ACTA ARITHMETICA
156.2 (2012)

Representation fields for cyclic orders

by

LUIS ARENAS-CARMONA (Santiago)

1. Introduction. Let K be a number field. Let $\mathfrak{A}$ be a central simple K-algebra, or K-CSA, satisfying the following condition:

CONDITION E (Eichler Condition). Either $\dim_K \mathfrak{A} = n^2 > 4$, or $\dim_K \mathfrak{A} = 4$ and $\mathfrak{A}$ splits at some infinite place.

Let Σ be the spinor class field for the set $\mathbb{O}$ of maximal orders in $\mathfrak{A}$ as defined in [Ar1]. This is an abelian extension that classifies maximal orders of $\mathfrak{A}$, in the sense that there exists an explicit map $\rho : \mathbb{O} \times \mathbb{O} \to \mathrm{Gal}(\Sigma/K)$ with the following properties:

- $\mathfrak{D}$ and $\mathfrak{D}'$ are conjugate if and only if $\rho(\mathfrak{D}, \mathfrak{D}') = \mathrm{Id}_\Sigma$.
- $\rho(\mathfrak{D}, \mathfrak{D}'') = \rho(\mathfrak{D}, \mathfrak{D}')\rho(\mathfrak{D}', \mathfrak{D}'')$ for all $(\mathfrak{D}, \mathfrak{D}', \mathfrak{D}'') \in \mathbb{O}^3$

(see [Ar1, §3]). Furthermore, for certain classes of orders $\mathfrak{H}$ in $\mathfrak{A}$ there exists a representation field $F = F(\mathfrak{H}) \subseteq \Sigma$ satisfying the following conditions:

- If $\mathfrak{H} \subseteq \mathfrak{D} \cap \mathfrak{D}'$ then $\rho(\mathfrak{D}, \mathfrak{D}')|_F = \mathrm{Id}_F$.
- If $\mathfrak{H} \subseteq \mathfrak{D}$ and $\rho(\mathfrak{D}, \mathfrak{D}')|_F = \mathrm{Id}_F$ then $\mathfrak{H}$ is contained in a conjugate of $\mathfrak{D}'$.

In particular, if the representation field $F(\mathfrak{H})$ is known, we can answer the following question:

QUESTION R. Which orders in $\mathbb{O}$ contain a copy of the order $\mathfrak{H}$?

Some arithmetic properties of the orders $\mathfrak{D}$ and $\mathfrak{H}$ can be reduced to particular cases of Question R. We give some examples in §5 below. Additional examples can be found in [Ar1] or [Ar5]. Question R is also of interest in the theory of hyperbolic varieties, as arithmetical Kleinian and Fuchsian groups can be described in terms of maximal orders [B]. The existence of

2010 *Mathematics Subject Classification*: Primary 11R52, 16G30; Secondary 11R56, 11R37, 16G10.
Key words and phrases: maximal orders, central simple algebras, spinor genera, spinor class fields.

DOI: 10.4064/aa156-2-3

a representation field F for $\mathfrak{H}$ implies that the number of conjugacy classes of maximal orders containing a conjugate of $\mathfrak{H}$ divides the total number of conjugacy classes. More precisely, the proportion of conjugacy classes whose orders contain copies of $\mathfrak{H}$ is $[F:K]^{-1}$. When Condition E fails, this number can still be interpreted as the proportion of spinor genera Φ of maximal orders containing at least one order $\mathfrak{D} \in \Phi$ representing $\mathfrak{H}$.

The first known result that is equivalent to the existence of a representation field is due to Chevalley [C], who studied the case in which $\mathfrak{A}$ is a matrix algebra and $\mathfrak{H}$ is the ring of integers in a maximal subfield of $\mathfrak{A}$. This result was extended by Chinburg and Friedman [CF1] to the case in which $\mathfrak{A}$ is a quaternion algebra and $\mathfrak{H}$ is a commutative suborder. Both works considered only embeddings of commutative suborders into maximal orders ([1]). One advantage of the use of representation fields is that sometimes they have a simple expression in terms of the algebra $L = K\mathfrak{H}$. This is in particular true when $\mathfrak{H}$ is the maximal order in a maximal subfield L of a matrix algebra $\mathfrak{A}$. In fact, Chevalley's result can be written $F(\mathfrak{H}) = L \cap \Sigma$. This was extended in [Ar1] under the assumption that the algebra $\mathfrak{A}$ has no partial ramification, i.e., it is locally either a matrix algebra $\mathbb{M}_n(K_\wp)$ or a division algebra.

The formula $F = L \cap \Sigma$ does not hold in general when $\mathfrak{A}$ has partial ramification, but the representation field is well defined for all commutative orders [Ar5]. In fact, Lemma 2.1 in §2 allows us to compute, for any suborder $\mathfrak{H}$, the lower representation field $F_-(\mathfrak{H}) := \Sigma_-(\mathfrak{D}|\mathfrak{H})$ defined in [Ar1, §3]. When $F(\mathfrak{H})$ is defined, we have $F_-(\mathfrak{H}) = F(\mathfrak{H})$. In [Ar4] we computed the representation field for a suborder of the type $\mathcal{O}_K[x,y]$ where x and y are standard generators of an n^2-dimensional cyclic algebra $\mathfrak{A}$, over a field K containing a primitive nth root of unity η. In other words, the powers x^n and y^n are in the ring $\mathcal{O}_K$ of algebraic integers in K and $xy = \eta yx$. The condition $x^n, y^n \in \mathcal{O}_K$ is necessary for the ring $\mathcal{O}_K[x,y]$ to be an order. In the present work we prove the existence of representation fields for a wider family of orders, that includes those in [Ar4], and also maximal orders in central simple subalgebras. Our main results are Theorems 1.4 and 1.10.

For the sake of completeness, we also consider the function field case, where K is the field of rational functions on a smooth projective curve C over a finite field $\mathbb{F}$. This can be done by fixing a finite set S of places in an arbitrary global field K and stating the results for S-orders. When K is a number field we must assume that S contains the archimedean places. All the preceding definitions extend to this setting, except that Condition E must be replaced by the following generalization:

([1]) There exist some partial generalizations to embeddings of commutative orders into some particular types of non-maximal orders in the quaternionic case [CX], [GQ], [M], [L].

Condition GE. The set S contains a place $\wp$ such that $\mathfrak{A}_\wp$ is not a division algebra.

Additionally, we consider the projective case, where lattices and orders are defined as modules over the structure sheaf $\mathcal{O}_C$ of the projective curve C. In this case, by definition, $S = \emptyset$. This case is interesting for a number of reasons. Isomorphism classes of maximal C-orders in an n-dimensional matrix algebra are in correspondence with isomorphism classes of vector bundles over C up to tensor product with invertible bundles. In other words, the vector bundles E and $E \otimes_{\mathcal{O}_C} L$, where L is invertible, correspond to isomorphic maximal orders. These bundles are of interest in coding theory [N], [J]. Some algebraic properties of the bundles are related to whether or not the corresponding maximal orders represent some particular suborders (§5). Certainly, no analog of Condition GE holds in this case, but the theory still gives information about spinor genera that can be recovered on affine subsets.

The spinor genus of the order associated to a vector bundle is an interesting invariant in its own right. J.-P. Serre [S, Ch. II] has used the theory of vector bundles to describe a quotient of the local Bruhat–Tits tree which can be used to find generators for arithmetic subgroups of the general linear group $\mathrm{GL}_n(K(C))$. This theory has been applied to the study of elliptic sheaves [Pa], which are related to Drinfeld modules [BS]. The vertices of these graphs correspond to bundles that coincide in the complement of one place ∞. In fact, the maximal orders corresponding to these bundles represent every isomorphism class in an explicit set of spinor genera. The theory of representations by spinor genera can be applied to simplify the task of explicitly describing these quotient graphs.

In all that follows we denote by X an A-curve with field of functions K as defined in [Ar5], i.e., X is either $\mathrm{Spec}(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}_{K,S}$ is the ring of S-units in K, for a finite set S of places, or a smooth projective curve whose field of functions is K. In the latter case, $S = \emptyset$, and $\mathcal{O}$ denotes the structure sheaf $\mathcal{O}_X$. We leave the notations $\mathcal{O}_K$ or $\mathcal{O}_X$ only for specific examples. In any case, we denote by $|X| = S^c$ the set of closed points in X, or equivalently, the set of finite places of K. Lattices, orders and fractional ideals are to be understood as $\mathcal{O}$-modules in either context. As in [Ar5], all our results are stated in the context of spinor genera, so that Condition GE is not needed in their statement. In this general setting, the map ρ defined above can only classify orders up to spinor genera. However, when strong approximation holds for the universal cover of $\mathrm{Aut}(\mathfrak{A})$, spinor genera coincide with conjugacy classes [Ar1, §2], and strong approximation for this group is equivalent to Condition GE (see [K], [Pr]).

A global cyclic order $\mathfrak{H}$ of degree m is the order generated by a commutative order $\mathfrak{H}_0$, and a one-dimensional lattice $\mathfrak{I}y$, satisfying the following conditions:

- $F = K\mathfrak{H}_0$ is an m-dimensional separable commutative K-algebra.
- $y^m \in K$ and the map $x \mapsto yxy^{-1}$ is an automorphism of order m in F whose fixed subalgebra is K.
- $\mathfrak{I}$ is a fractional ideal in K, and $y\mathfrak{H}_0 y^{-1} = \mathfrak{H}_0$.

The algebra $\mathfrak{A}_0 \subseteq \mathfrak{A}$ generated by a cyclic order is called a *cyclic algebra* and it is a CSA. In fact, every CSA over a global field has this form [PY, §3.4]. Our definition of cyclic algebra is slightly different from the one in the literature, e.g. [KMRT, §30.A], but we prove in Lemma 3.2 that both definitions coincide. The definition of local cyclic order is analogous to the global definition. We call an order $\mathfrak{H}$ *locally cyclic* if every completion $\mathfrak{H}_\wp$ is cyclic. Any global cyclic order is locally cyclic.

Example 1.1. Let X be a smooth irreducible projective curve over a finite field, with field of functions $K = K(X)$. Let x and y be generators of a K-CSA $\mathfrak{A}$ satisfying $a = x^n \in K$, $b = y^n \in K$, and $xy = \eta yx$ for a primitive nth root of unity $\eta \in K$. In particular, we assume that the characteristic of K does not divide n. The sheaf of rings $\mathcal{O}_X[x, y]$ is an order only when a and b are constants, which forces $\mathfrak{A}$ to be a matrix algebra. However, for any pair $\{x, y\}$ as above, the sheaf of rings $\mathcal{O}_X[\mathfrak{I}x, \mathfrak{I}y]$ is an order as soon as $a\mathfrak{I}^n$ and $b\mathfrak{I}^n$ are contained in $\mathcal{O}_X$. They can be chosen to make the order $\mathcal{O}_X[\mathfrak{I}x, \mathfrak{I}y]$ maximal only if the principal divisors $\mathrm{div}(a)$ and $\mathrm{div}(b)$ are nth powers in the Picard group of X.

Example 1.2. If K is a number field, then the number field analog $\mathcal{O}_{K,S}[\mathfrak{I}x, \mathfrak{I}y]$ of the previous example generalizes the order $\mathcal{D}(a, b)$ defined in [CF2] and [Ar3].

Example 1.3. Let K be the maximal real subfield of the cyclotomic field $\mathbb{Q}(\mu_n)$, for $n > 2$. Let $\mathfrak{A}_0$ be a quaternion division algebra over K that is split by the quadratic extension $\mathbb{Q}(\mu_n)/K$. Let $\mathfrak{H} = \mathcal{O}_K[x, y]$ be an order generated by an nth root of unity x in $\mathfrak{A}_0$ and a pure quaternion y inducing the complex conjugation on $K(x)$. Then $\mathfrak{H}$ is a cyclic order.

In this paper we prove:

Theorem 1.4. *Let $\mathfrak{A}$ be a CSA and let $\mathfrak{A}_0 \subseteq \mathfrak{A}$ be an m^2-dimensional CSA. Let $\mathfrak{H} \subseteq \mathfrak{A}_0$ be an order of maximal rank. Assume that at every finite place $\wp \in |X|$, at least one of the following conditions holds:*

1. *The local order $\mathfrak{H}_\wp$ is maximal in $\mathfrak{A}_{0\wp}$.*
2. *The local order $\mathfrak{H}_\wp$ is cyclic, and $K_\wp$ contains a primitive mth root of unity.*

Then the representation field $F(\mathfrak{H})$ is defined.

In fact, the field $F(\mathfrak{H})$ can be computed by the same formula given in [Ar5] for the commutative case, as we prove in Lemma 2.1 below.

COROLLARY 1.5. *If $\mathfrak{H}$ is the maximal order of $\mathfrak{A}_0$, then the representation field is defined.* ∎

COROLLARY 1.6. *If $\mathfrak{H}$ is a locally cyclic order and K contains a primitive mth root of unity, then the representation field is defined. In particular, the conclusion holds if $\mathfrak{H}$ is a cyclic order and K contains a primitive mth root of unity.* ∎

COROLLARY 1.7. *Let $\mathfrak{J}$ and $\mathfrak{I}$ be fractional ideals, i.e., 1-dimensional lattices in K. If $\mathfrak{H} = \mathcal{O}[\mathfrak{J}x, \mathfrak{I}y]$ is an order in the central simple algebra $\mathfrak{A}$ such that the elements x and y satisfy $x^m, y^m \in K$ and $xy = \eta yx$ for a primitive mth root of unity $\eta \in K$, then the representation field $F(\mathfrak{H})$ is defined.* ∎

Note that Corollary 1.7 generalizes the results in [Ar4], even in the number field case when $\mathfrak{I} = \mathfrak{J} = \mathcal{O}$, since we no longer require that $m = n$.

EXAMPLE 1.8. In [CF2] and [Ar3], the distance $\rho(\mathfrak{H}_1, \mathfrak{H}_2)$ was explicitly computed for the orders $\mathfrak{H}_i = \mathcal{D}(a_i, b_i)$, which are orders of the type $\mathfrak{H}_i = \mathcal{O}_{K,S}[\mathfrak{J}_i x_i, \mathfrak{I}_i y_i]$ as in Corollary 1.7. The references assume that these orders are maximal. In fact, for arbitrary orders $\mathfrak{H}_1$ and $\mathfrak{H}_2$ of this type, the set of distances

$$\{\rho(\mathfrak{D}_1, \mathfrak{D}_2) \mid (\mathfrak{D}_1, \mathfrak{D}_2) \in \mathbb{O}^2,\ \mathfrak{H}_1 \subseteq \mathfrak{D}_1,\ \mathfrak{H}_2 \subseteq \mathfrak{D}_2\}$$

is a coset in $\mathrm{Gal}(\Sigma/K)/\mathrm{Gal}(\Sigma/F)$, where $F = F(\mathfrak{H}_1) \cap F(\mathfrak{H}_2)$. In particular, the distance between $\mathfrak{H}_1$ and $\mathfrak{H}_2$ can be defined as an element of $\mathrm{Gal}(F/K)$.

EXAMPLE 1.9. Let $\mathfrak{A}_0 \subseteq \mathfrak{A}$ be two CSAs. Let $\mathfrak{B}$ be a maximal order in $\mathfrak{A}_0$ and let $\mathfrak{L} \subseteq \mathfrak{B}$ be a cyclic order of maximal rank in $\mathfrak{A}_0$. Let $\mathfrak{I}$ be an integral ideal such that, at every place $\wp \in |X|$, we have either $\mathfrak{L}_\wp \supseteq \mathfrak{I}_\wp \mathfrak{B}_\wp$ or $\mathfrak{I}_\wp = \mathcal{O}_\wp$. Then if $\mathfrak{H} = \mathfrak{L} + \mathfrak{I}\mathfrak{B}$, Theorem 1.4 shows that the representation field $F(\mathfrak{H})$ is defined.

In fact, the local condition for $\mathfrak{I}$ is unnecessary, since we have:

THEOREM 1.10. *Let $\mathfrak{A}$ be a CSA, let $\mathfrak{A}_0 \subseteq \mathfrak{A}$ be an m^2-dimensional CSA, and let $\mathfrak{B}$ be a maximal order in $\mathfrak{A}_0$. Let $\mathfrak{H} \subseteq \mathfrak{B}$ be an order satisfying the hypotheses of Theorem 1.4, and let $\mathfrak{H}' \subseteq \mathfrak{B}$ be another order satisfying $\mathfrak{H}_\wp + \wp\mathfrak{B}_\wp = \mathfrak{H}'_\wp + \wp\mathfrak{B}_\wp$ for every place $\wp \in |X|$. Then the representation field $F(\mathfrak{H}')$ is defined, and in fact $F(\mathfrak{H}') = F(\mathfrak{H})$.*

It is however not true for arbitrary orders $\mathfrak{H}$ that the existence of a representation field depends only on the local orders $\mathfrak{H}_\wp + \wp\mathfrak{B}_\wp$ [Ar5, Example 3.6].

2. Representation fields and residual algebras. Let K be a global field and let $\mathfrak{A}$ be a K-CSA. Let J_K be the idele group of K and, for any vector space or algebraic group Y, denote by $Y_{\mathbb{A}}$ the corresponding adelization [PR, Chapter 5]. Similarly, when Λ is a lattice in a vector space V we denote by $\Lambda_{\mathbb{A}}$ the group $\prod_{\wp\in|X|}\Lambda_\wp\times\prod_{\wp\in S}V_\wp$. Note that $\Lambda_{\mathbb{A}}$ is the closure of Λ in $V_{\mathbb{A}}$ if $S\neq\emptyset$. This notation is applied in particular to orders. For any maximal order $\mathfrak{D}$, the *spinor class field* Σ is the class field corresponding to the class group $K^*H(\mathfrak{D})$, where $H(\mathfrak{D})=\{n(a)\mid a\mathfrak{D}_{\mathbb{A}}a^{-1}=\mathfrak{D}_{\mathbb{A}},\ a\in\mathfrak{A}_{\mathbb{A}}\}$, and $n:\mathfrak{A}^*_{\mathbb{A}}\to J_K$ denotes the reduced norm on ideles.

Recall that a maximal order $\mathfrak{D}'$ is said to be *in the genus of* $\mathfrak{D}$ when

$$\mathfrak{D}'_{\mathbb{A}}=a\mathfrak{D}_{\mathbb{A}}a^{-1} \tag{2.1}$$

for some adelic element a, while they are said to be *in the same spinor genus* if a can be chosen of the form $a=bc$, where $b\in\mathfrak{A}$ is a global element, while c is an adelic element with trivial reduced norm. The distance map ρ is defined by $\rho(\mathfrak{D},\mathfrak{D}')=[a,\Sigma/K]$, where a is any adelic element satisfying (2.1), and $x\mapsto[x,\Sigma/K]$ denotes the Artin map on ideles. The map ρ thus defined classifies maximal orders up to spinor equivalence. In particular, when strong aproximation holds, $\rho(\mathfrak{D},\mathfrak{D}')$ is trivial if and only if the orders $\mathfrak{D}$ and $\mathfrak{D}'$ are globally conjugate [Ar5, §2]. Analogously, let $H(\mathfrak{D}|\mathfrak{H})=\{n(a)\mid a\mathfrak{H}_{\mathbb{A}}a^{-1}\subseteq\mathfrak{D}_{\mathbb{A}},\ a\in\mathfrak{A}^*_{\mathbb{A}}\}\subseteq J_K$. We say that the representation field $F(\mathfrak{H})$ *is defined* if any of the following equivalent conditions holds:

- The set $K^*H(\mathfrak{D}|\mathfrak{H})\subseteq J_K$ is a group.
- The set $\Phi=\{\rho(\mathfrak{D},\mathfrak{D}')\mid\mathfrak{H}\subseteq\mathfrak{D}'\}\subseteq\mathrm{Gal}(\Sigma/K)$ is a group.

When this is the case, $F(\mathfrak{H})$ is the class field corresponding to $K^*H(\mathfrak{D}|\mathfrak{H})$, or equivalently, the fixed field Σ^{Φ}. The representation field is not always defined, but it is defined for some important families of orders. (In fact [Ar2] is mostly devoted to describing a counterexample.)

More generally, for every order $\mathfrak{H}\subseteq\mathfrak{D}$, we can define two intermediate subfields:

- The lower representation field $F_-(\mathfrak{H})$ is the fixed field $\Sigma^{\langle\Phi\rangle}$ of the group $\langle\Phi\rangle$ generated by Φ. It is the largest subfield F satisfying $\rho(\mathfrak{D}',\mathfrak{D}'')|_F=\mathrm{Id}_F$ whenever $\mathfrak{H}\subseteq\mathfrak{D}'\cap\mathfrak{D}''$.
- The upper representation field $F^-(\mathfrak{H})$ is the fixed field $\Sigma^{\mathcal{N}}$ of the group $\mathcal{N}=\{\sigma\in\mathrm{Gal}(\Sigma/K)\mid\sigma\Phi=\Phi\}$.

Note that $F^-(\mathfrak{H})\supseteq F_-(\mathfrak{H})$, since Φ contains the identity, and the representation field is defined if and only if $F^-(\mathfrak{H})=F_-(\mathfrak{H})$. When $\mathfrak{H}$ is a commutative order contained in a maximal subfield L, it is easy to prove that $L\supseteq F^-(\mathfrak{H})$, and this is the reason why the proportion of spinor genera containing a copy of $\mathfrak{H}$ is 1, 0, or 1/2 in the quaternionic case [CF1]. In this section we give a formula for $F_-(\mathfrak{H})$ valid for every suborder $\mathfrak{H}$. This is a generalization of the results in [Ar5]. For any finite place $\wp \in |X|$ we denote by $I_\wp$ the unique maximal two-sided ideal of $\mathfrak{D}$ containing $\wp 1_{\mathfrak{A}}$, and define the residual algebra $\mathbb{H}_\wp$ as the image of $\mathfrak{H}$ in $\mathfrak{D}/I_\wp$. Note that $\mathfrak{A}_\wp \cong \mathbb{M}_f(E)$ for some division algebra E with ring of integers $\mathcal{O}_E$ and residue field $\mathbb{E}_\wp$, so that we can always assume $\mathfrak{D}_\wp = \mathbb{M}_f(\mathcal{O}_E)$, and therefore $\mathfrak{D}/I_\wp \cong \mathbb{M}_f(\mathbb{E}_\wp)$.

LEMMA 2.1. *Let K, $\mathfrak{A}$ and $\mathfrak{D}$ be as above. For any suborder $\mathfrak{H}$ of $\mathfrak{D}$, the lower representation field $F_-(\mathfrak{H})$ is the maximal subfield F of Σ whose inertia degree $f_\wp(F/K)$ divides the dimension of all irreducible representations of the $\mathbb{E}_\wp$-algebra $\mathbb{E}_\wp\mathbb{H}_\wp$. Furthermore, if for every $\wp \in |X|$, all irreducible representations have the same degree, then $F(\mathfrak{H})$ is defined.*

Proof. Set $H(\mathfrak{H}|\mathfrak{D}) = \prod_\wp H_\wp(\mathfrak{H}|\mathfrak{D})$, where $H_\wp(\mathfrak{H}|\mathfrak{D})$ is the set of norms of local generators as defined in [Ar5], so in particular $H_\wp(\mathfrak{D}) = H_\wp(\mathfrak{D}|\mathfrak{D})$. Recall that an element $u \in \mathfrak{A}_\wp^*$ is called a *local generator* if $u\mathfrak{H}_\wp u^{-1} \subseteq \mathfrak{D}_\wp$. Let $d_1, \ldots, d_r$ be the dimensions of the irreducible representations of the algebra $\mathbb{H}_\wp$, and let d be their greatest common divisor. It suffices to prove that, for every place $\wp \in |X|$, the set $H_\wp(\mathfrak{D}|\mathfrak{H})$ spans the product $\prod_{i=1}^r \mathcal{O}_\wp^* K_\wp^{*d_i} = \mathcal{O}_\wp^* K_\wp^{*d}$ locally at all places, while $H_\wp(\mathfrak{D}|\mathfrak{H}) = \mathcal{O}_\wp^* K_\wp^{*d}$ when the dimensions are equal. For this, we prove the following three statements:

1. For any local generator u for $\mathfrak{D}_\wp|\mathfrak{H}_\wp$ we have $n(u) \in \mathcal{O}_\wp^* K_\wp^{*d}$.
2. There exist local generators $u_1, \ldots, u_k$ such that the greatest common divisor of the valuations $v_\wp(n(u_1)), \ldots, v_\wp(n(u_k))$ is exactly d.
3. If $d_1 = \cdots = d_r = d$, then there is a local generator $\tilde{u}_t$ such that $v_\wp(n(\tilde{u}_t)) = td$ for every integer t.

Since $\mathcal{O}_\wp^* \subseteq n(\mathfrak{D}_\wp^*) \subseteq H_\wp(\mathfrak{D})$, and therefore $\mathcal{O}_\wp^* H_\wp(\mathfrak{D}|\mathfrak{H}) = H_\wp(\mathfrak{D}|\mathfrak{H})$ [Ar1, Lemma 3.2], this finishes the proof.

The statements can be proved as in [Ar5, Lemmas 3.1–3.2]. Here we give a simplified argument. Assume $\mathfrak{A}_\wp \cong \mathbb{M}_f(E)$, where E is a local central division algebra with uniformizing parameter π_E. Let u be a local generator. Write $u = PDQ$ where $P, Q \in \mathfrak{D}^*$ and D is a diagonal matrix of the form $\mathrm{diag}(\pi_E^{r_1}, \ldots, \pi_E^{r_f})$ with $r_1 \le r_2 \le \cdots$, as in [Ar5]. Replacing $\mathfrak{H}$ by $P\mathfrak{H}P^{-1}$ if needed, we can assume $u = D$. Let x be an arbitrary element in $\mathfrak{H}$ and let $\bar{x}$ be its image in the residual algebra $\mathbb{H}_\wp$. The condition $uxu^{-1} \in \mathfrak{D}$ implies that x belongs to the order

$$\begin{pmatrix} \mathcal{O}_E & \mathcal{O}_E & \cdots & \mathcal{O}_E \\ \pi_E^{r_2-r_1}\mathcal{O}_E & \mathcal{O}_E & \cdots & \mathcal{O}_E \\ \vdots & \vdots & \ddots & \vdots \\ \pi_E^{r_N-r_1}\mathcal{O}_E & \pi_E^{r_N-r_2}\mathcal{O}_E & \cdots & \mathcal{O}_E \end{pmatrix}.$$

We conclude that $\bar{x}$ has the form

$$(2.2)\qquad \begin{pmatrix} X_1 & * & \cdots & * \\ 0 & X_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X_k \end{pmatrix},$$

where the size s_i of the square matrix X_i is independent of x, and therefore is the dimension of a representation of the residual algebra. Now note that $n(u) = v\pi_K^{r_1+\cdots+r_e} = v\pi_K^{r_{i(1)}s_1+\cdots+r_{i(k)}s_k}$, where $i(1) = 1$, $i(t) = s_1 + \cdots + s_{t-1} + 1$ for $t > 1$, and v is a unit. The first statement follows. Conversely, if every element in $\mathbb{H}_\wp$ has the form (2.2), then every diagonal matrix of the form

$$u_t = \mathrm{diag}(\underbrace{1, \ldots, 1}_{s_1+\cdots+s_t}, \underbrace{\pi_E, \ldots, \pi_E}_{s_{t+1}+\cdots+s_k}),$$

is a generator, and $v_\wp(n(u_t)) = s_{t+1}+\cdots+s_k$. The second statement follows, since the sets $\{s_1, \ldots, s_k\}$ and $\{s_1 + \cdots + s_k, \ldots, s_{k-1} + s_k, s_k\}$ have the same greatest common divisor. The last statement is similar. Assume that $s_1 = \cdots = s_k = d$, so that in particular $dk = f$, and write $t = kl + r$ with $0 \le r < k$. Then set $\tilde{u}_t = \pi_E^l u_{k-r}$, where u_{k-r} is as above. ∎

Example 2.2. Let $K, \mathfrak{A}_0$, and $\mathfrak{H}$ be as in Example 1.3. Note that, for any $\wp \in |X|$, the irreducible representations of the residue algebra $\mathbb{H}_\wp = \mathbb{K}_\wp[\bar{x}, \bar{y}]$, where $\bar{x}$ and $\bar{y}$ are the images of x and y, have dimension 2 unless one of the following conditions holds:

1. $y^2 \in \wp$, i.e., $\bar{y}^2 = 0$, and $\wp$ splits or ramifies in $\mathbb{Q}(\mu_n)/K$.
2. $\bar{y}^2 \in \mathbb{K}_\wp^{*2}$, and $\bar{x}^2 = \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = 1_{\mathbb{H}_\wp}$.

The second condition can occur only if n is p^r or $2p^r$, where p is the rational prime in $\wp$. Note that $yx = x^{-1}y$, so that their images generate a matrix algebra whenever they fail to commute, by Lemma 3.2 below. The representation field $F(\mathfrak{H})$, in this case, is the maximal subfield of the representation field $F(\mathfrak{B})$, of a maximal order $\mathfrak{B}$ of $\mathfrak{A}_0$, splitting at all places for which either condition is satisfied.

3. Algebraic lemmas

Lemma 3.1. *Let F and $H = \mathbb{M}_r(L)$ be two commuting subalgebras of a K-algebra A. Assume F is a direct product of isomorphic Galois field extensions of K and the same holds for L. Then FH is isomorphic to a cartesian product ring $(\mathbb{M}_r(E))^m$ for some integer m and some field E depending only on the isomorphism type of the factors of F and H.*

Proof. There exists a surjection $\phi : F \otimes_K H \to FH$, and every quotient of a direct product of CSAs is isomorphic to a direct subproduct. It suffices, therefore, to prove the result for the tensor product $F \otimes_K H \cong \mathbb{M}_r(F \otimes_K L)$. Since $\mathbb{M}_r(A\times B) \cong \mathbb{M}_r(A)\times\mathbb{M}_r(B)$, the result follows if we prove that $F\otimes_K L$ is a direct product of isomorphic fields. It follows from [Re, Th. 7.18] that $F \otimes_K L \cong \prod_i E_i$ is a product of fields. We conclude that each E_i is generated by a quotient of F and a quotient of L, and since all extensions considered are Galois, there exists a unique extension of K with that property, so all E_i are isomorphic. ∎

LEMMA 3.2. *Let k be a field. Let L be a separable commutative subalgebra of a K-algebra A. Assume that $z \in A^*$ satisfies $b = z^m \in K^*$, and conjugation by z induces an automorphism of order m on L fixing only the elements of K. Then the algebra $B = K[z, L]$ is isomorphic to the m^2-dimensional cyclic algebra (L, b) as defined in* [Al, §IV.1]. *In particular, B is a CSA.*

Proof. It is rather straightforward that $B = \sum_{i=0}^{m-1} Lz^i$, so it suffices to prove that the sum is direct and $\dim_K(L) = m$ [Al, §IV.1]. By extending scalars if needed, we can assume K is algebraically closed, so in particular, L is isomorphic to the product ring $K^t = K \times \cdots \times K$. Since the fixed subspace of the map $x \mapsto zxz^{-1}$ is one-dimensional, this map must cyclically permute the minimal idempotents in L and therefore $t = m$. It follows that L and z satisfy the same relations as the generators of a matrix algebra. We conclude that B is isomorphic to a quotient of a matrix algebra, and therefore to a matrix algebra since matrix algebras are simple. In particular, this proves that the sum $B = \sum_{i=0}^{m-1} Lz^i$ is direct since this is the case for the generators of a matrix algebra. ∎

LEMMA 3.3. *Let $\mathbb{K}$ be a finite field. Let L be a semisimple commutative subalgebra of a $\mathbb{K}$-algebra A. Assume that $\mathbb{K}$, L, and $y \in A^*$ satisfy the following conditions:*

- *$y^m \in \mathbb{K}$ and $yLy^{-1} = L$.*
- *y acts transitively on minimal idempotents of L by conjugation.*
- *$\mathbb{K}$ contains the group* (2) *$\mu_m = \{\eta \in \overline{\mathbb{K}} \mid \eta^m = 1\}$.*

Then the quotient of the algebra $B = \mathbb{K}[y, L]$ by its radical is isomorphic to a direct product of matrix algebras of the same dimension over a fixed field extension of $\mathbb{K}$.

Proof. Without loss of generality, we may assume that B is semisimple. Let $b = y^m \in \mathbb{K}$. The conjugation action of $\langle y\rangle$ on L has no non-trivial invariant idempotent. In particular, if E is the centralizer $C_L(y)$, then E

(2) Note that we are not assuming here that m is relatively prime to the characteristic of $\mathbb{K}$.

contains neither nilpotent elements nor non-trivial idempotents. We conclude that E is a field. Let s be the smallest positive integer such that y^s commutes with L, so in particular s divides m. Let $F = E[y^s] = E \cdot \mathbb{K}[y^s]$. Since F is central in B, it must be semisimple. In particular $\mathbb{K}[y^s]$ is a direct product of fields of the form $\mathbb{K}[\beta_i]$ with $\beta_i^{m/s} = b$. Since $\mu_m \subseteq \mathbb{K}$, we see that $\mathbb{K}[y^s]$ is a direct product of isomorphic fields, and the same holds for F by Lemma 3.1. Let $P_1, \ldots, P_s$ be the minimal idempotents of F, so that $F \cong \prod_{i=1}^{s} F_i$ is the product of the fields $F_i = P_i F$. Since F is central in B, we also have $B \cong \prod_{i=1}^{s} B_i$ for $B_i = P_i B$.

Let F' be the centralizer $C_{L[y^s]}(y)$. We claim that in fact $F = F'$. From the claim, it follows that F_i is the centralizer of $y_i = P_i y$ in $L_i = P_i L[y^s]$, and therefore $B_i \cong (L_i, y_i^s) \cong \mathbb{M}_s(F_i)$ by the previous lemma and [W, §I.1, Th. 1]. The result follows.

To prove the claim, we note that $L[y^s]$ is a quotient of $L \otimes_{\mathbb{K}} \mathbb{K}[y^s]$ and, since the latter is a product of isomorphic fields as before, the former can be identified with $P(L \otimes_{\mathbb{K}} \mathbb{K}[y^s])$ for some idempotent P. The map $T : L \to L$ defined by $T(x) = yxy^{-1}$ extends to $L \otimes_{\mathbb{K}} \mathbb{K}[y^s]$ by extension of scalars, and the eigenspace corresponding to $1 \in \mathbb{K}$ is $E \otimes_{\mathbb{K}} \mathbb{K}[y^s]$. Since T is invertible and well defined in the quotient $L[y^s]$, we have $T(P) = P$, and the eigenspace corresponding to 1 in $L[y^s]$ is $P(E \otimes_{\mathbb{K}} \mathbb{K}[y^s]) = E[y^s] \subseteq L[y^s]$. ∎

4. Proof of Theorems 1.4 and 1.10. Theorem 1.4 is proved by showing that the last condition of Lemma 2.1 above holds locally at all places. This is proved in Lemmas 4.1 and 4.2 below. Theorem 1.10 follows since the order $\mathfrak{H}'$ satisfies the condition in Lemma 2.1 at a given place $\wp \in |X|$, for some $d = d(\wp)$, if and only if $\mathfrak{H}$ does.

Lemma 4.1. *In the notation of Theorem* 1.4, *if for some* $\wp \in |X|$, *the order* $\mathfrak{H}_\wp$ *is a maximal order of the local CSA* $\mathfrak{A}_{0\wp}$, *then the last condition of Lemma* 2.1 *holds at* $\wp$.

Proof. Let $\mathfrak{A}_{0\wp} = \mathbb{M}_r(B)$ for a local division algebra B. Then $\mathfrak{H}_\wp \cong \mathbb{M}_r(\mathcal{O}_B)$ where $\mathcal{O}_B$ is the unique maximal order of B. Let $\mathbb{H}_\wp$ be as defined in Lemma 2.1 and let $\overline{\mathbb{H}}_\wp$ be the quotient of $\mathbb{H}_\wp$ by its radical. We claim that $\overline{\mathbb{H}}_\wp \cong \mathbb{M}_r(\mathbb{B})$ where $\mathbb{B}$ is the residue field of B. It follows that $\overline{\mathbb{E}}_\wp \overline{\mathbb{H}}_\wp$ is a direct product of isomorphic matrix algebras by Lemma 3.1. This finishes the proof.

To prove the claim we observe that the filter generated by the powers of the maximal two-sided ideal m_B of $\mathcal{O}_B$ converges to 0, whence any finite image of m_B under a continuous homomorphism of $\mathcal{O}_B$ is nilpotent. The same holds therefore for the two-sided ideal $I = \mathbb{M}_r(m_B)$ in $\mathfrak{H}_\wp$. We conclude that the image of I in $\overline{\mathbb{H}}_\wp$ must be trivial, and the claim follows since $\mathbb{M}_r(\mathcal{O}_B)/I \cong \mathbb{M}_r(\mathbb{B})$ is simple. ∎

LEMMA 4.2. *If $\mathfrak{H}_\wp = \mathcal{O}_\wp[\mathfrak{H}_{0\wp}, \mathfrak{I}_\wp y]$ is a local cyclic algebra as defined in* §1, *and if $K_\wp$ contains a primitive mth root of unity, then the last condition of Lemma* 2.1 *holds at $\wp$.*

Proof. Assume $\mathfrak{H}_\wp$ is a cyclic order of degree m. The local fractional ideal $\mathfrak{I}_\wp$ must be of the form $\mathfrak{I}_\wp = (\pi_\wp^{t(\wp)})$ for some $t(\wp) \in \mathbb{Z}$. Replacing y by $\pi_\wp^{t(\wp)} y$ if needed, we can assume $\mathfrak{I}_\wp = \mathcal{O}_\wp$. Since $\mathfrak{H}_\wp$ is a lattice, the element $b = y^m \in K_\wp$ must belong to $\mathcal{O}_\wp$.

First assume that the image $\beta \in \mathbb{K}_\wp$ of b vanishes. Then the image $Y \in \mathbb{H}_\wp$ of y is in the radical of $\mathbb{H}_\wp$, whence the quotient $\overline{\mathbb{H}}_\wp$ of $\mathbb{H}_\wp$ by its radical coincides with the image $\overline{\mathbb{H}}_{0\wp}$ of the commutative order $\mathfrak{H}_{0\wp}$. We claim that every irreducible representation of this algebra has the same dimension. The result follows in this case.

Now we prove the claim. By [Re, Th. 6.18] every idempotent of the ring $\mathbb{H}_{0\wp}$ can be lifted to an idempotent of $\mathfrak{H}_{0\wp}$ and therefore of the algebra $L = K_\wp \mathfrak{H}_{0\wp}$. Conjugation by y cannot leave invariant an element of $L \backslash K_\wp$, whence it must permute transitively all the minimal idempotents in L. Hence, if $\mathbb{H}_{0\wp}$ is written as a product $\prod_i \mathbb{L}_i$ of algebras $\mathbb{L}_i$ with no idempotents, then there is an automorphism of $\mathbb{H}_{0\wp}$ that transitively permutes the algebras $\mathbb{L}_i$. It follows that the quotient of the ring $\mathbb{H}_{0\wp}$ by its nilradical $\mathbb{R}_{0\wp}$ is a direct product of isomorphic fields $\widehat{\mathbb{H}_{0\wp}} = \prod_i \widehat{\mathbb{L}_i}$. The same must hold, by Lemma 3.1, for the algebra $\widetilde{\mathbb{E}}_\wp \widetilde{\mathbb{H}}_{0\wp} = \mathbb{E}_\wp \mathbb{H}_{0\wp} / \mathbb{E}_\wp \mathbb{R}_{0\wp}$, where $\widetilde{\mathbb{H}}_{0\wp}$ and $\widetilde{\mathbb{E}}_\wp \cong \mathbb{E}_\wp$ are the images of $\mathbb{H}_{0\wp}$ and $\mathbb{E}_\wp$, since every extension of finite fields is Galois, and $\widetilde{\mathbb{H}}_{0\wp}$ is a quotient of $\widehat{\mathbb{H}_{0\wp}}$.

Now we assume that b is a unit in $\mathcal{O}_\wp$, and therefore the image Y of y in $\mathbb{H}_\wp$ is invertible. Let $\mathbb{H}_{0\wp}$ be the image of $\mathfrak{H}_{0\wp}$ in $\mathbb{H}_\wp$. It follows as in the previous case that the quotient $\widehat{\mathbb{H}_{0\wp}}$ of $\mathbb{H}_{0\wp}$ by its radical $\mathbb{R}_{0\wp}$ is the product of isomorphic fields $\prod_i \widehat{\mathbb{L}_i}$. Let $\mathbb{R}_\wp$ be the two-sided ideal of $\mathbb{H}_\wp$ spanned by $\mathbb{R}_{0\wp}$. Since conjugation by Y preserves $\mathbb{R}_{0\wp}$, it follows from a straightforward computation that $\mathbb{R}_\wp$ is nilpotent. Furthermore, the image $\overline{\mathbb{H}_{0\wp}}$ of $\mathbb{H}_{0\wp}$ in $\overline{\mathbb{H}_\wp} = \mathbb{H}_\wp / \mathbb{R}_\wp$ is a quotient of $\widehat{\mathbb{H}_{0\wp}}$, and therefore it is also a product of isomorphic fields. The image $\overline{Y}$ of Y in $\overline{\mathbb{H}_\wp}$ permutes transitively the minimal idempotents of $\overline{\mathbb{H}_{0\wp}}$, since they all can be lifted to idempotents of $\mathfrak{H}_\wp$ [Re, Th. 6.18]. It follows from Lemma 3.3 that $\overline{\mathbb{H}_\wp}$ is a direct product of isomorphic matrix algebras, since we are assuming that $K_\wp$ contains a primitive mth root of unity. Now the result follows by Lemma 3.1 as before. ∎

5. Applications and examples

Matrix rings and orders. The theory of representation fields can be used to study some structural properties of maximal orders in matrix algebras. In [Ar5, Corollary 3] we proved that every spinor genus of maximal orders in a matrix algebra contains a split order, i.e., an order that has a decomposition of the form

$$\begin{pmatrix} \mathcal{O} & J_{1,2} & \cdots & J_{1,n} \\ J_{2,1} & \mathcal{O} & \cdots & J_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ J_{n,1} & J_{n,2} & \cdots & \mathcal{O} \end{pmatrix},$$

where each $J_{i,j}$ is an ideal, i.e., a 1-dimensional lattice in K. A consequence of Theorem 1.4 is the following:

PROPOSITION 5.1. *Let* $\mathfrak{A} = \mathbb{M}_m(B)$ *where* B *is a CSA, let* $\mathfrak{B}$ *be a maximal order in* B*, and let* $\mathfrak{D}_0 = \mathbb{M}_m(\mathfrak{B})$*. Then a spinor genus* $\mathrm{Spin}(\mathfrak{D})$ *contains* $\mathbb{M}_m(\mathfrak{R})$*, for some order* $\mathfrak{R}$*, if and only if* $\rho(\mathfrak{D}_0, \mathfrak{D})$ *is trivial on the maximal exponent-*m *subextension of* Σ*.*

Proof. Note that an order $\mathfrak{D}$ has the form $\mathfrak{D} \cong \mathbb{M}_m(\mathfrak{R})$, for some order $\mathfrak{R}$, if and only if $\mathfrak{D}$ represents the order $\mathfrak{H} = \mathbb{M}_m(\mathcal{O})$ by the Matrix Unit Theorem [Ro, p. 30]. Then the residual algebra $\mathbb{H}_\wp$, as defined in §2, is isomorphic to $\mathbb{M}_m(\mathbb{K}_\wp)$, where $\mathbb{K}_\wp$ is the residue field at $\wp$. Since the only irreducible representation of $\mathbb{H}_\wp$ has degree m, the representation field F is the maximal subextension of Σ whose residual degree $f_\wp(F/K)$ divides m for every place $\wp$. Since every element in $\mathrm{Gal}(\Sigma/K)$ is the Frobenius at some place $\wp \in |X|$, it follows that the representation field $F = F(\mathfrak{H})$ is the maximal subfield of the spinor class field Σ having exponent m over K. The result follows. ∎

EXAMPLE 5.2. Let X be the projective line $\mathbb{P}^1(\mathbb{F}_p)$, where $\mathbb{F}_p$ is the field with p elements. In particular, $K = \mathbb{F}_p(t)$. If $\mathfrak{A} = \mathbb{M}_n(K)$, then the spinor class field Σ is the maximal unramified extension of K of exponent n, i.e., $\Sigma = \mathbb{F}_{p^n}(t)$. If $\mathfrak{H}$ is as in Proposition 5.1, then the representation field is $F(\mathfrak{H}) = \mathbb{F}_{p^m}(t)$. It follows that only in n/m of the n spinor genera are there orders of the form $\mathbb{M}_m(\mathfrak{R})$. Let $\wp$ be a point of degree n and $U = X - \{\wp\}$. Then n/m of the n conjugacy classes of maximal $\mathcal{O}_X(U)$-orders in $\mathfrak{A}$ are made of orders of the form $\mathbb{M}_m(\mathfrak{R})$. Note that when $m = n$, there is a unique global order of this form, namely $\mathbb{M}_n(\mathcal{O}_X)$. However, the spinor genus of $\mathbb{M}_n(\mathcal{O}_X)$ contains infinitely many isomorphism classes of maximal orders (Example 5.4 below).

Rings acting on vector bundles. When X is a smooth curve C defined over a finite field $\mathbb{F}$, isomorphism classes of C-lattices on K^n can be identified with isomorphism classes of n-dimensional vector bundles on X [S, §II.2]. In particular, there is a correspondence between isomorphism classes of maximal C-orders in $\mathbb{M}_n(K)$ and isomorphism classes of vector bundles on X up to tensor product with invertible bundles. In this context, split maximal orders correspond to direct sums of one-dimensional vector bundles. Not all maximal orders are split, since not all vector bundles are decomposable (see e.g. [S, §II.2.4.4]). An algebra $A \subseteq \mathbb{M}_n(\mathbb{F})$ acts on a vector bundle E if and only if the C-order $\mathcal{O}_C \otimes_{\mathbb{F}} A$ embeds into the maximal order $\mathfrak{D}_E = \mathcal{E}nd_{\mathcal{O}_C}(E)$ corresponding to E.

EXAMPLE 5.3. If X, $\mathfrak{A}$, and $\mathfrak{H}$ are as in Example 5.2, it follows from previous computations that exactly m of the n spinor genera contain orders corresponding to vector bundles on which the algebra $\mathbb{M}_m(\mathbb{F})$ acts by left multiplication. These are the m-fold products $E = B \times \cdots \times B$ of isomorphic bundles.

EXAMPLE 5.4. Let $\mathfrak{J}$ be a line bundle over X, considered as a 1-dimensional lattice in K. Define $\Lambda_{\mathfrak{J}} = \mathcal{O}_X \times \cdots \times \mathcal{O}_X \times \mathfrak{J}$, a rank-$n$ vector bundle in K^n, and $\mathfrak{D}_{\mathfrak{J}} = \mathcal{E}nd_{\mathcal{O}_X}(\Lambda_{\mathfrak{J}})$, a maximal order in $\mathbb{M}_n(K)$. Let $\{E_{i,j}\}_{i,j}$ be the canonical basis of $\mathbb{M}_n(K)$. Then for any global section $f \in \mathfrak{J}(X) = \Gamma(\mathfrak{J}, X)$ the element $fE_{1,n} \in \mathbb{M}_n(K)$ is a global section in $\mathfrak{D}_{\mathfrak{J}}(X) = \Gamma(\mathfrak{D}_{\mathfrak{J}}, X)$. Since, by the Riemann–Roch Theorem, the dimension of the space of global sections of a line bundle goes to infinity with its degree, the same holds for the maximal orders $\mathfrak{D}_{\mathfrak{J}}$. Note that $\Lambda_{\mathfrak{J}} = b\Lambda_{\mathcal{O}_X}$ for an adelic matrix b whose determinant spans $\mathfrak{J}$. In particular, $\mathfrak{D}_{\mathfrak{J}} = b\mathfrak{D}_{\mathcal{O}_X}b^{-1}$, and therefore $\rho(\mathfrak{D}_{\mathcal{O}_X}, \mathfrak{D}_{\mathfrak{J}}) = [[\mathfrak{J}, \Sigma/K]]$, where $\mathfrak{J} \mapsto [[\mathfrak{J}, \Sigma/K]]$ denotes the Artin map on ideals. It follows that $\mathfrak{D}_{\mathcal{O}_X}$ and $\mathfrak{D}_{\mathfrak{J}}$ are in the same spinor genus as soon as $\mathfrak{J}$ is an nth power, and therefore the spinor genus of $\mathfrak{D}_{\mathcal{O}_X}$ has infinitely many conjugacy classes.

Fractional ideals and representation fields. Representation fields can be applied to the study of the lattice structure of fractional ideals. Let L be an arbitrary n-dimensional K-algebra, and let $\mathfrak{H}$ be an order of maximal rank in L. By a *fractional $\mathfrak{H}$-ideal* in L we mean a lattice Λ of maximal rank in L satisfying $\mathfrak{H}\Lambda = \Lambda$. This extends the usual definition when L is a semisimple commutative algebra and $\mathfrak{H} = \mathcal{O}_L$ is the maximal order. Recall that, if X is affine, every rank-n lattice on K has the form $\mathcal{O}^{n-1} \times I$ for some ideal I of $\mathcal{O}$ [PR, §1.5.3]. Note that the action of L on itself by left multiplication (the regular representation) defines an embedding $\phi : L \to \mathrm{End}_K(L) \cong \mathbb{M}_n(K)$. In this context, we have the following result:

PROPOSITION 5.5. *Assume $\mathfrak{H} \cong \mathcal{O}^{n-1} \times I_0$ as lattices. Then there exists a fractional $\mathfrak{H}$-ideal isomorphic to $\mathcal{O}^{n-1} \times I$ if and only if $[[II_0^{-1}, F/K]] = \mathrm{Id}_F$ where $F \subseteq \Sigma$ is the representation field of $\phi(\mathfrak{H})$.*

Proof. If $\mathfrak{H} \cong \mathcal{O}^{n-1} \times I_0$, and $\Lambda \cong \mathcal{O}^{n-1} \times I$ is an arbitrary lattice in $\mathfrak{A}$, we can write $\Lambda = b\mathfrak{H}$ for a suitable adelic matrix $b \in \mathrm{End}_{\mathbb{A}}(L_{\mathbb{A}}) \cong \mathbb{M}_n(\mathbb{A})$ satisfying $(\det(b)) = II_0^{-1}$, i.e., $\det(b_\wp)$ generates $(II_0^{-1})_\wp$ at every place

$\wp \in |X|$. Let $\mathfrak{D} = \mathrm{End}_{\mathcal{O}}(\Lambda)$ and $\mathfrak{D}_0 = \mathrm{End}_{\mathcal{O}}(\mathfrak{H})$, so that $\mathfrak{D} = b\mathfrak{D}_0 b^{-1}$. We conclude that $\rho(\mathfrak{D}_0, \mathfrak{D}) = [[II_0^{-1}, \Sigma/K]]$, since Σ/K is unramified. On the other hand, Λ is a fractional $\mathfrak{H}$-ideal if and only if $\phi(\mathfrak{H}) \subseteq \mathrm{End}_{\mathcal{O}}(\Lambda)$. The result follows since $\mathfrak{H}$ is a fractional $\mathfrak{H}$-ideal. ∎

EXAMPLE 5.6. The matrix $L = \mathbb{M}_m(K)$ can be identified with a subalgebra of $\mathbb{M}_{m^2}(K)$ via the regular representation. We conclude from Proposition 5.5 and the proof of Proposition 5.1 that, whenever X is affine, every fractional ideal over the order $\mathfrak{H} = \mathbb{M}_m(\mathcal{O})$ is isomorphic as a lattice to $\mathcal{O}^{n-1} \times J$, where the ideal class $[J]$ is an mth power in the ideal class group of $\mathcal{O}$.

Examples of cyclic/non-cyclic orders. Let $\mathfrak{A}_0 \subseteq \mathfrak{A}$ be an m^2-dimensional CSA. Fix a place $\wp$ and assume $\mathfrak{A}_{0\wp}$ can be identified with the ring of matrices $\mathbb{M}_f(B)$ over some local e^2-dimensional division algebra B with maximal order $\mathcal{O}_B$ and uniformizing parameter π_B with $\pi_B^e \in K_\wp$ [W, §I.4, Prop. 5]. Let $T \subseteq \mathfrak{A}_{0\wp}$ be the algebra of upper triangular matrices, and let $\mathfrak{T} = T \cap \mathbb{M}_f(\mathcal{O}_B)$. Let $\mathfrak{H}_\wp = \mathfrak{T} + \pi_B \mathbb{M}_f(\mathcal{O}_B)$. This is an example of a local cyclic order. In fact, $\mathfrak{H}_\wp$ is generated by the order $\mathrm{diag}(\mathcal{O}_F, \ldots, \mathcal{O}_F)$, where F is an unramified maximal subfield of B, and the lattice $\mathcal{O}_\wp y$, where

$$y = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \pi_B & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Note that $y^m = \pi_B^e \,\mathrm{Id}$, and

$$y\,\mathrm{diag}(\lambda_1, \ldots, \lambda_f) y^{-1} = \mathrm{diag}(\lambda_2, \ldots, \lambda_f, \pi_B \lambda_1 \pi_B^{-1}).$$

In this case all irreducible representations of the residual algebra $\mathbb{H}_\wp$ have dimension 1.

Our results can be used to prove that some particular orders are not cyclic. For instance, the next proposition follows from [Ar5, Example 3.6] and Lemma 4.2 above:

PROPOSITION 5.7. *In the notation of* §2, *if* $\mu_n \subseteq K_\wp$, *then no order* $\mathfrak{H}_\wp$ *whose residue image* $\mathbb{H}_\wp$ *is isomorphic to*

$$\left\{ \begin{pmatrix} x & v \\ 0 & A \end{pmatrix} \,\middle|\, x \in \mathbb{K}_\wp,\ v \in \mathbb{K}_\wp^{n-1},\ A \in \mathbb{M}_{n-1}(\mathbb{K}_\wp) \right\}$$

can be a cyclic order.

Finite subgroups of Kleinian or Fuchsian groups. For any maximal order $\mathfrak{D}$ in a quaternion algebra $\mathfrak{A}$, the group $\Gamma_{\mathfrak{D}} = K^*\mathfrak{D}^*/K^*$ embeds into $\mathrm{PSL}_2(\mathbb{C})$ by identifying the completion $K_\wp^*$ at any archimedean place $\wp$

with either $\mathbb{R}$ or $\mathbb{C}$. In general, the image of $\Gamma_{\mathfrak{D}}$ is not a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})$; however, this does hold in some particular cases, namely:

1. if $\wp$ is the unique complex place of K and $\mathfrak{A}$ ramifies at every real place,
2. if K is totally real and $\mathfrak{A}$ ramifies at every archimedean place except $\wp$.

In the first case, any subgroup of $\mathrm{PSL}_2(\mathbb{C})$ commensurable with $\Gamma_{\mathfrak{D}}$ is called an *arithmetic Kleinian group* [MR, p. 257]. In the second case, any subgroup of $\mathrm{PSL}_2(\mathbb{R})$ commensurable with $\Gamma_{\mathfrak{D}}$ is called an *arithmetic Fuchsian group* [MR, p. 259]. The problem of finding finite groups in the arithmetic Kleinian or Fuchsian group $\Gamma_{\mathfrak{D}}$ can be studied in the context of representation fields, as the next example shows:

Example 5.8. Let K, $\mathfrak{A}$, and $\mathfrak{H}$ be as in Example 2.2. Assume that $\mathfrak{A}$ ramifies at every archimedean place of K except one, which we denote by $\wp$. Then, for every maximal order $\mathfrak{D}$, the group $\Gamma_{\mathfrak{D}}$ defined above is an arithmetic Fuchsian group. If y is a unit, then there is an embedding $\Lambda : D_n \to \Gamma_{\mathfrak{D}}$ sending the standard generators a and b of the dihedral group $D_n = \langle a, b \mid a^n = b^2 = e,\ bab = a^{-1}\rangle$ to the classes $\bar{x}$ and $\bar{y}$ respectively. Then a second group $\Gamma_{\mathfrak{D}'}$ contains a conjugate of $\Lambda(D_n)$ if and only if $\mathfrak{D}'$ contains a copy of $\mathfrak{H}$. Note that the conditions can be satisfied whenever K has a unit that is positive only at $\wp$. For example, if $n = 5$ we can take $y^2 = 2 + \sqrt{5}$.

Acknowledgements. This research was partly supported by Fondecyt (grant no. 1100127).

References

[Al] A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. 24, Amer. Math. Soc., New York, 1939.

[Ar1] L. Arenas-Carmona, *Applications of spinor class fields: embeddings of orders and quaternionic lattices*, Ann. Inst. Fourier (Grenoble) 53 (2003), 2021–2038.

[Ar2] L. Arenas-Carmona, *Relative spinor class fields: a counterexample*, Arch. Math. (Basel) 91 (2008), 486–491.

[Ar3] L. Arenas-Carmona, *Arithmetical Hilbert symbols, distance maps and cohomology*, Acta Arith. 140 (2009), 305–315.

[Ar4] L. Arenas-Carmona, *An embedding theorem for orders in central simple algebras*, J. Number Theory 132 (2012), 2474–2480.

[Ar5] L. Arenas-Carmona, *Representation fields for commutative orders*, Ann. Inst. Fourier (Grenoble) 62 (2012), 807–819.

[BS] A. Blum and U. Stuhler, *Drinfeld modules and elliptic sheaves*, in: Vector Bundles on Curves: New Directions, Lecture Notes in Math. 1649, Springer, Berlin, 1997, 110–193.

[B] A. Borel, *Commensurability classes and volumes of hyperbolic 3-manifolds*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 8 (1981), 1–33.

[CX] W. K. Chan and F. Xu, *On representations of spinor genera*, Compos. Math. 140 (2004), 287–300.

[C] C. Chevalley, *L'arithmétique dans les algèbres de matrices*, Hermann, Paris, 1936.

[CF1] T. Chinburg and E. Friedman, *An embedding theorem for quaternion algebras*, J. London Math. Soc. 60 (1999), 33–44.

[CF2] T. Chinburg and E. Friedman, *Hilbert symbols, class groups and quaternion algebras*, J. Théor. Nombres Bordeaux 12 (2000), 367–377.

[GQ] X. Guo and H. Qin, *An embedding theorem for Eichler orders*, J. Number Theory 107 (2004), 207–214.

[J] T. Johnsen, *Rank two bundles on algebraic curves and decoding of Goppa codes*, Int. J. Pure Appl. Math. 4 (2003), 31–42.

[K] M. Kneser, *Strong approximation*, in: Algebraic Groups and Discontinuous Subgroups, Proc. Sympos. Pure Math. 9, Amer. Math. Soc., Providence, RI, 1966, 187–196.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The Book of Involutions*, Amer. Math. Soc. Colloq. Publ. 44, Amer. Math. Soc., Providence, RI, 1998.

[L] B. Linowitz, *Selectivity in quaternion algebras*, J. Number Theory 132 (2012), 1425–1437.

[M] C. Maclachlan, *Optimal embeddings in quaternion algebras*, J. Number Theory 128 (2008), 2852–2860.

[MR] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Springer, New York, 2003.

[N] T. Nakashima, *AG codes from vector bundles*, Des. Codes Cryptogr. 57 (2010), 107–115.

[Pa] M. Papikian, *Local diophantine properties of modular curves of $\mathcal{D}$-elliptic sheaves*, J. Reine Angew. Math. 64 (2012), 115–140.

[PR] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, Boston, 1994.

[PY] V. P. Platonov and V. I. Yanchevskii, *Finite-dimensional division algebras*, in: Algebra IX, Encyclopaedia Math. Sci. 77, Springer, Berlin, 1996, 121–233.

[Pr] G. Prasad, *Strong approximation for semi-simple groups over function fields*, Ann. of Math. 105 (1977), 553–572.

[Re] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

[Ro] L. Rowen, *Ring Theory I*, Academic Press, Boston, 1988.

[S] J.-P. Serre, *Trees*, Springer, Berlin, 1980.

[W] A. Weil, *Basic Number Theory*, 2nd ed., Springer, Berlin, 1973.

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

Received on 7.7.2011
and in revised form on 31.5.2012 (6756)