Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 189–199.

Traces of Eichler–Brandt matrices and type numbers of quaternion orders

OTTO KÖRNER

Abteilung für Mathematik IV der Universität, Oberer Eselsberg, D 7900 Ulm, FRG

Abstract. Let A be a totally definite quaternion algebra over a totally real algebraic number field F and M be the ring of algebraic integers of F. For any M-order G of A we derive formulas for the mass $m(G)$ and the type number $t(G)$ of G and for the trace of the Eichler–Brandt matrix $B(G, J)$ of G and any integral ideal J of M in terms of genus invariants of G and of invariants of F and J. Applications to class numbers of quaternion orders and of ternary quadratic forms are indicated.

Keywords. Quaternion orders; class numbers; Eichler–Brandt matrices.

1. Introduction

Let $F, M, A, G, m(G), t(G)$ and $B(G, J)$ be as in the abstract above (s. definitions of these concepts in the following sections). The formulas for $m(G)$ (s. Theorem 1) and for the trace $\mathrm{Tr}\, B(G, J)$ (s. Theorem 2) and for $t(G)$ (s. Theorem 3) we derive in this paper generalize results that were obtained by Eichler [2], Peters [10] and Pizer [11], [12] for M-orders G of special type. For general G some of our results were stated without proof in [8]. Similarly as Pizer [11] we use for our proofs integration on some quotient spaces of the idele group of A and an elementary version of Selberg's trace formula (s. Lemma 2). It is clear that the results can be applied to the computation of the class number $h(G)$ of G because of the relation $h(G) = \mathrm{Tr}\, B(G, M)$. An application to any totally definite ternary quadratic M-lattice L is as follows. The second Clifford algebra C_2 of the quadratic F-vector space $F \otimes_M L$ is a totally definite quaternion algebra over F. Consider the M-order O_L of C_2 corresponding to L in the sense of Eichler [3], § 14. Then the type number $t(O_L)$ equals the number of all classes in the genus of L, as can be seen by deductions analogous to [10].

2. Notations, definitions and known consequences

By $|S|$ we denote the cardinality of any set S. For any ring R with unit element we denote the multiplicative group of all units of R by $U(R)$.

First, more generally than in the introduction, let F be the quotient field of any Dedekind domain M and A be a separable finite dimensional F-algebra. Subalgebras (e.g. F) of A are supposed to have the same unit element as A. Denote by P the set of all maximal ideals of M. If $p \in P$, then the spot of F corresponding to p is also denoted by p. An M-lattice on A is defined to be a finitely generated submodule of the M-module A containing an F-basis of A. An M-order of A is by definition an M-lattice on A containing M and being a subring of A. For any M-lattice Λ on A the sets $\Lambda^{(l)} = \{x \in A \mid x\Lambda \subset \Lambda\}$ and $\Lambda^{(r)} = \{x \in A \mid \Lambda x \subset \Lambda\}$ are M-orders of A. Let G be any M-order of A. Then an M-lattice Λ on A with $G \subset \Lambda^{(l)}$ or $G \subset \Lambda^{(l)} \cap \Lambda^{(r)}$ is called a left ideal or a two-sided ideal of G respectively. A left ideal Λ of G is called invertible, if $\Lambda\Lambda^{-1} = G$, where $\Lambda^{-1} = \{x \in A \mid \Lambda x \Lambda \subset \Lambda\}$; Λ is called integral, if $\Lambda \subset G$; it is called primitive, if Λ is integral, invertible and not contained in pG for all $p \in P$.

Now let F be an algebraic number field or the completion of such a field at a discrete spot, and let M be the ring of integers of F. For any spot p of F (not necessarily in P) we denote by F_p the completion of the field F at p and by A_p the topological F_p-algebra being the completion of A with respect to the p-adic topology. Denote by P_o the set of all spots p of F for which A_p is a skew field. If S is a subset of A, then let S_p denote its closure in A_p. If $p \in P$, then $U(A_p)$ is an open subset of A_p and (with respect to the subset topology) a locally compact group with a countable basis for its topology, and $U(G_p)$ is an open compact subgroup. In the following Π always means the product over all $p \in P$. The restricted idele group $\hat{U}(A)$ of A is a subgroup of $\Pi U(A_p)$ and defined to be the union of all sets of the form $T = \Pi T^{(p)}$, where $T^{(p)}$ is any open subset of $U(A_p)$ such that $T^{(p)} = U(G_p)$ for almost all p (i.e. for all but finitely many); and the sets T are to form a basis for the (open sets of the) topology of $\hat{U}(A)$. This way $\hat{U}(A)$ becomes a topological group whose definition is independent of the choice of the order G, since for any other M-order G' of A one has $G'_p = G_p$ for almost all p by the Local–Global Principle for M-lattices [9]. The group $\hat{U}(A)$ is locally compact and has a countable basis for its topology. The group $U(A)$ is viewed as a subgroup of $\hat{U}(A)$ by the diagonal embedding. If K is any subalgebra of A, then $\hat{U}(K)$ is regarded as a subgroup of $\hat{U}(A)$ by the canonical inclusion map. If Λ is an M-lattice on A and $x = (x_p) \in \hat{U}(A)$, then we denote by Λx the unique M-lattice on A satisfying $(\Lambda x)_p = \Lambda_p x_p$ for all $p \in P$. Analogously $x\Lambda$ is defined.

Additionally let A be F or a two-dimensional separable F-algebra or a quaternion algebra over F. Then it is known [6] that an M-lattice Λ on A is an invertible left ideal of G, if and only if $\Lambda = Gy$ for some $y \in \hat{U}(A)$. Two invertible left ideals Λ, Λ' of G are said to be in the same class, if $\Lambda' = \Lambda x$ for some $x \in U(A)$. The number $h(G)$ (possibly infinite) of the classes of all invertible left ideals of G is called the class number of G. Since $\Lambda = Gy$, $\Lambda' = Gy'$, $y, y' \in \hat{U}(A)$, we have Λ and Λ' in the same class, if and only if y' lies in the double coset $\hat{U}(G)yU(A)$, where $\hat{U}(G)$ denotes the subgroup $\Pi U(G_p)$ of $\hat{U}(A)$. Hence $h(G)$ equals the cardinality of the set $\hat{U}(G)\backslash\hat{U}(A)/U(A)$ of all double cosets. Since $\hat{U}(M) = \Pi U(M_p)$ is a subgroup of $\hat{U}(G)$ and of the centre of $\hat{U}(A)$, the canonical homomorphism $k\colon \hat{U}(A) \to \hat{U}(A)/\hat{U}(M)$ yields

$$h(G) = |\hat{U}(G)\backslash\hat{U}(A)/U(A)| = |k(\hat{U}(G))\backslash k(\hat{U}(A))/k(U(A))|. \qquad (1)$$

Additionally let $A \neq F$. Then we denote by $T(x) = x + x^*$ the reduced trace and by $N(x) = xx^*$ the reduced norm of any $x \in A$, where $x \mapsto x^*$ is the standard involution of A. The norm $N(\Lambda)$ of any M-lattice Λ on A is defined to be the submodule of the M-module F generated by the reduced norms of all elements of Λ. Apparently $N(\Lambda)$ is a fractional ideal of M (i.e. an M-lattice on F). We denote by $\nu(G)$ the set of the norms of all primitive two-sided ideals of G.

From now on let F, M, A and G be as in the introduction. That A be totally definite means that all archimedian spots of F belong to P_o, in other words: $N(x)$ is a totally positive number in F for all non-zero $x \in A$. The reduced discriminant $d_r(G)$ of G is defined to be the integral ideal of M satisfying $(d_r^2(G))_p = M_p \det(T(x_{ip}x_{jp}^*))$ for all $p \in P$, where $x_{1p}, \ldots, x_{4p}$ is any M_p-basis of G_p. In the Theorems 1–3 and their proofs Π' means always the product over all $p \in P$ satisfying $p \mid d_r(G)$.

3. Tools from integration on groups

The following elementary lemma (whose proof is obvious) is convenient for proving the finiteness of class numbers.

Lemma 1. Let D be a discrete subgroup of a locally compact group L and B be an open compact subgroup of L. Then the set $B \backslash L/D$ is finite, if and only if the homogeneous space L/D is compact.

Let D, L, B be as in Lemma 1 and suppose that L/D is compact and that L has a countable basis for its topology. Then D as a discrete subgroup of L is countable (possibly finite), and L is unimodular. Denote by μ the left invariant Haar measure on L with $\mu(B) = 1$. That L is unimodular means that μ is also right invariant. For any $s \in D$ let $D(s)$ denote the centralizer of s in D, and μ_s be the L-left invariant quotient measure of μ on $L/D(s)$ normalized by the condition

$$\int_L f(x)\,\mathrm{d}\mu(x) = \int_{L/D(s)} \left(\sum_{q \in D(s)} f(xq) \right) \mathrm{d}\mu_s(xD(s)) \tag{2}$$

for every complex-valued continuous function f on L with compact support. A consequence of (2) is

$$\mu_s(BxD(s)/D(s)) = |x^{-1}Bx \cap D(s)|^{-1} \tag{3}$$

for all $x \in L$. Under the conditions for D, L, B assumed as above one has

Lemma 2. Let Bx_iD $(i = 1, \ldots, H)$ be the different double cosets with $x_i \in L$, and let f be a complex-valued continuous function on L, with compact support such that $f(b_1xb_2) = f(x)$ for all $x \in L$, $b_1, b_2 \in B$. Then in the series $R(x) = \sum_{g \in D} f(xgx^{-1})$ almost all terms vanish, if the variable x is restricted to any compact subset of L. Furthermore

$$\sum_{i=1}^{H} |x_i^{-1}Bx_i \cap D|^{-1} R(x_i) = \sum_{s \in S} I_s, \tag{4}$$

where

$$I_s = \int_{L/D(s)} f(xsx^{-1})\,\mathrm{d}\mu_s(xD(s))$$

and S denotes any fixed system of representatives for the conjugacy classes in D.

Proof. From Selberg's trace formula [13] it is possible to deduce (4); but for the convenience of the reader I prefer to present here an elementary direct proof. Since f has compact support and D is discrete, almost all terms of the series $R(x)$ vanish on every fixed compact subset of L. The series defines a continuous function on L/D

being constant of value $R(x_i)$ on each set Bx_iD/D. These sets form a disjoint covering of L/D. Therefore, if one denotes the left hand side of (4) by Γ, it follows from (3) that

$$\Gamma = \int_{L/D} R(x)\,\mathrm{d}\mu_1(xD) \quad (1 = \text{unit element of } D).$$

Denote by $M(s)$ any system of representatives for the cosets $gD(s)$ with $g \in D$. Then $R(x) = \sum_{s \in S} \sum_{g \in M(s)} f_s(xg)$ with the abbreviation $f_s(x) = f(xsx^{-1})$, and hence

$$\Gamma = \sum_{s \in S} J_s, \quad J_s = \int_{L/D} \left(\sum_{g \in M(s)} f_s(xg) \right) \mathrm{d}\mu_1(xD).$$

The substitution formula for integrals based on (2) shows that $J_s = I_s$, q.e.d.

4. Mass and Eichler–Brandt matrix

The finiteness of the class number $h(G)$ is evident from (1), Lemma 1 and the following lemma.

Lemma 3. (a) The group index $(U(G):U(M))$ is finite. (b) The group $k(\hat{U}(A))$ is locally compact, has a countable basis for its topology and $k(\hat{U}(G))$ as an open compact subgroup and $k(\hat{U}(A))$ as a discrete subgroup. The homogeneous space $k(\hat{U}(A))/k(U(A))$ is compact.

Proof. The group homomorphism $U(G) \to U(M)/(U(M))^2$, defined by $x \mapsto N(x)(U(M))^2$, has the kernel $U_1 U(M)$, where the set $U_1 = \{x \in G \mid N(x) = 1\}$ is finite, since A is totally definite. Hence $(U(G):U(M)) \leqslant |U_1|(U(M):(U(M))^2)$, where the last term is finite by the Dirichlet Unit Theorem. This proves (a). Since $\hat{U}(M)$ is a closed subgroup of $\hat{U}(A)$, the group $k(\hat{U}(A))$ is Hausdorff. Since $\hat{U}(A)$ is locally compact, has a countable basis and $\hat{U}(G)$ as an open compact subgroup, the corresponding images under k have the same properties. In order to prove that $k(U(A))$ is discrete, it suffices to show that its intersection with the open set $k(\hat{U}(G))$ is finite. This intersection equals $k(\hat{U}(G) \cap U(A)) = k(U(G)) \cong U(G)/(U(G) \cap \hat{U}(M)) = U(G)/U(M)$, and this is finite by (a). If G is a maximal M-order of A, then $h(G)$ is known to be finite [1], hence $k(\hat{U}(A))/k(U(A))$ is compact by (1) and Lemma 1, q.e.d.

Let $G_1, \ldots, G_h$ $(h = h(G))$ be any system of representatives for the classes of all invertible left ideals of G. Then the mass $m(G)$ of G is defined by

$$m(G) = \sum_{i=1}^{h} (U(G_i^{(r)}):U(M))^{-1}.$$

This is independent of the choice of the representatives G_i, as is clear e.g. by the following theorem.

Theorem 1. *One has*

$$m(G) = \frac{2D_F^{3/2} h_F \zeta_F(2)}{(2\pi)^{2n}} N_a(d_r(G)) \prod{}' \frac{1 - N_a(p)^{-2}}{1 - (G_p/p) N_a(p)^{-1}};$$

here D_F is the absolute discriminant, h_F the class number, n the degree, $\zeta_F(\ )$ the Dedekind zetafunction of the number field F, and $N_a(\ )$ means taking the absolute norm of ideals of M, and (G_p/p) is the Eichler symbol of the M_p-order G_p of A_p as defined in [7].

Proof. We have $G_i = Ga_i$ with $a_i \in \hat{U}(A)$, hence $G_i^{(r)} = a_i^{-1}Ga_i$. According to Lemma 3 we may apply (3) to the case $L = k(\hat{U}(A))$, $B = k(\hat{U}(G))$, $D = k(U(A))$. By (1) there is the disjoint union

$$L = \bigcup_{i=1}^{h} Bk(a_i)D, \tag{5}$$

hence from (3) it follows that $\mu_1(L/D) = \sum |k(a_i)^{-1}Bk(a_i) \cap D|^{-1}$.
Now

$$|k(a_i)^{-1}Bk(a_i) \cap D| = |k(\hat{U}(G_i^{(r)}) \cap U(A))| = |k(U(G_i^{(r)}))|$$
$$= (U(G_i^{(r)}): U(G_i^{(r)}) \cap \hat{U}(M)) = (U(G_i^{(r)}): U(M)),$$

hence $\mu_1(L/D) = m(G)$ with respect to the normalization $\mu(B) = 1$ of the Haar measure μ on L. Therefore, if G' is any maximal M-order of A containing G, we obtain $m(G) = m(G')(\hat{U}(G'): \hat{U}(G))$. Because of $(U(G'_p): U(G_p)) = 1$ for all $p \nmid d_r(G)$ this becomes $m(G) = m(G')\Pi'(U(G'_p): U(G_p))$. Inserting here the value of $m(G')$ obtained by Eichler [1] and the value of $(U(G'_p): U(G_p))$ derived in [8], we arrive immediately at the assertion of Theorem 1, q.e.d.

Let $G_1, \ldots, G_h$ be as before. Then $G_i^{-1}G_1, \ldots, G_i^{-1}G_h$ is a system of representatives for the classes of all invertible left ideals of $G_i^{(r)}$. Let J be any integral ideal of M and denote by $\pi_{ij}(J)$ the number of all integral invertible left ideals of $G_i^{(r)}$ that are in the same class as $G_i^{-1}G_j$ and whose norms equal J. Following [2] we define the Eichler–Brandt matrix $B(G, J)$ of G and J to be the matrix $(\pi_{ij}(J))$. Its trace $\sum \pi_{ii}(J)$ is denoted by $\operatorname{Tr} B(G, J)$, in particular it follows that $\operatorname{Tr} B(G, M) = h(G)$.

We denote by R any system of representatives in the multiplicative group $U^+(M)$ of all totally positive units of M for the cosets of the subgroup $(U(M))^2$. According to the Dirichlet Unit Theorem R is finite. For a fractional ideal I of M and $\beta \in U(F)$ we denote by $C(I, \beta)$ the finite set consisting of all $\alpha \in I$ with $\alpha^2 - 4\beta \notin F_p^2$ for all $p \in P_0$. For each $\alpha \in C(I, \beta)$ we fix any algebraic number $x = x(\alpha, \beta)$ satisfying $x^2 - \alpha x + \beta = 0$. Then our result on the trace of Eichler–Brandt matrices is as follows.

Theorem 2. *Let J be any integral ideal of M. If* $\operatorname{Tr} B(G, J) \neq 0$, *then* $J = \beta M$ *for some totally positive* $\beta \in M$ *and*

$$\operatorname{Tr} B(G, J) = \delta_\beta m(G) + \sum_{\varepsilon, \alpha, \Omega} E_G(\Omega) \frac{h(\Omega)}{2(U(\Omega): U(M))}.$$

Here $\delta_\beta = 1$ *or* 0 *according as J is the square of a principal ideal of M or not. The conditions for summation are:* $\varepsilon \in R$, $\alpha \in C(M, \varepsilon\beta)$, *and the sum is over the finitely many M-orders* Ω *of the quadratic field extension* $F[x]$ *of F satisfying* $x = x(\alpha, \varepsilon\beta) \in \Omega$. *There* $h(\Omega)$ *is the class number of* Ω *and* $E_G(\Omega) = \Pi' E(\Omega_p, G_p)$, *and* $E(\Omega_p, G_p)$ *is the number of the classes of all optimal embeddings* $\Omega_p \to G_p$.

For numerical applications of Theorem 2 it remains to compute the embedding numbers $E(\Omega_p, G_p)$. For orders G of special type this has essentially been done by Eichler [2], Hijikata [5] and Pizer [12]. Before proving Theorem 2 we have to say something on the definition and general properties of the embedding numbers. Let K be any quadratic field extension of F and Ω be an M-order of K. We fix any $p \in P$. Then Ω_p is an M_p-order of the separable F_p-algebra K_p. An optimal embedding $\psi: \Omega_p \to G_p$ is by definition an F_p-algebra monomorphism $\psi: K_p \to A_p$ such that $G_p \cap \psi(K_p) = \psi(\Omega_p)$. We say that two optimal embeddings $\psi, \psi': \Omega_p \to G_p$ are in the same class, if there exists an element u of $U(G_p)$ with $\psi' = \tau_u \psi$, where τ_u denotes the inner automorphism $x \mapsto uxu^{-1}$ of A_p. We denote by $[\psi]$ the class of an optimal embedding ψ. The embedding number $E(\Omega_p, G_p)$ turns out to be finite by the next lemma (which is a slight generalization of results in [5]). In order to prove the finiteness one may assume that K_p is a subalgebra of the F_p-algebra A_p. Under this assumption one has

Lemma 4. (*a*) *An one-to-one correspondence between the classes of all optimal embeddings $\Omega_p \to G_p$ and the double cosets $U(G_p)aU(K_p)$ with $a \in U(A_p)$ and $a^{-1}G_p a \cap K_p = \Omega_p$ is given by the assignment $U(G_p)aU(K_p) \mapsto [\psi_a]$, where ψ_a denotes the restriction of the inner automorphism τ_a of A_p to K_p.* (*b*) *The number $E(\Omega_p, G_p)$ is finite. It equals* 1, *if $p \nmid d_r(G)$.*

Proof. Since every F_p-algebra monomorphism $K_p \to A_p$ can be extended to an inner automorphism of A_p by the Skolem–Noether Theorem [14], the assignment described above produces the classes of all optimal embeddings $\Omega_p \to G_p$. The assignment is also injective, since $[\psi_a] = [\psi_b]$ implies that $\psi_a = \tau_u \psi_b$ for some $u \in U(G_p)$, hence $a^{-1}ub$ commutes with all elements of K_p and therefore lies in $U(K_p)$ by Lemma 5 (s. below). This proves (a). Replacing G in the double cosets by any maximal M-order G' of A containing G shows that

$$E(\Omega_p, G_p) \leqslant (U(G'_p): U(G_p)) \sum E(\Omega', G'_p), \tag{6}$$

where the sum is over all M_p-orders Ω' of K_p containing Ω_p. The number of these Ω' is finite, because Ω' is determined by its conductor which divides the conductor of Ω_p. If $p \nmid d_r(G)$, then $E(\Omega_p, G_p) = 1$ by [5], Corollary 2.6. It remains to consider the case $p \mid d_r(G')$. Here it is known [2] that $(U(A_p): U(F_p)U(G'_p)) = 2$, hence $E(\Omega', G'_p) \leqslant 2$ by part (a), hence $E(\Omega_p, G_p)$ is finite by (6), q.e.d.

The following lemma is well known (for part (b) s.e.g. [11], Lemma 8).

Lemma 5. Let A_0 be a quaternion algebra over a field F_0 (the centre of A_0) of characteristic $\neq 2$ and let $x \in A_0$, $\alpha \in F_0$, $\alpha \neq 1$.
(*a*) *if $x \notin F_0$, then the centralizer of x in A_0 is $F_0[x]$.*
(*b*) *If $x \in U(A_0)$, then there exists an element y of $U(A_0)$ such that $yxy^{-1} = \alpha x$ if and only if $\alpha = -1$ and $T(x) = 0$.*

Proof of Theorem 2. We use all notations of the proof of Theorem 1. By definition $\pi_{ii}(J)$ equals the number of all sets $G_i^{(r)}x$ with $x \in G_i^{(r)}$ and $N(x)M = J$. We suppose that $\operatorname{Tr} B(G, J) \neq 0$. Then $J = \beta M$ for some totally positive $\beta \in M$. On L we define a function f as follows. Let $y \in \hat{U}(A)$. Put $f(k(y)) = 1$, if $y_p \in G_p$ and $N(y_p)M_p = J_p$ for all $p \in P$.

Otherwise put $f(k(y))=0$. By Lemma 2 and (5), equation (4) holds for f with $x_i=k(a_i)$. Because of $G_i^{(r)}=a_i^{-1}Ga_i$ the term $R(x_i)$ equals the number of all cosets $x\hat{U}(M)$ with $x\in G_i^{(r)}$ and $N(x)M=J$, hence $R(x_i)=(U(G_i^{(r)}):U(M))\pi_{ii}(J)$. On the other hand $(U(G_i^{(r)}):U(M))=|x_i^{-1}Bx_i\cap D|$ by the proof of Theorem 1. Therefore $\operatorname{Tr} B(G,J)$ equals the left hand side of (4). It remains to evaluate the integrals I_s on the right hand side of (4) and to describe the set S. We write $s=k(x)$ for some $x\in U(A)$ and distinguish the following two cases.

Case 1: $x\in U(F)$.
Here $I_s=f(s)\mu_1(L/D)$. Since $\mu_1(L/D)=m(G)$ by the proof of Theorem 1, we obtain $I_s=m(G)$ or 0, according as $x^2M=J$ or not.

Case 2: $x\notin U(F)$.
We put $K=F[x]$ and $D'(s)=k(U(K))$. By Lemma 5 the group index $t_s=(D(s):D'(s))$ satisfies $t_s=2$ or 1, according as $T(x)=0$ or not. It follows that

$$I_s=t_s^{-1}I_s',\quad I_s'=\int_{L/D'(s)} f(ysy^{-1})\,\mathrm{d}\mu_s'(yD'(s)),\tag{7}$$

where μ_s' is the L-left invariant quotient measure of μ on the compact homogeneous space $L/D'(s)$ normalized by the condition $\mu_s'(L/D'(s))=t_s\mu_s(L/D(s))$. The integral I_s' is non-zero, if and only if $N(x)M=J$ and $x\in y_0^{-1}Gy_0$ for some $y_0\in\hat{U}(A)$, in particular

$$x^2-\alpha x+\varepsilon\beta=0\tag{8}$$

for some $\alpha\in M$ and $\varepsilon\in U^+(M)$ with $\alpha^2-4\varepsilon\beta\notin F_p^2$ for all $p\in P_0$, since K_p is a subfield of A_p for all $p\in P_0$. Under the condition (8) we have $I_s'=\mu_s'(\cup W(y))$, where $W(y)=Bk(y\hat{U}(K))/D'(s)$ and the union $\cup$ is over all $y\in\hat{U}(A)$ with $x\in y^{-1}Gy$. Different sets of $W(y)$ are disjoint because of $D'(s)\subset k(\hat{U}(K))$. The condition $x\in y^{-1}Gy$ implies that $\Omega=y^{-1}Gy\cap K$ is an M-order of K containing x. If Ω is kept fixed, we denote by $W(y_j)$ $(j=1,\ldots,E(\Omega))$ the different sets among the $W(y)$ with $y^{-1}Gy\cap K=\Omega$. Then $E(\Omega)$ is the number of double cosets $\hat{U}(G)z\hat{U}(K)$ with $z\in\hat{U}(A)$ and $z_p^{-1}G_pz_p\cap K_p=\Omega_p$ for all $p\in P$. By Lemma 4 it follows that $E(\Omega)=E_G(\Omega)$. Denote by $G^{(j)}$ the M-order $y_j^{-1}Gy_j$ of A. Then $\mu_s'(W(y_j))=\mu_s'(k(\hat{U}(G^{(j)})\hat{U}(K))/D'(s))$ by the left invariance of μ_s', hence

$$I_s'=\sum_{\Omega,j}\mu_s'(k(\hat{U}(G^{(j)})\hat{U}(K))/D'(s)),$$

where the sum is over all M-orders Ω of K containing x and over $j=1,\ldots,E_G(\Omega)$. Since $h(\Omega)=(\hat{U}(K):\hat{U}(\Omega)U(K))$ by (1), we have for each Ω the disjoint union

$$\hat{U}(K)=\bigcup_\rho \hat{U}(\Omega)U(K)\beta_\rho$$

for some $\beta_\rho\in\hat{U}(K)$, where $\rho=1,\ldots,h(\Omega)$, hence

$$\hat{U}(G^{(j)})\hat{U}(K)=\bigcup_\rho \hat{U}(G^{(j)})U(K)\beta_\rho.\tag{9}$$

This union is also disjoint, since $\beta_\sigma\in\hat{U}(G^{(j)})U(K)\beta_\rho$ implies $\beta_\sigma\beta_\rho^{-1}\in(U(G^{(j)})\cap\hat{U}(K))U(K)=$

$\hat{U}(\Omega)U(K)$. Because of $D'(s)=k(U(K))$ the application of the canonical map $\hat{U}(A)\to L/D'(s)$ to (9) yields again a disjoint union, hence

$$I'_s=\sum_{\Omega,j,\rho}\mu'_s(k(\hat{U}(G^{(j)})\beta_\rho)D'(s)/D'(s)), \tag{10}$$

where the conditions of summation for Ω, j, ρ are as before. We denote by $G^{(j,\rho)}$ the M-order $\beta_\rho^{-1}G^{(j)}\beta_\rho$ of A and put $B_{j\rho}=k(\hat{U}(G^{(j,\rho)}))$. Then $\mu(B_{j\rho})=\mu(B)=1$, since μ is left and right invariant. The left invariance of μ'_s implies $\mu'_s(k(\hat{U}(G^{(j)})\beta_\rho)D'(s)/D'(s))=\mu'_s(B_{j\rho}D'(s)/D'(s))$, and this equals $|B_{j\rho}\cap D'(s)|^{-1}$ by the analogue of (3) and because of $\mu(\beta_{j\rho})=1$. Furthermore $|B_{j\rho}\cap D'(s)|=|k(\hat{U}(G^{(j,\rho)})\cap U(K))|=|k(\hat{U}(G^{(j)})\cap U(K))|=|k(U(\Omega))|=(U(\Omega):U(M))$. Therefore it follows from (10) and (7) that

$$I_s=t_s^{-1}\sum_{\Omega}E_G(\Omega)h(\Omega)/(U(\Omega):U(M)), \tag{11}$$

where the sum is over all M-orders Ω of $F[x]$ containing x. Note that any quadratic field extension $F[y]$ of F, where y is any root of equation (8), can be embedded as F-algebra in the F-algebra A (s. [14], page 78). Therefore (11) remains valid, if x is replaced by such y. Now we describe a system S (as needed in (4)) of representatives for the conjugacy classes in D. In Case 1 different elements s represent different conjugacy classes. Consequently the contribution of Case 1 to $\mathrm{Tr}\,B(G,J)$ is $\delta_\beta m(G)$. In Case 2 elements $s=k(x)$, $s'=k(x')$ with $x,x'\in U(A)-U(F)$ represent the same conjugacy class if and only if ηx and x' are conjugate in $U(A)$ for some $\eta\in U(M)$. By the Skolem–Noether Theorem [14] this amounts to the conditions $T(\eta x)=T(x')$, $N(\eta x)=N(x')$. Therefore in Case 2 we may restrict ourselves to elements s of the form $s=k(x)$ with $T(x)=\alpha$, $N(x)=\varepsilon\beta$, $\varepsilon\in R$, $\alpha\in C(M,\varepsilon\beta)$. Then two elements $s=k(x)$, $s'=k(x')$ of this form are conjugate in D, if and only if $\varepsilon=\varepsilon'$, $\alpha=\pm\alpha'$, i.e. each conjugacy class is represented twice, except in the case $T(x)=0$, there only once. This and (11) show that Theorem 2 is true.

5. The type number

Two M-orders G, G' of A are said to be in the same genus, if G_p and G'_p are isomorphic as M_p-algebras for all $p\in P$. The orders G, G' are said to be in the same isomorphism class, if they are isomorphic as M-algebras. The type number $t(G)$ of G is defined as the number of all isomorphism classes in the genus of G. Let $\Gamma(G)$ be the normalizer of G in $U(A)$, i.e. the subgroup $\{x\in U(A)\,|\,xGx^{-1}=G\}$ of $U(A)$. Then the normalizer $\hat{\Gamma}(G)$ of G in $\hat{U}(A)$ equals $\hat{U}(A)\cap\Pi\Gamma(G_p)$, where $\Gamma(G_p)$ denotes the normalizer of G_p in $U(A_p)$. Since any isomorphism $G_p\cong G'_p$ or $G\cong G'$ can be extended to an inner automorphism of the corresponding quaternion algebra by the Skolem–Noether Theorem [14], the group $\hat{U}(A)$ acts via conjugation transitively on the genus of G and the group $U(A)$ acts via conjugation transitively on the isomorphism class of G, hence

$$t(G)=|\hat{\Gamma}(G)\backslash\hat{U}(A)/U(A)|. \tag{12}$$

From this and (1) it follows that $t(G)\leqslant h(G)$; in particular $t(G)$ is finite. For the sequel we shall need the group index $q:=(\hat{\Gamma}(G):\hat{U}(F)\hat{U}(G))$. Note that $(\Gamma(G_p):U(F_p)U(G_p))$ is the cardinality of the central Picard group of G_p (s. [8]) and therefore finite [4] for all $p \in P$ and equal to 1 for $p \nmid d_r(G)$ (s. [2]). This implies

$$q = \Pi'(\Gamma(G_p): U(F_p)U(G_p)). \tag{13}$$

Since the factors of this product have been computed in [8], the index q is explicitly known. Furthermore we shall need the set $\nu(G)$ as defined in the second section. The Local–Global principle shows that $\nu(G)$ is the set of all integral ideals J of M such that $J_p \in \nu(G_p)$ for all $p \in P$. Each set $\nu(G_p)$ is finite and explicitly known [8]. Since $\nu(G_p) = \{M_p\}$ for $p \nmid d_r(G)$, the set $\nu(G)$ is also finite and known. With the same notations as in Theorem 2 we state

Theorem 3. *For any M-order G of A one has*

$$qh_F t(G) = m(G) + \sum_{\varepsilon, I, J} \sum_{\alpha, \Omega} E'_G(\Omega) \frac{h(\Omega)}{2(U(\Omega): U(M))}.$$

The sum is over all $\varepsilon \in R$, over all fractional ideals I of M in an arbitrarily fixed system of representatives for the ideal classes of M and over all integral ideals J of M satisfying $J \in \nu(G)$ and $I^2 J = \beta M$ for at least one totally positive $\beta \in F$. Having fixed such β for each J, one takes the second sum over all $\alpha \in C(I, \varepsilon\beta)$ and over all M-orders Ω of $F[x]$ with $x = x(\alpha, \varepsilon\beta)$ and $x \in I\Omega - pI\Omega$ for all $p \in P$. Here q is obtained by (13) *and $E'_G(\Omega) = \Pi' E'(\Omega_p, G_p)$, where $E'(\Omega_p, G_p)$ denotes the number of classes of all optimal embeddings $\psi: \Omega_p \to G_p$ satisfying $\psi(x)G_p = G_p\psi(x)$.*

For numerical applications of Theorem 3 it remains to compute the restricted embedding numbers $E'(\Omega_p, G_p)$. For special orders G this can be achieved by using results of [5], [10], [11], [12].

Proof of Theorem 3. Again we use all notations of the proof of Theorem 1. The group $\hat{U}(A)$ is the union of the double cosets $\hat{\Gamma}(G)a_i U(A)$. Such a double coset is the disjoint union of finitely many, say t_i, double cosets of the form $\hat{U}(G)ca_i U(A)$ with $c \in \hat{\Gamma}(G)$. Since $a_i^{-1}Ga_i = G_i^{(r)}$ and $\hat{U}(G)$ is a normal subgroup of $\hat{\Gamma}(G)$, we obtain for c the condition $a_i^{-1}ca_i\hat{U}(G_i^{(r)})U(A) \subset \hat{\Gamma}(G_i^{(r)})U(A)$, hence $t_i = (\hat{\Gamma}(G_i^{(r)})U(A): \hat{U}(G_i^{(r)})U(A))$, and this term we denote by $g(G_i^{(r)})$. Since $\hat{U}(A)$ is the disjoint union of the double cosets $\hat{U}(G)a_i U(A)$, we see from (12) that

$$t(G) = \sum_{i=1}^{h} (g(G_i^{(r)}))^{-1},$$

where

$$g(G) = (\hat{\Gamma}(G): \hat{\Gamma}(G) \cap \hat{U}(G)U(A)) = (\hat{\Gamma}(G): \hat{U}(G)\Gamma(G))$$

$$= \frac{q(\hat{U}(F)\hat{U}(G): U(F)\hat{U}(G))}{(\hat{U}(G)\Gamma(G): U(F)\hat{U}(G))} = \frac{q(\hat{U}(F): \hat{U}(F) \cap U(F)\hat{U}(G))}{(\Gamma(G): \Gamma(G) \cap U(F)\hat{U}(G))}$$

$$= \frac{q(\hat{U}(F): U(F)\hat{U}(M))}{(\Gamma(G): U(F)U(G))} = \frac{qh_F}{(\Gamma(G): U(F)U(G))},$$

hence

$$qh_F t(G) = \sum_{i=1}^{h} (\Gamma(G_i^{(r)}): U(F)U(G_i^{(r)})). \tag{14}$$

We fix any system $\{C_\rho | \rho = 1, \ldots, h_F\}$ of representatives for the ideal classes of M. In particular we have $C_\rho = \gamma_\rho M$ for some $\gamma_\rho \in \hat{U}(F)$. For $x \in \Gamma(G)$ the set Gx is a two-sided ideal of G, hence $Gx = \alpha C_\rho \Lambda$ with $\alpha \in U(F)$, some primitive two-sided ideal Λ of G and some ρ. The pair ρ, Λ is uniquely determined by the coset $xU(F)U(G)$, and conversely. Therefore

$$(\Gamma(G): U(F)U(G)) = \sum_\rho \sigma_\rho(G),$$

where $\sigma_\rho(G)$ denotes the number of all sets of the form $Gx = C_\rho \Lambda$ with $x \in U(A)$ and a primitive two sided ideal Λ of G; in particular $N(x)M = C_\rho^2 J$ for some $J \in \nu(G)$. We denote by $\hat{\Gamma}_0(G)$ the set of all $y \in \hat{\Gamma}(G)$ satisfying $y_p \in G_p - pG_p$ for all $p \in P$. Then $\{Gy | y \in \hat{\Gamma}_0(G)\}$ is the set of all primitive two-sided ideals of G. Therefore from (14) it follows that

$$qh_F t(G) = \sum_{\rho, J} S_\rho(J), \tag{15}$$

where the sum is over $\rho = 1, \ldots, h_F$ and over all $J \in \nu(G)$ and where

$$S_\rho(J) = \sum_{i=1}^{h} q_i(\rho, J)$$

and $q_i(\rho, J)$ denotes the number of all sets $G_i^{(r)}x$ with $x \in U(A) \cap \gamma_\rho \hat{\Gamma}_0(G_i^{(r)})$ and $N(x)M = C_\rho^2 J$. Now for any fixed ρ we compute the sum $S_\rho(J)$ by the method that we used for the evaluation of $\operatorname{Tr} B(G, J)$ in the proof of Theorem 2. For this we define a function f on L as follows. Let $y \in \hat{U}(A)$. Put $f(k(y)) = 1$, if $y \in \gamma_\rho \hat{\Gamma}_0(G)$ and $N(y_p)M_p = C_{\rho p}^2 J_p$ for all $p \in P$. Otherwise put $f(k(y)) = 0$. By Lemma 2 and (5), equation (4) holds for f with $x_i = k(a_i)$. As in the proof of Theorem 2 it follows that $S_\rho(J)$ equals the left hand side of (4). We suppose that $S_\rho(J) \neq 0$. Then there exists a totally positive $\beta \in F$ with $C_\rho^2 J = \beta M$. For computation of the integrals I_s on the right hand side of (4) we write $s = k(x)$ with $x \in U(A)$ and distinguish two cases.

Case 1: $x \in U(F)$.
As in the proof of Theorem 2 we conclude that $I_s = m(G)$ or 0, according as $C_\rho = Mx$ and $J = M$ or not.

Case 2: $x \notin U(F)$.
We put $K = F[x]$ and $D'(s) = k(U(K))$ and obtain as in the proof of Theorem 2 equation (7), and in the case $I'_s \neq 0$ also equation (8), but now with the conditions

$$\varepsilon \in U^+(M), \quad \alpha \in C(C_\rho, \varepsilon\beta). \tag{16}$$

Under the conditions (8) and (16) we have $I'_s = \mu'_s(\cup W(y))$, where $W(y) = Bk(y\hat{U}(K))/D'(s)$ and the union $\cup$ is over all $y \in \hat{U}(A)$ with $x \in \hat{\Gamma}(y^{-1}Gy)$ and

$$x \in C_\rho \Omega - pC_\rho \Omega \quad \text{for all} \quad p \in P. \tag{17}$$

Here Ω denotes the M-order $y^{-1}Gy \cap K$ of the F-algebra K. If Ω is kept fixed and x satisfies (8), (16) and (17), we denote by $W(y_j)$ $(j = 1, \ldots, E'(\Omega))$ the different sets $W(y)$

with $y \in \hat{U}(A)$, $y^{-1}Gy \cap K = \Omega$ and $yxy^{-1} \in \hat{\Gamma}(G)$. Then we have $E'(\Omega) = \Pi E'(\Omega_p, G_p)$ by Lemma 4. For $p \nmid d_r(G)$ the element $z_p = \gamma_{pp}^{-1}x$ of $y_p^{-1}G_py_p$ satisfies $N(z_p)M_p = J_p = M_p$, hence $z_p \in U(y_p^{-1}G_py_p)$, hence $x \in \Gamma(y_p^{-1}G_py_p)$, hence $E'(\Omega_p, G_p) = E(\Omega_p, G_p) = 1$ by Lemma 4. Therefore $E'(\Omega) = E'_G(\Omega)$. It is clear that from here on the evaluation of I_s and the construction of the system S can be carried out as in the proof of Theorem 2. This way we obtain for $S_\rho(J)$ an expression analogous to that for $\mathrm{Tr}\, B(G, J)$ in Theorem 2. Inserting this in (15) completes the proof of Theorem 3.

References

[1] Eichler M, Über die Klassenzahl total definiter Quaternionenalgebren, *Math. Z.* **43** (1937) 102–109

[2] Eichler M, Zur Zahlentheorie der Quaternionen algebren, *J. reine angew. Math.* **195** (1955) 127–151

[3] Eichler M, Quadratische Formen und orthogonale Gruppen 1974 2nd edn (Berlin: Springer Verlag)

[4] Fröhlich A, The Picard group of non-commutative rings, in particular of orders, *Trans. Am. Math. Soc.* **180** (1973) 1–45

[5] Hijikata H, Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$, *J. Math. Soc. Jpn.* **26** (1974) 56–82

[6] Kaplansky I, Submodules of quaternion algebras, *Proc. London Math. Soc.* (3) **19** (1969) 219–232

[7] Körner O, Ordnungen von Quaternionenalgebren über lokalen Körpern, *J. reine angew. Math.* **333** (1982) 162–178

[8] Körner O, Über die zentrale Picard-Gruppe und die Einheiten lokaler Quaternionenordnungen, *Manuscripta Math.* **52** (1985) 203–225

[9] O'Meara O T, Introduction to quadratic forms 1963 (Berlin: Springer-Verlag)

[10] Peters M, Ternäre und quaternäre quadratische Formen und Quaternionen algebren *Acta Arith.* **15** (1969) 329–365

[11] Pizer A, Type numbers of Eichler orders, *J. reine angew. Math.* **264** (1973) 76–102

[12] Pizer A, On the arithmetic of quaternion algebras, *Acta Arith.* **31** (1976) 61–89

[13] Tamagawa T, On Selberg's Trace Formula, *J. Fac. Sci. Univ. Tokyo, Sect. I* **8** (1960) 363–386

[14] Vignéras M F, Arithmétique des Algébres de Quaternions, *Lecture Notes in Mathematics* 800 (1980) (Berlin: Springer Verlag)