Comment. Math. Helvetici 59 (1984) 509–538 0010–2571/84/040509-30$01.50 + 0.20/0

Definite unimodular lattices having an automorphism of given characteristic polynomial

EVA BAYER-FLUCKIGER*

Introduction

A *lattice* will be an integral symmetric bilinear form of non-zero discriminant. The orthogonal group of a definite lattice is finite. This implies that the characteristic polynomial of an automorphism of a definite lattice is a product of cyclotomic polynomials. Conversely, let f be a product of cyclotomic polynomials. Does there exists a definite and *unimodular* lattice which has an automorphism with characteristic polynomial f? The first part of the present paper is devoted to the study of this problem. We shall give a complete solution in the case where f is a power of a cyclotomic polynomial. As an example, let us discuss the case $f=\phi_m$, the mth cyclotomic polynomial, where m is not a power of 2. We shall give some necessary conditions for the existence of a definite unimodular lattice (L, S) having an automorphism t with characteristic polynomial ϕ_m. One of these conditions is that m must be *mixed*, i.e. m is not of the form p^r or $2p^r$ where p is a prime. Indeed, if $m=p^r$ or $2p^r$ then $\det(1-t)\det(1+t)=\phi_m(1)\phi_m(-1)=p$ (cf. e.g. [13] Chap. VIII, §3, 1 and 3). Therefore the determinant of $S'=S(t-t^{-1})$ is p. But this is impossible because S' is skew-symmetric so $\det(S')$ must be a square. On the other hand it is not difficult to prove that (L, S) must be *even*, i.e. $S(x, x)$ is divisible by 2 for all x in L (see Lemma 1.4). The rank of an even, definite lattice is divisible by 8 (cf. e.g. [21], Chapitre V, 2.1) therefore $\varphi(m)=\deg\phi_m$ must be divisible by 8.

It turns out that these necessary conditions are also sufficient:

THEOREM. *Let m be a positive integer such that m is not a power of 2. Then there exists a definite unimodular lattice having an automorphism with characteristic polynomial ϕ_m if and only if m is mixed and $\varphi(m)$ is divisible by 8.*

---

* Supported by the "Fonds National de la Recherche Scientifique" of Switzerland.

In the second part of the paper we shall investigate some properties of definite lattices which have an automorphism of characteristic polynomial ϕ_m^n:

DEFINITION. A lattice is said to be *indecomposable* if it cannot be written as the orthogonal sum of two non-trivial lattices. We shall say that a lattice (L, S) *represents* 2 if there exists $x \in L$ such that $S(x, x) = 2$.

For instance we shall prove the following theorem, which also holds for *non unimodular* lattices:

THEOREM. *Let m be a square free integer, and let (L, S) be a definite lattice having an isometry with characteristic polynomial ϕ_m. Then (L, S) is indecomposable. If moreover $\varphi(m) > 8$ and m is not prime, then (L, S) does not represent* 2.

It is possible to apply these results to obtain some interesting examples. The first theorem implies that for $m = 35$, 39, 56 and 84 there exist definite unimodular lattices of rank 24 having an automorphism of characteristic polynomial ϕ_m. Using the second theorem and similar results, we see that these lattices do not represent 2, so by a theorem of Conway [3] they are isometric to the Leech lattice. We also obtain lattices of minimum 4 in dimensions 32 and 40. In higher dimensions we obtain lattices of minimum at least 4.

In the last part of the paper we shall study the classification problem of lattices having an automorphism with characteristic polynomial ϕ_m, and also the possibility of constructing such lattices explicitly. This leads to difficult problems concerning the signatures of units of a cyclotomic field.

I thank R. Gillard for useful conversations about the signatures of the units of a number field. I thank M. Kervaire for many useful comments on my manuscript.

1.

Let f be a product of cyclotomic polynomials. We shall say that (L, S) is an *f-lattice* if (L, S) has an automorphism with characteristic polynomial f. Let us denote ϕ_m the mth cyclotomic polynomial. In this section we shall solve the existence problem of definite unimodular ϕ_m^n-lattices, and then we shall make a few remarks on the corresponding problem for an arbitrary f.

THEOREM 1.1.

I. *Assume that m is not a power of* 2. *Then we have:*

a) *If n is divisible by* 4, *then there exists a definite unimodular ϕ_m^n-lattice for any m.*

b) *If* $n \equiv 2 \bmod 4$, *then there exists a definite unimodular* ϕ_m^n*-lattice if and only if* $\varphi(m)$ *is divisible by* 4.

c) *If* n *is odd, then there exists a definite unimodular* ϕ_m^n*-lattice if and only if* m *is mixed and* $\varphi(m)$ *is divisible by* 8.

II. *If* m *is a power of* 2, *then there exists a definite unimodular* ϕ_m^n*-lattice for any* n.

Moreover if m is not a power of 2 then the lattices will be even (cf. Lemma 1.4).

COROLLARY 1.2. *Let* f *be a product of cyclotomic polynomials. There exists a definite unimodular lattice having an automorphism with minimal polynomial* f *if and only if* f *has no repeated factors.*

Proof of Corollary 1.2. Let (L, S) be a definite lattice and let $t: L \to L$ be an automorphism of (L, S). Let f be the minimal polynomial of t. Then f has no repeated factors: indeed, if $f = g^2h$, then $M = gh(t)(L)$ is an isotropic submodule of L.

By taking orthogonal sums it suffices to prove the corollary for $f = \phi_m$. But this follows immediately from Theorem 1.1. □

Remark 1.3. Let $f = f_1 \cdots f_r$ where f_i is a power of a cyclotomic polynomial, $i = 1, \ldots, r$. Assume that the resultants $\operatorname{Res}(f_i, f_j) = \pm 1$ for all $i \neq j$. Then there exists a definite unimodular f-lattice if and only if there exists a definite unimodular f_i-lattice for all $i = 1, \ldots, r$.

Indeed, let (L, S) be a definite unimodular lattice having an automorphism t with characteristic polynomial f. Let $F = f_2 \cdots f_r$. There exist integral polynomials G and H such that

$$f_1 G + FH = 1.$$

Let $L_1 = F(t)(L)$ and $L_2 = f_1(t)(L)$, and let S_1 and S_2 be the restrictions of S to L_1 and L_2. Then it is easy to check that

$$(L, S) = (L_1, S_1) \boxplus (L_2, S_2)$$

where $\boxplus$ denotes the orthogonal sum, and that (L_1, S_1) is an f_1-lattice.

We have $\operatorname{Res}(\phi_n, \phi_m) = \pm 1$ except if $m = p^r n$, where p is a prime (see for instance [23], Proposition 3.4).

The remainder of this section will be devoted to the proof of Theorem 1.1. We shall need a few lemmas:

LEMMA 1.4. *If* (L, S) *is a* ϕ_m^n*-lattice with* m *not a power of* 2, *then* (L, S) *is even.*

Proof. Let t be an automorphism of (L, S) with characteristic polynomial ϕ_m^n. As m is not a power of 2, we have $\det(1-t)=1$ or $\det(1+t)=1$ (cf. e.g. [13] Chap. VII §3). By replacing t with $-t$ if necessary we may assume that $1-t$ is invertible. We have $S(wx, y)=S(x, w'y)$ with $w=(1-t)^{-1}$, $w'=(1-t^{-1})^{-1}$. It is easy to check that $w+w'=id_L$. Therefore $S(x, x)=S((w+w')x, x)=2S(wx, x)$ so (L, S) is even. □

Let ζ be a primitive mth root of unity, and let $K=\mathbb{Q}(\zeta)$. We shall denote by an overbar the $\mathbb{Q}$-involution of K which sends ζ to ζ^{-1}. Let I be a fractional $\mathbb{Z}[\zeta]$-ideal such that $\bar{I}=I$, let L be a torsion free $\mathbb{Z}[\zeta]$-module of finite rank and let $h: L\times L \to I$ be a hermitian or skew-hermitian form. We shall say that (L, h) is *unimodular* if and only if the adjoint of h, $\mathrm{ad}(h): L \to \mathrm{Hom}_{\mathbb{Z}[\zeta]}(L, I)$, is bijective.

The following lemma will be important for the construction of ϕ_m^n-lattices:

LEMMA 1.5 (Stoltzfus [23], Lemma 2.6 and Addendum). *Let* Δ *be the inverse different of* $K/\mathbb{Q}$. *Let* $h: L\times L\to\Delta$ *be a unimodular hermitian form, and let* $n=\mathrm{rank}_{\mathbb{Z}[\zeta]}(L)$. *Set*

$$S(x, y)=\mathrm{Tr}_{K/\mathbb{Q}}(h(x, y)). \tag{1}$$

Then (L, S) *is a unimodular* ϕ_m^n*-lattice. Conversely, if* (L, S) *is a* ϕ_m^n*-lattice then there exists a unique hermitian form* $h: L\times L\to\Delta$ *such that* (1) *holds. If moreover* (L, S) *is unimodular, then* h *is unimodular.*

Let $F=\mathbb{Q}(\zeta+\zeta^{-1})$ be the fixed field of the involution. We shall denote by ψ the minimal polynomial of $\eta=\zeta+\zeta^{-1}$, and by ψ' the derivative of ψ.

We shall also need the following lemma:

LEMMA 1.6. *The different of* $K/\mathbb{Q}$ *is* $(\zeta-\zeta^{-1})\psi'(\eta)\mathbb{Z}[\zeta]$.

Proof. The different of K/F is $(\zeta-\zeta^{-1})\mathbb{Z}[\zeta]$ and the different of $F/\mathbb{Q}$ is $\psi'(\eta)\mathbb{Z}[\eta]$, see for instance [14], III, §1. The lemma now follows by the multiplicative property of the differents, see [14], III, §1.

Notice that this lemma gives a bijection between unimodular hermitian forms with values in the inverse different and unimodular skew-hermitian forms with values in $\mathbb{Z}[\zeta]$.

Let V be a finite dimensional K-vector space and let $h_K: V\times V \to K$ be a non-singular ε-hermitian form, where $\varepsilon = \pm 1$. We shall need to know under what conditions (V, h_K) contains a unimodular lattice, i.e. under what conditions there exists a unimodular ε-hermitian form $h: L\times L \to \mathbb{Z}[\zeta]$ such that $(L, h)\otimes_{\mathbb{Z}[\zeta]} K = (V, h_K)$. If $\varepsilon = -1$, then we only need to consider the case where $\dim_K(V)$ is even. In this case $\det(h_K)$ is an element of $F^{\cdot}$, and we shall denote $D = \det(h_K) \in F^{\cdot}/N_{K/F}(K^{\cdot})$ the *discriminant* of (V, h_K).

LEMMA 1.7. (Wall [27] Proposition 6, or Levine [16] Lemma 24.3). *Let $\theta = (\zeta - \zeta^{-1})^2$ and let $(,)_P$ be the Hilbert symbol. Let us denote D the discriminant of h_K.*

$\varepsilon = +1$ (V, h_K) contains a unimodular lattice if and only if $(D, \theta)_P = 1$ for every finite prime P of F which does not ramify in K.

$\varepsilon = -1$, $\dim(V)$ even. Then (V, h_K) contains a unimodular lattice if and only if $(D, \theta)_P = 1$ for every finite prime P of F which does not ramify in K, and for every non-dyadic finite prime of F which ramifies in K.

Proof of Theorem 1.1. Let us check that the conditions of the theorem are necessary. If m is not a power of 2 then a ϕ_m^n-lattice (L, S) is even by Lemma 1.4. If moreover (L, S) is definite then $\mathrm{rank}_{\mathbb{Z}}(L)$ is divisible by 8, see for instance [21], Chapitre V, 2.1. Therefore $n\varphi(m)$ must be divisible by 8. We have already proved in the introduction that the condition m mixed is necessary in part c.) of the theorem.

We shall now prove that the conditions are also sufficient:

I.a) Notice that it is sufficient to consider the case $n = 4$. Let $d \in F^{\cdot}$ such that $d\psi'(\sigma)$ is totally positive and set $a = (\zeta - \zeta^{-1})d$. Let us denote $\langle a\rangle$ the skew-hermitian form $g: K\times K \to K$ such that $g(x, y) = ax\bar{y}$. Set $V = K^4$, and let h_K be the form $\langle a\rangle \boxplus \langle a\rangle \boxplus \langle a\rangle \boxplus \langle a\rangle$ where $\boxplus$ denotes the orthogonal sum. Lemma 1.7 implies that (V, h_K) contains a unimodular lattice (L, h). Now let

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\zeta - \zeta^{-1}}\frac{1}{\psi'(\eta)}h(x, y)\right)$$

then (L, S) is a unimodular ϕ_m^4-lattice by Lemma 1.5 and Lemma 1.6.

We have to show that (L, S) is positive definite. It suffices to show that the form $S_{\mathbb{Q}}: V\times V \to \mathbb{Q}$, obtained by extension of the scalars, is positive definite. We have $S_{\mathbb{Q}} = S'_{\mathbb{Q}} \boxplus S'_{\mathbb{Q}} \boxplus S'_{\mathbb{Q}} \boxplus S'_{\mathbb{Q}}$ where

$$S'_{\mathbb{Q}}(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\zeta - \zeta^{-1}} \frac{1}{\psi'(\eta)} ax\bar{y}\right)$$

with $x, y \in K$. Now

$$S'_{\mathbb{Q}}(x, x) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{d}{\psi'(\eta)} x\bar{x}\right), \quad \text{and} \quad \frac{d}{\psi'(\eta)}$$

is totally positive. Therefore $S'_{\mathbb{Q}}$ is positive definite.

b) It is sufficient to consider the case $n = 2$. Let $d \in F^{\cdot}$ such that $d\psi'(\sigma)$ is totally positive and set $a = (\zeta - \zeta^{-1})d$. Let $V = K^2$, and let $h_K : V \times V \to K$ be the skew-hermitian form $\langle a \rangle \boxplus \langle a \rangle$. The discriminant of h_k is $D = (\zeta - \zeta^{-1})^2 d^2 = -1 \in F^{\cdot}/N_{K/F}(K^{\cdot})$. We have $(-1, \theta)_P = 1$ if P is a finite prime of F which does not ramify in K (cf. [14], IX, §3). If m is mixed then no finite prime of F ramifies in K (see [28], Proposition 2.15) so the conditions of Lemma 1.7 are satisfied in this case. If $m = p^r$ or $2p^r$, then exactly one finite prime P of F ramifies in K, and $N_{K/\mathbb{Q}}(P) = p$. We have $\varphi(m) = (p-1)p^{r-1}$. We are assuming that p is odd and that $\varphi(m)$ is divisible by 4. This implies that $p \equiv 1 \bmod 4$. Therefore -1 is a square mod p, and by Hensel's lemma this implies that $(-1, \theta)_P = 1$. So the conditions of Lemma 1.7 are satisfied in this case also, therefore (V, h_K) contains a unimodular lattice (L, h). Set

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\zeta - \zeta^{-1}} \frac{1}{\psi'(\eta)} h(x, y)\right)$$

for $x, y \in L$. As in the proof of case a) we check that (L, S) is a positive definite ϕ_m^2-lattice.

The case 1. (c) of Theorem 1.1 will follow from a description of unimodular definite ϕ_m-lattices, given by Proposition 1.8. In order to state this proposition we need the notion of signature.

Recall that the field F is totally real. Let $G = \mathrm{Gal}\,(F/\mathbb{Q})$, which can be identified with the set of real embeddings of F over $\mathbb{Q}$. Define $\sigma : \mathbb{R}^{\cdot} \to \mathbb{F}_2 G$ by $\sigma(\alpha) = 0$ if α is positive, $\sigma(\alpha) = 1$ if α is negative. The signature $\mathrm{sgn} : F^{\cdot} \to \mathbb{F}_2 G$ is given by:

$$\mathrm{sgn}\,(x) = \sum_{g \in G} \sigma(gx) g^{-1}.$$

This is an equivariant homomorphism.

Let $\zeta_1, \ldots, \zeta_N, \zeta_1^{-1}, \ldots, \zeta_N^{-1}$ where $N = \varphi(m)/2$ be a list of the primitive mth roots of unity such that, if we set $\eta_j = \zeta_j + \zeta_j^{-1}$, then $\eta_j > \eta_k$ for $j < k$.

Let g_k be the real embedding of F which sends η to η_k.

Recall that $(,)_P$ is the Hilbert symbol, and that $\theta = (\zeta - \zeta^{-1})^2$.

PROPOSITION 1.8. *Let m be a positive integer such that m is mixed that $\varphi(m)$ is divisible by* 8.

1) *There exists an $a \in F^{\cdot}$ such that $(a, \theta)_P = 1$ for all finite primes P of F, and that*

$$\operatorname{sgn}(a) = \sum_{k=1}^{M} g_{2k}^{-1}$$

where

$$M = \frac{\varphi(m)}{4}.$$

2) *If $a \in F^{\cdot}$ is as in* 1) *then there exists a fractional $\mathbb{Z}[\zeta]$-ideal I such that the hermitian form*

$$h : I \times I \to \mathbb{Z}[\zeta]$$

defined by

$$h(x, y) = ax\bar{y}$$

is unimodular.

3) *Let a and I be as above. Set*

$$S(x, y) = \operatorname{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\, ax\bar{y}\right) \tag{2}$$

then (I, S) is a definite unimodular ϕ_m-lattice.

Conversely, if (I, S) is a definite unimodular ϕ_m-lattice then I can be identified with a fractional $\mathbb{Z}[\zeta]$-ideal, and S can be written under the form (2) *so that the hermitian form $h : I \times I \to \mathbb{Z}[\zeta]$ defined by $h(x, y) = ax\bar{y}$ is unimodular, and that $a \in F^{\cdot}$ satisfies the conditions of* 1).

Proof of Proposition 1.8. 1) Let P_j be the infinite prime of F corresponding to g_j. Then the condition

$$\operatorname{sgn}(a) = \sum_{k=1}^{M} g_{2k}^{-1}$$

is equivalent with $(a, \theta)_{P_j} = (-1)^j$ for $j = 1, \ldots, N = \varphi(m)/2$. By Hilbert reciprocity there exists an $a \in F^\cdot$ such that $(a, \theta)_{P_j} = (-1)^j$ for $j = 1, \ldots, N$ and that $(a, \theta)_P = 1$ for P finite if and only if $\prod_{j=1}^{N} (-1)^j = 1$. This is the case if and only if $\varphi(m)$ is divisible by 8.

2) Let $V = K$ and let h_k be the 1-dimensional hermitian form $\langle a \rangle$. By Lemma 1.7 the form (V, h_k) contains a unimodular lattice, i.e. there exists a fractional $\mathbb{Z}[\zeta]$-ideal I such that $h: I \times I \to \mathbb{Z}[\zeta]$, $h(x, y) = ax\bar{y}$ is unimodular.

3) If m is mixed then no finite prime of F ramifies in K, and $\zeta - \zeta^{-1}$ is a unit. Therefore by Lemma 1.6 the inverse different of $K/\mathbb{Q}$ is $1/\psi'(\eta)\mathbb{Z}[\zeta]$. By Lemma 1.5 this implies that the lattice (I, S) defined by (2) is unimodular. Let us check that (I, S) is also definite: it suffices to prove that $a\psi'(\eta)$ is totally positive, i.e. that

$$\operatorname{sgn}(\psi'(\eta)) = \sum_{k=1}^{M} g_{2k}^{-1}.$$

We have

$$\psi(X) = \prod_{j=1}^{N} (X - \eta_j), \quad \text{so} \quad \psi'(\eta_k) = \prod_{\substack{j \neq k \\ j=1}}^{N} (\eta_k - \eta_j).$$

Recall that $\eta_j > \eta_k$ if $j < k$. Therefore it is immediate that the signature of $\psi'(\eta)$ is as above.

Conversely let (I, S) be a positive definite ϕ_m-lattice. We have seen in the first part of the proof that the inverse different of $K/\mathbb{Q}$ is $1/\psi'(\eta)\mathbb{Z}[\zeta]$. Therefore by Lemma 1.5 we can write S under the form (2) where $h: I \times I \to \mathbb{Z}[\zeta]$, $h(x, y) = ax\bar{y}$ is a unimodular hermitian form. Therefore $(a, \theta)_P = 1$ if P is a finite prime of F.

It is easy to check that S positive definite implies $a\psi'(\eta)$ totally positive (use weak approximation). Therefore

$$\operatorname{sgn}(a) = \operatorname{sgn}(\psi'(\eta)) = \sum_{k=1}^{M} g_{2k}^{-1}. \quad \square$$

It is clear that this proposition implies I. c), therefore the proof of part I of Theorem 1.1 is complete.

Part II of Theorem 1.1 can be proved by direct computation: the form $\langle 1 \rangle \boxplus \cdots \boxplus \langle 1 \rangle$ is a ϕ_m-lattice if $m = 2^r$. It also follows from the description of definite unimodular ϕ_m-lattices, $m = 2^r$, given by Proposition 1.9:

PROPOSITION 1.9. *Let $m = 2^r$ and set $k = m/4$.*

1) *Let $a \in F^\cdot$ be totally positive and such that $(a, \theta)_P = 1$ if P is a non-dyadic finite prime of F. Then there exists a fractional $\mathbb{Z}[\zeta]$-ideal I such that the skew-*

hermitian form

$$h: I \times I \to \mathbb{Z}[\zeta]$$

defined by

$$h(x, y) = \zeta^k a x \bar{y}$$

is unimodular.

2) *Let a and I be as in* 1). *Set*

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\frac{1}{\zeta-\zeta^{-1}}\zeta^k a x \bar{y}\right) \tag{3}$$

then (I, S) *is a definite unimodular* ϕ_m*-lattice.*

Conversely, if (I, S) *is a definite unimodular* ϕ_m*-lattice then* S *can be written under the form* (3) *with* $a \in F^{\cdot}$ *as in* 1).

Proof. 1) By Lemma 1.7 there exists a fractional ideal I such that the hermitian form $g: I \times I \to \mathbb{Z}[\zeta]$ defined by $g(x, y) = a x \bar{y}$ is unimodular. As ζ^k is a unit, this implies that (I, h) is also unimodular.

2) By Lemma 1.5 and Lemma 1.6 we see that (I, S) is unimodular. Let $\alpha = (\zeta - \zeta^{-1})\zeta^{-k}$. In order to prove that (I, S) is positive definite, it suffices to prove that

$$\mathrm{sgn}\,(\alpha) = \mathrm{sgn}\,(\psi'(\eta)).$$

As in the proof of Proposition 1.8 we see that

$$\mathrm{sgn}\,(\psi'(\eta)) = \sum_{h=1}^{M} g_{2h}^{-1}$$

where $M = \varphi(m)/4 = k/2$ if $m \neq 4$ and $M = 0$ if $m = 4$. Notice that

$$g_j(\eta) = \eta_j = \exp\left(\frac{2i\pi(2j-1)}{m}\right) + \exp\left(\frac{-2i\pi(2j-1)}{m}\right) \qquad j = 1, \ldots, k.$$

We have

$$\alpha = \zeta^{k-1} + \zeta^{-k+1}.$$

It is easy to check that $g_j(\alpha)$ is positive if j is odd and negative if j is even. Therefore (I, S) is positive definite.

Conversely let (I, S) be a definite unimodular ϕ_m-lattice. By Lemma 1.6 and Lemma 1.5 we have

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\frac{1}{\zeta-\zeta^{-1}}bx\bar{y}\right)$$

where $h: I \times I \to \mathbb{Z}[\zeta]$ defined by $h(x, y) = bx\bar{y}$ is a unimodular skew-hermitian form.

Set $a = b\zeta^{-k}$. Then $a \in F^{\cdot}$, and

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\frac{1}{\zeta-\zeta^{-1}}\zeta^k ax\bar{y}\right).$$

Let us check that a satisfies the conditions of 1). As (I, h) is unimodular, the hermitian form $g: I \times I \to \mathbb{Z}[\zeta]$ defined by $g(x, y) = ax\bar{y}$ is also unimodular. Therefore by Lemma 1.7 we have $(a, \theta)_P = 1$ for all finite non-dyadic primes P of F. We have seen in the proof of 1) that $\psi'(\eta)(\zeta-\zeta^{-1})\zeta^{-k}$ is totally positive. Therefore a is also totally positive.

Remark 1.10. Let $m = 2^r$. It is easy to check that if we take $a = 1$ and $I = \mathbb{Z}[\zeta]$ in Proposition 1.9, we obtain the lattice $\langle 1\rangle \boxplus \cdots \boxplus \langle 1\rangle$. On the other hand, if (I, S) is a definite ϕ_m-lattice such that I is a non-principal $\mathbb{Z}[\zeta]$-ideal then (I, S) does not respresent 1. Indeed, suppose that there exists an $x \in I$ such that $S(x, x) = 1$. Then $(\mathbb{Z}x, S)$ is an orthogonal summand of (L, S). A definite lattice factorizes uniquely into the orthogonal sum of indecomposable sublattices (cf. [19], 105.1). This implies that either $t(x) = \pm x$, or $S(x, t(x)) = 0$. Let $a = m/2 - 1$. Then the elements $x, t(x), \ldots, t^a(x)$ are linearly independent, so we must have $S(t^i(x), t^j(x)) = 0$ if $i \neq j$. But we also have $S(t^i(x), t^i(x)) = 1$, so the lattice $(\mathbb{Z}[\zeta]x, S)$ is unimodular. As $\mathbb{Z}[\zeta]x \subset I$, this implies that $\mathbb{Z}[\zeta]x = I$ so I is a principal ideal.

Remark 1.11. I thank J. Milnor for the following observations. Theorem 1 implies that for all integers $m > 1$, there exists a definite unimodular lattice L such that the orthogonal group of L contain a cyclic group C_m of order m, and such that C_m acts freely on $L \backslash \{0\}$.

Let t be an automorphism of order m of a lattice L. Then the cyclic group generated by t acts freely on $L \backslash \{0\}$ if and only if the characteristic polynomial of t is a power of the cyclotomic polynomial ϕ_m.

2.

In this section we shall investigate some properties of definite ϕ_m^n-lattices. If there is no ambiguity we shall write just L instead of (L, S). We shall be interested in the decompositions $L = L_1 \boxplus \cdots \boxplus L_k$ into the orthogonal sum of sublattices (the sublattices L_i are not supposed to be stables by an automorphism of L). We shall say that L is *indecomposable* if L cannot be written as the orthogonal sum of two non-trivial lattices.

Let us recall that ζ is a primitive mth root of unity, that $K = \mathbb{Q}(\zeta)$ and that Δ is the inverse different of $K/\mathbb{Q}$.

THEOREM 2.1. *Let (L, S) be a positive definite ϕ_m^n-lattice such that*

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(h(x, y))$$

where $h: L \times L \to \Delta$ is an indecomposable hermitian form.

Let $L = L_1 \boxplus \cdots \boxplus L_k$ where the L_i's are indecomposable lattices.

Then $L_i \simeq L_j$ for all i and j. The number of indecomposable components k divides m and $n\varphi(m)$. We have $\mathrm{rank}_{\mathbb{Z}}(L_i) = n\varphi(m)/k$, and L_i is a $\phi_{m/k}^r$-lattice for some r. In particular $\varphi(m/k)$ divides $n\varphi(m)/k$.

If (L, S) is unimodular and if m is not a power of 2, then $n\varphi(m)/k$ is divisible by 8. If moreover $n = 1$, then $m \neq kp^r$, $m \neq 2kp^r$ where p is an odd prime.

Proof. Let $t: L \to L$ be an automorphism of (L, S) with characteristic polynomial ϕ_m^n. Then t permutes the L_i's: $t(L_i) = L_j$, because the decomposition into the orthogonal sum of indecomposable sublattices is unique (cf. [19], 105.1). Suppose that $L = M \boxplus N$ with $t(M) = M$ (therefore also $t(N) = N$). Then M and N are sub $\mathbb{Z}[\zeta]$-modules of L. By Lemma 1.5 there exist hermitian forms $g: M \times M \to \Delta$ and $g': N \times N \to \Delta$ such that

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(g(x, y)) \qquad x, y \in M$$

and

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(g'(x, y)) \qquad x, y \in N.$$

Then $(L, h) = (M, g) \boxplus (N, g')$, but we have supposed (L, h) indecomposable so this implies $M = 0$ or $N = 0$. Therefore t induces a cyclic permutation of the L_i's. So k divides m. On the other hand the L_i's are all isometric, and in particular $k \cdot \mathrm{rank}_{\mathbb{Z}}(L_i) = n\varphi(m)$. We have $t^k(L_i) = L_i$, so the L_i's are $\phi_{m/k}^r$-lattices for some r. Then $\mathrm{rank}_{\mathbb{Z}}(L_i) = r\varphi(m/k)$, so $r\varphi(m/k) = n\varphi(m)/k$.

If (L, S) is unimodular, then the L_i's are unimodular too, therefore $\operatorname{rank}_{\mathbb{Z}}(L_i) = n\varphi(m)/k$ must be divisible by 8 (see e.g. [21] Chapitre V, 2.1). Let $n=1$. We have $\varphi(m/k) \leqslant \varphi(m)/k$, therefore $r=1$, and L_i is a $\phi_{m/k}$-lattice. By Theorem 1.1 this implies that m/k must be mixed or a power of 2. □

We shall say that a lattice (L, S) *represents* 2 if there exists an $x \in L$ such that $S(x, x) = 2$.

COROLLARY 2.2. *Let (L, S) be a definite ϕ_m-lattice with m square free. Then (L, S) is indecomposable. If moreover $m \neq p$, $2p$ where p is a prime and if $\varphi(m) > 8$ then (L, S) does not represent 2.*

Proof. As (L, S) is a ϕ_m-lattice, by Lemma 1.5 it is the trace of a rank one hermitian form, which is of course indecomposable. Let k be a common divisor of m and of $\varphi(m)$. It is easy to check that as m is square free, we have $\varphi(m)/k < \varphi(m/k)$ if $k \neq 1$. Therefore by Theorem 2.1 we must have $k=1$, so (L, S) is indecomposable.

Let $R = \{x \in L \text{ such that } S(x, x) = 2\}$ and set $M = \mathbb{Z}R$. Let t be an automorphism of (L, S) with characteristic polynomial ϕ_m. Then $t(M) = M$. As ϕ_m is irreducible, we have either $M = 0$ or $\operatorname{rank}_{\mathbb{Z}}(M) = \varphi(m)$. If $M \neq 0$, then (M, S) is a definite ϕ_m-lattice, so by the first part of Corollary 2.2, (M, S) is indecomposable. Then R is an indecomposable root system, therefore $R = A_h$ or D_h with $h = \varphi(m)$, cf. for instance [18] p. 145–146. The automorphism group of A_h is the product of the symmetric group of $h+1$ letters S_{h+1} with $C_2 = \mathbb{Z}/2\mathbb{Z}$ and the automorphism group of D_h is a semi-direct product of S_h with C_2^h (cf. [2], Chap. VI, no 4.7 and no 4.8) and it is easy to check that these groups do not contain any element t such that the characteristic polynomial of the automorphism $t: \mathbb{Z}R \to \mathbb{Z}R$ is ϕ_m. Therefore $M = 0$ and R is empty. □

In the following Corollary we shall assume that (L, S) is unimodular:

COROLLARY 2.3. *Let (L, S) be a definite unimodular ϕ_m^n-lattice such that one of the following holds:*

a) *$n=1$, m is mixed and for all divisors k of m and of $\varphi(m)$ such that $\varphi(m/k) = \varphi(m)/k$, either m/k is not mixed or $\varphi(m/k)$ is not divisible by 8.*

b) *$n=2$, $m=p$ or $2 \cdot p$ with p prime and $p \equiv 1 \bmod 4$.*

c) *$n=4$, $m=p$ or $2 \cdot p$ with p prime and $p \equiv 3 \bmod 4$.*

Then (L, S) is indecomposable.

Proof. By Lemma 1.5, $S(x, y) = \operatorname{Tr}_{K/\mathbb{Q}}(h(x, y))$ where $h: L \times L \to \Delta$ is a unimodular hermitian form. By Theorem 1.1 we see that h is indecomposable. The indecomposability of (L, S) then follows immediately from Theorem 2.1. □

Let (L, S) be a definite lattice and let α be a positive integer. Set $R=\{x\in L$ such that $S(x, x)=\alpha\}$. We shall say that R is decomposable if $R=R_1\cup R_2$ such that R_1 and R_2 are disjoint and $S(x, y)=0$ for $x\in R_1$, $y\in R_2$.

If $\alpha=2$ then R is a root system.

The following Corollary is a consequence of Theorem 2.1 and of results of Kervaire:

COROLLARY 2.4. *Let (L, S) be a definite ϕ_m^n-lattice. Let $T\subset R$ such that T is indecomposable.*

a) *If R contains exactly k copies of T, then $k\cdot \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}T)=r\varphi(m)$ for some integer $1\leqslant r\leqslant n$. If $r=1$, then k divides m, and $\mathbb{Z}T$ is a $\phi_{m/k}$-lattice. In particular* $\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}T)=\varphi(m/k)$.

b) *Suppose that $\alpha=2$ (so R is a root system) and that m is not a power of 2. Then T is either D_4, E_6, E_8 or A_h with h even.*

Proof. a) Let t be an automorphism of (L, S) with characteristic polynomial ϕ_m^n. We have $t(R)=R$. Let M be an orthogonal summand of $(\mathbb{Z}R, S)$ such that $t(M)=M$ and that M does not have any orthogonal summands N with $t(N)=N$. By Lemma 1.5 it is clear that (M, S) satisfies the hypothesis of Theorem 2.1. Let $M=L_1\boxplus\cdots\boxplus L_a$ then by Theorem 2.1 we have $L_i\simeq L_j$ for all i and j, so $a\cdot\operatorname{rank}_{\mathbb{Z}}(L_i)=\operatorname{rank}_{\mathbb{Z}}(M)$ which is divisible by $\varphi(m)$. Notice that $L_i\simeq\mathbb{Z}T$ for some indecomposable $T\subset R$. It is easy to see that this implies that $k\cdot\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}T)=r\varphi(m)$ for some integer $1\leqslant r\leqslant n$.

If $r=1$, then there exists a unique $M\subset\mathbb{Z}R$ as above such that $\mathbb{Z}T\subset M$. By Theorem 2.1, $\mathbb{Z}T$ is a $\phi_{m/k}^b$-lattice for some integer b. We have $\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}T)=b\varphi(m/k)$, so $b\varphi(m/k)=\varphi(m)/k$. But $\varphi(m/k)\geqslant\varphi(m)/k$, so $b=1$.

b) If m is not a power of 2, then either $1-t$ or $1+t$ is invertible (indeed, t is the multiplication by a primitive mth root of unity). Therefore (L, S) has an automorphism s such that $1-s$ is invertible. Kervaire has proved that this implies that $(\mathbb{Z}T, S)$ also has an automorphism s' such that $1-s'$ is invertible (cf. [8] Proposition 2). On the other hand be also proved that this implies that T must be one of the root systems D_4, E_6, E_8 or A_h with h even (see [8] Proposition 3). $\square$

COROLLARY 2.5. *Let (L, S) be a definite indecomposable ϕ_m-lattice. Assume that for all common divisors k of m and of $\varphi(m)$ such that $\varphi(m/k)=\varphi(m)/k$ we have : $\varphi(m)\neq 4k$, $\varphi(m)\neq 6k$, and either $\varphi(m)/k$ is odd, or*

$$\frac{m}{k}>2\frac{\varphi(m)}{k}+2.$$

Then (L, S) does not represent 2.

Proof. Let $R=\{x\in L$ such that $S(x,x)=2\}$, and let T be an indecomposable root system. Assume that R contains exactly k copies of T. Then part a) of Corollary 2.4 implies that k divides m and $\varphi(m)$ and that $\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}T)=\varphi(m)/k=\varphi(m/k)$.

Moreover $(\mathbb{Z}T, S)$ is a $\phi_{m/k}$-lattice. By part b) of Corollary 2.4 we have $T=D_4$, E_6 or A_h with h even. But we have assumed that $\varphi(m/k)\neq 4, 6$ so $T=A_h$ where $h=\varphi(m/k)$. The automorphism group of A_h is $S_{h+1}\times C_2$ (cf. [2], Chap. VI, no 4.7). We have assumed that $m/k>2(h+1)$, therefore the automorphism group of $A_h=T$ does not contain any element of characteristic polynomial $\phi_{m/k}$. Therefore T is empty, so (L, S) does not represent 2. □

We shall give an application of Theorem 2.1 to the indecomposability of tensor products of definite lattices. We shall need the following lemma:

LEMMA 2.6. *Let ζ be a primitive* mth *root of unity, and let (L, S) be a definite lattice. Set $M=L\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta]$, and let $h: M\times M\to\mathbb{Z}[\zeta]$ be the hermitian form defined by*

$$h(x\otimes\alpha, y\otimes\beta)=\alpha\bar{\beta}S(x, y).$$

If (L, S) is indecomposable, then (M, h) is also indecomposable.

Proof. The proof is essentially the same as Kitaoka's proof of a similar statement for quadratic forms, cf. [9] Corollary of Theorem 4.

COROLLARY 2.7. *Let (L, S) and (L', S') be indecomposable definite lattices such that (L', S') is a ϕ_m-lattice. Let $r=\operatorname{rank}_{\mathbb{Z}}(L)$. Assume that if k is a common divisor of m and of $r\varphi(m)$, then $\varphi(m/k)$ does not divide $r\varphi(m)/k$.*

Then $(L, S)\otimes_{\mathbb{Z}}(L', S')$ is indecomposable.

Proof. Let $(M, h)=(L, S)\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta]$ as in Lemma 2.6. Then (M, h) is indecomposable. We have $S'(x, y)=\operatorname{Tr}_{K/\mathbb{Q}}(g(x, y))$, where $g: L'\times L'\to\Delta$ is a hermitian form, and L' is a rank one $\mathbb{Z}[\zeta]$-module (cf. Lemma 1.5). Then

$$(N, f)=(M, h)\otimes_{\mathbb{Z}[\zeta]}(L', g')$$

is also indecomposable.

Let (N, S'') be defined by

$$S''(x, y)=\operatorname{Tr}_{K/\mathbb{Q}}(f(x, y)).$$

Then (N, S'') is indecomposable by Theorem 2.1. On the other hand, it is easy to see that (N, S'') is isometric to $(L, S) \otimes_{\mathbb{Z}} (L', S')$, the proof is similar to the proof of [12], Chapter VII, Theorem 1.3. □

Kitaoka has proved a theorem in [10] with same conclusion as Corollary 2.7. The precise relationship between Kitaoka's hypothesis and the hypothesis of Corollary 2.6 is not known.

3. The classification problem of definite unimodular ϕ_m-lattices

Let (L, S) be a definite unimodular ϕ_m-lattice. In Section 1 we have found necessary and sufficient conditions for the existence of such a lattice: namely either m is a power of 2, or m is mixed and $\varphi(m)$ is divisible by 8. In the present section we shall study the classification up to isometry of these lattices.

Let us recall some notations: ζ is a primitive mth root of unity, $K = \mathbb{Q}(\zeta)$, $F = \mathbb{Q}(\zeta + \zeta^{-1})$ is the fixed field of the $\mathbb{Q}$-involution of K which sends ζ to ζ^{-1}. We denote by ψ the minimal polynomial of $\eta = \zeta + \zeta^{-1}$, and by ψ' the derivative of ψ.

Let h^- be the *relative class number* of K (i.e. the class number of K divided by the class number of F).

Let C_K and C_F be the ideal class groups of K and F. We have a homomorphism $N_{K/F}: C_K \to C_F$ which is induced by the norm of ideals. Notice that h^- is the cardinality of the kernel of this homomorphism (see for instance [15] Theorem 4.4).

In this section we shall assume that h^- is *odd*. If m is a power of 2 then this hypothesis is always satisfied, see Weber [29].

PROPOSITION 3.1. *Assume that h^- is odd. Let J be a fractional $\mathbb{Z}[\zeta]$-ideal such that $N_{K/F}([J]) = 1$, where $[J]$ is the class of J in C_K.*

Then there exists $S: J \times J \to \mathbb{Z}$ such that (J, S) is a definite unimodular ϕ_m-lattice.

Conversely if (J, S) is a unimodular ϕ_m-lattice, then $N_{K/F}([J]) = 1$.

Moreover if (J, S_1) and (J, S_2) are two definite unimodular ϕ_m-lattices, then $(J, S_1) \simeq (J, S_2)$.

Let us recall that $G = \mathrm{Gal}(F/\mathbb{Q})$, and that we have defined the signature homomorphism $\mathrm{sgn}: F^{\cdot} \to \mathbb{F}_2 G$ by

$$\mathrm{sgn}(x) = \sum_{g \in G} \sigma(gx) g^{-1}$$

where $\sigma(\alpha) = 0$ or 1 according as α is positive or negative.

Let U_F and U_K denote the group of units of F and of K. We have $N_{K/F}: U_K \to U_F$ defined by $N_{K/F}(u) = u\bar{u}$.

For the proof of Proposition 3.1 we shall need the following lemma (which I believe is well known):

LEMMA 3.2. *Assume that h^- is odd.*
Let us denote IG the augmentation ideal of $\mathbb{F}_2G$. Then we have:
a) *If m is mixed, then*

$$\mathrm{sgn}: U_F/N_{K/F}(U_K) \to IG$$

is bijective.
b) *If m is a prime power, then*

$$\mathrm{sgn}: U_F/N_{K/F}(U_K) \to \mathbb{F}_2G$$

is bijective.

Proof of Lemma 3.2. Let us denote U_F^+ the totally positive units of F.
a) If m is mixed then by Shimura [22] Proposition A.2 we see that $[U_F^+ : U_F^2] = 2$. But it is well known that $[N_{K/F}(U_K): U_F^2] = 2$, see Hasse [7], §21 and §22. Therefore $U_F^+ = N_{K/F}(U_K)$, so $\mathrm{sgn}: U_F/N_{K/F}(U_K) \to IG$ is injective. But $U_F/N_{K/F}(U_K)$ and IG have the same cardinality, (see [1] Example 2.5) therefore sgn is also onto.
b) If $m = 2^r$, then by Shimura [22] Proposition A.2 we see that $U_F^+ = U_F^2 = N_{K/F}(U_K)$. On the other hand, $U_F/N_{K/F}(U_K)$ and $\mathbb{F}_2G$ have the same cardinality (see [1] Example 2.5). Therefore $\mathrm{sgn}: U_F/N_{K/F}(U_K) \to \mathbb{F}_2G$ is bijective. □

Proof of Proposition 3.1. We have two cases to consider: either m is mixed and $\varphi(m)$ is divisible by 8, or m is a power of 2.
1) Let us assume that m is mixed and that $\varphi(m)$ is divisible by 8. Let J be a fractional $\mathbb{Z}[\zeta]$-ideal such that $N_{K/F}([J]) = 1$. Then there exists a $b \in F^{\cdot}$ such that the hermitian form $h: J \times J \to \mathbb{Z}[\zeta]$ defined by $h(x, y) = bx\bar{y}$ is unimodular (cf. [1], Proposition 1.2).
Recall that $\theta = (\zeta - \zeta^{-1})^2$, and that $(,)_P$ is the Hilbert symbol. No finite prime of F ramifies in K, therefore by Lemma 1.7 we have $(b, \theta)_P = 1$ for all finite primes P of F. By Hilbert reciprocity we have $\prod_{P \in \Omega} (b, \theta)_P = 1$, where Ω is the set of infinite primes of F. It is easy to see that this implies that $\mathrm{sgn}\,(b) \in IG$.

Let $x = \sum_{k=1}^{M} g_{2k}^{-1}$, where $M = \varphi(m)/4$ (see Proposition 1.8 for the definition of g_i). As $\varphi(m)$ is divisible by 8, we have $x \in IG$.
By part a) of Lemma 3.2 we see that there exists $u \in U_F$ such that

$$\operatorname{sgn}(u) = x + \operatorname{sgn}(b).$$

Let $a = ub$, then $\operatorname{sgn}(a) = \sum_{k=1}^{M} g_{2k}^{-1}$, and $(a, \theta)_P = 1$ for all finite primes P of F. Set

$$S(x, y) = \operatorname{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\, ax\bar{y}\right) \tag{2}$$

then by Proposition 1.8, (J, S) is a definite unimodular ϕ_m-lattice.
If (J, S) is a unimodular ϕ_m-lattice, then we can identify J with a fractional $\mathbb{Z}[\zeta]$-ideal. By Lemma 1.5 and Lemma 1.6 we have

$$S(x, y) = \operatorname{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\, h(x, y)\right)$$

where $h: J \times J \to \mathbb{Z}[\zeta]$ is unimodular. Therefore by [1], Proposition 1.2 we have $N([J]) = 1$.
If (J, S_1) and (J, S_2) are two unimodular, definite ϕ_m-lattices, then by Proposition 1.8 we have

$$S_i(x, y) = \operatorname{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\, a_i x\bar{y}\right)$$

such that $h_i: J \times J \to \mathbb{Z}[\zeta]$ defined by $h_i(x, y) = a_i x\bar{y}$ is unimodular. Therefore $u = a_1 a_2^{-1} \in U_F$ (cf. [1], §2). As S_1 and S_2 are definite, by Proposition 1.8 we have $\operatorname{sgn}(a_1) = \operatorname{sgn}(a_2)$. Therefore u is totally positive. By Lemma 3.2 this implies that there exists $v \in U_K$ such that $u = v\bar{v}$. Therefore $f: J \to J$ defined by $f(x) = vx$ gives an isometry between (J, S_1) and (J, S_2).

2) Let $m = 2^r$. Let J be a fractional $\mathbb{Z}[\zeta]$-ideal such that $N_{K/F}([J]) = 1$. Then there exists $b \in F^{\cdot}$ such that the hermitian form $h: J \times J \to \mathbb{Z}[\zeta]$ defined by $h(x, y) = bx\bar{y}$ is unimodular (cf. [1], Proposition 1.2). By Lemma 3.2 there exists $u \in U_F$ such that $\operatorname{sgn}(u) = \operatorname{sgn}(b)$. Set

$$S(x, y) = \operatorname{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)}\frac{1}{\zeta - \zeta^{-1}}\, \zeta^k aux\bar{y}\right). \tag{3}$$

By Proposition 1.9, (J, S) is a definite unimodular ϕ_m-lattice. The end of the proof if similar to the case m mixed. □

Let us denote by C^- the kernel of $N_{K/F}: C_K \to C_F$ and let h be the cardinality of $C^-/\mathrm{Gal}\,(K/\mathbb{Q})$.

COROLLARY 3.3. *Assume that h^- is odd. The number of isometry classes of definite unimodular ϕ_m-lattices is at most h.*

Proof. By Proposition 3.1 we have a surjective map from C^- to the set of isometry classes of definite unimodular ϕ_m-lattices. Let $c_1, c_2 \in C^-$ and suppose that there exists a $g \in \mathrm{Gal}\,(K/\mathbb{Q})$ such that $c_1^g = c_2$.

It is easy to see that the definite unimodular ϕ_m-lattices associated to c_1 and c_1^g are isometric (write the ϕ_m-lattice under the form (2) or (3)). □

It would be interesting to know the exact number of isometry classes of definite unimodular ϕ_m-lattices. A similar problem (for automorphisms of prime order) has been solved by H.-G. Quebbemann, cf. [20].

4. The signature of cyclotomic units

We have seen in the preceding section that in order to construct definite unimodular ϕ_m-lattices, we have to find units of $F = \mathbb{Q}(\zeta + \zeta^{-1})$ (where ζ is a primitive mth root of unity) of prescribed signatures. If the relative class number h^- of $K = \mathbb{Q}(\zeta)$ is odd, then such units exist by Lemma 3.2. The present section deals with the problem of constructing these units explicitly.

We shall expose here a method of computing the signature of cyclotomic units which uses some ideas of G. Gras (cf. [6]). This method has been communicated to me by R. Gillard.

DEFINITION 4.1. Let ξ be a primitive $2m$th root of unity, and let a be a positive integer relatively prime to m. Set

$$w_a = \frac{\xi^a - \xi^{-a}}{\xi - \xi^{-1}}.$$

It is easy to check that w_a is a unit of F (cf. e.g. [5]). We shall say that w_a is a *cyclotomic unit.*

Recall that $G = \mathrm{Gal}(F/\mathbb{Q})$ and that

$$\mathrm{sgn}(x) = \sum_{g\in G} \sigma(gx)g^{-1} \in \mathbb{F}_2G$$

where $\sigma(\alpha)=0$ if α is positive and $\sigma(\alpha)=1$ if α is negative.

We shall give formulas for $\mathrm{sgn}(w_a)$. We have to distinguish the cases m odd and m even.

m odd

Set

$$\xi = \exp\left(\frac{\pi i}{m} + \pi i\right).$$

Let b be an integer relatively prime to m, and let $\rho(b)$ be the element of G which sends $\xi+\xi^{-1}$ to $\xi^b+\xi^{-b}$. Let us denote $R(b)$ the remainder of the division of b modulo m. We have:

$$\rho(b)w_a = \frac{\xi^{ab}-\xi^{-ab}}{\xi^b-\xi^{-b}} = \frac{\sin\left(\dfrac{\pi R(ab)}{m} + \pi R(ab)\right)}{\sin\left(\dfrac{\pi R(b)}{m} + \pi R(b)\right)}$$

$$= (-1)^{R(ab)-R(b)}\left(\frac{\sin\dfrac{\pi R(ab)}{m}}{\sin\dfrac{\pi R(b)}{m}}\right).$$

Therefore the sign of $\sigma(b)w_a$ is determined by the parity of $R(ab)-R(b)$. We have

$$\mathrm{sgn}(w_a) = \sum_{\substack{(b,m)=1\\ 0<b<m/2}} [R(ab)-R(b)]\rho(b)^{-1}$$

where $[x]$ denotes the remainder of the division of x modulo 2.

m even

We may assume that m is divisible by 4. Set

$$\xi = \exp\left(\frac{\pi i}{m} + \pi i\right).$$

Let $0<b<m$, we have:

$$\rho(b)w_a=\frac{\xi^{ab}-\xi^{-ab}}{\xi^b-\xi^{-b}}=\frac{\sin\left(\dfrac{\pi ab}{m}+\pi ab\right)}{\sin\left(\dfrac{\pi b}{m}+\pi b)\right)}$$

$$=(-1)^{ab-b}\frac{\sin\left(\dfrac{\pi ab}{m}\right)}{\sin\left(\dfrac{\pi b}{m}\right)}.$$

As a is odd, $(-1)^{ab-b}=1$. We have $0<b<m$, so $\sin(\pi b/m)$ is positive. Therefore we have:

$$\operatorname{sgn}(a)=\sum_{\substack{(b,m)=1\\ 0<b<m/2}}\left[\frac{ab}{m}\right]\rho(b)^{-1}$$

where $[x]$ denotes the remainder of the division of the integral part of x modulo 2.

Assume that m is mixed and that $\varphi(m)$ is divisible by 8. By Proposition 1.8 there exists a ϕ_m-lattice (I, S) with $I\simeq\mathbb{Z}[\zeta]$ if and only if there exists a $u\in U_F$ such that

$$\operatorname{sgn}(u)=\sum_{k=1}^{M} g_{2k}^{-1} \tag{4}$$

where $M=\varphi(m)/4$.

(See Proposition 1.8 for the definition of the g_i's).

In the following examples we shall construct such units. This construction makes use of the formulas for the signature of cyclotomic units.

EXAMPLE 4.2. $m=15$. Then $g=\rho(2)$ generates G. We want to find $u\in U_F$ satisfying (4), i.e.

$$\operatorname{sgn}(u)=\rho(2)+\rho(7)=g+g^3.$$

The formula for the signature of cyclotomic units in the case m odd shows that $\operatorname{sgn}(w_2)=1+g$. We have $(1+g^3)(1+g)=g+g^3$, so $u=w_2\cdot w_2^{\rho(7)}=(\zeta+\zeta^{-1})(\zeta^7+\zeta^{-7})$ has signature $g+g^3$.

By Proposition 1.8 the ϕ_{15}-lattice $(\mathbb{Z}[\zeta], S)$, with

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)} ux\bar{y}\right)$$

is definite and unimodular. By Lemma 1.4 this lattice is even. As the rank of this lattice is 8, it must be isometric to Γ_8 (see for instance [21] Chapitre V, 2.3).

EXAMPLE 4.3. $m = 24$. Then $G = \{1, \rho(5), \rho(7), \rho(11)\}$. Using the formula for the case m even, we see that $\mathrm{sgn}(w_7) = \rho(5)^{-1} + \rho(11)^{-1}$. Therefore $u = w_7$ satisfies the relation (4). As in Example 4.1 we obtain the lattice Γ_8.

EXAMPLE 4.4. $m = 35$. Then $g = \rho(2)$ generates G. We want to find $u \in U_F$ satisfifying (4), i.e.

$$\begin{aligned} \mathrm{sgn}(u) &= \rho(2)^{-1} + \rho(4)^{-1} + \rho(8)^{-1} + \rho(11)^{-1} + \rho(13)^{-1} + \rho(17)^{-1} \\ &= g + g^3 + g^4 + g^9 + g^{10} + g^{11}. \end{aligned}$$

By the formula for the case m odd we have

$$\mathrm{sgn}(w_2) = 1 + g + g^2 + g^3 + g^4 + g^7.$$

We see by direct computation that

$$(g^6 + g^7 + g^9 + g^{11})\,\mathrm{sgn}(w_2) = g + g^3 + g^4 + g^9 + g^{10} + g^{11}.$$

Let $\alpha = g^{-6} + g^{-7} + g^{-9} + g^{-11}$. Then the unit

$$u = w_2^{\alpha} = (\zeta^6 + \zeta^{-6})(\zeta^7 + \zeta^{-7})(\zeta^9 + \zeta^{-9})(\zeta^{11} + \zeta^{-11})$$

Satisfies the relation (4).

Therefore by Proposition 1.8 the ϕ_{35}-lattice $(\mathbb{Z}[\zeta], S)$ with

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)} ux\bar{y}\right)$$

is definite and unimodular. As 35 is square free we can apply Corollary 2.2: the lattice $(\mathbb{Z}[\zeta], S)$ is indecomposable and does not represent 2. By Lemma 1.4 the lattice is also even. As the rank of this lattice is 24, the above properties imply that it must be isometric to the Leech lattice (cf. Conway [3]).

5. Examples

There exists a complete list of the isometry classes of definite unimodular and even lattices of rank at most 24 (cf. Niemeier [18]). For all mixed integer m such that $\varphi(m) \leqslant 24$, we shall determine which of these lattices are ϕ_m-lattices.

Recall that if m is mixed and if $\varphi(m)$ is divisible by 8, then there exists a definite unimodular and even ϕ_m-lattice (see Theorem 1.1).

1) *Lattices of rank* 8

We have $\varphi(m)=8$, so $m=15(30)$, 20 or 24. As Γ_8 is up to isometry the unique definite, unimodular and even lattice of rank 8, we see that Γ_8 is a ϕ_m-lattice for these values of m.

2) *Lattices of rank* 16

We have $\varphi(m)=16$, so $m=40$, 48 or 60. For these values of m the corresponding cyclotomic field has relative class number $h^-=1$ (cf. [28], p. 353). Therefore there exists a unique definite unimodular ϕ_m-lattice with $m=40$, 48 or 60 (see Section 3, Proposition 3.1). This lattice is $\Gamma_8 \boxplus \Gamma_8$ in each case. Indeed, Γ_8 is a $\phi_{m/2}$-lattice (cf. 1)). Let t be an automorphism of Γ_8 with characteristic polynomial $\phi_{m/2}$. Then $\begin{pmatrix} 0 & t \\ I & 0 \end{pmatrix}$ is an automorphism of $\Gamma_8 \boxplus \Gamma_8$ with characteristic polynomial ϕ_m.

Every definite, unimodular and even lattice of rank 16 is isometric to $\Gamma_8 \boxplus \Gamma_8$ or to Γ_{16}. The above discussion shows that Γ_{16} cannot be a ϕ_m-lattice. This also follows from Corollary 2.4: indeed, the root system of Γ_{16} is D_{16}.

3) *Lattices of rank* 24

We have $\varphi(m)=24$, so $m=35(70)$, $39(78)$, $45(90)$, 52, 56, 72 or 84. We shall study each case separately.

$m=35$

As 35 is square free, we can apply Corollary 2.2: Every definite ϕ_{35}-lattice is indecomposable and does not represent 2. Therefore if (L, S) is a definite unimodular ϕ_{35}-lattice, then (L, S) is isometric to the Leech lattice (cf. Conway [3]). Explicitly, we have $L \simeq \mathbb{Z}[\zeta]$ where ζ is a primitive 35th root of unity, and

$$S(x, y)=\operatorname{Tr}_{K/\mathbb{Q}}\left(\frac{1}{\psi'(\eta)} ux\bar{y}\right), \qquad x, y \in \mathbb{Z}[\zeta]$$

where $u=(\zeta^6+\zeta^{-6})(\zeta^7+\zeta^{-7})(\zeta^9+\zeta^{-9})(\zeta^{11}+\zeta^{-11})$, ψ is the minimal polynomial of $\eta=\zeta+\zeta^{-1}$ and ψ' is the derivative of ψ (cf. Example 4.4).

$m=39$

As 39 is square free, we can again apply Corollary 2.2 to deduce that every definite unimodular ϕ_{39}-lattice (L, S) is isometric to the Leech lattice. We shall give a description of (L, S) which is similar to Craig's presentation of the Leech lattice (cf. [4]). Let $K=\mathbb{Q}(\zeta)$ where ζ is a primitive 39th root of unity. It is straightforward to check that the different of $K/\mathbb{Q}$ is

$$P_1\bar{P}_1P_2\bar{P}_2Q^{11}\bar{Q}^{11}$$

where P_1, P_2 and Q are prime $\mathbb{Z}[\zeta]$-ideals with norms 3^3, 3^3 and 13 respectively. Let $I=(P_1P_2Q^{11})^{-1}$, and let us denote Δ the inverse different of $K/\mathbb{Q}$. Then $\Delta=I\bar{I}$. Therefore we can take $L\simeq I$ and

$$S(x, y)=\mathrm{Tr}_{K/\mathbb{Q}}(x\bar{y}), \qquad x, y\in I.$$

(This corresponds to $a=\psi'(\eta)$ in Proposition 1.8.)

Notice that for $m=35$ one cannot write the inverse different under the form $J\bar{J}$, therefore this type of description is not possible.

$m=45$

$\Gamma_8\boxplus\Gamma_8\boxplus\Gamma_8$ is a ϕ_{45}-lattice. Indeed, let t be an automorphism of Γ_8 with characteristic polynomial ϕ_{15} (cf. 1). Then

$$\begin{pmatrix} 0 & 0 & I \\ t & 0 & 0 \\ 0 & I & 0 \end{pmatrix}$$

is an automorphism of $\Gamma_8\boxplus\Gamma_8\boxplus\Gamma_8$ with characteristic polynomial ϕ_{45}.

Let $K=\mathbb{Q}(\zeta)$, where ζ is a primitive 45th root of unity. The relative class number of K is 1 (cf. [28], p. 353). By Proposition 3.1 this implies that up to isometry $\Gamma_8\boxplus\Gamma_8\boxplus\Gamma_8$ is the unique unimodular definite ϕ_{45}-lattice.

$m=52$

Let (L, S) be a definite unimodular ϕ_{52}-lattice. Then Corollary 2.3 implies that (L, S) is indecomposable. Indeed, $k=2$ is the only common divisor of 52 and of $\varphi(52)=24$ such that $\varphi(52/k)=24/k$. But $24/2=12$ is not divisible by 8, therefore (L, S) is indecomposable. Let $R=\{x\in L$ such that $S(x, x)=2\}$ be the associated root system. Then Corollary 2.4 implies that either R is empty or $R=2A_{12}$. We shall see that there exists a definite unimodular ϕ_{52}-lattice (L, S) having root system $2A_{12}$.

The automorphism group of A_{12} is $S_{13}\times C_2$ (cf. [2], Chap. VI, no 4.7), therefore there exists an automorphism $t:\mathbb{Z}A_{12}\to\mathbb{Z}A_{12}$ with characteristic polynomial ϕ_{26}. Set $R=2A_{12}$, and let $T:\mathbb{Z}R\to\mathbb{Z}R$ be the automorphism which is given by the matrix

$$\begin{pmatrix} 0 & t \\ I & 0 \end{pmatrix}$$

Then the characteristic polynomial of T is ϕ_{52}.

Let us identify the ith copy of $\mathbb{Z}A_{12}$ with

$$\left\{\sum_{j=1}^{13} x_{ji}e_{ji} \text{ such that } x_{ji}\in\mathbb{Z}, \sum_{j=1}^{13} x_{ji}=0\right\}$$

for $i=1,2$. Let

$$y_{1i}=\tfrac{1}{13}\sum_{j=1}^{12} e_{ji}-\tfrac{12}{13}e_{13i}$$

and let $y_{ri}=ry_{1i}$. Set $R=2A_{12}$, and let $L=\mathbb{Z}R+\mathbb{Z}(y_{11}+y_{52})$. Then L is unimodular (cf. Niemeier [18] p. 163). It is easy to check that $T(y_{11}+y_{52})=y_{51}-y_{12}$ modulo $\mathbb{Z}R$. An easy computation shows that $S(y_{11}+y_{52}, T(y_{11}+y_{52}))=1$, therefore $T(y_{11}+y_{52})\in L$. So T is an automorphism of (L, S).

The relative class number of the cyclotomic field corresponding to the 52th roots of unity is $h^-=3$ (see [28], p. 353). therefore by Corollary 3.3 there are at most two isometry classes of definite unimodular ϕ_{52}-lattices. We already know that there exists such a lattice (L, S) with root system $2A_{12}$. But Niemeier has shown that every definite unimodular lattice of rank 24 having root system $2A_{12}$ is isometric to (L, S). We have seen that there are no other root systems R such that $\mathbb{Z}R$ is a ϕ_{52}-lattice. Therefore if there exists another definite unimodular ϕ_{52}-lattice, it must be isometric to the Leech lattice.

$m=56$

Let (L, S) be a definite unimodular ϕ_{56}-lattice. Then Corollary 2.3 implies that (L, S) is indecomposable. Indeed, $k=2$ and $k=4$ are the only common divisors of 56 and of 24 such that $\varphi(56/k)=24/k$, and in each case $24/k$ is not divisible by 8.

Let $R=\{x\in L \text{ such that } S(x, x)=2\}$ be the associated root system. Then

Corollary 2.4 implies that if R is not empty, then $R=2A_{12}$, $4E_6$ or $4A_6$. It is easy to check that the automorphism groups of $2A_{12}$ and of $4E_6$ do not contain any element of characteristic polynomial ϕ_{56} (cf. [2], Chap. VI, no 4.7 and no 4.12).

We shall see that $R=4A_6$ is also impossible. Indeed, let $R=4A_6$. The automorphism group of A_6 is $S_7\times C_2$ (cf. [2], Chap. VI, no 4.7) therefore A_6 has automorphisms of characteristic polynomial ϕ_{14}. Let T be an automorphism of R with characteristic polynomial ϕ_{56}. Then T is the composition of

$$\begin{pmatrix} t_1 & 0 & 0 & 0 \\ 0 & t_2 & 0 & 0 \\ 0 & 0 & t_3 & 0 \\ 0 & 0 & 0 & t_4 \end{pmatrix}$$

with a permutation matrix of order 4, where $t_i=\pm I$ or an automorphism of A_6 with characteristic polynomial ϕ_{14} or ϕ_7. Niemeier has proved that the unimodular lattice (L, S) with root system $R=4A_6$ is unique up to isometry (cf. [18], p. 165). We shall see that T does not extend to an automorphism of L.

We shall identify the ith copy of $\mathbb{Z}A_6$ with

$$\left\{\sum_{j=1}^{7} \alpha_{ji}e_{ji} \text{ such that } \alpha_{ji}\in\mathbb{Z}, \sum_{j=1}^{7} \alpha_{ji}=0\right\}.$$

Let $y_{1i}=\frac{1}{7}\sum_{j=1}^{6} e_{ji}-\frac{6}{7}e_{7i}$ and let $y_{ri}=ry_{1i}$, for $r=1,\dots,6$. Let $x_1=y_{11}+y_{22}+y_{33}$, $x_2=y_{32}-y_{23}+y_{14}$. then $L=\mathbb{Z}R+\mathbb{Z}x_1+\mathbb{Z}x_2$ is a unimodular lattice (cf. Niemeier [18], p. 166). It is easy to check that

$$T(y_{1i})=\pm y_{1\sigma(i)} \text{ modulo } R$$

where σ is a permutation of order 4. To simplify notations, we shall write ab instead of $S(a, b)$. We see that $x_1T(x_1)$ is either $\pm y_1y_2\pm y_2y_3$ or $y_1y_3\pm y_2y_3$, or $\pm y_1y_2\pm y_1y_3$ (we omit the second index which is irrelevant here). But none of these can be an integer, as $y_1y_2=\frac{5}{7}$, $y_1y_3=\frac{4}{7}$ and $y_2y_3=\frac{8}{7}$. Therefore $T(x_1)\notin L$.

This implies that up to isometry the Leech lattice is the unique definite unimodular ϕ_{56}-lattice.

$m=72$

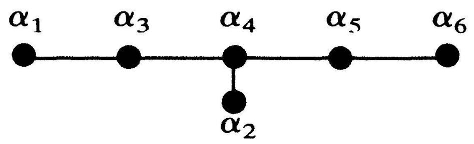
a) $\Gamma_8\boxplus\Gamma_8\boxplus\Gamma_8$ *is a* ϕ_{72}-lattice. Indeed, Γ_8 has an automorphism t with characteristic polynomial ϕ_{24} (see 1)). Then

$$\begin{pmatrix} 0 & 0 & I \\ t & 0 & 0 \\ 0 & I & 0 \end{pmatrix}$$

is an automorphism of $\Gamma_8 \boxplus \Gamma_8 \boxplus \Gamma_8$ with characteristic polynomial ϕ_{72}.

b) There exists a unimodular lattice (L, S) with root system $R = 4E_6$. Moreover, (L, S) is unique up to isometry with these properties (cf. Niemeier [18], p. 160). We shall see that (L, S) is a ϕ_{72}-lattice.

The root system E_6 is generated by 6 simple roots $\alpha_1, \alpha_2, \ldots, \alpha_6$, with Dynkin diagram



The corresponding matrix of inner products is

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

We have $\det(M) = 3$.

We see that $\mathbb{Z}E_6$ is a ϕ_9-lattice. Indeed, one can identify $\mathbb{Z}E_6$ with the lattice $(\mathbb{Z}[\zeta], S')$, with

$$S'(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{\eta}{3(\eta+1)} x\bar{y}\right)$$

where ζ is a primitive 9th root of unity, $K = \mathbb{Q}(\zeta)$ and $\eta = \zeta + \zeta^{-1}$. Notice that the different of $K/\mathbb{Q}$ is $3(\zeta - \zeta^{-1})(\eta^2 - 1)$, see Lemma 1.6. On the other hand, $N_{K/\mathbb{Q}}(\zeta - \zeta^{-1}) = 3$. As η and $\eta - 1$ are units, it is easy to deduce from this that $\det(S') = 3$. It is easy to check that $\eta/\eta + 1$ is totally positive. Therefore S' is positive definite. Theorem 2.1 implies that S' is indecomposable. But Kneser has proved (cf. [11]) that there exists only one isometry class of definite indecomposable lattices of rank 6 and determinant 3, so $(\mathbb{Z}[\zeta], S')$ is isometric to E_6.

I thank Michel Kervaire for the following explicit identification of $(\mathbb{Z}[\zeta], S')$ and E_6: set $\alpha_1 = \zeta^2 + \zeta^3$, $\alpha_2 = 1$, $\alpha_3 = -(\zeta + \zeta^2)$, $\alpha_4 = \zeta$, $\alpha_5 = \zeta^4$, $\alpha_6 = -1 + \zeta^2 - \zeta^3 - \zeta^4 + \zeta^5$. Using this identification, he also obtains formulas for an automorphism θ of E_6 with characteristic polynomial ϕ_9:

$$\theta(\alpha_1) = \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5$$
$$\theta(\alpha_2) = \alpha_4$$
$$\theta(\alpha_3) = -\alpha_1$$
$$\theta(\alpha_4) = -(\alpha_3 + \alpha_4)$$
$$\theta(\alpha_5) = \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5 + \alpha_6$$
$$\theta(\alpha_6) = -(\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6).$$

Let $t = -\theta$. Then t is an automorphism of E_6 with characteristic polynomial ϕ_{18}. Set

$$\mathrm{T} = \begin{pmatrix} 0 & 0 & 0 & I \\ t & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \end{pmatrix}$$

Then T is an automorphism of $4E_6$ with characteristic polynomial ϕ_{72}.

If (M, S) is a lattice, we shall denote

$$M^{\#} = \{x \in \mathbb{Q}M \text{ such that } S(x, M) \in \mathbb{Z}\}.$$

We have $X = \mathbb{Z}E_6^{\#}/\mathbb{Z}E_6 = \mathbb{F}_3 x$, with $x = \frac{1}{3}(-\alpha_1 + \alpha_3 - \alpha_5 + \alpha_6)$, $x^2 = \frac{4}{3}$. The automorphism t of $\mathbb{Z}E_6$ extends to an automorphism of $\mathbb{Z}E_6^{\#}$, and induces $t: X \to X$. It is easy to check that $t(x) = -x$.

Following Niemeier (cf. [18] p. 160) we shall denote $\pm x_i \pm y_i \pm z_i \pm s_i$, $i = 0, 1$, the elements of

$$\bigoplus_{k=1}^{4} (\mathbb{Z}E_6^{\#}/\mathbb{Z}E_6)$$

Let $L = \mathbb{Z}R + \mathbb{Z}a + \mathbb{Z}b$, where $a = x_1 + y_1 + z_1 + s_0 = x_1 + y_1 + z_1$, and $b = x_0 - y_1 + z_1 + s_1 = -y_1 + z_1 + s_1$. It is easy to check that $aT(a) = aT(b) = bT(b) = 0$ and that $bT(a) = 4$. As these are all integral, we have $T(L) = L$.

The relative class number of the cyclotomic field corresponding to the 72th roots of unity is 3. Therefore by Corollary 3.3 there are at most 2 isometry classes of definite unimodular ϕ_{72}-lattices. This implies that up to isometry the only definite unimodular ϕ_{72}-lattices are $\Gamma_8 \boxplus \Gamma_8 \boxplus \Gamma_8$ and the lattice with root system $4E_6$.

$m = 84$

Let (L, S) be a definite unimodular ϕ_{84}-lattice. The only common divisor k of 84 and of 24 such that $\varphi(84/k) = 24/k$ is $k = 2$. As 12 is not divisible by 8, Corollary 2.3 implies that (L, S) is indecomposable. As $41 > 26$, Corollary 2.5 implies that (L, S) does not represent 2. Therefore by Conway's result [3] the lattice (L, S) is isometric to the Leech lattice.

The following Proposition summarizes the above results on ϕ_m-lattices of rank 24:

PROPOSITION 5.1. *Every definite unimodular ϕ_m-lattice of rank* 24 *is isometric to one of the following:*

a) *the Leech lattice* $(m = 35, 39, 56, 84)$

b) $\Gamma_8 \boxplus \Gamma_8 \boxplus \Gamma_8$ $(m = 45, 72)$

c) *the Niemeier lattice with root system* $2A_{12}$ $(m = 52)$

d) *the Niemeier lattice with root system* $4E_6$ $(m = 72)$.

Remark 5.2. J. Tits has given four presentations of the Leech lattice (cf. [24], [25]) which also make use of trace maps. M.-F. Vignéras has generalized one of these constructions and obtained lattices of higher rank (cf. [26]).

4) *Lattices of rank* $r \geqslant 32$

We shall give some values of m such that every definite unimodular ϕ_m-lattice is indecomposable and does not represent 2 (this can be proved by easy applications of Corollaries 2.2, 2.3 or 2.5). We shall also give the relative class number h^- of the corresponding cyclotomic field (cf. [24], p. 353).

$r = 32$	$m = 51$,	$h^- = 5$
$r = 40$	$m = 55$,	$h^- = 10$
	$m = 132$,	$h^- = 11$
$r = 48$	$m = 65$,	$h^- = 64$
	$m = 105$,	$h^- = 13$
$r = 56$	$m = 87$,	$h^- = 1536$
$r = 64$	$m = 85$,	$h^- = 6205$

$r=72 \quad m=91, \quad h^{-}=53872$

$ \quad m=228, \quad h^{-}=238203$

$r=96 \quad m=119, \quad h^{-}=1238459625$

This list is not always complete for the given values of r: if $r \geqslant 72$, it is easy to find more examples.

REFERENCES

[1] BAYER, E. *Unimodular hermitian and skew-hermitian forms*, J. Algebra *74* (1982), 341–373.
[2] BOURBAKI, N. *Groupes et algèbres de Lie* (1968) Hermann.
[3] CONWAY J. H. *A characterisation of Leech's lattice*, Invent. Math. *7* (1969), 137–143.
[4] CRAIG, M. *A cyclotomic construction for Leech's lattice*. Mathematika *25* (1978), 236–241.
[5] GARBANATI, D. *Unit signatures, and even class numbers, and relative class numbers*. J. Reine angew. Math. *274/275* (1975), 376–384.
[6] GRAS, G. *Nombres de φ-classes invariantes. Applications aux classes des corps abéliens*. Bull. Soc. Math. de France *106* (1978), 337–364.
[7] HASSE, H. *Über die Klassenzahl abelscher Zahlkörper* (1952) Akademia-Verlag, Berlin.
[8] KERVAIRE, M. *Formes de Seifert et formes quadratiques entières*, to appear.
[9] KITAOKA, Y. *Scalar extension of quadratic lattices*. Nagoya Math. J. *66* (1977), 139–149.
[10] KITAOKA, Y. *Tensor products of positive definite quadradic forms*, V. Nagoya Math. J. *82* (1981), 99–111.
[11] KNESER, M. *Klassenzahlen definiter quadratischer Formen*. Arch. Math. *8* (1957), 241–250.
[12] LAM, T. Y. *The algebraic theory of quadratic forms* (1973) W. A. Benjamin, Inc.
[13] LANG, S. *Algebra* (1969). Addison-Wesley Publishing Company.
[14] ——, *Algebraic number theory* (1970) Addison-Wesley Publishing Company.
[15] ——, *Cyclotomic fields* (1978). Springer-Verlag, New York, Heidelberg, Berlin.
[16] LEVINE, J. P. *Algebraic structure of knot modules*. Lecture Notes in Mathematics 772 (1980), Springer-Verlag, New York, Heidelberg, Berlin.
[17] MILNOR, J. *On isometries of inner product spaces*, Invent. Math. *8* (1969), 83–97.
[18] NIEMEIER, H.-V. *Definite quadratische Formen der Dimension 24 und Diskriminante 1*. J. Number Theory *5* (1973), 142–178.
[19] O'MEARA, O. T. *Introduction to quadratic forms* (1973). Springer-Verlag, Berlin, Heidelberg, New York.
[20] QUEBBEMANN, H.-G. *Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung*, J. Reine agnew. Math. *326* (1981), 158–170.
[21] SERRE, J.-P. *Cours d'arithmétique* (1970) Presses Universitaires de France.
[22] SHIMURA, G. *On abelian varieties with complex multiplication*. Proc. London Math. Soc. *34* (1977), 65–86.
[23] STOLTZFUS, N. W. *Unraveling the integral knot concordance group*. Mem. Amer. Math. Soc. *12*, no. 192 (1977), 1–91.
[24] TITS, J. *Four presentations of Leech's lattice. Finite simple groups II*, 303–307. Academic Press, 1980.
[25] TITS, J. *Quaternions over* $\mathbb{Q}(\sqrt{5})$, *Leech's lattice and the sporadic groups of Hall-Janko*. J. Algebra 63 (1980), 56–75.
[26] VIGNÉRAS, M.-F. *Arithmétique des algèbres de quaternions*. Springer Lecture Notes in Mathematics 800, (1980).

[27] WALL, C. T. C. *On the classification of hermitian forms I.* Ring of algebraic integers. Compos. Math. *22* (1970), 424–451.
[28] WASHINGTON, L. C. Introduction to cyclotomic fields. Graduate Texts in Mathematics 83 (1982) Springer-Verlag, New York, Heidelberg, Berlin.
[29] WEBER, H. Theorie der abelschen Zahlkörper. Acta Math. *8* (1886).

Universitéde Genève
Section de mathématiques
Rue du Lièvre 2–4
Case postale 240
CH-1211 Genève 24

(Current address:
The Institute for Advanced Study
School of Mathematics
Princeton, New Jersey 08540, USA)