$.)

Therefore all we have to do is to consider if we can eliminate the first row vector of $B_1^{(1)-1}\Gamma_{12}^{(11)}$. If we can eliminate A_{12}, (4.4) means $\Gamma_{12} = O$. Therefore, if we cannot eliminate Γ_{12}, we cannot eliminate A_{12} either.

Let us consider the first row vector of $B_1^{(1)-1}\Gamma_{12}^{(11)}$. This is given as

$$(\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_1)}^{(1)}) = (1, \zeta_{m_1}, \dots, (\zeta_{m_1})^{\varphi(m_1)-1})A_{12}^{(11)}(e^{i\theta_1} - Y_2)^{-1}$$

and

$$\det(e^{i\theta_1} - Y_2) = \Phi_{m_2}(\zeta_{m_1}).$$

Therefore two cases can occur.

1. $\Phi_{m_2}(\zeta_{m_1}) \in \mathfrak{o}_{m_1}^{\times}$ ($\mathfrak{o}_{m_1}^{\times}$ is the unit group of $\mathfrak{o}_{m_1}$.)

In this case, $(e^{i\theta_1} - Y_2) \in GL(\varphi(m_1), \mathfrak{o}_{m_1})$. Therefore all elements of $A_{12}^{(11)}(e^{i\theta_1} - Y_2)^{-1}$ are contained in $\mathfrak{o}_{m_1}$. Hence for all j, $\alpha_j^{(1)} \in \mathfrak{o}_{m_1}$. Therefore some integral matrix $Z_{12}^{(11)}$ exists, which satisfies

$$(\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_1)}^{(1)}) = (1, \zeta_{m_1}, \dots, (\zeta_{m_1})^{\varphi(m_1)-1})Z_{12}^{(11)}.$$

This means $B_1^{(1)-1}\Gamma_{12}^{(11)} = B_1^{(1)-1}\Gamma_{11}^{(1)}Z_{12}^{(11)}$, i.e., $\Gamma_{12}^{(11)} = \Gamma_{11}^{(1)}Z_{12}^{(11)}$. Therefore changing the basis of Γ by the following $GL(n, Z)$-transformation,

$$\begin{pmatrix} I & & & -Z_{12}^{(11)} & \\ & \ddots & & O & \\ & & \ddots & \vdots & \\ & & I & O & \\ & & & I & \\ & & & & \ddots \end{pmatrix}$$

we can eliminate $\Gamma_{12}^{(11)}$. Similarly we can eliminate all $\Gamma_{12}^{(ij)}$. Therefore we can eliminate Γ_{12}.

2. $\Phi_{m_2}(\zeta_{m_1}) \notin \mathfrak{o}_{m_1}^{\times}$

In this case it is possible that for some j, $\alpha_j^{(1)} \notin \mathfrak{o}_{m_1}$. Then there exists no integral matrix $Z_{12}^{(11)}$ which satisfies

$$(\alpha_1^{(1)}, \ldots, \alpha_{\varphi(m_1)}^{(1)}) = (1, \zeta_{m_1}, \ldots, (\zeta_{m_1})^{\varphi(m_1)-1}) Z_{12}^{(11)}.$$

Therefore we cannot eliminate $\Gamma_{12}^{(11)}$. Hence this time Γ is not a direct sum of small lattices.

Hence Γ is not always a direct sum of small lattices.

As for the problem about if $\Phi_{m_2}(\zeta_{m_1}) \in \mathfrak{o}_{m_1}^{\times}$, refer to Appendix B.

4.2. How Many Kinds of Lattices Exist? As we saw above, we cannot always eliminate off-diagonal blocks of Γ, i.e., Γ is not always a direct sum of small lattices. Next let us consider the number of possibilities for Γ_{ij} $(i<j)$.

First let us consider Γ_{12}. As we saw above, Γ_{12} satisfies the next relation,

$$X_1 \Gamma_{12} = \Gamma_{11} A_{12} + \Gamma_{12} A_{22}.$$

From this relation we get the following:

$$Y_1 \Gamma_{12}^{(11)} = \Gamma_{11}^{(1)} A_{12}^{(11)} + \Gamma_{12}^{(11)} Y_2.$$

Notice that by the same consideration as we did in Sect. 4.1 case (1), we can always change all column vectors of $\Gamma_{12}^{(11)}$ by arbitrary vectors contained in a lattice spanned by column vectors of $\Gamma_{11}^{(1)}$. Therefore we must consider all column vectors of $\Gamma_{12}^{(11)}$ by mod $\Gamma_{11}^{(1)}$, when we count the number of possibilities for $\Gamma_{12}^{(11)}$. With the basis we used in Sect. 4.1, this means that we must consider $\alpha_j^{(1)}$ $(1 \leqq j \leqq \varphi(m_2))$ by mod $\mathfrak{o}_{m_1}$. Writing (4.3) (with $j=1$) again, we have

$$\zeta_{m_1}(\alpha_1^{(1)}, \ldots, \alpha_{\varphi(m_2)}^{(1)}) = (1, \zeta_{m_1}, \ldots, (\zeta_{m_1})^{\varphi(m_1)-1}) A_{12}^{(11)} + (\alpha_1^{(1)}, \ldots, \alpha_{\varphi(m_2)}^{(1)}) Y_2. \quad (4.5)$$

Using the explicit form of Y_2, which is given in Sect. 3.2, we get

$$\zeta_{m_1}(\alpha_1^{(1)}, \ldots, \alpha_{\varphi(m_2)}^{(1)}) \equiv (\alpha_2^{(1)}, \ldots, \alpha_{\varphi(m_2)}^{(1)}, -\sum_{i=0}^{\varphi(m_2)-1} \delta_i \alpha_{i+1}^{(1)}) \pmod{\mathfrak{o}_{m_1}}.$$

From this relation, we have

$$\zeta_{m_1} \alpha_j^{(1)} \equiv \alpha_{j+1}^{(1)} \pmod{\mathfrak{o}_{m_1}} (1 \leqq j \leqq \varphi(m_2)-1), \quad (4.6)$$

$$\zeta_{m_1} \alpha_{\varphi(m_2)}^{(1)} \equiv -\sum_{i=0}^{\varphi(m_2)-1} \delta_i \alpha_{i+1}^{(1)} \pmod{\mathfrak{o}_{m_1}}. \quad (4.7)$$

From (4.6), we obtain

$$\alpha_j^{(1)} \equiv (\zeta_{m_1})^{j-1} \alpha_1^{(1)} \pmod{\mathfrak{o}_{m_1}} (2 \leqq j \leqq \varphi(m_2)). \quad (4.8)$$

Then from (4.7) and (4.8), we obtain

$$\Phi_{m_2}(\zeta_{m_1}) \alpha_1^{(1)} \equiv 0 \pmod{\mathfrak{o}_{m_1}}. \quad (4.9)$$

Since we must consider $\alpha_j^{(1)}$ $(1 \leqq j \leqq \varphi(m_2))$ by mod $\mathfrak{o}_{m_1}$, (4.8) means that all $\alpha_j^{(1)}$ $(2 \leqq j \leqq \varphi(m_2))$ are determined if we choose $\alpha_1^{(1)}$. Therefore what we have to do is to count the number of possibilities for $\alpha_1^{(1)}$ by mod $\mathfrak{o}_{m_1}$.

First, $\alpha_1^{(1)}$ must satisfy (4.9). Conversely, suppose that some $\alpha_1^{(1)}$ which satisfies (4.9) is given. Then if we choose $\alpha_j^{(1)}$ $(2 \leqq j \leqq \varphi(m_2))$ to satisfy (4.8), all elements of next vector are contained in $\mathfrak{o}_{m_1}$,

$$\zeta_{m_1}(\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_2)}^{(1)}) - (\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_2)}^{(1)})Y_2.$$

Therefore some integral matrix $A_{12}^{(11)}$ exists, which satisfies

$$\zeta_{m_1}(\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_2)}^{(1)}) - (\alpha_1^{(1)}, \dots, \alpha_{\varphi(m_2)}^{(1)})Y_2 = (1, \zeta_{m_1}, \dots, (\zeta_{m_1})^{\varphi(m_1)-1})A_{12}^{(11)}. \quad (4.10)$$

This implies that (4.5) is satisfied. Therefore the number of possibilities for $\Gamma_{12}^{(11)}$ is given by that of $\alpha_1^{(1)}$ which satisfies (4.9), and it is known from number theory that this number is given by $|N_{m_1}\Phi_{m_2}(\zeta_{m_1})|$. (Here "$N_{m_1}$" means "norm considered in $Q(\zeta_{m_1})$".)

Similarly, for all i, j, the number of possibilities for $\Gamma_{12}^{(ij)}$ is given by $|N_{m_1}\Phi_{m_2}(\zeta_{m_1})|$. Hence the number of possibilities for Γ_{12} is given by $|N_{m_1}\Phi_{m_2}(\zeta_{m_1})|^{n_1 n_2}$. Notice that if Γ_{12} is given, A_{12} is determined by (4.10).

Similarly, the number of possibilities for $\Gamma_{j,j+1}$ is given by $|N_{m_{j+1}}(\zeta_{m_j})|^{n_j n_{j+1}}$, and if $\Gamma_{j,j+1}$ is given, $A_{j,j+1}$ is determined.

Next let us consider the number of possibilities for Γ_{13}, assuming that $\Gamma_{j,j+1}$ $(1 \leqq j \leqq k-1)$ are given. Notice, since we assume $\Gamma_{j,j+1}$ $(1 \leqq j \leqq k-1)$ are given, $A_{j,j+1}$ $(1 \leqq j \leqq k-1)$ are also given. Also in this case, we obtain a similar result in the following.

As we saw above, Γ_{13} satisfies next relation,

$$X_1\Gamma_{13} = \Gamma_{11}A_{13} + \Gamma_{12}A_{23} + \Gamma_{13}A_{33}.$$

From this relation we get the followings.

$$Y_1\Gamma_{13}^{(11)} = \Gamma_{11}^{(1)}A_{13}^{(11)} + \sum_{i=1}^{n_2} \Gamma_{12}^{(1i)}A_{23}^{(i1)} + \Gamma_{13}^{(11)}Y_3.$$

This time, we can change all column vectors of $\Gamma_{13}^{(11)}$ by arbitrary vectors contained in a lattice spanned by column vectors of $\Gamma_{11}^{(1)}$ and $\Gamma_{12}^{(1i)}$ $(1 \leqq i \leqq n_2)$. This is performed by the next $GL(n, Z)$ matrix

$$\begin{pmatrix}
I & & & & & & Z_{13}^{(11)} & \\
 & \ddots & & & & & O & \\
 & & \ddots & & & & \vdots & \\
 & & & \ddots & & & O & \\
 & & & & \ddots & & Z_{23}^{(11)} & \\
 & & & & & \ddots & \vdots & \\
 & & & & & I & Z_{23}^{(n_2 1)} & \\
 & & & & & & I & \\
 & & & & & & & \ddots
\end{pmatrix}$$

But, unless $Z_{23}^{(ij)} = 0$ $(\forall i, \forall j)$, this basis transformation also changes Γ_{23}. Therefore if we want to leave Γ_{23} unchanged, we must consider only the case $Z_{23}^{(ij)} = 0$ $(\forall i, \forall j)$.

This means that we can change column vectors of $\Gamma_{23}^{(11)}$ only by arbitrary vectors contained in a lattice spanned by column vectors of $\Gamma_{11}^{(1)}$.

Let $B_1^{(1)}$ be the same matrix as we used in Sect. 4.1. Denoting the first row vector of $B_1^{(1)-1}\Gamma_{13}^{(11)}$ as $(\beta_1,\dots,\beta_{\varphi(m_3)})$, and the first row vector of $B_1^{(1)-1}\sum_{i=1}^{n_2}\Gamma_{12}^{(1i)}A_{23}^{(i1)}$ as $(-\xi_1,\dots,-\xi_{\varphi(m_3)})$, we get the following relation:

$$\begin{aligned}\zeta_{m_1}(\beta_1,\dots,\beta_{\varphi(m_3)})&=(1,\zeta_{m_1},\dots,(\zeta_{m_1})^{\varphi(m_1)-1})A_{13}^{(11)}\\&\quad-(\xi_1,\dots,\xi_{\varphi(m_3)})+(\beta_1,\dots,\beta_{\varphi(m_3)})Y_3.\end{aligned}\tag{4.11}$$

Since we assumed that $\Gamma_{j,j+1}$ and $A_{j,j+1}$ $(1\leqq j\leqq k-1)$ are given, ξ_i $(1\leqq i\leqq\varphi(m_3))$ are known numbers. With this basis, we must consider β_i $(1\leqq i\leqq\varphi(m_3))$ by mod $\mathfrak{o}_{m_1}$.

Using the explicit form of Y_3, we have the following relations:

$$\zeta_{m_1}\beta_j\equiv-\xi_j+\beta_{j+1}\quad(\operatorname{mod}\mathfrak{o}_{m_1})(1\leqq j\leqq\varphi(m_3)-1),\tag{4.12}$$

$$\zeta_{m_1}\beta_{\varphi(m_3)}\equiv-\xi_{\varphi(m_3)}-\sum_{i=0}^{\varphi(m_3)-1}\delta_i\beta_{i+1}\quad(\operatorname{mod}\mathfrak{o}_{m_1}).\tag{4.13}$$

From (4.12), we obtain

$$\beta_j=(\zeta_{m_1})^{j-1}\beta_1+\eta_{j-1}\quad(\operatorname{mod}\mathfrak{o}_{m_1})(2\leqq j\leqq\varphi(m_3)),\tag{4.14}$$

where $\eta_l=\sum_{j=0}^{l-1}(\zeta_{m_1})^j\xi_{l-j}$ $(1\leqq l\leqq\varphi(m_3)-1)$. (Notice that since ξ_i $(1\leqq i\leqq\varphi(m_3))$ are known, η_i $(1\leqq i\leqq\varphi(m_3)-1)$ are also known.)

From (4.13) and (4.14), we obtain

$$\Phi_{m_3}(\zeta_{m_1})\beta_1\equiv\eta_0\quad(\operatorname{mod}\mathfrak{o}_{m_1}),\tag{4.15}$$

where $\eta_0=-\xi_{\varphi(m_3)}-\zeta_{m_1}\eta_{\varphi(m_3)-1}-\sum_{i=1}^{\varphi(m_3)-1}\delta_i\eta_i$. (Notice that η_0 is also a known number.)

Since we must consider β_i $(1\leqq i\leqq\varphi(m_3))$ by mod $\mathfrak{o}_{m_1}$, (4.14) means that β_i $(2\leqq i\leqq\varphi(m_3))$ are determined, if we choose β_1. Therefore what we have to do is to count the number of possibilities for β_1 by mod $\mathfrak{o}_{m_1}$. By the same consideration as we did above, this number is given by $|N_{m_1}\Phi_{m_3}(\zeta_{m_1})|$, and β_1 is given by (4.15). Therefore the number of possibilities for $\Gamma_{13}^{(11)}$ is given by $|N_{m_1}\Phi_{m_3}(\zeta_{m_1})|$.

By the same consideration as we did above, the number of possibilities for Γ_{13} is given by $|N_{m_1}\Phi_{m_3}(\zeta_{m_1})|^{n_1n_3}$. If Γ_{13} is given, A_{13} is determined by (4.11).

Repeating this consideration again and again, the number of possibilities for Γ_{jl} $(j<l)$ is given by $|N_{m_j}\Phi_{m_l}(\zeta_{m_j})|^{n_jn_l}$. And if Γ_{jl} is given, A_{jl} is determined.

As for $N_{m_j}\Phi_{m_l}(\zeta_{m_j})$, refer to Appendix C.

5. Conclusion

We have studied n-dimensional lattices which have Z_m symmetries. We have seen that such lattices are embedded in an orthogonal sum of some smaller lattices, each of which is a lattice whose automorphism transformation has the primitive m_jth roots of 1 only as its eigenvalues. Such smaller lattices are direct sums of minimal lattices. Minimal lattices can be considered as some (fractional) ideals of some cyclotomic field, and the number of different minimal lattices are given by the class number of that cyclotomic field.

Furthermore, we have studied how general lattices are embedded in the orthogonal sum of smaller lattices. We have seen that how many kinds of lattices exist can be calculated by a norm of some integer of some cyclotomic field.

For 6-dimensional lattices, which are relevant to superstring compactification problems we give the number of different lattices, their symmetries and eigenvalues of their automorphism transformations in Tables 1, 2 and 3. For example, the lattice for the Z_3-orbifold of [1, 5, 6] belongs to the type (3^3) and the lattice for the Z_7-orbifold of [7] belongs to the type (7^1).

What we have done in this paper is not a classification or orbifold models, but a classification of lattices. Therefore we have considered nothing from phenomenological viewpoints. So what we would like to do next is to consider phenomenological problems. In this paper, we have considered lattices with Z_m

Table 1. Number of 6-dimensional Lattices

Z_m	Type[a]	Number of Lattices
Z_{30}	$(10^1, 6^1)$	1
	$(10^1, 3^1)$	1
	$(5^1, 6^1)$	1
Z_{24}	$(8^1, 6^1)$	1
	$(8^1, 3^1)$	1
Z_{20}	$(10^1, 4^1)$	1
	$(5^1, 4^1)$	1
Z_{18}	(18^1)	1
Z_{15}	$(5^1, 3^1)$	1
Z_{14}	(14^1)	1
Z_{12}	$(12^1, 6^1)$	4
	$(12^1, 4^1)$	9
	$(12^1, 3^1)$	4
	$(12^1, 2^1, 1^1)$	2
	$(12^1, 2^2)$	1
	$(12^1, 1^2)$	1
	$(6^2, 4^1)$	1
	$(6^1, 4^2)$	1
	$(6^1, 4^1, 3^1)$	4
	$(6^1, 4^1, 2^2)$	$3^2 \cdot 2^2$
	$(6^1, 4^1, 2^1, 1^1)$	$3 \cdot 2 \cdot 2 \cdot 2$
	$(6^1, 4^1, 1^2)$	2^2
	$(4^2, 3^1)$	1
	$(4^1, 3^2)$	1
	$(4^1, 3^1, 2^2)$	2^2
	$(4^1, 3^1, 2^1, 1^1)$	$2 \cdot 2 \cdot 3 \cdot 2$
	$(4^1, 3^1, 1^2)$	$2^2 \cdot 3^2$

[a] Type of the lattice implies $(m_1^{n_1}, \ldots, m_k^{n_k})$

Table 2. Number of 6-dimensional Lattices. (cont'd)

Z_m	Type	Number of Lattices
Z_{10}	$(10^1, 2^2)$	5^2
	$(10^1, 2^1, 1^1)$	$5 \cdot 2$
	$(5^1, 2^1, 1^1)$	$5 \cdot 2$
	$(10^1, 1^2)$	1
	$(5^1, 2^2)$	1
Z_9	(9^1)	1
Z_8	$(8^1, 4^1)$	4
	$(8^1, 2^2)$	2^2
	$(8^1, 2^1, 1^1)$	$2 \cdot 2 \cdot 2$
	$(8^1, 1^2)$	2^2
Z_7	(7^1)	1
Z_6	(6^3)	1
	$(6^2, 3^1)$	4^2
	$(6^1, 3^2)$	4^2
	$(6^2, 2^2)$	3^4
	$(6^2, 2^1, 1^1)$	$3^2 \cdot 2$
	$(6^2, 1^2)$	1
	$(6^1, 3^1, 2^2)$	$4 \cdot 3^2$
	$(6^1, 3^1, 2^1, 1^1)$	$4 \cdot 3 \cdot 3 \cdot 2$
	$(6^1, 3^1, 1^2)$	$4 \cdot 3^2$
	$(6^1, 2^4)$	3^4
	$(6^1, 2^3, 1^1)$	$3^3 \cdot 2^3$
	$(6^1, 2^2, 1^2)$	$3^2 \cdot 2^4$
	$(6^1, 2^1, 1^3)$	$3 \cdot 2^3$
	$(6^1, 1^4)$	1
	$(3^2, 2^2)$	1
	$(3^2, 2^1, 1^1)$	$3^2 \cdot 2$
	$(3^1, 2^4)$	1
	$(3^1, 2^3, 1^1)$	$3 \cdot 2^3$
	$(3^1, 2^2, 1^2)$	$3^2 \cdot 2^4$
	$(3^1, 2^1, 1^3)$	$3^3 \cdot 2^3$
Z_5	$(5^1, 1^2)$	5^2

symmetry only. So to consider lattices with general symmetry is one of the remaining problems.

Appendix A. Two Lemmas

In this appendix, we consider two lemmas which we will use in Appendix B and C.

Lemma 1. *Let $\{p\}_{1 \leqq j \leqq l}$ $(l \geqq 1)$ be all different prime numbers, and let y be a primitive m^{th} root of* 1 $(m \neq 1)$. *Then the next relation is satisfied,*

$$\left(m, \prod_{j=1}^{l} p_j\right) = 1 \Rightarrow \Phi_{\prod_{j=1}^{l} p_j}(y) \in \mathfrak{o}^{\times},$$

Table 3. Number of 6-dimensional Lattice. (cont'd)

Z_m	Type	Number of Lattices
Z_4	(4^3)	1
	$(4^2,2^2)$	2^4
	$(4^2,2^1,1^1)$	$2^2{\cdot}2^2{\cdot}2$
	$(4^2,1^2)$	2^4
	$(4^1,2^4)$	2^4
	$(4^1,2^3,1^1)$	$2^3{\cdot}2{\cdot}2^3$
	$(4^1,2^2,1^2)$	$2^2{\cdot}2^2{\cdot}2^4$
	$(4^1,2^1,1^3)$	$2{\cdot}2^3{\cdot}2^3$
	$(4^1,1^4)$	2^4
Z_3	(3^3)	1
	$(3^2,1^2)$	3^4
	$(3^1,1^4)$	3^4
Z_2	(2^6)	1
	$(2^5,1^1)$	2^5
	$(2^4,1^2)$	2^8
	$(2^3,1^3)$	2^9
	$(2^2,1^4)$	2^8
	$(2^1,1^5)$	2^5
Z_1	(1^6)	1

where (a,b) is the greatest common divisor of a and b, and $\mathfrak{o}^\times$ is the unit group of the ring of algebraic integers, which satisfies $\mathfrak{o}^\times \cap Q(\zeta_m) = \mathfrak{o}_m^\times$.

Proof. We prove this by reduction about l.

1. $l=1$.

In this case, $\Phi_{p_1}(y)$ is given as

$$\Phi_{p_1}(y)=\frac{y^{p_1}-1}{y-1}.$$

Now by the supposition $(m,\, p_1)=1$, there exist two integers n_1, n_2 which satisfy $n_1p_1+n_2m=1$, $n_1>0$. Then using $y^m=1$, we get

$$\Phi_{p_1}(y)=\frac{y^{p_1}-1}{y^{n_1p_1+n_2m}-1}=\frac{y^{p_1}-1}{(y^{p_1})^{n_1}-1}=\frac{1}{(y^{p_1})^{n_1-1}+\cdots+y^{p_1}+1}.$$

Since the denominator of the right-hand side is an element of $\mathfrak{o}$($\mathfrak{o}$ is the ring of algebraic integers), we obtain

$$\Phi_{p_1}(y)\in\mathfrak{o}^\times.$$

2. Suppose for $l=k$, $(k\geqq 1)$, the lemma is true.

Let $\{p_j\}_{1\leqq j\leqq k+1}$ be all different prime numbers, and y be a primitive mth root of 1 $(m\neq 1)$, and suppose $\left(m,\, \prod_{j=1}^{k+1} p_j\right)=1$. Then $y^{p_{k+1}}$ is also a primitive mth root of

1. Clearly, $\left(m, \prod_{j=1}^{k} p_j\right) = 1$. Therefore by recduction hypothesis, we have

$$\Phi_{\prod_{j=1}^{k} p_j}(y), \Phi_{\prod_{j=1}^{k} p_j}(y^{p_{k+1}}) \in \mathfrak{o}^{\times}.$$

It is known from number theory that

$$\Phi_{\prod_{j=1}^{k+1} p_j}(y) = \frac{\Phi_{\prod_{j=1}^{k} p_j}(y^{p_{k+1}})}{\Phi_{\prod_{j=1}^{k} p_j}(y)},$$

therefore we obtain

$$\Phi_{\prod_{j=1}^{k+1} p_j}(y) \in \mathfrak{o}^{\times}.$$

Hence the lemma is true for $l = k + 1$. q.e.d.

Lemma 2. *Let ζ_m be a primitive m^{th} root of* 1. *Then*

$$1 - \zeta_m \notin \mathfrak{o}^{\times} \quad (if m = p^f \, (p\!:\! primenumber)),$$
$$1 - \zeta_m \in \mathfrak{o}^{\times} \quad (otherwise).$$

Proof.

1. $m = p^f$. Since

$$\Phi_{p^f}(x) = \prod_{(j,p)=1} (x - (\zeta_m)^j),$$

we get

$$p = \prod_{(j,p)=1} (1 - (\zeta_m)^j)$$

by letting $x = 1$.
(It is known from number theory that

$$\Phi_m(1) = \begin{cases} p & (m = p^f \, (p\text{:prime number})) \\ 1 & (\text{otherwise}) \end{cases} \tag{A.1}$$

is satisfied.)

For an arbitrary j which satisfies $(j, p) = 1$, there exist two integers n_1, n_2 which satisfy $n_ij + n_2m = 1$, $n_1 > 0$. Therefore we get

$$\frac{\zeta_m - 1}{(\zeta_m)^j - 1} = \frac{(\zeta_m)^{n_1 j + n_2 m} - 1}{(\zeta_m)^j - 1} = \frac{((\zeta_m)^j)^{n_1} - 1}{(\zeta_m)^j - 1} = ((\zeta_m)^j)^{n_1 - 1} + \cdots + (\zeta_m)^j + 1 \in \mathfrak{o}.$$

Clearly

$$\frac{(\zeta_m)^j - 1}{\zeta_m - 1} = (\zeta_m)^{j-1} + \cdots + \zeta_m + 1 \in \mathfrak{o}.$$

These relations imply

$$\frac{(\zeta_m)^j - 1}{\zeta_m - 1} \in \mathfrak{o}^\times .$$

Hence

$$p = \xi(1-\zeta_m)^{\varphi(m)} \quad \xi \in \mathfrak{o}^\times .$$

Therefore if $(1-\zeta_m) \in \mathfrak{o}^\times$, this relation means $p \in \mathfrak{o}^\times$. But $p \notin \mathfrak{o}^\times$.
Hence $(1-\zeta_m) \notin \mathfrak{o}^\times$.

2. $m \neq p^f$
Since

$$\Phi_m(x) = \prod_{(j,m)=1} (x - (\zeta_m)^j),$$

we get

$$1 = \prod_{(j,m)=1} (1 - (\zeta_m)^j)$$

by letting x be 1 (see (A.1)).

Notice $\prod_{(j,m)=1, j \neq 1} (1 - (\zeta_m)^j) \in \mathfrak{o}$. Therefore $(1-\zeta_m)^{-1} \in \mathfrak{o}$.
Hence $(1-\zeta_m) \in \mathfrak{o}^\times$. q.e.d.

Appendix B. Condition for $\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times$

Let the factorization of n be $\sum_{j=1}^{g} p_j^{e_j}$. Then it is known from number theory that the next relation is satisfied,

$$\Phi_n(x) = \Phi_{n'}(x^{n/n'}),$$

where $n' = \prod_{j=1}^{g} p_j$. Therefore if we denote $(\zeta_m)^{n/n'} = y$, we get

$$\Phi_n(\zeta_m) = \Phi_{n'}(y).$$

Notice that since n/n' is a natural number, some powers of y are equal to 1. Therefore three cases can occur.

1. $y = 1$. In this case

$$\Phi_n(\zeta_m) = \Phi_{n'}(y) = \begin{cases} p_1 & (g=1) \\ 1 & (g>1) \end{cases}.$$

Hence

$$\Phi_n(\zeta_m) \notin \mathfrak{o}_m^\times \quad (g=1),$$
$$\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times \quad (g>1).$$

2. $y \neq 1$, $y^{n'} = 1$. This time, the order of y is $\prod_{j=1}^{g} p_j^{f_j}$ $(f_j = 0, 1)(1 \leqq j \leqq g)$. We lose no generality if we assume the following:

$$\text{There exists some integer } k \text{ which satisfies } \begin{cases} f_j = 1 & (1 \leqq j \leqq k) \\ f_j = 0 & (\text{otherwise}) \end{cases}$$

(2-1) $k = g$

This means that ζ_m is a primitive nth root of 1. Therefore $\Phi_n(\zeta_m) = 0$, i.e., $\Phi_n(\zeta_m) \notin \mathfrak{o}_m^\times$.

(2-2) $k < g$

It is known from number theory that the next relation is satisfied

$$\Phi_n(\zeta_m) = \Phi_{n'}(y) = \frac{\Phi_*\left(y \prod_{j=1}^{k} p_j\right) \cdot \left\{ \prod_{i<j} \Phi_*(y^{p_1 \cdots [p_i] \cdots [p_j] \cdots p_k}) \right\} \cdots}{\left\{ \prod_{j=1}^{k} \Phi_*(y^{p_1 \cdots [p_j] \cdots p_k}) \right\} \cdots},$$

where $* = \prod_{j=k+1}^{g} p_j$, and "[ ]" means to eliminate that prime number from the product.

In the right hand side, every factor except $\Phi_*(y^{\prod_{j=1}^{k} p_j})$ is an element of $\mathfrak{o}_m^\times$ (see Lemma 1), and $\Phi_*(y^{\prod_{j=1}^{k} p_j})$ satisfies

$$\Phi_*(y^{\prod_{j=1}^{k} p_j}) = \Phi_*(1) = \begin{cases} p_g & (k = g-1) \\ 1 & (k < g-1) \end{cases}.$$

Hence

$$\Phi_n(\zeta_m) \notin \mathfrak{o}_m^\times \quad (k = g-1),$$
$$\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times \quad (k < g-1).$$

3. $y \neq 1$, $y^{n'} \neq 1$. Let the order of y be N.

(3-1) $(N, n') \neq n'$

This means some prime number p_0 exists, which satisfies $p_0 | n'$ and $p_0 \nmid N$. We lose no generality if we assume $p_0 = p_1$. Then we get the following:

$$\Phi_n(\zeta_m) = \Phi_{n'}(y) = \frac{\Phi_{p_1}(y^{\prod_{j=2}^{g} p_j}) \cdot \left\{ \prod_{i<j} \Phi_{p_1}(y^{p_2 \cdots [p_i] \cdots [p_j] \cdots p_g}) \right\} \cdots}{\left\{ \prod_{j=2}^{g} \Phi_{p_1}(y^{p_2 \cdots [p_j] \cdots p_g}) \right\} \cdots}.$$

Every factor which appears in the right-hand side is an element of $\mathfrak{o}_m^\times$ (see Lemma 1).

Hence $\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times$.

(3-2) $(N, n') = n'$

This means $n'|N$

(3-2-1) $\frac{N}{n'} = p_0^q, \quad p_0 \neq p_j \ (1 \leqq j \leqq g)$

In this case, we get

$$\Phi_n(\zeta_m) = \Phi_{n'}(y) = \frac{(y^{\prod_{j=1}^{g} p_j} - 1)\cdot\left\{\prod_{i<j}(y^{p_1\cdots[p_i]\cdots[p_j]\cdots p_g} - 1)\right\}\cdots}{\left\{\sum_{j=1}^{g}(y^{p_1\cdots[p_j]\cdots p_g} - 1)\right\}\cdots}.$$

In the right-hand side, all factors except $y^{\prod_{j=1}^{g} p_j} - 1$ are contained in $\mathfrak{o}^{\times}$, and $y^{\prod_{j=1}^{g} p_j} - 1$ is not (see Lemma 2).

Therefore $\Phi_n(\zeta_m) \notin \mathfrak{o}_m^{\times}$.

(3-2-2) $\frac{N}{n'} = p_j^q, \ (\exists j, 1 \leqq j \leqq g)$

We lose no generality if we assume $p_j = p_1$. Then we get

$$\Phi_n(\zeta_m) = \Phi_{n'}(y) = \frac{(y^{\prod_{j=1}^{g} p_j} - 1)\cdot\left\{\prod_{i<j}(y^{p_1\cdots[p_i]\cdots[p_j]\cdots p_g} - 1)\right\}\cdots}{(y^{\prod_{j=2}^{g} p_j} - 1)\cdot\left\{\prod_{j=2}^{g}(y^{p_1\cdots[p_j]\cdots p_g} - 1)\right\}\cdots}.$$

In the right-hand side, all factors except $y^{\prod_{j=1}^{g} p_j} - 1$ and $y^{\prod_{j=2}^{g} p_j} - 1$ are contained in $\mathfrak{o}^{\times}$, and $y^{\prod_{j=1}^{g} p_j} - 1$ and $y^{\prod_{j=2}^{g} p_j} - 1$ are not (see Lemma 2). And

$$\pm N \frac{y^{\prod_{j=1}^{g} p_j} - 1}{y^{\prod_{j=2}^{g} p_j} - 1} = \frac{\{\Phi_{p_1^q}(1)\}^{p_1}}{\Phi_{p_1^{q+1}}(1)} = \frac{p_1^{p_1}}{p_1} = p_1^{p_1 - 1} \neq 1,$$

where "N" means "norm considered in $Q(\zeta_{p_1^{q+1}})$." From now on, "$\pm$" means "we do not mind whether it is $+$ or $-$."

Hence $\Phi_n(\zeta_m) \notin \mathfrak{o}_m^{\times}$.

(3-2-3) $\frac{N}{n'} \neq p_0^q$

In this case, we get

$$\Phi_n(\zeta_m) = \Phi_{n'}(y) = \frac{(y^{\prod_{j=1}^{g} p_j} - 1)\cdot\left\{\prod_{i<j}(y^{p_1\cdots[p_i]\cdots[p_j]\cdots p_g} - 1)\right\}\cdots}{\left\{\prod_{j=1}^{g}(y^{p_1\cdots[p_j]\cdots p_g} - 1)\right\}\cdots}.$$

In the right-hand side, all elements are contained in $\mathfrak{o}^\times$ (see Lemma 2).

Therefore $\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times$.

To conclude this appendix, we obtain the following result:

$$\Phi_n(\zeta_m) \notin \mathfrak{o}_m^\times \quad \left(\text{if} \frac{n}{m} = p^f \,(p\text{:prime number}, f \in Z)\right),$$
$$\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times \quad (\text{otherwise}).$$

Appendix C. Norm of $\Phi_n(\zeta_m)$

In Appendix B, we got

$$\Phi_n(\zeta_m) \notin \mathfrak{o}_m^\times \quad \left(\text{if} \frac{n}{m} = p^f \,(p\text{:prime number}, f \in Z)\right), \tag{C.1}$$
$$\Phi_n(\zeta_m) \in \mathfrak{o}_m^\times \quad (\text{otherwise}). \tag{C.2}$$

Therefore in the case (C.2), it is trivial that

$$N_m \Phi_n(\zeta_m) = \pm 1,$$

since $\xi \in \mathfrak{o}_m^\times \Rightarrow N_m \xi = \pm 1$.

Let us consider the case (C.1).

1. $f > 0$

In this case, from Appendix B, $\Phi_n(\zeta_m)$ can be written as

$$\Phi_n(\zeta_m) = p\xi \quad (\xi \in \mathfrak{o}_m^\times).$$

Hence we get

$$N_m \Phi_n(\zeta_m) = (N_m p)(N_m \xi) = \pm N_m p = \pm p^{\varphi(m)}.$$

2. $f = 0$

In this case, since $\Phi_n(\zeta_m) = 0$, it is trivial that

$$N_m \Phi_n(\zeta_m) = 0.$$

3. $f < 0$, i.e., $m = np^f$

There are two cases.

(3-1) $(n, p) = 1$

In this case, from Appendix B, $\Phi_n(\zeta_m)$ can be written as

$$\Phi_n(\zeta_m) = (\zeta_{p^f} - 1)\xi \quad (\xi \in \mathfrak{o}_m^\times).$$

Hence we get

$$\begin{aligned} N_m \Phi_n(\zeta_m) &= \pm N_m(\zeta_{p^f} - 1) = \pm N_{m/p^f}(N_{p^f}(\zeta_{p^f} - 1)) = \pm N_{m/p^f}(\Phi_{p^f}(1)) \\ &= \pm N_{m/p^f} p = \pm p^{\varphi(n)}. \end{aligned}$$

(Here "N_{m/p^f}" means "relative norm considered in relative algebraic number field $Q(\zeta_m)/Q(\zeta_{p^f})$.")

(3-2) $(n, p) = p$

Let $n = n'p^e$ $((n', p) = 1)$. Then we get $m = n'p^{e+f}$. In this case, from Appendix B, $\Phi_n(\zeta_m)$ can be written as

$$\Phi_n(\zeta_m) = \frac{(\zeta_{p^f} - 1)}{(\zeta_{p^{f+1}} - 1)}\xi \quad (\xi \in \mathfrak{o}_m^\times).$$

Hence we get

$$\begin{aligned} N_m\Phi_n(\zeta_m) &= \pm\frac{N_m(\zeta_{p^f} - 1)}{N_m(\zeta_{p^{f+1}} - 1)} = \pm\frac{N_{m/p^{e+f}}(N_{p^{e+f}}(\zeta_{p^f} - 1))}{N_{m/p^{e+f}}(N_{p^{e+f}}(\zeta_{p^{f+1}} - 1))} \\ &= \pm\frac{N_{m/p^{e+f}}(\Phi_{p^f}(1))^{P^e}}{N_{m/p^{e+f}}(\Phi_{p^{f+1}}(1))^{p^{e-1}}} = \pm N_{m/p^{e+f}}p^{p^e - p^{e-1}} = \pm N_{m/p^{e+f}}p^{\varphi(p^e)} \\ &= \pm p^{\varphi(n')\varphi(p^e)} = \pm p^{\varphi(n)}. \end{aligned}$$

To conclude this appendix, we obtain the following result:

$$\pm N_m\Phi_n(\zeta_m) = \begin{cases} p^{\varphi(m)} & \left(\text{if} \frac{n}{m} = p^f\,(p\text{:prime number}, f > 0)\right) \\ 0 & (\text{if}\, m = n) \\ p^{\varphi(n)} & \left(\text{if} \frac{m}{n} = p^f\,(p\text{:prime number}, f > 0)\right) \\ 1 & (\text{otherwise}) \end{cases}.$$

Acknowledgements. I would like to thank Professor K. Igi and Dr. Y. Kitazawa for useful suggestions and discussions and careful reading of this manuscript. I am also grateful to Professor H. Kawai, Mr. N. Ishibashi, Mr. S. Odake and Mr. A. Kato for useful discussions and comments.

References

1. Dixon, L., Harvey, J. A., Vafa, C., Witten, E.: Nucl. Phys. **B261**, 678–686 (1985) and **B274**, 285–314 (1986)
2. Candelas, P., Horowitz, G. T., Strominger, A., Witten, E.: Nucl. Phys. **B258**, 46–74 (1985)
3. Narain, K. S.: Phys. Lett. **B169**, 41–46 (1986)
4. Kawai, H., Lewellen, D. C., Tye, S.-H. H.: Phys. Rev. Lett. **57**, 1832–1835 (1986), Phys. Rev. **D34**, 3794–3804 (1986), Nucl. Phys. **B288**, 1–76 (1987) and Phys. Lett. **B191**, 63–69 (1987)
5. Ibàñez, L. E., Kim, J. E., Nilles, H. P., Quevedo, F.: Phys. Lett. **B191**, 282–286 (1987)
6. Ibàñez, L. E., Nilles, H. P., Quevedo, F.: Phys. Lett. **B187**, 25–32 (1987)
7. Katsuki, Y., Kawamura, Y., Kobayashi, T., Ohtsubo, N.: Phys. Lett. **B212**, 339–342 (1988)
8. Ono, T.: Sûron Jyosetsu, pp. 1–104. Japan: Syôkabô 1987
9. Takagi, T.: Daisûteki Seisûron, 2nd ed., pp. 1–138. Japan: Iwanami 1971
10. Ireland, K., Rosen, M.: A classical introduction to modern number theory, pp. 172–202. Berlin Heidelberg, New York: Springer 1982
11. Washington, L. C.: Introduction to Cyclotomic Fields, pp. 1–18. Berlin, Heidelberg, New York: Springer 1982
12. Washington, L. C.: Introduction to Cyclotomic Fields, pp. 352–360. Berlin, Heidelberg, New York: Springer 1982

Communicated by H. Araki

Received December 15, 1988