Comment. Math. Helvetici 63 (1988) 209–225 0010-2571/88/020209-17$01.50+0.20/0

Maximal hermitian forms over $\mathbb{Z}G$

JORGE F. MORALES

0. Introduction

Let G be a finite group and let V denote a representation of G over the field of rational numbers. It is a standard fact that V admits a symmetric nondegenerate bilinear form $B: V \times V \to \mathbb{Q}$ invariant under G. Let B be such a form on V and let L be a full $\mathbb{Z}G$-lattice in V. We denote by L_B^* the dual lattice of L with respect to B, that is

$$L_B^* = \{x \in V : B(x, L) \subset \mathbb{Z}\}$$

A full $\mathbb{Z}G$-lattice L is said to be *integral* with respect to B if the form B takes integral values on L, or equivalently, if L is contained in L_B^*. We define the *minimal discriminant* of (V, B) to be the positive integer

$$d_B(V) = \min_L \,[L_B^* : L]$$

where L runs over all full $\mathbb{Z}G$-lattices of V integral with respect to B.

We define the *absolute minimal discriminant* of V to be the integer

$$d(V) = \min_B d_B(V)$$

where B runs over all symmetric nondegenerate G-invariant bilinear forms on V. Clearly $d(V)$ depends only on the representation V and is a measure of the extent to which V fails to admit a self-dual $\mathbb{Z}G$-lattice. If V is a permutation representation, obviously $d(V) = 1$. If V is an absolutely simple representation of G, it follows from a theorem of W. Feit (see [F] Thm. 3.2) that the prime divisors of $d(V)$ divide $|G|$.

In Section 1 we show that for a given form B, the set of lattices of V realizing the minimal discriminant $d_B(V)$ has a natural structure of a connected graph. In the case where V is absolutely simple, this graph is finite.

In Section 2 we consider the case where G is a p-group and V is a simple representation of G over $\mathbb{Q}$. We show that in this case the absolute minimal discriminant $d(V)$ is equal to p. We give a lower bound for the number of distinct (i.e. non equivariantly isometric) lattices realizing the minimal discriminant in terms of class numbers of cyclotomic fields. Under slightly more restrictive hypothesis, we show that the lattices with minimal discriminant are (non canonically) in 1–1 correspondance with an ideal class group. We show that all the maximal lattices in V belong to the same genus if and only if the cohomological condition $H^1(G, L) \cong \mathbb{F}_p$ is verified by some maximal lattice L. Finally, to illustrate this result, we define G to be the semidirect product of C_p by $C_p \times C_p$ and V to be the unique simple nonabelian representation of this group over $\mathbb{Q}$. In this example V contains only one genus of maximal lattices for $p = 3$ and at least $(p+1)$ genera for $p \geq 5$.

1. The graph of lattices with minimal discriminant

In this section G will denote a finite group, V a representation of G over $\mathbb{Q}$ and $B: V \times V \to \mathbb{Q}$ a symmetric nondegenerate G-form on V.

DEFINITION. A full $\mathbb{Z}G$-lattice L in V, integral with respect to B, is maximal if it is not properly contained in any full $\mathbb{Z}G$-lattice integral with respect to B.

(1.1) LEMMA. *The following properties are equivalent*

a) $[L_B^*: L] = d_B(V)$
b) *L is maximal*
c) *The associated torsion form $(L_B^*/L, B)$ is anisotropic (i.e. does not admit any non zero totally isotropic subgroup preserved by G).*

Proof. Clearly a)$\Rightarrow$b)$\Rightarrow$c). To see that c)$\Rightarrow$a) we recall that the weak Witt class of $(L_B^*/L, B)$ as a torsion G-form is independent of the choice of L and has a unique anisotropic representative (see for instance [Sch] Chapter 5 and Chapter 7 Section 5). Let M be an integral $\mathbb{Z}G$-lattice with $[M_B^*: M] = d_B(V)$. The torsion form $(M_B^*/M, B)$ is also anisotropic and lies in the same weak Witt class as $(L_B^*/L, B)$. By uniqueness of the anisotropic representative, they are actually isometric. In particular, the underlying finite $\mathbb{Z}G$-modules both have the same order. $\square$

(1.2) LEMMA. *Let L be a maximal integral $\mathbb{Z}G$-lattice. Then L_B^*/L is a semi-simple $\mathbb{Z}G$-module.*

Proof. Let $X \subset L_B^*/L$ be the intersection of all maximal sub $\mathbb{Z}G$-modules of L_B^*/L (i.e. the radical of L_B^*/L). Let $X^\perp$ be the orthogonal complement of X. Since L_B^*/L is anisotropic, we have $X \cap X^\perp = \{0\}$ and therefore $X + X^\perp = L_B^*/L$. By Nakayama's lemma we have $X^\perp = L_B^*/L$ and therefore $X = \{0\}$. □

(1.3) PROPOSITION. *Let L_1 and L_2 be maximal integral $\mathbb{Z}G$-lattices in (V, B). Then we have*

$$\ell(L_1/L_1 \cap L_2) = \ell(L_2/L_1 \cap L_2)$$

where $\ell(X)$ is the length of X as a $\mathbb{Z}G$-module, that is the length of a composition series for X (see [C–R] §3).

Proof. Let $L_1 \cap L_2 = S_0 \subsetneqq S_1 \subsetneqq \cdots \subsetneqq S_n = L_1$ be a composition series. Dualizing this series using the form B we obtain

$$L_1^* + L_2^* = S_0^* \supsetneqq S_1^* \supsetneqq \cdots \supsetneqq S_n^* = L_1^*$$

and intersecting with L_2 we obtain

$$L_2 = S_0^* \cap L_2 \supset S_1^* \cap L_2 \supset \cdots \supset S_n^* \cap L_2 = L_1^* \cap L_2$$

By the maximality of L_1 we have $L_1^* \cap L_2 = L_1 \cap L_2$. On the other hand, the quotient $(S_i^* \cap L_2)/(S_{i+1}^* \cap L_2)$ is naturally embedded in the simple module S_i^*/S_{i+1}^*. Thus $(S_i^* \cap L_2)/(S_{i+1}^* \cap L_2)$ is either 0 or a simple module. Hence,

$$n = \ell(L_1/L_1 \cap L_2) \geq \ell(L_2/L_1 \cap L_2).$$

By symmetry we conclude

$$\ell(L_1/L_1 \cap L_2) = \ell(L_2/L_1 \cap L_2) \quad \square$$

DEFINITION. Let L_1 and L_2 be maximal $\mathbb{Z}G$-lattices in (V, B). We define the distance between L_1 and L_2 by

$$\delta(L_1, L_2) := \ell(L_1/L_1 \cap L_2).$$

Observe that δ is a symmetric function by Proposition 1.3. The lattices L_1 and L_2 are said to be adjacent (or neighbors) if $\delta(L_1, L_2) = 1$. The notion of neighbors (benachbarte Formen) was introduced by M. Kneser (see [K]) for quadratic forms without a group action, and has proved to be a powerful tool for explicit constructions.

The set $\Gamma_B(V)$ of all integral maximal $\mathbb{Z}G$-lattices in V has a natural graph structure. The vertices are the elements of $\Gamma_B(V)$ and two vertices are joined by an edge if they represent adjacent lattices in the sense previously defined.

(1.4) THEOREM. *The graph $\Gamma_B(V)$ is connected.*

Proof. Let L_1 and L_2 be two distinct maximal lattices. By induction, it is enough to show there exists a maximal lattice L such that

$$\delta(L, L_1) = 1 \quad \text{and} \quad \delta(L, L_2) < \delta(L_1, L_2)$$

The lattices L_1 and L_2 being distinct, the intersection $L_1 \cap L_2$ is contained in a proper sublattice M of L_1, where L_1/M is a simple $\mathbb{Z}G$-module.

We define

$$L := M^* \cap L_2 + M$$

where $M^* = M_B^*$. Clearly L is integral. Let us now compute the index $[L : M^* \cap L_2]$. We have

$$[L : M^* \cap L_2] = [M : M \cap M^* \cap L_2] = [M : M \cap L_2]$$

On the other hand

$$[L_2 : M^* \cap L_2] = [M + L_2^* : L_2^*] = [M : L_2^* \cap M] = [M : L_2 \cap M]$$

(the last equality uses $L_2 \cap M = L_2^* \cap M$ which is a consequence of the maximality of L_2).

Thus we have $[L : M^* \cap L_2] = [L_2 : M^* \cap L_2]$. Consequently $[L^* : L] = [L_2^* : L_2] = d_B(V)$. According to Lemma 1.1 the lattice L is maximal.

Now

$$L \cap L_1 = M^* \cap L_2 \cap L_1 + M = L_2 \cap L_1 + M = M$$

thus

$$\delta(L, L_1) = \ell(L_1/L_1 \cap L) = \ell(L_1/M) = 1.$$

It is left to show that $\delta(L, L_2) < \delta(L_1, L_2)$. We have

$$L \cap L_2 = (M^* \cap L_2 + M) \cap L_2 = M^* \cap L_2$$

Hence

$$\delta(L, L_2) = \ell(L_2/L \cap L_2) = \ell(L_2/M^* \cap L_2) \overset{(1)}{=} \ell((M + L_2^*)/L_2)$$

$$= \ell(M/L_2^* \cap M) \overset{(2)}{=} \ell(M/L_2 \cap M)$$

where (1) uses the fact that a finite module and its character module have the same length and (2) uses the maximality of L_2.

On the other hand we have

$$L_1 \cap L_2 \subset M \cap L_2 \subset M \subsetneqq L_1.$$

Hence,

$$\delta(L_1, L_2) = \ell(L_1/L_1 \cap L_2) > \ell(M/M \cap L_2) = \delta(L, L_2) \quad \square$$

(1.5) THEOREM. *If V is an absolutely simple representation of G, then the graph $\Gamma_B(V)$ is finite and connected.*

Proof. Recall that absolutely simple means $\mathrm{End}_G(V) = \mathbb{Q}$. The lattices in $\Gamma_B(V)$ all have the same discriminant. It follows from this fact and Theorem 1.1 in [M] that $\Gamma_B(V)$ has finitely many orbits under the action of the automorphism group of the G-form (V, B). It remains to show that each orbit is finite. In fact each orbit consists of precisely one lattice: since $\mathrm{End}_G(V) = \mathbb{Q}$, the only G-endomorphisms of V which additionally preserve the form B are 1 and -1, and clearly they preserve any lattice. $\square$

2. The case where G is a p-group

In this section G will be a p-group, where p is an *odd* prime number, and V will be a *faithful* simple $\mathbb{Q}G$-module. The endomorphism field $\mathrm{End}_G(V)$ will be denoted by E.

(2.1) LEMMA. *The endomorphism field E is equal to a cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive p^m-th root of* 1.

Proof. From representation theory (see for instance [H] 14.7b) we know that the center $Z(E)$ of E is equal to the field $\mathbb{Q}(\chi)$, where χ is an absolutely irreducible factor of the character of V. Indeed $\mathbb{Q}(\chi)$ is contained in the cyclotomic field $\mathbb{Q}(\zeta_{p^a})$, where p^a is the exponent of G. Since $E=Z(E)$ by Schilling's Theorem (see [R] Theorem 41.9), E is contained in $\mathbb{Q}(\zeta_{p^a})$.

On the other hand, since G is a p-group, its center $Z(G)$ is nontrivial and since V is faithful, it maps non trivially into the multiplicative group of E, generating a cyclotomic subfield $\mathbb{Q}(\zeta_{p^b})$ of E, where p^b is the exponent of $Z(G)$. The relative Galois group Gal $(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}(\zeta_{p^b}))$ is cyclic of order p^{a-b}. Thus all the intermediate subfields between $\mathbb{Q}(\zeta_{p^a})$ and $\mathbb{Q}(\zeta_{p^b})$ are cyclotomic. So is, in particular, the field E. □

The $\mathbb{Q}G$-module V can be regarded as a vector space over its endomorphism ring E. Furthermore, V can be regarded as an absolutely simple EG-module.

(2.2) LEMMA. *Let $L \subset V$ be a full $\mathbb{Z}G$-lattice and let O_E be the maximal order of E. Then for every prime $q \neq p$ we have*

$$\mathrm{End}_G(L)_q = (O_E)_q$$

Proof. For $q \neq p$, the ring $\mathbb{Z}_qG$ is a maximal order (see [R] Theorem 41.1). Hence $\mathrm{End}_G(L_q)$ is a maximal order as well (see [R] Chap. 21, Exercise 1). Therefore, using the canonical identification $\mathrm{End}_G(L_q) = \mathrm{End}_G(L)_q$, we get the equality $(O_E)_q = \mathrm{End}_G(L)_q$. □

Let $B: V \times V \to \mathbb{Q}$ be a G-invariant symmetric form. It is easy to see that the adjoint involution on $E = \mathrm{End}_G(V)$ is actually complex conjugatation. Let $h: V \times V \to E$ be the unique hermitian form on V such that the following triangle commutes

$$\begin{tikzcd} V \arrow[rr, "ad(B)"] \arrow[dr, "ad(h)"'] & & \mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q}) \\ & \mathrm{Hom}_E(V, E) \arrow[ur, "Tr_{E/\mathbb{Q}}"'] & \end{tikzcd}$$

Clearly h is also G-invariant. Now let L be a full $\mathbb{Z}G$-lattice in V on which B takes integral values. Suppose in addition that $\mathrm{End}_G(L)$ is equal to the maximal order O_E. Then the hermitian form h restricted to L takes values in the co-different $D_{E/\mathbb{Q}}^{-1}$ of $E/\mathbb{Q}$. It is well known that $D_{E/\mathbb{Q}}$ is an odd power of the prime ideal $\mathfrak{p}$ lying above p. The prime ideal $\mathfrak{p}$ is generated by $\alpha = \zeta - \zeta^{-1}$ and therefore $D_{E/\mathbb{Q}} = (\alpha^v)$, where v is an odd power. Let f denote the scaled form $\alpha^v h$, which is indeed skew-hermitian and takes integral values on L.

(2.3) LEMMA. *Let L be a full $O_E G$-lattice in V. Then we have*

a) $L_f^* = L_B^*$
b) *L is integral maximal with respect to B if and only if it is integral maximal with respect to f*

Proof. The proof of Lemma 2.3 is straightforward from the definition of f. □

(2.4) PROPOSITION. *Let $L \subset V$ be a $\mathbb{Z}G$-lattice maximal with respect to B. Then* $\operatorname{ord}_p [L_B^* : L] = 1$.

Proof. Since, by Lemma 1.1, all maximal lattices L have the same index $[L_B^* : L]$, it will be enough, using Lemma 2.3, to prove Proposition 2.4 for a $O_E G$-lattice L in V maximal with respect to f.

Since V is absolutely simple as an EG-module, its dimension over E divides $|G|$ (see for instance [H] Theorem 12.6). It is in particular an odd number (we assumed p odd), consequently

$$\overline{\det(f)} = \det(f^*) = \det(-f) = -\det(f).$$

It is easy to see that an element $x \in E$ with the property $\bar{x} = -x$ has necessarily odd order at the prime ideal $\mathfrak{p}$ of E which lies above p. This applies in particular to $\det(f)$.

Hence

$$\operatorname{ord}_p [L^* : L] = \operatorname{ord}_p (N_{E/\mathbb{Q}}(\det(f)) = \operatorname{ord}_{\mathfrak{p}} (\det(f)) \equiv 1(2)$$

(where L^* is the simplified notation for L_B^* or L_f^*).

On the other hand, L being maximal, the torsion G-form $(L_p^*/L_p, B)$ is anisotropic and the underlying $\mathbb{Z}G$-module is semi-simple (see Lemma 1.2). Since G is a p-group, it acts trivially on semi-simple $\mathbb{Z}_p G$-modules (see [C-R] Theorem 5.24). Therefore $(L_p^*/L_p, B)$ is nothing but an anisotropic quadratic space over $\mathbb{F}_p$. Therefore $\operatorname{ord}_p [L_p^* : L_p] = \dim_{\mathbb{F}_p} (L_p^*/L_p) \leq 2$. But we already know that $\operatorname{ord}_p [L_p^* : L_p]$ is odd. Thus $\operatorname{ord}_p [L_p^* : L_p] = 1$. □

(2.5) COROLLARY. *The discriminant of a full $\mathbb{Z}G$-lattice in V, integral with respect to B, is divisible by p.*

Our next goal is to prove the existence of G-forms on V which admit a full

$\mathbb{Z}G$-lattice with discriminant exactly equal to p. This will prove that the number $d(V)$ defined in Section 1 is equal to p.

The main ingredient in the existence theorem is the following result of Galois cohomology that was kindly communicated to me by P. Conner.

(2.6) PROPOSITION. *Let S be the set containing all the infinite primes of E and the unique finite ramified prime $\mathfrak{p}$. Let $\mathfrak{a}$ be an S-ideal preserved by the involution on E. Then there exists $\lambda \in F := \{x \in E : \bar{x} = x\}$ totally positive and an S-ideal $\mathfrak{b}$ such that $\mathfrak{a} = \lambda N_{E/F}(\mathfrak{b})$.*

Proof. It is enough to prove the proposition for an inert prime ideal $\mathfrak{a}$, the decomposed case being trivial.

Let $\pi = N_{E/F}(\Pi)$, where Π is a generator of $\mathfrak{p}$. The prime element π, being a norm, is totally positive. There is an element $\lambda \in F'$ such that the Hilbert symbol $(\lambda, \pi)_{\mathfrak{q}} = -1$ for $\mathfrak{q} = \mathfrak{a}$ or $\mathfrak{q} = (\pi)$ and $(\lambda, \pi)_{\mathfrak{q}} = 1$ otherwise (see for instance [O] Theorem 71.19). We claim that λ has the required properties. By definition λ is a norm locally at all primes except $\mathfrak{a}$ and (π). It is in particular totally positive. The prime $\mathfrak{a}$ being inert, we have the isomorphism (see [S] Chap. V, Prop. 3)

$$\mathrm{ord}_{\mathfrak{a}} : \hat{H}^0(\mathrm{Gal}\,(E_{\mathfrak{a}}/F_{\mathfrak{a}}), E_{\mathfrak{a}}^{\cdot}) \to \mathbb{Z}/2\mathbb{Z}.$$

By construction, λ is not a norm in $E_{\mathfrak{a}}$, therefore $\mathrm{ord}_{\mathfrak{a}}(\lambda) \equiv 1(2)$. Hence $\lambda^{-1}\mathfrak{a}$ is locally a norm at all S-primes, i.e. $\lambda^{-1}\mathfrak{a} = N_{E/F}(\mathfrak{b})$ for some S-ideal $\mathfrak{b}$. □

(2.7) THEOREM. *Let R denote the ring $\mathbb{Z}[p^{-1}]$. There exists a symmetric G-form $B : V \times V \to \mathbb{Q}$ which admits a unimodular RG-lattice M. Furthermore, B can be chosen to be positive definite and is the only (up to equivariant isometry) positive definite G-form on V admitting a unimodular RG-lattice.*

Proof. Let S be the set of all ramified primes of E. The ring O_S of S-integers of E is precisely the integral closure of R in E. The RG-lattices in V can be, by lemma 2.2, regarded as O_SG-lattices.

We observe first that any two RG-lattices M and N are ideal-equivalent, that is, there exists an S-ideal $\mathfrak{a}$ of E such that $\mathfrak{a}M = N$. Notice that if such an ideal exists, it is uniquely determined by $\mathfrak{a} = \mathrm{Hom}_{RG}(M, N)$. Let us define $\mathfrak{a} = \mathrm{Hom}_{RG}(M, N)$ and show $\mathfrak{a}M = N$.

Since the order RG is maximal (see [C] Theorem 41.1), M is projective as an RG-module, that is the functor $\mathrm{Hom}_{RG}(M, -)$ is exact. By applying it to the exact sequence

$$0 \to \mathfrak{a}M \to N \to N/\mathfrak{a}M \to 0$$

we obtain

$$0 \to \mathfrak{a} \to \mathfrak{a} \to \mathrm{Hom}_{RG}(M, N/\mathfrak{a}M) \to 0$$

where the map $\mathfrak{a} \to \mathfrak{a}$ is the identity. Therefore $\mathrm{Hom}_{RG}(M, N/\mathfrak{a}M) = 0$. The projectivity of M implies immediately $N/\mathfrak{a}M = 0$.

Let $C: V \times V \to \mathbb{Q}$ be a positive definite G-form on V and N any RG-lattice in V. Let $\mathfrak{a}$ be the S-ideal $\mathrm{Hom}_{RG}(N, N_C^*)$. The ideal $\mathfrak{a}$ is by construction preserved by the involution in E. By Proposition 2.6 there exists $\lambda \in F^{\cdot}$ totally positive and an S-ideal $\mathfrak{b}$ such that $\mathfrak{a} = \lambda \mathfrak{b}\bar{\mathfrak{b}}$.

Let $M = \mathfrak{b}N$ and $B(x, y) = C(\lambda x, y)$. We have

$$M_B^* = \lambda^{-1} M_C^* = \lambda^{-1}(\bar{\mathfrak{b}})^{-1} N_C^* = \lambda^{-1}(\bar{\mathfrak{b}})^{-1}\mathfrak{a}N = \mathfrak{b}N = M$$

Thus M is unimodular with respect to B. Since λ has been chosen totally positive and C positive definite, the form $B(x, y) = C(\lambda x, y)$ is positive definite as well.

Let us now prove the uniqueness of B. Let B' be another positive definite G-form on V which also admits a unimodular RG-lattice. Since V is a simple representation there exists $\mu \in F^{\cdot}$ such that $B'(x, y) = B(\mu x, y)$. Clearly μ is totally positive and therefore it is a norm at all infinite primes. Let $h: V \times V \to E$ be the hermitian form canonically associated to B. The scaled form μh is indeed the hermitian form corresponding to B'. Since h and μh both admit unimodular $O_S G$-lattices, $\det(h)$ and $\det(\mu h) = \mu^{[V:E]} \det(h)$ are both S-units modulo the norms. Since $[V:E]$ is odd, this implies that μ is a S-unit modulo the norms. We can therefore assume that μ is a S-unit.

We want now to show that μ is a norm everywhere locally. If $\mathfrak{q}$ is an inert prime of F, the units of $F_{\mathfrak{q}}$ are all norms from $E_{\mathfrak{q}}$ (see [S] Proposition 3 and Corollary), thus μ is a norm at $\mathfrak{q}$. If $\mathfrak{q}$ is a decomposed prime, everything is a norm from $E_{\mathfrak{q}}$. Thus μ is a norm at all unramified primes and at the infinite primes. By Hilbert's Reciprocity Theorem, μ is also a norm at the unique ramified finite prime. We conclude by Hasse's Norm Theorem that μ is a global norm, that is, there exists $\alpha \in E'$ such that $\mu = \alpha\bar{\alpha}$. Indeed $B'(x, y) = B(\mu x, y) = B(\alpha x, \alpha y)$. □

DEFINITION. *Let $C: V \times V \to \mathbb{Q}$ be a G-form and $B: V \times V \to \mathbb{Q}$ a positive definite G-form. We know that $C(x, y) = B(\lambda x, y)$ for some $\lambda \in F^{\cdot}$. We define the G-signature $s_G(C)$ of C as the signature of λ (that is, the collection of signs for the various embeddings of F in $\mathbb{R}$). Clearly this definition is independent of the choice of B.*

(2.8) THEOREM. *For a given signature $s=(s_v)$ there exists a unique (up to equivariant isometry) G-form C with $s_G(C)=s$ which admits an integral $\mathbb{Z}G$-lattice of discriminant equal to p.*

Proof. Note that the element $\lambda \in F$ of Proposition 2.6 can be chosen with any prescribed signature. It follows from this observation and from the proof of Theorem 2.7 that there exists a unique (up to equivariant isometry) G-form C on V with $s_G(C)=s$ which in addition admits a unimodular RG-lattice M. To construct a $\mathbb{Z}G$-lattice L of discriminant p from M, we take a maximal $\mathbb{Z}_pG$-lattice $N \subset V_p$ and define $L =: N \cap M$. The lattice L constructed in this way will have discriminant p in virtue of Proposition 2.4. □

Our next goal is to describe (up to equivariant isometry) the $\mathbb{Z}G$-lattices in V integral with discriminant p for a given form B on V.

Let $I^1(E)$ denote the group of ideals $\mathfrak{a}$ of E satisfying $\mathfrak{a}\bar{\mathfrak{a}}=O_E$. Notice that such an ideal does not contain any ramification. Let $P^1(E)$ denote the group of principal ideals (a) with $a\bar{a}=1$.

(2.9) THEOREM. *Let $B: V \times V \to \mathbb{Q}$ be a G-form on V which admits a $\mathbb{Z}G$-lattice $L \subset V$ with discriminant p. Then*

a) *The group $I^1(E)/P^1(E)$ acts freely on the set of isomorphism classes of lattices in the genus of L.*
b) *If in addition $\mathrm{End}_{\mathbb{Z}G}(L)=O_E$ then the action of $I^1(E)/P^1(E)$ on the set of isomorphism classes of lattices in the genus of L is transitive.*

Proof. a) Let $L \subset V$ be a maximal integral $\mathbb{Z}G$-lattice in V. As in the proof of Theorem 2.7, we denote by O_S the ring of S-integers of E, where S is the finite set of ramified primes. We denote by L_S the tensor product $L \otimes \mathbb{Z}[p^{-1}]$, which is, by Lemma 2.2, an O_SG-lattice. For $\mathfrak{a} \in I^1(E)$ we define $\mathfrak{a}L$ as the unique $\mathbb{Z}G$-lattice in V such that $(\mathfrak{a}L)_S=\mathfrak{a}L_S$ and $(\mathfrak{a}L)_p=L_p$. To show that $\mathfrak{a}L$ has discriminant p, it is enough to check that $\mathfrak{a}L_S$ is unimodular:

$$(\mathfrak{a}L_S)^*_B=(\bar{\mathfrak{a}})^{-1}(L_S)^*_B=(\bar{\mathfrak{a}})^{-1}L_S=\mathfrak{a}L_S$$

Since $\mathfrak{a}$ does not contain any ramification, $\mathfrak{a}$ is generated at a given prime $\mathfrak{q}$ by an element $a \in E_{\mathfrak{q}}$ satisfying $a\bar{a}=1$. Therefore L and $\mathfrak{a}L$ belong to the same genus.

If $L \cong \mathfrak{a}L$, there exists $\alpha \in E^{\cdot}$ such that $\alpha\bar{\alpha}=1$ and $\alpha L=\mathfrak{a}L$. Thus $\mathfrak{a}O_S=$

αO_S. On the other hand, neither α nor $\mathfrak{a}$ contain any ramification, therefore $\mathfrak{a} = \alpha O_E$. Hence $I^1(E)/P^1(E)$ acts freely on the classes.

b) Assume now that $\mathrm{End}_{\mathbb{Z}G}(L) = O_E$ and let L' be another lattice in the genus of L.

Observe first that $L_p = L'_p$: let $a \in E_p = E_\mathfrak{p}$ such that $a\bar{a} = 1$ and $aL_p = L'_p$. The isometry a is necessarily a $\mathfrak{p}$-unit, and, since L_p is preserved by $O_{E_\mathfrak{p}}$, we must have $aL_p = L_p$.

On the other hand, from the proof of Theorem 2.7, we know that there exist an S-ideal $\mathfrak{a}$ such that $\mathfrak{a}L_S = L'_S$. But we also have $L_p = L'_p$, therefore $\mathfrak{a}L = L'$. Thus $I^1(E)$ acts transitively on the genus of L. □

(2.10) COROLLARY. a) *The number of classes in the genus of L is divisible by the relative class number $h(E)/h(F)$ of E/F.*

b) *If in addition* $\mathrm{End}_{\mathbb{Z}G}(L) = O_E$, *then the number of classes in the genus of L is equal to the relative class number $h(E)/h(F)$.*

Proof. I owe the following observation to *P.* Conner: let $C(E)$ and $C(F)$ denote the ideal class group of E and F respectively. Let $N_{E/F}: C(E) \to C(F)$ be the norm map. We have an exact sequence

$$0 \to \hat{H}^0(\mathrm{Gal}(E/F), C(E)) \xrightarrow{i} I^1(E)/P^1(E) \xrightarrow{\varphi} \mathrm{Ker}\, N_{E/F}$$

$$\xrightarrow{j} H^1(\mathrm{Gal}(E/F), C(E)) \to 0$$

where φ is induced by the restriction of the canonical projection $I(E) \to C(E)$; the homomorphism i is defined by $i[\mathfrak{a}] = [\mathfrak{a}]$ and the homomorphism j is defined by $j[\mathfrak{b}] = [\mathfrak{b}\bar{\mathfrak{b}}^{-1}]$, the brackets being interpreted as classes in the appropriate group. The verification of exactness is routine. On the other hand, the Herbrand quotient of a finite module is equal to 1 (see [S], Chap. VIII Proposition 8), this applies in particular to $C(E)$. Hence, by exactness, $I^1(E)/P^1(E)$ and $\mathrm{Ker}\, N_{E/F}$ have the same order. It is well known that $N_{E/F}: C(E) \to C(F)$ is surjective (see for instance [W] Theorem 10.1); therefore $[I^1(E): P^1(E)] = h(E)/h(F)$. Corollary 2.10 follows immediately from Theorem 2.9 and this observation. □

Remark. The order of $I^1(E)/P^1(E)$ was calculated with the help of the mass formula in [M] Corollary 3.10. E. Bayer carried out similar calculations for more general fields in [B1].

We want next to estimate the number of genera of maximal integral $\mathbb{Z}G$-lattices contained in V. In order to prove our main result in this direction (Theorem 2.12), we need the following technical lemma:

(2.11) LEMMA. *Let τ be a generator of C_p and T a $\mathbb{F}_p C_p$-module of dimension 3 over $\mathbb{F}_p$ such that C_p preserves a nondegenerate quadratic form on T. Then either T is C_p-trivial or T is isomorphic to $\mathbb{F}_p[t]/(t-1)^3$, where the generator τ of C_p acts by multiplication by t.*

Proof. By the classification of the $\mathbb{F}_p C_p$-modules, we may assume that T^G has dimension at least 2 over $\mathbb{F}_p$ (otherwise T would be indecomposable and therefore isomorphic to $\mathbb{F}_p[t]/(t-1)^3$). Since in this case T^G cannot be totally isotropic, we choose an anisotropic vector $x \in T^G$. Thus we have an orthogonal decomposition

$$T \cong \mathbb{F}_p x \perp (\mathbb{F}_p x)^{\perp}$$

On the other hand, p does not divide the order of the orthogonal group of a quadratic form of rank 2 over $\mathbb{F}_p$ (see [C] 1.4). Therefore, the second factor $(\mathbb{F}_p x)^{\perp}$ is also C_p-trivial. □

(2.12) THEOREM. *The following conditions are equivalent:*

a) *All the maximal $\mathbb{Z}G$-lattices $L \subset V$ satisfy $H^1(G, L) \cong \mathbb{F}_p$*
b) *There exists a maximal $\mathbb{Z}G$-lattice $L \subset V$ such that $H^1(G, L) \cong \mathbb{F}_p$*
c) *All the maximal $\mathbb{Z}G$-lattices of V belong to the same equivariant genus*

Proof. a)⇒b) is obvious.

b)⇒c). Let $L \subset V$ be a maximal $\mathbb{Z}G$-lattice satisfying condition b). Let L' be another maximal $\mathbb{Z}G$-lattice. We know (proof of Theorem 2.7) that L and L' are ideal-equivalent over the S-integers O_S, that is, there is an S-ideal $\mathfrak{a}$ such that $\mathfrak{a}L'_S = L_S$. It is easy to see that $\mathfrak{a}$ must verify $\mathfrak{a}\bar{\mathfrak{a}} = O_S$ and to check that $L'_q \cong L_q$ for all $q \neq p$. It is then enough to prove that L_p is the only maximal $\mathbb{Z}_p G$-lattice in V_p.

We have $H^1(G, L) = (V/L)^G$ from the cohomology exact sequence associated to $0 \to L \to V \to V/L \to 0$. On the other hand, $(V/L)^G = (I_G L^*)^*/L$, where I_G is the augmentation ideal of $\mathbb{Z}G$. Thus $L^*/I_G L^*$ is canonically identified with the character group of $H^1(G, L)$, which is by hypothesis isomorphic to $\mathbb{F}_p$. Therefore $I_G L^*$ has index p in L^*.

By connectivity of the graph of lattices in V_p (Theorem 1.4 is clearly also valid locally), we may assume $\delta(L'_p, L_p) \leq 1$. With this hypothesis we have $I_G L_p^* \subset L_p'^*$. Since $I_G L_p^*$ is contained in L_p and has index p in L^*, we have $I_G L_p^* = L_p$. Therefore $L_p \subset L_p'^*$. By maximality of L'_p, we conclude $L_p \subset L'_p$ and by maximality of L_p we get the equality $L_p = L'_p$.

c)⇒b). Suppose that for all maximal $\mathbb{Z}G$-lattices L we have $|H^1(G, L)| \geq p^2$.

Let L be a maximal O_EG-lattice. Then there exists a O_EG-lattice M with $I_GL^* \subset M \subset L$ and $[M:L] = p$. We will show that M^*/M is a trivial $\mathbb{Z}G$-module. We have

$$I_GM^* \subset I_G(I_GL^*)^* \subset L$$

Therefore the order of $(M^*/M)^G$ is at least p^2. Let ζ be a generator of the image of $Z(G)$ in E, which is a nontrivial root of 1. We have

$$pM^* \subset (\zeta - 1)^2M^* \subset I_G^2M^* \subset I_GL \subset M.$$

Therefore $T := M^*/M$ is a $\mathbb{F}_pG$-module of dimension 3. It is well known from the order of the finite classic groups (see for instance [C] 1.4) that the p-subgroup of the orthogonal group of a quadratic form of rank 3 over $\mathbb{F}_p$ is cyclic of order p. Hence the action of G on T factors through a cyclic quotient of order p of G. According to Lemma 2.11, since $\dim_{\mathbb{F}_p}(T^G) \geq 2$ and T has a quadratic form preserved by G, T must be G-trivial. A quadratic space of dim 3 over $\mathbb{F}_p$ has $(p+1)$ isotropic sub-spaces of dimension 1, each one of them corresponding to a maximal lattice N with $M \subset N \subset M^*$. They belong indeed to different genera.

c)$\Rightarrow$a). The cohomology $H^*(G, L)$ depends only on the local component L_p of L. It is therefore in particular an invariant of the genus of L. On the other hand, according to c)$\Rightarrow$b), we know that $H^1(G, L) = \mathbb{F}_p$ for some maximal $\mathbb{Z}G$-lattice L. □

(2.13) COROLLARY. *If G is cyclic, then V contains only one genus of maximal $\mathbb{Z}G$-lattices.*

Proof. In this case V has dimension 1 over E and a $\mathbb{Z}G$-lattice L in V can be identified with an ideal of E. Let $\zeta \in E$ be the image in E of a generator of G. Clearly ζ is a root of 1 and generates E over $\mathbb{Q}$. Then we have $H^1(G, L) = L/(\zeta - 1)L \cong \mathbb{F}_p$. We apply Theorem 2.12. □

(2.14) LEMMA. *Let H be the group $C_p \times C_p$ with generators x and y. Let G be the semi-direct product $G = C_p \tilde{\times} (C_p \times C_p)$ which admits a presentation*

$$G = \langle x, y, t \mid x^p = y^p = t^p = [x, y] = [x, t] = 1, \quad [t, y] = x \rangle$$

Let E be the cyclotomic field $\mathbb{Q}(\zeta_p)$ and U be the representation of H over $\mathbb{Q}$ defined by $U = E$ as a $\mathbb{Q}$-vector space and $xu = \zeta_p u$ and $yu = u$. Then the induced representation $V = \mathrm{Ind}_H^G(U)$ is simple and is the only nonabelian simple repre-

sentation of G *(by nonabelian representation we mean a representation on which the commutator subgroup* $[G, G]$ *does not act trivially).*

Proof. By definition V has a decomposition

$$V = U \oplus tU \oplus \cdots \oplus t^{p-1}U.$$

It is easy to check that t^iU and t^jU are nonisomorphic simple $\mathbb{Q}H$-modules for $i \neq j$. Thus, by Frobenius Reciprocity, we obtain

$$\mathrm{End}_G(V) \cong \mathrm{Hom}_H(U, V) \cong E$$

Therefore V is simple. By Wedderburn's Theorem, the algebra $\mathbb{Q}G^{ab} \times M_p(E)$ splits off the group algebra $\mathbb{Q}G$. It is easy to check from the presentation of G that $G^{ab} \cong C_p \times C_p$. Thus both $\mathbb{Q}G^{ab} \times M_p(E)$ and $\mathbb{Q}G$ have dimension p^3 over $\mathbb{Q}$ and therefore are equal. Hence V is the only nonabelian simple representation of G. It can also be checked that V is faithful. □

(2.15) PROPOSITION. *Let* G *and* V *as in Lemma* 2.14 *and let* $B: V \times V \to \mathbb{Q}$ *be a* G*-invariant form. Then* V *contains only one genus of maximal* $\mathbb{Z}G$*-lattices for* $p = 3$ *and* V *contains at least* $(p+1)$ *distinct genera of maximal* $\mathbb{Z}G$*-lattices for* $p \geq 5$.

Proof. Let U be the $\mathbb{Q}H$-module defined in Lemma 2.14. Clearly the decomposition $V = U \oplus tU \oplus \cdots \oplus t^{p-1}U$ is orthogonal. Let $L \subset U$ be a maximal $\mathbb{Z}H$-lattice and $M \supset \mathrm{Ind}_H^G(L)$ be a maximal $\mathbb{Z}G$-lattice of V. By Theorem 2.12, it will be enough to prove that $H^1(G, M) = \mathbb{F}_p$ for $p = 3$ and $H^1(G, M) = \mathbb{F}_p \oplus \mathbb{F}_p$ for $p \geq 5$.

Let $N = \mathrm{Ind}_H^G(L)$ and consider the following cohomology diagram associated to the chain $N \subset M \subset M^* \subset N^*$

$$\begin{tikzcd}
 & & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & & (N^*/M)^G \arrow[r, equal] \arrow[d] & (N^*/M)^G \arrow[d] & \\
0 \arrow[r] & (M/N)^G \arrow[r] \arrow[d, equal] & H^1(G, N) \arrow[r] \arrow[d, equal] & H^1(G, M) \arrow[r] \arrow[d] & H^1(G, M/N) \arrow[r] \arrow[d] & H^2(G, N) \arrow[d, equal] \\
0 \arrow[r] & (N^*/N)^G \arrow[r] & H^1(G, N) \arrow[r] & H^1(G, N^*) \arrow[r] & H^1(G, N^*/N) \arrow[r] & H^2(G, N)
\end{tikzcd}$$

Note that by construction $(N^*/N)_p \cong \mathrm{Ind}_H^G(L^*/L)_p \cong \mathrm{Ind}_H^G(\mathbb{F}_p) \cong \mathbb{F}_pG/H \cong \mathbb{F}_cC_p$. Thus $(M/N)_p^G = (N^*/N)_p^G = \mathbb{F}_p$. On the other hand we have $H^1(G, N) \cong H^1(H, L)$ (see [S] Chap. V Section 5). A straightforward computation shows $H^1(H, L) \cong (\zeta_p - 1)^{-1}L/L \cong \mathbb{F}_p$. Similarly $H^1(G, N^*) \cong H^1(H, L^*) \cong \mathbb{F}_p$. Thus we have a simplified diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] \\
 & \mathbb{F}_p \arrow[r, equal] \arrow[d] & \mathbb{F}_p \arrow[d] \\
0 \arrow[r] & H^1(G, M) \arrow[r] \arrow[d, "\alpha"'] & H^1(G, M/N) \arrow[r] \arrow[d, "\beta"'] & H^2(G, N) \arrow[d, equal] \\
0 \arrow[r] & \mathbb{F}_p \arrow[r] & H^1(G, N^*/N) \arrow[r] & H^2(G, N).
\end{tikzcd}$$

We will show that β is surjective for $p \geq 5$. It will follow from the diagram that α is also surjective. We consider the following inflation-restriction sequences (see [S] Chap. VII Section 6)

$$\begin{tikzcd}
0 \arrow[r] & H^1(G/H, M/N) \arrow[r, "\mathrm{inf}"] & H^1(G, M/N) \arrow[r, "\mathrm{res}"] \arrow[d, "\beta"'] & H^1(H, M^*/N)^{G/H} \arrow[d, "\gamma"'] \\
 & & H^1(G, N^*/N) \arrow[r, "\mathrm{res}"] & H^1(H, N^*/N)^{G/H}
\end{tikzcd}$$

To show that β is surjective, it is enough to show that γ is surjective. The subgroup H acts trivially on both M_p/N_p and N_p^*/N_p, therefore

$$H^1(H, M/N)^{G/H} = \mathrm{Hom}_{G/H}(H, M/N)$$
$$H^1(H, N^*/N)^{G/H} = \mathrm{Hom}_{G/H}(H, N^*/N).$$

Let τ be a generator of $C_p \cong G/H$. We have the following isomorphisms of $\mathbb{F}_pG/H$-modules

$$H \cong \mathbb{F}_p[t]/(t-1)^2$$
$$M_p/N_p \cong \mathbb{F}_p[t]/(t-1)^{(p-1)/2}$$
$$N_p^*/N_p \cong \mathbb{F}_p[t]/(t-1)^p,$$

where the generator τ acts by multiplication by t.

Thus the equality

$$\mathrm{Hom}_{G/H}(H, M/N) = \mathrm{Hom}_{G/H}(H, N^*/N)$$

holds provided $(p-1)/2 \geq 2$. Hence β and α are surjective for $p \geq 5$ and $H^1(G, L) \cong \mathbb{F}_p \oplus \mathbb{F}_p$.

The case $p = 3$ requires a special consideration. We put $\Pi = \zeta_3 - 1$ and consider the exact sequence

$$0 \longrightarrow M \xrightarrow{\Pi} M \longrightarrow M/\Pi M \longrightarrow 0$$

which induces a natural isomorphism $(M/\Pi M)^G \xrightarrow[\cong]{} H^1(G, M)$. We will compute the group $(M/\Pi M)^G$.

By construction $N_p^* \cong O_{E_p}^3$ where the coordinates are permuted cyclically by τ. Indeed M_p is the inverse image of $(N_p^*/N_p)^G$ in N_p^*. Therefore M_p is generated over O_{E_p} by the vectors

$$(1, 1, 1); \qquad (0, \Pi, 0); \qquad (0, 0, \Pi)$$

The matrix of t in this basis is

$$T = \begin{bmatrix} 1 & 0 & \Pi \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}$$

It is elementary to check that the reduction modulo Π of $(T-1)$ has rank 2 over $\mathbb{F}_3$. Therefore

$$H^1(G, M) \cong (M/\Pi M)^G \cong \mathrm{Ker}\,(T-1) \cong \mathbb{F}_3. \quad \square$$

Acknowledgement

The work that has led to this paper began while the author was visiting the University of Goettingen, West Germany, the year 84/85, supported by a post-doctoral fellowship of the Fonds National de la Recherche Scientifique (Switzerland). The author thanks both institutions and his host Professor Martin Kneser.

I am particularly grateful to Professor Pierre Conner whose comments made it possible to give much clearer formulations of many results in Section 2. Special thanks go also to Professor Robert Perlis for his many useful observations.

REFERENCES

[B1] E. BAYER, *Unimodular hermitian and skew hermitian forms*, J. Algebra *74* (1982), 341–372.
[B2] E. BAYER, *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comment. Math. Helvetici *59* (1984) 509–538.
[C] R. W. CARTER, *Simple Groups of Lie Type*, Wiley and Sons, London-New York (1972).
[C–H] P. CONNER and J. HURRELBRINK, *Parity of Class Numbers*, preprint Baton Rouge, 1986.
[C–R] C. W. CURTIS and I. REINER, *Methods of Representation Theory*, vol. I, Wiley and Sons, New York 1981.
[F] W. FEIT, *On integral representations of finite groups*, Proc. London Math. Soc (3) *29* (1974) 633–683.
[H] B. HUPPERT, *Endliche Gruppen I*, Springer-Verlag Berlin-Heidelberg-New York (1967).
[K] M. KNESER, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. *8* (1957), 241–250.
[M] J. MORALES, *Integral Bilinear Forms with a Group Action*, Journal of Algebra *98* (1986) 470–484.
[O] O. T. O'MEARA, *Introduction to quadratic forms*, Grundlehren der Math. Wiss. 117, Springer-Verlag Berlin, Goettingen and Heidelberg (1963).
[Q] H. G. QUEBBEMANN, *Zur Klassification unimodularer Gitter mit Isometrie von Primzahlordnung*, J. Reine angew. Math *306* (1981), 158–170.
[R] I. REINER, *Maximal orders, Academic Press*, London-New York-San Francisco (1975).
[S] J.-P. SERRE, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag Berlin-Heidelberg-New York (1985).
[Sch] W. SCHARLAU, *Quadratic and Hermitian Forms*, Springer-Verlag Berlin-Heidelberg-New York-Tokyo (1985).
[W] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer-Verlag New York-Heidelberg-Berlin (1982).

Dept of Mathematics
Louisiana State University
Baton Rogue, LA 70803
USA

Received August 10, 1986