J. reine angew. Math. **426** (1992), 107—116

Journal für die reine und angewandte Mathematik

On some invariants for systems of quadratic forms over the integers

By *Jorge Morales* at Bâton Rouge

Introduction

Let K be throughout a number field with ring of integers R. This paper deals with systems $S = (M; b_1, b_2, \ldots, b_r)$ consisting of a torsion-free finitely generated R-module M and r nondegenerate (i.e. injective) symmetric homomorphisms $b_i : M \to M^* = \mathrm{Hom}_R(M, R)$. Two such systems $S = (M; b_1, b_2, \ldots, b_r)$ and $S' = (M'; b'_1, b'_2, \ldots, b'_r)$ are said to be *equivalent* if there is an R-isomorphism $f : M \to M'$ such that $f^* b'_i f = b_i$ for $1 \leqq i \leqq r$.

There is a natural construction which associates in a functorial way to every system $S = (M; b_1, b_2, \ldots, b_r)$ a module V_S over the free algebra A on $r-1$ generators over K (see Section 1). We prove that there are only finitely many equivalence classes of systems S having prescribed associated semi-simple A-module V_S and prescribed multivolume (Theorem 1.1). This result is in some sense the best finiteness statement possible: elementary counterexamples show that in general there are infinitely many classes of systems of given module and multivolume if no semi-simplicity is assumed (Remark 1.4).

Section 2 is devoted to the particular case of pairs (i.e. $r = 2$). In addition to the invariants of Section 1 we associate to a pair S an R-order Λ_S in $\mathrm{End}_A(V_S)$. We prove, under some restrictive hypotheses, that the set of equivalence classes of pairs S with prescribed multivolume, module V_S and order Λ_S, admits a transitive action of an abelian group related to the Picard group of Λ_S (Theorem 2.1). This result leads to explicit class-number formulas (Theorem 2.5) and implies in particular the formulas of Hardy and Williams [6] for pairs of binary quadratic forms over $\mathbb{Z}$ (Example 2.7). We also give an explicit criterion for the existence of pairs with given invariants (Theorem 2.6). Finally we develop genus theory for pairs, that is we study pairs under local equivalence at all primes of K. We describe explicitly the genera (Theorem 2.8) and show in particular that if the associated order Λ_S is maximal then each genus contains exactly one equivalence class (Corollary 2.9).

The author thanks the Fonds National Suisse de la Recherche Scientifique for its support, and the Institut des Hautes Études Scientifiques for its hospitality during the writing of this paper.

1. Finiteness

Let $(M; b)$ be a symmetric form over R and write $M = \mathfrak{a}_1 e_1 + \mathfrak{a}_2 e_2 + \cdots + \mathfrak{a}_n e_n$, where $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are nonzero R-ideals and $e_1, \ldots, e_n$ is a K-basis for KM. We recall that the *volume* $\mathfrak{v}(M; b)$ is defined by

$$\mathfrak{v}(M; b) = (\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_n)^2 \det\big(b(e_i, e_j)\big) .$$

The volume is of course independent of the choice of a decomposition for M as sum of ideals (see [9], § 82 E). For a system $S = (M; b_1, \ldots, b_r)$ we denote by $\mathfrak{V}_S$ the r-tuple $\big(\mathfrak{v}(M; b_1), \ldots, \mathfrak{v}(M; b_r)\big)$. This invariant will be called throughout the *multivolume* of S.

Let $A = K\{T_1, \ldots, T_{r-1}\}$ be the free algebra (non-commutative polynomials) in $r-1$ generators $T_1, T_2, \ldots, T_{r-1}$. We associate to $S = (M; b_1, \ldots, b_r)$ an A-module V_S in the following way: $V_S = KM$ as vector spaces and

$$T_i v = b_1^{-1} b_{i+1} v \quad \text{for} \quad 1 \leqq i \leqq r-1 .$$

We leave to the reader to show that the isomorphism class of V_S as an A-module depends solely on the equivalence class of S (see also [10], Chapter 7, Example 11.8).

Let $\mathfrak{V} = (\mathfrak{v}_1, \ldots, \mathfrak{v}_r)$ be a multivolume and V and A-module. We denote by $H(\mathfrak{V}, V)$ the set of equivalence classes of systems $S = (M; b_1, \ldots, b_r)$ with $\mathfrak{V}_S = \mathfrak{V}$ and $V_S \simeq V$. We can now state the main theorem in this section.

(1.1) Theorem. *If V is semi-simple then $H(\mathfrak{V}, V)$ is finite.*

Proof. We first reduce Theorem 1.1 to the case when $R = \mathbb{Z}$. Let $\xi \in R$ be a generator of K as a $\mathbb{Q}$-algebra. Let $s : R \to \mathbb{Z}$ be any non-zero linear form (for instance the trace form). The linear form s induces an isomorphism $s_* : \mathrm{Hom}_K(V, K) \to \mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$ that we use to associate to a system $S = (M; b_1, b_2, \ldots, b_r)$ over R a system $\tilde{S} = (M; \tilde{b}_1, \ldots, \tilde{b}_r, \tilde{b}_{r+1})$ over $\mathbb{Z}$ as follows:

$$\tilde{b}_i = s_* \circ b_i \quad \text{for} \quad 1 \leqq i \leqq r ,$$

$$\tilde{b}_{r+1} = s_* \circ (\beta b_1) .$$

Notice that this construction increases by one the number of forms in the system; this is the trade-off for restricting the ground field down to $\mathbb{Q}$. It follows immediately from the definition of $\tilde{S}$ that the associated module $V_{\tilde{S}}$ over $\mathbb{Q}\{T_1, T_2, \ldots, T_r\}$ is given by $V_{\tilde{S}} = KM$ as $\mathbb{Q}$-vector spaces, and

$$(1) \qquad \begin{aligned} T_i v &= b_1^{-1} b_{i+1} v \quad \text{for} \quad 1 \leqq i \leqq r-1 , \\ T_r v &= \xi v . \end{aligned}$$

Thus $\mathrm{End}(V_{\tilde{S}}) = \mathrm{End}(V_S)$. In particular, if V_S is semi-simple then so is $V_{\tilde{S}}$. Any $\mathbb{Z}$-linear equivalence $\tilde{S} \to \tilde{S}'$ is automatically R-linear, for it must commute with ξ by (1); and therefore it induces an R-linear equivalence $S \to S'$. Consequently it is sufficient to prove Theorem 1.1 for $R = \mathbb{Z}$.

We shall now translate our finiteness statement into the language of linear algebraic groups in order to apply the following ([2], Theorem 6.9).

(1.2) Theorem (Borel-Harish-Chandra). *Let G be a reductive algebraic group defined over $\mathbb{Z}$ and let W be a representation of G defined over $\mathbb{Q}$. Let $L \subset W(\mathbb{Q})$ be a $\mathbb{Z}$-lattice preserved by $G(\mathbb{Z})$* and *$X \subset W(\mathbb{C})$ a closed orbit of $G(\mathbb{C})$. Then $X \cap L$ consists of finitely many $G(\mathbb{Z})$-orbits.*

We take $G = \mathrm{SL}_n$ and $W = (\mathrm{Sym}_n)^r$, where Sym_n denotes the symmetric $n \times n$-matrices. The algebraic group G acts on W by $g \cdot (B_1, \ldots, B_r) = (g^t B_1 g, \ldots, g^t B_r g)$ and this action is obviously defined over $\mathbb{Q}$. Let $d \in \mathbb{Z}^r$ with $d_i \neq 0$ for all i. We define $Y_d = \{(B_1, \ldots, B_r) \in W(C) \mid \det(B_i) = \pm d_i\}$. The group SL_n acts also on M_n^{r-1} by simultaneous conjugation, and the algebraic map

$$f: Y_d \to M_n(\mathbb{C})^{r-1},$$

$$(B_1, B_2, \ldots, B_r) \mapsto (B_1^{-1} B_2, B_1^{-1} B_2, \ldots, B_1^{-1} B_r).$$

is clearly $\mathrm{SL}_n(\mathbb{C})$-equivariant. Let $Z \subset M_n(\mathbb{C})^{r-1}$ be a $\mathrm{SL}_n(\mathbb{C})$-orbit. We want to show that if the module corresponding to Z is semi-simple then $f^{-1}(Z) \cap \mathrm{Sym}_n(\mathbb{Z})^r$ consists of a finite number of $\mathrm{SL}_n(\mathbb{Z})$-orbits; and *a fortiori*, of a finite number of $\mathrm{GL}_n(\mathbb{Z})$-orbits. This is an immediate consequence of Theorem 1.2 provided we know the two following facts:

(a) If the module correspnding to Z is semi-simple then Z is closed in $M_n(\mathbb{C})^{r-1}$.

(b) $f^{-1}(Z)$ consists of finitely many $\mathrm{SL}_n(\mathbb{C})$-orbits.

It is known that an orbit Z in $M_n(\mathbb{C})^{r-1}$ is closed if and only if the associated module is semi-simple (see Kraft's book [7], Kapitel II, 2.7, Satz 2). Hence (a) is settled.

Statement (b) is a relatively straightforward consequence of a general result in the theory of hermitian categories ([10], Chapter 7, Corollary 11.4), which in our particular case reads:

(1.3) Proposition. *The systems of nondegenerate $n \times n$ symmetric matrices $S = (B_1, \ldots, B_r)$ over $\mathbb{C}$ are classified up to $\mathrm{SL}_n(\mathbb{C})$-equivalence by the determinants $\det(B_i)$ and the associated module structure V_S.* □

(1.4) Remark. The semi-simplicity hypothesis in Theorem 1.1 is not superfluous as shown by the following counterexample: Let m be a nonzero integer. We define

$$S_m = \left(\mathbb{Z}^2; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix}\right).$$

Clearly $\mathfrak{B}_{S_m} = \mathfrak{B}_{S_1}$ and $V_{S_m} \simeq V_{S_1}$. Now, it is easy to see that the only automorphisms of the first form over $\mathbb{Z}$ are

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \pm\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix};$$

therefore S_m and S_n cannot be equivalent for $m \neq n$.

(1.5) Remark. Other finiteness statements for systems of quadratic forms can be found in [1], Theorem 4.1 and Theorem 4.2.

2. Pairs of forms

In this section we shall study pairs $S = (M; b_1, b_2)$ of forms over R of arbitrary rank. The invariant V_S defined in the previous section is now given by the conjugacy class of a single automorphism $t = b_1^{-1} b_2$. We shall denote by φ_S its characteristic polynomial.

It is convenient for our purposes in this section to merge the invariants $\mathfrak{V}_S$ and φ_S into a single invariant. We define

$$\Phi_S = \mathfrak{v}(R[T] \oplus_R M; b_1 T - b_2)\,. \tag{2}$$

The invariant Φ_S could be defined alternatively by

$$\Phi_S = \mathfrak{v}(M; b_1)\varphi_S(T)\,. \tag{3}$$

It follows immediately from (3) that $\mathfrak{v}(M; b_1)$ is the "dominant coefficient" of Φ_S and from (2) that $\mathfrak{v}(M; b_2)$ is the "constant term" of Φ_S.

The following hypotheses will be in force from now on:

H_1: φ_S has no multiple factors,

H_2: Φ_S is *primitive*, i.e. it is not divisible by any prime ideal of R.

Hypothesis H_1 is very natural in geometrical terms: it is known that H_1 is equivalent to requiring that the intersection of the quadrics $b_1(x, x) = 0$ and $b_2(x, x) = 0$ in the projective space $\mathbb{P}_{n-1}$ is smooth of codimension 2 (see [3], Remark 1.13.1).

We will see later that hypothesis H_2 can be regarded to some extent as the analogue for pairs of the primitivity hypothesis in Gauss' theory of binary quadratic forms, for its role is to guarantee the invertibility of certain ideals.

Let $E = K[T]/(\varphi(T))$ and let t denote the class of T in E. By virtue of hypothesis H_1, the underlying module $V = KM$ is semi-simple and free of rank one over E (t acting via $b_1^{-1} b_2$). We attach now to S an order in E by

$$\Lambda_S = \{x \in E \mid xM \subseteq M\}\,.$$

It is easy to verify that Λ_S is an invariant of $S = (M; b_1, b_2)$, and that it must contain the order $R[\mathfrak{v}(M; b_1)t]$.

We shall now study for given Φ and Λ the set $H(\Phi, \Lambda)$ of equivalence classes of pairs $S = (M; b_1, b_1)$ such that $\Phi_S = \Phi$ and $\Lambda_S = \Lambda$. By Theorem 1.1 we know *a priori* that $H(\Phi, \Lambda)$ is finite.

Let $\mathfrak{I}(\Lambda)$ be the group of all invertible (i.e. locally free) ideals of Λ. Let $G(\Lambda)$ be the subgroup of $\mathfrak{I}(\Lambda) \times E^*$ given by

$$G(\Lambda) = \{(I, x) \mid I^2 x = \Lambda\}.$$

Let $S = (M; b_1, b_2) \in H(\Phi, \Lambda)$ and let $(I, x) \in G(\Lambda)$. We define

$$(I, x) \cdot (M; b_1, b_2) = (IM; b_1 x, b_2 x). \tag{4}$$

We shall now verify that $S' = (IM; b_1 x, b_2 x)$ is also in $H(\Phi, \Lambda)$. Let $\mathfrak{p}$ be a prime of R and choose a local generator $\alpha_\mathfrak{p} \in I_\mathfrak{p}$. From the definition (2) we have

$$\begin{aligned} \Phi_{S',\mathfrak{p}} &= N_{E/K}(\alpha_\mathfrak{p})^2 N_{E/K}(x) \Phi_{S,\mathfrak{p}} \\ &= N_{E/K}(\alpha_\mathfrak{p}^2 x) \Phi_{S,\mathfrak{p}} \\ &= \Phi_{S,\mathfrak{p}}. \end{aligned}$$

Thus $G(\Lambda)$ acts on $H(\Phi, \Lambda)$. Our main goal is to prove that the action (4) is transitive on $H(\Phi, \Lambda)$. We shall need to assume that Λ is *weakly self-dual.* Following Fröhlich's terminology [5], we shall say that an order Λ is *weakly self-dual* if the dual module

$$\hat{\Lambda} = \{x \in E \mid \mathrm{Tr}_{E/K}(x\Lambda) \subseteqq R\}$$

is locally free over Λ.

Fröhlich ([5], Section 8, Theorem 10) showed that weak self-duality is equivalent to the property that every Λ-module M with $\mathrm{End}_\Lambda(M) = \Lambda$ is locally free. It is actually in the latter form that we shall use this hypothesis. Examples of weakly self-dual orders are maximal orders, or more generally, orders of odd index in the maximal order. Orders generated as R-algebras by a single element are also examples (see [5], Section 8). Thus we shall assume henceforth

H_3: The order Λ is weakly self-dual.

We are now ready to state our main result in this section.

(2.1) Theorem. *Assume* H_1, H_2, *and* H_3. *Then* $G(\Lambda)$ *acts transitively on* $H(\Phi, \Lambda)$.

We need two technical statements in order to prove Theorem 2.1:

(2.2) Lemma. *Let* E/K *be a semi-simple commutative algebra and let* $t \in E^*$. *Let* $\varphi(T)$ *be the minimal polynomial of* t *and* $I = O_E + tO_E$, *where* O_E *is the maximal order of* E. *Then the ideal* $N_{E/K}(I)^{-1} \varphi(T)$ *is primitive in* $R[T]$.

Proof. It is sufficient to prove the lemma locally. Assume that K is a local field. We have two cases:

(a) If either t or t^{-1} is in O_E the lemma is obvious.

(b) If neither t nor t^{-1} is in O_E then there is a splitting $E = E_1 \times E_2$ as K-algebras such that $t = (t_1, t_2)$ with $t_1 \in O_{E_1}$ and $t_2^{-1} \in O_{E_2}$ (here we use that we are in the local case). Let $\varphi_i(T)$ be the minimal polynomial of t_i and let $I_i = O_{E_i} + t_i O_{E_i}$ $(i = 1, 2)$. By (a) the ideal $N_{E_i/K}(I_i)^{-1}\varphi_i(T)$ is primitive for $i = 1, 2$. So must be their product $N_{E/K}(I)^{-1}\phi(T) = \big(N_{E_1/K}(I_1)^{-1}\varphi_1(T)\big)\big(N_{E_2/K}(I_2)^{-1}\varphi_2(T)\big)$ by Gauss Lemma. □

The trace form $\mathrm{Tr}_{E/K}$ induces an isomorphism of Λ-modules $\mathrm{Hom}_\Lambda(M, \hat{\Lambda}) \to \mathrm{Hom}_R(M, R)$. Thus there exists a unique $\beta : M \to \mathrm{Hom}_\Lambda(M, \hat{\Lambda})$ such that $b_1(x, y) = \mathrm{Tr}_{E/K}\big(\beta(x, y)\big)$ and $b_2(x, y) = \mathrm{Tr}_{E/K}\big(t\beta(x, y)\big)$. Since both b_1 and b_2 take integral values on M we must have $\beta(M, M) \subseteq \hat{\Lambda} \cap t^{-1}\hat{\Lambda}$. The following lemma shows that we have in fact equality. To simplify our notation, we set $J = \Lambda + t\Lambda$ (and thus $\hat{J} = \hat{\Lambda} \cap t^{-1}\hat{\Lambda}$).

(2.3) Lemma. *Assume* H_1, H_2 *and* H_3. *Then*

$$\beta(M, M) = \hat{J}.$$

In particular, the ideal J is locally free over Λ.

Proof. Let $N \subseteq M$ be full R-lattices in V. We denote by $(M : N)$ the product $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$, where $R/\mathfrak{p}_i$ $(1 \leq i \leq r)$ are the simple Jordan-Hölder factors of the quotient M/N over R. The symbol $(M : N)$ is obviously a generalization of the usual index and has the same multiplicative properties.

From the sequence of injective maps

$$M \xhookrightarrow{\beta} \mathrm{Hom}_\Lambda(M, \hat{J}) \hookrightarrow \mathrm{Hom}_\Lambda(M, \hat{\Lambda}) \overset{\mathrm{Tr}_{E/K}}{\simeq} \mathrm{Hom}_R(M, R)$$

we deduce

$$\begin{aligned} \mathfrak{v}(M; b_1) &= \big(\mathrm{Hom}_R(M, R) : b_1(M)\big) \\ &= \big(\mathrm{Hom}_\Lambda(M, \hat{J}) : \beta(M)\big)\big(\mathrm{Hom}_\Lambda(M, \hat{\Lambda}) : \mathrm{Hom}_\Lambda(M, \hat{J})\big) \\ &= \big(\hat{J} : \beta(M, M)\big)(\hat{\Lambda} : \hat{J}) \qquad (5) \\ &= \big(\hat{J} : \beta(M, M)\big)(J : \Lambda). \qquad (6) \end{aligned}$$

Notice that (5) uses that M is locally free, which needs hypothesis H_3 as already pointed out. We shall finish the proof by showing that $(J : \Lambda) = \mathfrak{v}(M; b_1)$. On the one hand we have by (6)

$$(J : \Lambda) \supseteq \mathfrak{v}(M; b_1). \qquad (7)$$

On the other hand, by multiplicativity of the index, we have

$$(J : \Lambda)(O_E J : O_E)^{-1} = (O_E : \Lambda)(O_E J : J)^{-1}.$$

The right hand side of this identity is essentially the invariant introduced by Fröhlich [5], Section 5, Corollary 1, as a criterion for local freeness: the ideal $(O_E : \Lambda)(O_E J : J)^{-1}$ is always contained in R and is equal to R if and only if J is locally free (see also [4], Corollary 35.12). Hence, in particular,

$$(J : \Lambda) \subseteq (O_E J : O_E) . \tag{8}$$

Now, by the usual properties of the norm in maximal orders, we also have $(O_E J : O_E)^{-1} = N_{E/K}(O_E J)$. And by Lemma 2.2 we have

$$(O_E J : O_E)\varphi(T) \subseteq R[T] .$$

Thus, using hypothesis H_2 (primitivity), we have

$$(O_E J : O_E) \subseteq \mathfrak{v}(M; b_1) . \tag{9}$$

Finally, combining (8) and (9) we obtain

$$(J : \Lambda) \subseteq \mathfrak{v}(M; b_1)$$

as desired. Thus $(J : \Lambda) = \mathfrak{v}(M; b_1)$ and by (6) $\beta(M, M) = \hat{J}$. It follows immediately from this equality that J is locally free, since M is so. Fröhlich's Criterion [5], Section 5, Corollary 1, could also have been easily applied to prove this fact. □

Proof of Theorem 2.1. To avoid trivial considerations we shall assume that $H(\Phi, \Lambda)$ is not empty. Let $S = (M; b_1, b_2)$ and $S' = (M'; b_1', b_2')$ be representatives of two classes in $H(\Phi, \Lambda)$. With no loss of generality we can assume that M and M' are Λ-lattices in a given E-module V. By hypothesis H_1, V is free of rank one over E. Therefore $\mathrm{End}_E(V) \simeq E$. By definition we have $\Lambda = \mathrm{End}_R(M) \cap E$, therefore $\Lambda = \mathrm{End}_\Lambda(M)$. By weak self-duality, M is projective as Λ-modules and so is of course M'. We must now show the existence of an element (I, x) in $G(\Lambda)$ taking S to S'. Replacing if needed S by an equivalent pair we can assume $b_1^{-1} b_2 = b_1'^{-1} b_2'$. The obvious candidate for (I, x) is $I = \mathrm{Hom}_\Lambda(M, M')$, and $x = b_1^{-1} b_1' = b_2^{-1} b_2'$. Since M is locally free we have $IM = M'$; thus we only need to show that (I, x) belongs to $G(\Lambda)$ i.e. satisfies the condition $xI^2 = \Lambda$. Let $\beta : M \times M \to \hat{\Lambda}$ and $\beta' : M \times M' \to \hat{\Lambda}$ be such that $\mathrm{Tr}_{E/K}(\beta) = b_1$ and $\mathrm{Tr}_{E/K}(\beta') = b_1'$. Using Lemma 2.3 we have

$$\begin{aligned} \beta(M, M) &= \beta'(M', M') \\ &= xI^2 \beta(M, M) . \end{aligned}$$

Thus $xI^2 = \Lambda$ as desired. □

Clearly the kernel of the action defined in (4) is given by

$$G_0(\Lambda) = \{(a^{-1}\Lambda, a^2) \mid a \in E^*\} .$$

We shall see next that the quotient $G(\Lambda)/G_0(\Lambda)$ has a very simple description in terms of the Picard group of Λ. We recall that the *Picard group* of Λ is by definition

$$\mathrm{Pic}(\Lambda) = \mathfrak{J}(\Lambda)/\{a\Lambda \mid a \in E^*\}\,.$$

The following Proposition gives the structure of $G(\Lambda)/G_0(\Lambda)$.

(2.4) Proposition. *Let* ${}_2\mathrm{Pic}(\Lambda)$ *be the subgroup of* $\mathrm{Pic}(\Lambda)$ *of elements of order* $\leqq 2$. *The group* $G(\Lambda)/G_0(\Lambda)$ *is an elementary 2-group and is related to* ${}_2\mathrm{Pic}(\Lambda)$ *by the exact sequence*

$$0 \longrightarrow \Lambda^*/\Lambda^{*2} \xrightarrow{j} G(\Lambda)/G_0(\Lambda) \xrightarrow{k} {}_2\mathrm{Pic}(\Lambda) \longrightarrow 0\,,$$

where Λ^* *is the group of units of* Λ, *the map* j *is given by* $j(u) = (\Lambda, u)$, *and* $k(I, a) = I$.

Proof. The proof of exactness is routine and is left as exercise. Observe that the identity $(I, a)^2 = (I^2, a^2) = (a^{-1}\Lambda, a^2)$ holds for (I, a) in $G(\Lambda)$, which shows that the quotient $G(\Lambda)/G_0(\Lambda)$ is an elementary 2-group. □

An immediate consequence is the following class-number formula:

(2.5) Theorem. (With the same hypotheses and notation of Theorem 2.1). *Let* $h(\Phi, \Lambda)$ *denote the cardinality of the set* $H(\Phi, \Lambda)$. *If* $h(\Phi, \Lambda) \neq 0$ *then we have*

$$h(\Phi, \Lambda) = [\Lambda^* : \Lambda^{*2}]\,|\,{}_2\mathrm{Pic}(\Lambda)|\,.$$

It seems natural to ask whether for given invariants (Φ, Λ) there exists a pair having these invariants, or in other words, whether $h(\Phi, \Lambda) \neq 0$. This is answered by the following theorem. As in Lemma 2.3 we set $J = \Lambda + t\Lambda$.

(2.6) Theorem. *Assume* $\mathrm{H}_1, \mathrm{H}_2$ *and* H_3. *There exists a pair with invariants* (Φ, Λ) *if and only if* J *is locally free and* $\hat{J}$ *is a square class in the group* $\mathrm{Pic}(\Lambda)$.

Proof. Suppose that there exists a pair $(M; b_1, b_2)$ with the given invariants. Since M is a locally free Λ-module of rank one we can write $M = Iv$, where I is a locally free ideal in E. Thus, by Lemma 2.3, we have

$$I^2\beta(v, v) = \hat{J}\,,$$

which proves that J is locally free and that $\hat{J}$ is a square in $\mathrm{Pic}(\Lambda)$.

Conversely, suppose that $\hat{J} = I^2\beta$ for some $\beta \in E^*$ and some locally free Λ-ideal I. Set $M = I$, $b_1(x, y) = \mathrm{Tr}_{E/K}(\beta xy)$, $b_2(x, y) = \mathrm{Tr}_{E/K}(t\beta xy)$ and $S = (M; b_1, b_2)$. We must check that Φ_S is primitive. On the one hand, by (6), we have $\Phi_S = (J : \Lambda)\varphi$. On the other hand, since J is locally free, we have $(J : \Lambda) = N_{E/K}(O_E J)^{-1}$. According to Lemma 2.2, Φ_S is primitive as desired. □

A very interesting example of application of Theorems 2.5 and 2.6 is the case of pairs of binary quadratic forms over $\mathbb{Z}$. This case was studied in detail in a separate article [8] and inspired the general theory contained in this paper. We shall only quote here without proofs some of the computationally explicit results that can be obtained applying Theorems 2.5 and 2.6 in this case. We refer to [8] for details. There are some minor differences in our approach

in [8] and the approach here: in [8] we fix the actual determinants δ_1 and δ_2 whereas in this paper we prescribe only the ideals they generate in $\mathbb{Z}$. In [8] we consider $\mathrm{SL}_2(\mathbb{Z})$-equivalence, while here we use $\mathrm{GL}_2(\mathbb{Z})$-equivalence. The results quoted below have been adjusted to our present viewpoint.

(2.7) Example. Take $R = \mathbb{Z}$ and $n = 2$. We write

$$\Phi = (\delta_1 T^2 + \Delta T + \delta_2)\mathbb{Z}[T],$$

where δ_1, δ_2, Δ are in $\mathbb{Z}$. We shall assume H_1, i.e. $\Delta^2 - 4\delta_1\delta_2 \neq 0$ and H_2, i.e. $\gcd(\delta_1, \delta_2, \Delta) = 1$. Notice that in the quadratic case H_3 is always satisfied. Under some minor further technical restrictions on $\delta_1, \delta_2, \Delta$ (see [8], Theorem 3.5) and assuming also for simplicity that O_E does not contain a unit of norm -1, we have

$$h(\Phi, \Delta) = c \sum_{\substack{n \mid \mathrm{disc}(\Delta) \\ n \text{ square free}}} \left\{\left(\frac{\delta_1}{n}\right) + \left(\frac{-\delta_1}{n}\right)\right\},$$

where $c = 1$ if $\mathrm{disc}(O_E) > 0$ and $c = 1/2$ otherwise. As usual $(-)$ denotes the Jacobi symbol. Taking the sum over all possible Δ (recall that $\Delta \supseteq \mathbb{Z}[\delta_1 t]$) we obtain a formula for the number $h(\Phi)$ of classes of pairs of forms with invariant Φ.

$$h(\Phi) = \sum_{\mathbb{Z}[\delta_1 t] \subseteq \Delta \subseteq O_E} h(\Phi, \Delta) \tag{11}$$

$$= c \sum_{n \mid D} \left\{\left(\frac{\delta_1}{n}\right) + \left(\frac{-\delta_1}{n}\right)\right\},$$

where $D = \mathrm{disc}(\mathbb{Z}[\delta_1 t]) = \Delta^2 - 4\delta_1\delta_2$. The equality (11) is essentially the Hardy-Williams class-number formula [6]. □

To complete our view of the problem we shall now study genus-equivalence of pairs of forms. Two pairs are said to be in the *same genus* if they are locally equivalent at all primes. All the invariants that we have defined are obviously genus invariants. In view of Theorem 2.1 it is natural to expect that there is a subgroup $G^{\mathrm{gen}}(\Delta)$ of the group $G(\Delta)$ that acts transitively on the set of classes in a given genus. We define

$$G^{\mathrm{gen}}(\Delta) = \{(I, 1) \in G(\Delta) \mid I_{\mathfrak{p}} = \varepsilon_{\mathfrak{p}} \Delta_{\mathfrak{p}} \text{ with } \varepsilon_{\mathfrak{p}}^2 = 1 \text{ for all } \mathfrak{p}\}. \tag{12}$$

We claim that $G^{\mathrm{gen}}(\Delta)$ has the required property.

(2.8) Theorem. *Assume* H_1, H_2, *and* H_3. *The action of* $G^{\mathrm{gen}}(\Delta)$ *on* $H(\Phi, \Delta)$ *given by* (4) *is transitive on the set of classes belonging to a given genus.*

Proof. Let $S = (M; b_1, b_2)$ and $S' = (M'; b_1', b_2')$ be representatives of classes in $H(\Phi, \Delta)$ in the same genus. According to Theorem 2.1 there exists $(I, x) \in G(\Delta)$ such hat $M' = IM$ and $b_i' = b_i x$. By virtue of our hypothesis, for all primes $\mathfrak{p}$ there exists $u_{\mathfrak{p}} \in E_{\mathfrak{p}}^*$ such that $u_{\mathfrak{p}} M = M'$ and $b_i' = b_i u_{\mathfrak{p}}^2$. Thus $x = u_{\mathfrak{p}}^{-2}$ and therefore x must be a global square, say $x = y^2$ with $y \in E^*$. Hence $u_{\mathfrak{p}} = \varepsilon_{\mathfrak{p}} y^{-1}$, where $\varepsilon_{\mathfrak{p}}^2 = 1$. Let J be the ideal whose

local components are $J_\mathfrak{p} = \varepsilon_\mathfrak{p} \Lambda_\mathfrak{p}$. With these notation we have $(I, x) = (y^{-1}\Lambda, y^2)(J, 1)$. Since $(y^{-1}\Lambda, y^2)$ acts trivially on the classes, this finishes the proof. □

(2.9) Corollary. *Assume* H_1 *and* H_2. *If* Λ *is maximal then each genus contains exactly one class.*

Proof. It follows immediately from the definition (12) that $G^{\mathrm{gen}}(\Lambda) = 1$ if Λ is maximal. □

Finally, we shall give a description of the image of $G^{\mathrm{gen}}(\Lambda)$ in $G(\Lambda)/G_0(\Lambda)$. For any ring B we denote by $\mu_2(B)$ the set of elements $x \in B$ satisfying $x^2 = 1$.

(2.10) Proposition. *There is an exact sequence*

$$\mu_2(E) \prod_\mathfrak{p} \mu_2(\Lambda_\mathfrak{p}) \to \prod_\mathfrak{p} \mu_2(E_\mathfrak{p}) \to G^{\mathrm{gen}}(\Lambda)/G^{\mathrm{gen}}(\Lambda) \cap G_0(\Lambda) \to 0,$$

where the product is taken over all primes $\mathfrak{p}$ *dividing the index* $(O_E : \Lambda)$.

The proof of Proposition 2.10 is straightforward. □

References

[1] *E. Bayer, C. Kearton, S.M.J. Wilson*, Hermitian forms in additive categories: finiteness results, J. Algebra **123(2)** (1989), 336–350.
[2] *A. Borel* and *Harish-Chandra*, Arithmetic subgroups of algebraic groups, Ann. Math. **75** (1962), 485–535.
[3] *J.-L. Colliot-Thélène, J.-J. Sansuc, P. Swinnerton-Dyer*, Intersections of two quadrics and Châtelet surfaces, J. reine angew. Math. **373** (1987), 37–107.
[4] *C.W. Curtis, I. Reiner*, Methods of representation theory I, New York 1981.
[5] *A. Fröhlich*, Invariants for modules over separable algebras, Quart. J. Math. Oxford (2) **16** (1965), 193–232.
[6] *K. Hardy* and *S. Williams*, The class number of pairs of positive-definite binary quadratic forms, Acta Arith. **LII.2** (1989), 103–117.
[7] *H. Kraft*, Geometrische Methode in der Invariantentheorie, Braunschweig 1984.
[8] *J. Morales*, The classification of pairs of binary forms, Acta Arith., to appear.
[9] *O.T. O'Meara*, Introduction to Quadratic Forms, Grundl. math. Wiss. **117**, Berlin–Heidelberg–New York 1963.
[10] *W. Scharlau*, Quadratic and Hermitian Forms, Grundl. math. Wiss. **270**, Berlin–Heidelberg–New York 1985.

Louisiana State University, Department of Mathematics, Bâton Rouge, la 70803–4918, USA

Eingegangen 12. April 1991