ACTA ARITHMETICA
140.4 (2009)

Arithmetical Hilbert symbols, distance maps and cohomology

by

Luis Arenas-Carmona (Santiago)

1. Introduction. Let k be a field of characteristic 0 containing the group μ_n of nth roots of unity, and let η be a generator of μ_n. The Hilbert symbol is a map that associates a central simple algebra $(a,b)_\eta$ of dimension n^2 to every element (a,b) in $k^* \times k^*$ [9]. It is defined as the k-algebra with generators x and y satisfying the relations

$$x^n = a, \quad y^n = b, \quad \text{and} \quad xy = \eta yx. \tag{1}$$

Up to isomorphism, the algebra $(a,b)_\eta$ depends only on the images of a and b in k^*/k^{*n}. This raises the question of whether there are any additional structures on the set of pairs (a,b) defining the same algebra. When k is a number field with ring of integers $\mathcal{O}_k$, we can study the order $\langle a,b\rangle_\eta = \mathcal{O}_k[x,y]$, where x and y still satisfy (1) for algebraic integers a and b in k. This is the natural integral version of the algebra $(a,b)_\eta$, so that we can think of it as a refinement of the Hilbert symbol map. Since the classification of maximal orders in a central simple algebra is better understood than the general case, it is desirable to replace the ring $\langle a,b\rangle_\eta$ by a related maximal order $\mathcal{D}(a,b)$ in $(a,b)_\eta$. This can be done by inverting a finite set R of primes and defining $\mathcal{D}(a,b)$ as an R-order. We need to assume that R contains both the set $P(n)$ of all places $\wp$ of k such that $\mathrm{ord}_\wp(n) \neq 0$, and the set $R(a,b)$ of all places $\wp$ such that n divides neither $\mathrm{ord}_\wp(a)$ nor $\mathrm{ord}_\wp(b)$. Then we set $\mathcal{D}(a,b) = \mathcal{O}[\mathcal{A}^{-1}x \cup \mathcal{B}^{-1}y]$, where $\mathcal{O} = \mathcal{O}_R$ is the ring of R-integers, and the ideals $\mathcal{A}$ and $\mathcal{B}$ are the nth roots of the principal R-ideals $a\mathcal{O}$ and $b\mathcal{O}$. These nth roots exist since $\mathrm{ord}_\wp(a)$ and $\mathrm{ord}_\wp(b)$ are divisible by n for all $\wp \notin R$. It is known that maximal R-orders in a central simple algebra can be classified into spinor genera [2] by a distance function that associates, to every pair

2010 *Mathematics Subject Classification*: 11R52, 11R34, 11E72, 11R56.
Key words and phrases: central simple algebras, maximal orders, arithmetical Hilbert symbols.

DOI: 10.4064/aa140-4-1

of maximal R-orders $\mathfrak{D}$ and $\mathfrak{D}'$, an ideal class $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ in some quotient of the strict R-ideal class group $\mathfrak{cl}_k(R)$ of k. In our case this quotient is

$$\mathfrak{T}_n(\mathfrak{A}) = \mathfrak{cl}_k(R)/\mathfrak{cl}_k(R)^n\mathfrak{p}(\mathfrak{A}),$$

where $\mathfrak{p}(\mathfrak{A})$ is the group of principal ideals with a generator that is positive at all infinite places that are ramified for $\mathfrak{A} = (a,b)_\eta$. The directed distance $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is defined as follows [1]:

> For every place $\wp \notin R$, choose an element $h_\wp \in \mathfrak{A}_\wp$ satisfying $\mathfrak{D}'_\wp = h_\wp \mathfrak{D}_\wp h_\wp^{-1}$. Since $\mathfrak{D}_\wp$ and $\mathfrak{D}'_\wp$ coincide at all but a finite number of places ([5, p. 218]), we can assume that $h_\wp = 1$ for all but a finite number of places $\wp$. Then $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is the class in $\mathfrak{T}_n(\mathfrak{A})$ of the ideal $\prod_\wp \wp^{v_\wp}$, where the completion at $\wp$ of $\wp^{v_\wp}$ is the principal ideal generated by the reduced norm $N(h_\wp)$.

The orders $\mathfrak{D}$ and $\mathfrak{D}'$ are in the same spinor genus if and only if $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is the trivial class [2]. If $n > 2$, or if the Eichler condition is satisfied ([1]), the orders $\mathfrak{D}$ and $\mathfrak{D}'$ are conjugate (or isomorphic) if and only if they are in the same spinor genus.

For the case $n = 2$, the distance map $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ can be defined as follows: If $\mathfrak{D}/(\mathfrak{D}\cap\mathfrak{D}')$ is isomorphic to a sum of cyclic $\mathcal{O}$-modules $\mathcal{O}/\mathcal{I}_1 \oplus \cdots \oplus \mathcal{O}/\mathcal{I}_m$, then $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is the class of the product ideal $\mathcal{I}_1 \cdots \mathcal{I}_m$ in $\mathfrak{T}_2(\mathfrak{A})$. This is the definition used by Chinburg and Friedman [3] to compute the invariant $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$. In Proposition 3.4 we prove that both definitions coincide for $n = 2$. The latter definition fails to be conjugation invariant for general n.

Let $n = 2$ as above, whence $\eta = -1$. Assume that we have two pairs (a,b) and (c,d) such that $(a,b)_\eta = (c,d)_\eta = \mathfrak{A}$. Assume further that R contains $P(n) \cup R(a,b) \cup R(c,d)$, so that $\mathfrak{D} = \mathcal{D}(a,b)$ and $\mathfrak{D}' = \mathcal{D}(c,d)$ are two maximal R-orders in the central simple algebra $\mathfrak{A}$. In this setting, Chinburg and Friedman [3] asked whether the ideal class $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ can be computed in terms of the arithmetic of some finite extension K/k depending only on a, b, c, and d. They could only perform this computation when $a = c$. Their results are as follows:

> Let $\mathcal{B}$ be a fractional R-ideal in k such that $\mathcal{B}^2 = (b/d)\mathcal{O}$, as must exist due to the restrictions on R.
>
> (A) If a is a perfect square in k then $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is the class of $\mathcal{B}$.

([1]) The *Eichler condition* is satisfied if the completion $\mathfrak{A}_\rho$ is not $\mathbb{H}$, the non-trivial quaternion $\mathbb{R}$-algebra, at some infinite place ρ ([8, p. 81]). This holds in particular when k is not totally real.

(B) If a is not a perfect square, then $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is computed as follows: Let $R(F)$ be the set of places of $F=k(\sqrt{a})$ lying over the elements of R. Let $\mathcal{O}_F$ be the ring of $R(F)$-integers in F, and let $\mathcal{B}_F$ be the fractional $R(F)$-ideal in $\mathcal{O}_F$ generated by the elements of $\mathcal{B}$. Let $\tau\in F$ be such that $N_{F/k}(\tau)=b/d$. Then there exists a fractional $R(F)$-ideal $\mathcal{C}$ in F satisfying $\mathcal{C}\sigma(\mathcal{C})^{-1}=\tau^{-1}\mathcal{B}_F$, where σ is the non-trivial k-automorphism of F. For any such $\mathcal{C}$, the distance $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is the class of $N_{F/k}(\mathcal{C})$.

In this work, we generalize (A) and (B) to the case $n>2$. Assume, as in the case $n=2$, that the pairs (a,b) and (c,d) satisfy the conditions $(a,b)_\eta=(c,d)_\eta=\mathfrak{A}$ and $R\supseteq P(n)\cup R(a,b)\cup R(c,d)$, so that $\mathfrak{D}=\mathcal{D}(a,b)$ and $\mathfrak{D}'=\mathcal{D}(c,d)$ are maximal. Let $\mathcal{B}$ be an ideal satisfying $\mathcal{B}^n=(b/d)$. Let $F=k(\sqrt[n]{a})$. The field F is independent of the choice of $\sqrt[n]{a}$ since k contains the n-roots of unity. For the case $a=c$, we prove the following:

(A′) If $F=k$, i.e., if a is an nth power in k, then $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is trivial if n is odd, and is the class of $\mathcal{B}^{n/2}$ otherwise.

(B′) If $[F:k]=n$, and we let $\sigma\in\mathrm{Gal}(F/k)$ be defined by $\sigma(\sqrt[n]{a})=\eta\sqrt[n]{a}$, then $\mathfrak{P}_R(\mathfrak{D},\mathfrak{D}')$ is the class of $N_{F/k}(\mathcal{C})$, where $\mathcal{C}\sigma(\mathcal{C})^{-1}=\tau^{-1}\mathcal{B}_F$ and $N_{F/k}(\tau)=b/d$, in the notations of (B). Furthermore, any τ and $\mathcal{C}$ satisfying these conditions can be used in this computation.

In particular, all orders of the form $D(1,b)$ are conjugate if n is odd. If n is even, and if $\wp$ is a prime ideal whose order is exactly n in the class group, then the generator b of $\wp^n$ defines an order $D(1,b)$ not isomorphic to $D(1,1)$. If $x\in\mathfrak{A}$ is as in (1), the field F is isomorphic to a quotient of the n-dimensional algebra $k[x]$. In particular, $[F:k]=n$ if and only if $k[x]$ is a field. For example, if $\mathfrak{A}$ is a division algebra then $[F:k]=n$.

We prove in §4 that (A′) and (B′) are particular cases of Theorem 1 below. For this general statement, we need some additional notations. Set $L=k[x]=\bigoplus_{i=1}^m L_i$, where every L_i is a field. Note that every L_i is generated over k by an nth root of a, whence is isomorphic to $F=k(\sqrt[n]{a})$. No assumption is made on the degree $[F:k]$ or equivalently, on the number $m=n/[F:k]$. If N denotes the reduced norm on $\mathfrak{A}$, then for any element $l\in L$ we have $N(l)=\prod_{i=1}^m N_{L_i/k}(l_i)$, where $l_i\in L_i$ for all i and $l=l_1+\cdots+l_m$. We identify L with the subset $L\otimes_k k$ of $L_F=L\otimes_k F$. There exists a unique isomorphism $\psi:L_F\to F^n$ such that $\psi(x)=(\sqrt[n]{a},\eta\sqrt[n]{a},\dots,\eta^{n-1}\sqrt[n]{a})$. If $\mathcal{I}$ is a fractional R-ideal in L, we denote by $N_{L/k}(\mathcal{I})$ the fractional R-ideal in k generated by the norms of the elements of $\mathcal{I}$, and by $\mathcal{I}_F$ the fractional $R(F)$-ideal in the F-algebra L_F generated by $\mathcal{I}$. Let $\Gamma:\mathrm{Gal}(F/k)\to\mathbb{Z}/n\mathbb{Z}$ be the Kummer homomorphism defined by $\lambda(\sqrt[n]{a})=\eta^{\Gamma(\lambda)}\sqrt[n]{a}$.

THEOREM 1. *Let $\mathfrak{D} = D(a,b)$ and $\mathfrak{D}' = D(a,d)$, where $(a,b)_\eta = (a,d)_\eta = \mathfrak{A}$ and $R \supseteq P(n) \cup R(a,b) \cup R(a,d)$. Then there exist elements $\tau_1, \dots, \tau_n$ in F such that $\prod_{i=1}^n \tau_i = b/d$ and $\lambda(\tau_i) = \tau_{i+\Gamma(\lambda)}$ for any $\lambda \in \mathrm{Gal}(F/k)$. For any such elements $\tau_1, \dots, \tau_n$, there exist fractional R-ideals $\mathcal{C}_1, \dots, \mathcal{C}_n$ in F such that $\mathcal{C}_i \mathcal{C}_{i+1}^{-1} = \tau_i \mathcal{B}_F$ and $\mathcal{C}_1 \times \cdots \times \mathcal{C}_n = \psi(\mathcal{I}_F)$ for some fractional R-ideal $\mathcal{I}$ in L. For any such $\mathcal{I}$ the class of $N_{L/k}(\mathcal{I})$ equals $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$.*

One of the main results of this paper states that the map $\mathfrak{P}_R$ can be defined alternatively using Galois extensions instead of adelizations. This is made precise by Theorem 2.

THEOREM 2. *Let $\mathfrak{D} = D(a,b)$, where $(a,b)_\eta = \mathfrak{A}$, and let R be a finite set of places satisfying $R \supseteq P(n) \cup R(a,b)$. Let $\mathfrak{D}'$ be an arbitrary maximal R-order in $\mathfrak{A}$. Then there exist a finite extension K/k and an element $g \in \mathfrak{A}_K$ satisfying the following conditions*:

(a) *The extensions of $\mathfrak{D}$ and $\mathfrak{D}'$ to $\mathcal{O}_K$ satisfy $\mathfrak{D}'_K = g\mathfrak{D}_K g^{-1}$.*
(b) *There exists an R-lattice Λ in $\mathfrak{A}$ such that $\mathfrak{D}_K g^{-1} = \Lambda_K$.*

For any such g, there exists a fractional R-ideal $\mathcal{I}$ in k whose extension $\mathcal{I}_K$ is the principal fractional $R(K)$-ideal $N(g)\mathcal{O}_K$ of K, where N is the reduced norm on $\mathfrak{A}_K$. The distance $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$ is the ideal class of $\mathcal{I}$.

It seems to us that Theorem 1 looks more natural as a diagonalized version of Theorem 2.

2. Non-abelian cohomology and classification. Let $\mathcal{G}$ be a finite group. Let X be a set with a $\mathcal{G}$-action and let B be a group with a $\mathcal{G}$-action. Let $x \mapsto {}^\sigma x$ denote the $\mathcal{G}$-action on X or B ([6, §1.3.2]). Assume B acts transitively on X in a way that ${}^\sigma b({}^\sigma x) = {}^\sigma[b(x)]$ for all σ in $\mathcal{G}$, all b in B, and all x in X. Then we can identify X, as a $\mathcal{G}$-set, with the quotient set B/A, where the $\mathcal{G}$-invariant subgroup A is the stabilizer in B of a point $x_0 \in X$. This identification depends on the choice of the base point x_0. Recall that in non-abelian cohomology, the set $H^1(\mathcal{G}, B)$ is defined as the pointed set of cohomology classes of maps $\sigma \mapsto \alpha_\sigma$ from $\mathcal{G}$ to B such that $\alpha_{\lambda\sigma} = \alpha_\lambda {}^\lambda\alpha_\sigma$ for any σ and λ in $\mathcal{G}$. Two such maps α and β are cohomologous if there exists $b \in B$ such that $\alpha_\sigma = b\beta_\sigma {}^\sigma b^{-1}$ for all $\sigma \in \mathcal{G}$. The distinguished element of the pointed set $H^1(\mathcal{G}, B)$ is the class of the trivial map. Recall that the kernel of a map $P \to P'$ of pointed sets is the inverse image of the distinguished element in P'. The subgroup $B^{\mathcal{G}}$ of invariant elements of B acts on the invariant set $X^{\mathcal{G}}$. The orbits of this action can be described as follows ([6, p. 22]):

PROPOSITION 2.1 (Classification Principle). *Let B act transitively on X. Let A be the stabilizer of the element $x_0 \in X^{\mathcal{G}}$. Assume that ${}^\sigma b({}^\sigma x) = {}^\sigma[b(x)]$ for all σ in $\mathcal{G}$, all b in B, and all x in X. Then the set of $B^{\mathcal{G}}$-orbits in $X^{\mathcal{G}}$*

can be identified with the kernel of the map $H^1(\mathcal{G}, A) \to H^1(\mathcal{G}, B)$ *induced by the inclusion. The cocycle class corresponding to some element* $b(x_0) \in X^{\mathcal{G}}$ *is the class of the cocycle* α *defined by* $\alpha_\sigma = b^{-1}\,{}^\sigma b$. ∎

In all that follows, $\mathcal{G} = \mathrm{Gal}(K/k)$ is the Galois group of a finite Galois extension K/k of either local or number fields. The set $H^1(\mathcal{G}, A)$ is denoted $H^1(K/k, A)$, or $H^1(A)$ if K and k are clear from the context.

Let X_k be a linear algebraic group, i.e., a subgroup of the general linear group $GL(n, k)$ defined by algebraic equations over k. For an arbitrary field extension E/k we denote by X_E the subgroup of $GL(n, E)$ defined by the same set of equations. The group X_k can be canonically identified with a subset of X_E. In particular, if K/k is a Galois extension, the group X_K has a natural $\mathcal{G}$-action and $X_K^{\mathcal{G}} = X_k$. Similarly, if V is a k-vector space we define $V_E = V \otimes_k E$ and identify V with the subset $V \otimes_k k$. In particular, we have $V_K^{\mathcal{G}} = V$ when $\mathcal{G}$ is the Galois group of a Galois extension K/k.

An arithmetically defined subgroup ([2]) of X_k is a subgroup of the form $X_k(\rho, \Lambda) = \{x \in X_k \mid \rho(x)\Lambda = \Lambda\}$, where ρ is a representation of X_k on a space V and Λ an R-lattice in V, for a finite set R of places of k. In this work, a number-theoretical extension E of the number field k is either an algebraic extension of the field k or an algebraic extension of a completion of k at a finite place. Let $R(E)$ be the set of places of E lying over R. Every R-lattice Λ of k has a unique minimal $R(E)$-lattice $\Lambda_E \subseteq V_E$ containing it. Similarly, every representation $\rho : X_k \to V$ can be extended to a representation $\rho_E : X_E \to V_E$. If $Y_k = X_k(\rho, \Lambda)$ and if E is a number-theoretical extension of k, then Y_E denotes the subgroup of X_E defined by $Y_E = X_E(\rho_E, \Lambda_E)$. Note that again $Y_K^{\mathcal{G}} = Y_k$ for a Galois extension K/k.

We define the locally trivial cohomology set $\widetilde{H}^1(Y_K)$ by

$$\widetilde{H}^1(Y_K) = \ker\Big(H^1(Y_K) \to \prod_{\substack{\wp \text{ finite} \\ \wp \notin R}} H^1_\wp(Y)\Big), \tag{2}$$

where, for every finite place $\wp$, we denote by $H^1_\wp(Y)$ the local cohomology set $H^1(K_\mathcal{P}/k_\wp, Y_{K_\mathcal{P}})$ for some fixed place $\mathcal{P}$ of K lying over $\wp$.

Let $\mathfrak{D}$ be a maximal R-order of the central simple algebra $\mathfrak{A}$. The group $\mathfrak{D}^*$ of units of the order $\mathfrak{D}$ is an arithmetically defined subgroup of the group $\mathfrak{A}^*$ of invertible elements of $\mathfrak{A}$. Another important arithmetically defined subgroup of the same group is the group $\mathcal{N}$ of elements $u \in \mathfrak{A}$ satisfying $u^{-1}\mathfrak{D}u = \mathfrak{D}$. Since $H^1(\mathfrak{A}_K^*) = 1$ ([4, Ex. 1, p. 16]), there exists a map

([2]) Since we do not require the representation ρ to be faithful, an arithmetically defined subgroup is not necessarily an arithmetic subgroup in the sense that the term is widely used in the literature. As the examples in the text show, two arithmetically defined subgroups of the same group need not be commensurable.

ϕ that associates an element of $H^1(\mathcal{N}_K)$ to every $\mathfrak{A}$-conjugacy class of $\mathcal{G}$-invariant maximal orders in $\mathfrak{A}_K$ that are $\mathfrak{A}_K$-conjugate to $\mathfrak{D}_K$. Since all maximal orders are locally conjugate, the subset of orders of the form $\mathfrak{D}'_K$, where $\mathfrak{D}'$ is a maximal order in $\mathfrak{A}$, corresponds to the subset $\widetilde{H}^1(\mathcal{N}_K)$. The map ϕ is defined on an $\mathfrak{A}$-conjugacy class α as follows: If $u \in \mathfrak{A}_K$ satisfies $u\mathfrak{D}_K u^{-1} \in \alpha$, then $\phi(\alpha)$ is the cocycle class of β defined by $\beta_\sigma = u^{-1}\,{}^\sigma u$.

3. Cohomological definition of $\mathfrak{P}$. From now on fix a set R of places of k containing the set $P(n)$ of all finite places dividing n. Fix an order $\mathfrak{D} = \mathcal{D}(a,b)$ of the central simple algebra $\mathfrak{A}$ such that both $\mathrm{ord}_\wp(a)$ and $\mathrm{ord}_\wp(b)$ are divisible by n for all $\wp \notin R$. All finite places outside R split $\mathfrak{A}$ completely ([9, Prop. 6, p. 260]). Let $R(K)$ and $\mathcal{O}_K$ be defined as in the introduction.

LEMMA 3.1. *Assume that $\mathfrak{A}_{K_\mathcal{P}}$ is isomorphic to a matrix algebra for any place $\mathcal{P} \notin R(K)$. Then the principal ideal $N(u)\mathcal{O}_K$ is an nth power in I_K for every $u \in \mathcal{N}_K$. Furthermore, if $N(u)$ is a unit then $u \in \mathfrak{D}_K^*$. In particular, we have a short exact sequence $\mathfrak{D}_K^* \hookrightarrow \mathcal{N}_K \overset{\tau}{\twoheadrightarrow} J_K$, where*

$$P_K^n \subseteq J_K \subseteq I_K^n \tag{3}$$

and $\tau(u) = N(u)\mathcal{O}_K$.

Proof. It suffices to work locally and assume that $\mathfrak{D}_{K_\mathcal{P}}$ is the order $\mathbb{M}(\mathcal{O}_{K_\mathcal{P}})$ of matrices with integral coefficients. If $u \in \mathcal{N}_{K_\mathcal{P}}$, by the theory of invariant factors, we can write $u = vdw$ where $d = \mathrm{diag}(\delta_1, \dots, \delta_n)$ is a diagonal matrix, while both v and w are in $\mathfrak{D}^*_{K_\mathcal{P}}$. Without loss of generality we may assume $u = d$. Let $E_{i,j}$ be the matrix that has 1 in position (i,j) and 0 elsewhere. Then $dE_{i,j}d^{-1} = \delta_j^{-1}\delta_i E_{i,j}$. It follows that $\delta_j^{-1}\delta_i$ is a unit for every pair (i,j), so that the principal ideals $\delta_1\mathcal{O}_{K_\mathcal{P}}, \dots, \delta_n\mathcal{O}_{K_\mathcal{P}}$ coincide. This proves the first statement. If $N(u)$ is a unit, then every δ_i, as defined above, is a unit. It follows that u and u^{-1} are in $\mathfrak{D}_K$ locally everywhere and hence globally. This proves the second statement and therefore the existence of the short exact sequence. The second contention of (3) follows from what we already proved. For the first contention we observe that $N(\lambda 1_\mathfrak{A}) = \lambda^n$ for $\lambda \in K$. ∎

Let $J_{\bar{\mathbb{Q}}}$ be defined as the direct limit of the groups J_K for all finite extensions K/k. Define $I_{\bar{\mathbb{Q}}}$ and $P_{\bar{\mathbb{Q}}}$ analogously. As any ideal becomes principal on some finite extension, we have $P_{\bar{\mathbb{Q}}} = P^n_{\bar{\mathbb{Q}}} = J_{\bar{\mathbb{Q}}} = I^n_{\bar{\mathbb{Q}}}$. It follows that the cohomology map

$$\tau_* : H^1(\bar{\mathbb{Q}}/k, \mathcal{N}_{\bar{\mathbb{Q}}}) \to H^1(\bar{\mathbb{Q}}/k, J_{\bar{\mathbb{Q}}}) = H^1(\bar{\mathbb{Q}}/k, P_{\bar{\mathbb{Q}}})$$

factors through $H^1(\bar{\mathbb{Q}}/k, \bar{\mathbb{Q}}^*) = \{1\}$. By the cohomological theory of profinite groups [7], it follows that for every Galois extension K and any cocycle

in $H^1(\mathcal{N}_K)$, its image in $H^1(J_K)$ becomes trivial under some finite field extension. Since $\widetilde{H}^1(\mathcal{N}_K)$ corresponds to a subset of the finite set of conjugacy classes of maximal orders in $\mathfrak{A}$, it is itself finite and the next result follows:

LEMMA 3.2. *There exists a finite extension L of k such that, for every finite Galois extension K of k containing L, the map $\tau_* : \widetilde{H}^1(\mathcal{N}_K) \to \widetilde{H}^1(J_K)$ is trivial.*

LEMMA 3.3. *There is a finite extension Σ of k such that, for any Galois extension F of k containing Σ, the map $\phi : \widetilde{H}^1(\mathfrak{D}_F^*) \to \widetilde{H}^1(\mathcal{N}_F)$ is surjective.*

Proof. It follows from §I.5.5 in [7] that the invariant subgroup $J_K^{\mathcal{G}}$ acts on $H^1(\mathfrak{D}_K^*)$ and

$$\ker[H^1(\mathcal{N}_K) \to H^1(J_K)] \cong H^1(\mathfrak{D}_K^*)/J_K^{\mathcal{G}}, \tag{4}$$

where the isomorphism is induced by the map $\phi_2 : H^1(\mathfrak{D}_K^*) \to H^1(\mathcal{N}_K)$. Consider the commutative diagram

$$\begin{array}{ccccccc}
J_k & \xrightarrow{\psi_1} & \widetilde{H}^1(\mathfrak{D}_K^*) & \xrightarrow{\phi=\phi_1} & \widetilde{H}^1(\mathcal{N}_K) & & \\
\downarrow & & \downarrow & & \downarrow & \searrow^{\tau_1} & \\
J_K^{\mathcal{G}} & \xrightarrow{\psi_2} & H^1(\mathfrak{D}_K^*) & \xrightarrow{\phi_2} & H^1(\mathcal{N}_K) & \xrightarrow{\tau_2} & H^1(J_K) \\
\downarrow & & \downarrow l_1 & & \downarrow l_2 & & \\
\prod_\wp \mathcal{N}_{k_\wp} & \xrightarrow{\Psi} & \prod_\wp J_\wp & \xrightarrow{\psi_3} & \prod_\wp H^1_\wp(\mathfrak{D}^*) & \xrightarrow{\phi_3} & \prod_\wp H^1_\wp(\mathcal{N})
\end{array}$$

where for a finite place $\wp$ not in R, we define $J_\wp$ as the group of n-powers of fractional ideals in $K_\mathcal{P}$. We claim that the last row of the diagram is exact. By the analogue of Lemma 3.1 for the local field extension $K_\mathcal{P}/k_\wp$, we have a short exact sequence $\mathfrak{D}^*_{K_\mathcal{P}} \hookrightarrow \mathcal{N}_{K_\mathcal{P}} \twoheadrightarrow J_\wp$, since all local ideals are principal. Now the last row of the diagram is the product of the corresponding long exact sequences in cohomology, since the Galois group of a local field extension acts trivially on local ideals. The result follows.

The columns containing l_1 and l_2 are exact by definition. Assume that K contains the field L defined in the previous lemma, whence the map τ_1 is trivial. Let $u \in \widetilde{H}^1(\mathcal{N}_K)$. A diagram chasing argument shows that $u = \phi_2(a)$ for some $a \in H^1(\mathfrak{D}_K^*)$ and there exists $c \in \prod_\wp J_\wp$ such that $l_1(a) = \psi_3(c)$. Since the local component $\Psi_\wp$ of Ψ is surjective for all places $\wp$ that are unramified for K/k, the element $\psi_3(c)$ depends only on finitely many local coordinates of c, so we may assume that c has finitely many non-trivial coordinates, i.e., is the image of the nth power $\mathcal{I}^n$ of an invariant fractional ideal $\mathcal{I}$ of K.

Note that all maps in the diagram commute with co-restriction maps, whence we can replace K by its Hilbert class field. Then there exists an

element $\lambda \in K$ such that $\mathcal{I}_K = \lambda \mathcal{O}_K$, hence $\mathcal{I}_K^n \in P_K^n \subseteq J_K$. Equation (4) shows that $u = \phi_2(\mathcal{I}_K^{-1} * a_K)$, where $*$ denotes the action of $J_E^{\mathcal{G}}$ on $H^1(\mathfrak{D}_K^*)$, but $\mathcal{I}_K^{-1} * a \in \widetilde{H}^1(\mathfrak{D}_K^*)$.

Recall that the set $\widetilde{H}^1(\mathcal{N}_K)$ is in correspondence with the set of conjugacy classes of maximal R-orders in $\mathfrak{A}$ that become conjugate to $\mathfrak{D}$ over K. In fact, the explicit description of this correspondence given in §2 shows that it commutes with the co-restriction maps $\widetilde{H}^1(\mathcal{N}_K) \to \widetilde{H}^1(\mathcal{N}_F)$ for $K \subseteq F$. Since the set of conjugacy classes of orders is finite, there exists a finite extension Φ of L such that $\widetilde{H}^1(\mathcal{N}_F)$ does not depend on F provided $F \supseteq \Phi$ and we choose Σ as the Hilbert class field of Φ. ∎

Proof of Theorem 2. Find a field K where $\mathfrak{D}_K$ and $\mathfrak{D}'_K$ are conjugate. Since the definition of $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$ is invariant under field extensions, this holds for any field K satisfying the following two conditions:

- The extension $\mathcal{I}_K$ of one ideal $\mathcal{I}$ in the class $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$ is an nth power.
- The field K is not totally real. In particular, $PSL_1(\mathfrak{A}_K)$ has strong approximation.

Let $\mathfrak{c} \in \widetilde{H}^1(\mathcal{N}_K)$ be the cocycle class corresponding to the order $\mathfrak{D}'$ and let $b \in \mathfrak{c}$. By the previous lemma, we may assume that $b_\sigma \in \mathfrak{D}^*$ for all $\sigma \in \mathcal{G}$ and the cocycle b is locally trivial. There exists $g \in \mathfrak{A}_K$ such that $b_\sigma = g^{-1}\,{}^\sigma g$. Since the cocycle $N(b)$ has values in $\mathcal{O}_K^*$ and is locally trivial, the ideal $N(g)\mathcal{O}_K$ is the extension $\mathcal{I}_K$ of a fractional ideal $\mathcal{I}$ of k. Let $\mathfrak{A}_{\mathbb{A}_K}^*$ be the adelic group of $\mathfrak{A}_K^*$ ([6, p. 249]). Let $\mathfrak{D}_{\mathbb{A}_K}^* = \{j \in \mathfrak{A}_{\mathbb{A}_K}^* \mid j_{\mathcal{P}} \in \mathfrak{D}_{K_{\mathcal{P}}}^* \text{ for all } K_{\mathcal{P}} \notin R(K)\}$. As the cocycle b is locally trivial, we can write $g^{-1}\,{}^\sigma g = j^{-1}\,{}^\sigma j$ for some fixed j in $\mathfrak{D}_{\mathbb{A}_K}^*$. It follows that $h = gj^{-1} \in \mathfrak{A}_{\mathbb{A}_k}$. Since $N(j)$ is a unit everywhere, the ideal $\mathcal{I}$ equals $N(h)\mathcal{O} = \prod_{\wp \notin R} \wp^{\operatorname{ord}_\wp[N(h_\wp)]}$. However, the class of the ideal $N(h)\mathcal{O}$ is, by definition, equal to $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$. The lattice Λ in (b) is the lattice $\mathfrak{D}h^{-1}$ defined locally by the relations $(\mathfrak{D}h^{-1})_\wp = \mathfrak{D}_\wp h_\wp^{-1}$. Conversely, if g satisfies condition (b), the cocycle $g^{-1}\,{}^\sigma g$ is in $\widetilde{H}^1(\mathfrak{D}_K^*)$, and therefore any element g satisfying (a) and (b) can be used in this computation. ∎

Proposition 3.4. *When $n = 2$, the distance $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$ is the ideal class of $\mathcal{I}_1 \cdots \mathcal{I}_m$ in $\mathfrak{T}_2(\mathfrak{A})$, where $\mathfrak{D}/(\mathfrak{D} \cap \mathfrak{D}')$ is isomorphic to the Cartesian product $\mathcal{O}/\mathcal{I}_1 \times \cdots \times \mathcal{O}/\mathcal{I}_m$ as $\mathcal{O}$-modules.*

Proof. It suffices to work locally. Let $\wp \notin R$. Let $h_\wp$ satisfy $\mathfrak{D}'_{k_\wp} = h_\wp \mathfrak{D}_{k_\wp} h_\wp^{-1}$. We have an isomorphism $\phi : \mathfrak{A}_{k_\wp} \to \mathbb{M}(k_\wp)$ such that $\phi(\mathfrak{D}_{k_\wp}) = \mathbb{M}_2(\mathcal{O}_\wp)$. By the theory of invariant factors, $\phi(h_\wp) = uzv$ where $u, v \in \mathbb{M}_2(\mathcal{O}_\wp)$ and z is a diagonal matrix. Replacing ϕ by $t \mapsto u^{-1}\phi(t)u$ and $h_\wp$ by $h_\wp \phi^{-1}(v^{-1}u^{-1})$ if needed, we can assume that $\phi(h_\wp)$ is diagonal. Multiplying

by an element in the center we can further assume that $\phi(h_\wp) = \mathrm{diag}(r, 1)$. Then $\phi(\mathfrak{D}_{k_\wp} \cap \mathfrak{D}'_{k_\wp})$ is the set of integral matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ such that r divides β and the result follows. ∎

4. The diagonal case. Now we consider the case $a = c$. To simplify notations, we say that $\mathcal{D}(a, b)$ is generated by (x, y) if x and y satisfy (1) and $\mathcal{D}(a, b) = \mathcal{O}[\mathcal{A}^{-1}x \cup \mathcal{B}^{-1}y]$ where $\mathcal{A}^n = a\mathcal{O}$ and $\mathcal{B}^n = b\mathcal{O}$ as in the introduction. Locally, this means the following: For a place $\wp \notin R$, the local component ([5, §81E]) at $\wp$ of $\mathcal{D}(a, b)$ is defined as

$$\mathcal{D}(a, b)_\wp = \mathcal{O}_\wp[\pi_\wp^{-\mathrm{ord}_\wp(a)/n} x, \pi_\wp^{-\mathrm{ord}_\wp(b)/n} y], \tag{5}$$

where $\pi_\wp$ is a uniformizing parameter of the completion $\mathcal{O}_\wp$ of $\mathcal{O}$ at $\wp$. By the Skolem–Noether theorem we can assume that $\mathcal{D}(a, b)$ is generated by (x, y) and $\mathcal{D}(a, d)$ is generated by (x, y') for some $y' \in \mathfrak{A}$. Let $K_0 = k(\sqrt[n]{a}, \sqrt[n]{b}, \sqrt[n]{d})$. Let K be a field extension of K_0. We define the matrices

$$\Phi_1 = \mathrm{diag}(1, \eta, \dots, \eta^{n-1}) = \sum_{i=1}^{n} \eta^{i-1} E_{i,i}, \qquad \Phi_2 = \sum_{i=1}^{n} E_{i,i+1},$$

where $E_{i,j}$ is the matrix with a 1 in position (i, j) and 0's elsewhere. We can find an isomorphism $\phi : \mathfrak{A}_K \to \mathbb{M}_n(K)$ such that $\phi(x) = \sqrt[n]{a}\Phi_1$ and $\phi(y) = \sqrt[n]{b}\Phi_2$. Then $y'y^{-1}$ is in the centralizer of x, so we can write $\phi(y'y^{-1}) = \mathrm{diag}(\tau_1, \dots, \tau_n)$. By taking reduced norms we get $\tau_1 \cdots \tau_n = d/b$. As x, y, and $y'y^{-1}$ are in $\mathfrak{A}$, they are invariant under the action of the Galois group. It follows that ${}^\lambda E_{i,i} = E_{i+\Gamma(\lambda), i+\Gamma(\lambda)}$, where Γ is the Kummer homomorphism defined in the introduction. In particular,

$${}^\lambda \tau_i = \tau_{i+\Gamma(\lambda)} \tag{6}$$

for any automorphism λ. This implies in particular that $\tau_i \in F = k(\sqrt[n]{a})$. Notice that for any $\tau_1, \dots, \tau_n$ satisfying (6), the pre-image y' of the matrix $\sqrt[n]{b}\,\mathrm{diag}(\tau_1, \dots, \tau_n)\Phi_2$ is in $\mathfrak{A}$ and (x, y') can be assumed to generate $\mathcal{D}(a, d)$. It follows that $\tau_1, \dots, \tau_n$ are arbitrary elements in F satisfying (6). Any element $g \in \mathfrak{A}_K$ satisfying $g^{-1}xg = x$ and $g^{-1}yg = y'$ must be of the form $g = \mathrm{diag}(s_1, \dots, s_n)$, where $s_i s_{i+1}^{-1} = \tau_i \sqrt[n]{b/d}$.

LEMMA 4.1. *For some finite extension K of K_0, there exist $s_1, \dots, s_n \in K$ satisfying the following*:

- $s_i s_{i+1}^{-1} = \tau_i \sqrt[n]{b/d}$ *for all* i.
- *The lattice* $\mathcal{O}_K s_1 E_{1,1} + \cdots + \mathcal{O}_K s_n E_{n,n}$ *in* $\phi(K[x])$ *equals* $\phi(\mathcal{I}_K)$ *for some fractional ideal* $\mathcal{I}$ *in* $k[x]$.

Proof. Take an element $g \in \mathfrak{A}_K^*$ satisfying the conclusions of Theorem 2. By the Skolem–Noether Theorem, we can modify g by an element of $\mathfrak{A}_k^*$ if needed, so that $g^{-1}xg = x$ and $g^{-1}yg = \sqrt[n]{b/d}\, y'$. The cocycle b defined by

$b_\sigma = g^{-1}\,{}^\sigma g$ has values in $\mathcal{M}_K = \mathcal{N}_K \cap K[x]$. Since the localizations $\mathfrak{D}_{k_\wp}$ and $\mathfrak{D}'_{k_\wp}$ are conjugate by an element of the algebra $k_\wp[x]$ for every $\wp \notin R$, the class of the cocycle b is in $\widetilde{H}^1(\mathcal{M}_K)$. We may reason as in the proof of Lemma 3.3, for the short exact sequence $\Omega_K^* \hookrightarrow \mathcal{M}_K \twoheadrightarrow J'_K$ instead of $\mathfrak{D}_K^* \hookrightarrow \mathcal{N}_K \twoheadrightarrow J_K$, where $\Omega = k[x] \cap \mathfrak{D}$ and J'_K is the image of $\mathcal{M}_K$ in J_K. Note that we still have $P_K^n \subseteq J'_K$. It follows that, for K large enough, we can find $u \in \mathcal{M}_K$ such that $b'_\sigma = (gu)^{-1}\,{}^\sigma(gu)$ defines a cocycle class in $\widetilde{H}^1(\Omega_K^*)$. This implies, as before, that $gu\Omega_K = h\Omega_K$ for some $h \in \mathbb{A}_k[x]^*$. Note that, since $\mathcal{A}^{-1}x \subseteq \Omega$ and n is an R-unit, the ring Ω is the maximal R-order of the k-algebra $k[x]$. Furthermore, Ω_K is the maximal $R(K)$-order of $K[x]$. Let $\mathcal{I}$ be the fractional ideal defined locally by $\mathcal{I}_\wp = h_\wp \Omega_{k_\wp}$. Then, if $\phi(gu) = \operatorname{diag}(s_1, \dots, s_n)$, the elements $s_1, \dots, s_n$ are as required. ∎

Proof of Theorem 1. Let $s_1, \dots, s_n$ be as in the previous lemma. By Theorem 2 we know that $\mathfrak{P}_R(\mathfrak{D}, \mathfrak{D}')$ is the ideal class of $\mathcal{E}$, where $\mathcal{E}_K = N(g)\mathcal{O}_K = s_1 \cdots s_n \mathcal{O}_K$. If $\mathcal{I}$ is as in the last lemma, $\psi(\mathcal{I}_F) = \mathcal{C}_1 \times \cdots \times \mathcal{C}_n$, for some fractional ideals $\mathcal{C}_i$ in F, whence $(\mathcal{C}_i)_K = s_i \mathcal{O}_K$. It follows that $\mathcal{C}_i \mathcal{C}_{i+1}^{-1} = \tau_i \mathcal{B}_F$. This proves the existence of $\mathcal{C}_1, \dots, \mathcal{C}_n$. Assume next that $\mathcal{C}'_1, \dots, \mathcal{C}'_n$ also satisfy $\mathcal{C}'_i (\mathcal{C}')_{i+1}^{-1} = \tau_i \mathcal{B}_F$ and $\mathcal{C}'_1 \times \cdots \times \mathcal{C}'_n = \mathcal{I}'_F$ for some fractional ideal $\mathcal{I}'$ in $k[x]$. The first condition proves that $\mathcal{C}'_i = \mathcal{C}_i \mathcal{F}'$ for some fractional ideal $\mathcal{F}'$ in F, and $\mathcal{F}'\mathbf{1} = \psi[(\mathcal{I}'/\mathcal{I})_F]$, where $\mathbf{1}$ is the unity in the ring F^n. This implies that $\mathcal{F}'$ is invariant under the action of the Galois group $\operatorname{Gal}(F/k)$. Since the extension F/k is unramified outside $R(a,b) \subseteq R$, it follows that $\mathcal{F}' = \mathcal{F}_F$ for some fractional ideal $\mathcal{F}$ of k. We conclude that $N_{L/k}(\mathcal{I}') = \mathcal{F}^n N_{L/k}(\mathcal{I})$, hence the class of $N_{L/k}(\mathcal{I})$ does not depend on the choice of $\mathcal{C}_1, \dots, \mathcal{C}_n$. ∎

Proof of (A′). If a is an nth power in k, the homomorphism Γ is trivial and $F = k$. One can set $\tau_i = 1$ for $i < n$, $\tau_n = d/b$, and $\mathcal{C}_i = \mathcal{B}^{1-i}$, so that if $\psi(\mathcal{I}) = \mathcal{C}_1 \times \cdots \times \mathcal{C}_n$, then $N_{L/k}(\mathcal{I}) = \mathcal{C}_1 \cdots \mathcal{C}_n = \mathcal{B}^{n(1-n)/2}$. ∎

Proof of (B′). If L is a field, then Γ is a surjection. Let $\sigma \in \operatorname{Gal}(F/k)$ satisfy $\Gamma(\sigma) = 1$. Since $(a,b)_\eta = (a,d)_\eta$ there exists $\tau \in L \cong F$ such that $N_{L/k}(\tau) = d/b$. Set $\tau_i = \sigma^{i-1}(\tau)$. Since $N_{F/k}(\tau \mathcal{B}_F) = (1)$, there exists a fractional ideal $\mathcal{C}$ of F such that $\sigma(\mathcal{C})^{-1}\mathcal{C} = \tau \mathcal{B}_F$. We set $\mathcal{C}_i = \sigma^{i-1}(\mathcal{C})$. Furthermore, we consider $\mathcal{C}$ as a fractional ideal of L, and under that identification $\mathcal{C}_1 \times \cdots \times \mathcal{C}_n = \psi(\mathcal{C}_F)$. The result follows. ∎

Acknowledgements. This research was supported by Fondecyt, proyecto No 1040227.

References

[1] L. E. Arenas-Carmona, *Applications of spinor class fields: embeddings of orders and quaternionic lattices*, Ann. Inst. Fourier (Grenoble) 53 (2003), 2021–2038.

[2] J. Brzezinski, *Spinor class groups of orders*, J. Algebra 84 (1983), 468–481.
[3] T. Chinburg and E. Friedman, *Hilbert symbols, class groups and quaternion algebras*, J. Théor. Nombres Bordeaux 12 (2000), 367–377.
[4] M. Kneser, *Lectures on Galois Cohomology of Classical Groups*, Tata Inst. Fund. Res., Bombay, 1969.
[5] O. T. O'Meara, *Introduction to Quadratic Forms*, Academic Press, New York, 1963.
[6] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, Boston, 1994.
[7] J.-P. Serre, *Cohomologie Galoisienne*, 5th ed., Springer, Berlin, 1997.
[8] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Springer, Berlin, 1980.
[9] A. Weil, *Basic Number Theory*, 2nd ed., Springer, Berlin, 1973.

Universidad de Chile
Facultad de Ciencias
Casilla 653, Santiago, Chile
E-mail: learenas@uchile.cl

Received on 13.12.2006
and in revised form on 9.12.2008 (5347)