Abstract

Let R be the ring of integers in a totally real algebraic number field K and let $f(x_1, x_2, x_3)$ be a totally definite ternary quadratic form with coefficients in R. The purpose of this paper is to study representations of the elements in R by f. We prove a quantitative formula relating the number of representations of $N \in R$ by different classes in the genus of f to the class number of $R[\sqrt{-N}]$. We use this formula when the class number is one. In particular, we give an algebraic proof of a classical result of H. Maass on representations by sums of three squares over the integers in $\mathbb{Q}[\sqrt{5}]$, and moreover, we obtain an explicit dependence between the number of representations and the class numbers of the corresponding biquadratic fields.

Keywords: ternary quadratic form, quaternion order, even Clifford algebra, quaternion algebra, embedding number.

AMS 1991 Subject classification: 11E12, 16H05, 11E20, 11E25, 11E88.

Acknowledgement

I would like to thank my advisor Juliusz Brzezinski. I'm most grateful for his patience, guidance and support.

Contents

0 Introduction

Let $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$. Let $N \in \mathbb{Z}$ be a square-free positive integer such that $N \neq 1, 3$ and let $S = \mathbb{Z}[\sqrt{-N}]$. Gauss proved that the number of solutions $(x_1, x_2, x_3) \in \mathbb{Z}^3$ to the equation $f(x_1, x_2, x_3) = N$ is

$$r_f(N) = \begin{cases} 12h(S) & \text{for } N \equiv 1, 2 \pmod 4, \\ 8h(S) & \text{for } N \equiv 3 \pmod 8, \\ 0 & \text{for } N \equiv 7 \pmod 8, \end{cases}$$

where $h(S)$ denotes the class number of S. In 1940 it was shown by Hans Maass that every totally positive number $N \in R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ can be represented by f, where $x_1, x_2, x_3 \in R$ (see [13]). One of the results of the present paper is an algebraic proof of this. Moreover, we prove that there is always a primitive representation of N by f (see Thm. 6.2). Furthermore, using a result on the stability of embedding numbers, given in Section 5, we find that the number of primitive representations of a totally positive $N \in R$, denoted by $r_f^0(N)$, is given by

$$r_f^0(N) = \gamma_i h(S),$$

where $S = R[\sqrt{-N}]$ and $\gamma_i = 12, 24, 32, 96$ or 384.

In this paper, we shall discuss similar results for representations of integers by totally definite ternary quadratic forms with integer coefficients in totally real algebraic number fields.

More generally, let R be a principal ideal domain and let K denote its quotient field. Let A be a quaternion algebra over K, i.e. a central simple K-algebra of dimension four, and let Λ denote an R-order in A. In Section 3, we prove that one can always find a free R-lattice $L = Re_1 + Re_2 + Re_3$ and a ternary quadratic form $q(x_1e_1 + x_2e_2 + x_3e_3) = \sum a_{ij} r_i r_j$ such that $\Lambda \cong C_0(L, q)$, where $C_0(L, q)$ denotes the even Clifford algebra. In Section 4, we show that there is a one-to-one correspondence between similarity classes of R-lattices with non-degenerate ternary quadratic forms and isomorphism classes of quaternion orders over R. The similarity class of (L, q) corresponds to the isomorphism class of $C_0(L, q)$. This is useful when we examine repre-

sentations of totally positive algebraic integers by ternary quadratic forms.

Assume K to be an algebraic number field. Given a totally positive definite ternary quadratic form, we can construct an R-order Λ in a quaternion algebra over K, such that the representations of a totally positive integer $N \in R$ by f are in one-to-one correspondence with the solutions to $x^2 = -c_f N$ in Λ, where $c_f \in R$ is a totally positive constant. Hence the representations are in one-to-one correspondence with the embeddings of $S = R[\sqrt{-c_f N}]$ in Λ. We will also find that the primitive solutions to $f(x_1, x_2, x_3) = N$ correspond to optimal embeddings of S in Λ. Furthermore, with this construction the classes of quadratic forms in the genus of f correspond to the classes of orders in the genus of Λ (see Section 4 for further details).

In [4], it was proved that

$$\sum_{i=1}^{t} H(\Lambda_i) e_{\Lambda^*}(S, \Lambda) = h(S) e_{U(\Lambda)}(S, \Lambda),$$

where t is the type number of Λ, S is a maximal commutative suborder of Λ, $e_{\Lambda^*}(S, \Lambda)$ denotes the number of Λ^* orbits on the set of embeddings of S in Λ, $H(\Lambda_i)$ is the number of Λ_i-isomorphism classes of two-sided locally free Λ_i-ideals modulo principal two-sided Λ_i-ideals. $h(S)$ denotes the class number of S and $e_{U(\Lambda)}(S, \Lambda) = \prod_{\mathfrak{p}} e(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}})$, where $\mathfrak{p} \neq 0$ are the prime ideals in R and $e(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}})$ denotes the number of optimal embeddings of $S_{\mathfrak{p}}$ in $\Lambda_{\mathfrak{p}}$. Using this and the relation between ternary quadratic forms and quaternion orders described above, we prove the equality

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|Aut^+(f_i)|} = \delta_\Lambda \sum_{S} \frac{1}{|S^*/R^*|} h(S) e_{U(\Lambda)}(S, \Lambda),$$

where $f_1 = f, \ldots, f_t$ represent the classes in the genus of f, $Aut^+(f_i)$ denotes the group of integral automorphisms of f_i with determinant 1 and $r_{f_i}(N)$ denotes the number of representations of N by f_i. Λ is the order corresponding to f according to the results described above, δ_Λ is a factor independent of N and the sum is taken over all R-orders S such that

$R[\sqrt{-c_f N}] \subseteq S \subset K(\sqrt{-c_f N})$ and S is a maximal commutative suborder of Λ (see Thm. 4.12).

Since the primitive solutions correspond to optimal embeddings of $S = R[\sqrt{-c_f N}]$ in Λ_i, we get the equality

$$\sum_{i=1}^{t} \frac{r_{f_i}^0(N)}{|Aut^+(f_i)|} = \delta_\Lambda \frac{1}{|S^*/R^*|} h(S) e_{U(\Lambda)}(S, \Lambda),$$

(see Section 4). This gives a generalization of the results for $K = \mathbb{Q}$ and $R = \mathbb{Z}$ in [4].

Let a ternary quadratic form f be such that the corresponding quaternion order Λ_f has a Gorenstein clousure $G(\Lambda_f)$, which is a Bass order. In Section 5, we will examine the stability of embedding numbers when $K = \mathbb{Q}(\sqrt{d})$, $d \not\equiv 1 \pmod 8$ and $d > 0$ is a square-free rational integer such that the ring of integers R in K is a principal ideal domain. We find that for $c_f N = N_1 N_0^2$, a totally positive number in R with N_1 square-free and $N_1, N_0 \in R$, there exist positive rational integers M_0 and M_1 such that the values of $e_{U(\Lambda_f)}(S, \Lambda_f)$, where $S = R[\sqrt{-c_f N}]$, are determined by N_0 modulo M_0 and N_1 modulo M_1. This was proved for $K = \mathbb{Q}$ in Sec. 3 in [6].

Section 1 contains a short introduction to the well-known theory of lattices and orders. In Section 2 we will use idèles to obtain some auxiliary results concerning class numbers and type numbers.

1 Lattices and orders

We shall start by describing some of the well-known theory of lattices and orders, which will be needed later on. Almost all propositions and theorems in this Section will be stated without proofs but we will often indicate where a proof can be found.

Let R be a Dedekind ring and denote by K its quotient field. Let V be a vector space over K of dimension n, $0 < n < \infty$. An R-lattice on V is a finitely generated R-module L such that $KL = V$. Since an R-lattice is torsion-free, it is R-projective (see [14], Thm. 1.13).

1.1. Definition. *Let L and L' be R-lattices on V. The index $[L' : L]$ is the fractional ideal of R generated by the determinants of all linear transformations $\varphi : V \to V$ such that $\varphi(L') \subseteq L$.*

In the following proposition, we state some of the properties of the index.

1.2. Proposition.
a) Let $L = Re_1 + \cdots + Re_n$ and $L' = Re'_1 + \cdots + Re'_n$. Then $[L' : L] = (det\varphi)$, where $\varphi(e'_i) = e_i$ for $i = 1, \ldots, n$.

b) $[L' : L]_{\mathfrak{p}} = [L'_{\mathfrak{p}} : L_{\mathfrak{p}}]$ for each prime ideal $\mathfrak{p}$ in R, where $R_{\mathfrak{p}}$ is the localization of R with respect to the prime ideal $\mathfrak{p}$ and $L_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R L$, $L'_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R L'$ are considered as $R_{\mathfrak{p}}$-lattices on V.

c) $[L'' : L'][L' : L] = [L'' : L]$ for any R-lattices L, L', L'' on V.

d) If $L \subseteq L'$, then $[L' : L] = R$ if and only if $L' = L$.

1.3. Definition. *Let $b : V \times V \to K$ be a non-degenerate symmetric bilinear form and let L be an R-lattice on V. We define $L^{\#} = \{x \in V : b(x, L) \subseteq R\}$.*

1.4. Proposition. *$L^{\#}$ is an R-lattice on V. If $L = Re_1 + \cdots + Re_n$, then $L^{\#} = Rf_1 + \cdots + Rf_n$, where $f_1, \ldots, f_n$ is the dual basis of $e_1, \ldots, e_n$ with respect to b, i.e. $b(e_i, f_i) = 1$ and $b(e_i, f_j) = 0$ for $i \neq j$.*

Proof. It is clear that $L^{\#}$ is an R-module. Assume that $L = Re_1 + \cdots + Re_n$, then $V = Ke_1 + \cdots + Ke_n$ We have an isomorphism $\varphi : V \to V^* =$

$Hom_K(V,K)$ given by $\varphi(x) = b(x,\cdot)$, since b is non-degenerate. Let g_i, $i = 1,\ldots,n$, be the basis of V^* such that $g_i(e_j) = \delta_{ij}$. Denote by $f_1,\ldots,f_n$ the elements of V such that $\varphi(f_i) = g_i$. Then $\varphi(f_i)(e_j) = \delta_{ij}$ that is, $b(f_i,e_j) = \delta_{ij}$. Let $x \in L^{\#}$. Then $x = \sum_{i=1}^n k_i f_i$ and $b(x,e_i) = k_i \in R$, so $L^{\#} \subseteq Rf_1 + \cdots + Rf_n$. But $b(f_i,e_j) = \delta_{ij}$, so $Rf_1 + \cdots + Rf_n \subseteq L^{\#}$. Thus $L^{\#} = Rf_1 + \cdots + Rf_n$. For an arbitrary R-lattice L, we may choose a basis for V which is contained in L (since $KL = V$). Denote this basis by $e_1,\ldots,e_n$. Using the above, we see that $L^{\#} \subseteq Rf_1 + \cdots + Rf_n = N$. Denote by $a_1,\ldots,a_m$ a set of generators of L. We have $b(e_i,a_j) = k_{ij} \in K$ and it is possible to choose $r \in R$ such that $r \neq 0$ and $rk_{ij} \in R$, $i = 1,\ldots,n$, $j = 1,\ldots,m$. Then $M = Rre_1 + \cdots + Rre_n$ is an R-lattice such that $M \subseteq L^{\#}$. We have $M \subseteq L^{\#} \subseteq N$ and $V = KM \subseteq KL^{\#} \subseteq KN = V$, thus $KL^{\#} = V$. Moreover $L^{\#}$ is finitely generated, since N is finitely generated and R is noetherian. □

1.5. Definition. *The index $[L^{\#} : L]$ is called the discriminant of L and will be denoted by $D(L)$.*

1.6. Proposition.
a) If $L = Re_1 + \cdots + Re_n$, then $D(L) = (det[b(e_i,e_j)])$.

b) $D(L) = [L' : L]^2 D(L')$ for any R-lattices L, L' on V.

c) If $L \subseteq L'$ and $D(L') = D(L)$, then $L' = L$.

The proposition follows easily from Prop. 1.2 and 1.4.

Let $V = Ke_1 + \cdots + Ke_n$ and let $\varphi : V \to V$ be a linear map such that $\varphi(e_i) = \sum_{j=1}^n a_{ij}e_j$. Then the characteristic polynomial of φ over K is defined to be $P_\varphi(x) = det(xI_n - [a_{ij}])$, where I_n is the identity matrix of rank n. Let $P_\varphi(x) = x^n - Tr(\varphi)x^{n-1} + \cdots + (-1)^n Nr(\varphi)$. The coefficients $Tr(\varphi)$ and $Nr(\varphi)$ are called the trace and the norm of φ. Notice that

$$Tr(\varphi + \psi) = Tr(\varphi) + Tr(\psi)$$

and

$$Nr(\varphi\psi) = Nr(\varphi)Nr(\psi).$$

The minimum polynomial of φ over K is the polynomial $m_\varphi(x) \in K[x]$ of the least possible degree such that $m_\varphi(\varphi) = 0$. By the Cayley-Hamilton theorem $P_\varphi(\varphi) = 0$, so $m_\varphi | P_\varphi$.

Let A be a finite dimensional algebra over K. Then we have a linear mapping $f_a : A \to A$ for every $a \in A$ defined by $f_a(x) = ax$.

1.7. Definition. *The characteristic polynomial and the minimum polynomial of f_a over K are called the characteristic polynomial and the minimum polynomial of a over K and will be denoted by P_a and m_a. The norm and the trace of f_a will be denoted by $Nr_{A/K}(a)$ and $Tr_{A/K}(a)$.*

For the remaining part of this Section, we assume that the finite dimensional K-algebra A is central and simple with $dim_K A = n^2$. By Wedderburn's theorem there exists a skew-field D such that $A \cong M_n(D)$. There exists a maximal subfield $E \subseteq D$, such that E is a finite separable extension field of K which splits A (see [17], §7b). This means that there is an isomorphism, which we denote by h, of E-algebras such that

$$E \otimes_K A \cong M_n(E).$$

1.8. Definition. *For $a \in A$ we define its reduced characteristic polynomial, denoted by $p_{a,A/K}$, as the characteristic polynomial of $h(1 \otimes a)$.*

The reduced characteristic polynomial is independent of the choice of the splitting field E and the E-isomorphism h, see [17], p. 113.

1.9. Definition. *If $p_{a,A/K}(x) = x^n - tr_{A/K}(a)x^{n-1} + \cdots + (-1)^n nr_{A/K}(a)$, then $tr_{A/K}$ is called the reduced trace and $nr_{A/K}$ is called the reduced norm.*

The following proposition will be useful later on (for a proof see [17], Thm. 9.9).

1.10. Proposition. *Let A be a central simple algebra and define $\psi : A \times A \to K$, by $\psi(a, b) = tr_{A/K}(ab)$. Then ψ is a non-degenerate symmetric bilinear form.*

1.11. Theorem (Skolem-Noether). *Let $K \subseteq B \subseteq A$, where B is a simple subring of the central simple K-algebra A. Then every K-isomorphism φ of B onto a sub-algebra $\tilde{B}$ of A extends to an inner automorphism of A, that is, there exists an invertible element $a \in A$ such that $\varphi(b) = aba^{-1}$, $b \in B$.*

For a proof see [17], Thm. 7.21.

1.12. Definition. *A subring Λ of A containing R, which is finitely generated and projective as an R-module and such that $K\Lambda = A$ is called an R-order.*

Let L be an arbitrary R-lattice on A and let

$$\mathcal{O}_l(L) = \{a \in A : aL \subseteq L\},$$
$$\mathcal{O}_r(L) = \{a \in A : La \subseteq L\}.$$

Then $\mathcal{O}_l(L)$ and $\mathcal{O}_r(L)$ are R-orders in R, see [17], p. 109.

1.13. Proposition. *Every element of an R-order Λ is integral over R. Furthermore, the minimum polynomial and the characteristic polynomial of any $a \in \Lambda$ belong to $R[x]$.*

For a proof see [17], Thm. 8.6.

1.14. Definition. *Let Λ be an R-order in A. The discriminant of Λ is $D(\Lambda) = [\Lambda^{\#} : \Lambda]$, where $\Lambda^{\#} = \{x \in A : tr_{A/K}(x\Lambda) \subseteq R\}$.*

Since $\Lambda \subseteq \Lambda^{\#}$, we have $D(\Lambda) \subseteq R$. An R-order Λ is called maximal if there are no other R-orders Λ' such that $\Lambda \subset \Lambda' \subset A$. Every R-order in the central simple K-algebra A is contained in a maximal one. If R is a discrete valuation ring, then all maximal R-orders Λ in A are isomorphic and furthermore, the left Λ-ideals I in A are principal, that is, $I = \Lambda\alpha$ where $\alpha \in A^*$. For proofs of these facts see [17], Chap. 10 and 18.

A proof of the following proposition can be found in [17], Cor. 11.2 and Cor. 11.6.

1.15. Proposition. *The following conditions are equivalent:*

a) An R-order Λ in A is maximal;

b) Every localization $\Lambda_{\mathfrak{p}}$ is maximal as an $R_{\mathfrak{p}}$-order in $A_{\mathfrak{p}}$;

c) Every completion $\hat{\Lambda}_{\mathfrak{p}} = \hat{R}_{\mathfrak{p}} \otimes_R \Lambda$ is maximal as an $\hat{R}_{\mathfrak{p}}$-order in $\hat{A}_{\mathfrak{p}} = \hat{K}_{\mathfrak{p}} \otimes_K A$.

2 Idèles, class numbers and type numbers

In this Section, we will use idèles to obtain some auxiliary results concerning class numbers and type numbers for orders in finite dimensional central simple algebras.

We assume, as before, that R is a Dedekind ring. Its quotient field is denoted by K and assumed to be an algebraic number field. We let A denote a finite dimensional central simple K-algebra. An infinite prime of K is an equivalence class of archimedian valuations on K. These primes arise from embeddings of K in $\mathbb{R}$ or in $\mathbb{C}$. The finite primes of K are the equivalence classes of non-archimedian valuations on K, we always exclude the trivial valuation. The finite primes originate from the prime ideals $\mathfrak{p}$ of R. They are also called the $\mathfrak{p}$-adic valuations.

2.1. Definition. *Let Λ be an R-order in A and I a left Λ-ideal. The ideal class $[I]$ consists of all left Λ-ideals that are isomorphic to I as Λ-modules. I is called locally free if for each prime ideal $\mathfrak{p}$ in R the completion $\hat{I}_{\mathfrak{p}}$ is a free $\hat{\Lambda}_{\mathfrak{p}}$-ideal, that is, $\hat{I}_{\mathfrak{p}} = \hat{\Lambda}_{\mathfrak{p}}\alpha_{\mathfrak{p}}$, where $\alpha_{\mathfrak{p}} \in \hat{A}^*_{\mathfrak{p}}$.*

We will only consider Λ-ideals I such that $KI = A$. A proof of the following Theorem can be found in [17], Thm. 26.4.

2.2. Theorem (Jordan-Zassenhaus). *Let R be a Dedekind ring such that its quotient field K is global. Then for each R-order Λ in a semi-simple K-algebra A, and for each positive integer t there are only finitely many isomorphism classes of left Λ-lattices of R-rank at most t.*

We observe that the number of classes of locally free left Λ-ideals for a central simple K-algebra A over a global field K is finite by Thm. 2.2. The set of isomorphism classes of locally free, (left), Λ-ideals is denoted by $Cl^f(\Lambda)$. Observe that $Cl^f(\Lambda)$ need not be a group. The cardinality of $Cl^f(\Lambda)$ will be denoted by h_Λ.

Remark. Let I and I' denote left Λ-ideals in the same ideal class. Then there is an isomorphism of Λ-modules, $\varphi : I' \to I$ where $\varphi(\lambda i') = \lambda\varphi(i')$ for $\lambda \in \Lambda$. We may extend φ to $A = KI' = KI$, $\varphi' : A \to A$, since for an element $x \in A$ we can choose $r \neq 0$, $r \in R$ such that $rx \in I'$ and define $\varphi'(x) = r^{-1}\varphi(rx)$. This definition is independent of our choice of r. We have

$\varphi'(\lambda) = \lambda\varphi'(1) = \lambda\alpha$ for some $\alpha \in A^*$. For $x \in A$ we now choose $r \neq 0$ such that $rx \in I \cap \Lambda$, this is possible since $K\Lambda = A$. We get $\varphi'(x) = x\alpha$. Hence I and I' are in the same ideal class if and only if there is an element $\alpha \in A^*$ such that $I'\alpha = I$.

2.3. Definition. *Two R-orders Λ and Λ' in a K-algebra A are of the same type if they are R-isomorphic. Λ and Λ' are in the same genus of R-orders if for each prime ideal $\mathfrak{p}$ in R the completions $\hat{\Lambda}_\mathfrak{p} = \hat{R}_\mathfrak{p} \otimes \Lambda$ and $\hat{\Lambda}'_\mathfrak{p} = \hat{R}_\mathfrak{p} \otimes \Lambda'$ are $\hat{R}_\mathfrak{p}$-isomorphic. We shall denote the number of types of orders in the genus of Λ by t_Λ.*

2.4. Definition. *For an R-order Λ in the K-algebra A, $\mathcal{H}(\Lambda)$ denotes the group of locally-free two-sided Λ-ideals modulo the principal two-sided ideals. The order of $\mathcal{H}(\Lambda)$ will be denoted by $H(\Lambda)$.*

We shall denote by $(\alpha_\mathfrak{p})_\mathfrak{p}$ or $(\alpha_\mathfrak{p})$ a vector such that $\alpha_\mathfrak{p} \in \hat{A}^*_\mathfrak{p}$ for each $\mathfrak{p} \in Spec(R)$, $\mathfrak{p} \neq 0$.

2.5. Definition. *Let Λ be an R-order in A. $\mathcal{J}(A) = \{(\alpha_\mathfrak{p}) : \alpha_\mathfrak{p} \in \hat{A}^*_\mathfrak{p}$ and $\alpha_\mathfrak{p} \in \hat{\Lambda}^*_\mathfrak{p}$ for almost all $\mathfrak{p} \in Spec(R)\}$ with the operation $(\alpha_\mathfrak{p})(\beta_\mathfrak{p}) = (\alpha_\mathfrak{p}\beta_\mathfrak{p})$ is called the idèle group of A.*

$\mathcal{J}(A)$ does not depend on the choice of Λ, since for another R-order Λ' in A we have $\hat{\Lambda}_\mathfrak{p} = \hat{\Lambda}'_\mathfrak{p}$ for almost all $\mathfrak{p}$.

There is a local-global correspondence according to the following proposition, (see [19], Chap. III, Prop. 5.1):

2.6. Proposition. *Let L be an R-lattice on A. For every $\mathfrak{p} \neq 0$, let $L_{(\mathfrak{p})}$ be a lattice on $\hat{A}_\mathfrak{p}$ such that $L_{(\mathfrak{p})} = \hat{L}_\mathfrak{p}$ for almost all $\mathfrak{p}$. Then there exists a unique lattice L' in A such that $\hat{L'}_\mathfrak{p} = L_{(\mathfrak{p})}$ for all $\mathfrak{p}$. In fact, this is a bijection between lattices on A and $\{(L_{(\mathfrak{p})})_\mathfrak{p} : L_{(\mathfrak{p})}$ a lattice on $\hat{A}_\mathfrak{p}$ and $L_{(\mathfrak{p})} = \hat{L}_\mathfrak{p}$ for almost all $\mathfrak{p}\}$.*

Let $\mathcal{N}(\Lambda) = \{\alpha \in \mathcal{J}(A) : \alpha\Lambda\alpha^{-1} = \Lambda\}$ and let $\mathcal{U}(\Lambda) = \{(\alpha_\mathfrak{p}) \in \mathcal{J}(A) : \alpha_\mathfrak{p} \in \hat{\Lambda}^*_\mathfrak{p}\}$.

2.7. Proposition. *Let Λ denote an R-order in A. Then there is a bijective correspondence between*

a) the locally free left Λ-ideals in A and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{J}(A)$.

b) the isomorphism classes of locally free left Λ-ideals in A and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{J}(A)/A^*$.

c) the locally free two-sided Λ-ideals in A and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{N}(\Lambda)$.

d) the isomorphism classes of locally free two-sided Λ-ideals in A and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{N}(\Lambda)/(A^*\cap\mathcal{N}(\Lambda))$.

e) the types of the orders in the genus of Λ and the elements of $\mathcal{N}(\Lambda)\backslash\mathcal{J}(A)/A^*$.

Proof. a) Using the local-global correspondence we have a bijection where a locally free left Λ-ideal I such that $\hat{I}_\mathfrak{p}=\hat{\Lambda}_\mathfrak{p}\alpha_\mathfrak{p}$ corresponds to $\alpha=(\alpha_\mathfrak{p})$. We also observe that $\alpha_\mathfrak{p}\in\hat{A}^*_\mathfrak{p}$ and $\alpha_\mathfrak{p}\in\hat{\Lambda}^*_\mathfrak{p}$ for almost all $\mathfrak{p}$, so $\alpha\in\mathcal{J}(A)$. For $\beta=(\beta_\mathfrak{p})\in\mathcal{J}(A)$, we define $\Lambda\beta=A\cap(\bigcap\hat{\Lambda}_\mathfrak{p}\beta_\mathfrak{p})=\bigcap(A\cap\hat{\Lambda}_\mathfrak{p}\beta_\mathfrak{p})$. $\Lambda\beta$ will then denote the uniqely determined locally free left Λ-ideal that corresponds to $\hat{\Lambda}_\mathfrak{p}\beta_\mathfrak{p}$. Since $\hat{\Lambda}_\mathfrak{p}\varepsilon_\mathfrak{p}\beta_\mathfrak{p}=\hat{\Lambda}_\mathfrak{p}\beta_\mathfrak{p}$, for all $\varepsilon_\mathfrak{p}\in\hat{\Lambda}^*_\mathfrak{p}$, we have a bijection between the ideals and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{J}(A)$.

b) Let I and I' belong to the same ideal class. Then there is an $\alpha\in A^*$ such that $\hat{\Lambda}_\mathfrak{p}\alpha'_\mathfrak{p}\alpha=\hat{\Lambda}_\mathfrak{p}\alpha_\mathfrak{p}$ and we find that $\epsilon_\mathfrak{p}\alpha'_\mathfrak{p}\alpha=\alpha_\mathfrak{p}$ for some $\epsilon_\mathfrak{p}\in\hat{\Lambda}^*_\mathfrak{p}$. Hence, we have a bijection between the ideal classes and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{J}(A)/A^*$.

c) Let I denote a locally free two-sided Λ-ideal. Then $\hat{I}_\mathfrak{p}=\hat{\Lambda}_\mathfrak{p}\alpha_\mathfrak{p}=\alpha_\mathfrak{p}\hat{\Lambda}_\mathfrak{p}$ for all $\mathfrak{p}$ so $\alpha=(\alpha_\mathfrak{p})\in\mathcal{N}(\Lambda)$ and the two-sided locally free Λ-ideals correspond bijectively to the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{N}(\Lambda)$.

d) Now we let I and I' denote two locally free two-sided Λ-ideals in the same ideal class. We have $I'=I\alpha$, where $\alpha\in A^*$, and $\hat{\Lambda}_\mathfrak{p}\alpha'_\mathfrak{p}=\hat{\Lambda}_\mathfrak{p}\alpha_\mathfrak{p}\alpha$ for all $\mathfrak{p}$. Then $\alpha'_\mathfrak{p}=\epsilon_\mathfrak{p}\alpha_\mathfrak{p}\alpha$ and we know that $\alpha'_\mathfrak{p},\epsilon_\mathfrak{p},\alpha_\mathfrak{p}\in\mathcal{N}(\hat{\Lambda}_\mathfrak{p})$ so $\alpha\in\mathcal{N}(\hat{\Lambda}_\mathfrak{p})$ for all $\mathfrak{p}$. But then $\alpha\in\mathcal{N}(\Lambda)\cap A^*$ and we have a bijection between the elements of $\mathcal{H}(\Lambda)$ and the elements of $\mathcal{U}(\Lambda)\backslash\mathcal{N}(\Lambda)/(\mathcal{N}(\Lambda)\cap A^*)$.

e) Let I_i and I_j represent two different ideal classes such that $O_r(I_i)=\Lambda_i\cong\Lambda_j=O_r(I_j)$. Then there is an element $\alpha\in A^*$ such that $\Lambda_i=\alpha\Lambda_j\alpha^{-1}$. We have $1\in\hat{\Lambda}_{i\mathfrak{p}}=\mathcal{O}_r(\hat{I}_{i\mathfrak{p}})$ so

$$(*)\qquad \hat{I}_{i\mathfrak{p}}=\hat{I}_{i\mathfrak{p}}\hat{\Lambda}_{i\mathfrak{p}}=\hat{I}_{i\mathfrak{p}}\alpha\hat{\Lambda}_{j\mathfrak{p}}\alpha^{-1}$$

Since $\hat{I}_{j\mathfrak{p}} = \hat{\Lambda}_{\mathfrak{p}}\alpha_{j\mathfrak{p}}$, we have $\mathcal{O}_r(\hat{I}_{j\mathfrak{p}}) = \alpha_{j\mathfrak{p}}^{-1}\hat{\Lambda}_{\mathfrak{p}}\alpha_{j\mathfrak{p}} = \hat{\Lambda}_{j\mathfrak{p}}$. Substituting this into $(*)$, we get

$$\hat{I}_{i\mathfrak{p}} = \hat{I}_{i\mathfrak{p}}\alpha\alpha_{j\mathfrak{p}}^{-1}\hat{I}_{j\mathfrak{p}}\alpha^{-1} = \hat{\Lambda}_{\mathfrak{p}}\alpha_{i\mathfrak{p}}\alpha\alpha_{j\mathfrak{p}}^{-1}\hat{\Lambda}_{\mathfrak{p}}\alpha_{j\mathfrak{p}}\alpha^{-1}.$$

We also have

$$\alpha_{i\mathfrak{p}}\alpha\alpha_{j\mathfrak{p}}^{-1}\hat{\Lambda}_{\mathfrak{p}}\alpha_{j\mathfrak{p}}\alpha^{-1}\alpha_{i\mathfrak{p}}^{-1} = \alpha_{i\mathfrak{p}}\alpha\hat{\Lambda}_{j\mathfrak{p}}\alpha^{-1}\alpha_{i\mathfrak{p}}^{-1} = \alpha_{j\mathfrak{p}}\hat{\Lambda}_{i\mathfrak{p}}\alpha_{i\mathfrak{p}}^{-1} = \hat{\Lambda}_{\mathfrak{p}},$$

so

$$\hat{I}_{i\mathfrak{p}} = \hat{\Lambda}_{\mathfrak{p}}\beta_{\mathfrak{p}}\alpha_{j\mathfrak{p}}\alpha^{-1},$$

where $\beta_{\mathfrak{p}} = \alpha_{i\mathfrak{p}}\alpha\alpha_{j\mathfrak{p}}^{-1} \in \mathcal{N}(\Lambda_{\mathfrak{p}})$ for all $\mathfrak{p}$.

Hence $(\beta_{\mathfrak{p}}) \in \mathcal{N}(\Lambda)$ and both I_i and I_j can be represented by elements in $\mathcal{N}(\Lambda)\alpha_j A^*$. Using the following lemma, we are done.

□

2.8. Lemma. *The type number t_Λ for an R-order Λ in A is given by the number of non-isomorphic orders among $\mathcal{O}_r(I_1), \ldots, \mathcal{O}_r(I_h)$, where $I_1, \ldots, I_h$ represent the classes of locally free left Λ-ideals.*

Proof. Let $I \cong I_k$, for some k. Then there exists an element $\alpha \in A^*$ such that $I = I_k\alpha$. Hence $O_r(I) = \alpha^{-1}O_r(I_k)\alpha$ and $O_r(I) \cong O_r(I_k)$.

Let Λ' be an R-order in the genus of Λ. Then, for every $\mathfrak{p} \in SpecR$, $\mathfrak{p} \neq 0$, there exists $\alpha_{\mathfrak{p}} \in \hat{A}_{\mathfrak{p}}^*$ such that $\hat{\Lambda}_{\mathfrak{p}}' = \alpha_{\mathfrak{p}}^{-1}\hat{\Lambda}_{\mathfrak{p}}\alpha_{\mathfrak{p}}$. Since $\hat{\Lambda}_{\mathfrak{p}}' = \hat{\Lambda}_{\mathfrak{p}}$ for almost all $\mathfrak{p}$, we can choose $(\alpha_{\mathfrak{p}}) \in \mathcal{J}(A)$. Then $I' = \bigcap(A \cap \hat{\Lambda}_{\mathfrak{p}}\alpha_{\mathfrak{p}})$ will be a locally free left Λ-ideal with $\mathcal{O}_r(I') = \Lambda'$.

We also need to know that all $O_r(I_i)$, $i = 1, \ldots, h$, belong to the same genus. Let $\Lambda_i = \mathcal{O}_r(I_i)$ and $\Lambda_j = \mathcal{O}_r(I_j)$. Then $\hat{I}_{i\mathfrak{p}} = \hat{\Lambda}_{\mathfrak{p}}\alpha_{i\mathfrak{p}}$ and $\hat{I}_{j_{\mathfrak{p}}} = \hat{\Lambda}_{\mathfrak{p}}\alpha_{j\mathfrak{p}}$ so

$$\mathcal{O}_r(\hat{I}_{i\mathfrak{p}}) = \alpha_{i\mathfrak{p}}^{-1}\hat{\Lambda}_{\mathfrak{p}}\alpha_{i\mathfrak{p}} = \alpha_{i\mathfrak{p}}^{-1}\alpha_{j\mathfrak{p}}\mathcal{O}_r(\hat{I}_{j_{\mathfrak{p}}})(\alpha_{i\mathfrak{p}}^{-1}\alpha_{j\mathfrak{p}})^{-1}$$

and $\alpha_{i\mathfrak{p}}^{-1}\alpha_{j\mathfrak{p}} \in \hat{A}_{\mathfrak{p}}^*$. Hence $\Lambda_{i\mathfrak{p}}$ and $\Lambda_{j\mathfrak{p}}$ are isomorphic for all $\mathfrak{p} \in SpecR$, $\mathfrak{p} \neq 0$, that is, Λ_i and Λ_j belong to the same genus. □

2.9. Proposition. *Let $\Lambda_1, \ldots, \Lambda_t$, where $t = t_\Lambda$, denote the non-isomorphic orders among $\mathcal{O}_r(I_i)$, $i = 1, \ldots, h$, where $I_1, \ldots, I_h$ represent the locally free left Λ-ideal classes and $h = h_\Lambda$. Then*

$$h = \sum_{j=1}^{t} H(\Lambda_k).$$

Proof. We know that $\mathcal{J}(A) = \cup_{j=1}^{t} \mathcal{N}(\Lambda)\alpha_j A^*$, so

$$\mathcal{N}(\Lambda)\backslash\mathcal{J}(A)/A^* = \cup_{j=1}^{t} \mathcal{N}(\Lambda)\backslash\mathcal{N}(\Lambda)\alpha_j A^*/A^*.$$

We also observe that $\mathcal{N}(\Lambda_j) = \alpha_j^{-1}\mathcal{N}(\Lambda)\alpha_j$ and $\mathcal{U}(\Lambda_j) = \alpha_j^{-1}\mathcal{U}(\Lambda)\alpha_j$. Then $\mathcal{N}(\Lambda)\alpha_j A^* = \alpha_j \mathcal{N}(\Lambda_j)A^*$ and

$$|\mathcal{U}(\Lambda)\backslash\mathcal{N}(\Lambda)\alpha_j A^*/A^*| = |\mathcal{U}(\Lambda_j)\backslash\mathcal{N}(\Lambda_j)/(A^* \cap \mathcal{N}(\Lambda_j))| = H(\Lambda_j).$$

□

3 Even Clifford algebras and quaternion orders

In this Section, we shall see that for an R-order Λ in a quaternion K-algebra, one can always find an R-lattice L and a ternary quadratic form q such that the even Clifford algebra $C_0(L,q)$ is isomorphic to Λ.

Let R be a principal ideal domain with quotient field K. If L is a free R-lattice with basis $e_1,\ldots,e_n$ and q is a quadratic form,

$$q : L \to R, \quad q(x_1e_1 + \cdots + x_ne_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j,$$

then the Clifford algebra, which we denote by $C(L,q)$ or $C(q)$, is $\mathcal{T}(L)/\mathcal{I}$ where $\mathcal{T}(L)$ is the tensor algebra of L and $\mathcal{I}$ is the ideal in $\mathcal{T}(L)$ generated by $x \otimes x - q(x)$ for $x \in L$. The even Clifford algebra is defined to be

$$C_0(L,q) = \mathcal{T}_0(L)/\mathcal{I}$$

where $\mathcal{T}_0(L) = \bigoplus \mathcal{T}^{\otimes 2r}(L)$ is the even part of the tensor algebra of L. We will denote the images of x and $x \otimes y$ in $C(L,q)$ by x and xy. We then have

$$x^2 = q(x), \ x \in L$$

and

$$xy + yx = (x+y)^2 - x^2 - y^2 = q(x+y) - q(x) - q(y).$$

We find that

$$e_i^2 = a_{ii} \text{ and } e_ie_j + e_je_i = a_{ij} \text{ when } i \neq j. \tag{3.1}$$

It is clear that the elements $1, e_{i_1} \ldots e_{i_k}$, where $k \leq n$ and $i_j < i_m$ for $j < m$, generate $C(L,q)$ as an R-module and it is not difficult to show that these elements are linearly independent over R. The R-algebra $C_0(L,q)$ is generated by 1 and the images of $e_{i_1} \otimes \cdots \otimes e_{i_{2r}} \in \mathcal{T}^{\otimes 2r}(L)$, $r > 0$.

Let q be a ternary quadratic form and e_1, e_2, e_3 an R-basis for L. Then we know that $C_0(L,q)$ is generated by 1, $E_1 = e_2e_3$, $E_2 = e_3e_1$ and $E_3 = e_1e_2$. Using 3.1, we get

$$E_i^2 = a_{jk}E_i - a_{jj}a_{kk} \tag{3.2}$$

$$E_jE_i = a_{1k}E_1 + a_{2k}E_2 + a_{3k}E_3 - a_{ik}a_{jk} \tag{3.3}$$

$$E_iE_j = a_{kk}(a_{ij} - E_k) \tag{3.4}$$

where i, j, k is an even permutation of $1, 2, 3$.

3.5. Definition. *Let* $f(x_1, x_2, x_3) = \sum_{1\leq i\leq j\leq 3} a_{ij}x_ix_j = q(x_1e_1 + x_2e_2 + x_3e_3)$. *The matrix*

$$M_f = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{pmatrix}$$

is called the matrix of f *and* $d(f) = \frac{1}{2}detM_f$ *is called the discriminant of* f. *Notice that*

$$d(f) = 4a_{11}a_{22}a_{33} + a_{12}a_{13}a_{23} - a_{11}a_{23}^2 - a_{22}a_{13}^2 - a_{33}a_{12}^2$$

so $d(f) \in R$ *when* $a_{ij} \in R$.

3.6. Definition. *A quaternion* K*-algebra* A *is a central simple algebra of dimension four over the field* K.

If $char(K) \neq 2$ one can show that A has a K-basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$, where $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ and $a, b \in K^*$. For a proof see [16], p. 236.

3.7. Definition. *Let* K *be an algebraic number field. A quaternion* K*-algebra* A *is called totally definite if every infinite prime* $\mathfrak{P}$ *of* K *is ramified in* A, *that is,* $\hat{A}_{\mathfrak{P}} \cong \mathbb{H}$ *for each such* $\mathfrak{P}$, *where* $\mathbb{H}$ *denotes the Hamiltonian quaternions over the real field* $\hat{K}_{\mathfrak{P}}$.

For an R-order Λ in a quaternion algebra it can be checked that $D(\Lambda) = \mathfrak{a}^2$ for some ideal $\mathfrak{a}$ in R (see [1], p. 21).

3.8. Definition. *For an R-order Λ the reduced discriminant $d(\Lambda)$ is defined as the square-root of $D(\Lambda)$, where $D(\Lambda)$ is defined according to Def.* 1.14.

In the following propositions, we gather some information which we will need later on.

3.9. Proposition. *Let $q(x_1e_1 + x_2e_2 + x_3e_3) = \sum_{1\leq i\leq j\leq 3} a_{ij}x_ix_j$, $a_{ij} \in R$. Then*

a) $C_0(L,q) = R + RE_1 + RE_2 + RE_3$, where E_1,E_2,E_3 satisfy the equalities 3.2, 3.3 *and* 3.4, *is an R-order.*

b) If q is non-degenerate, then $C_0(L,q) \otimes_R K$ is a quaternion K-algebra.

c) The function $x \mapsto \bar{x}$, where $x = x_0+x_1E_1+x_2E_2+x_3E_3$, $x_0, x_1, x_2, x_3 \in K$ and $\bar{x} = x_0 + x_1(a_{23} - E_1) + x_2(a_{13} - E_2) + x_3(a_{12} - E_3)$ is an antiinvolution on $C_0(L,q)\otimes_R K$ such that $tr(x) = x+\bar{x}$ is the reduced trace and $nr(x) = x\bar{x}$ is the reduced norm of x.

Proof. *a)* Obviously $C_0(L,q)$ is a finitely generated ring containing R. It is not difficult to check that $1, E_1, E_2, E_3$ is an R-basis for $C_0(L,q)$ and that $K \otimes C_0(L,q)$ is an K-algebra. For a proof of *b)* see [12], Chap. IV, Prop. 3.2.4, Chap. III Thm. 5.1.1 and Lemma 5.1.3. *c)* Let $A = C_0(L,q) \otimes_R K$ and $x = x_0 + x_1E_1 + x_2E_2 + x_3E_3$. Then $\bar{x} = x_0 + x_1a_{23} + x_2a_{13} + x_3a_{12} - x_1E_1 - x_2E_2 - x_3E_3$, $x + \bar{x} \in K$ and $x\bar{x} \in K$. □

3.10. Proposition. *Let*

$$f(x_1,x_2,x_3) = \sum_{1\leq i\leq j\leq 3} a_{ij}x_ix_j = q(x_1e_1 + x_2e_2 + x_3e_3).$$

Then the discriminant of $C_0(L,q) = C_0(f)$ is $D(C_0(f)) = (d(f))^2$.

Proof. Let $\Lambda = C_0(L,q) = R + RE_1 + RE_2 + RE_3$, with multiplication as in 3.2, 3.3 and 3.4. Using Prop. 3.9 c), we have

$$tr(E_i) = a_{jk},$$
$$tr(E_i^2) = a_{jk}^2 - 2a_{jj}a_{kk},$$
$$tr(E_iE_j) = tr(E_jE_i) = a_{ij}a_{kk},$$

and a straightforward calculation will give the result.

□

Hence $(d(f))$ is the reduced discriminant of $\Lambda = C_0(f)$.

3.11. Proposition. *Let A be a quaternion K-algebra and Λ an R-order in A with reduced discriminant $d(\Lambda) = (d_\Lambda)$, $d_\Lambda \in R$. Let*

$$A_0 = \{x \in A : tr(x) = 0\}$$

and

$$\Lambda^\# = \{x \in A : tr(x\Lambda) \subseteq R\}.$$

Then $L = \Lambda^\# \cap A_0$ is an R-lattice on A_0 and

$$q(x_1f_1 + x_2f_2 + x_3f_3) = d_\Lambda nr(x_1f_1 + x_2f_2 + x_3f_3),$$

where f_1, f_2, f_3 is an R-basis for L and $nr = nr_{A/K}$ denotes the reduced norm, is a ternary quadratic form such that $\Lambda \cong C_0(L,q)$.

Proof. We follow the proof of Prop. 3.2 in [1]. Every R-lattice in A is free since R is a principal ideal domain. Let $\Lambda = R + Re_1 + Re_2 + Re_3$. Then $\Lambda^\# = Rf_0 + Rf_1 + Rf_2 + Rf_3$, where f_0, f_1, f_2, f_3 is the basis for A over K dual to $1, e_1, e_2, e_3$ with respect to the reduced trace form. Since $tr(f_i) = 0$, for $i = 1, 2, 3$, we get $A_0 = Kf_1 + Kf_2 + Kf_3$. Hence

$$L = A_0 \cap \Lambda^\# = Rf_1 + Rf_2 + Rf_3$$

and

$$nr(r_1f_1 + r_2f_2 + r_3f_3) = nr(f_1)r_1^2 + nr(f_2)r_2^2 + nr(f_3)r_3^2 - tr(f_1f_2)r_1r_2 - tr(f_3f_1)r_3r_1 - tr(f_2f_3)r_2r_3.$$

One can easily check that

$$(a) \qquad f_i f_j = tr(f_i f_j f_0) + tr(f_1 f_2 f_3) e_k,$$

$$(b) \qquad e_k = tr(f_1 f_2 f_3)^{-1}(f_i f_j - tr(f_i f_j f_0)),$$

where (i, j, k) is an even permutation of $(1, 2, 3)$.

We know that the element $d = tr((e_1 e_2 - e_2 e_1)\bar{e_3})$ generates the ideal $d(\Lambda)$, where $x \mapsto \bar{x}$ is as in Prop. 3.9.c) (see [1] Lemma(1.1)). Using (b), we get $d = -tr(f_1 f_2 f_3)^{-1}$. Let $d_\Lambda = tr(f_1 f_2 f_3)^{-1}$ and denote by $N(\Lambda^\#)$ the ideal generated by all norms $nr(\lambda)$, where $\lambda \in \Lambda^\#$. Then $N(\Lambda^\#)d(\Lambda) \subseteq R$ (see [1], p. 21) , and $N(\Lambda^\#)^{-1}\Lambda^\#\Lambda^\#$ is an R-order (see [11] Thm. 6). Since $d(\Lambda)\Lambda^\#\Lambda^\# \subseteq N(\Lambda^\#)^{-1}\Lambda^\#\Lambda^\#$, the products $d_\Lambda f_i f_j$ are integral over R. Using this fact and (a), we get, $d_\Lambda tr(f_i f_j f_0) \in R$. Hence

$$\Lambda = R + R d_\Lambda f_1 f_2 + R d_\Lambda f_3 f_1 + R d_\Lambda f_2 f_3.$$

Observe that all products $d_\Lambda f_i f_j$, where $i, j \in \{0, 1, 2, 3\}$, are in Λ. This follows from the equalities

$$f_0^2 = f_0 - nr(f_0), \ f_i^2 = -nr(f_i) \ \text{ for } \ i = 1, 2, 3$$

and

$$f_i f_j = \sum_{n=0}^{3} tr(f_i f_j f_n) e_n \ \text{ with } \ e_0 = 1.$$

Let $\tilde{E}_i = d_\Lambda f_j f_k$, where (i, j, k) is an even permutation of $(1, 2, 3)$. Choose a basis of $C_0(L, d_\Lambda nr)$ according to Prop. 3.9.a). Denote this basis by $1, E_1, E_2, E_3$. It is now easy to check that $E_i \mapsto -\tilde{E}_i$ defines an isomorphism. $\square$

4 Representations by ternary quadratic forms

If f is a positive definite ternary quadratic form over $\mathbb{Z}$, $Aut^+(f)$ the group of integral automorphisms of f with determinant 1, $r_f(N)$ the number of integral representations of a positive integer N by f and $f_1 = f, \ldots, f_t$ represent all classes in the genus of f, then

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|Aut^+(f_i)|}$$

can be expressed as a product of $h(\mathbb{Z}[\sqrt{-c_f N}])$ for an integer $c_f > 0$, depending only on the genus of f, and some locally computable factors. This result was obtained in [4] applying a combinatorial class number formula to quaternion orders. Using the same approach and some results from [4], we will now give a generalization.

Let R be a principal ideal domain such that K, its quotient field, is a totally real algebraic number field. A number $a \in K$ is called totally positive if for all embeddings $i : K \to \mathbb{R}$ we have $i(a) > 0$. We will denote this by $a \gg 0$. Let $f : R^3 \to R$ be a totally positive definite quadratic form. We let $Aut^+(f)$ denote the group of integral automorphisms of f with determinant 1 and $r_f(N)$ the number of integral representations of N by f, where $N \in R$ is a totally positive integer. It can be checked, without difficulty, that $|Aut^+(f)|$ is finite for a totally positive definite quadratic form f.

4.1. Definition. *Two quadratic forms f and g in $R[x_1, \ldots, x_n]$ are equivalent over R if there is a linear mapping $\varphi(x_i) = \sum a_{ij}x_j$, where $a_{ij} \in R$, such that $det[a_{ij}] \in R^*$ and $f(\varphi(x_1), \ldots, \varphi(x_n)) = g(x_1, \ldots, x_n)$. The quadratic forms f and g are in the same genus if they are equivalent over $\hat{R}_\mathfrak{p}$ for each prime ideal $\mathfrak{p} \neq 0$ in R.*

The following proposition is a generalization of Prop. 3.2 in [4]. It describes a relation between representations of integers by ternary quadratic forms and solutions to quadratic equations in quaternion orders.

4.2. Proposition. *Let f be a totally positive definite ternary quadratic form. There is an R-order Λ in a quaternion algebra A over K and a totally positive*

constant $c_f \in R$, such that the integral representations of $N \in R$, $N \gg 0$, by f are in one-to-one correspondence with the solutions $\lambda \in \Lambda$ to $x^2 = -c_f N$.

Proof. Let

$$f(x_1, x_2, x_3) = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3$$

where $a_{ij} \in R$. Let $V = Ke_1 + Ke_2 + Ke_3$, $q(\sum_{i=1}^3 x_i e_i) = f(x_1, x_2, x_3)$ and $T(x, y) = q(x + y) - q(x) - q(y)$. Let $L = Re_1 + Re_2 + Re_3$ and $T_L = T|_L$. Recall that

$$M_f = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{pmatrix}.$$

Since q is non-degenerate over K, we have $det(M_f) \neq 0$. Let

$$M_f^{-1} = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \gamma_{12} & \gamma_{22} & \gamma_{23} \\ \gamma_{13} & \gamma_{23} & \gamma_{33} \end{pmatrix}$$

and $L^\# = \{v \in V : T(v, L) \subseteq R\}$. We then have the dual basis $f_j = \gamma_{1j}e_1 + \gamma_{2j}e_2 + \gamma_{3j}e_3$ such that $T(e_i, f_i) = 1$ and $T(e_i, f_j) = 0$ for $i \neq j$ and $L^\# = Rf_1 + Rf_2 + Rf_3$ by Prop. 1.4. We observe that

$$T(f_i, f_i) = \gamma_{ii},\ T(f_i, f_j) = \gamma_{ij}$$

and

$$q(x_1f_1 + x_2f_2 + x_3f_3) =$$

$$\frac{1}{2}(\gamma_{11}x_1^2 + \gamma_{22}x_2^2 + \gamma_{33}x_3^2) + \gamma_{12}x_1x_2 + \gamma_{13}x_1x_3 + \gamma_{23}x_2x_3.$$

Let I be the R-ideal such that $I = \{c \in R : cT(L^\#, L^\#) \subseteq 2R\}$. Let c_0 be a generator of this ideal. We may choose $c_0 = \frac{2det(M_f)}{\Omega_f}$, where Ω_f is the greatest common divisor of the elements in the adjoint matrix of M_f. Let

$c_f = \frac{c_0^2}{2det(M_f)}$ and $\Lambda = C_0(L^{\#}, c_0 q)$. We find that $c_f \in R$. Since $c_0 q$ is non-degenerate $K \otimes \Lambda = A$ is a quaternion algebra, by Prop. 3.9 b), so Λ is a quaternion order. We have $\Lambda = R + RE_1 + RE_2 + RE_3$ with $E_i = f_j f_k$ and

$$(a) \qquad E_i^2 = c_0(\gamma_{jk} E_i - \frac{1}{4} c_0 \gamma_{jj} \gamma_{kk}),$$

$$(b) \qquad E_i E_j = \frac{1}{2} c_0 \gamma_{kk} (c_0 \gamma_{ij} - E_k),$$

$$(c) \qquad E_j E_i = c_0(\gamma_{ik} E_i + \gamma_{jk} E_j + \frac{1}{2} \gamma_{kk} E_k - c_0 \gamma_{ik} \gamma_{jk}),$$

where i, j, k is an even permutation of $1, 2, 3$. Let $\lambda \in \Lambda$, $\lambda = r_0 + r_1 E_1 + r_2 E_2 + r_3 E_3$. Then

$$(*) \qquad \lambda^2 = r_0^2 - \frac{c_0^2}{4}(r_1^2 \gamma_{22}\gamma_{33} + r_2^2 \gamma_{11}\gamma_{33} + r_3^2 \gamma_{11}\gamma_{22}) +$$

$$c_0^2(r_1 r_2(\frac{1}{2}\gamma_{12}\gamma_{33} - \gamma_{13}\gamma_{23}) + r_1 r_3(\frac{1}{2}\gamma_{22}\gamma_{13} - \gamma_{12}\gamma_{23}) + r_2 r_3(\frac{1}{2}\gamma_{11}\gamma_{23} - \gamma_{12}\gamma_{13})) +$$

$$(2r_0 + c_0(r_1\gamma_{23} + r_2\gamma_{13} + r_3\gamma_{12}))(r_1 E_1 + r_2 E_2 + r_3 E_3).$$

If $N = f(r_1, r_2, r_3)$, we let $r_0 = -\frac{c_0}{2}(r_1\gamma_{23} + r_2\gamma_{13} + r_3\gamma_{12})$. This is an element in R, since $c_0\gamma_{ij} \in 2R$ for all i, j. With this choice of r_0, we have $\lambda^2 = -c_f f(r_1, r_2, r_3)$ and we can choose $r_1 = x_1$, $r_2 = x_2$ and $r_3 = x_3$. Then the element $\lambda \in \Lambda$ is such that $\lambda^2 = -c_f N$.

Assume now that we have $\lambda \in \Lambda$ such that $\lambda^2 = -c_f N$, $N \gg 0$. We observe, using $(*)$, that $0 = 2r_0 + c_0(r_1\gamma_{23} + r_2\gamma_{13} + r_3\gamma_{12})$. Substituting r_0 in $(*)$ we get $\lambda^2 = -c_f f(r_1, r_2, r_3)$ i.e. $f(r_1, r_2, r_3) = N$.

□

4.3. Definition. *Two quadratic R-lattices (L, q) and (L', q') are similar, $(L, q) \sim (L', q')$, if and only if there is an R-linear mapping $\varphi : L \to L'$, $\varphi(L) = L'$ and an element $c \in R^*$ such that $q'(\varphi(x)) = cq(x)$ for all $x \in L$.*

We need the following fact about a correspondence between similarity classes of quadratic lattices and isomorphism classes of quaternion orders.

4.4. Proposition. *There is a one-to-one correspondence between similarity classes of quadratic R-lattices (L, q), where q is a ternary non-degenerate form, and isomorphism classes of quaternion orders over R.*

Proof. Let τ be a mapping from similarity classes of lattices to isomorphism classes of quaternion orders such that the similarity class of (L, q) is mapped to the isomorphism class of $\Lambda = C_0(L, q)$. This mapping is well-defined since $(L_1, q_1) \sim (L_2, q_2)$ means that there is an element $\varepsilon \in R^*$ such that $(L_1, \varepsilon q_1) \cong (L_2, q_2)$ and it is easily seen from the definition of $C_0(L, q)$ that $C_0(L, q) \cong C_0(L, \varepsilon q)$ for any $\varepsilon \in R^*$.

Let ψ be the mapping from isomorphism classes of quaternion orders to similarity classes of lattices such that ψ maps the isomorphism class of Λ to the similarity class of (L, q), where L and q are found using Prop. 3.11. If $\Lambda \cong \Lambda'$, let $\varphi : \Lambda \to \Lambda'$ be an isomorphism. We can extend this isomorphism to an automorphism of the quaternion algebra A, also denoted by φ. This automorphism is an inner automorphism by the Skolem-Noether theorem so $\varphi(x) = \alpha^{-1} x \alpha$ for some $\alpha \in A^*$. Using this we see that $nr(x) = nr(\varphi(x))$, $tr(xy) = tr(\varphi(xy))$ and also that φ restricted to L is an isomorphism of L and L'. We also know that $d(\Lambda) = d(\Lambda')$, since $\Lambda \cong \Lambda'$, so $d_\Lambda = \varepsilon d_{\Lambda'}$ for some $\varepsilon \in R^*$. Hence $(L, q) \sim (L', q')$ and ψ is well-defined.

We know that $C_0(\psi(\Lambda)) \cong \Lambda$ (by Prop. 3.11), so all we have to check is that $\psi(C_0(L, q)) \sim (L, q)$.

Let $L = Re_1 + Re_2 + Re_3$ and $q(r_1e_1 + r_2e_2 + r_3e_3) = \sum_{i,j} a_{ij} r_i r_j$. We then have $C_0(L, q) = \Lambda = R + RE_1 + RE_2 + RE_3$, with the usual multiplication rules. An easy calculation will show that F_1, F_2, F_3 in the dual basis are given by

$$F_i = \frac{2}{detM_f}(a_{ii}a_{jk} + a_{ij}a_{ik} - 2a_{ii}E_i - a_{ij}E_j - a_{ik}E_k).$$

We know that $nr(r_1F_1 + r_2F_2 + r_3F_3) = \sum_{i=1}^{3} nr(F_i) r_i^2 - tr(F_1F_2) r_1 r_2 - tr(F_3F_1) r_1 r_3 - tr(F_2F_3) r_2 r_3$, see the proof of Prop. 3.11. Calculating these norms and traces, we get

$$nr(r_1F_1 + r_2F_2 + r_3F_3) = \frac{2}{detM_f} q(r_1e_1 + r_2e_2 + r_3e_3)$$

and since $\frac{1}{2}detM_f$ generates $d(\Lambda)$, we have $d_\Lambda = \frac{1}{2}\varepsilon detM_f$ for some $\varepsilon \in R^*$. Thus, $\psi(C_0(L,q)) = (L^{'}, q^{'})$, where $L^{'} = RF_1 + RF_2 + RF_3$ and $q^{'}(r_1F_1 + r_2F_2 + r_3F_3) = \varepsilon q(r_1e_1 + r_2e_2 + r_3e_3)$. Hence $\psi(C_0(L,q)) \sim (L,q)$.

□

Let $L = Re_1 + Re_2 + Re_3$ and let q be a quadratic form defined on L. Define f by $f(r_1,r_2,r_3) = \sum a_{ij}r_ir_j = q(r_1e_1 + r_2e_2 + r_3e_3)$ and let $\Lambda = C_0(L^{\#}, c_0q)$, with notations as in Prop. 4.2. Let $\sigma : L \to L$ be R-linear, $\sigma(L) = L$ and σ such that $q(\sigma(l)) = cq(l)$ for some $c \in R^*$ and for all $l \in L$. Denote by A the matrix representing σ in the basis e_1, e_2, e_3. We have $A^tM_qA = cM_q$, so $(det(A))^2 = c^3$, which implies that $c = \tilde{c}^2$ for some $\tilde{c} \in R^*$. We can now define $\sigma_{\tilde{c}} : L \to L$, where $\sigma_{\tilde{c}}(e_i) = \varepsilon\tilde{c}^{-1}\sigma(e_i)$, ε is 1 if $det(A) > 0$ and -1 otherwise. Let $\tilde{A}$ be the matrix for $\sigma_{\tilde{c}}$. We have $\sigma_{\tilde{c}}(L) = L$, $det(\tilde{A}) = 1$ and $q(\sigma_{\tilde{c}}(l)) = q(l)$ for all $l \in L$. Using this we find that $|Aut(\Lambda)| = |Aut^+(f)|$. Also note that for f_i in the genus of f, the determinants of M_{f_i} and M_f are equal up to multiplication by a unit in R, moreover Ω_{f_i} and Ω_f are defined up to multiplication by a unit, so c_{f_i} can be choosen equal to c_f.

4.5. Lemma. *Let $(L_1,q_1) = (L,q), \ldots, (L_t,q_t)$ represent all classes in the genus of (L,q). Then the orders $\Lambda_1 = \Lambda, \ldots, \Lambda_t$, constructed as in the proof of Prop. 4.2, represent all the classes in the genus of Λ.*

Proof. The notations will be same as in the proof of Prop. 4.2. Since $(L_1,q_1) = (L,q), \ldots, (L_t,q_t)$ represent all classes in the genus of (L,q), we know that $(L_1^{\#}, c_0q_1), \ldots, (L_t^{\#}, c_0q_t)$ will represent all classes in the genus of $(L^{\#}, c_0q)$. Assume that $\Lambda^{'}$ and $\Lambda = C_0(L^{\#}, c_0q)$ are in the same genus. Then $d(\Lambda) = d(\Lambda^{'})$ and we may choose $d_\Lambda = d_{\Lambda'}$. Using Prop. 3.11, we have $\Lambda^{'} \cong C_0(L^{'}, q^{'})$ and $\Lambda \cong C_0(L^{''}, q^{''})$, where $q^{'} = d_{\Lambda'}nr_{A/K}$ and $q^{''} = d_\Lambda nr_{A/K}$. Let $M_{q'}$ and $M_{q''}$ be matrices corresponding to the lattices $(L^{'}, q^{'})$ and $(L^{''}, q^{''})$ respectively. We find that the determinants $det(M_{q'})$ and $det(M_{q''})$ can only differ by the square of a unit in R^*. This implies that $(L^{'}, q^{'})$ and $(L^{''}, q^{''})$ are in the same genus, so $\Lambda^{'}$ is isomorphic to one of the orders Λ_i.

□

4.6. Definition. *Let Λ be an R-order in the quaternion algebra A over K and S an R-order in a commutative K-algebra B. An R-embedding $\varphi : S \to \Lambda$ is called optimal if $\Lambda/\varphi(S)$ is R-projective.*

Let $S_0 = R[\sqrt{-c_f N}]$. Then the integral representations of N by f, where $N \gg 0$ and f is as in Prop. 4.2, are in one-to-one correspondence with all embeddings $S_0 \to \Lambda$. Notice that each embedding can be extended to an optimal embedding of an R-order S such that $S_0 \subseteq S \subset K(\sqrt{-c_f N})$. We have $r_f(N) = \sum_S e(S, \Lambda)$, where $e(S, \Lambda)$ denotes the number of optimal embeddings $S \to \Lambda$.

Λ^* acts on the set of embeddings $\varphi : S \to \Lambda$ by inner automorphisms, that is, for $\alpha \in \Lambda^*$, we define $(\alpha \circ \varphi)(s) = \alpha\varphi(s)\alpha^{-1}$, $s \in S$. The isotropy group for φ consists of all elements α in Λ^* such that $\alpha \circ \varphi = \varphi$, that is, those elements $\alpha \in \Lambda$ which commute with each element in $\varphi(S)$ i.e. the isotropy group is $K\varphi(S) \cap \Lambda^*$. Since φ is an optimal embedding $K\varphi(S) \cap \Lambda^* \cong S^*$ and the number of elements in each orbit of Λ^* is $[\Lambda^* : S^*]$. Let $e_{\Lambda^*}(S, \Lambda)$ denote the number of Λ^*-orbits on the set of embeddings of S in Λ. We know that $[\Lambda^* : S^*] < \infty$ since $[\Lambda^* : R^*] < \infty$, see [9], Satz 2. Thus, we have the equality

$$e(S, \Lambda) = [\Lambda^* : S^*] e_{\Lambda^*}(S, \Lambda) = [\Lambda^*/R^* : S^*/R^*] e_{\Lambda^*}(S, \Lambda) \tag{4.7}$$

Using 4.7 and the expression of r_{f_i} by $e(S, \Lambda_i)$, we get

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|Aut^+(f_i)|} = \sum_{i=1}^{t} \sum_{S} \frac{e(S, \Lambda_i)}{|Aut(\Lambda_i)|} = \tag{4.8}$$

$$\sum_{i=1}^{t} \sum_{S} \frac{|\Lambda_i^*/R^*|}{|S^*/R^*||Aut(\Lambda_i)|H(\Lambda_i)} H(\Lambda_i) e_{\Lambda_i^*}(S, \Lambda_i).$$

We will now see that the first factor in this expression does not depend on i.

4.9. Proposition. *$|\Lambda_i^*/R^*|/H(\Lambda_i)|Aut(\Lambda_i)|$ is the same for all i.*

Proof. Let $\mathcal{A}ut(\Lambda) = \{\sigma = (\sigma_\mathfrak{p})_\mathfrak{p}\colon\ \sigma_\mathfrak{p}(x) = \alpha_\mathfrak{p} x \alpha_\mathfrak{p}^{-1},\ \alpha = (\alpha_\mathfrak{p})_\mathfrak{p} \in \mathcal{J}(A)$ and $\sigma_\mathfrak{p}(\hat{\Lambda}_\mathfrak{p}) = \hat{\Lambda}_\mathfrak{p}\}$, where $\mathfrak{p} \in SpecR$, $\mathfrak{p} \neq 0$, and $\mathcal{J}(A)$ is the idèle group of A. Denote $\sigma = [\alpha]$. Then $[\alpha] = [\beta]$ if and only if $\alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p} \in \hat{K}_\mathfrak{p}^*$ ($[\alpha] = [\beta] \Leftrightarrow \alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p} x = x\alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p}$, where $x \in \hat{\Lambda}_\mathfrak{p} \Leftrightarrow \alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p}$ commutes with all elements of $\hat{A}_\mathfrak{p} \Leftrightarrow \alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p} \in \hat{K}_\mathfrak{p}^*$). Let $\mathcal{A}ut^*(\Lambda)$ be the subgroup of $\mathcal{A}ut(\Lambda)$ consisting of

$\sigma = [(\alpha_\mathfrak{p})_\mathfrak{p}]$ such that $\alpha_\mathfrak{p} \in \Lambda^*$. There is a surjective group homomorphism $\varphi : \mathcal{A}ut(\Lambda)/\mathcal{A}ut^*(\Lambda) \to \mathcal{H}(\Lambda)$ such that $\sigma = [\alpha]$ is mapped onto the class of $\Lambda\alpha$. The kernel of this homomorphism will be

$$\frac{\mathcal{A}ut^*(\Lambda)Aut(\Lambda)}{\mathcal{A}ut^*(\Lambda)} \cong \frac{Aut(\Lambda)}{Aut^*(\Lambda)},$$

where $Aut(\Lambda)$ is the automorphism group of Λ and $Aut^*(\Lambda)$ is the subgroup induced by the elements of Λ^*. Hence we get

$$|\mathcal{A}ut(\Lambda)/\mathcal{A}ut^*(\Lambda)| = |Aut(\Lambda)/Aut^*(\Lambda)|H(\Lambda). \tag{4.10}$$

Every automorphism of Λ can be extended to an automorphism of A, so we know that this is an inner automorphism, (by the Skolem-Noether theorem), given by an element $\alpha \in A^*$ and hence $Aut^*(\Lambda) \cong \Lambda^*/R^*$. We also notice that $|\mathcal{A}ut(\Lambda_i)/\mathcal{A}ut^*(\Lambda_i)|$ remains the same for all orders Λ_i in the genus of Λ. This observation concludes the proof. □

We also need the following proposition from [4], p. 204.

4.11. Proposition. *Let $\Lambda_1 = \Lambda, \ldots, \Lambda_t$ represent all the isomorphism classes in the genus of Λ. If S is a maximal commutative suborder of Λ, then*

$$\sum_{i=1}^{t} H(\Lambda_i)e_{\Lambda_i^*}(S, \Lambda_i) = h(S)e_{U(\Lambda)}(S, \Lambda),$$

where $H(\Lambda_i)$ is the two-sided class number of Λ_i, $h(S)$ is the locally free class number of S and $e_{U(\Lambda)}(S, \Lambda) = \prod_\mathfrak{p} e(\hat{S}_\mathfrak{p}, \hat{\Lambda}_\mathfrak{p})$, $\mathfrak{p} \in Spec(R)$, $\mathfrak{p} \neq (0)$.

Interchanging the summation order in 4.8 and applying Prop. 4.9 and 4.11, we get

4.12. Theorem. *Let f be a totally positive definite ternary quadratic form and $\Lambda = C_0(L^\#, c_0 q)$ the quaternion order corresponding to f according to Prop. 4.2. Let $f_1 = f, \ldots, f_t$ represent the classes in the genus of f. Then*

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|Aut^+(f_i)|} = \delta_\Lambda \sum_S \frac{1}{|S^*/R^*|} h(S) e_{U(\Lambda)}(S,\Lambda)$$

where $\delta_\Lambda = \frac{|\Lambda^*/R^*|}{|Aut(\Lambda)|H(\Lambda)}$ *and the sum is taken over all* R*-orders* S *such that* $R[\sqrt{-c_f N}] \subseteq S \subset K(\sqrt{-c_f N})$ *and* S *is a maximal commutative suborder of* Λ.

We make the following observation.

4.13. Lemma. *Let* f *be a totally positive definite ternary quadratic form and let* Λ *be the quaternion order constructed as in the proof of Prop.* 4.2. *Denote by* $r_f^0(N)$ *the number of primitive solutions to* $f(x_1,x_2,x_3) = N$ *(that is, solutions such that* $GCD(x_1,x_2,x_3) = 1$*). The primitive solutions correspond to optimal embeddings of* $S = R[\sqrt{-c_f N}]$ *in* Λ.

Proof. Let $\Lambda = R + RE_1 + RE_2 + RE_3$. We have an embedding $\varphi : S \to \Lambda$, where $\varphi(\sqrt{-c_f N}) = \lambda$, $\lambda^2 = -c_f N$ and $\varphi(S) = R + R\lambda$. $R + R\lambda \subset \Lambda$ and R is PID, so there exists a basis, a_0, a_1, a_2, a_3, for Λ such that $\Lambda = Ra_0 + Ra_1 + Ra_2 + Ra_3$ and $\varphi(S) = Rd_0a_0 + Rd_1a_1$, where $d_0, d_1 \in R$ and $d_0 | d_1$. Then

$$\Lambda/\varphi(S) \cong R/(d_0) \oplus R/(d_1) \oplus R^2$$

so $\Lambda/\varphi(S)$ is R-projective if and only if $d_0, d_1 \in R^*$. Let $f(r_1,r_2,r_3) = N$ be a primitive solution, that is, $GCD(r_1,r_2,r_3) = 1$. Using Prop. 4.2, we get $\lambda = r_0 + r_1E_1 + r_2E_2 + r_3E_3$ such that $\lambda^2 = -c_f N$. We know that $1 = r_0'd_0a_0 + r_1'd_1a_1$ and $\lambda = r_0''d_0a_0 + r_1''d_1a_1$. Then $d_0|1$, since $d_0|d_1$, so $d_0 \in R^*$. We also know that

$$\begin{vmatrix} r_0' & r_0'' \\ r_1' & r_1'' \end{vmatrix} = r_0'r_1'' - r_0''r_1' \in R^*.$$

We observe that $\lambda r_0' - r_0'' = (r_0'r_1'' - r_0''r_1')d_1a_1$. Then $d_1 | r_0'$ and $d_1 | r_0''$, since $GCD(r_1,r_2,r_3) = 1$, so d_1 divides the determinant and we find that $d_1 \in R^*$. Hence the embedding of S in Λ is optimal. Now we assume that $f(r_1,r_2,r_3) = N$ is not primitive. Let $d = GCD(r_1,r_2,r_3)$. Then we know that $d | r_i$, $i = 0,1,2,3$, where r_i denote the coefficients of $\lambda \in \Lambda$. But then $\varphi(S) =$

$R + R\lambda \subset R + R\frac{\lambda}{d}$, that is, $\varphi(S)$ is not a maximal commutative subring of Λ. Hence $\Lambda/\varphi(S)$ is not projective.

□

Using this lemma, we have a Corollary.

4.14. Corollary. *With the same notations as in Prop.* 4.12*,*

$$\sum_{i=1}^{t} \frac{{r^0}_{f_i}(N)}{|Aut^+(f_i)|} = \delta_\Lambda \frac{1}{|S^*/R^*|} h(S) e_{U(\Lambda)}(S, \Lambda),$$

where $S = R[\sqrt{-c_f N}]$.

5 Stability of the embedding numbers

In this Section, we will obtain a result concerning the stability of the embedding numbers in a special case. This result will be needed later on when we calculate the number of primitive representations of $N \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $N \gg 0$, as a sum of three squares.

5.1. Lemma. *Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$, $d > 0$ and d is squarefree. Denote by R the integers in K. Let $S = R[\sqrt{-\alpha}]$ where $\alpha \in R$, $\alpha \notin R^*$ and $\alpha \gg 0$. Then $S^* = R^*$.*

Proof. Let $K' = K(\sqrt{-\alpha})$ and denote by R' the integers in K'. Then $S \subseteq R'$ is a suborder and by Thm. 12.12 in [15], $rank(S^*) = rank(R'^*)$ and $|R'^*/S^*| < \infty$. Then $|S^*/R^*| < \infty$ since $|R'^*/R^*| < \infty$ and furthermore, S^* is a fintely generated $\mathbb{Z}$-module, so $S^* \cong T \oplus \mathbb{Z}^k$, for some k, where T denotes the torsion elements in S^*. Using Dirichlet's unit theorem, we have $R'^* \cong W_{R'} \times \mathbb{Z}$ and $R^* \cong W_R \times \mathbb{Z}$, where $W_{R'}$ and W_R denote the sets of roots of unity in R'^* and in R^* respectively. $R^* \subseteq S^* \subseteq R'^*$, so $S^* \cong W_S \times \mathbb{Z}$. We will now consider possible roots of unity in S. We know that $W_R = \{1, -1\}$, $R = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2$ or $3 \pmod 4$ and $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$. Let ε_n denote an n:th root of unity. Then the minimum polynomial m_{ε_n} is of degree $\varphi(n)$, where φ is the Euler function. In our case, $\varphi(n)|4$, so the only possibilities are $n = 2, 3, 4, 5, 8, 10, 12$. Observing how these roots of unity are related to each other, we find that it is enough to check if any of the following numbers

$$i, \frac{-1+i\sqrt{3}}{2}, \frac{\sqrt{2}+i\sqrt{2}}{2}, \frac{\sqrt{5}-1+i\sqrt{10+2\sqrt{5}}}{4},$$

is an element of S. This can be performed without difficulty and the result is that none of these numbers belong to S, so $W_S = \{1, -1\}$. Now we let ε denote the fundamental unit in R and let ε' denote the fundamental unit in S. We then have that $(\varepsilon')^k = \varepsilon$ for some k. Since $\varepsilon \in \mathbb{R}$ and $S = R + R\sqrt{-\alpha}$, we get $\varepsilon' \in R$, so $\varepsilon' = \varepsilon$. □

5.2. Definition. *An R-order Λ is called left hereditary if every left ideal of Λ is a projective Λ-module.*

Remark. An R-order Λ in a quaternion algebra A is hereditary if and only if $d(\Lambda)$ is square-free (see [2] Prop. 1.2).

5.3. Definition. *An R-order Λ is called Gorenstein if $\Lambda^{\#}$ is projective as a left Λ-module. Λ is a Bass order if each R-order Λ', in A, containing Λ is Gorenstein.*

Given an R-order Λ, we use Prop. 3.11 to find a ternary quadratic form $f(x_1, x_2, x_3) = \sum a_{ij}x_ix_j$ such that $\Lambda \cong C_0(f)$. Λ is a Gorenstein order if and only if the greatest common divisor for the a_{ij}'s is equal to 1 (see [1] Thm. 3.4).

Λ is a Bass order if and only if each completion $\hat{\Lambda}_{\mathfrak{p}}$ is a Bass order for every prime $\mathfrak{p}$ in R (see [7] p. 778). We also recall that an R-order Λ in a quaternion algebra is a Bass order if the reduced discriminant $d(\Lambda)$ is cube-free according to Cor. 1.6 in [2].

For a quaternion order Λ there is a Gorenstein order $G(\Lambda)$ containing Λ such that $\Lambda = R + b(\Lambda)G(\Lambda)$, where $b(\Lambda)$ is an R-ideal. $G(\Lambda)$ and $b(\Lambda)$ are unique (see Prop. 1.4 in [2]).

Let f be a totally positive definite ternary quadratic form, such that $G(\Lambda_f)$ is a Bass order, where Λ_f is the order corresponding to f according to Prop. 4.2. We then have the following generalization of Thm. 3.4 in [6].

5.4. Theorem. *Let $K = \mathbb{Q}(\sqrt{d})$, where d is a positive squarefree rational integer, $d \not\equiv 1 \pmod 8$, such that the ring of integers in K, denoted by R, is a principal ideal domain. Let*

$$\sum_{i=1}^{t} \frac{r^0_{f_i}(N)}{|Aut^+(f_i)|} = \gamma(N)h(S),$$

as in Cor. 4.14, where $r^0_{f_i}(N)$ denotes the number of primitive representations of N by f_i, $S = R[\sqrt{-c_f N}]$ and

$$\gamma(N) = \frac{|\Lambda^*/R^*|}{|Aut(\Lambda)|H(\Lambda)|S^*/R^*|} \prod_{\mathfrak{p}} e(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}}).$$

Then there is a positive rational integer M_0 such that γ has the following property: Let $c_f N = N_0^2 N_1$ and $c_f N' = N_0'^2 N_1'$ be two totally positive non-units in R, where $N_0, N_1, N_0', N_1' \in R$ and N_1, N_1' are squarefree, such that for all $\mathfrak{p} | d(\Lambda_f)$ we have

$$v_{\mathfrak{p}}(N_0) = v_{\mathfrak{p}}(N_0') \text{ or } min(v_{\mathfrak{p}}(N_0), v_{\mathfrak{p}}(N_0')) \geq v_{\mathfrak{p}}(M_0) \tag{5.5}$$

$$N_1 \mathfrak{p}^{-v_{\mathfrak{p}}(N_1)} \equiv N_1' \mathfrak{p}^{-v_{\mathfrak{p}}(N_1')} \pmod{\mathfrak{p}^{2v_{\mathfrak{p}}(2)+1}} \tag{5.6}$$

$$N_1 \equiv N_1' \pmod{16} \tag{5.7}$$

Then $\gamma(N) = \gamma(N')$ and furthermore, one may choose $M_0 = d_{\Lambda_f}$, where $d(\Lambda_f) = (d_{\Lambda_f})$. $v_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic valuation.

Proof. Let $L = K(\sqrt{-c_f N}) = K(\sqrt{-N_1})$ and $L' = K(\sqrt{-N_1'})$. If $c_f N \notin R^*$, then $|S^*/R^*| = 1$ and the factor

$$\frac{|\Lambda^*/R^*|}{|Aut(\Lambda)|H(\Lambda)|S^*/R^*|}$$

is independent of N.

According to Prop. 2.4 and 2.5 in [6], we have $e(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}}) = e(\hat{S}_{\mathfrak{p}}', \hat{\Lambda}_{\mathfrak{p}})$ if the discriminants

$$\Delta(\hat{L}_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}}) \equiv \Delta(\hat{L}_{\mathfrak{p}}'/\hat{K}_{\mathfrak{p}}) \pmod{\mathfrak{p}^{\delta(\hat{L}_{\mathfrak{p}}, \hat{L}_{\mathfrak{p}}')}} \tag{$*$}$$

and the conductors

$$f_{\mathfrak{p}} \equiv f_{\mathfrak{p}}' \pmod{\mathfrak{p}^{i(\mathfrak{p})}}, \tag{$**$}$$

where $\delta(\hat{L}_{\mathfrak{p}}, \hat{L}_{\mathfrak{p}}') = 2v_{\mathfrak{p}}(2) + 1 + \min(v_{\mathfrak{p}}(\Delta(\hat{L}_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}})), v_{\mathfrak{p}}(\Delta(\hat{L}_{\mathfrak{p}}'/\hat{K}_{\mathfrak{p}})))$ and $i(\mathfrak{p})$ is a given rational non-negative integer such that $i(\mathfrak{p}) \leq v_{\mathfrak{p}}(d(\Lambda_f))$. Hence the factor

$$\prod_{\mathfrak{p}} e(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}})$$

depends on the conductor f and the relative discriminant $\Delta(L/K)$. Let $R^{'}$ denote the integers in L. R is a PID, so $R^{'} = R + R\omega$, for some $\omega \in R^{'}$. For a suborder $O \subseteq R^{'}$, we have $O = R + Ra\omega$ for some $a \in R$. Then $f = a$, using the same notation for the generator and the ideal. Using the relation $D(O) = f^2\Delta(L/K)$, (where $D(O)$ denotes the discriminant of the order O, as before), and the fact that $\{1, \sqrt{-N_1}\}$ is a basis for L over K, we find that $\Delta(L/K) = -c^2N_1$ and $f = \frac{2}{c}N_0$ for some $c \in R$ such that $c|2$. We use Thm. 1 in [18] and the classfication of possible cases given in [10] in Tables A-C to see, that the factor c of the relative discriminant will be the same for N_1 and $N_1^{'}$ if $N_1 \equiv N_1^{'} \pmod{16}$.

Assume that the prime $\mathfrak{p}$ does not divide $d(\Lambda_f)$ and let Λ denote a maximal order in A such that $\Lambda_f \subseteq \Lambda$. Then $\mathfrak{p}$ does not divide $d(\Lambda)$, so $\hat{A}_{\mathfrak{p}} = A \otimes \hat{K}_{\mathfrak{p}}$ is split, see Cor. 5.3 in [19]. Since $\mathfrak{p}$ does not divide $d(\Lambda_f)$ we also know that $\hat{\Lambda}_{f\mathfrak{p}}$ is a maximal order and thereby hereditary, see Thm. 17.3 in [17]. According to Prop. 3.1.(b) in [5], we have $e(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{f\mathfrak{p}}) = 1$. Let $\mathfrak{p}|d_{\Lambda_f}$. Then 5.5, 5.6 and 5.7 will ensure that the conditions $(*)$ and $(**)$ are satisfied. Hence $\gamma(N) = \gamma(N^{'})$. The choice $M_0 = d_{\Lambda_f}$ is possible since $i(\mathfrak{p}) \leq v_{\mathfrak{p}}(d_{\Lambda_f})$. □

Remark. If we impose further conditions on N_1 and $N_1^{'}$ a similar Theorem may still be true for $d \equiv 1$ (*mod* 8).

5.8. Corollary. *The notations are as in Thm.* 5.4. *There exist positive rational integers M_0 and M_1 such that the value of $\gamma(N) = \gamma(N_0, N_1)$ is determined by the residues of N_0 modulo M_0 and N_1 modulo M_1.*

Proof. Let d_1 denote the product of all different primes $\mathfrak{p}$ in R such that $\mathfrak{p}$ divides d_{Λ_f} but $\mathfrak{p}$ does not divide 2. It follows from Thm. 5.4 that it is possible to choose $M_0 = d(\Lambda_f)$ and $M_1 = (4d_1)^2$. □

6 Examples and applications

As an application of the theory described in Section 4 and 5, we prove that every totally positive number in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ has a primitive representation as a sum of three squares and we calculate the number of primitive representations. We will also demonstrate a different method to calculate the number of primitive representations of totally positive integers in quadratic real number fields K, by a quadratic form corresponding to a maximal order Λ in a totally definite quaternion algebra over K, such that $d(\Lambda) = R$ and $h_\Lambda = 1$.

We assume as before that R is a principal ideal domain such that its quotient field K is a totally real algebraic number field. We now recall the definition of the Eichler symbol:

6.1. Definition. *Denote by $J(\Lambda)$ the Jacobson radical of Λ. Then*

$e_\mathfrak{p}(\Lambda) = -1$ *if* $\hat{\Lambda}_\mathfrak{p}/J(\hat{\Lambda}_\mathfrak{p})$ *is a quadratic field extension of* $\hat{R}_\mathfrak{p}/\mathfrak{m}$,

$e_\mathfrak{p}(\Lambda) = 0$ *if* $\hat{\Lambda}_\mathfrak{p}/J(\hat{\Lambda}_\mathfrak{p}) \cong \hat{R}_\mathfrak{p}/\mathfrak{m}$,

$e_\mathfrak{p}(\Lambda) = 1$ *if* $\hat{\Lambda}_\mathfrak{p}/J(\hat{\Lambda}_\mathfrak{p}) \cong \hat{R}_\mathfrak{p}/\mathfrak{m} \times \hat{R}_\mathfrak{p}/\mathfrak{m}$,

where $\mathfrak{m}$ denotes the maximal ideal in $\hat{R}_\mathfrak{p}$.

Let f be a ternary quadratic form such that the even Clifford algebra $C_0(f)$ is isomorphic to Λ. If $\hat{\Lambda}_\mathfrak{p}$ is not a maximal order in a matrix algebra over K, then according to [3], (2.6), $|e_\mathfrak{p}(\Lambda)| + 1$ is equal to the rank of f modulo $\mathfrak{p}$, and moreover, if $e_\mathfrak{p}(\Lambda) = 1$, then f modulo $\mathfrak{p}$ is a product of two different linear factors and if $e_\mathfrak{p}(\Lambda) = -1$, then f is irreducible modulo $\mathfrak{p}$.

Let $K = \mathbb{Q}(\sqrt{5})$, $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and let $f : R^3 \to R$, $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$. Denote by Λ_f the quaternion order $C_0(L^\#, c_0 q)$ corresponding to f according to Thm. 4.2 and denote by A the quaternion algebra $K \otimes \Lambda_f$. We have $c_f = 1$ and $\Lambda_f = R + RE_1 + RE_2 + RE_3$, where $E_i^2 = E_j^2 = -1$ and $E_iE_j = -E_jE_i = -E_k$, where i, j, k is an even permutation of $1, 2, 3$. The type number of $C_0(f) \cong \Lambda_f$ is 1, since the type number of f is 1 (see [8] Satz 24). Since $d(\Lambda_f) = 4$ is cube-free, we know that Λ_f is a Bass order.

It was proved in [13] that every totally positive number N in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ can be represented as a sum of three squares. We will now give a proof of

this, based on algebraic methods. Moreover, we will prove that there is a primitive representation for every totally positive number.

6.2. Theorem. *Every totally positive number N in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ can be represented by $f : R^3 \to R$, where*

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2.$$

Moreover, there is always $(x_1, x_2, x_3) \in R^3$ such that $GCD(x_1, x_2, x_3) = 1$ and $f(x_1, x_2, x_3) = N$.

Proof. Let Λ denote the order corresponding to f, described above, let $N \in R$ be totally positive with $N = N_1 N_0^2$ where $N_0, N_1 \in R$ and N_1 is square-free. Let $L = K(\sqrt{-N_1})$. It can then be checked that the discriminant $\Delta(L/K) = -N_1$ if $-N_1 \equiv 1, \quad \omega + 1$ or $(\omega + 1)^2$, where $\omega = \frac{1+\sqrt{5}}{2}$, and $\Delta(L/K) = -4N_1$ otherwise. A is a totally definite quaternion algebra so it ramifies at both infinte primes. We know that A ramifies at an even number of primes and that the finite primes where A ramifies divide the reduced discriminant of the maximal orders (see [19], Chap. II, Cor. 5.3 and Chap. III, Thm. 3.1). Since $d_\Lambda = 4$, we then know that A only ramifies at the infinite primes. Furthermore, $\hat{\Lambda}_2$ is not maximal, but $\hat{\Lambda}_\mathfrak{p}$ is maximal for all primes $\mathfrak{p} \neq 2$ in R.

Using Lemma 4.13 and Cor. 4.14, all we need to show is that for a totally positive integer $N \in R$ it is possible to embedd $S = R[\sqrt{-N}]$ as a maximal commutative suborder of Λ, that is, $e_{U(\Lambda)}(S, \Lambda) \neq 0$. We start by observing that by Thm. 3.2. in [19], we have $e(\hat{S}_\mathfrak{p}, \hat{\Lambda}_\mathfrak{p}) = 1$, for all $\mathfrak{p} \neq 2$ and all orders S in a commutative algebra of degree two over K, since $\hat{\Lambda}_\mathfrak{p}$ is maximal.

The rank of f modulo 2 is 1, so $e_2(\Lambda) = 0$. If 2 divides $\Delta(L/K)$, then $e(\hat{S}_2, \hat{\Lambda}_2) \neq 0$, by 3.14 in [5] if $\hat{S}_2$ is maximal in $\hat{L}_2$, since L is ramified over K, and by 3.17 in [5] if it is not maximal. If 2 does not divide $\Delta(L/K)$, then the maximal order of L will be $R[\frac{a+\sqrt{-N_1}}{2}]$, where $a = 1$ for $-N_1 \equiv 1$, $a = \omega + 1$ for $-N_1 \equiv (\omega + 1)^2$ and $a = (\omega + 1)^2$ for $-N_1 \equiv \omega + 1$. We have $S = R[\sqrt{-N}]$. Hence, $\hat{S}_2$ will not be maximal in $\hat{L}_2$, so by 3.17 in [5], we have $e(\hat{S}_2, \hat{\Lambda}_2) \neq 0$. Hence $e_{U(\Lambda)}(S, \Lambda) \neq 0$. □

To conclude the example we shall now calculate the number of primitive representations. We have $|Aut^+(f)| = 24$. Using Cor. 5.8 we may choose $M_0 = 4$ and $M_1 = 16$. We also observe that for N_1 not divisible by 2, $M_1 = 8$ suffices (see Tables A-C in [10], Thm. 1 in [18] and Thm. 5.4). Choosing a suitable limited set of numbers N to represent all congruence classes modulo

M_0 and M_1, we compute $h(R[\sqrt{-N}])$. We also compute the number of primitive representations of N by f. ¿From these results we deduce that the only possible values for $\gamma(N)$ are $\frac{1}{2}, 1, \frac{4}{3}, 4$ and 16. PARI-GP was used for these computations. The values of $r_f^0(N)$ for $N = N_0^2 N_1$ will be

$$r_f^0(N) = \begin{cases} 384h(S) & \text{if } N_0 \equiv 0 \pmod 4 \\ & \qquad \text{and } N_1 \equiv 3, 2+\omega, 3+3\omega \pmod 4, \\ 96h(S) & \text{if } N_0 \equiv 0 \pmod 4 \\ & \qquad \text{and } N_1 \not\equiv 3, 2+\omega, 3+3\omega \pmod 4, \\ & \text{or } N_0 \equiv 0 \pmod 2,\ N_0 \not\equiv 0 \pmod 4 \\ & \qquad \text{and } N_1 \equiv 3, 2+\omega, 3+3\omega \pmod 4, \\ 32h(S) & \text{if } N_0 \not\equiv 0 \pmod 2 \\ & \qquad \text{and } N_1 \equiv 3, 7, 3+3\omega, 6+\omega, 6+5\omega, 7+7\omega \pmod 8, \\ 24h(S) & \text{if } N_0 \equiv 0 \pmod 2,\ N_0 \not\equiv 0 \pmod 4 \\ & \qquad \text{and } N_1 \not\equiv 3, 2+\omega, 3+3\omega \pmod 4, \\ & \text{or } N_0 \not\equiv 0 \pmod 2 \\ & \qquad \text{and } N_1 \equiv 2+\omega, 2+5\omega, 3+4\omega, 3+7\omega, 7+3\omega, 7+4\omega \pmod 8, \\ 12h(S) & \text{otherwise,} \end{cases}$$

where $S = R[\sqrt{-N}]$.

In the following example, we use a different method. We start with maximal R-orders Λ in totally definite quaternion algebras over quadratic real number fields $\mathbb{Q}(\sqrt{m})$ such that $d(\Lambda) = R$ and $h_\Lambda = 1$. There are only four such cases and these are $m = 2, 5, 13, 17$, see [19] p. 155. We will denote the maximal orders by $\Lambda^{(m)}$. We have $\Lambda^{(m)} \cong C_0(f_m)$ with m and f_m as in the following table.

m	f_m
2	$x_1^2 + x_2^2 + x_3^2 + \sqrt{2}x_1x_2 + x_1x_3$
5	$x_1^2 + x_2^2 + x_3^2 + \omega x_1x_2 + \omega^{-1}x_1x_3$
13	$2x_1^2 + 2x_2^2 + x_3^2 + \sqrt{13}x_1x_2 + x_1x_3$
17	$6x_1^2 + 3x_2^2 + x_3^2 + 2\sqrt{17}x_1x_2 + x_1x_3$

We would now like to find the number of primitive representations of a totally positive number N by f_m. We start with the following observation.

6.3. Lemma. *Let $\Lambda = C_0(f)$ be an R-order, in A, such that $d(\Lambda) = R$. Let $L = \Lambda \cap A_0$ and $L^\# = \Lambda^\# \cap A_0$, with notations as in Prop.* 3.11. *Then $(L, nr_{A/K}) \cong (L^\#, nr_{A/K})$.*

Proof. Let $f(r_1, r_2, r_3) = \sum a_{ij}r_ir_j$ and let $1, E_1, E_2, E_3$ denote an R-basis for Λ. We have $\Lambda \cong C_0(L^\#, nr_{A/K})$ by Prop. 3.11. $\Lambda^\# = \{x \in A : tr(x\Lambda) \subseteq R\}$, so $\Lambda \subseteq \Lambda^\#$ and $L \subseteq L^\#$. We also know that $L^\# = RF_1 + RF_2 + RF_3$, where $F_i = a_{ii}a_{jk} - a_{ij}a_{ik} - 2a_{ii}E_i - a_{ij}E_j - a_{ik}E_k$ (see Prop. 4.4), so $F_i \in \Lambda$ for $i = 1, 2, 3$. Hence $L^\# \subseteq L$ and $(L, nr_{A/K}) \cong (L^\#, nr_{A/K})$. □

For an element $\lambda \in \Lambda^{(m)}$, we have $\lambda^2 - tr(\lambda)\lambda + nr(\lambda) = 0$, so $\lambda^2 = -nr(\lambda)$ for $\lambda \in L = \Lambda \cap A_0$. Using the condition $tr(\lambda) = 0$ to substitute one of the variables in the expression for $nr(x_0 + x_1E_1 + x_2E_2 + x_3E_3)$ we get a ternary quadratic form $f : R^3 \to R$. We then have a one-to-one correspondence between representations of N by f and the solutions $\lambda \in \Lambda$ to the equation $x^2 = -N$, that is, we have a one-to-one correspondence between representations of N by f and the embeddings of $S_0 = R[\sqrt{-N}]$ in $\Lambda^{(m)}$. We observe that each embedding can be extended to an optimal embedding of an R-order S, where $S_0 \subseteq S \subset K(\sqrt{-N})$, so $r_f(N) = \sum_S e(S, \Lambda^{(m)})$. Using (4.7), Prop. 4.11 and the fact that $h_{\Lambda^{(m)}} = 1$, we find that

$$r_f(N) = |\Lambda^{(m)*}/R^*| \sum_S \frac{h(S)}{|S^*/R^*|} e_{U(\Lambda^{(m)})}(S, \Lambda^{(m)}) \,. \tag{6.4}$$

Since $\Lambda^{(m)}$ is a maximal order and $\hat{A}_{\mathfrak{p}}$ is split for all finite primes $\mathfrak{p}$, we have $e_{U(\Lambda^{(m)})}(S, \Lambda^{(m)}) = 1$ (see [5], Prop. 3.1 b)). Hence

$$r_f(N) = |\Lambda^{(m)*}/R^*| \sum_S \frac{h(S)}{|S^*/R^*|}. \tag{6.5}$$

Using the lemma above and observing that $C_0(f_m) \cong C_0(L^{\#}, nr_{A/K})$, by Prop. 3.11, so $r_f(N) = r_{f_m}(N)$. Then we also know that $r_f^0(N) = r_{f_m}^0(N)$. We are interested in the number of primitive representations of a totally positive integer N by f. We have to determine the maximal commutative suborders S of $\Lambda^{(m)}$ and calculate $\frac{|\Lambda^{(m)*}/R^*|}{|S^*/R^*|}$ to get an explicit formula. We will begin with the case $m = 5$.

Calculating the norm of an element $\lambda = r_0 + r_1E_1 + r_2E_2 + r_3E_3$ in $C_0(f_5)$ and using the condition $tr(\lambda) = 0$, we get the quadratic form

$$f(x_1, x_2, x_3) = x_1^2 + 2\omega^{-2}x_2^2 + (7 - 4\omega)x_3^2 + (-3 + \omega)x_1x_2 -$$

$$2\omega^{-2}x_1x_3 + (10 - 6\omega)x_2x_3.$$

When we use the condition $tr(\lambda) = 0$, we may choose to substitute a different variable (this would give us an equivalent form). We observe that if $f(r_1, r_2, r_3) = N$, then $\lambda = r_3 + r_1E_1 + r_2E_2 + (-2r_3\omega^{-1} + \omega^{-2}r_2)E_3$ is such that $\lambda^2 = -N$. Using this correspondence and assuming that we have a primitive representation by f of $N = N_0^2N_1$, where $N_0, N_1 \in R$ and N_1 is square-free, we find that $S = R[N_0\frac{a+\sqrt{-N_1}}{2}]$ if $2|GCD(r_1, r_2)$, where $a = 1, 1+\omega, (1+\omega)^2$ for $N_1 \equiv 3, 2+\omega, 3+3\omega \pmod 4$ respectively, and $S = R[\sqrt{-N}]$ otherwise. Hence, for $N_1 \equiv 3, 2+\omega, 3+3\omega \pmod 4$, there will be contributions from $S_1 = R[N_0\frac{a+\sqrt{-N_1}}{2}]$ and $S_0 = R[\sqrt{-N}]$. In all other cases only $S_0 = R[\sqrt{-N}]$ will contribute.

To calculate $|\Lambda^{(m)*}/R^*|$, we start by observing that $nr(\lambda) \gg 0$ for $\lambda \in \Lambda^{(m)}$. Hence, for $\lambda \in \Lambda^{(m)*}$, we have $nr(\lambda) = \varepsilon^2 \in R^*$. It is then enough to find the elements $\lambda \in \Lambda^{(m)}$ such that $nr(\lambda) = 1$ and look at these modulo R^*. We get $|\Lambda^{(5)*}/R^*| = 60$.

Calculations similar to those in the proof of Lemma 5.1 will give us the value of $|S_i^*/R^*|$ for $i = 0, 1$.

The other cases have been calculated in the same way. For $m = 2, 13$, [18] was used to find relative integral bases. Our final results are given by the formula

$$r_f^0(N) = |\Lambda^{(m)*}/R^*| \sum_i \frac{h(S_i)}{|S_i^*/R^*|}. \tag{6.6}$$

and the following tables:

m=2

Then $R = \mathbb{Z}[\sqrt{2}]$. We choose $f(x_1, x_2, x_3) = x_1^2 + 3x_2^2 + x_3^2 + 2\sqrt{2}x_1x_2 + x_1x_3 + 2\sqrt{2}x_2x_3$. The explicit correspondence between the solutions to $f(x_1, x_2, x_3) = N$ and elements $\lambda \in \Lambda^{(2)}$ will be that $\lambda = r_2 + r_1E_1 - (2r_2 + \sqrt{2}r_3)E_2 + r_3E_3$ corresponds to $f(r_1, r_2, r_3) = N$. We also have $|\Lambda^{(2)*}/R^*| = 24$. The summation in (6.6) should be done according to the following:

$\mathbf{N_1}$ **(mod 4)**	**Sum over**	**a**
$3, 1 + 2\sqrt{2}$	$S_0 = R[\sqrt{-N}]$ $S_1 = R[N_0\frac{1+\sqrt{-N_1}}{\sqrt{2}}]$ $S_2 = R[N_0\frac{a+\sqrt{-N_1}}{2}]$	1 for $N_1 \equiv 3$ $1 + \sqrt{2}$ for $N_1 \equiv 1 + 2\sqrt{2}$
$1, 3 + 2\sqrt{2}$	$S_0 = R[\sqrt{-N}]$ $S_1 = R[N_0\frac{1+\sqrt{-N_1}}{\sqrt{2}}]$	
otherwise	$S_0 = R[\sqrt{-N}]$	

The values of $|S_i^*/R^*|$ will be

$$|S_2^*/R^*| = \begin{cases} 3 & \text{if } N_1 = 3 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise,} \end{cases}$$

$$|S_1^*/R^*| = \begin{cases} 4 & \text{if } N_1 = 1 \quad \text{and } N_0 \in R^* \\ 2 & \text{if } N_1 = 1 \quad \text{and } N_0 = \sqrt{2}\varepsilon,\ \varepsilon \in R^* \\ 1 & \text{otherwise,} \end{cases}$$

$$|S_0^*/R^*| = \begin{cases} 2 & \text{if } N_1 = 1 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise.} \end{cases}$$

Then $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathbb{Z}[\omega]$. We choose $f(x_1, x_2, x_3) = x_1^2 + 2\omega^{-2}x_2^2 + (7 - 4\omega)x_3^2 + (-3+\omega)x_1x_2 - 2\omega^{-2}x_1x_3 + (10-6\omega)x_2x_3$. The explicit correspondence will be that $\lambda = r_3 + r_1E_1 + r_2E_2 + (-2r_3\omega^{-1} + \omega^{-2}r_2)E_3$ corresponds to $f(r_1, r_2, r_3) = N$. We have $|\Lambda^{(5)*}/R^*| = 60$ and the summation in (6.6) should be done according to the following:

$\mathbf{N_1}$ **(mod 4)**	**Sum over**	**a**
$3, 2+\omega, 3+3\omega$	$S_0 = R[\sqrt{-N}]$ $S_1 = R[N_0\frac{a+\sqrt{-N_1}}{2}]$	1 for $N_1 \equiv 3$ $1+\omega$ for $N_1 \equiv 2+\omega$ $(1+\omega)^2$ for $N_1 \equiv 3+3\omega$
otherwise	$S_0 = R[\sqrt{-N}]$	

The values of $|S_i^*/R^*|$ will be

$$|S_1^*/R^*| = \begin{cases} 5 & \text{if } N_1 = 2+\omega \quad \text{and } N_0 \in R^* \\ 3 & \text{if } N_1 = 3 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise,} \end{cases}$$

$$|S_0^*/R^*| = \begin{cases} 2 & \text{if } N_1 = 1 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise.} \end{cases}$$

m=13

Then $R = \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$. We let $\mu = \frac{1+\sqrt{13}}{2}$. We choose $f(x_1, x_2, x_3) = 2x_1^2 + 7x_2^2 + 17x_3^2 + 2\sqrt{13}x_1x_2 + 11x_1x_3 + 6\sqrt{13}x_2x_3$. The explicit correspondence will be that $\lambda = r_2 + r_1E_1 - (2r_2 + \sqrt{13}r_3)E_2 + r_3E_3$ corresponds to $f(r_1, r_2, r_3) = N$. We have $|\Lambda^{(13)*}/R^*| = 6$ and the summation in (6.6) should be done according to the following:

$\mathbf{N_1}$ **(mod 4)**	**Sum over**	**a**
$3, \mu, 1 + 3\mu$	$S_0 = R[\sqrt{-N}]$ $S_1 = R[N_0\frac{a+\sqrt{-N_1}}{2}]$	1 for $N_1 \equiv 3$ $1 + \mu$ for $N_1 \equiv \mu$ μ for $N_1 \equiv 1 + 3\mu$
otherwise	$S_0 = R[\sqrt{-N}]$	

The values of $|S_i^*/R^*|$ will be

$$|S_1^*/R^*| = \begin{cases} 3 & \text{if } N_1 = 3 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise,} \end{cases}$$

$$|S_0^*/R^*| = \begin{cases} 2 & \text{if } N_1 = 1 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise.} \end{cases}$$

m=17

Then $R = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$. We let $\gamma = \frac{1+\sqrt{17}}{2}$, $\mathfrak{p}_1 = 1+\gamma$ and $\mathfrak{p}_2 = -2+\gamma$. Then $\mathfrak{p}_1\mathfrak{p}_2 = 2$. We choosee $f(x_1,x_2,x_3) = 3x_1^2 + 23x_2^2 + 358x_3^2 + 4\sqrt{17}x_1x_2 + 65x_1x_3 + 44\sqrt{17}x_2x_3$. The explicit correspondence will be that $\lambda = r_2 + r_1E_1 - 2(r_2+\sqrt{17}r_3)E_2 + r_3E_3$ corresponds to $f(r_1,r_2,r_3) = N$. We have $|\Lambda^{(17)*}/R^*| = 4$ and the summation in (6.6) should be done according to the following:

$\mathbf{N_1}$ **(mod 4)**	**Sum over**	
3	$S_0 = R[\sqrt{-N}]$ $S_1 = R[N_0\frac{1+\sqrt{-N_1}}{\mathfrak{p}_1}]$ $S_2 = R[N_0\frac{1+\sqrt{-N_1}}{\mathfrak{p}_2}]$ $S_3 = R[N_0\frac{1+\sqrt{-N_1}}{2}]$	
$3+\gamma, 3+2\gamma, 3+3\gamma$	$S_0 = R[\sqrt{-N}]$ $S_2 = R[N_0\frac{1+\sqrt{-N_1}}{\mathfrak{p}_2}]$	
$3\gamma, 1+2\gamma, 2+\gamma$	$S_0 = R[\sqrt{-N}]$ $S_1 = R[N_0\frac{1+\sqrt{-N_1}}{\mathfrak{p}_1}]$	
otherwise	$S_0 = R[\sqrt{-N}]$	

The values of $|S_i^*/R^*|$ will be

$$|S_3^*/R^*| = \begin{cases} 3 & \text{if } N_1 = 3 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise,} \end{cases}$$

$$|S_2^*/R^*| = |S_1^*/R^*| = 1.$$

$$|S_0^*/R^*| = \begin{cases} 2 & \text{if } N_1 = 1 \quad \text{and } N_0 \in R^* \\ 1 & \text{otherwise.} \end{cases}$$

References

[1] J. Brzezinski, A Characterisation of Gorenstein Orders, Math. Scand. 50 (1982), 19-24.

[2] J. Brzezinski, On orders in quaternion algebras, Communications in Algebra, 11(5) (1983), 501-522.

[3] J. Brzezinski, Spinor Class Groups of Orders, Journal of Algebra 84, 1983, 468-481.

[4] J. Brzezinski, A combinatorial class number formula, J.reine angew. Math. 402, (1989), 199-210.

[5] J. Brzezinski, On automorphisms of quaternion orders, J.reine angew. Math. 403, (1990), 166-186.

[6] J. Brzezinski, On embedding numbers into quaternion orders, Comment. Math. Helvetici 66 (1991), 302-318.

[7] C. W. Curtis and I. Reiner, Methods of representation theory, Vol. I, John Wiley & Sons, Inc., New York, 1981.

[8] J. Dzewas, Quadratsummen in reell-quadratischen Zahlörpern, Matematische Nachrichten 21, 1960, 233-284.

[9] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math. 195 (1955), 127-151.

[10] J. G. Huard, B. K. Spearman and K. S. Williams, Integral Bases for Quartic Fields with Quadratic Subfields, J. Number Theory 51 (1995), 87-102.

[11] I. Kaplansky, Submodules of quaternion algebras, Proc. London Math. Soc. 19, (1969), 219-232.

[12] M.-A. Knus, Quadratic and Hermitian Forms over Rings, Springer-Verlag Berlin Heidelberg, 1991.

[13] H. Maass, Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten, Abh. Math. Sem. Hamburg 14 (1941), 185-191.

[14] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd ed., Springer-Verlag New York, 1990.

[15] J. Neukirch, Algebraische Zahlentheorie, Springer-Verlag Berlin Heidelberg, 1992.

[16] R. Pierce, Associative Algebras, Springer-Verlag New York Inc, 1982.

[17] I. Reiner, Maximal Orders, Academic Press Inc. (London) Ltd, 1975.

[18] B. K. Spearman and K. S. Williams, Relative integral bases for quartic fields over quadratic subfields, Acta Math. Hungar. 70 (3) (1996), 185-192.

[19] M-F. Vignéras, Arithmétic des Algèbres de Quaternions, Springer-Verlag Berlin Heidelberg, 1980.