On embedding numbers into quaternion orders.

Comment. Math. Helvetici **66** (1991) 302–318 0010–2571/91/020302–17$1.50 + 0.20/0

On embedding numbers into quaternion orders

J. BRZEZINSKI

Abstract. A generalization of the Chevalley-Hasse-Noether theorem from maximal orders to arbitrary Eichler orders in quaternion algebras is given. A stability property for the numbers of orbits for unit groups in quaternion orders acting on optimal embeddings of quadratic orders is proved. The results are applied to Siegel's meanvalue of integral representations by genera of integral definite ternary quadratic forms.

Introduction

Let R be a Dedekind ring with quotient field K, and let A be a K-algebra. An R-order in A is a subring of A containing R and a K-basis of A over K, which is finitely generated and projective as an R-module. If S and Λ are R-orders in K-algebras, then an injective R-homomorphism $\varphi : S \to \Lambda$ is called an optimal embedding if $\Lambda/\varphi(S)$ is R-projective. The unit group Λ^* acts by conjugation on optimal embeddings ($\varphi \mapsto \lambda \circ \varphi$, where $(\lambda \circ \varphi)(x) = \lambda\varphi(x)\lambda^{-1}$ for $\lambda \in \Lambda^*$). We shall assume that there is only a finite number $e_\Lambda^*(S, \Lambda)$ of orbits for this action of Λ^*.

The embedding numbers $e_\Lambda^*(S, \Lambda)$ play a very essential roll in different contexts and were computed by many authors in special cases. If A is a quaternion algebra (that is, A is central, simple and $\dim_K A = 4$) and S is an R-order in an algebra of dimension 2 over a global field K, then $e_\Lambda^*(S, \Lambda)$ were computed in [4] for hereditary orders, in [5] for Eichler orders with particular choice of S, and in [2] and [6] for other types of Bass orders.

The first purpose of the present paper is to compute the numbers $e_\Lambda^*(S, \Lambda)$ for arbitrary orders S in algebras of dimension 2 over K, when Λ is an Eichler order. The method follows an idea of E. Noether [10] in connection with her version of the proof of the Chevalley–Hasse–Noether theorem, and the results of Section 1 can be considered as a generalization of this theorem to the case of arbitrary Eichler orders in quaternion algebras (see (1.14)). The final result of the computations are explicit formulas for $e_\Lambda^*(S, \Lambda)$ similar to those in [2] for the case of primary Bass orders. This is the content of Section 1.

The second purpose of the paper is to establish a stability property of the embedding numbers. The results of Section 1 together with the results of [2] show that if Λ and a quadratic K-algebra L are fixed, then the values of $e_\Lambda^*(S, \Lambda)$ do not

depend on S, when the conductor of S in the maximal order of L is sufficiently small as an R-ideal (for exact meaning see Section 1). Unfortunately, this result is only proved for quaternion orders whose Gorenstein closure is a Bass order. It would be desirable to have a proof covering arbitrary quaternion orders.

In the last section, we give some applications of the stability property of the embedding numbers to representations of integers by genera of definite integral ternary quadratic forms and to Eisenstein series defined by such genera. If $f(x_1, x_2, x_3)$ is a definite integral ternary quadratic form, $\mathrm{Aut}^+(f)$ the group of its integral automorphisms with determinant 1, and for an integer N, $r_f(N)$ the number of integral solutions to $f(x_1, x_2, x_3) = N$ such that $GCD(x_1, x_2, x_3) = 1$, then

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} = \gamma(N)h(S),$$

where $f_1 = f, \ldots, f_t$ represent all classes in the genus of f, $S = \mathbb{Z}[\sqrt{-c_f N}]$ for an integer $c_f > 0$, $h(S)$ is the class number of S, and $\gamma(N)$ is a constant depending on the embedding number of S into a suitable quaternion order Λ_f (see [1]). If f is the sum of 3 squares, then $S = \mathbb{Z}[\sqrt{-N}]$ and $\gamma(N)$ is periodic modulo 8 according to Gauss' Three-Square-Theorem. A rather unexpected result of the analysis of the embedding numbers is the fact that, in general, $\gamma(N)$ depends on two periods: if $c_f N = N_0^2 N_1 \neq 1$, where N_0, N_1 are integers and N_1 is square-free, then there are integers M_0 and M_1 such that $\gamma(N) = \gamma(N_0, N_1)$ only depends on the residues of N_0 modulo M_0 and N_1 modulo M_1. Moreover, one can choose $M_0 = d(\Lambda_f)$ and $M_1 = 4d_1(\Lambda_f)$, where $d(\Lambda_f)$ is the discriminant of Λ_f, and $d_1(\Lambda_f)$ is the product of different primes dividing it. This property has a natural interpretation as a statement about coefficients of Eisenstein series defined by genera of integral definite ternary quadratic forms (see (3.10)).

1. Bouquets of Eichler orders

Let R be a complete discrete valuation ring of characteristic $\neq 2$ with quotient field K. Let π be a generator of the maximal ideal $\mathfrak{m}$ of R, and let v be the valuation of K corresponding to R and such that $v(\pi) = 1$. Recall that an R-lattice on a vector space over K is a finitely generated free R-module containing a basis of the space.

Let L be an n-dimensional separable commutative K-algebra, and let I be an R-lattice on L. It is well-known that $\mathrm{End}_R(I) = \{\varphi \in \mathrm{End}_K(L) : \varphi(I) \subseteq I\}$ is a maximal R-order in the central simple K-algebra $A = \mathrm{End}_K(L)$. We denote this maximal order by $\Gamma(I)$. It is also well-known that every maximal R-order in A can be represented in that way for a suitable R-lattice I on L. Moreover, $\Gamma(I_1) = \Gamma(I_2)$

if and only if there is $a \in K^*$ such that $I_2 = aI_1$. There is a natural embedding $\iota : L \to \mathrm{End}_K(L)$ mapping $\ell \in L$ onto $x \mapsto \ell x$, $x \in L$. The image of ℓ will be denoted by ℓ as well (so L will be identified with its image). Let S be an R-order in L. If $SI \subseteq I$, then the embedding ι restricts to an embedding $S \to \Gamma(I)$, and conversely, if the restriction of ι to S gives such an embedding, then I is an S-ideal. This embedding is optimal if and only if $S = O(I)$; where $O(I) = \{\alpha \in L : \alpha I \subseteq I\}$. Notice that $\Gamma(I\alpha) = \alpha\Gamma(I)\alpha^{-1}$ when $\alpha \in L^*$. (For these facts see [8], pp. 26–27 and p. 107).

We say that R-lattices aI, $a \in K^*$, form a K-class. We shall write $I_1 \sim I_2$, when I_1 and I_2 are in the same K-class. Recall that the distance between the classes of I_1 and I_2, denoted by $d(I_1, I_2)$, may be defined as $v(\mathrm{Ann}\,(I_1/(I_1 \cap I_2)) + v(\mathrm{Ann}\,(I_2/(I_1 \cap I_2))$, where $\mathrm{Ann}\,(X)$ denotes the annihilator ideal of an R-module X, and $v(\mathfrak{a}) = r$ if $\mathfrak{a} = \mathfrak{m}^r (\mathfrak{m}^0 = R)$. (It is not difficult to prove that d really is a distance in usual sense.)

Assume now that $n = 2$ and recall that an R-order Λ in A is called an Eichler order if Λ is an intersection of two maximal orders, that is, $\Lambda = \Gamma(I_1) \cap \Gamma(I_2)$ for suitable R-lattices I_1 and I_2. Recall also that the maximal orders $\Gamma(I_j)$, $j = 1, 2$, are uniquely determined by Λ (see [3], (26.28)). Choosing a basis e_1, e_2 such that $I_1 = Re_1 + Re_2$ and $I_2 = R\pi^a e_1 + R\pi^b e_2$, where $a \leq b$ (see [3], (4.13)), it is easy to see that Λ is isomorphic to the order Λ_d consisting of matrices:

$$\begin{bmatrix} R & R \\ \pi^d R & R \end{bmatrix},$$

where $d = b - a$. The ideal $d(\Lambda) = (\pi^d)$ will be called the discriminant of Λ. Only in this section, we also call d the discriminant of Λ. $d(\Lambda)$ characterizes the isomorphism class of Λ (see [3], (26.28)). Thus, we have:

(1.1) PROPOSITION. *If* $\Lambda = \Gamma(I_1) \cap \Gamma(I_2)$, *then* $d(\Lambda) = (\pi^d)$, *where* $d = d(I_1, I_2)$.

Recall that if S_0 is the maximal R-order in L, then every other R-order in L is equal to $S_i = R + \pi^i S_0$, $i \geq 0$. Notice that $d(S_i, S_0) = i$. Let $x \mapsto \bar{x}$ be the non-trivial automorphism of L over K, and let $N(x) = x\bar{x}$. The following Lemma will be very useful in many computations:

(1.2) LEMMA. *If* $\Lambda = \Gamma(S) \cap \Gamma(S'\alpha)$, *where* $S \subseteq S'$ *are* R*-orders in* L *and* $\alpha \in L^*$ *is such that* $S'\alpha \subseteq S'$ *but* $S'\alpha\pi^{-1} \not\subseteq S'$, *then*

(*a*) $d(S', S'\alpha) = v(N(\alpha))$,

(*b*) $d(\Lambda) = d(S, S') + v(N(\alpha))$.

Proof. (a) See [3], (4.20a).

(b) Let $S = R + \pi^i S'$, so $d(S, S') = i$. Since $S'\bar{\alpha} \subseteq S'$ and $S'\bar{\alpha}\pi^{-1} \not\subseteq S'$, there are $u_1, u_2 \in L$ such that $S'\bar{\alpha}^{-1} = Ru_1 + Ru_2$ and $S' = Ru_1 + R\pi^j u_2, j \geq 0$ (see [3], (4.14)). The case $j = 0$ is trivial, so assume that $j > 0$. Then $1 = au_1 + b\pi^j u_2$, gives $a \in R^*$. Thus, $S'\bar{\alpha}^{-1} = R + Ru_2$, $S' = R + R\pi^j u_2$ and $S = R + R\pi^{i+j}u_2$, which shows that $d(S, S'\bar{\alpha}^{-1}) = d(S, S') + d(S', S'\bar{\alpha}^{-1})$. But $S'\bar{\alpha}^{-1} \sim S'\alpha$, so the required equality follows from (a) and (1.1).

Let S be an R-order in L. By an S-bouquet in A we mean the set $\mathfrak{B}(S, \Lambda)$ of all Eichler orders in A isomorphic to Λ, which optimally contain S. The group L^* acts on $\mathfrak{B}(S, \Lambda)$ by conjugation: If $\Lambda' \in \mathfrak{B}(S, \Lambda)$ and $\alpha \in L^*$, then $\alpha\Lambda'\alpha^{-1} \in \mathfrak{B}(S, \Lambda)$. Let $e_*(S, \Lambda)$ be the number of L^*-orbits on $\mathfrak{B}(S, \Lambda)$. Our objective is to compute these numbers for arbitrary quadratic R-orders S and arbitrary Eichler orders Λ, when $R/\mathfrak{m}$ is finite. The first step in this direction is the following useful result:

(1.3) LEMMA. (*a*) *Each L^*-orbit on $\mathfrak{B}(S, \Lambda)$ contains an order $\Gamma(S) \cap \Gamma(S'\alpha)$, where $S' \supseteq S$.*

(*b*) *Two different orders $\Gamma(S) \cap \Gamma(S'\alpha)$ and $\Gamma(S) \cap \Gamma(S''\beta)$ are in the same L^*-orbit if and only if $S'' = S' = S$ and $S\beta \sim S\bar{\alpha}$.*

Proof. (a) Since $\dim_K L = 2$, each R-lattice I on L is principal over its order $O(I)$, that is, $I = O(I)\alpha$ for a suitable $\alpha \in L^*$ (see [3], (35.14)). Let $\Lambda = \Gamma(I_1) \cap \Gamma(I_2)$. Since the R-orders in L are linearly ordered by inclusion, S must be optimally embedded in at least one of the orders $\Gamma(I_j), j = 1, 2$. Thus, we may choose $I_1 = S\alpha_1$ and $I_2 = S'\alpha_2$, where $S' \supseteq S$. Hence $\alpha_1^{-1}\Lambda\alpha_1 = \Gamma(S) \cap \Gamma(S'\alpha)$, where $\alpha = \alpha_2\alpha_1^{-1} \in L^*$.

(b) Let $\Lambda' = \Gamma(S) \cap \Gamma(S'\alpha)$ and $\Lambda'' = \Gamma(S) \cap \Gamma(S''\beta)$. If $\gamma\Lambda'\gamma^{-1} = \Lambda''$, $\gamma \in L^*$, then $\Gamma(S\gamma) = \Gamma(S)$ and $\Gamma(S'\alpha\gamma) = \Gamma(S''\beta\gamma)$, or $\Gamma(S\gamma) = \Gamma(S''\beta)$ and $\Gamma(S'\alpha\gamma) = \Gamma(S)$, since the maximal orders containing an Eichler order are unique. In the first case, $S\gamma \sim S$ and $S'\alpha\gamma \sim S''\beta\gamma$, so $S' = S''$, and consequently, $\Lambda' = \Lambda''$. In the second case, we get $S\gamma \sim S''\beta$ and $S'\alpha\gamma \sim S$, so $S = S' = S''$ and $S\alpha\beta \sim S$, which is equivalent to $S\beta \sim S\bar{\alpha}$. Conversely, if $S\beta \sim S\bar{\alpha}$, then clearly $\Gamma(S) \cap \Gamma(S\alpha)$ and $\Gamma(S) \cap \Gamma(S\beta)$ are in the same L^*-orbit.

Let S be an R-order in L. The last proposition and (1.1) show that in order to compute the numbers $e_*(S, \Lambda)$, we have to describe all K-classes of S-ideals $S\alpha$ and compute $d(S, S\alpha)$ for them. Let $C\ell(S/R)$ denote the multiplicative group of all principal S-ideals in L modulo the S-ideals generated by the elements of K^*. We have to distinguish between 3 cases: L is an unramified field extension of K (unramified case), L is a ramified field extension of K (ramified case), and $L = K \times K$ (split case). Recall that the R-orders in L are $S_i = R + \pi^i S_0, i \geq 0$,

where S_0 is the maximal R-order. Let $e = v(2)$, and let $k = |R/\mathfrak{m}|$ be the number of elements in the residue field of R. In order to simplify formulations, we assume that $k^n = 0$, when $n < 0$.

(1.4) PROPOSITION. (*a*) *Let* $L \supset K$ *be unramified, that is,* $L = K(\omega)$ *and* $S_0 = R[\omega]$, *where* $\omega^2 - \omega + \varepsilon = 0$, $\varepsilon \in R^*$ *and* $1 - 4\varepsilon \in R^* \backslash R^{*2}$. *Then* $C\ell(S_i/R)$ *consists of K-classes of* $S_i(a + \beta)$ *and* $S_i(1 + b\omega)$ *where* $\pi | b$ *and* $i \geqq 1$, *for a and b representing different residue classes in* $R/(\pi^i)$. *We have* $d(S_i, S_i(a + \omega)) = 2i$ *for* k^i *elements of* $C\ell(S_i/R)$, *and* $d(S_i, S_i(1 + b\omega)) = 2i - 2r$ *for* $k^{i-r} - k^{i-r-1}$ *elements of* $C\ell(S_i/R)$ *corresponding to* $b \in \pi^r R^*$ *and* $r \in \{1, \ldots, i\}$.

(*b*) *Let* $L \supset K$ *be ramified, that is,* $L = K(\omega)$ *and* $S_0 = R[\omega]$, *where* $\omega^2 - \pi^\rho \omega + \varepsilon\pi = 0$, $\varepsilon \in R^*$ *and* $\rho \in \{1, \ldots, e + 1\}$. *Then* $C\ell(S_i/R)$ *consists of K-classes of* $S_i(a + \omega)$, *where* $\pi | a$, *and* $S_i(1 + b\omega)$ *for* a/π *and b representing different residue classes in* $R/(\pi^i)$. *We have* $d(S_i, S_i(a + \omega)) = 2i + 1$ *for* k^i *elements of* $C\ell(S_i/R)$, *and* $d(S_i, S_i(1 + b\omega)) = 2i - 2r$ *for* $k^{i-r} - k^{i-r-1}$ *elements of* $C\ell(S_i/R)$ *corresponding to* $b \in \pi^r R^*$ *and* $r \in \{0, \ldots, i\}$.

(*c*) *Let* $L \supset K$ *be split, that is,* $L = K \times K$ *and* $S_0 = R \times R$. *Then* $C\ell(S_i/R)$ *consists of K-classes of* $S_i(1, a)(\pi^r, 1)$, $r \geqq 0$ *and* $S_i(1, a)(1, \pi^r)$, $r \geqq 1$ *for a representing different residue classes in* $(R/(\pi^i))^*$. *We have* $d(S_i, S_i(1, a)(\pi^r, 1)) = d(S_i, S_i(1, a)(1, \pi^r)) = 2i + r$ *if* $r \neq 0$ *or* $a \neq 1$, *for* $k^i - k^{i-1} - 1$ *elements of* $C\ell(S_i/R)$ *when* $r = 0$, *and for* $2(k^i - k^{i-1})$ *such elements when* $r \geqq 1$.

Proof. (a) Without changing the class of a principal S_i-ideal I, one can choose $\alpha \in S_0$ such that $I = S_i\alpha$. Since $C\ell(S_0/R)$ is trivial, one can assume that $\alpha \in S_0^*$, that is, $\alpha = a + b\omega$, where $\pi \nmid a$ or $\pi \nmid b$. Therefore, one can further reduce assuming that each class of S_i-ideals contains either an ideal $S_i(a + \omega)$ or $S_i(1 + b\omega)$ with $\pi | b$. Now it is easy to check that the classes of $S_i(a + \omega)$ and $S_i(1 + b\omega)$ are different if $i \geqq 1$, while $S_i(a + \omega) \sim S_i(a' + \omega)$ (or $S_i(1 + b\omega) \sim S_i(1 + b'\omega)$) if and only if $a \equiv a' \pmod{\pi^i}$ (or $b \equiv b' \pmod{\pi^i}$). The last statement in (a) now follows from (1.2)(a).

(b) It is well-known that $C\ell(S_0/R)$ has two elements represented by S_0 and $S_0\omega$. The same arguments as in (a) show that the elements of $C\ell(S_i/R)$ are represented by $S_i\alpha$ with $S_0\alpha = S_0$ or $S_0\alpha = S_0\omega$. In the first case, one can assume that $\alpha = 1 + b\omega$, and in the second, that $\alpha = (1 + b\omega)\omega = a + \omega$ for a suitable $a \in (\pi)$. The remaining arguments are the same as in (a), with the only difference that $S_i(a + \omega) \sim S_i(a' + \omega)$ if and only if $a \equiv a' \pmod{\pi^{i+1}}$.

(c) The group $C\ell(S_0/R)$ is infinite and its elements are represented by the ideals $S_0(\pi^r, 1)$, $r \geqq 0$, and $S_0(1, \pi^r)$, $r \geqq 1$. The proof is similar to that of (a) and (b).

The last proposition together with (1.2) give an easy possibility to compute the number of intersections $\Gamma(S) \cap \Gamma(S'\ \delta)$ (not necessarily different) equal to an Eichler order with fixed discriminant.

(1.5) PROPOSITION. *Let the notations be the same as in* (1.4). *All Eichler orders* $\Gamma(S_i) \cap \Gamma(S_j\,\delta)$ *with discriminant* d *and* $0 \leqq j \leqq i$ *are given in the following way*:

(*a*) *Let* $L \supset K$ *be unramified. Then* $0 \leqq d \leqq 2i$. *For* $0 \leqq d \leqq 2i-2$, *and for each* $j \in [|i-d|, i]$ *such that* $j \equiv i-d \pmod 2$ *and* $j \geqq 2$ *when* $d \geqq i$, *there are* $k^{j-v(b)} - k^{j-v(b)-1}$ *orders with* $\delta = 1 + b\omega$ *and* $v(b) = (j+i-d)/2$. *For* $i \leqq d \leqq 2i$ *and* $j = d - i$ *there are* k^j *orders with* $\delta = a + \omega$.

(*b*) *Let* $L \supset K$ *be ramified. Then* $0 \leqq d \leqq 2i+1$. *For* $0 \leqq d \leqq 2i$, *and for each* $j \in [|i-d|, i]$ *such that* $j \equiv i-d \pmod 2$, *there are* $k^{j-v(b)} - k^{j-v(b)-1}$ *orders with* $\delta = 1 + b\omega$ *and* $v(b) = (j+i-d)/2$. *For* $i+1 \leqq d \leqq 2i+1$ *and* $j = d-i-1$ *there are* k^j *orders with* $\delta = a + \omega$.

(*c*) *Let* $L \supset K$ *be split. For* $0 \leqq d \leqq i$ *and* $j = i - d$ *there is one order with* $\delta = 1$. *For* $d > i$ *and for each* $j \in [0, \min(d-i, i)]$ *there are* $2(k^j - k^{j-1})$ *orders with the exception of* $j = d - i$, *when the number of orders is* $k^j - k^{j-1} - 1$, *with* $\delta = (1, a)(\pi^r, 1), r \geqq 0$ *or* $(1, a)(1, \pi^r), r \geqq 1$ *and* $r = d - i - j$.

Proof. According to (1.2), $d = j - i + d(S_j, S_j\,\delta)$, and it suffices to use the results of (1.4) in order to obtain all possible intersections when d and i are fixed.

Using (1.5), it is very easy to compute the total number of intersections $\Gamma(S) \cap \Gamma(S'\,\delta)$, $S' \supseteq S$, which give an Eichler order with fixed discriminant d. This number is very close to the number of L^*-orbits on the corresponding S-bouquet. Unfortunately, the special case $S' = S$ (see (1.3)(b)) introduces a correcting term, which needs some additional computations. Let us start with a definition:

$$\kappa(x, y, i) = \left|\{(x, y) \in R/(\pi^i) \times R/(\pi^i) : x^2 \equiv y^2 (\bmod \pi^i)\}\right| \tag{1.6}$$

and

$$\kappa(x, y, i, r) = \left|\{(x, y) \in R/(\pi^i) \times R/(\pi^i) : x^2 \equiv y^2 (\bmod \pi^i) \quad \text{and } \bar{v}(x-y) = r\}\right|. \tag{1.7}$$

$\bar{v}$ is the valuation on $R/(\pi^i)$ induced by v on R. We assume that $\bar{v}(0) = i$ for $0 \in R/(\pi^i)$. $[x]$ will denote the integer part of the number x. We are now ready to compute the numbers $e_*(S, \Lambda)$:

(1.8) THEOREM. *Let* $S = S_i$ *be an* R*-order in* L, *and let* Λ *be an Eichler* R*-order in* A *with discriminant* d.

(*a*) *If* $L \supset K$ *is unramified, then*

$$e_*(S, \Lambda) = \begin{cases} 0 & \text{if } d > 2i, \\ \frac{1}{2}(k^{1/2d} + \kappa(x, x+1, i)) & \text{if } d = 2i, \\ k^{1/2(d-1)} & \text{if } 0 < d < 2i,\ d \text{ odd}, \\ \frac{1}{2}(k^{1/2d} + k^{1/2d-1} + \kappa(x, 1, i, i - \frac{1}{2}d)) & \text{if } 0 \leqq d < 2i,\ d \text{ even}, \end{cases}$$

where

$$\kappa(x, x+1, i) = \begin{cases} 1 & \text{if } e = 0 \text{ or } i = 0, \\ 0 & \text{otherwise}, \end{cases} \tag{1.9}$$

and

$$\kappa(x, 1, i, i - \tfrac{1}{2}d) = \begin{cases} k^{1/2d} - k^{1/2d-1} & \text{if } 0 \leqq d \leqq 2e < i \text{ or } 0 \leqq d \leqq i \leqq 2e, \\ k^e & \text{if } i \geqq 2e+1 \text{ and } d = 2i - 2k, \\ 0 & \text{otherwise.} \end{cases} \tag{1.10}$$

(*b*) *If* $L \supset K$ *is ramified, then*

$$e_*(S, \Lambda) = \begin{cases} 0 & \text{if } d > 2i+1, \\ \frac{1}{2}(k^{1/2(d-1)} + \kappa(x, x+\pi^\rho, i+\rho+1)) & \text{if } d = 2i+1, \\ k^{1/2(d-1)} & \text{if } 0 < d < 2i,\ d \text{ odd}, \\ \frac{1}{2}(k^{1/2d} + k^{1/2d-1} + \kappa(x, 1, i+\rho, i+\rho-\frac{1}{2}d)) & \text{if } 0 \leqq d \leqq 2i,\ d \text{ even}, \end{cases}$$

where

$$\kappa(x, x+\pi^\rho, i+\rho+1) = \begin{cases} k^i & \text{if } i \leqq \rho - 1 \\ k^e & \text{if } i > \rho - 1 = e \\ 0 & \text{otherwise} \end{cases} \tag{1.11}$$

and $\kappa(x, 1, i+\rho, i+\rho-\frac{1}{2}d)$ *is given by* (1.10) (*with* i *replaced by* $i+\rho$).

(*c*) *If* $L \supset K$ *is split, then*

$$e_*(S, \Lambda) = \begin{cases} k^i + k^{i-1} & \text{if } d > 2i, \\ \frac{1}{2}(k^{1/2d} + 3k^{1/2d-1} + \kappa(x, 1, i)) - 1 & \text{if } d = 2i, \\ k^{d-i} + k^{d-i-1} - 1 & \text{if } i < d < 2i, \\ 1 & \text{if } 0 \leqq d \leqq i, \end{cases}$$

where

$$\kappa(x, 1, i) = \begin{cases} k^{[1/2i]} & \text{if } 0 \leqq i \leqq 2e, \\ 2k^e & \text{if } i \geqq 2e+1. \end{cases} \tag{1.12}$$

Proof. (a) According to (1.5)(a), $e_*(S, \Lambda) = 0$ when $d > 2i$. It easily follows from (1.5)(a) that the total number of intersections $\Gamma(S) \cap \Gamma(S'\alpha)$ with discriminant d is equal to $k^{[1/2d]}$. This number is equal to $e_*(S, \Lambda)$ if in all intersections $S' \neq S$, which holds when $0 \leqq d \leqq 2i$ and d is odd. If $d = 2i$, then we have to consider the number of L^*-orbits on k^i intersections $\Gamma(S_i) \cap \Gamma(S_i\alpha)$, where $\alpha = a + \omega$. According to (1.3)(b), we need the number of α such that $S_i\bar{\alpha} = S_i\alpha$, that is, the number of a satisfying $2a + 1 \equiv 0 \pmod{\pi^i}$. This number is given by (1.9). If d is even and $0 \leqq d \leqq 2i$, then we have the intersections $\Gamma(S_i) \cap \Gamma(S_i\alpha)$ with $\alpha = 1 + b\omega$ and $v(b) = i - \frac{1}{2}d$. In this case, $S_i\bar{\alpha} = S_i\alpha$ if and only if $b^2 + 2b \equiv 0 \pmod{\pi^i}$. The number of solutions, which is equal to $\kappa(x, 1, i, i - \frac{1}{2}d)$, can be obtained from the following easy to prove result: if R is a discrete valuation ring, then $\kappa(x, 1, i)$ is given by (1.12) and the solutions to $x^2 \equiv 1 \pmod{\pi^i}$ are

$$x = \begin{cases} 1 + \pi^{[1/2(i+1)]}r & \text{for } 0 \leqq \bar{v}(r) \leqq [\frac{1}{2}i] \quad \text{if } 0 \leqq i \leqq 2e, \\ 1 + \pi^{i-e}r \quad \text{or } 1 - \varepsilon\pi^e + \pi^{i-e}r & \text{for } 0 \leqq v(r) \leqq e \quad \text{if } i \geqq 2e+1, \end{cases} \tag{1.13}$$

where $2 = \pi^e\varepsilon$.

(b) (1.5)(b) says that $e_*(S, \Lambda) = 0$ when $d > 2i + 1$. The total number of intersections $\Gamma(S) \cap \Gamma(S'\alpha)$ with discriminant d is also equal to $k^{[1/2d]}$. The intersections $\Gamma(S_i) \cap \Gamma(S_i\alpha)$ only appear for odd $d \leqq 2i + 1$. If $d = 2i + 1$, then $\alpha = a + \omega$, where $\pi | a$, give k^i intersections, and $S_i\bar{\alpha} = S_i\alpha$ if and only if $2a + \pi^\rho \equiv 0 \pmod{\pi^{i+1}}$. The number of solutions, which is equal to $\kappa(x, x + \pi^\rho, i + \rho + 1)$, can be obtained by elementary considerations. If $0 < d < 2i$, then $\alpha = 1 + a\omega$, where $v(a) = i - \frac{1}{2}d$ ($k^{1/2d} - k^{1/2d-1}$ intersections), and $S_i\bar{\alpha} = S_i\alpha$ if and only if $\pi^\rho a^2 + 2a \equiv 0 \pmod{\pi^i}$. The number of solutions is $\kappa(x, 1, i + \rho, i + \rho - \frac{1}{2}d)$ and can be computed using (1.13).

(c) The total number of intersections $\Gamma(S) \cap (S'\alpha)$ is 1 when $0 \leqq d \leqq i$, $k^{d-i} + k^{d-i-1} - 1$ when $i < d \leqq 2i$, and $2k^i$ when $d > 2i$. The intersections $\Gamma(S_i) \cap \Gamma(S_i\alpha)$ only appear if $d = 2i$ with $\alpha = (1, a)$, $a \in R^*$, $a \neq 1$ for $d > 0$ ($k^i - k^{i-1}$ possibilities) or $d > 2i$ with $\alpha = (1, a)(1, \pi^r)$ or $(1, a)(\pi^r, 1)$, where $r = d - 2i$ ($2(k^i - k^{i-1})$ possibilities). In the first case, $S_i\bar{\alpha} = S_i\alpha$ if and only if $a^2 \equiv 1 \pmod{\pi^i}$, which contributes with $\kappa(x, 1, i)$, while in the second case, the equality $S_i\bar{\alpha} = S_i\alpha$ is not possible.

(1.14) REMARK. It follows from (1.8) that $e_*(S, \Lambda) = 1$ when Λ is maximal, that is, $d = 0$. This is a special case of the Chevalley–Hasse–Noether theorem (see

[10], p. 13 or [4], Satz 6). The same is true when Λ is hereditary, that is, $d = 1$. This case was proved by M. Eichler (see [4], Satz 6).

Our main interest in Section 2 will be in the numbers of orbits of Λ^* acting by conjugation on the optimal embeddings of S into Λ. More exactly, if $\varphi : S \to \Lambda$ is an optimal embedding and $\sigma \in \mathrm{Aut}(\Lambda)$ (the automorphism group of Λ), then $\sigma \circ \varphi$ is also optimal. For simplicity of notations, we write σ to denote the inner automorphism $x \mapsto \sigma x \sigma^{-1}$ induced by $\sigma \in A^*$. Let $e_{\mathrm{Aut}(\Lambda)}(S, \Lambda)$ be the number of orbits for the action of $\mathrm{Aut}(\Lambda)$ on the optimal embeddings $S \to \Lambda$. It follows from a general theory that $e_{\mathrm{Aut}(\Lambda)}(S, \Lambda) = e_{L^*}(S, \Lambda)$ (see [1], (1.1) and (2.1)). Let us recall that any optimal embedding $\varphi : S \to \Lambda$ is given by $\varphi(x) = \sigma x \sigma^{-1}$, where $\sigma \in A^*$. Hence φ extends to an automorphism of A, and $\varphi^{-1}(\Lambda) \in \mathscr{B}(S, \Lambda)$. Conversely, if $\Lambda' \in \mathscr{B}(S, \Lambda)$, when $\Lambda' = \varphi(\Lambda)$ for a suitable automorphism of A, so φ^{-1} restricted to S gives an optimal embedding of S into Λ. In this way, we get a bijection between optimal embeddings in any $\mathrm{Aut}(\Lambda)$-orbit and the orders in the corresponding L^*-orbit.

We have $\Lambda^* \subseteq \mathrm{Aut}(\Lambda)$, and we want to compute the numbers $e^*_\Lambda(S, \Lambda)$ of Λ^*-orbits on the optimal embeddings $S \to \Lambda$. For simplicity, we shall write $e(S, \Lambda)$ instead of $e^*_\Lambda(S, \Lambda)$. Recall that for non-maximal Eichler order, $\mathrm{Aut}(\Lambda) = \Lambda^* \cup \Lambda^* \sigma$, where σ is a generator of the Jacobson radical $J(\Lambda)$ (see [2], (2.2)).

(1.15) LEMMA. *Let Λ be a non-maximal Eichler order in A. Then*

$$e(S, \Lambda) = 2e_*(S, \Lambda) - \kappa,$$

where κ is the term $\kappa(x, y, i)$ or $\kappa(x, y, i, r)$ in the formulas (1.8) *for $e_*(S, \Lambda)$ when it appears there and* 0 *otherwise.*

Proof. Let $\varphi : S \to \Lambda$ be an optimal embedding, and let $\Lambda = \Gamma(S) \cap \Gamma(S'\alpha)$. According to the comments concerning the equality $e_{\mathrm{Aut}(\Lambda)}(S, \Lambda) = e_{L^*}(S, \Lambda)$, we can suppose that φ is the identity. Since $L = KS$ is a maximal commutative subring of A, the stabilizer of φ in $\mathrm{Aut}(\Lambda) = \Lambda^* \cup \Lambda^* \sigma$ is $\mathrm{Aut}(\Lambda) \cap L^*$. The optimality of φ implies that $\Lambda^* \cap L^* = S^*$, and $\Lambda^* \sigma \cap L^* \neq \phi$ if and only if there is $\beta \in \mathrm{Aut}(\Lambda)$ and $\beta \in L^* \backslash S^*$. Thus $\mathrm{Aut}(\Lambda) \cap L^* = S^*$ or $\mathrm{Aut}(\Lambda) \cap L^* = S^* \cup S^* \beta$. In the first case, there are two Λ^*-orbits in the $\mathrm{Aut}(\Lambda)$-orbit of φ, while in the second, the Λ^*-orbit coincides with the $\mathrm{Aut}(\Lambda)$-orbit of φ. Assume now that such a β exists. Then we have $\Lambda = \beta \Lambda \beta^{-1} = \Gamma(S\beta) \cap \Gamma(S'\alpha\beta)$, which, as we already know (see the proof of (1.3)(b)), is valid if and only if $S' = S$ and $S\beta \sim S\alpha \sim S\bar{\alpha}$. Conversely, if $\Lambda = \Gamma(S) \cap \Gamma(S\alpha)$ and $S\alpha \sim S\bar{\alpha}$, then $\beta = \alpha$ is the desired element. Therefore, the number of Λ^*-orbits on the optimal embeddings $\varphi : S \to \Lambda$ which coincide with the corresponding $\mathrm{Aut}(\Lambda)$-orbits is equal to the number of L^*-orbits on $\mathscr{B}(S, \Lambda)$, which

are represented by $\Gamma(S) \cap \Gamma(S\alpha)$ with $S\alpha \sim S\bar{\alpha}$. These numbers, which were computed in the course of the proof of (1.8) as suitable values of the functions κ defined in (1.6) and (1.7), should be subtracted from the double of the number of all L^*-orbits on $\mathscr{B}(S, \Lambda)$.

Because of the importance of the embedding numbers $e(S, \Lambda)$ and for the convenience of references, we record the values of $e(S, \Lambda)$ in a form suitable for applications in the next section:

(1.6) COROLLARY. *Let $S = S_i$ be an R-order in L, and let Λ be an Eichler R-order in A with discriminant $d > 0$. Then*

$$e(S, \Lambda) = \begin{cases} 0 & \text{if } 0 \leqq i < \tfrac{1}{2}d, \\ k^{1/2d} & \text{if } i = \tfrac{1}{2}d, \\ k^{[1/2d]} + k^{[1/2(d-1)]} & \text{if } i > \tfrac{1}{2}d, \end{cases}$$

when $L \supset K$ is unramified,

$$e(S, \Lambda) = \begin{cases} 0 & \text{if } 0 \leqq i < \tfrac{1}{2}(d-1), \\ k^{1/2(d-1)} & \text{if } i = \tfrac{1}{2}(d-1), \\ k^{[1/2d]} + k^{[1/2(d-1)]} & \text{if } i \geqq \tfrac{1}{2}d, \end{cases}$$

when $L \supset K$ is ramified, and

$$e(S, \Lambda) = \begin{cases} 2(k^i + k^{i-1}) & \text{if } 0 \leqq i < \tfrac{1}{2}d, \\ k^{1/2d} + 3k^{1/2d-1} - 2 & \text{if } i = \tfrac{1}{2}d, \\ 2(k^{d-i} + k^{d-i-1} - 1) & \text{if } \tfrac{1}{2}d < i < d, \\ 2 & \text{if } i \geqq d, \end{cases}$$

when $L \supset K$ is split.

2. Stability of embedding numbers

As in Section 1, let R be a complete discrete valuation ring of characteristic $\neq 2$ with quotient field K. Let A be an arbitrary quaternion K-algebra (that is, a central simple algebra of dimension 4 over K), and let Λ be an R-order in A. In this Section, using the fact that $e(S, \Lambda)$ only depends on Λ when the conductor of S is sufficiently small, we show how to decide whether $e(S, \Lambda) = e(S', \Lambda)$ where S' is an R-order in another quadratic extension $L' \supset K$.

Let us start with some definitions. If X denotes an R-order in L or in A and $J(X)$ its Jacobson radical, define $e(X) = 1$ if $X/J(X) \cong R/\mathfrak{m} \times R/\mathfrak{m}$, $e(X) = 0$ if $X/J(X) \cong R/\mathfrak{m}$, and $e(X) = -1$ if $X/J(X)$ is a quadratic field extension of $R/\mathfrak{m}$. Let $L \subset K$ be a quadratic separable extension. Define $e(L/K) = e(S_0)$, where S_0 is the maximal R-order in L (that is, $e(L/K) = 1$, 0 or -1 depending on whether $L \supset K$ is split, ramified or unramified). Let $\Delta(L/K)$ be the discriminant of $L \supset K$, that is, the discriminant of any basis of the maximal R-order in L (computed with respect to the trace form $T : L \times L \to K$, $(x, y) \mapsto T(x, y)$, where T is the trace function from L to K). $\Delta(L/K)$ is defined up to a square of a unit in R.

If L and L' are two separable quadratic K-algebras, define:

$$\delta(L, L') = 2e + 1 + \min(v(\Delta(L/K)), v(\Delta(L'/K))), \tag{2.1}$$

where v is the valuation corresponding to R and $e = v(2)$. Recall that $e(L/K) = \pm 1$ if and only if $\Delta(L/K) \in R^*$, and $e(L/K) = 1$ if and only if $\Delta(L/K) \in R^{*2}$. If $e(L/K) = 0$, then $\Delta(L/K) \in \pi^\rho R^*$, where $\rho \in \{1, \ldots, e + 1\}$. The following well-known result is a direct consequence of the remarks above and the local square theorem (see [11], 63:1a):

(2.2) PROPOSITION. (*a*) *If* $\delta(L, L') = 2e + 1$, *then* $\Delta(L/K) \equiv (L'/K) (\mathrm{mod}\ 4\pi)$ *implies* $e(L/K) = e(L'/K)$. *If* $\delta(L, L') > 2e + 1$, *then* $e(L/K) = e(L'/K)$.

(*b*) $L \cong L'$ *if and only if* $\Delta(L/K) \equiv \Delta(L'/K) (\mathrm{mod}\ \pi^{\delta(L,L')})$.

It is clear from (1.16) that the numbers $e(S, \Lambda)$ depend on $e(L/K)$. In general, when Eichler orders are replaced by arbitrary quaternion orders, it is easy to construct examples showing the dependence of $e(S, \Lambda)$ on the isomorphism class of $L \supset K$ (see (13.9)(b)). Of course, they also depend on the conductor of S with respect to the maximal R-order S_0 in L. Recall that if $S = R + \pi^i S_0$, then the conductor $f(S/R)$ is the ideal (π^i) (that is, $f(S/R) = (\pi^{d(S,S_0)}) = \mathrm{Ann}\ (S_0/S)$).

The most important property of the embedding numbers $e(S, \Lambda)$ from the point of view of applications, which we have in mind, is that they stabilize when $f(S/R)$ is sufficiently small with respect to the discriminant of Λ. Unfortunately, we cannot prove this for arbitrary quaternion orders, since our proof is based on the explicit computations of $e(S, \Lambda)$ for Eichler orders in Section 1, and in [2] for other classes of Bass orders. We slightly extend these results to orders whose Gorenstein closure is a Bass order (see (2.3)), but the embedding numbers $e(S, \Lambda)$ still have to be computed for Gorenstein non-Bass orders. Recall that Λ is a Gorenstein order if $\mathrm{Hom}_R(\Lambda, R)$ is Λ-projective as left (or right) Λ-module (see [3], p. 776). Λ is a Bass order if each R-order Λ' in A containing Λ is Gorenstein. If Λ is an arbitrary R-order in A, then $\Lambda = R + \pi^r G(\Lambda)$, where $G(\Lambda)$ is a Gorenstein R-order contain-

ing Λ and $r > 0$. Both $G(\Lambda)$ and r are uniquely determined by the above presentation of Λ (see [2], Section 1).

(2.3) PROPOSITION. *Let $S_i = R + \pi^i S_0$ be an R-order in L, and let $\Lambda = R + \pi^r G(\Lambda)$ be an R-order in A with Gorenstein closure $G(\Lambda)$. Then*

$$e(S_i, \Lambda) = k^{2r+1} \frac{1 - e(G(\Lambda))k^{-1}}{k - e(S_{i-r})} e(S_{i-r}, G(\Lambda)),$$

where we put $e(G(\Lambda)) = 1/k$ when $G(\Lambda)$ is a maximal order in a split K-algebra A.

Proof. It is easy to see that any optimal embedding $S' \to G(\Lambda)$ restricts to an optimal embedding $S = R + \pi^r S' \to \Lambda$, and conversely, any optimal embedding $S \to \Lambda$ can be uniquely extended to an optimal embedding $S' \to G(\Lambda)$, where $S = R + \pi^r S'$. In particular, if $S_i \to \Lambda$ is an embedding, then $i \geqq r$. Since Λ^* is normal in $G(\Lambda)^*$, the last group acts on optimal embeddings $S_i \to \Lambda$. The number of Λ^*-orbits in one $G(\Lambda)^*$-orbit for this action is equal to $(G(\Lambda)^* : \Lambda^*)/(S_{i-r}^* : S_i^*)$, since the optimality of the embeddings $S_i \to \Lambda$ and $S_{i-r} \to G(\Lambda)$ implies that the stabilizer of $S_i \to \Lambda$ in $G(\Lambda)^*$ is S_{i-r}^*. Now it is an easy task to compute the indices: $(G(\Lambda)^* : \Lambda^*) = k^{3r}(1 - e(G(\Lambda))k^{-1})$ and $(S_{i-r}^* : S_i^*) = k^{r-1}(k - e(S_{i-r}))$.

Let $d(\Lambda)$ denote the discriminant ideal of Λ (see [2], p. 167). We can now prove that $e(S_i, \Lambda)$ stabilize when i is sufficiently large.

(2.4) PROPOSITION. *Let S_i be an R-order in L, and let $\Lambda = R + \pi^r G(\Lambda)$ be an R-order in A whose Gorenstein closure is a Bass order. Then $e(S_i, \Lambda)$ have the same value for $i \geqq v(d(\Lambda)) - 2r$ when $e(\Lambda) = e(L/K) = 1$, and for $i > \frac{1}{2}(v(d(\Lambda)) - r)$ in all other cases.*

Proof. Let $r = 0$ and let $v(d(\Lambda)) = d$. It follows from (1.16) that $e(S_i, \Lambda) = k^{[1/2d]} + k^{[1/2(d-1)]}$ for $i > \frac{1}{2}d$ and $e(L/K) \neq 1$, while $e(S_i, \Lambda) = 2$ for $i \geqq d$, when $e(L/K) = 1$. Similarly, from [2], (3.3) and (3.10), we get $e(S_i, \Lambda) = 0$ for $i > \frac{1}{2}d$ when A is ramified. If A is split, the same references give $e(S_i, \Lambda) = c(k^{[1/2d]} - k^{[1/2d]-1})$, where $c = 0$ or 2 if $e(\Lambda) = 0$ or $e(\Lambda) = e(L/K) = -1$, and $c = 1$ if $e(\Lambda) = -1$ and $e(L/K) \neq -1$.

If $r > 0$, then the estimates for i now follow from the equality $v(d(\Lambda)) = v(d(G(\Lambda))) + 3r$ and (2.3).

Let Λ be an R-order in A. Denote by $i(\Lambda, L/K)$ the least non-negative integer such that $e(S_i, \Lambda)$ have the same value for $i \geqq i(\Lambda, L/K)$. The existence of $i(\Lambda, L/K)$ follow from (2.4) for quaternion orders whose Gorenstein closure is a Bass order

(and it remains to be proved for Gorenstein non-Bass orders). The following result is a direct consequence of (2.2) and the definition of $i(\Lambda, L/K)$:

(2.5) PROPOSITION. *Let S be an R-order in L, S' an R-order in L' and Λ an R order in A. If (a) $\Delta(L/K) \equiv \Delta(L'/K) (\mathrm{mod}\ \pi^{\delta(L,L')})$ and (b) $f(S/R) \equiv f(S'/R) (\mathrm{mod}\ \pi^{i(\Lambda,L/K)})$, then $e(S, \Lambda) = e(S', \Lambda)$.*

(2.6) REMARK. It follows from (2.4) that for an order $\Lambda = R + \pi' G(\Lambda)$ whose Gorenstein closure $G(\Lambda)$ is a Bass order, we have $i(\Lambda, L/K) \leqq v(d(\Lambda)) - 2r$, when $e(\Lambda) = e(L/K) = 1$ and $i(\Lambda, L/K) \leqq [\frac{1}{2}(v(d(\Lambda)) - r)] + 1$ in all other cases. It follows from (1.16) and from [2], (3.3), (3.10) that the second estimate can be improved. In fact, $i(\Lambda, L/K) \leqq [\frac{1}{2}(d(\Lambda) - r + 1)]$ if A is a division algebra and $(e(\Lambda), e(L/K)) \neq (0, -1)$, or A is a split algebra and $(e(\Lambda), e(L/K)) = (0, 0), (0, -1)$ or $(1, 0)$.

3. Representations of integers

We are now ready to discuss some applications of the embedding numbers to representations of integers by ternary quadratic forms.

Let $f(x_1, x_2, x_3) = \Sigma_{i \leq j} a_{ij} x_i x_j$ be a definite integral primitive ternary quadratic form, $\mathrm{Aut}^+(f)$ the group of its integral automorphisms with determinant 1, and $r_f(N)$ the number of primitive representations of N by f, that is, the number of $(x_1, x_2, x_3) \in \mathbb{Z}^3$ such that $N = f(x_1, x_2, x_3)$ and $GCD(x_1, x_2, x_3) = 1$. The following result was proved in [1], (3.8):

(3.1) THEOREM. *Let f be a definite integral ternary quadratic form and let $f_1 = f, \ldots, f_t$ represent all classes in the genus of f. Then there exist a quaternion $\mathbb{Z}$-order Λ and an integer $c_f > 0$ such that*

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} = \rho_\Lambda \frac{1}{|S^*|} \prod_p e(S_p, \Lambda_p), \tag{3.2}$$

where ρ_Λ is a rational number which only depends on Λ, $S = \mathbb{Z}[\sqrt{-c_f N}]$, $h(S)$ is the class number of S, and $e(S_p, \Lambda_p)$ are the embedding numbers for p-adic completions of S and Λ at all prime numbers p.

Let us recall how to find $\Lambda = \Lambda_f$ and c_f. Let

$$M(f) = \begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}$$

be the matrix of the quadratic form f, and let c_0 be the least positive integer such that $c_0 M(f)^{-1}$ is a matrix whose all elements are even integers. It is easy to show that $c_0 = 4d(f)/\Omega(f)$, where $d(f) = \frac{1}{2}\det M(f)$ is the discriminant of f, and $\Omega(f)$ is the *GCD* of the elements of the adjoint matrix $M(f)^d$ (notice that c_0 is closely related to the "level" of f). Let f_* be the quadratic form whose matrix is $c_0 M(f)$. Then $\Lambda_f = O(f_*)$, where $O(f_*)$ is the even Clifford algebra corresponding to the quadratic form f_* (see [1], Section 3) and $c_f = 4d(f)/\Omega(f)^2$. It is not difficult to show that $d(\Lambda_f)$ is generated by $16d(f)^2/\Omega(f)^3$. Notice that f_* need not be primitive, since the *GCD* of its coefficients may be equal to 2. In such a case, $O(f_*) = \mathbb{Z} + 2G(O(f_*))$. (In general, if f is an integral ternary quadratic form and $f = af_0$, then $O(f) = \mathbb{Z} + aO(f_0)$, and $O(f_0)$ is Gorenstein if and only if f_0 is primitive.)

Our objective is to analyse the right hand side in (3.2) using the information about the embedding numbers $e(S_p, \Lambda_p)$. Unfortunately, we only know these numbers for Λ such that $G(\Lambda)$ is a Bass order. Therefore, we have to restrict the class of quadratic forms f to those satisfying the following condition:

$$G(\Lambda_f) \text{ is a Bass order.} \tag{3.3}$$

Notice that it is very easy to recognize f satisfying (3.3): $G(\Lambda_f)$ is the order corresponding to f_* divided by the *GCD* of its coefficients. If, in general, $\Lambda = O(g)$, where g is an integral primitive quadratic form, then Λ is a Bass order at p if and only if $p \nmid \Omega(g)$ or $p \| \Omega(g)$ and a non-zero element of $(p)/(p)^2$ is represented over $\mathbb{Z}_p$ (the p-adic integers) by g reduced modulo p^2 (see [2], (3.21)). Λ is a Bass order if and only if it is a Bass order at each p (see [3], p. 778). We have $e(\Lambda_p) = 1$, 0 or -1 depending on whether the reduction of g modulo p is a product of two different linear factors, two equal linear factors or is irreducible over $\mathbb{Z}/(p)$ (see [2], (3.21)).

Before we can formulate the main result of this section, we need some notations. We write v_p to denote the valuation on $\mathbb{Q}$ or $\mathbb{Q}_p$ corresponding to p and such that $v_p(p) = 1$. We let $d(\Lambda)$ denote the positive generator of the discriminant ideal of Λ (denoted by $d(\Lambda)$ as well).

(3.4) THEOREM. *Keeping the notations of* (3.1) *assume that f satisfies* (3.3), *and let*

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} = \gamma(N)h(S),$$

where $S = \mathbb{Z}[\sqrt{-c_f N}]$ *and* $\gamma(N) = \rho_\Lambda(1/|S^*|)\,\Pi_p\, e(S_p, \Lambda_p)$.

There exists a positive integer M_0 such that γ has the following property: Let $c_f N = N_0^2 N_1 \neq 1$, $c_f N' = N_0'^2 N_1'$, where N_0, N_1, N_0', N_1' are integers and N_1, N_1' are square-free, and let for all $p | d(\Lambda_f)$:

$$v_p(N_0) = v_p(N_0') \quad \text{or} \quad \min(v_p(N_0), v_p(N_0')) \geqq \min v_p(M_0), \tag{3.5}$$

and

$$N_1 p^{-v_p(N_1)} \equiv N_1' p^{-v_p(N_1')} (\mathrm{mod}\, p^{2e+1}), \tag{3.6}$$

where $e = v(2)$. Then $\gamma(N) = \gamma(N')$. Moreover, one can choose $M_0 = d(\Lambda_f)$.

Proof. If $-c_f N \neq 1$, then $|S^*| = 2$, so the factor $\rho_\Lambda(1/|S^*|)$ in $\gamma(N)$ is independent of N. The factor following it depends on the discriminant of $Q(\sqrt{-c_f N})$ (that is, $4N_1$ or N_1 when $N_1 \equiv 3 (\mathrm{mod}\, 4)$) and the conductor of S (that is, N_0 or $2N_0$ when $N_1 \equiv 3 (\mathrm{mod}\, 4)$). Thus the property of γ directly follows from (2.5). The (not always optimal) choice of M_0 follows from (2.4) (see (3.8)).

It follows from (3.4) that the values of $\gamma(N) = \gamma(N_0, N_1)$ depend on the residues of N_0 modulo M_0 and N_1 modulo a positive integer M_1. According to (3.6), one can choose $M_1 = 4d_1(\Lambda_f)$, where $d_1(\Lambda_f)$ is the square-free part of $d(\Lambda_f)$ (notice that $d(\Lambda_f)$ is always divisible by 2). Thus, we have

(3.7) COROLLARY. *There exist positive integers M_0 and M_1 such that the values of the function $\gamma(N) = \gamma(N_1, N_1)$ for $c_f N \neq 1$ are determined by the residues of N_0 modulo M_0 and N_1 modulo M_1.*

(3.8) REMARK. (a) A special case of the above result was proved in [7] for N relatively prime to the discriminant of f. Probably, Siegel's formula for the weighted average of the number of integral representations by genus in case of ternary quadratic forms also can lead to a proof of (3.4).

(b) $\gamma(N) = \gamma(N_0, N_1)$ can be computed using a finite number of "test values" for N. But the choice of M_0 in (3.4) often can be improved. First of all, if $p = 2$, and $N_1 \equiv 3 (\mathrm{mod}\, 4)$, then $d(\Lambda_f)$ can be replaced by $\frac{1}{2} d(\Lambda_f)$, since the conductor of S is $2N_0$. If Λ_f is not a Gorenstein order, then one can take $M_0 = \frac{1}{4} d(\Lambda_f)$ (see (2.6)). If $e(G(\Lambda_f)_p) \neq 1$, then one can choose M_0 with $v_p(M_0) = [\frac{1}{2}(v_p(d(\Lambda_f)) - r] + 1$ where $r = 0$ or 1 and $r = 1$ if and only if $p = 2$ and Λ_f is not Gorenstein (see (2.6)). Slightly better estimates can be obtained in particular cases mentioned at the end of (2.6).

(3.9) EXAMPLES. (a) Three-Square-Theorem. Let $f = X^2 + Y^2 + Z^2$. Then $t = 1$, $|\mathrm{Aut}^+(f)| = 24$, $d(\Lambda_f) = 4$ and $c_f = 1$ (see [1], (3.9)(a)). Since $e((\Lambda_f)_2) = 0$, we can choose $M_0 = 2$ using (3.8) (instead of $M_0 = 4$ in (3.4)). Since there are 8 quadratic extensions of $\mathbb{Q}_2$, we have to compute $\gamma(N)$ for 16 values of N corresponding to N such that $v_2(N_0) = 0$ or 1 and N_1 giving non-isomorphic quadratic extensions (and $N \neq 1$). If $v_2(N_0) = 1$, we easily find that $r_f(N) = 0$, so $\gamma(N) = 0$. If $v_2(N_0) = 0$, we choose $N_1 = 3$ (unramified case), $N_1 = 7$ (split case), and $N_1 = 1, 5, 2, 6, 10, 14$ (ramified case). Choosing $N_0 = 1$ if $N_1 \neq 1$, and $N_0 = 3$ for $N_1 = 1$, we get $\gamma(N)$ for all integers $N \neq 1$. The final result is $\gamma(N) = 0$ if $N \equiv 0, 4, 7 \pmod 8$, $\gamma(N) = \frac{1}{3}$ if $N \equiv 3 \pmod 8$ and $\gamma(N) = \frac{1}{2}$ if $N \equiv 1, 2 \pmod 4$. It is, of course, a coincidence that the congruence conditions on N_0 and N_1 can be replaced by such a condition on N. It is also a coincidence that $\gamma(N)$ only depends on the type of the quadratic extension of $\mathbb{Q}_0$ corresponding to N_1.

(b) As a more typical example, let us consider $f = X^2 + Y^2 + 2Z^2$. In this case, $t = 1$, $|\mathrm{Aut}^+(f)| = 8$, $d(\Lambda_f) = 16$ and $c_f = 2$. (Notice that $\Lambda_f = \mathbb{Z} + \mathbb{Z}I + \mathbb{Z}J + \mathbb{Z}K$, where $I = i + j$, $J = i - j$, $K = 2k$ and i, j, k are the quaternion units.) We have $e((\Lambda_f)_2) = 0$. Hence if $e(\mathbb{Q}_2(\sqrt{-N_1})/\mathbb{Q}_2) \neq -1$, then $v_2(M_0) = [\frac{1}{2}(v_2(d(\Lambda_f)) + 1)] = 2$, and if $e(\mathbb{Q}_2(\sqrt{-N_1})/\mathbb{Q}_2) = -1$, then the conductor of S is $2N_0$, so $v_2(M_0) = [\frac{1}{2}v_2(d(\Lambda_f))] = 2$. Thus, we can choose $M_0 = 4$ and we have to look at the values of $\gamma(N)$ corresponding to $v_2(N_0) = 0, 1, 2$ and N_1 as in (a), where $2N = N_0^2 N_1$. If $v_2(N_0) = 0$, then N_1 must be even, so we can choose $N_0 = 1$ and $N_1 = 2, 6, 10, 14$. If $v_2(N_0) = 2$, then we easily get $r_f(N) = 0$, that is, $\gamma(N) = 0$. If $v_2(N_0) = 1$, we take $N_0 = 2$ and we compute $\gamma(N)$ for 8 possible N_1 as in (a) obtaining two different values of $\gamma(N)$, when $\mathbb{Q}_2(\sqrt{-N_1})$ is ramified. More exactly, we get:

$$r_f(N) = \left\{ \begin{array}{lll} 0 & \text{if } v_2(N_0) = 1 \text{ and } N_1 \equiv 7 \pmod 8 \text{ or } v_2(N_0) \geqq 0 & \\ & & (\gamma(N) = 0), \\ 2h(\mathbb{Z}[\sqrt{-2N}]) & \text{if } v_2(N_0) = 1 \text{ and } N_1 \equiv 3 \pmod 8 & (\gamma(N) = \tfrac{1}{4}), \\ 4h(\mathbb{Z}[\sqrt{-2N}]) & \text{if } v_2(N_0) = 0 \text{ or } 1 \text{ and } N_1 \equiv 0 \pmod 2 & (\gamma(N) = \tfrac{1}{2}), \\ 6h(\mathbb{Z}[\sqrt{-2N}]) & \text{if } v_2(N_0) = 1 \text{ and } N_1 \equiv 1 \pmod 4 & (\gamma(N) = \tfrac{3}{4}). \end{array} \right\}$$

(3.10) REMARK. Let

$$\theta(\mathrm{gen}\, f, z) = M_f^{-1} \sum_{i=1}^{t} \frac{\theta(f_i, z)}{|\mathrm{Aut}^+(f_i)|},$$

where

$$M_f = \sum_{i=1}^{t} \frac{1}{|\mathrm{Aut}^+(f_i)|},$$

be the theta series of the genus of f. This function is an Eisenstein series in the sense of [12], whose N-th coefficient for square-free N is $M_f^{-1}\gamma(N)h(S)$. (Notice that the N-th coefficient of $\theta(f, z)$ is equal to the number of all integral solutions to $f = N$, while $r_f(N)$ in (3.4) only counts the primitive ones. If N is square-free, then $r_f(N)$ is the coefficient.) Corollary (3.7) gives the periodicity of the factor following $h(S)$. A similar property is well-known for the coefficients of Eisenstein series of weight $k/2$, $k \geq 5$, as defined in [9] (see Prop. 5, p. 188). One can expect that when the group $\Gamma_0(4)$ (which is related to the sum of three squares by [12], Kor. 1, p. 289) is replaced by $\Gamma_0(N)$, then for all coefficients the period 8 in [9], Prop. 5, p. 188, will be replaced by two periods as in (3.6).

REFERENCES

[1] J. BRZEZINSKI, *A combinatorial class number formula*, J. reine angew. Math. *402* (1989) 199–210.
[2] J. BRZEZINSKI, *On automorphisms of quaternion orders*, J. reine angew. Math. *403* (1990) 166–186.
[3] C. W. CURTIS and I. REINER, Methods of representation theory, Vol. I, New York 1981.
[4] M. EICHLER, *Zur Zahlentheorie der quaternionen-Algebren*, J. reine angew. Math. *195* (1955) 127–151.
[5] H. HIJIKATA, *Explicit formula of the traces of the Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan *26* (1974) 56–82.
[6] H. HIJIKATA, A. PIZER and T. SHEMANSKE, *Orders in quaternion algebras*, J. reine angew. Math. *394* (1989) 59–106.
[7] B. W. JONES, *Representations by quadratic forms*, Ann. of Math. *50* (1949) 884–899.
[8] M.-A. KNUS and M. OJANGUREN, *Théorie de la Descente et Algèbres d'Azumaya*, Lecture Notes in Mathematics *389*, Berlin–Heidelberg–New York 1974.
[9] N. KOBLITZ, Introduction to elliptic curves and modular forms, Berlin–Heidelberg–New York 1984.
[10] E. NOETHER, *Zerfallende verschränkte Produkte und ihre Maximalordnungen*, Act. Sci. Ind. Paris *148* (1934) 5–15.
[11] O. T. O'MEARA, Introduction to quadratic forms, Berlin–Heidelberg–New York 1973.
[12] R. SCHULZE-PILLOT, *Thetareihen positiv definiter quadratischer Formen*, Invent. math. *75* (1984) 283–299.

Department of Mathematics
Chalmers University of Technology and University of Göteborg
S-412 96 Göteborg, Sweden

Received September 18, 1990