ANNALES

DE

L'INSTITUT FOURIER

Luis ARENAS-CARMONA

Representation fields for commutative orders

REPRESENTATION FIELDS
FOR COMMUTATIVE ORDERS

by Luis ARENAS-CARMONA (*)

———

ABSTRACT. — A representation field for a non-maximal order $\mathfrak{H}$ in a central simple algebra is a subfield of the spinor class field of maximal orders which determines the set of spinor genera of maximal orders containing a copy of $\mathfrak{H}$. Not every non-maximal order has a representation field. In this work we prove that every commutative order has a representation field and give a formula for it. The main result is proved for central simple algebras over arbitrary global fields.

RÉSUMÉ. — Un corps de représentation pour un ordre non maximal $\mathfrak{H}$ dans une algèbre centrale simple est un sous-corps du corps de classes spinoriel d'ordres maximaux qui détermine l'ensemble de genres spinoriels d'ordres maximaux qui contiennent un conjugué de $\mathfrak{H}$. Un ordre non maximal ne possède pas forcément un corps de représentation. Dans ce travail, nous montrons que chaque ordre commutatif a un corps de représentation F et nous donnons une formule pour F. Le résultat principal est prouvé pour des algèbres simples centrales sur des corps globaux arbitraires.

1. Introduction

Let K be a number field. Let $\mathfrak{A}$ be either, a central simple K-algebra of degree $n > 2$, or a quaternion algebra satisfying Eichler condition [5]. The set $\mathbb{O}$ of maximal orders in $\mathfrak{A}$ can be split into isomorphism classes or, equivalently, conjugacy classes [8]. Let $\overline{\mathbb{O}}$ be the set of isomorphism classes. In [2] we found a field extension Σ/K whose Galois group $\mathrm{Gal}(\Sigma/K)$ yields a natural free and transitive action on $\overline{\mathbb{O}}$. For some families of orders $\mathfrak{H}$ in $\mathfrak{A}$ we found a field $F = F(\mathfrak{H})$ between K and Σ such that the set $\overline{\mathbb{O}}_{\mathfrak{H}}$ of classes of orders containing a conjugate of $\mathfrak{H}$ is exactly one orbit of the subgroup $\mathrm{Gal}(\Sigma/F)$. In particular, the number of isomorphism classes

of such orders is $[\Sigma : F]$. The first result in this direction seems to be
due to Chevalley who considered the case when $\mathfrak{A}$ is a matrix algebra
and $\mathfrak{H}$ is the maximal order of a maximal subfield L [4]. In our notation,
Chevalley result implies $F(\mathfrak{H}) = L \cap \Sigma$. In [2] we extended this result to
algebras $\mathfrak{A}$ with no partial ramification. Chinburg and Friedman have given
a similar result in which $\mathfrak{H}$ is an arbitrary rank-two commutative order in
a quaternion algebra $\mathfrak{A}$ satisfying Eichler condition [5]. In case $L = K\mathfrak{H}$ is
a field, the representation field F is a subfield of $L \cap \Sigma$ that depends on
the relative discriminant of the order $\mathfrak{H}$. A more recent article by Linowitz
and Shemanske [6] extends this result to central simple algebras of prime
degree. Here we extend these results by proving the existence and providing
a formula for the representation field for every commutative order $\mathfrak{H}$ in a
central simple algebra $\mathfrak{A}$ of arbitrary degree.

   We use the language of spinor genera in all of this work for the sake
of generality. In this general setting, the set $\overline{\mathbb{O}}$ is not the set of conjugacy
classes but the set of spinor genera of maximal orders, while $\overline{\mathbb{O}}_{\mathfrak{H}}$ is the
set of spinor genera Φ with at least one order $\mathfrak{D} \in \Phi$ containing $\mathfrak{H}$ as a
sub-order. All of the above extends to this setting. A single spinor genera
can have more than one class only when $\mathfrak{A}$ is a quaternion algebra failing
to satisfy Eichler condition [2].

   THEOREM 1.1. — *Let $\mathfrak{A}$ be a central simple algebra over the number
field K. Let $\mathfrak{H}$ be an arbitrary commutative order. Let $\mathfrak{D}$ be a maximal
order containing $\mathfrak{H}$. For every maximal ideal $\wp$ in the ring of integers $\mathcal{O}_K$
we let $I_\wp$ be the only maximal two-sided ideal of $\mathfrak{D}$ containing $\wp 1_{\mathfrak{D}}$, and let
$\mathbb{H}_\wp$ be the image of $\mathfrak{H}$ in $\mathfrak{D}/I_\wp$. Let $\mathbb{E}_\wp$ be the center of the ring $\mathfrak{D}/I_\wp$. Let
$t_\wp$ be the greatest common divisor of the dimensions of the irreducible $\mathbb{E}_\wp$-
representations of the algebra $\mathbb{E}_\wp \mathbb{H}_\wp$. Then the representation field $F(\mathfrak{H})$
is the maximal subfield F, of the spinor class field Σ, such that the inertia
degree $f_\wp(F/K)$ divides $t_\wp$ for every place $\wp$.*

   In the above statement, it is implied that $\mathbb{E}_\wp$ is a field. In fact, $\mathbb{E}_\wp$ is
the residue field of a local division algebra $E_\wp$ such that $\mathfrak{A}_\wp \cong \mathbb{M}_m(E_\wp)$.
We show in § 5 that Theorem 1.1 is indeed a generalization of the results
in [2], [5], and [6]. For the sake of generality, we prove a generalization of
Theorem 1.1 that includes also the function field case studied in [1]. In
order to consider both cases simultaneously, we introduce the concept of
A-curve in § 2.

2. A-curves and Spinor class fields

In all that follows, we say that X is an A-curve with field of functions K, in any of the following cases:

CASE 2.1. — *X is a smooth irreducible curve over a finite field $\mathbb{F}$ and K is the field of rational functions on X.*

CASE 2.2. — *$X = \operatorname{Spec} \mathcal{O}_S$ where $\mathcal{O}_S$ is the ring of S-integers for a non-empty finite set S of places over a global field K containing the archimedean places.*

In both cases X is provided with its Zariski Topology and its structure sheaf $\mathcal{O}_X$. Furthermore, in Case 2.2 every S-lattice Λ_0 in a K-vector space V_K defines a locally free sheaf Λ by $\Lambda(U) = \mathcal{O}_X(U)\Lambda_0$, and the stalk at a place $\wp \in X$ is just the free $\mathcal{O}_{[\wp]}$-lattice $\Lambda_{0[\wp]}$, where $\mathcal{O}_{[\wp]}$ and $\Lambda_{0[\wp]}$ denote the localizations at $\wp$ (as opposed to completions). The sheaf Λ thus defined is called an X-lattice. Analogously, we define an X-lattice in Case 2.1 as a locally free sheaf of lattices as in [1]. The space W spanned by $\Lambda(U)$ is independent of the affine set U. We call W the space generated by Λ and denote it $K\Lambda$. The affine sub-case in Case 2.1 is also a sub-case of Case 2.2, if we let S be the complement of X in its smooth projective completion, and both definitions of X-lattice coincide in this case. We say that $S = \emptyset$ when X is a projective curve over a finite field.

Note that the completion $\Lambda_\wp$ of the sheaf Λ at a place $\wp \in X$ is defined as the completion of the stalk $\Lambda_{[\wp]}$, or equivalently the completion of the lattice $\Lambda(U)$ for any affine set $U \subseteq X$ containing $\wp$. Since X-lattices can be defined by pasting lattices defined on the sets of an affine cover, some properties of usual lattices ([7] § 81) are inherited by X-lattices, namely:

- A lattice Λ is determined by it set of completions $\{\Lambda_\wp\}_\wp$, and it can be modified at a finite number of places to get a new lattice .
- The adelization $\operatorname{GL}_{\mathbb{A}}(V)$ of the group $\operatorname{GL}(V)$ of K-linear maps on V acts on the set of lattices by acting on the set of completions at every place $\wp$.
- If $V = \mathfrak{A}$ is an algebra, an X-lattice $\mathfrak{D}$ is an order (*i.e.*, a sheaf of orders) if and only if every completion is an order. The same holds for maximal orders[1].

Since any two local maximal orders are conjugate in any completion $\mathfrak{A}_\wp$ with $\wp \in X$, it follows that for any two global maximal orders $\mathfrak{D}$ and $\mathfrak{D}'$

---

[1] This is not in the reference, but follows easily from the previous results, since a lattice $\mathfrak{D}$ is an order if and only if $1 \in \mathfrak{D}$ and $\mathfrak{D}\mathfrak{D} = \mathfrak{D}$.

there exist an element a in the adelization $\mathfrak{A}_{\mathbb{A}}^*$ satisfying $\mathfrak{D}_{\mathbb{A}}' = a\mathfrak{D}_{\mathbb{A}}a^{-1}$, where

$$\mathfrak{D}_{\mathbb{A}} = \prod_{\wp \in S} \mathfrak{A}_\wp \times \prod_{\wp \in X} \mathfrak{D}_\wp$$

and $\mathfrak{D}_{\mathbb{A}}'$ is defined analogously. As usual we write simply $\mathfrak{D}' = a\mathfrak{D}a^{-1}$, since no other action of adelic points on orders is considered in this work. The orders $\mathfrak{D}$ and $\mathfrak{D}'$ are conjugate if we can choose $a \in \mathfrak{A}^*$. We say that these orders are in the same spinor genus if we can choose $a = bc$ where $b \in \mathfrak{A}^*$ and $c_\wp$ has reduced norm 1 for every place $\wp \in X$. The following result is needed in what follows. It is proved in [2] for Case 2.1 and follows easily from [8] (Theorem 33.4 and Theorem 33.15), or remark 2.5 in [1], for Case 2.2.

> The set of spinor genera of maximal orders in $\mathfrak{A}$ is in correspondence with the group $J_K/K^*H(\mathfrak{D})$, where J_K is the idele group of K and $H(\mathfrak{D}) \subseteq J_K$ is the image under the reduced norm of the conjugation-stabilizer $(\mathfrak{A}_{\mathbb{A}}^*)^{\mathfrak{D}}$.

By the strong approximation theorem, two orders in the same spinor genus are always conjugate if the automorphism group of $\mathfrak{A}$ is non-compact at some place $\wp \in S$. When K is a number field and $S = \infty$, this condition is equivalent to Eichler condition if $\mathfrak{A}$ is a quaternion algebra, and it is always satisfied for algebras of higher dimension. When X is a projective curve we have $S = \emptyset$, so the condition cannot hold. Note however that spinor genera of orders over projective curves still carry some global information that can be recovered in any affine subset of X [1]. When X is an affine curve, the condition holds unless every infinite place of X is totally ramified for $\mathfrak{A}/K$. Since we express our main result in terms of spinor genera, this result holds in full generality, but it is important to keep in mind the previous remark in the applications.

We let Σ be the class field corresponding to the group $K^*H(\mathfrak{D})$ ([10], § XIII.9). For every $\rho \in \text{Gal}(\Sigma/K)$, let $a_\rho \in \mathfrak{A}_{\mathbb{A}}^*$ be any element satisfying $\rho = [n(a_\rho), \Sigma/K]$, where $t \mapsto [t, \Sigma/K]$ denotes the Artin maps on ideles and $n : \mathfrak{A}_{\mathbb{A}}^* \to J_K$ denotes the reduced norm. The action of $\text{Gal}(\Sigma/K)$ on the set $\overline{\mathbb{O}}$ of spinor genera of maximal orders is given by

$$\rho.\text{spin}(\mathfrak{D}) = \text{spin}(a_\rho \mathfrak{D} a_\rho^{-1}), \qquad \forall(\rho, \mathfrak{D}) \in \text{Gal}(\Sigma/K) \times \mathbb{O}.$$

Assume in all that follows that $\mathfrak{H}$ is a suborder of $\mathfrak{D}$. A generator for $\mathfrak{D}|\mathfrak{H}$ is an element $u \in \mathfrak{A}_{\mathbb{A}}^*$ such that $\mathfrak{H} \subseteq u\mathfrak{D}u^{-1}$. Let $\lceil(\mathfrak{D}|\mathfrak{H})$ the set of reduced norms of generators. There is no reason a priori for this set to be a group. Note that if a normalizes $\mathfrak{D}$ and b normalizes $\mathfrak{H}$, then for any generator

u the element bua is a generator. In particular $H(\mathfrak{D})\lceil(\mathfrak{D}|\mathfrak{H}) = \lceil(\mathfrak{D}|\mathfrak{H})$. We conclude that the set $K^*\lceil(\mathfrak{D}|\mathfrak{H})$ is completely determined by its image $\mathcal{G}(\mathfrak{D}|\mathfrak{H}) \subseteq \mathrm{Gal}(\Sigma/K)$ under the Artin map. If $\mathcal{G}(\mathfrak{D}|\mathfrak{H})$ is a group we define

$$F(\mathfrak{H}) = \big\{a \in \Sigma \big| g(a) = a \ \forall g \in \mathcal{G}(\mathfrak{D}|\mathfrak{H})\big\},$$

and call $F = F(\mathfrak{H})$ the representation field for $\mathfrak{H}$. It follows from the definition that an order $\mathfrak{D}' = b\mathfrak{D}b^{-1}$, for $b \in \mathfrak{A}_{\mathbb{A}}^*$, is in the same spinor genus than some maximal order containing a conjugate of $\mathfrak{H}$, if and only if $n(b) \in n(u)K^*H(\mathfrak{D})$ for some generator u for $\mathfrak{D}|\mathfrak{H}$, or equivalently $[n(b), F/K] = \mathrm{id}_F$. We conclude that F satisfies the properties stated in § 1. If $\mathcal{G}(\mathfrak{D}|\mathfrak{H})$ fails to be a group we say that the representation field for $\mathfrak{H}$ is not defined. For examples of non-commutative orders for which the representation field is not defined, see [3] or Example 3.6 below.

3. Spinor image and representations

Let K be a local field of arbitrary characteristic. Assume in all of this section that $\mathfrak{A} = \mathbb{M}_m(E)$ where E is a central division algebra over K with ring of integers $\mathcal{O}_E$, maximal ideal $\mathfrak{m}_E$, and residue field $\mathbb{E} = \mathcal{O}_E/\mathfrak{m}_E$. Let π_E and π_K be uniformizing parameters of E and K respectively. Recall that if $n : \mathfrak{A}^* \to K^*$ is the reduced norm, then $n(\pi_E 1_\mathfrak{A}) = v\pi_K^m$ for some unit $v \in \mathcal{O}_K^*$.

Let $\mathfrak{H} \subseteq \mathfrak{D}$ be orders in $\mathfrak{A}$. Then a local generator u, or simply a generator whenever confusion is unlikely, is an element $u \in \mathfrak{A}^*$ satisfying $\mathfrak{H} \subseteq u\mathfrak{D}u^{-1}$. In the rest of this section, we assume that $\mathfrak{D}$ is maximal, but we make no assumption on $\mathfrak{H}$ for the sake of generality. The purpose of this section is to characterize the set of reduced norms of local generators in terms of the degrees of the representations of the reduction of $\mathfrak{H}$ módulo $\pi_E\mathfrak{D}$.

For short, we let $\vec{1}_q$ and $\vec{0}_q$ denote vectors $(1,\ldots,1)$ and $(0,\ldots,0)$ of length q. For example $(\vec{1}_3, 2\cdot \vec{1}_2, \vec{0}_3) = (1,1,1,2,2,0,0,0)$. For any ring A we denote by A^m the free A-module with m generators, while A^{*m} denotes the set of m-powers of invertible elements in A.

LEMMA 3.1. — *Let $\mathfrak{H}$ be a suborder of the maximal order $\mathfrak{D} = \mathbb{M}_m(\mathcal{O}_E)$, and let $\mathbb{H}$ be its image in $\mathbb{M}_m(\mathbb{E})$. Assume that the reduced norm of a generator u for $\mathfrak{D}|\mathfrak{H}$ spans the principal ideal $\big(n(u)\big) = (\pi_K^s) = \pi_K^s \mathcal{O}_K$. Then there exists a flag of $\mathbb{H}$-modules*

$$\{0\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_t = \mathbb{E}^m$$

and integers $r_1, \ldots, r_t$ satisfying

$$s = \sum_{i=1}^{t} r_i \dim_{\mathbb{E}}(V_i/V_{i-1}).$$

Proof. — Let $P, Q \in \mathbb{M}_m(\mathcal{O}_E)^*$ be such that $u = PDQ$ for a diagonal matrix $D = \operatorname{diag}(\pi_E^{r_1} \overrightarrow{1}_{q_1}, \ldots, \pi_E^{r_t} \overrightarrow{1}_{q_t})$, where $r_1 < r_2 < \cdots < r_t$ and $q_1 + \cdots + q_t = m$. The condition $\mathfrak{H} \subseteq u\mathfrak{D}u^{-1}$ is equivalent to $\mathfrak{H}(u\mathcal{O}_E^m) \subseteq u\mathcal{O}_E^m$, or equivalently

$$(P^{-1}\mathfrak{H}P)D\mathcal{O}_E^m \subseteq D\mathcal{O}_E^m.$$

Replacing $\mathfrak{H}$ by $P^{-1}\mathfrak{H}P$ if needed, we can assume that P is the identity. Now we define $V_i \subseteq \mathbb{E}^n$ as the image of the matrix

$$\operatorname{diag}(\overrightarrow{1}_{q_1}, \ldots, \overrightarrow{1}_{q_i}, \overrightarrow{0}_{q_{i+1}}, \ldots, \overrightarrow{0}_{q_t}) \in \mathbb{M}_m(\mathbb{E}).$$

Certainly the flag $V_0 \subseteq \cdots \subseteq V_t$ satisfies the last condition. We claim that every V_i is a submodule. Otherwise, there exists an element $\overline{v} \in V_i$, for some i, and an element $\overline{h} \in \mathbb{H}$ such that $\overline{h}\overline{v} \notin V_i$. Now take pre-images $h \in \mathfrak{H}$ and $v \in \widetilde{V}_i$ of $\overline{h}$ and $\overline{v}$ respectively, where $\widetilde{V}_i \subseteq \mathcal{O}_E^m$ is the image of the matrix

$$\operatorname{diag}(\overrightarrow{1}_{q_1}, \ldots, \overrightarrow{1}_{q_i}, \overrightarrow{0}_{q_{i+1}}, \ldots, \overrightarrow{0}_{q_t}) \in \mathbb{M}_m(\mathcal{O}_E).$$

Then $\pi_E^{r_i} v \in D\mathcal{O}_E^m$, whence $h(\pi_E^{r_i} v) \in D\mathcal{O}_E^m$. Since conjugation by π_E leaves $\mathfrak{D}$ invariant, then $\pi_E^{-r_i} h \pi_E^{r_i}$ is an integral matrix with reduction $\hat{h}$. Since $h(\pi_E^{r_i} v) \in D\mathcal{O}_E^m$, then

$$\pi_E^{-r_i} h(\pi_E^{r_i} v) \in \pi_E^{-r_i}(D\mathcal{O}_E^m) \cap \mathcal{O}_E^m \subseteq \widetilde{V}_i + \pi_E \mathcal{O}_E^m,$$

whence $\hat{h}(\overline{v}) \in V_i$. Since V_i is generated by $V_{i\mathbb{K}} = V_i \cap \mathbb{K}^m$, where $\mathbb{K}$ is the residue field of K, we may assume that $\overline{v} \in \mathbb{K}^m$. Note that $\hat{h}$ is the image of $\overline{h}$ under an automorphism $\sigma \in \operatorname{Gal}(\mathbb{E}/\mathbb{K})$, and since $\overline{v} \in \mathbb{K}^m$, we have $\hat{h}(\overline{v}) = \sigma[\overline{h}(\overline{v})]$. Since σ fixes $V_{i\mathbb{K}}$ point-wise, then necessarily $\sigma(V_i) = V_i$. It follows that $\hat{h}(\overline{v}) \in V_i$ if and only if $\overline{h}(\overline{v}) \in V_i$. This contradicts the choice of $\overline{v}$. $\qquad\square$

LEMMA 3.2. — *Let $\mathfrak{H}$ be a suborder of the maximal order $\mathfrak{D} = \mathbb{M}_m(\mathcal{O}_E)$, and let $\mathbb{H}$ be its image in $\mathbb{M}_m(\mathbb{E})$. Assume that there is an $\mathbb{H}$-module $V \subseteq \mathbb{E}^m$ of dimension r. Then there exists a local generator u for $\mathfrak{D}|\mathfrak{H}$ whose reduced norm generates the ideal (π_K^{m-r}).*

Proof. — Let $M \in \mathbb{M}_m(\mathbb{E})$ be a matrix of rank r. We claim that M has a pre-image $\tilde{M}$ in $\mathbb{M}_m(\mathcal{O}_E)$, satisfying the following conditions:

- $\tilde{M}$ is invertible in $\mathbb{M}_m(E)$.

- The reduced norm $n(\tilde{M})$ is a generator of the ideal (π_K^{m-r}).
- $\pi_E \tilde{M}^{-1} \in \mathbb{M}_m(\mathcal{O}_E)$ and its reduction $L \in \mathbb{M}_m(\mathbb{E})$ satisfies $\mathrm{Im}(M) = \ker(L)$.

To define the lifting $\tilde{M}$ we write $M = PDQ$, where P and Q are invertible in $\mathbb{M}_m(\mathbb{E})$ and $D = \mathrm{diag}(\vec{1}_r, \vec{0}_{m-r})$, then chose arbitrary liftings $\tilde{P}$ and $\tilde{Q}$ in $\mathbb{M}_m(\mathcal{O}_E)^*$, and finally set $\tilde{M} = \tilde{P}\tilde{D}\tilde{Q}$, where $\tilde{D} = \mathrm{diag}(\vec{1}_r, \pi_E \vec{1}_{m-r}) \in \mathbb{M}_m(\mathcal{O}_E)$. Then

$$\pi_E \tilde{M}^{-1} = (\pi_E \tilde{Q}^{-1} \pi_E^{-1}) \Big(\mathrm{diag}(\pi_E \vec{1}_r, \vec{1}_{m-r}) \Big) \tilde{P}^{-1} \in \mathbb{M}_m(\mathcal{O}_E).$$

Note that the matrix $\pi_E \tilde{Q}^{-1} \pi_E^{-1}$ is invertible in $\mathbb{M}_m(\mathcal{O}_E)$, whence the reduction L of $\pi_E \tilde{M}^{-1}$ has the right rank. The last condition follows now if we prove $LM = 0$, but this is clear since it is the reduction of $\pi_E \tilde{M}^{-1} \tilde{M} = \pi_E \, \mathrm{Id}$.

Let M be a projection matrix with image V and let L be as above. Then M has rank r and satisfies $LXM = 0$ for every $X \in \mathbb{H}$, since X leaves $V = \mathrm{Im}(M)$ invariant. We claim that $\tilde{M}$ is a generator for $\mathfrak{D}|\mathfrak{H}$, this concludes the proof. Since every element $X \in \mathbb{H}$ leaves the $\mathbb{E}$-vector space $V = M(\mathbb{E}^m)$ invariant, then every element x of $\mathfrak{H}$ must leave invariant its pre-image, i.e., the module $\tilde{M}(\mathcal{O}_E^m) + \pi_E \mathcal{O}_E^m$. Now we have

$$\pi_E \mathcal{O}_E^m = \tilde{M}(\tilde{M}^{-1} \pi_E \mathcal{O}_E^m) \subseteq \tilde{M} \mathcal{O}_E^m,$$

since $\tilde{M}^{-1} \pi_E = \pi_E^{-1} (\pi_E \tilde{M}^{-1}) \pi_E \in \mathbb{M}_m(\mathcal{O}_E)$. As this implies $x(\tilde{M} \mathcal{O}_E^m) \subseteq \tilde{M} \mathcal{O}_E^m$ for any $x \in \mathfrak{H}$, we conclude that $\tilde{M}$ is a generator. The result follows. $\square$

LEMMA 3.3. — *Let $\mathfrak{H}$ be a suborder of the maximal order $\mathfrak{D} = \mathbb{M}_m(\mathcal{O}_E)$ and let $\mathbb{H}$ be its image in $\mathbb{M}_m(\mathbb{E})$. Assume that every irreducible representation of the $\mathbb{E}$-algebra $\mathbb{E}\mathbb{H}$ has dimension d. Then there exists a local generator for $\mathfrak{D}|\mathfrak{H}$ whose reduced norm generates (π_K^s) if and only if d divides s.*

Proof. — On one hand, assume d divides s. Since conjugation by any power of π_E leaves $\mathfrak{D}$ invariant and the reduced norm of the diagonal matrix $\pi_E 1_{\mathfrak{A}}$ spans the ideal (π_K^m), we may assume $0 \leqslant s < m$. It suffices to show that there exists a $\mathbb{H}$-submodule of $\mathbb{E}^m$ of dimension $m - s$. By the representation theory for finite dimensional algebras, there exists a composition series

$$\{0\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{m/d} = \mathbb{E}^m$$

where the submodule V_i has dimension di, and the result follows. On the other hand, if there exists a local generator for $\mathfrak{D}|\mathfrak{H}$ whose reduced norm

spans (π_K^s), then there exists a sequence of submodules $V_1, \ldots, V_t$ and integers $r_1, \ldots, r_t$ as in Lemma 3.1 satisfying $s = \sum_i r_i \dim_{\mathbb{E}}(V_i/V_{i-1})$. Refining the sequence if needed, we may assume it is a composition series, whence $\dim_{\mathbb{E}}(V_i/V_{i-1}) = d$ for every i, and therefore d divides s. $\qquad\square$

Next result is now immediate from the previous lemma:

LEMMA 3.4. — Let $\mathfrak{H}$ be a suborder of $\mathfrak{D} = \mathbb{M}_m(\mathcal{O}_E)$ and let $\mathbb{H}$ be its image in $\mathbb{M}_m(\mathbb{E})$. Assume that any irreducible representation of the $\mathbb{E}$-algebra $\mathbb{E}\mathbb{H}$ has the same degree d. Then the set of reduced norms of generators for $\mathfrak{D}|\mathfrak{H}$ is $\lceil (\mathfrak{D}|\mathfrak{H}) = K^{*d}\mathcal{O}_K^*$.

The results in this section seem to indicate that the existence of a representation field depends only on the dimensions of the representations of the algebra $\mathbb{E}\mathbb{H}$. This is not so, as illustrated by Example 3.6. It holds, however, when $\mathfrak{H}$ is the largest order with reduction $\mathbb{H}$ as next lemma shows.

LEMMA 3.5. — Let $\mathfrak{H} = p^{-1}(\mathbb{H})$ be a suborder of $\mathfrak{D} = \mathbb{M}_m(\mathcal{O}_E)$, where $\mathbb{H}$ is a subalgebra of $\mathbb{M}_m(\mathbb{E})$ and $p : \mathbb{M}_m(\mathcal{O}_E) \to \mathbb{M}_m(\mathbb{E})$ the usual projection. Then there exists a local generator for $\mathfrak{D}|\mathfrak{H}$ whose reduced norm generates (π_K^s) if and only if there exists an $\mathbb{H}$-module $V \subseteq \mathbb{E}^m$ of dimension t, where $m - t$ is the remainder of s when divided by m.

Proof. — It suffices to prove that if u is a generator whose reduced norm generates (π_K^s) then there exists an $\mathbb{H}$-module V of dimension t. Since u is a generator, we have $\mathfrak{H}(u\mathcal{O}_E^m) \subseteq u\mathcal{O}_E^m$. Post-multiplying u by a power of π_E we may assume $u\mathcal{O}_E^m \subseteq \mathcal{O}_E^m$, but $u\mathcal{O}_E^m$ is not contained in $\pi_E\mathcal{O}_E^m$. Since $\mathfrak{H}$ contains every matrix of the form $\pi_E a$ with $a \in \mathfrak{D}$, we conclude that $\pi_E\mathcal{O}_E^m \subseteq u\mathcal{O}_E^m$. It follows that $u = PDQ$ where P and Q are units in $\mathbb{M}_m(\mathcal{O}_E)$ and $D = \mathrm{diag}(\pi_E \vec{1}_r, \vec{1}_d)$. Let V be the image of $u\mathcal{O}_E^m$ in $\mathbb{E}^m$. It follows that $\dim_{\mathbb{E}} V = d$ while on the other hand the reduced norm of u generates (π_K^r), so that $r = s$. It follows that $d = m - r = t$, since they are congruent modulo m and $0 < d, t \leqslant m$. $\qquad\square$

Example 3.6. — Let $\mathfrak{A} = \mathbb{M}_n(K)$ and let $L = \{a \in \mathfrak{A}|ae_1 \in Ke_1\}$, where $\{e_1, \ldots, e_n\}$ is the canonical basis of K^n. Let I be an integral ideal, i.e., a sub-lattice of $\mathcal{O}_X$, and let $\mathfrak{H} = \mathfrak{H}(I)$ be the order

$$\mathfrak{H}(I) = \left(L \cap \mathbb{M}_n(\mathcal{O}_X)\right) + \mathbb{M}_n(I),$$

where $\mathbb{M}_n(I)$ is the sheaf defined by $\mathbb{M}_n(I)(U) = \mathbb{M}_n\left(I(U)\right)$ for any affine set U and $\mathbb{M}_n(\mathcal{O}_X)$ is defined analogously.

The set of reductions $\mathbb{H}_\wp$ depends only on the primes $\wp$ such that $I_\wp \neq \mathcal{O}_\wp$, but this is not so for the set of norms of generators. In fact, if $I_\wp$ is

the maximal ideal of $\mathcal{O}_\wp$, then Lemma 3.5 applies and any local generator at $\wp$ must have reduced norm in $\mathcal{O}_\wp^* K_\wp^{*n}$ or $\pi_\wp^{n-1} \mathcal{O}_\wp^* K_\wp^{*n}$. In particular, if $I = \wp$ and if $[\wp, \Sigma/K]$ has order at least 3 in the Galois group $\mathrm{Gal}(\Sigma/K)$, then the representation field does not exist. However, if $I_\wp = (\pi_\wp^t)$, then $\mathrm{diag}\left(\pi_\wp^{-s}, \vec{1}_{n-1}\right) = \mathrm{diag}(\pi_\wp^{-s}, 1, \ldots, 1)$ is a generator for any $s \leqslant t$. In particular, if $t = t(\wp)$ is big enough for every prime $\wp$ dividing I, then the representation fields is defined.

4. Proof of Theorem 1.1

LEMMA 4.1. — *Let R be a commutative ring that is complete with respect to an ideal J. Then any idempotent $P \in R/J$ can be lifted to an idempotent $\tilde{P} \in R$.*

Proof. — Let P_1 an arbitrary lifting of P to R and define recursively $P_{n+1} = P_n + (1 - 2P_n)(P_n^2 - P_n)$. Note that

$$P_{n+1}^2 - P_{n+1} = (P_n^2 - P_n)\left[1 - (1 - 2P_n)^2[1 - (P_n^2 - P_n)]\right].$$

Since $(1 - 2P_n)^2 = 1 + 4(P_n^2 - P_n) \equiv 1$ (modulo J), we prove by recursion that $P_n^2 - P_n \in J^n$ and the result follows by completeness. $\qquad\square$

LEMMA 4.2. — *Let $\mathfrak{H}$ be an commutative order in a local central simple algebra $\mathfrak{A}$ and let $\mathfrak{P}$ be the sub-order generated by the idempotents of $\mathfrak{H}$. Let C be the centralizer of $\mathfrak{P}$ in $\mathfrak{A}$. Write $\mathfrak{H}$ as a direct product $\mathfrak{H} = \prod_{i \in I} \mathfrak{H}_i$ with $\mathfrak{H}_i$ connected. Then we have a decomposition $C = \prod_{i \in I} C_i$, where every C_i is a central simple algebra. Furthermore, there exist a family of maximal orders $\{\mathfrak{D}_i\}_{i \in I}$, with $\mathfrak{H}_i \subseteq \mathfrak{D}_i \subseteq C_i$ and a maximal order $\mathfrak{D} \subseteq \mathfrak{A}$ such that*

$$\lceil(\mathfrak{D}|\mathfrak{H}) \supseteq \prod_{i \in I} \lceil(\mathfrak{D}_i|\mathfrak{H}_i).$$

Proof. — If $\mathfrak{H} = \prod_{i \in I} \mathfrak{H}_i$ as above, we let P_i be the idempotent corresponding to the factor $\mathfrak{H}_i$. Then P_i is a central idempotent in C, whence there exists a decomposition of C as above where $C_i \cong P_i C$. Assume $\mathfrak{A} = \mathbb{M}_m(E)$, where E is a division algebra. Note that $E^m = \prod_i P_i E^m$ as either left C-modules or right E-modules. By taking an E-basis of each $P_i E^m$, we obtain a basis of E^m in which the order $\mathfrak{P}$ is the ring of diagonal

matrices of the form

$$
\begin{pmatrix}
a_1 I_{q_1} & 0 & \cdots & 0 \\
0 & a_2 I_{q_2} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \vdots & a_r I_{q_r}
\end{pmatrix}, \quad a_1, \dots, a_r \in \mathcal{O}_K,
$$

where I_q is the q by q identity matrix. It follows that C is the algebra of matrices of the form

$$
A = \begin{pmatrix}
A_1 & 0 & \cdots & 0 \\
0 & A_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \vdots & A_r
\end{pmatrix}, \quad A_i \in \mathbb{M}_{q_i}(E).
$$

We can identify $C_i \cong \mathbb{M}_{q_i}(E)$ with the set of matrices A, as above, such that $A_j = 0$ for $j \neq i$. In particular C_i is central simple. By a suitable change of basis in every $P_i E^m$, we can assume $\mathfrak{H}_i \subseteq \mathbb{M}_{q_i}(\mathcal{O}_E)$. Now we can choose $\mathfrak{D} = \mathbb{M}_m(\mathcal{O}_E)$ and $\mathfrak{D}_i = \mathbb{M}_{q_i}(\mathcal{O}_E)$ for $i = 1, \dots, r$.

Let $u_i \in C_i^*$ be a generator for $\mathfrak{D}_i | \mathfrak{H}_i$ as defined in § 2, for every i. Then $u = \sum_i u_i \in C^*$ is a generator for $\mathfrak{D} | \mathfrak{H}$, since

$$
\mathfrak{H} = \prod_i \mathfrak{H}_i \subseteq \prod_i (u_i \mathfrak{D}_i u_i^{-1}) = u \left(\prod_i \mathfrak{D}_i \right) u^{-1} \subseteq u \mathfrak{D} u^{-1}.
$$

Furthermore, from the explicit description of C given above we see that the reduced norm of u is $n(u) = \prod_i n(u_i)$. Now the conclusion follows. $\square$

Now we are ready to prove the following generalization of Theorem 1.1.

PROPOSITION 4.3. — *Let X be an A-curve and let K be the field of functions of X. Let $\mathfrak{A}$ be a central simple K-algebra. Let $\mathfrak{H}$ be an arbitrary commutative order in $\mathfrak{A}$. Let $\mathfrak{D}$ be a maximal order containing $\mathfrak{H}$. For every place $\wp \in X$ we let $I_\wp$ be the only maximal two-sided ideal of the completion $\mathfrak{D}_\wp$, and let $\mathbb{H}_\wp$ be the image of $\mathfrak{H}$ in $\mathfrak{D}_\wp / I_\wp$. Let $\mathbb{E}_\wp$ be the center of the ring $\mathfrak{D}_\wp / I_\wp$. Let $t_\wp$ be the greatest common divisor of the dimensions of the irreducible $\mathbb{E}_\wp$-representations of the algebra $\mathbb{E}_\wp \mathbb{H}_\wp$. Then the representation field $F(\mathfrak{H})$ is the maximal subfield F of the spinor class field Σ such that the inertia degree $f_\wp(F/K)$ divides $t_\wp$, for every place $\wp$.*

Proof. — We let $\overline{\mathbb{H}}_\wp$ be the quotient of $\mathbb{H}_\wp$ by its radical. In particular, $\overline{\mathbb{H}}_\wp = \mathfrak{H}_\wp / J$ for an ideal J such that $J^n \subseteq \pi_E \mathfrak{D}$ for some n. It follows that $\mathfrak{H}_\wp$ is complete with respect to J, so any idempotent in $\overline{\mathbb{H}}_\wp$ can be lifted to an idempotent in $\mathfrak{H}_\wp$ by Lemma 4.1. We conclude that the image $\overline{\mathbb{H}}_i$ of

every $\mathfrak{H}_i$ in $\overline{\mathbb{H}}_\wp$, defined as in last lemma, has no idempotents and therefore $\overline{\mathbb{H}}_i$ is a field since $\overline{\mathbb{H}}_\wp$ is semisimple. It follows from Lemma 3.4 that the image of the local generators for each $\mathfrak{H}_i$ is $\lceil_\wp(\mathfrak{D}_i|\mathfrak{H}_i) = K_\wp^{*d_i}\mathcal{O}_\wp^*$, where every d_i is the dimension of the corresponding representation. On the other hand, by Lemma 3.1 we get the contention $\lceil_\wp(\mathfrak{D}|\mathfrak{H}) \subseteq K_\wp^{*t_\wp}\mathcal{O}_\wp^*$. Note that

$$K_\wp^{*t_\wp}\mathcal{O}_\wp^* = \prod_i K_\wp^{*d_i}\mathcal{O}_\wp^* = \prod_i \lceil_\wp(\mathfrak{D}_i|\mathfrak{H}_i) \subseteq \lceil_\wp(\mathfrak{D}|\mathfrak{H}) \subseteq K_\wp^{*t_\wp}\mathcal{O}_\wp^*,$$

whence equality follows. We conclude that $\lceil_\wp(\mathfrak{D}|\mathfrak{H}) = K_\wp^{*t_\wp}\mathcal{O}_\wp^*$ as claimed.

$\square$

5. Applications and examples

Example 5.1. — Let $\mathfrak{A} = \mathbb{M}_n(K)$ and let $\mathfrak{T}_n$ be the order of all upper triangular matrices of the form

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 0 & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_1 \end{pmatrix}, \quad a_1,\ldots,a_n \in \mathcal{O}_K.$$

Then $\mathbb{H}_\wp$ has only one irreducible representation of dimension 1 for all $\wp$. It follows that $t_\wp = 1$ for all $\wp$ and therefore $F(\mathfrak{T}_n) = K$. We conclude that every maximal order in $\mathbb{M}_n(K)$ contains a copy of the order $\mathfrak{T}_n$.

More generally, for an arbitrary commutative suborder $\mathfrak{H}$, the dimensions of the irreducible representations of $\mathfrak{H}$ are the same as the dimensions of the irreducible representations of the maximal semi-simple suborder $\mathfrak{H}_s$ of $\mathfrak{H}$. Next result follows:

COROLLARY 5.2. — *If $\mathfrak{H}$ is an arbitrary commutative order in the algebra $\mathfrak{A}$, and $\mathfrak{H}_s$ is the maximal semi-simple suborder of $\mathfrak{H}$, then $F(\mathfrak{H}_s) = F(\mathfrak{H})$. In particular, if a maximal order $\mathfrak{D}$ contains a conjugate of $\mathfrak{H}_s$, then there exists an order $\mathfrak{D}'$ in the spinor genus of $\mathfrak{D}$ satisfying $\mathfrak{H} \subseteq \mathfrak{D}'$.*

Recall that the inertia degree $f_\wp(F/K)$ of an unramified abelian extension F/K divides the inertia degree $f_\wp(L/K)$ of an arbitrary extension L/K, at every $\wp$, if and only if $F \subseteq L$. Next result follows (compare to Theorem 4.3.4 in [2]):

COROLLARY 5.3. — *If $\mathfrak{A}$ has no partial ramification outside of S and $\mathfrak{H} = \prod_i \mathfrak{H}_i$, where each $\mathfrak{H}_i$ is the maximal order of a field L_i, then $F(\mathfrak{H}) = \Sigma \cap (\bigcap_i L_i)$.*

Example 5.4. — If $\mathfrak{H}$ is the maximal order in a semi-simple commutative algebra of prime dimension that is not a field, then the greatest common divisor of the degrees $[L_i : K]$ is 1, and therefore $\mathfrak{H}$ is contained in at least one order in every spinor genus.

Example 5.5. — If $\mathfrak{H} = \mathcal{O}_K \times \mathfrak{H}_1$, then $\mathfrak{H}$ is contained in at least one order in every spinor genus.

Recall that a split order in $\mathbb{M}_n(K)$ is an order containing a copy of $\mathcal{O}_K^n = \mathcal{O}_K \times \cdots \times \mathcal{O}_K$ [9]. By applying last example to $\mathfrak{H} = \mathcal{O}_K^n$, we obtain a simple proof of the following generalization of Theorem 5 in [4].

COROLLARY 5.6. — *Every spinor genera of maximal X-orders in $\mathbb{M}_n(K)$ contains an split order. If X is affine, then every maximal order is split.*

An order $\mathfrak{H}$ in $\mathfrak{A}$ is called non-selective if for every spinor genus Φ of maximal orders, there exists an order $\mathfrak{D} \in \Phi$ containing $\mathfrak{H}$. An order $\mathfrak{H} \subseteq \mathfrak{A}$ is selective if it is not non-selective. This is the natural generalization of the concept of selective order defined in [5] and [6]. Assume now $[L : K] = p$ is a prime, and $\mathfrak{A}$ has no partial ramification, so if $\mathfrak{L}$ is the maximal order of L, Corollary 5.3 applies and $F(\mathfrak{L}) = \Sigma \cap L$. Since $[L : K]$ is a prime, the order $\mathfrak{L}$ is selective if and only if $L \subseteq \Sigma$. In this case the order is contained in $1/p$ of all conjugacy classes. Assume this is the case and let $\mathfrak{H} \subseteq \mathfrak{L}$ be an arbitrary suborder. Then $\mathfrak{H}$ is non-selective if and only if there is a place $\wp$ that is inert for L/K such that the image of $\mathfrak{H}$ in the residue field $\mathbb{L}_\wp$ coincide with the residue field $\mathbb{K}_\wp$ of K, since in this case $t_\wp = 1$, so $F(\mathfrak{H})$ splits at $\wp$, and therefore $F(\mathfrak{H}) = K$. Since the condition is equivalent to $\wp$ dividing the relative discriminant of $\mathfrak{H}/\mathcal{O}_K$, next result follows:

COROLLARY 5.7. — *Let $\mathfrak{A}$ be a central simple algebra without partial ramification and let $\mathfrak{L}$ be the maximal order of a field L of prime degree over K. Then $\mathfrak{L}$ is selective in $\mathfrak{A}$ if and only if $L \subseteq \Sigma$. In this case a suborder $\mathfrak{H} \subseteq \mathfrak{L}$ is selective unless there is a inert place of L/K dividing the relative discriminant of $\mathfrak{H}$ over $\mathcal{O}_K$.*

Note that we no longer require that $\dim_K \mathfrak{A} = p^2$ in the above result (see [5] and [6]). More generally, the field L always contains F, whence we have next result:

COROLLARY 5.8. — *Let $\mathfrak{A}$ be a central simple algebra without partial ramification and let $\mathfrak{H}$ be an order contained in a field $L \subseteq \mathfrak{A}$. Let N be the total number of spinor genera. Then*

$$\sharp\left\{\Phi \in \overline{\mathbb{O}}\,\middle|\,\exists\mathfrak{D} \in \Phi \text{ such that } \mathfrak{H} \subseteq \mathfrak{D}\right\} = \frac{N}{d},$$

for some divisor d of [L : K].

BIBLIOGRAPHY

[1] L. Arenas-Carmona, "Spinor class fields for sheaves of lattices", Preprint, arXiv:1009.3280v1 [math.NT] 16 Sep 2010.

[2] ———, "Applications of spinor class fields: embeddings of orders and quaternionic lattices", *Ann. Inst. Fourier (Grenoble)* **53** (2003), no. 7, p. 2021-2038.

[3] ———, "Relative spinor class fields: a counterexample", *Arch. Math. (Basel)* **91** (2008), no. 6, p. 486-491.

[4] C. Chevalley, *L'arithmétique sur les algèbres de matrices*, Herman, Paris, 1936.

[5] T. Chinburg & E. Friedman, "An embedding theorem for quaternion algebras", *J. London Math. Soc.* **60** (1999), no. 2, p. 33-44.

[6] B. Linowitz & T. R. Shemanske, "Embedding orders into central simple algebras", Preprint, arXiv:1006.3683v1 [math.NT] 18 Jun 2010.

[7] O. T. O'Meara, *Introduction to quadratic forms*, Academic press, New York, 1963.

[8] I. Reiner, *Maximal orders*, Academic press, London, 1975.

[9] T. R. Shemanske, "Split orders and convex polytopes in buildings", *J. Number Theory* **130** (2010), no. 1, p. 101-115.

[10] A. Weil, *Basic Number Theory*, second ed., Springer Verlag, Berlin, 1973.

Luis ARENAS-CARMONA
Universidad de Chile
Departamento de matematicas
Facultad de ciencia
Casilla 653
Santiago (Chile)
learenas@u.uchile.cl