If $\varepsilon = (B_1 - R)/B$, we find $h_n \in S_1$, $n = 1, 2, \ldots$, such that (28) holds. It suffices to put $g_{k(n)} = h_n$ $(n = 1, 2, \ldots)$ and (24) is satisfied. The proof of Theorem 3 is complete.

Acknowledgments. I would like to thank Professor A. Schinzel and Professor B. Novák for their encouragement.

References

[1] P. Erdős, *Some problems and results on the irrationality of the sum of infinite series*, J. Math. Sci. 10 (1975), 1–7.
[2] J. Galambos, *Representations of Real Numbers by Infinite Series*, Lecture Notes in Math. 502, Springer, 1976.
[3] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1981.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF OSTRAVA
DVOŘÁKOVA 7
701 03 OSTRAVA 1, CZECHOSLOVAKIA

Received on 12.1.1990
and in revised form on 24.9.1990 (2003)

ACTA ARITHMETICA
LIX.2 (1991)

The classification of pairs of binary quadratic forms

by

JORGE MORALES (Baton Rouge, La.)

Introduction. We consider ordered pairs (Q_1, Q_2) of binary quadratic forms with coefficients in $\boldsymbol{Z}$. In the present paper we classify such pairs up to equivalence, where two pairs of forms (Q_1, Q_2) and (Q_1', Q_2') are said to be *equivalent* if there is a transformation U in $\mathrm{SL}_2(\boldsymbol{Z})$ such that $Q_i(U\boldsymbol{x}) = Q_i'(\boldsymbol{x})$ for $i = 1$, or 2. If Q_1 and Q_2 are linearly dependent then the problem is obviously equivalent to the classification of single forms, which goes back to Gauss' *Disquisitiones Arithmeticae.*

It can be shown (see Appendices I and II) that the number of equivalence classes of pairs with given discriminants δ_1, δ_2 and codiscriminant Δ is finite if and only if $\Delta^2 \neq 4\delta_1\delta_2$. Moreover, the classification of pairs with $\Delta^2 = 4\delta_1\delta_2$ turns out to be elementary (see Appendix II).

Thus the interesting case is when $\Delta^2 \neq 4\delta_1\delta_2$. The classification we will give uses a new invariant, called the *index* and denoted by μ. Our main result is that there is a natural finite group $\mathfrak{G}$ that acts transitively and freely on the set of equivalence classes of pairs with prescribed set of invariants $(\delta_1, \delta_2, \Delta, \mu)$ (see Theorem 1.3 and Corollary 1.5). This approach to classification is illustrated by a numerical example in Appendix IV.

The group $\mathfrak{G}$ turns out to depend solely on the Sylow 2-subgroup of the Picard group of a certain quadratic order. As a consequence, the evaluation of the order of $\mathfrak{G}$ gives an explicit formula for the number of classes of pairs with given invariants $(\delta_1, \delta_2, \Delta, \mu)$. We also obtain the formula for the number of pairs with prescribed $(\delta_1, \delta_2, \Delta)$ found by Hardy and Williams (see [3]) for positive-definite forms with fundamental discriminant.

1. The index of a pair of symmetric forms. Recall that quadratic forms correspond bijectively to even symmetric bilinear forms. In this section we study triples (M, b_1, b_2) where M is an *oriented* free $\boldsymbol{Z}$-module of rank two and b_i: $M \to M^* = \mathrm{Hom}_{\boldsymbol{Z}}(M, \boldsymbol{Z})$ $(i = 1, 2)$ are nondegenerate (i.e. injective) symmetric homomorphisms. We shall say that (M, b_1, b_2) and (N, c_1, c_2) are *equivalent* if there exists an orientation-preserving isomorphism f: $M \to N$ such that $f^* c_i f = b_i$ for $i = 1, 2$, where as usual f^* stands for the dual map of f.

1980 Mathematics Subject Classification: 11D09, 11E41.

Our first task will be to define certain invariants for (M, b_1, b_2). For this, let $\boldsymbol{Q}[T]$ be the polynomial ring in one variable over $\boldsymbol{Q}$. The $\boldsymbol{Q}$-vector space $V_M = \boldsymbol{Q}M$ spanned by M carries the $\boldsymbol{Q}[T]$-module structure given by $Tx = b_1^{-1}b_2(x)$.

1.1. LEMMA. *The isomorphism class of V_M as a $\boldsymbol{Q}[T]$-module depends only on the equivalence class of (M, b_1, b_2).*

Proof. Let $f\colon (M, b_1, b_2) \to (N, c_1, c_2)$ be an equivalence. We check below that the induced map $f\colon V_M \to V_N$ is an isomorphism of $\boldsymbol{Q}[T]$-modules:

$$f(Tx) = (fb_1^{-1}b_2)(x) = (c_1^{-1}f^{*-1}b_2)(x) = (c_1^{-1}c_2 f)(x) = Tf(x). \quad \blacksquare$$

It follows from the lemma that the minimal polynomial $\phi(T)$ of $b_1^{-1}b_2$ is an invariant of the equivalence class of (M, b_1, b_2). By letting $\delta_i = -\det(b_i)$ be the discriminant of b_i we write $\phi(T)$ in the form

$$\phi(T) = T^2 + \frac{\Delta}{\delta_1}T + \frac{\delta_2}{\delta_1}, \tag{1}$$

where Δ is an integer that will be called the *codiscriminant* of the pair (b_1, b_2) (*a word of caution*: our definition of codiscriminant differs from the one given in [3] by a factor 2).

We shall assume from now on that $\phi(T)$ has two distinct roots, or equivalently that $\Delta^2 \neq 4\delta_1\delta_2$. It is shown under this assumption in Appendix I that there are only finitely many equivalence classes with fixed $(\delta_1, \delta_2, \Delta)$.

Let now V be a 2-dimensional oriented $\boldsymbol{Q}$-vector space equipped with a fixed automorphism $t\colon V \to V$ with minimal polynomial $\phi(T)$ as in (1). Let A denote the algebra $\boldsymbol{Q}[T]/(\phi(T))$. The vector space V (respectively V^*) is made into an A-module by setting $Tx = t(x)$ (respectively $Tf = t^*(f)$). In order to describe all (M, b_1, b_2) with given invariants $(\delta_1, \delta_2, \Delta)$ and $M \subset V$ we consider pairs (M, b) satisfying the following conditions:

(a) $M \subset V$ is a $\boldsymbol{Z}$-lattice with $\boldsymbol{Q}M = V$,
(b) $b\colon V \to V^*$ is a symmetric A-isomorphism,
(c) $b(M, M) \subseteqq \boldsymbol{Z}$ and $bt(M, M) \subseteqq \boldsymbol{Z}$,
(d) $\delta(b|_M) = \delta_1$.

Two such pairs (M, b) and (N, c) are said to be *equivalent* if there exists α in the subgroup $A^{\bullet +}$ of units of A with positive norm such that $\alpha M = N$ and $b = c\alpha^2$. Clearly the correspondence

$$(M, b) \mapsto (M, b, bt)$$

is a bijection between the pairs (M, b) satisfying (a)–(d) above and the triples (M, b_1, b_2) with invariants $(\delta_1, \delta_2, \Delta)$. This bijection is evidently compatible with the given equivalence relations.

To describe the equivalence classes of (M, b) we will use some concepts of ideal theory in A. We need an invariant that takes into accout the integral

module structure of M in addition to $\phi(T)$ which gives the rational structure. More precisely, for a lattice $M \subset V$ we will consider its associated order Λ_M in A, which is defined by

$$\Lambda_M = \{\alpha \in A : \alpha M \subseteqq M\},$$

and we will describe all pairs (M, b) with $\Lambda_M = \Lambda$ for a fixed order Λ. Notice in particular that M regarded as a Λ_M-module is projective (see Appendix III, Theorem III.1). We associate with every lattice $M \subset V$ the integer

$$\mu = [O_A : \Lambda_M],$$

where O_A is the maximal $\boldsymbol{Z}$-order in A. The integer μ will be called the *index* of M. To prescribe μ is equivalent to prescribe Λ_M, since orders in quadratic semi-simple algebras are determined by their index in O_A. Notice also that $\boldsymbol{Z}[\delta_1 t]$ is always contained in Λ_M. Thus $\operatorname{disc}(\Lambda_M) = \mu^2 \operatorname{disc}(O_A)$ divides $\operatorname{disc}(\boldsymbol{Z}[\delta_1 t]) = \Delta^2 - 4\delta_1\delta_2$. The following example shows that the index can distinguish pairs that the other invariants cannot.

1.2. EXAMPLE. Set

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 14 & 5 \\ 5 & 4 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 16 & 17 \\ 17 & 20 \end{pmatrix}.$$

By direct computation $\delta(B_1) = \delta(C_1) = -1$, $\delta(B_2) = \delta(C_2) = -31$, and $\Delta(B_1, B_2) = \Delta(C_1, C_2) = 18$. But $\mu(B_1, B_2) = 1$ and $\mu(C_1, C_2) = 5$.

Let $\mathscr{S} = \mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$ be set of equivalence classes of pairs (M, b) satisfying conditions (a)–(d) and with index μ. Let $\Lambda \subset A$ be the unique order of index μ in O_A and let $\mathfrak{I}(\Lambda)$ be the group of invertible Λ-ideals (see Appendix III for the definition). We define a subgroup $\mathfrak{D}(\Lambda)$ of the product $\mathfrak{I}(\Lambda) \times A^{\bullet +}$ by setting

$$\mathfrak{D}(\Lambda) = \{(I, \alpha) \in \mathfrak{I}(\Lambda) \times A^{\bullet +} : \alpha I^2 = \Lambda\}.$$

Here is the fundamental result in this section:

1.3. THEOREM. *If $\gcd(\delta_1, \delta_2, \Delta) = 1$ and $\mathscr{S}$ is not empty then the action of $\mathfrak{D}(\Lambda)$ on $\mathscr{S}$ defined by*

$$(I, \alpha)\cdot(M, b) = (IM, b\alpha)$$

is transitive.

Proof. We first prove that $\mathfrak{D}(\Lambda)$ acts on $\mathscr{S}$. Indeed, let (I, α) be in $\mathfrak{D}(\Lambda)$ and let (M, b) be in $\mathscr{S}$. Since $(IM, b\alpha)$ satisfies trivially Conditions (a) and (b), we shall only check Conditions (c) and (d).

We have

$$(b\alpha)(IM, IM) = b(\alpha I^2 M, M) = b(M, M).$$

Thus $(IM, b\alpha)$ fulfills Condition (c) (evidently the equality above also holds if

b is replaced by bt). By direct computation we have

$$\delta(b\alpha|_{IM}) = \mathrm{N}_{A/\boldsymbol{Q}}(\alpha)\mathbf{N}(I)^2\delta(b|_M) = \mathbf{N}(\alpha I^2)\delta(b|_M) = \delta(b|_M).$$

Hence $(IM, b\alpha)$ satisfies Condition (d).

The non-trivial part of the theorem is of course the transitivity of this action. Let (M, b) and (N, c) be in $\mathcal{S}$. Set $\alpha = b^{-1}c$ and $I = \mathrm{Hom}_\Lambda(M, N) = \{\lambda \in A |\ \lambda M \subseteq N\}$. Since M and N are projective Λ-modules (see Theorem III.1) we must have $IM = N$. In order to show that (I, α) belongs to $\mathfrak{D}(\Lambda)$ we use the following intermediate result that will be proved eventually:

1.4. Lemma. *Let Λ' be the dual ideal of the unit ideal Λ (see Appendix* III *for the definition). Let (M, b) be as above and let $\beta : M \to \mathrm{Hom}_\Lambda(M, \Lambda')$ be the unique symmetric Λ-bilinear form such that $\mathrm{Tr}_{A/\boldsymbol{Q}}\beta = b$. Then*

$$\beta(M, M) = \Lambda' \cap t^{-1}\Lambda'. \tag{2}$$

In particular, the ideal $\beta(M, M)$ depends only on the invariants $(\delta_1, \delta_2, \Delta, \mu)$.

Let γ: $N \to \mathrm{Hom}_\Lambda(N, \Lambda')$ be the Λ-bilinear form associated to (N, c) as in Lemma 1.4. We have

$$\gamma(N, N) = \beta\alpha(IM, IM) = \alpha I^2 \beta(M, M). \tag{3}$$

By Lemma 1.4 we have $\beta(M, M) = \gamma(N, N)$. Hence $\alpha I^2 = \Lambda$ as desired (all Λ-ideals involved in (3) are invertible). ∎

Proof Lemma 1.4. For simplicity we denote in this proof by $(x, y, z, \ldots)$ the Λ-ideal generated in A by $x, y, z, \ldots$ Let J denote the ideal $(1, t)$. Since both b and bt take integral values on M we must have

$$\beta(M, M) \subseteq \Lambda' \cap t^{-1}\Lambda' = J'.$$

We show now that the ideals $\beta(M, M)$ and J' have the same norm. Indeed, we have on the one hand

$$|\delta_1| = |\det(b|_M)| = \left|\det\left(\mathrm{Tr}_{A/\boldsymbol{Q}}(\beta|_M)\right)\right| = \mathbf{N}\big(\beta(M, M)\big)|\mathrm{disc}(\Lambda)|. \tag{4}$$

On the other hand, using the hypothesis $\gcd(\delta_1, \delta_2, \Delta) = 1$ we obtain

$$J\bar{J} = (1, t, \bar{t}, t\bar{t}) = (1, t, t+\bar{t}, t\bar{t}) = (1, t, \Delta\delta_1^{-1}, \delta_2\delta_1^{-1})$$
$$= (\delta_1^{-1})(\delta_1, \delta_2, \Delta, \delta_1 t) = (\delta_1^{-1}).$$

Hence J is invertible and $\mathbf{N}(J) = |\delta_1|^{-1}$. Using this equality we obtain

$$\mathbf{N}(J') = \mathbf{N}(J^{-1}\Lambda') = \mathbf{N}(J)^{-1}\mathbf{N}(\Lambda') = |\delta_1||\mathrm{disc}(\Lambda)|^{-1}. \tag{5}$$

Putting together (4) and (5) we get $\mathbf{N}\big(\beta(M, M)\big) = |\mathbf{N}(J')|$ as desired. ∎

Let $\mathfrak{G}(\Lambda)$ denote the quotient of $\mathfrak{D}(\Lambda)$ defined by the exact sequence

$$A^{*+} \to \mathfrak{D}(\Lambda) \to \mathfrak{G}(\Lambda) \to 0, \tag{6}$$

where the homomorphism $A^{*+} \to \mathfrak{D}(\Lambda)$ is given by $\alpha \mapsto (\alpha^{-1}\Lambda, \alpha^2)$. The following result is a straightforward consequence of Theorem 1.3.

1.5. Corollary. *If $\mathcal{S}$ is not empty then $\mathfrak{G}(\Lambda)$ acts freely on $\mathcal{S}$. If in addition $\gcd(\delta_1, \delta_2, \Delta) = 1$ then this action is transitive. In particular, if $h_{\mathcal{S}} = h_{\mathcal{S}}(\delta_1, \delta_2, \Delta, \mu)$ denotes the cardinal of $\mathcal{S}(\delta_1, \delta_2, \Delta, \mu)$ then*

$$h_{\mathcal{S}} = |\mathfrak{G}(\Lambda)|.$$

2. From symmetric bilinear forms to quadratic forms. Recall that to every quadratic form q with coefficients in $\boldsymbol{Z}$ corresponds a symmetric bilinear form b taking values in $\boldsymbol{Z}$ defined by $b(\boldsymbol{x}, \boldsymbol{y}) = q(\boldsymbol{x}+\boldsymbol{y}) - q(\boldsymbol{x}) - q(\boldsymbol{y})$. Conversely, to every $\boldsymbol{Z}$-valued *even* symmetric bilinear form b corresponds an integral quadratic form q defined by $q(\boldsymbol{x}) = (1/2)b(\boldsymbol{x}, \boldsymbol{x})$. Consequently we shall not make any distinction between quadratic forms and even symmetric bilinear forms. In particular, all invariants defined for pairs of symmetric bilinear forms in the previous section will also apply to pairs of quadratic forms.

Let $\mathcal{Q}(\delta_1, \delta_2, \Delta, \mu)$ be the set of equivalence classes of pairs of quadratic forms with invariants $(\delta_1, \delta_2, \Delta, \mu)$. By the preceding remarks $\mathcal{Q}(\delta_1, \delta_2, \Delta, \mu)$ can be viewed as a subset of the set $\mathcal{S}(\delta_1, \delta_2, \Delta, \mu)$ defined in the previous section. The aim of this section is to provide a version of Theorem 1.3 and Corollary 1.5 for $\mathcal{Q}(\delta_1, \delta_2, \Delta, \mu)$.

To avoid trivial cases we shall assume throughout this section that $\mathcal{Q}(\delta_1, \delta_2, \Delta, \mu)$ is not the empty set. As in the previous section $\phi(T)$ is assumed to have distinct roots, A denotes the algebra $\boldsymbol{Q}[T]/(\phi(T))$, and Λ is the order of index μ in the maximal order of A.

2.1. Theorem. (a) *If $\mathrm{disc}(\Lambda) \equiv 1 \pmod 4$ then $\delta_i \equiv 0 \pmod 4$ for $i = 1, 2$ and the map*

$$\mathcal{S}(\delta_1/4, \delta_2/4, \Delta/4, \mu) \to \mathcal{Q}(\delta_1, \delta_2, \Delta, \mu)$$
$$(M, b) \mapsto (M, 2b)$$

is bijective.

(b) *If $\mathrm{disc}(\Lambda) \equiv 0 \pmod 4$ then the map*

$$\mathcal{S}(\delta_1, \delta_2, \Delta, 2\mu) \to \mathcal{Q}(\delta_1, \delta_2, \Delta, \mu)$$
$$(M, b) \mapsto (\Lambda M, 2b)$$

is two-to-one and surjective.

Proof. (a) The injectivity of the map is obvious, so we shall only prove its surjectivity. Let (M, c) be in $\mathscr{Q}(\delta_1, \delta_2, \Delta, \mu)$; we shall prove that the bilinear form c takes only even values. Since M is Λ-projective, the module $M/2M$ is free of rank one over $\Lambda/2\Lambda$. Let m be a basis of $M/2M$ over $\Lambda/2\Lambda$. By hypothesis $\operatorname{disc}(\Lambda)$ is odd; thus the ring $\Lambda/2\Lambda$ is a semi-simple $\boldsymbol{F}_2$-algebra. Therefore $\Lambda/2\Lambda$ is perfect (that is every element in $\Lambda/2\Lambda$ is a square). Let x, y be in $\Lambda/2\Lambda$ and choose z so that $xy = z^2$. Then

$$c(xm, ym) = c(xym, m) \equiv c(z^2 m, m) \pmod 2 \tag{7}$$

$$\equiv c(zm, zm) \pmod 2 \equiv 0 \pmod 2.$$

The same argument shows that ct also takes only even values. Thus $\delta_i \equiv 0 \pmod 4$ and $(M, c/2)$ is in $\mathscr{S}(\delta_1/4, \delta_2/4, \Delta/4, \mu)$ as asserted.

(b) Let Λ_0 be the order of index 2 in Λ (or equivalently of index 2μ in O_A). Notice that if M is Λ_0-projective then M has index 2 in ΛM. Hence $\delta(2b|_{\Lambda M}) = \delta(b|_M) = \delta_1$.

We shall first deal with surjectivity. Let (N, c) be in $\mathscr{Q}(\delta_1, \delta_2, \Delta, \mu)$. We choose a sublattice $M \subset N$ of index 2 and Λ_0-projective (this is evidently possible since N is Λ-projective). We claim that the form c takes only even values on M, which will prove the surjectivity. Indeed, it is easy to see that the order Λ_0 is the inverse image of $\boldsymbol{F}_2$ under the canonical map

$$\Lambda \to \Lambda/2\Lambda \cong \boldsymbol{F}_2[X]/(X^2).$$

In particular, for all x in Λ_0 there exists z in Λ such that $x \equiv z^2 \pmod{2\Lambda}$. Let m be a basis for $M/2M$ over $\Lambda_0/2\Lambda_0$. For if x, y are in Λ_0 and z in Λ is chosen so that $z^2 = xy \pmod{2\Lambda}$, then $c(xm, ym) \equiv c(zm, zm) \equiv 0 \pmod 2$ by a computation similar to (7). We conclude by taking $b = c/2$.

In order to prove that the map is two-to-one we observe that the map

$$\mathscr{S}(\delta_1, \delta_2, \Delta, 2\mu) \to \mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$$

$$(M, b) \mapsto (\Lambda M, 2b),$$

whose image was proven to be $\mathscr{Q}(\delta_1, \delta_2, \Delta, \mu)$, is $\mathfrak{G}(\Lambda_0)$-equivariant (the group $\mathfrak{G}(\Lambda_0)$ acts on $\mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$ via the natural map $h\colon \mathfrak{G}(\Lambda_0) \to \mathfrak{G}(\Lambda)$). Since $\mathfrak{G}(\Lambda_0)$ (respectively $\mathfrak{G}(\Lambda)$) acts freely on $\mathscr{S}(\delta_1, \delta_2, \Delta, 2\mu)$ (respectively on $\mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$) by Corollary 1.5, it is enough to show that the kernel of h is cyclic of order 2. This will be proven in the next lemma. ∎

2.2. Lemma. *Suppose* $\operatorname{disc}(\Lambda) \equiv 0 \mod 4$ *and let* $\Lambda_0 \subset \Lambda$ *be the suborder of index* 2. *The kernel of the natural map*

$$\mathfrak{G}(\Lambda_0) \xrightarrow{h} \mathfrak{G}(\Lambda)$$

is cyclic of order 2.

Proof. Regarding invertible ideals as locally free modules (see Appendix III, Theorem III.1) we see readily that the following sequence is exact

$$0 \to (\Lambda \otimes \boldsymbol{Z}_2)^\bullet/(\Lambda_0 \otimes \boldsymbol{Z}_2)^\bullet \to \mathfrak{I}(\Lambda_0) \xrightarrow{g} \mathfrak{I}(\Lambda) \to 0.$$

But, since 2 is ramified in Λ one also has

$$(\Lambda \otimes \boldsymbol{Z}_2)^\bullet/(\Lambda_0 \otimes \boldsymbol{Z}_2)^\bullet \cong (\Lambda/2\Lambda)^\bullet \cong (\boldsymbol{F}_2[X]/(X^2))^\bullet \cong \boldsymbol{Z}/2\boldsymbol{Z}.$$

Thus $\operatorname{Ker}(g) \cong \boldsymbol{Z}/2\boldsymbol{Z}$. Consider now the following commutative diagram whose rows and columns are exact:

$$\begin{array}{ccccc} 0 & \to & \operatorname{Ker}(f) & \to & \operatorname{Ker}(g) \\ \downarrow & & \downarrow & & \downarrow \\ 0 \to \Lambda_0^{\bullet,+} & \to & \mathfrak{D}(\Lambda_0) & \to & \mathfrak{I}(\Lambda_0) \\ \downarrow & & \downarrow f & & \downarrow g \\ 0 \to \Lambda^{\bullet,+} & \to & \mathfrak{D}(\Lambda) & \to & \mathfrak{I}(\Lambda). \end{array}$$

It is evident that if I is the generator of $\operatorname{Ker}(g)$ then $(I, 1)$ belongs to $\operatorname{Ker}(f)$; hence $\operatorname{Ker}(f) \to \operatorname{Ker}(g)$ is surjective. So, by exactness of the first row, it must be an isomorphism. Thus $\operatorname{Ker}(f) \cong \boldsymbol{Z}/2\boldsymbol{Z}$. Finally, the diagram

$$\begin{array}{ccccccc} 0 & \to & A^{\bullet,+}/\{\pm 1\} & \to & \mathfrak{D}(\Lambda_0) & \to & \mathfrak{G}(\Lambda_0) \to 0 \\ & & \| & & \downarrow f & & \downarrow h \\ 0 & \to & A^{\bullet,+}/\{\pm 1\} & \to & \mathfrak{D}(\Lambda) & \to & \mathfrak{G}(\Lambda) \to 0 \end{array}$$

shows that $\operatorname{Ker}(h) = \operatorname{Ker}(f)$. Hence $\operatorname{Ker}(h) \cong \boldsymbol{Z}/2\boldsymbol{Z}$ as required. ∎

2.3. Corollary. *Assume that* $\mathscr{Q}(\delta_1, \delta_2, \Delta, \mu)$ *is not empty. Let* $h_{\mathscr{Q}}(\delta_1, \delta_2, \Delta, \mu)$ *be the cardinal of* $\mathscr{Q}(\delta_1, \delta_2, \Delta, \mu)$. *Then*

(a) *If* $\operatorname{disc}(\Lambda) \equiv 1 \pmod 4$ *and* $\gcd(\delta_1, \delta_2, \Delta) = 4$, *then*

$$h_{\mathscr{Q}}(\delta_1, \delta_2, \Delta, \mu) = h_{\mathscr{S}}(\delta_1/4, \delta_2/4, \Delta/4, \mu) = |\mathfrak{G}(\Lambda)|.$$

(b) *If* $\operatorname{disc}(\Lambda) \equiv 0 \pmod 4$ *and* $\gcd(\delta_1, \delta_2, \Delta) = 1$, *then*

$$h_{\mathscr{Q}}(\delta_1, \delta_2, \Delta, \mu) = \tfrac{1}{2} h_{\mathscr{S}}(\delta_1, \delta_2, \Delta, 2\mu) = \tfrac{1}{2}|\mathfrak{G}(\Lambda_0)|.$$

Proof. Combine Theorem 2.1 and Corollary 1.5.

3. The class number. This section is devoted to the explicit computation of the number $h_{\mathscr{S}}$ of equivalence classes of pairs of binary symmetric bilinear forms with given invariants.

In light of the results of the previous sections, this is essentially equivalent to the computation of the order of the group $\mathfrak{G}(\Lambda)$ defined in (6) for a given order Λ in a quadratic semi-simple algebra $A/\boldsymbol{Q}$. Let ${}_2\operatorname{Pic}^+(\Lambda)$ denote the subgroup of ${}_2\operatorname{Pic}^+(\Lambda)$ of elements of order at most 2. We define homomorphisms $j\colon \Lambda^{\bullet,+} \to \mathfrak{G}(\Lambda)$ and $k\colon \mathfrak{G}(\Lambda) \to {}_2\operatorname{Pic}^+(\Lambda)$ by setting $j(u) = (\Lambda, u)$ and $k(X, u) = (X)$. The proof of the following proposition is left to the reader.

3.1. PROPOSITION. *The sequence*

$$0 \to \Lambda^{\bullet +}/\Lambda^{\bullet +2} \xrightarrow{j} \mathfrak{G}(\Lambda) \xrightarrow{k} {}_2\mathrm{Pic}^+(\Lambda) \to 0$$

is exact.

3.2. PROPOSITION. *The order of* $\mathfrak{G}(\Lambda)$ *is given by*

$$|\mathfrak{G}(\Lambda)| = 2^{w(D)-1+l(D)}[\Lambda^{\bullet +} : (\Lambda^{\bullet +})^2], \tag{8}$$

where $w(D)$ *is the number of distinct prime divisor of* $D = \mathrm{disc}(\Lambda)$, *and* $l(D)$ *is the integer defined in Appendix* III, *Corollary* III.4.

Proof. By Corollary III.3 in Appendix III we know that the order of ${}_2\mathrm{Pic}^+(\Lambda)$ is $2^{w(D)-1+l(D)}$. The equality (8) follows now immediately from Proposition 3.1. ∎

Remark. It is very easy to see that the factor $[\Lambda^{\bullet +} : (\Lambda^{\bullet +})^2]$ is given by

$$[\Lambda^{\bullet +} : (\Lambda^{\bullet +})^2] = \begin{cases} 2 & \text{if } D_\Lambda \leqslant 1; \\ 4 & \text{if } D_\Lambda > 1, \end{cases}$$

where $D_\Lambda = \mathrm{disc}(O_\Lambda)$.

We shall now combine the result above with the classification theorems of the previous sections to obtain an explicit class number formula for pairs of binary symmetric bilinear forms with prescribed invariants.

3.3. THEOREM. *If* $\gcd(\delta_1, \delta_2, \Delta) = 1$ *and* $h_{\mathscr{S}}(\delta_1, \delta_2, \Delta, \mu) \neq 0$ *then*

$$h_{\mathscr{S}}(\delta_1, \delta_2, \Delta, \mu) = \begin{cases} 2^{w(D)-1+l(D)}[\Lambda^+ : (\Lambda^{\bullet +})^2] & \text{if } D \equiv 1 \pmod 4, \\ 2^{w(4D)-2+l(4D)}[\Lambda^{\bullet +} : (\Lambda^{\bullet +})^2] & \text{otherwise.} \end{cases}$$

Proof: The proof follows directly from Corollary 1.5, Corollary 2.3, and Proposition 3.2. ∎

The question is now how to decide effectively for prescribed $(\delta_1, \delta_2, \Delta, \mu)$ whether the set $\mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$ is not empty. The answer is given by the following theorem.

3.4. THEOREM. *Suppose* $\gcd(\delta_1, \delta_2, \Delta) = 1$ *and let* $J = \Lambda + t\Lambda$. *Then the following conditions are equivalent.*

(a) *The set* $\mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$ *is not empty.*

(b) *The equality*

$$[J] = \begin{cases} 1 & \text{if } \delta_1 > 0, \\ [\Lambda'] & \text{if } \delta_1 < 0 \end{cases}$$

holds in the group $\mathrm{Pic}^+(\Lambda)/\mathrm{Pic}^+(\Lambda)^2$.

Proof. (a)⇒(b). Let (M, b) be an element in $\mathscr{S}(\delta_1, \delta_2, \Delta, \mu)$. Let $\beta: M \to \mathrm{Hom}_\Lambda(M, \Lambda')$ be so that $b = \mathrm{Tr}_{A/\mathbf{Q}}\beta$. We proved in Lemma 1.4 the equality

$$\beta(M, M) = J'. \tag{9}$$

After choosing an A-basis v for V we can write $M = Iv$, where I is a Λ-ideal. Hence, by (9), we have $I^2\beta(v, v) = J'$. Using the identity $J' = J^{-1}\Lambda'$ we obtain

$$[J] = [\beta(v, v)\Lambda][\Lambda'] \tag{10}$$

in $\mathrm{Pic}^+(\Lambda)/\mathrm{Pic}^+(\Lambda)^2$. Suppose first $\delta_1 < 0$, that is b is a definite form. We leave as exercise to see that Λ must be a real order (use the fact a symmetric real matrix has real eigenvalues). From the identity

$$-\delta_1 = \mathrm{N}_{A/\mathbf{Q}}(\beta(v, v))\mathbf{N}(I)^2\mathrm{disc}(\Lambda)$$

we conclude that $\mathrm{N}_{A/\mathbf{Q}}(\beta(v, v)) > 0$. Thus $[J] = [\Lambda']$ in $\mathrm{Pic}^+(\Lambda)/\mathrm{Pic}^+(\Lambda)^2$.

Suppose now $\delta_1 > 0$. If Λ is an imaginary order, then it follows directly from (10) that $[J] = [\Lambda'] = 1$. If Λ is real, then $\mathrm{N}_{A/\mathbf{Q}}(\beta(v, v)) < 0$, so $[\beta(v, v)\Lambda] = [\Lambda']$ in $\mathrm{Pic}^+(\Lambda)$. Thus, again from (10), we have $[J] = 1$.

(b)⇒(a). The hypothesis implies that we may choose (I, α) such that $\alpha I^2 = J'$ with $\mathrm{N}_{A/\mathbf{Q}}(\alpha) > 0$ if $\delta_1 < 0$, and with $\mathrm{N}_{A/\mathbf{Q}}(\alpha) < 0$ if $\delta_1 > 0$ and Λ is real. As before we choose an A-basis v for V and we set $M = Iv$ and $b(xv, yv) = \mathrm{Tr}_{A/\mathbf{Q}}(\alpha xy)$. A routine verification shows that the pair (M, b) has the required invariants. ∎

In order to have an effective version of Theorem 3.4 we compute now the local symbols $\varepsilon_p(J)$ for the ideal $J = \Lambda + t\Lambda$ (see Appendix III for the definition). To avoid technical complications at primes ramified in Λ we shall assume henceforth

$$\gcd(\delta_1\delta_2, \Delta) = 1 \quad \text{and} \quad \Lambda \equiv 1 \pmod 2. \tag{11}$$

3.5. THEOREM. *Assume condition* (11) *above. Then* $h_{\mathscr{S}} = h_{\mathscr{S}}(\delta_1, \delta_2, \Delta, \mu)$ *is given by*

$$h_{\mathscr{S}} = m \sum_{\substack{n \mid \mu^2 D_\Lambda \\ n \text{ square free}}} \left(\frac{\delta_1}{n}\right) \quad \text{with} \quad m = \begin{cases} 2 & \text{if } D_\Lambda \geqslant 1, \\ 1 & \text{if } D_\Lambda < 0. \end{cases}$$

Proof. Let $D = \mathrm{disc}(\mathbf{Z}[\delta_1 t]) = \Delta^2 - 4\delta_1\delta_2$. The integer $\mathrm{disc}(\Lambda) = \mu^2 D_\Lambda$ is odd, since it is a divisor of D and Δ is odd by hypothesis. Let p be a prime divisor of $\mu^2 D_\Lambda$. By the proof of Lemma 1.4 we know $\mathbf{N}(J) = |\delta_1|^{-1}$, and, by (11), δ_1 is a p-unit. Thus we can choose $x_p = 1$ as a local basis of J at p. Hence

$$\varepsilon_p(J) = \left(\frac{|\delta_1|}{p}\right) \quad \text{for } p \mid \mu^2 D_\Lambda.$$

On the other hand, for $\delta_1 < 0$ we obtain

$$\varepsilon_p(\Lambda') = \left(\frac{-1}{p}\right).$$

Thus, by Theorem 3.4 and Theorem III.2 we have

$$h_{\mathscr{G}} \neq 0 \Leftrightarrow \left(\frac{\delta_1}{p}\right) = 1 \quad \text{for } p|\mu^2 D_\Lambda,$$

for both positive and negative δ_1. Hence

$$\frac{1}{2^{w(\mu^2 D_\Lambda)}} \prod_{p|\mu^2 D_\Lambda} \left(1+\left(\frac{\delta_1}{p}\right)\right) = \begin{cases} 1 & \text{if } h_{\mathscr{G}} \neq 0, \\ 0 & \text{if } h_{\mathscr{G}} = 0. \end{cases}$$

Using Proposition 3.2 we obtain

$$h_{\mathscr{G}} = 2^{w(\mu^2 D_\Lambda)-1+l(\mu^2 D_\Lambda)}[\Lambda^{**}:\Lambda^{**2}] \frac{1}{2^{w(\mu^2 D_\Lambda)}} \prod_{p|\mu^2 D_\Lambda} \left(1+\left(\frac{\delta_1}{p}\right)\right)$$

$$= m \prod_{p|\mu^2 D_\Lambda} \left(1+\left(\frac{\delta_1}{p}\right)\right) = m \sum_{\substack{n|\mu^2 D_\Lambda \\ n \text{ square free}}} \left(\frac{\delta_1}{n}\right). \blacksquare$$

3.6. COROLLARY. *Let $H = H(\delta_1, \delta_2, \Delta)$ be the number of equivalence classes of pairs of symmetric forms with invariants $(\delta_1, \delta_2, \Delta)$. With the same hypothesis as in Theorem 3.5 we have*

$$H = m \sum_{n|D} \left(\frac{\delta_1}{n}\right), \tag{12}$$

where $D = \Delta^2 - 4\delta_1\delta_2$.

Proof. We write $D = f^2 D_\Lambda$, where $D_\Lambda = \operatorname{disc}(O_\Lambda)$. Clearly we have

$$H = \sum_{\mu|f} h(\delta_1, \delta_2, \Delta, \mu).$$

Thus, by Theorem 3.5, we have,

$$H = m \sum_{\mu|f} \sum_{\substack{n|\mu^2 D_\Lambda \\ n \text{ square free}}} \left(\frac{\delta_1}{n}\right) = m \sum_{n|D} \left(\frac{\delta_1}{n}\right)$$

(note that D_Λ is square free). ■

Remark. Formula (12) was found by Hardy and Williams (see [3]) for pairs of positive-definite forms with fundamental discriminant, also with some restrictive hypotheses on $(\delta_1, \delta_2, \Delta)$. The factor m in equation (12) is in this case equal to 2, and is explained by the fact that our method allows also negative-definite forms.

Appendix I. Finiteness

Although finiteness in the case $\Delta^2 \neq 4\delta_1\delta_2$ can be also deduced from Theorem 1.3, we prefer to give an independent proof, which has the advantage of being valid without change for pairs of symmetric bilinear forms of any rank, and can even be easily reformulated for systems of an arbitrary number of forms. As many other finiteness results in number theory, Theorem I.1 below is an easy consequence of a deep result of Borel and Harish-Chandra in the theory of algebraic groups [1, Theorem 6.9].

I.1. THEOREM. *If $4\delta_1\delta_2 \neq \Delta^2$ then there are only finitely many equivalence classes of pairs of symmetric bilinear forms of rank 2 with invariants $(\delta_1, \delta_2, \Delta)$.*

Proof. For a ring $R \subset \boldsymbol{C}$ we denote by $\boldsymbol{X}_d(R)$ the set of symmetric 2×2-matrices with non-zero determinant d and with entries in R. The group $\mathrm{SL}_2(R)$ acts on $\boldsymbol{X}_d(R)$ in the obvious way: $(X, B) \mapsto X^t BX$. The algebraic map

$$f\colon \boldsymbol{X}_{d_1}(\boldsymbol{C}) \times \boldsymbol{X}_{d_2}(\boldsymbol{C}) \to \boldsymbol{M}_2(\boldsymbol{C})$$

given by $f(B_1, B_2) = B_1^{-1} B_2$ is $\mathrm{SL}_2(\boldsymbol{C})$-equivariant (the group $\mathrm{SL}_2(\boldsymbol{C})$ acts diagonally on $\boldsymbol{X}_{d_1}(\boldsymbol{C}) \times \boldsymbol{X}_{d_2}(\boldsymbol{C})$ and by conjugation of matrices on $\boldsymbol{M}_2(\boldsymbol{C})$). Let C be the conjugacy class in $\boldsymbol{M}_2(\boldsymbol{C})$ whose minimal polynomial is

$$\phi(T) = T^2 + \frac{\Delta}{\delta_1} T + \frac{\delta_2}{\delta_1}.$$

Our hypothesis implies that C is semi-simple. Therefore C is closed in $\boldsymbol{M}_2(\boldsymbol{C})$ for the usual topology (see for instance [4, Chap. II, 2.7, Satz 3]). Hence $f^{-1}(C)$ is closed in $\boldsymbol{X}_{d_1}(\boldsymbol{C}) \times \boldsymbol{X}_{d_2}(\boldsymbol{C})$.

It is easy to see that over $\boldsymbol{C}$ every equivalence class of pairs has a representative of the form (I, B), with B unique up to $\mathrm{SO}_2(\boldsymbol{C})$-conjugacy. Thus $f^{-1}(C)$ consists of a single orbit, which is therefore closed. By a theorem of Borel and Harish-Chandra (see [1, Theorem 6.9]), the intersection of a closed orbit with $\boldsymbol{X}_{d_1}(\boldsymbol{Z}) \times \boldsymbol{X}_{d_2}(\boldsymbol{Z})$ is the union of finitely many $\mathrm{SL}_2(\boldsymbol{Z})$-orbits. ■

Appendix II. The case $\Delta^2 = 4\delta_1\delta_2$

II.1. PROPOSITION. *Let B_1 and B_2 be linearly independent forms. The following conditions are equivalent.*

(a) *B_1 and B_2 represent zero simultaneously.*

(b) $\Delta^2 = 4\delta_1\delta_2$.

Proof. (a) $\Rightarrow$ (b). We can assume

$$B_i = \begin{pmatrix} a_i & b_i \\ b_i & 0 \end{pmatrix}.$$

By direct computation $\Delta^2 = (2b_1 b_2)^2 = 4\delta_1\delta_2$.

(b) $\Rightarrow$ (a). The hypothesis $\Delta^2 = 4\delta_1\delta_2$ implies that the matrix $S = B_1^{-1}B_2$ has a double eigenvalue λ. Since B_1 and B_2 are not proportional, there exists a vector x such that $v = (S-\lambda I)x$ is different from zero. Clearly $v^t B_i v = 0$ for $i = 1, 2$. ∎

The following proposition gives the classification of pairs (B_1, B_2) with prescribed δ_1, δ_2, and $\Delta^2 = 4\delta_1\delta_2$. Note that by Proposition II.1, δ_i must be a square.

II.2. Proposition. *Let b_1, b_2 be non-zero integers and let $\delta_i = b_i^2$, and $\Delta = 2b_1b_2$. The following is a complete list of non-equivalent pairs (B_1, B_2) with invariants $(\delta_1, \delta_2, \Delta)$:*

$$\left(\begin{pmatrix} a_1 & \varepsilon b_1 \\ \varepsilon b_1 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & \varepsilon b_2 \\ \varepsilon b_2 & 0 \end{pmatrix}\right)$$

where $0 \leqslant a_1 < 2|b_1|$, $\varepsilon = \pm 1$, and a_2 is any integer. In particular, there are infinitely many such classes.

Proof. Let (B_1, B_2) be a pair with invariants $(\delta_1, \delta_2, \Delta)$. By Proposition II.1, the pair (B_1, B_2) is equivalent to

$$\left(\begin{pmatrix} a_1 & \varepsilon b_1 \\ \varepsilon b_1 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & \varepsilon b_2 \\ \varepsilon b_2 & 0 \end{pmatrix}\right).$$

By performing if needed a transformation of the type

$$\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix},$$

which does not change the shape of either form, we can assume $0 \leqslant a_1 < 2|b_1|$. Observe that a_1 is uniquely determined modulo $2b_1$ and that the only automorphisms of the form

$$\begin{pmatrix} a_1 & \varepsilon b_1 \\ \varepsilon b_1 & 0 \end{pmatrix}$$

are $\mathbf{1}$ and $-\mathbf{1}$. Thus all pairs obtained in this manner belong to different equivalence classes. ∎

Appendix III. Quadratic orders

In this appendix we recall without proofs some well known results from the theory of quadratic orders. A good reference is [2, Chapter II].

Let $A/\boldsymbol{Q}$ be a quadratic semi-simple algebra, i.e. A is either a quadratic field or the split algebra $\boldsymbol{Q}\times\boldsymbol{Q}$. Let $\Lambda \subset A$ be an order, that is, a subring of rank two over $\boldsymbol{Z}$. By a *Λ-ideal* J we mean a finitely generated Λ-submodule of A with $\boldsymbol{Q}J = A$. For a Λ-ideal J we define the *dual* J' by

$$J' = \{x \in A \mid \mathrm{Tr}_{A/\boldsymbol{Q}}(xJ) \subseteq \boldsymbol{Z}\}.$$

An ideal J is *invertible* if there exists an ideal I such that $IJ = \Lambda$. Here is a useful criterion to recognize invertible ideals.

III.1. Theorem. *Let J be a Λ-ideal. The following conditions are equivalent.*

(a) $JJ' = \Lambda'$.

(b) *J is invertible.*

(c) *J is projective as a Λ-module.*

(d) *J is locally free, that is J_p is principal Λ_p-ideal for all primes p (as usual the subscript p means tensor product with the p-adic integers $\boldsymbol{Z}_p$).*

(e) $\mathrm{End}_\Lambda(J) = \Lambda$.

The set of invertible Λ-ideals forms a group under multiplication. This group will be denoted by $\mathfrak{I}(\Lambda)$. The *Picard group* $\mathrm{Pic}(\Lambda)$ is defined by the exact sequence

$$A^\bullet \to \mathfrak{I}(\Lambda) \to \mathrm{Pic}(\Lambda) \to 0$$

where $A^\bullet \to \mathfrak{I}(\Lambda)$ is the obvious map $a \mapsto \Lambda a$. Similarly, the *narrow Picard group* $\mathrm{Pic}^+(\Lambda)$ is defined by the exact sequence

$$A^{\bullet +} \to \mathfrak{I}(\Lambda) \to \mathrm{Pic}^+(\Lambda) \to 0$$

where $A^{\bullet +}$ is the subgroup of units of positive norm in A. For an ideal $J \subseteq \Lambda$ we define its *absolute norm* by $\mathbf{N}(J) = [\Lambda : J]$. The norm induces a homomorphism $\mathbf{N}\colon \mathfrak{I}(\Lambda) \to \boldsymbol{Q}^\bullet$. For an ideal J and for a prime number p we define

$$\varepsilon_p(J) = \mathrm{N}_{A/\boldsymbol{Q}}(x_p)/\mathbf{N}(J) \quad \text{in } H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_p^\bullet),$$

where x_p is a local basis for J, that is $J_p = x_p\Lambda_p$. It is very easy to see that ε_p defines a homomorphism $\mathrm{Pic}^+(\Lambda)/\mathrm{Pic}^+(\Lambda)^2 \to H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_p^\bullet)$. The following theorem is classical for $\Lambda = O_A$ (see for instance [2, Chap. III, Section 8, Theorems 7 and 8]. Its generalization to non-maximal orders is straightforward.

III.2. Theorem. *The homomorphism*

$$\varepsilon\colon \mathrm{Pic}^+(\Lambda)/\mathrm{Pic}^+(\Lambda)^2 \to \prod_{p|\mathrm{disc}(\Lambda)} H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_p^\bullet),$$

$$[J] \mapsto (\varepsilon_p(J)),$$

is injective. Furthermore, the image of ε consists exactly of the elements (ξ_p) satisfying the reciprocity condition

$$\prod_{p|D_A} (\xi_p, D_A)_p = 1,$$

where $D_A = \mathrm{disc}(O_A)$ and $(\ ,\ )_p$ is the Hasse symbol at p.

III.3. LEMMA. *The group* $H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_p^*)$ *is trivial for* p *not dividing* $\mathrm{disc}(\Lambda)$. *For an odd prime* p *dividing* $\mathrm{disc}(\Lambda)$ *the Legendre symbol defines an isomorphism*

$$H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_p^*) \to \{\pm 1\}, \qquad u \mapsto \left(\frac{u}{p}\right),$$

and for $p = 2$ *we have*

$$H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_2^*) \cong \begin{cases} \{1\} & \text{if } b = 0 \text{ and } a \leqslant 1; \\ (\boldsymbol{Z}/4\boldsymbol{Z})^* & \text{if } (b = 0 \text{ and } a = 2) \\ & \text{or } (b = 2 \text{ and } a \leqslant 1) \\ & \text{or } (b = 3 \text{ and } a = 0); \\ (\boldsymbol{Z}/8\boldsymbol{Z})^* & \text{in all other cases.} \end{cases} \tag{13}$$

where $a = \mathrm{ord}_2([O_A : \Lambda])/2$ *and* $b = \mathrm{ord}_2(D_A)$.

The following corollary gives the 2-rank of $\mathrm{Pic}^+(\Lambda)$.

III.4. COROLLARY. *Let* ${}_2\mathrm{Pic}^+(\Lambda)$ *denote the subgroup of* $\mathrm{Pic}^+(\Lambda)$ *of elements of order at most* 2. *Then*

$$|{}_2\mathrm{Pic}^+(\Lambda)| = 2^{w(D)-1+l(D)},$$

where $w(D)$ *is the number of distinct prime divisors of* $D = \mathrm{disc}(\Lambda)$ *and* $l(D)$ *is given by*

$$l(D) = \begin{cases} 1 & \text{if } D_A = 1 \text{ and } D \text{ odd}; \\ 0 & \text{if } D_A \neq 1 \text{ and } D \text{ odd}; \\ \mathrm{ord}_2(H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_2^*)) & \text{if } D_A = 1 \text{ and } D = 2^{2m} \ (m > 0); \\ \mathrm{ord}_2(H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_2^*)) - 1 & \text{in all other cases} \end{cases}$$

(*see equality* (13) *for the computation of* $H^2(\mathrm{Gal}(A/\boldsymbol{Q}), \Lambda_2^*)$).

Appendix IV. An explicit example

This appendix illustrates the computational aspects of Theorem 1.3 and Corollary 1.5. Starting from Example 1.2 we shall calculate here a complete set of representatives of the equivalence classes of pairs with invariants $\delta_1 = -1$, $\delta_2 = -31$, and $\Delta = 18$.

Since $\Delta^2 - 4\delta_1\delta_2 = 2^3 \cdot 5^2$, the orders relevant for our purposes are $\boldsymbol{Z}[\sqrt{2}]$ ($\mu = 1$) and $\boldsymbol{Z}[5\sqrt{2}]$ ($\mu = 5$). We know from Example 1.2 that both values of μ can be realized. Thus, according to Corollary 1.5, to get hold of a complete set of representatives of the equivalence classes of pairs with invariants $(-1, -31, 18, \mu)$, it will be sufficient to calculate the group $\mathfrak{G}(\boldsymbol{Z}[\mu\sqrt{2}])$ and take the orbits of the pairs given in Example 1.2 under the action of this group.

It is easy to see that ${}_2\mathrm{Pic}^+(\boldsymbol{Z}[\sqrt{2}])$ is trivial (use for instance Corollary III.4). Thus, by virtue of of Proposition 3.1, the group $\mathfrak{G}(\boldsymbol{Z}[\sqrt{2}])$ is given by

$$\mathfrak{G}(\boldsymbol{Z}[\sqrt{2}]) = \{(\boldsymbol{Z}[\sqrt{2}], \pm 1), (\boldsymbol{Z}[\sqrt{2}], \pm\varepsilon^2)\}, \tag{14}$$

where $\varepsilon = 1 + \sqrt{2}$ is the fundamental unit of $\boldsymbol{Z}[\sqrt{2}]$ (notice that ε has norm -1). Thus, by Corollary 1.5, there are four non-equivalent pairs of forms with invariants $\delta_1 = -1$, $\delta_2 = -31$, $\Delta = 18$, and $\mu = 1$.

Similarly, using Corollary III.4 we see that ${}_2\mathrm{Pic}^+(\boldsymbol{Z}[5\sqrt{2}])$ is cyclic of order 2. It is readily checked that $J = 5\boldsymbol{Z} + \sqrt{2}\boldsymbol{Z}$ is a $\boldsymbol{Z}[5\sqrt{2}]$-ideal and satisfies $J^2 = \boldsymbol{Z}[5\sqrt{2}]$. Moreover, since $\sqrt{2}$ is a local generator for J at $p = 5$, we have

$$\varepsilon_5(J) = \left(\frac{-2}{5}\right) = -1.$$

Hence J represents a non-trivial class in ${}_2\mathrm{Pic}^+(\boldsymbol{Z}[5\sqrt{2}])$. Thus, by Proposition 3.1, the group $\mathfrak{G}(\boldsymbol{Z}[5\sqrt{2}])$ is given by

$$\mathfrak{G}(\boldsymbol{Z}[5\sqrt{2}]) = \{(\boldsymbol{Z}[5\sqrt{2}], \pm 1), (\boldsymbol{Z}[5\sqrt{2}], \pm\eta^2), (J, \pm 1), (J, \pm\eta^2)\}, \tag{15}$$

where $\eta = (1+\sqrt{2})^3 = 7 + 5\sqrt{2}$ is the fundamental unit of $\boldsymbol{Z}[5\sqrt{2}]$ (notice that η has norm -1). In particular, there are eight non-equivalent pairs of forms with $\delta_1 = -1$, $\delta_2 = -31$, $\Delta = 18$ and $\mu = 5$.

The case $\mu = 1$. Let

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B_2 = \begin{pmatrix} 14 & 5 \\ 5 & 4 \end{pmatrix} \tag{16}$$

as in Example 1.2. Let $T = B_1^{-1}B_2$ and let $\tau = 9 - 5\sqrt{2}$ (remark that τ is an eigenvalue of T). The correspondence $T \mapsto \tau$ induces an isomorphism between the fields $\boldsymbol{Q}(T)$ and $\boldsymbol{Q}(\sqrt{2})$. The underlying module $M = \boldsymbol{Z}^2$ is equipped with the $\boldsymbol{Z}[\sqrt{2}]$-module structure given by this isomorphism (i.e. τ acts on M via the matrix T). According to Corollary 1.5, the orbit of (M, B_1) under the action of $\mathfrak{G}(\boldsymbol{Z}[\sqrt{2}])$ provides all the equivalence classes of pairs with invariants $\delta_1 = -1$, $\delta_2 = -31$, $\Delta = 18$, and $\mu = 1$. Let us now describe explicitly this orbit. Let E in $\boldsymbol{Q}(T)$ be the matrix corresponding to the fundamental unit ε of $\boldsymbol{Z}[\sqrt{2}]$. By the definition of the action of $\mathfrak{G}(\boldsymbol{Z}[\sqrt{2}])$ (see (1.3)) we have

$$(\boldsymbol{Z}[\sqrt{2}], \varepsilon^2)\cdot(M, B_1) = (M, B_1E^2).$$

By direct calculation we see $\varepsilon^2 = (33 - 2\tau)/5$; hence

$$E^2 = \tfrac{1}{5}(33I - 2T) = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}.$$

Thus the pair of forms corresponding to (M, B_1E^2) is

$$B_1E^2 = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}, \quad B_2E^2 = \begin{pmatrix} 4 & -3 \\ -3 & 10 \end{pmatrix}. \tag{17}$$

Multiplication by -1 in (16) and (17) yields the remaining two pairs in the orbit of (B_1, B_2). ∎

The case $\mu = 5$. We start out with the forms C_1 and C_2 of Example 1.2:

$$C_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 16 & 17 \\ 17 & 20 \end{pmatrix}. \tag{18}$$

Let $S = C_1^{-1}C_2$. The correspondence $S \mapsto \tau = 9 - 5\sqrt{2}$ induces an isomorphism between $\boldsymbol{Q}(S)$ and $\boldsymbol{Q}(\sqrt{2})$ and makes $M = \boldsymbol{Z}^2$ into a $\boldsymbol{Z}[5\sqrt{2}]$-module. Let N be the matrix corresponding to the fundamental unit $\eta = 7 + 5\sqrt{2}$ of $\boldsymbol{Z}[5\sqrt{2}]$. By (15) the orbit of (M, C_1) under the action of $\mathfrak{G}(\boldsymbol{Z}[5\sqrt{2}])$ is

$$\{(M, \pm C_1), (M, C_1N^2), (JM, \pm C_1), (JM, \pm C_1N^2)\}.$$

Using the identity $\eta^2 = 225 - 14\tau$ we have

$$N^2 = 225I - 14S = \begin{pmatrix} 15 & -196 \\ -14 & 183 \end{pmatrix}.$$

Thus the pair corresponding to (M, C_1N^2) is

$$C_1N^2 = \begin{pmatrix} 1 & -13 \\ -13 & 170 \end{pmatrix}, \quad C_2N^2 = \begin{pmatrix} 2 & -25 \\ -25 & 328 \end{pmatrix}. \tag{19}$$

We shall now calculate the pair corresponding to (JM, C_1). It is easy to see that the first basis vector $e_1 = (1, 0)$ generates $M = \boldsymbol{Z}^2$ as a $\boldsymbol{Z}[5\sqrt{2}]$-module. We also see by direct calculation that $\sqrt{2}$ corresponds to the matrix

$$\begin{pmatrix} -6/5 & -14/5 \\ -1/5 & 6/5 \end{pmatrix}.$$

Thus, recalling that $J = 5\boldsymbol{Z} + \sqrt{2}2\boldsymbol{Z}$, we see that JM admits the vectors $v_1 = (-6/5, -1/5)$ and $v_2 = (5, 0)$ as a $\boldsymbol{Z}$-basis. Let P be the change-of-basis matrix

$$P = \begin{pmatrix} -6/5 & 5 \\ -1/5 & 0 \end{pmatrix}.$$

Writting the forms C_1 and C_2 in the basis $\{v_1, v_2\}$ gives the pair corresponding to (JM, C_1):

$$P^tC_1P = \begin{pmatrix} 2 & -7 \\ -7 & 25 \end{pmatrix}, \quad P^tC_2P = \begin{pmatrix} 32 & -113 \\ -113 & 400 \end{pmatrix}. \tag{20}$$

Similarly, the pair corresponding to (JM, C_1N^2) is

$$P^tC_1N^2P = \begin{pmatrix} 2 & 7 \\ 7 & 25 \end{pmatrix}, \quad P^tC_2N^2P = \begin{pmatrix} 4 & 13 \\ 13 & 50 \end{pmatrix}. \tag{21}$$

As in the previous case, the remaining four pairs in the orbit of (C_1, C_2) are obtained by multiplying by -1 the forms in (18), (19), (20), and (21). ∎

Acknowledgements. The author is indebted to Professor M.-A. Knus who made possible his visit to the Forschungsinstitut für Mathematik der ETH-Zürich in the winter semester 89/90, during which this paper was written. The author also wishes to thank the referee for her/his helpful observations, and B. Erez for his careful reading and detailed suggestions.

References

[1] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. 75 (1962), 485–535.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York 1966.

[3] K. Hardy and S. Williams, *The class number of pairs of positive-definite binary quadratic forms*, Acta Arith. 52 (1989), 103–117.

[4] H. Kraft, *Geometrische Methode in der Invariantentheorie*, Vieweg & Sohn, Braunschweig 1984.

LOUISIANA STATE UNIVERSITY
DEPARTMENT OF MATHEMATICS
Baton Rouge, LA 70803-4918, U.S.A.

Received on 1.3.1990
and in revised form on 31.8.1990 (2013)