JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Benjamin LINOWITZ et Thomas R. SHEMANSKE

Embedding orders into central simple algebras

Tome 24, n° 2 (2012), p. 405-424.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_2_405_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 405-424

Embedding orders into central simple algebras

par Benjamin LINOWITZ et Thomas R. SHEMANSKE

Résumé. Soit B une algèbre centrale simple sur un corps de nombres K et L/K une extension finie de corps. Dans la théorie du corps de classes, on étudie les conditions sous lesquelles il existe un plongement de L dans B. Considérons un raffinement subtil de ce problème : soit Ω un ordre d'indice fini dans l'anneau des entiers de L, et R un ordre de rang maximal dans B. Sous quelles conditions existe-t-il un plongement de Ω dans R ? La première réponse à cette question est un résultat élégant de Chevalley [6]. Avec $B = M_n(K)$, $[L : K] = n$ et Ω l'anneau des entiers de L, Chevalley démontre que la proportion des ordres maximaux de B qui admettent un plongement de Ω est $[L \cap \widetilde{K} : K]^{-1}$, où $\widetilde{K}$ est le corps de classe de Hilbert de K. Chinburg et Friedman ([7]) étudient les plongements d'ordres arbitraires d'un corps de nombres quadratique dans des algèbres de quaternions satisfaisant la condition d'Eichler, et Arenas-Carmona [2] considère les plongements de l'anneau des entiers dans les ordres maximaux d'une grande classe d'algèbres centrales simples. Dans cet article, nous considérons les algèbres centrales simples de dimension p^2 où p est un nombre premier impair. Nous démontrons que soit aucune, toutes, ou exactement une des p classes d'isomorphisme des ordres maximaux dans B admettent un plongement d'un ordre Ω commutatif arbitraire d'une extension de K de degré p. Nous caractérisons de manière explicite ces ordres, dits sélectifs. Les corps de classes jouent un rôle central dans cette caractérisation. Un ingrédient important de l'argument de Chinburg et Friedman est la structure de l'arbre des ordres maximaux de SL_2 sur un corps local. Nous généralisons les résultats de Chinburg et Friedman en remplaçant l'arbre des ordres maximaux par l'immeuble affine de Bruhat-Tits pour SL_p.

Abstract. The question of embedding fields into central simple algebras B over a number field K was the realm of class field theory. The subject of embedding orders contained in the ring of integers of maximal subfields L of such an algebra into orders in that algebra is more nuanced. The first such result along those

Manuscrit reçu le 24 janvier 2011, révisé le 18 mars 2011.
Mots clefs. Order, central simple algebra, affine building, embedding.
Classification math. 11R54, 11S45, 20E42.

lines is an elegant result of Chevalley [6] which says that with $B = M_n(K)$ the ratio of the number of isomorphism classes of maximal orders in B into which the ring of integers of L can be embedded (to the total number of classes) is $[L \cap \widetilde{K} : K]^{-1}$ where $\widetilde{K}$ is the Hilbert class field of K. Chinburg and Friedman ([7]) consider arbitrary quadratic orders in quaternion algebras satisfying the Eichler condition, and Arenas-Carmona [2] considers embeddings of the ring of integers into maximal orders in a broad class of higher rank central simple algebras. In this paper, we consider central simple algebras of dimension p^2, p an odd prime, and we show that arbitrary commutative orders in a degree p extension of K, embed into none, all or exactly one out of p isomorphism classes of maximal orders. Those commutative orders which are selective in this sense are explicitly characterized; class fields play a pivotal role. A crucial ingredient of Chinburg and Friedman's argument was the structure of the tree of maximal orders for SL_2 over a local field. In this work, we generalize Chinburg and Friedman's results replacing the tree by the Bruhat-Tits building for SL_p.

1. Introduction

The subject of embedding fields and their orders into a central simple algebra defined over a number field has been a focus of interest for at least 80 years, going back to fundamental questions of class field theory surrounding the proof of the Albert-Brauer-Hasse-Noether theorem as well as work of Chevalley on matrix algebras.

To place the results of this paper in context, we offer a brief historical perspective. A major achievement of class field theory was the classification of central simple algebras defined over a number field, and the Albert-Brauer-Hasse-Noether theorem played a pivotal role in that endeavor. For quaternion algebras, this famous theorem can be stated as:

Theorem. *Let B be a quaternion algebra over a number field K, and let L/K be a quadratic extension of K. Then there is an embedding of L/K into B if and only if no prime of K which ramifies in B splits in L.*

The quaternion case is fairly straightforward to understand since a quaternion algebra over a field is either 2×2 matrices over the field or a (central simple) division algebra. The field extension L/K is necessarily Galois, so the term splits is unambiguous.

In the general setting, we have a central simple algebra B of dimension n^2 over a number field K. From [17] p 236, L/K embeds into B only if $[L : K] \mid n$, and an embeddable extension of degree n is called a strictly maximal extension. The theorem above generalizes as follows. For a number field K, and ν any prime of K (finite or infinite), let K_ν be the completion with respect to ν and let $B_\nu = B \otimes_K K_\nu$ be the local central simple algebra

of dimension n^2 over K_ν. The Wedderburn structure theorem says that $B_\nu \cong M_{\kappa_\nu}(D_\nu)$ where D_ν is a central simple division algebra of dimension m_ν^2 over K_ν, so of course $n^2 = \kappa_\nu^2 m_\nu^2$. We say that the algebra B ramifies at ν iff $m_\nu > 1$, and is split otherwise. The generalization of the classical theorem above follows from Theorem 32.15 of [18] and the corollary on p 241 of [17].

Theorem. *Let the notation be as above, and suppose that* $[L : K] = n$. *Then there is an embedding of* L/K *into* B *if and only if for each prime* ν *of* K *and for all primes* $\mathfrak{P}$ *of* L *lying above* ν, $m_\nu \mid [L_\mathfrak{P} : K_\nu]$.

For example, any extension L/K of degree n will embed in $M_n(K)$ as $m_\nu = 1$ for all ν. So now we turn to the question of embedding orders into central simple algebras which is considerably more subtle. Perhaps the first important result was due to Chevalley [6].

Let K be a number field, $B = M_n(K)$, L/K a field extension of degree n and we may assume (without loss of generality from above) that $L \subset B$. Let $\mathcal{O}_L$ be the ring of integers of L. We know (see exercise 5, p 131 of [18]) that $\mathcal{O}_L$ is contained in some maximal order $\mathcal{R}$ (rank n^2) of B, but not necessarily all maximal orders in B. Chevalley's elegant result is:

Theorem. *The ratio of the number of isomorphism classes of maximal orders in* B *into which* $\mathcal{O}_L$ *can be embedded to the total number of isomorphism classes of maximal orders is* $[\widetilde{K} \cap L : K]^{-1}$ *where* $\widetilde{K}$ *is the Hilbert class field of* K.

In the last decade or so, there have been a number of generalizations of Chevalley's result. In 1999, Chinburg and Friedman [7] considered general quaternion algebras (satisfying the Eichler condition), and arbitrary orders Ω in the ring of integers of an embedded quadratic extension of the center, and proved a ratio of $1/2$ or 1 with respect to maximal orders in the algebra (though the answer is not as simple as Chevalley's). Chan and Xu [5], and independently Guo and Qin [10], again considered quaternion algebras, but replaced maximal orders with Eichler orders of arbitrary level. Maclachlan [14] considered Eichler orders of square-free level, but replaced embeddings into Eichler orders with optimal embeddings. The first author of this paper [13] replaced Eichler orders with a broad class of Bass orders and considered both embeddings and optimal embeddings.

The first work beyond Chevalley's in the non-quaternion setting was by Arenas-Carmona [2]. The setting was a central simple algebra B over a number field K of dimension n^2, $n \geq 3$ with the proviso that the completions of B (at the non-archimedean primes) have the form (in the notation above) $B_\nu \cong M_{\kappa_\nu}(D_\nu)$, $n = \kappa_\nu m_\nu$, with $\kappa_\nu = 1$ or n. He considered embeddings of the ring of integers $\mathcal{O}_L$ of an extension L/K of degree n into maximal orders of B and proves a result (Theorem 1 of [2]) analogous to

Chevalley's with the Hilbert class field replaced by a spinor class field. Indeed, Arenas–Carmona proves and uses the key observation (Lemma 2.0.1 of [2]) that for $n \geq 3$, the set of isomorphism classes of maximal orders in B equals the set of spinor genera in the genus of any maximal order of B, which enables him to leverage results about spinor genera to deduce results about embedding in maximal orders.

In this paper, we too consider generalizations beyond the quaternionic case. We consider the case where B is a central simple algebra having dimension p^2 (p be an odd prime) over a number field K; this part of the setup is of course a special case of the one in [2]. On the other hand, there are other substantive differences between [2] and this work. Like Chinburg and Friedman, we are able to describe the embedding situation for all (full rank) orders $\Omega \subseteq \mathcal{O}_L$ where L/K is a degree p extension of K. As in [7], the question of the proportion of the isomorphism classes of maximal orders which admit an embedding of Ω is not simply dependent on an associated class field as in the case of the maximal order $\mathcal{O}_L$, but also on the relative discriminant (or conductor) of Ω, and it is these considerations which have constrained our consideration to algebras of degree p^2. Moreover, we are able to parametrize the isomorphism classes of maximal orders in the algebra so as to give an explicit description of those maximal orders into which Ω can be embedded, explicit enough to specify them via the local-global correspondence. Also as in [7] we are able to define the notion of a "distance ideal" associated to two maximal orders. We use this distance ideal together with the Artin map associated to L/K to characterize the isomorphism classes of maximal orders into which Ω can be embedded.

Central to the arguments of Chinburg and Friedman are properties of the tree of maximal orders over a local field (the Bruhat-Tits building for SL_2). To accommodate the issue of higher rank, this paper avails itself to the structure of the affine building for SL_p, and introduces new arguments to replace those where the quaternionic case utilized the structure of the building as a tree; smaller accommodations are required since the extension L/K need not be Galois as it is in the quadratic case.

One interesting observation about all the generalizations mentioned above is that class fields have played a central role. We now describe the main result. Since the question of embeddability of fields has been answered above, we presume throughout that L/K is a degree p extension and that $L \subset B$. Let $\mathcal{O}_K$ denote the ring of integers of K, and let Ω denote a commutative $\mathcal{O}_K$-order of rank p in L, so necessarily Ω is an integral domain with field of fractions equal to L. It follows that Ω is contained in a maximal order $\mathcal{R}$ (rank p^2) of B (see p 131 of [18]), so we fix $\mathcal{R}$ for the remainder of this paper. Finally, we define the conductor of Ω as $\mathfrak{f}_{\Omega/\mathcal{O}_K} = \{x \in \mathcal{O}_L \mid x\mathcal{O}_L \subseteq \Omega\}$ (see [16]).

Since we shall use the phrase extensively throughout this paper, we take a moment to explain what we mean when we say an isomorphism class of maximal orders in B admits an embedding of Ω. First suppose that $\mathcal{E}$ is any maximal order in B and $\varphi : \Omega \to \mathcal{E}$ is an embedding. By Skolem-Noether, φ extends to an inner automorphism of B, so $\mathcal{E}$ contains a conjugate of Ω. Since two maximal orders in B are in the same isomorphism class if and only if they are conjugate, if Ω embeds into a maximal order $\mathcal{E}$, then it embeds into every maximal order in the isomorphism class of $\mathcal{E}$, in particular every maximal order in the isomorphism class of $\mathcal{E}$ contains a conjugate of Ω which is generally different for each $\mathcal{E}$. In this case we simply say the isomorphism class of $\mathcal{E}$ admits an embedding of Ω. Thus either every maximal order in an isomorphism class in B contains a conjugate (admits an embedding) of Ω, or no maximal order in the class does.

Via class field theory, we associate an abelian extension $K(\mathcal{R})/K$ to our maximal order $\mathcal{R}$. We find that Ω embeds into every maximal order in B except when the following two conditions are satisfied:

(1) $L \subseteq K(\mathcal{R})$,

(2) Every prime ideal ν of K which divides $N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$ splits in L/K.

When these two conditions hold, precisely one-*pth* of the isomorphism classes of maximal orders admit an embedding of Ω, and those classes are characterized explicitly by means of the Artin map associated to L/K.

Following [7], an order $\Omega \subset \mathcal{R}$ which does not embed in all maximal orders is called selective. In section 3.4, we give examples and show that a degree p division algebra admits no selective orders.

Finally we note that our proof of Proposition 3.4 easily reduces to the case that $\Omega = \mathcal{O}_L$, and so our result could have effectively been quoted from [2] which addresses the maximal order case. But it is in that proposition that we set up and begin to use a recurrent argument involving parametrization of maximal orders which admit an embedding of Ω, so for the sake of clarity, we have given our own argument. Of course, perhaps of independent interest would be to prove that the spinor class field in [2] is the same as our class field $K(\mathcal{R})$, but doing so here would have provided no advantage since our arguments hinge on the characterization we give which requires only a knowledge of central simple algebras and class field theory.

2. Local results

We begin with some results about orders in matrix algebras over local fields. Let k be a non-archimedean local field, with unique maximal order $\mathcal{O}$, V an n-dimensional vector space over k, and identify $\mathrm{End}_k(V)$ with $\mathcal{B} = M_n(k)$, the central simple matrix algebra over k. The ring $M_n(\mathcal{O})$ is a maximal order in $\mathcal{B}$ and can be denoted as the endomorphism ring $\mathrm{End}_{\mathcal{O}}(\mathcal{L})$, where $\mathcal{L}$ is an $\mathcal{O}$-lattice in V of rank n. It is well-known ((17.3), (17.4) of

[18]) that every maximal order in $\mathcal{B}$ has the form $uM_n(\mathcal{O})u^{-1} = \mathrm{End}_{\mathcal{O}}(u\mathcal{L})$ for some $u \in \mathcal{B}^\times$, and is it trivial to check that for another $\mathcal{O}$-lattice $\mathcal{M}$, we have $\mathrm{End}_{\mathcal{O}}(\mathcal{L}) = \mathrm{End}_{\mathcal{O}}(\mathcal{M})$ iff $\mathcal{L}$ and $\mathcal{M}$ are homothetic: $\mathcal{L} = \lambda\mathcal{M}$ for some $\lambda \in k^\times$.

It is also the case that the maximal orders in $\mathcal{B}$ are in one-to-one correspondence with the vertices of the affine building associated to $SL_n(k)$ (see §6.9 of [1], or Chapter 19 of [9]), and so the vertices may be labeled by homothety classes of lattices in V, see p 148 of [3]. To realize such a labeling it is convenient to choose a basis $\{\omega_1, \ldots, \omega_n\}$ of V. This basis, actually the lines spanned by the basis elements, determines an apartment, and each vertex in that apartment can be identified uniquely with the homothety class of a lattice of the form $\mathcal{O}\pi^{a_1}\omega_1 \oplus \cdots \oplus \mathcal{O}\pi^{a_n}\omega_n$, where π is a local uniformizer of k. Since the basis and uniformizer are fixed, we shall denote this homothety class simply by $[a_1, \ldots, a_n]$, $((a_1, \ldots, a_n) \in \mathbb{Z}^n/\mathbb{Z}(1, 1, \ldots, 1))$.

Let $\mathfrak{M}_1, \mathfrak{M}_2$ be two maximal orders in $\mathcal{B} = M_n(k)$, and write $\mathfrak{M}_i = \mathrm{End}_{\mathcal{O}}(\mathcal{L}_i)$ $(i = 1, 2)$ for $\mathcal{O}$-lattices $\mathcal{L}_i$ in V. Since $\mathrm{End}_{\mathcal{O}}(\mathcal{L}_i)$ only depends upon the homothety class of $\mathcal{L}_i$, we may assume without loss that $\mathcal{L}_1 \subseteq \mathcal{L}_2$. As the lattices are both free modules over a PID, they have well-defined invariant factors: $\{\mathcal{L}_2 : \mathcal{L}_1\} = \{\pi^{a_1}, \ldots, \pi^{a_n}\}$, with $a_i \in \mathbb{Z}$, and $a_1 \leq \cdots \leq a_n$. Note that $\{\mathcal{L}_1 : \mathcal{L}_2\} = \{\pi^{-a_n}, \ldots, \pi^{-a_1}\}$. Define the 'type distance' between $\mathfrak{M}_1$ and $\mathfrak{M}_2$ via the $\mathcal{L}_i$ to be congruence class modulo n:

$$td_k(\mathfrak{M}_1, \mathfrak{M}_2) = td_\pi(\mathfrak{M}_1, \mathfrak{M}_2) \equiv \sum_{i=1}^{n} a_i \pmod{n},$$

where $\{\mathcal{L}_2 : \mathcal{L}_1\} = \{\pi^{a_1}, \ldots, \pi^{a_n}\}$. This definition depends only on the local field, not the choice of uniformizer. The motivation for this definition comes from a consideration of how to label the vertices of a building. Those in the building for $SL_n(k)$ have types $0, \ldots, n-1$. Any given vertex, say the one corresponding to the homothety class of $\mathcal{L}$, can be assigned type 0. Then if $\alpha \in GL_n(k) = \mathcal{B}^\times$, the vertex associated to the homothety class of $\alpha\mathcal{L}$ has type congruent to $\mathrm{ord}_\pi(\det \alpha) \pmod{n}$ (see [19]).

3. Maximal orders over number fields

In returning to the global setting, we recall that we are assuming that p is an odd prime, and B is a central simple algebra having dimension p^2 over a number field K. For a prime ν of K, we denote by K_ν its completion at ν and for ν a finite prime, $\mathcal{O}_\nu$ the maximal order of K_ν, and $\pi = \pi_\nu$ a fixed uniformizer. We will denote by J_K the idele group of K and by J_B the idele group of B. We denote by nr the reduced norm in numerous contexts: $nr : B \to K$, $nr : B_\nu \to K_\nu$, or $nr : J_B \to J_K$, with any possible ambiguity resolved by context.

Because the degree of B over K is odd, $B_\nu \cong M_p(K_\nu)$ for every infinite prime ν of K, and since p is prime, for any finite prime ν of K, B_ν is either $M_p(K_\nu)$ (ν is said to split in B) or a central simple division algebra over K_ν (ν is said to ramify in B) (see section 32 of [18]).

Given a maximal order $\mathcal{R} \subset B$, and a prime ν of K, we define completions $\mathcal{R}_\nu \subseteq B_\nu$ by:

$$\mathcal{R}_\nu = \begin{cases} \mathcal{R} \otimes_{\mathcal{O}} \mathcal{O}_\nu & \text{if } \nu \text{ is finite} \\ \mathcal{R} \otimes_{\mathcal{O}} K_\nu = B_\nu & \text{if } \nu \text{ is infinite} \end{cases}$$

We will also be interested in the normalizers of the local orders, as well as their reduced norms. Let $\mathcal{N}(\mathcal{R}_\nu)$ denote the normalizer of $\mathcal{R}_\nu$ in $B_\nu^\times$. When ν is an infinite prime, $\mathcal{N}(\mathcal{R}_\nu) = B_\nu^\times$ and $nr(\mathcal{N}(\mathcal{R}_\nu)) = K_\nu^\times$. If ν is finite, we have two cases: If ν splits in B, then $B_\nu \cong M_p(K_\nu)$ and every maximal order is conjugate by an element of $B_\nu^\times$ to $M_p(\mathcal{O}_\nu)$, so every normalizer is conjugate to $GL_p(\mathcal{O}_\nu)K_\nu^\times$ (37.26 of [18]), while if ν ramifies in B, $\mathcal{R}_\nu$ is the unique maximal order of the division algebra B_ν [18], so $\mathcal{N}(\mathcal{R}_\nu) = B_\nu^\times$. It follows that for ν split, $nr(\mathcal{N}(\mathcal{R}_\nu)) = \mathcal{O}_\nu^\times (K_\nu^\times)^p$, while for ν ramified p 153 of [18] gives that $nr(\mathcal{N}(\mathcal{R}_\nu)) = nr(B_\nu^\times) = K_\nu^\times$.

3.1. Type numbers of maximal orders. We say that two (maximal rank) orders $\mathcal{R}$ and $\mathcal{E}$ in B are in the same genus if $\mathcal{R}_\nu \cong \mathcal{E}_\nu$ for all (finite) primes ν of K. By the Skolem-Noether theorem, this means they are locally conjugate at all finite primes. Denote by $\text{gen}(\mathcal{R})$ the genus of $\mathcal{R}$, the set of orders $\mathcal{E}$ in B which are in the same genus as $\mathcal{R}$. Again by Skolem-Noether, $\text{gen}(\mathcal{R})$ is the disjoint union of isomorphism classes. The type number of $\mathcal{R}$, $t(\mathcal{R})$, is the number of isomorphism classes in $\text{gen}(\mathcal{R})$.

By Theorem 17.3 of [18], any two maximal orders in B are everywhere locally conjugate, so the genus of maximal orders is independent of the choice of representative. So if $\mathcal{R}$ is any maximal order in B, the type number of $\mathcal{R}$ is simply the number of isomorphism classes of maximal orders in B. Notice that if Ω embeds into a given maximal order $\mathcal{R}$, then it embeds into every maximal order in the isomorphism class of $\mathcal{R}$, since any two elements of an isomorphism class are (globally) conjugate. With this understanding, we simply refer to whether Ω embeds into an isomorphism class, and the question we answer is into what proportion of the isomorphism classes of maximal orders can an order Ω be embedded?

Adelically, the genus of an order $\mathcal{R}$ is characterized by the coset space $J_B/\mathfrak{N}(\mathcal{R})$, where $\mathfrak{N}(\mathcal{R}) = J_B \cap \prod_\nu \mathcal{N}(\mathcal{R}_\nu)$ where $\mathcal{N}(\mathcal{R}_\nu)$ is the normalizer of $\mathcal{R}_\nu$ in $B_\nu^\times$. The type number of $\mathcal{R}$ is the cardinality of the double coset space $B^\times \backslash J_B/\mathfrak{N}(\mathcal{R})$. To make use of class field theory, we need to realize this quotient in terms of the arithmetic of K.

Henceforth, let $\mathcal{R}$ be a maximal order in B. We prove

Theorem 3.1. *The reduced norm on B induces a bijection*

$$nr : B^\times \backslash J_B / \mathfrak{N}(\mathcal{R}) \to K^\times \backslash J_K / nr(\mathfrak{N}(\mathcal{R})).$$

Proof. The map is defined in the obvious way with $nr(B^\times \tilde{\alpha}\, \mathfrak{N}(\mathcal{R})) = K^\times nr(\tilde{\alpha})\ nr(\mathfrak{N}(\mathcal{R}))$ and where $nr((\alpha_\nu)_\nu) = (nr(\alpha_\nu))_\nu$. We observed above that no infinite prime of K ramifies in B, so it follows from Theorem 33.4 of [18], that $nr(B_\nu^\times) = K_\nu^\times$ for all primes of K, including the infinite ones. Let $\tilde{a} = (a_\nu)_\nu \in J_K$, and $K^\times \tilde{a}\ nr(\mathfrak{N}(\mathcal{R}))$ be an element of $K^\times \backslash J_K / nr(\mathfrak{N}(\mathcal{R}))$. We construct an idele $\tilde{\beta} = (\beta_\nu)_\nu \in J_B$ so that $B^\times \tilde{\beta}\ \mathfrak{N}(\mathcal{R}) \mapsto K^\times \tilde{a}\, nr(\mathfrak{N}(\mathcal{R}))$. For all but finitely many non-archimedean primes ν of K, $a_\nu \in \mathcal{O}_\nu^\times$ and $\mathcal{R}_\nu \cong M_p(\mathcal{O}_\nu)$. Define β_ν to be a conjugate of the diagonal matrix $\mathrm{diag}(a_\nu, 1, \ldots, 1)$ which is contained in $\mathcal{R}_\nu$. For the other primes, using the local surjectivity of the reduced norm described above, let β_ν be any preimage of in $B_\nu^\times$ of a_ν. The constructed element $\tilde{\beta}$ is trivially seen to be in J_B and given the invariance of the reduced norm under conjugation, we see that $nr(\tilde{\beta}) = \tilde{a}$ which establishes surjectivity.

For injectivity we first need a small claim: that the preimage of $K^\times nr(\mathfrak{N}(\mathcal{R}))$ under the reduced norm is $B^\times J_B^1 \mathfrak{N}(\mathcal{R})$, where J_B^1 is the kernel of the reduced norm map $nr : J_B \to J_K$. It is obvious that $B^\times J_B^1 \mathfrak{N}(\mathcal{R})$ is contained in the kernel. Let $\tilde{\gamma} \in J_B$ be such that $nr(B^\times \tilde{\gamma}\ \mathfrak{N}(\mathcal{R})) \in K^\times nr(\mathfrak{N}(\mathcal{R}))$. Then $nr(\tilde{\gamma}) \in K^\times nr(\mathfrak{N}(\mathcal{R}))$, so write $nr(\tilde{\gamma}) = k \cdot nr(\tilde{r})$ for $\tilde{r} \in \mathfrak{N}(\mathcal{R})$. Again noting that no infinite prime of K ramifies in B, the Hasse-Schilling-Maass theorem (Theorem 33.15 of [18]) implies there exists an element $b \in B^\times$ with $nr(b) = k$. Thus $nr(\tilde{\gamma}) = nr(b) \cdot nr(\tilde{r})$, hence $nr(b^{-1}) \cdot nr(\tilde{\gamma}) \cdot nr(\tilde{r}^{-1}) = 1 \in J_K$ which implies $B^\times \tilde{\gamma}\ \mathfrak{N}(\mathcal{R}) = B^\times b^{-1} \tilde{\gamma}\, \tilde{r}^{-1}\ \mathfrak{N}(\mathcal{R}) \in B^\times J_B^1 \mathfrak{N}(\mathcal{R})$ as claimed.

To continue with injectivity, suppose that there exist $\tilde{\alpha}, \tilde{\beta} \in J_B$ with $nr(B^\times \tilde{\alpha}\, \mathfrak{N}(\mathcal{R})) = nr(B^\times \tilde{\beta}\, \mathfrak{N}(\mathcal{R}))$. Then $K^\times nr(\tilde{\alpha}) nr(\mathfrak{N}(\mathcal{R})) = K^\times nr(\tilde{\beta})\ nr(\mathfrak{N}(\mathcal{R}))$ which, since J_K is abelian, implies $nr(\tilde{\alpha}^{-1}\tilde{\beta}) \in K^\times nr(\mathfrak{N}(\mathcal{R}))$. By the claim, we have that $\tilde{\alpha}^{-1}\tilde{\beta} \in B^\times J_B^1 \mathfrak{N}(\mathcal{R})$. As above, it is easy to check that $B^\times J_B^1$ is a normal subgroup of J_B, being the kernel of the induced homomorphism $nr : J_B \to J_K / K^\times$, so that $\tilde{\beta} \in \tilde{\alpha} B^\times J_B^1 \mathfrak{N}(\mathcal{R}) = B^\times J_B^1 \tilde{\alpha} \mathfrak{N}(\mathcal{R})$. By VI.iii and VII of [8], we have that $J_B^1 \subset B^\times \tilde{\gamma} \mathfrak{N}(\mathcal{R}) \tilde{\gamma}^{-1}$ for any $\tilde{\gamma} \in J_B$, so choosing $\tilde{\gamma} = \tilde{\alpha}$, we have

$$\tilde{\beta} \in B^\times J_B^1 \tilde{\alpha} \mathfrak{N}(\mathcal{R}) \subseteq B^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R}),$$

so $B^\times \tilde{\beta} \mathfrak{N}(\mathcal{R}) \subseteq B^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R})$, and by symmetry, we have equality. □

While it is well-known that the type number is finite (the type number of an order is trivially bounded above by its class number and the class number is finite (26.4 of [18])), we establish a stronger result in our special case of central simple algebras of dimension p^2 over K. We show that the type number is a power of p; more specifically, we show that

Theorem 3.2. *Let $\mathcal{R}$ be a maximal order in a central simple algebra of dimension p^2 over a number field K. Then the group $K^\times\backslash J_K/nr(\mathfrak{N}(\mathcal{R}))$ is an elementary abelian group of exponent p.*

Proof. Consider the quotient $J_K/nr(\mathfrak{N}(\mathcal{R}))$. Each factor in the product has the form $K_\nu^\times/nr(\mathcal{N}(R_\nu))$. From above, we see that this quotient is trivial when ν is infinite or finite and ramified. For finite split primes, $K_\nu^\times/nr(\mathcal{N}(R_\nu)) = K_\nu^\times/(\mathcal{O}_v^\times(K_\nu^\times)^p) \cong \mathbb{Z}/p\mathbb{Z}$. So it follows that $J_K/nr(\mathfrak{N}(\mathcal{R}))$ is an abelian group of exponent p. The canonical homomorphism $J_K/nr(\mathfrak{N}(\mathcal{R})) \to K^\times\backslash J_K/nr(\mathfrak{N}(\mathcal{R}))$ is surjective, so the resulting quotient is finite, abelian, and of exponent p which completes the proof. □

3.2. The class field associated to a maximal order. We have seen above that the distinct isomorphism classes of maximal orders in B (i.e., the isomorphism classes in the genus of any given maximal order $\mathcal{R}$) are in one-to-one correspondence with the double cosets in the group $G = K^\times\backslash J_K/nr(\mathfrak{N}(\mathcal{R}))$. Put $H_\mathcal{R} = K^\times nr(\mathfrak{N}(\mathcal{R}))$ and $G_\mathcal{R} = J_K/H_\mathcal{R}$. Since J_K is abelian, G and $G_\mathcal{R}$ are naturally isomorphic, and since $H_\mathcal{R}$ contains a neighborhood of the identity in J_K, it is an open subgroup (Proposition II.6 of [11]).

Since $H_\mathcal{R}$ is an open subgroup of J_K having finite index, there is by class field theory [12], a class field $K(\mathcal{R})$ associated to it. The extension $K(\mathcal{R})/K$ is an abelian extension with $Gal(K(\mathcal{R})/K) \cong G_\mathcal{R} = J_K/H_\mathcal{R}$ and with $H_\mathcal{R} = K^\times N_{K(\mathcal{R})/K}(J_{K(\mathcal{R})})$. Moreover, a prime ν of K (possibly infinite) is unramified in $K(\mathcal{R})$ if and only if $\mathcal{O}_\nu^\times \subset H_\mathcal{R}$, and splits completely if and only if $K_\nu^\times \subset H_\mathcal{R}$. Here if ν is archimedean, we take $\mathcal{O}_\nu^\times = K_\nu^\times$. From our computations at the beginning of this section, we saw that $nr(\mathcal{N}(\mathcal{R}_\nu)) = K_\nu^\times$ or $\mathcal{O}_\nu^\times(K_\nu^\times)^p$. In particular $K(\mathcal{R})/K$ is an everywhere unramified extension of K.

For any finite extension of fields F/K, we shall use the notation $(*, F/K)$ in many ways: for arbitrary F/K, and $\mathfrak{P}$ an unramified prime of F, the symbol $(\mathfrak{P}, F/K)$ denotes the Frobenius automorphism; when F/K is abelian and $\mathfrak{P}$ is an unramified prime of F lying above a prime ν of K, the symbol $(\nu, F/K)$ denotes the Artin symbol. Finally, we use the well-known relationship between the idele- and ideal-theoretic Artin symbols (p. 407 of [16]) as follows: for an abelian extension F/K, and ν a prime of K unramified in F, put $e_\nu = (1, \dots, 1, \pi_\nu, 1, \dots)$ with π_v a uniformizer in K_ν (and viewing e_ν in an appropriate quotient of the idele class group), we have $(e_\nu, F/K) = (\nu, F/K)$. For abelian F/K, we shall write $(*, F/K)$ for the Artin map.

Proposition 3.1. *Let S be any finite set of primes of K which includes the infinite primes. The group $G_{\mathcal{R}}$ can be generated by cosets having representatives of the form $e_{\nu_i} = (1, \dots, 1, \pi_{\nu_i}, 1, \dots)$ for $\nu_i \notin S$, π_{ν_i} a uniformizer in K_{ν_i}.*

Proof. The Artin map $(*, K(\mathcal{R})/K)$ induces the isomorphism

$$G_{\mathcal{R}} = J_K/H_{\mathcal{R}} \cong Gal(K(\mathcal{R})/K),$$

By the Chebotarev density theorem, for each $\sigma \in Gal(K(\mathcal{R})/K)$, there exist an infinite number of primes ν of K so that $\sigma = (\nu, K(\mathcal{R})/K)$, the Artin symbol on ideals. Using the relationship referenced above between the idele-and ideal-theoretic Artin maps, we see putting $e_\nu = (1, \dots, 1, \pi_\nu, 1, \dots)$ with π_v a uniformizer in K_ν, that $(e_\nu, K(\mathcal{R})/K) = \sigma = (\nu, K(\mathcal{R})/K)$ from which the result follows. □

We shall denote the generators of $G_{\mathcal{R}} \cong (\mathbb{Z}/p\mathbb{Z})^m$ as $\{\overline{e}_{\nu_i}\}_{i=1}^m$ where the e_{ν_i} are the ideles of the previous proposition. Let L/K be a field extension of degree p. We now show that the generators $\{\overline{e}_{\nu_i}\}$ can be chosen so that the K-primes ν_i have certain splitting properties in L.

Proposition 3.2. *With the notation as above, we have:*

(1) If $L \subseteq K(\mathcal{R})$, then we may assume that $G_{\mathcal{R}}$ is generated by elements $\{\overline{e}_{\nu_i}\}$ where ν_i splits completely in L for $i > 1$, and ν_1 is inert in L.

(2) If $L \not\subseteq K(\mathcal{R})$ then we may assume that $G_{\mathcal{R}}$ is generated by elements $\{\overline{e}_{\nu_i}\}$ where ν_i splits completely in L for all $i \geq 1$.

Remark. Recall that $[K(\mathcal{R}) : K] = p^m = t(\mathcal{R})$ for $m \geq 0$. The condition $L \subseteq K(\mathcal{R})$ clearly forces $m \geq 1$, however when $L \not\subseteq K(\mathcal{R})$, it is possible that the type number equals 1, though in that case the second part of the proposition is vacuously true.

Proof. To a certain extent, the cases can be handled simultaneously. Let $\widehat{L}$ denote the Galois closure of L. We claim that $L \cap K(\mathcal{R}) = \widehat{L} \cap K(\mathcal{R})$. If $L \subseteq K(\mathcal{R})$, then since $K(\mathcal{R})/K$ is abelian, $L = \widehat{L}$, and we are done. If $L \not\subseteq K(\mathcal{R})$, then since $[L : K]$ is prime, $L \cap K(\mathcal{R}) = K$. We show $N = \widehat{L} \cap K(\mathcal{R}) = K$. Without loss, we may assume $\widehat{L} \neq L$. The inclusions $K \subseteq N \subseteq K(\mathcal{R})$ and $K \subseteq N \subseteq \widehat{L}$ imply that $[N : K]$ is a power of p, and since $[\widehat{L} : K] \mid p!$, that $[N : K] \mid p!$. Thus $[N : K] = 1$ or p. We proceed by contradiction, and assume that $[N : K] = p$. Since $N \subseteq K(\mathcal{R})$, N is an abelian extension of K, so in particular $N \neq L$ since L/K is not Galois. Then NL/L is Galois with $Gal(NL/L) \cong Gal(N/K)$. This implies that $[NL : L] = p$ which means $[NL : K] = p^2$. But $NL \subseteq \widehat{L}$ which implies $p^2 \mid p!$, a contradiction which establishes the claim.

As in the previous paragraph, set $N = \widehat{L} \cap K(\mathcal{R})$, and let $\sigma \in Gal(K(\mathcal{R})/N)$ viewed as a subgroup of $Gal(K(\mathcal{R})/K)$. By Lemma 7.14 of

[15], there exist infinitely many primes ν of K for which $\sigma = (\nu, K(\mathcal{R})/K)$, and for which there exists a prime $\mathfrak{P}$ of $\widehat{L}$ lying above ν with inertia degree $f(\mathfrak{P} \mid \nu) = 1$. Without loss, ν splits completely in $\widehat{L}$, hence in L. This establishes (2).

To finish (1), we first note $N = L$ has degree p over K, so $|Gal(K(\mathcal{R})/N)| = p^{m-1}$ and the argument above has produced the $m-1$ generators e_{ν_i} for which ν_i splits completely in L. To characterize the last generator, we note that Galois theory provides the following exact sequence:

$$1 \longrightarrow Gal(K(\mathcal{R})/L) \overset{\iota}{\hookrightarrow} Gal(K(\mathcal{R})/K) \xrightarrow{\mathrm{res}_L} Gal(L/K) \longrightarrow 1\ .$$

Now let τ be any element of $Gal(K(\mathcal{R})/K)$ not in $Gal(K(\mathcal{R})/L)$. Writing $\tau = (\mu, K(\mathcal{R})/K)$ (μ unramified), we see that since $\tau|_L = (\mu, L/K) \neq 1$ which means μ does not split completely in L. But L/K having prime degree means μ is inert in L. Note that for any $\tau \notin Gal(K(\mathcal{R})/L)$, $Gal(K(\mathcal{R})/K)$ is the internal direct product of $\langle\tau\rangle$ and $Gal(K(\mathcal{R})/L)$ from which assertion (1) follows. In particular, if μ is any prime of K inert in L, $Gal(K(\mathcal{R})/K)$ is generated by $(\mu, K(\mathcal{R})/K)$ and $Gal(K(\mathcal{R})/L)$. □

3.3. Parametrizing the isomorphism classes. Let $\mathcal{R}$ be a fixed maximal order in B, and recall $G_{\mathcal{R}} = J_K/K^\times nr(\mathfrak{N}(\mathcal{R})) \cong (\mathbb{Z}/p\mathbb{Z})^m$, $m \geq 0$. Let $\{e_{\nu_i}\}_{i=1}^m \subset J_K$ so that their images $\{\overline{e}_{\nu_i}\}_{i=1}^m$ generate $G_{\mathcal{R}}$. By Proposition 3.1, we may choose the ν_i to avoid any finite set of primes; for now we simply assume that all the ν_i are non-archimedean and split in B, in particular that $B_{\nu_i} \cong M_p(K_{\nu_i})$. For each ν_i we shall regard $\mathcal{R}_{\nu_i}$ as a vertex in the building for $SL_p(K_{\nu_i})$, and let C_i be any chamber containing $\mathcal{R}_{\nu_i}$. We may assume that in a given labeling of the building, $\mathcal{R}_{\nu_i}$ has type zero [19], and we label the remaining vertices of the chamber C_i as $\mathcal{R}_{\nu_i}^{(k)}$, (having type k) $k = 1, \ldots, p-1$, putting $\mathcal{R}_{\nu_i}^{(0)} = \mathcal{R}_{\nu_i}$.

We define p^m distinct maximal orders, $\mathcal{D}^\gamma$, in B (indexed by $\gamma = (\gamma_i) \in (\mathbb{Z}/p\mathbb{Z})^m$) via the local-global correspondence by providing the following local data:

$$\mathcal{D}_\nu^\gamma = \begin{cases} \mathcal{R}_{\nu_i}^{(\gamma_i)} & \text{if } \nu = \nu_i \\ \mathcal{R}_\nu & \text{otherwise.} \end{cases} \tag{3.1}$$

We claim that any such collection of maximal orders parametrizes the genus of $\mathcal{R}$, that is given any maximal order $\mathcal{E}$, there is a unique $\gamma \in (\mathbb{Z}/p\mathbb{Z})^m$, so that $\mathcal{E} \cong \mathcal{D}^\gamma$. To show this, let $\mathfrak{M}$ denote the set of all maximal orders in B, and define a map $\rho : \mathfrak{M} \times \mathfrak{M} \to G_{\mathcal{R}}$ as follows.

Let $\mathcal{R}_1, \mathcal{R}_2 \in \mathfrak{M}$. For ν a finite prime of K (split in B), we have defined the type distance between their localizations: $td_\nu(\mathcal{R}_{1\nu}, \mathcal{R}_{2\nu}) \in \mathbb{Z}/p\mathbb{Z}$. For ν archimedean or ν finite and ramified in B, define $td_\nu(\mathcal{R}_{1\nu}, \mathcal{R}_{2\nu}) = 0$. Recall

that since $\mathcal{R}_{1\nu} = \mathcal{R}_{2\nu}$ for almost all ν, $td_\nu(\mathcal{R}_{1\nu}, \mathcal{R}_{2\nu}) = 0$ for almost all primes ν. Let $\rho(\mathcal{R}_1, \mathcal{R}_2)$ be the image in $G_{\mathcal{R}}$ of the idele $(\pi_\nu^{td_\nu(\mathcal{R}_{1\nu}, \mathcal{R}_{2\nu})})_\nu$. Note that while the idele is not well-defined, its image in $G_{\mathcal{R}}$ is, since the local factor of $G_{\mathcal{R}} = J_K/K^\times nr(\mathfrak{N}(\mathcal{R}))$ at the finite split primes has the form $K_\nu^\times/\mathcal{O}_\nu^\times(K_\nu^\times)^p$.

We now show that any such collection of maximal orders given as the $\mathcal{D}^\gamma$ parametrizes the genus.

Proposition 3.3. *Let $\mathcal{R}$ be a fixed maximal order in B, and consider the collection of maximal orders $\mathcal{D}^\gamma$ defined above.*

(1) If $\mathcal{E}$ is a maximal order in B and $\mathcal{E} \cong \mathcal{R}$, then $\rho(\mathcal{R}, \mathcal{E})$ is trivial.

(2) If $\mathcal{E} \cong \mathcal{E}'$ are maximal orders in B, then $\rho(\mathcal{R}, \mathcal{E}) = \rho(\mathcal{R}, \mathcal{E}')$.

(3) $\mathcal{D}^\gamma \cong \mathcal{D}^{\gamma'}$ if and only if $\gamma = \gamma'$.

Proof. For the first assertion, we may assume that $\mathcal{E} = b\mathcal{R}b^{-1}$ for some $b \in B^\times$ by Skolem-Noether, which of course means $\mathcal{E}_\nu = b\mathcal{R}_\nu b^{-1}$ for each prime ν. For a finite prime ν which splits in B, we may take $\mathcal{R}_\nu = \mathrm{End}(\Lambda_\nu)$ for some $\mathcal{O}_\nu$-lattice Λ_ν, and so $\mathcal{E}_\nu = \mathrm{End}(b\Lambda_\nu)$. It follows that

$$td_\nu(\mathcal{R}_\nu, \mathcal{E}_\nu) \equiv \mathrm{ord}_\nu(\det(b^{-1})) \equiv \mathrm{ord}_\nu(nr(b^{-1})) \pmod{p},$$

and since $G_{\mathcal{R}}$ is trivial at the archimedean primes and the finite primes which ramify in B, we conclude that $\rho(\mathcal{R}, \mathcal{E}) = (\overline{nr(b^{-1})})_\nu = 1$ in $G_{\mathcal{R}} = J_K/K^\times nr(\mathfrak{N}(\mathcal{R}))$ as $(nr(b^{-1}))_\nu$ is in the image of $K^\times$ in J_K.

To see the second assertion, we have as above $\mathcal{E}' = b\mathcal{E}b^{-1}$ for some $b \in B^\times$ and so $\mathcal{E}'_\nu = b\mathcal{E}_\nu b^{-1}$ for each prime ν. If we write $\mathcal{R}_\nu = \mathrm{End}(\Lambda_\nu)$ and $\mathcal{E}_\nu = \mathrm{End}(\Gamma_\nu)$ for $\mathcal{O}_\nu$-lattices Λ_ν and Γ_ν, then $\mathcal{E}'_\nu = \mathrm{End}(b\Gamma_\nu)$. Considering the elementary divisors of the lattices Λ_ν, Γ_ν and $b\Gamma_\nu$, we easily see that $td_\nu(\mathcal{R}_\nu, \mathcal{E}'_\nu) \equiv td_\nu(\mathcal{R}_\nu, \mathcal{E}_\nu) + \mathrm{ord}_\nu(\det(b^{-1})) \pmod{p}$, from which the result follows as in the first case.

For the last assertion, we need only show one direction. Fix a prime $\nu = \nu_i$ among the finite number used to determine the parametrization $\mathcal{D}^\gamma$. Then we are comparing $\mathcal{R}_\nu^{(\gamma_i)}$ and $\mathcal{R}_\nu^{(\gamma'_i)}$. Since the $\mathcal{R}_\nu^{(k)}$ $k = 0, \ldots, p-1$ are the vertices of a fixed chamber in the affine building for $SL_p(K_\nu)$, they can be realized (p 362 of [1]) as $\mathcal{R}_\nu^{(k)} = \mathrm{End}_{\mathcal{O}_\nu}(\Lambda^{(k)})$ with $\Lambda^{(k)} = \mathcal{O}_\nu\pi\omega_1 \oplus \cdots \oplus \mathcal{O}_\nu\pi\omega_k \oplus \mathcal{O}_\nu\omega_{k+1} \oplus \cdots \oplus \mathcal{O}_\nu\omega_p$. Here the set $\{\omega_i\}$ is a basis of a vector space V/K_ν through which we have identified $B_\nu = \mathrm{End}_{K_\nu}(V)$. It follows that $td_\nu(\mathcal{R}_\nu^{(\gamma_i)}, \mathcal{R}_\nu^{(\gamma'_i)}) = \gamma'_i - \gamma_i \pmod{p}$. It is now easy to see that if $\gamma \neq \gamma'$, then $\rho(\mathcal{D}^\gamma, \mathcal{D}^{\gamma'}) \neq 1$, so $\mathcal{D}^\gamma \ncong \mathcal{D}^{\gamma'}$. □

3.4. Selective orders and the main theorem. We reestablish the notation from the introduction. Let p an odd prime, B a central simple algebra of dimension p^2 over a number field K, and L/K a field extension of degree p which satisfies $L \subset B$. Let $\mathcal{O}_K$ denote the ring of integers of K, and

let Ω denote a commutative $\mathcal{O}_K$-order of rank p in L. Necessarily Ω is an integral domain with field of fractions equal to L, and we have seen that Ω is contained in a maximal order $\mathcal{R}$ (rank n^2) of B which we now fix.

Given that Ω is contained in $\mathcal{R}$, the question is which other isomorphism classes in the genus of $\mathcal{R}$ admit an embedding of Ω? Recall that since $\mathcal{R}$ is maximal, this simply asks which isomorphism classes of maximal orders in B admit an embedding of Ω? The generic case is that every isomorphism class admits an embedding of Ω, but when it does not, we follow [7] and call Ω selective. Selectivity is characterized by our main theorem.

Theorem 3.3. *With the notation fixed as above, every maximal order in B contains a conjugate (by $B^\times$) of Ω except when the following conditions hold:*

(1) $L \subseteq K(\mathcal{R})$, that is L is contained in the class field associated to $\mathcal{R}$.

(2) Every prime ideal ν of K which divides $N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$ splits in L/K.

Suppose now that both conditions (1) and (2) hold. Then precisely one-pth of the isomorphism classes of maximal orders admit an embedding of Ω. Those classes are characterized by means of the idelic Artin map $(*, L/K)$ as follows: $\mathcal{E}$ is a maximal order which contains a conjugate of Ω if and only if the Artin symbol $(\rho(\mathcal{R}, \mathcal{E}), L/K)$ is trivial in $Gal(L/K)$.

First we give some examples of selective and non-selective orders. Let S_∞ denote the set of infinite primes of K and let $Ram(B)$ denote the set of primes in K which ramify in B. Put $S = S_\infty \cup Ram(B)$.

Example. Let p be an odd prime, K a number field with class number p, let $B = M_p(K)$, and $\mathcal{R} = M_p(\mathcal{O}_K)$. Then $G_\mathcal{R} = J_K/K^\times J_K^p J_{K,S_\infty} \cong C_K/C_K^p \cong C_K$, where C_K is the ideal class group of K, and C_K^p the subgroup of pth powers. We conclude the type number $t(\mathcal{R}) = |G_\mathcal{R}| = p$. This means that $[K(\mathcal{R}) : K] = p$ and $K(\mathcal{R})/K$ is an everywhere unramified abelian extension of K, so $K(\mathcal{R}) \subseteq \widetilde{K}$, where $\widetilde{K}$ is the Hilbert class field of K. Degree considerations force $K(\mathcal{R}) = \widetilde{K}$. Put $L = K(\mathcal{R}) = \widetilde{K}$. Because B is everywhere split, L embeds into B. So, in particular, we have $L \subseteq K(\mathcal{R})$, $L \subset B$. This means that $\mathcal{O}_L$ is selective as established in [2], [6] as well as our main theorem. Now let ν be a prime of K, necessarily unramified in $L = \widetilde{K}$, and consider the order $\Omega = \mathcal{O}_K + \nu\mathcal{O}_L$. We easily see that $\nu\mathcal{O}_L \subseteq \mathfrak{f}_{\Omega/\mathcal{O}_K}$ which implies $\mathfrak{f}_{\Omega/\mathcal{O}_K} \mid \nu\mathcal{O}_L$, hence $N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K}) \mid N_{L/K}(\nu\mathcal{O}_L) = \nu^p\mathcal{O}_K$ whether ν is inert or splits completely in L. Since $\mathfrak{f}_{\Omega/\mathcal{O}_K} \neq \mathcal{O}_L$, we see that $\nu \mid N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$, so by condition (2) of the theorem, in the case that ν is inert, we see Ω is not selective, but when ν splits completely, Ω is selective.

Indeed, given the theorem, we have the following interesting corollary.

Corollary 3.1. *Suppose there exists a field extension L/K with $[L : K] = p$ which embeds into B, and which contains an order $\Omega \subseteq \mathcal{O}_L$ which is*

selective. Then $B \cong M_p(K)$. Said alternatively, suppose we are given any number field L/K of degree p, and any suborder $\Omega \subseteq \mathcal{O}_L$. If B is a degree p division algebra, then Ω embeds into every maximal order in B if and only if L embeds into B. In particular, a degree p division algebra admits no selective orders.

Proof. Given $L \subset B$ and Ω selective, we must have $L \subseteq K(\mathcal{R})$. Now $K(\mathcal{R})$ is the class field associated to the subgroup $H_{\mathcal{R}} = K^{\times}\Big(J_K \cap \Big[\prod_{\nu \in S} K_{\nu}^{\times} \times \prod_{\nu \notin S} \mathcal{O}_{\nu}^{\times}(K_{\nu}^{\times})^p\Big]\Big)$. In particular, if $\nu \in Ram(B) \subset S$, then $K_{\nu}^{\times} \subset H_{\mathcal{R}}$ which means that ν splits completely in the class field $K(\mathcal{R})$, hence in L. But this violates the Albert-Brauer-Hasse-Noether theorem which implies that no prime that ramifies in B splits in L. □

We give the proof of the main theorem via a sequence of propositions.

Proposition 3.4. *Let Ω denote an $\mathcal{O}_K$-order which is an integral domain whose field of fractions L is a degree p extension of K which is contained in B. We assume that Ω is contained in a fixed maximal order $\mathcal{R}$ of B. If $L \not\subseteq K(\mathcal{R})$ then every maximal order in B contains a conjugate (by $B^{\times}$) of Ω.*

Proof. Note that if the type number $t(\mathcal{R}) = 1$, the proposition is obviously true, so we assume $t(\mathcal{R}) = [K(\mathcal{R}) : K] = p^m$ with $m \geq 1$. By Proposition 3.2, we may choose elements $\{e_{\nu_1}, \ldots, e_{\nu_m}\} \subset J_K$ so that the cosets $\{\overline{e}_{\nu_i}\}$ generate $G_{\mathcal{R}} = J_K/K^{\times} nr(\mathfrak{N}(\mathcal{R}))$, and so that the primes ν_i of K are finite and split completely in L. Since $[L : K] = p$, L is a strictly maximal subfield of B (section 13.1 of [17]) and consequently (Corollary 13.3 [17]), L is a splitting field for B. We claim that all the ν_i are split in B. Fix $\nu = \nu_i$ and let $\mathfrak{P}$ be any prime of L lying above ν. As ν splits completely in L, $[L_{\mathfrak{P}} : K_{\nu}] = 1$. By Theorem 32.15 of [18], m_{ν} which is the local index of B_{ν}/K_{ν} must divide $[L_{\mathfrak{P}} : K_{\nu}]$, thus $B_{\nu} \cong M_p(K_{\nu})$, as desired. Now, $L \subset B$ implies that $L \otimes_K K_{\nu} \cong \oplus_{\mathfrak{P}|\nu} L_{\mathfrak{P}} \cong K_{\nu}^p \hookrightarrow B \otimes_K K_{\nu} = B_{\nu}$. By a slight generalization of Skolem-Noether to commutative semisimple subalgebras of matrix algebras (Lemma 2.2 of [4]), we may assume we have a K_{ν}-algebra isomorphism $\varphi : B_{\nu} \to M_p(K_{\nu})$ such that

$$\varphi(L) \subset \begin{pmatrix} K_{\nu} & & & 0 \\ & K_{\nu} & & \\ & & \ddots & \\ 0 & & & K_{\nu} \end{pmatrix}$$

and hence

$$\varphi(\Omega) \subseteq \varphi(\mathcal{O}_L) \subset \begin{pmatrix} \mathcal{O}_\nu & & & 0 \\ & \mathcal{O}_\nu & & \\ & & \ddots & \\ 0 & & & \mathcal{O}_\nu \end{pmatrix}.$$

By Corollary 2.3 of [20] all maximal orders containing $\mathrm{diag}(\mathcal{O}_\nu, \ldots, \mathcal{O}_\nu)$ have a prescribed form and lie in a fixed apartment in the affine building for $SL_p(K_\nu)$ and so it follows that by a rescaling of basis we may assume in addition that $\varphi(\mathcal{R}_\nu) = M_p(\mathcal{O}_\nu)$.

With π a uniformizer in K_ν, let $\delta_k = \mathrm{diag}(\underbrace{\pi, \ldots, \pi}_{k}, 1, \ldots, 1) \in M_p(K_\nu)$, $k = 0, \ldots, p-1$, and define maximal orders $\mathcal{E}_k = \delta_k M_p(\mathcal{O}_\nu)\delta_k^{-1}$. These are all maximal orders containing $\mathrm{diag}(\mathcal{O}_\nu, \ldots, \mathcal{O}_\nu)$, and are all the vertices of a fixed chamber in the building for $SL_p(K_\nu)$. If we put $\mathcal{R}_\nu^{(k)} = \varphi^{-1}(\mathcal{E}_k)$ for $k = 0, \ldots, p-1$, and $\nu \in \{\nu_1, \ldots, \nu_m\}$ we then obtain a parametrization $\mathcal{D}^\gamma$ of the isomorphism classes of all maximal orders in B as in Equation (3.1). Since $\Omega \subset \mathcal{R}$, and by construction $\Omega \subset \mathcal{R}_{\nu_i}^{(0)} \cap \cdots \cap \mathcal{R}_{\nu_i}^{(p-1)}$ for each ν_i, we have that $\Omega \subset \mathcal{D}_\nu^\gamma$ for all primes ν and all γ. Since every maximal order is conjugate to one of the $\mathcal{D}_\gamma$'s, every maximal order in B contains a conjugate of Ω. □

Next we assume that condition (1) of the theorem holds, but not condition (2). Note that since $L \subseteq K(\mathcal{R})$ and $K(\mathcal{R})/K$ is an everywhere unramified abelian extension, so is L/K. Moreover, since L/K is of prime degree (and Galois), any unramified prime splits completely or is inert.

Proposition 3.5. *Assume that Ω is an integral domain contained in $\mathcal{R}$ whose field of fractions $L \subseteq K(\mathcal{R})$. Assume that there is a prime ν of K which divides $N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$, the norm of the conductor $\mathfrak{f}_{\Omega/\mathcal{O}_K}$ of Ω, but which does not split completely in L. Then every maximal order in B contains a conjugate of Ω.*

Proof. Since condition (2) is assumed not to hold, we may assume by the comments above that there is a prime ν of K which divides $N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$ and which is inert in L. Thus we may assume that $\nu\mathcal{O}_L \mid \mathfrak{f}_{\Omega/\mathcal{O}_K}$. Our first goal is to show that $\Omega \subseteq \mathcal{O}_K + \nu\mathcal{O}_L$.

We first assume that Ω has the form $\Omega = \mathcal{O}_K[a]$ for some $a \in \mathcal{O}_L$, and let f be the minimal polynomial of a over K. Since $\Omega \otimes_{\mathcal{O}_K} K \cong L$, f is irreducible of degree p, and since a is integral, $f \in \mathcal{O}_K[x]$. By Proposition 4.12 of [15], $\mathfrak{f}_{\Omega/\mathcal{O}_K} = f'(a)\partial_{L/K}^{-1} = f'(a)\mathcal{O}_L$ since L/K everywhere unramified implies that the different $\partial_{L/K} = \mathcal{O}_L$. So it follows that $f'(a) \equiv 0 \pmod{\nu}$. Put $\overline{a} = a + \nu\mathcal{O}_L$ and consider the tower of fields:

$$O_K/\nu\mathcal{O}_K \subseteq \mathcal{O}_K/\nu\mathcal{O}_K[\overline{a}] \subseteq \mathcal{O}_L/\nu\mathcal{O}_L.$$

From top to bottom, this is a degree p extension of finite fields since ν is inert in L, and the ring in the middle is a field since it is a finite integral domain. Since the total extension has prime degree, there are two cases.

If $\mathcal{O}_K/\nu\mathcal{O}_K[\overline{a}] = \mathcal{O}_L/\nu\mathcal{O}_L$, then $\overline{f}$ (the reduction of f mod $\nu\mathcal{O}_K$) is irreducible and hence is the minimal polynomial of $\overline{a}$. In particular $\overline{f}$ must be separable polynomial since finite fields are perfect. On the other hand, $\overline{f}$ and $\overline{f'}$ share the common root $\overline{a}$, so $\overline{f}$ is not separable, a contradiction.

Thus $\mathcal{O}_K/\nu\mathcal{O}_K[\overline{a}] = \mathcal{O}_K/\nu\mathcal{O}_K$ where we view $\mathcal{O}_K/\nu\mathcal{O}_K$ embedded as usual in $\mathcal{O}_L/\nu\mathcal{O}_L$. Thus $\overline{a} = a + \nu\mathcal{O}_L \in \mathcal{O}_K/\nu\mathcal{O}_K$ which means that $a + \nu\mathcal{O}_L = b + \nu\mathcal{O}_L$ for some $b \in \mathcal{O}_K$. This means that $a \in b + \nu\mathcal{O}_L$ which in turn means that $\Omega = \mathcal{O}_k[a] \subseteq \mathcal{O}_K + \nu\mathcal{O}_L$.

Now consider the general case of an order Ω. We show $\Omega \subseteq \mathcal{O}_K + \nu\mathcal{O}_L$ by showing each element of Ω is in $\mathcal{O}_K + \nu\mathcal{O}_L$. Choose $a \in \Omega$. Without loss assume $a \notin \mathcal{O}_K$. Then $\mathcal{O}_K[a]$ is an integral domain whose field of fractions is all of L since L/K has prime degree. Moreover, $\mathfrak{f}_{\Omega/\mathcal{O}_K} \mid \mathfrak{f}_{\mathcal{O}_K[a]/\mathcal{O}_K}$, so we may use the same inert prime ν for all elements of Ω, and the special case now implies the general result.

By Proposition 3.2 (and its proof), we may choose primes $\nu_1, \ldots, \nu_m$ of K so that the $\{\overline{e}_{\nu_i}\}$ generate $G_{\mathcal{R}}$, where ν_i splits completely in L for $i > 1$ and where ν_1 is inert in L. Consider the situation locally at $\nu = \nu_1$. We have that $\Omega_\nu \subseteq \mathcal{O}_\nu + \nu\mathcal{O}_{L_\nu} \subseteq \mathcal{O}_{L_\nu}$. As in the previous proposition, we have a K_ν-algebra isomorphism $\varphi : B_\nu \to M_p(K_\nu)$. Let $\mathcal{D}_\nu$ be a maximal order in $M_p(K_\nu)$ containing $\varphi(\mathcal{O}_{L_\nu})$ and hence $\varphi(\Omega)$. Since all maximal orders in $M_p(K_\nu)$ are conjugate, writing $\mathcal{D}_\nu = \mathrm{End}_{\mathcal{O}_\nu}(\Lambda_\nu)$ for some $\mathcal{O}_\nu$-lattice Λ_ν, we may assume that φ is defined so that $\mathcal{D}_\nu = M_p(\mathcal{O}_\nu)$. As in the previous proposition, let $\delta_k = \mathrm{diag}(\underbrace{\pi, \ldots, \pi}_{k}, 1, \ldots, 1) \in M_p(K_\nu)$, $k = 0, \ldots, p-1$, and define maximal orders $\mathcal{D}_\nu^{(k)} = \delta_k M_p(\mathcal{O}_\nu)\delta_k^{-1}$. One trivially checks that $\nu\mathcal{D}_\nu \subset \mathcal{D}_\nu^{(k)}$ for $k = 0, \ldots, p-1$, so that $\varphi(\Omega) \subseteq \varphi(\mathcal{O}_\nu + \nu\mathcal{O}_{L_\nu}) \subset \mathcal{O}_\nu + \nu\mathcal{D}_\nu \subseteq \mathcal{D}_\nu^{(k)}$ for $k = 0, \ldots, p-1$. Putting $\mathcal{R}_\nu^{(k)} = \varphi^{-1}(\mathcal{D}_\nu^{(k)})$, we have $\Omega \subset \mathcal{R}_\nu^{(k)}$ for $k = 0, \ldots, p-1$, and we may use these $\mathcal{R}_\nu^{(k)}$ as part of the parametrization of the isomorphism classes of maximal orders. The other primes $\nu_2, \ldots, \nu_m$ all split completely in L, and the proof of the previous proposition shows that Ω is contained in all the local factors of our parametrization. So as before, every maximal order in B contains a conjugate of Ω. □

Finally, we assume that conditions (1) and (2) hold, and show that Ω is contained in only one-pth of the isomorphism classes of $\mathcal{R}$. We require a small technical lemma.

Lemma 3.1. *As above, let Ω denote an $\mathcal{O}_K$-order which is an integral domain whose field of fractions L is a cyclic extension of K having prime degree p. We assume that L is contained in B, and let ν be a prime of K*

which is inert in L. If $\nu \nmid N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$, then there exists an $a \in \Omega \setminus \mathcal{O}_K$ so that $\nu \nmid N_{L/K}(\mathfrak{f}_{\mathcal{O}_K[a]/\mathcal{O}_K})$.

We remark that this lemma represents a statement that in this narrow context Ω has no common non-essential discriminantal divisors, see [15], a frequent obstruction to assuming that an order has a power basis.

Proof. First note that since ν is inert in L, the stated condition on the conductor $\mathfrak{f}_{\Omega/\mathcal{O}_K}$ is equivalent to $\nu\mathcal{O}_L \nmid \mathfrak{f}_{\Omega/\mathcal{O}_K}$. Let $a \in \Omega$, and consider the tower of fields (the quotient ring in the middle being a finite integral domain):

$$\mathcal{O}_K/\nu\mathcal{O}_K \hookrightarrow (\mathcal{O}_K/\nu\mathcal{O}_K)[a+\nu\mathcal{O}_L] \hookrightarrow \mathcal{O}_L/\nu\mathcal{O}_L\ .$$

Since ν is inert in L, $[\mathcal{O}_L/\nu\mathcal{O}_L : \mathcal{O}_K/\nu\mathcal{O}_K] = p$, so the field in the middle coincides with one of the ends. If $(\mathcal{O}_K/\nu\mathcal{O}_K)[a+\nu\mathcal{O}_L] = \mathcal{O}_K/\nu\mathcal{O}_K$, then $a+\nu\mathcal{O}_L = b+\nu\mathcal{O}_L$ for some $b \in \mathcal{O}_K$, hence $\mathcal{O}_K[a] \subseteq \mathcal{O}_K + \nu\mathcal{O}_L$. If this happens for each $a \in \Omega$, then $\Omega \subseteq \mathcal{O}_K + \nu\mathcal{O}_L$. Consider the conductors of these orders: Certainly, $\mathfrak{f}_{(\mathcal{O}_K+\nu\mathcal{O}_L)/\mathcal{O}_K} \mid \mathfrak{f}_{\Omega/\mathcal{O}_K}$, and $\nu\mathcal{O}_L \subseteq \mathfrak{f}_{(\mathcal{O}_K+\nu\mathcal{O}_L)/\mathcal{O}_K} = \{x \in \mathcal{O}_L \mid x\mathcal{O}_L \subseteq \mathcal{O}_K+\nu\mathcal{O}_L\}$. But as ν is inert in L, $\nu\mathcal{O}_L$ is a maximal ideal, and since $\mathcal{O}_K + \nu\mathcal{O}_L \neq \mathcal{O}_L$, $\mathfrak{f}_{(\mathcal{O}_K+\nu\mathcal{O}_L)/\mathcal{O}_K} \neq \mathcal{O}_L$, so $\mathfrak{f}_{(\mathcal{O}_K+\nu\mathcal{O}_L)/\mathcal{O}_K} = \nu\mathcal{O}_L$. This implies $\nu\mathcal{O}_L \mid \mathfrak{f}_{\Omega/\mathcal{O}_K}$, a contradiction.

So there must exist an $a \in \Omega \setminus \mathcal{O}_K$ so that $a \notin \mathcal{O}_K + \nu\mathcal{O}_L$. This implies $\mathcal{O}_K[a]/(\nu\mathcal{O}_L \cap \mathcal{O}_K[a]) \ncong (\mathcal{O}_K/\nu\mathcal{O}_K)$, so we have $\mathcal{O}_L/\nu\mathcal{O}_L \cong \mathcal{O}_K[a]/(\nu\mathcal{O}_L \cap \mathcal{O}_K[a])$. By Lemma 4.7 of [15], $\nu \nmid N_{L/K}(\mathfrak{f}_{\mathcal{O}_K[a]/\mathcal{O}_K})$, as required. □

Proposition 3.6. *Suppose now that conditions (1) and (2) hold. Then precisely one-pth of the isomorphism classes of maximal orders in B admit an embedding of Ω. Those classes are characterized by means of the idelic Artin map $(*, L/K)$ as follows: $\mathcal{E}$ is a maximal order which contains a conjugate of Ω if and only if $(\rho(\mathcal{R},\mathcal{E}), L/K)$ is trivial in $Gal(L/K)$.*

Remark. We indicate our meaning of the Artin symbol $(\rho(\mathcal{R},\mathcal{E}), L/K)$. Recall that $\rho(\mathcal{R},\mathcal{E}) \in G_{\mathcal{R}} = J_K/H_{\mathcal{R}}$, and the Artin map $(*, K(\mathcal{R})/K)$ induces an isomorphism $G_{\mathcal{R}} \cong Gal(K(\mathcal{R})/K)$. Thus the Artin symbol $(\rho(\mathcal{R},\mathcal{E}), K(\mathcal{R})/K)$ is an element of $Gal(K(\mathcal{R})/K)$ which we restrict to L. The Artin map is compatible with this restriction giving that $(\rho(\mathcal{R},\mathcal{E}), K(\mathcal{R})/K))|_L = (\rho(\mathcal{R},\mathcal{E}), L/K)$.

Proof. We have assumed that $\Omega \subset \mathcal{R}$, and suppose that $\mathcal{E}$ is another maximal order in B. We shall show that $\mathcal{E}$ contains a conjugate of Ω (i.e. admits an embedding) if and only if the Artin symbol $(\rho(\mathcal{R},\mathcal{E}), L/K)$ is trivial in $Gal(L/K)$. We first show that $(\rho(\mathcal{R},\mathcal{E}), L/K)$ non-trivial in $Gal(L/K)$ implies that $\mathcal{E}$ does not contain a conjugate of Ω. We proceed by contradiction and assume that $\mathcal{E}$ does contain a conjugate of Ω. Then there is $b \in B^\times$ so that $\Omega \subset \mathcal{E}^* = b\mathcal{E}b^{-1}$. By Propositions 3.2 and 3.3,

$(\rho(\mathcal{R},\mathcal{E}),L/K) = (\rho(\mathcal{R},\mathcal{E}^*),L/K) \neq 1$, so there exists a prime ν of K which is inert in L so that $td_\nu(\mathcal{R}_\nu,\mathcal{E}_\nu^*) \not\equiv 0 \pmod p$. In particular, $\mathcal{R}_\nu$ and $\mathcal{E}_\nu^*$ are of different types, so indeed $\mathcal{R}_\nu \neq \mathcal{E}_\nu^*$. View these two maximal orders as vertices in the building for $SL_p(K_\nu)$, and choose an apartment containing them. We may assume that a basis $\{\omega_i\}$ for the apartment is chosen in such a way that one maximal order is $\mathrm{End}_{O_\nu}(\oplus\mathcal{O}_\nu\omega_i)$ which we identify with $M_p(\mathcal{O}_\nu)$ and the other with $\mathrm{End}_{O_\nu}(\oplus\mathcal{O}_\nu\pi^{m_i}\omega_i)$ $(0 \leq m_1 \leq \cdots \leq m_p)$, which is identified with $\mathrm{diag}(\pi^{m_1},\ldots,\pi^{m_p})M_p(\mathcal{O}_\nu)\mathrm{diag}(\pi^{m_1},\ldots,\pi^{m_p})^{-1} =$

$$\Lambda(m_1,\ldots,m_p) = \begin{pmatrix} \mathcal{O} & \nu^{m_1-m_2} & \nu^{m_1-m_3} & \cdots & \nu^{m_1-m_p} \\ \nu^{m_2-m_1} & \mathcal{O} & \nu^{m_2-m_3} & \cdots & \nu^{m_2-m_p} \\ \nu^{m_3-m_1} & \nu^{m_3-m_2} & \ddots & \cdots & \nu^{m_3-m_p} \\ \vdots & \vdots & & \mathcal{O} & \vdots \\ \nu^{m_p-m_1} & \cdots & & \nu^{m_p-m_{p-1}} & \mathcal{O} \end{pmatrix}.$$

We may assume without loss that $m_1 = 0$ since $\mathrm{End}(L)$ is unchanged by the homothety class of the lattice L, and since $\mathcal{R}_\nu \neq \mathcal{E}_\nu^*$, we must have that $m_p \geq 1$. Let ℓ be the smallest index so that $m_\ell \geq 1$. Note that the image of $M_p(\mathcal{O}_\nu) \cap \Lambda(m_1,\ldots,m_p)$ under the projection from $M_p(\mathcal{O}_\nu) \to M_p(\mathcal{O}_\nu/\nu\mathcal{O}_\nu)$ is contained in $\begin{pmatrix} M_{\ell-1}(\mathcal{O}_\nu/\nu\mathcal{O}_\nu) & * \\ 0 & M_{p-\ell+1}(\mathcal{O}_\nu/\nu\mathcal{O}_\nu) \end{pmatrix}$.

Since ν is inert and so by hypothesis $\nu \nmid N_{L/K}(\mathfrak{f}_{\Omega/\mathcal{O}_K})$, we can choose by the lemma, an element $a \in \Omega \setminus \mathcal{O}_K$, with $\nu \nmid N_{L/K}(\mathfrak{f}_{\mathcal{O}_K[a]/\mathcal{O}_K})$, and since L/K has prime degree, L is the field of fractions of $\mathcal{O}_K[a]$. This allows us to invoke the Dedekind-Kummer theorem (Theorem 4.12 of [15]). Let f be the minimal polynomial of a over K. Because L/K has prime degree and a is integral, $f \in \mathcal{O}_K[x]$ and is irreducible. Since Dedekind-Kummer applies, we consider the factorization of $\overline{f} \in (\mathcal{O}_K/\nu\mathcal{O}_K)[x]$ which will mirror the factorization of ν in the field L. Of course we know that ν is inert, so that $\overline{f}$ is irreducible in $(\mathcal{O}_K/\nu\mathcal{O}_K)[x]$. Now since $L \subset B$, we can view $a \in B_\nu \cong M_p(K_\nu)$. Without loss we identify B_ν with the matrix algebra. Let F be the characteristic polynomial of a over K_ν which, because a is integral, will have coefficients in $\mathcal{O}_\nu[x]$. Consider $\overline{F} \in (\mathcal{O}_\nu/\nu\mathcal{O}_\nu)[x] \cong (\mathcal{O}_K/\nu\mathcal{O}_K)[x]$. Now both $\overline{f}$ and $\overline{F}$ are polynomials of degree p in $(\mathcal{O}_K/\nu)[x]$ having $\bar{a}$ for a root. We know that $\overline{f}$ is irreducible, so $\overline{f} \mid \overline{F}$, from which it follows that $\overline{F} = \overline{f}$ by degree considerations, and hence is irreducible. On the other hand, since $a \in R_\nu \cap \mathcal{E}_\nu^*$ we know that its image under the projection from $M_p(\mathcal{O}_\nu) \to M_p(\mathcal{O}_\nu/\nu\mathcal{O}_\nu)$ lies in $\begin{pmatrix} M_{\ell-1}(\mathcal{O}_\nu/\nu\mathcal{O}_\nu) & * \\ 0 & M_{p-\ell+1}(\mathcal{O}_\nu/\nu\mathcal{O}_\nu) \end{pmatrix}$ which means that $\overline{F}$ (the characteristic polynomial of a) will be reducible over $\mathcal{O}_\nu/\nu\mathcal{O}_\nu$ by the inherent block structure, a contradiction.

Now we show the converse: Recall that $\Omega \subset \mathcal{R}$, and let $\mathcal{E}$ be another maximal order in B. We shall show that if the Artin symbol $(\rho(\mathcal{R},\mathcal{E}), L/K)$ is trivial in $Gal(L/K)$ then $\mathcal{E}$ contains a conjugate of Ω. By Proposition 3.2, we may choose primes $\nu_1, \ldots, \nu_m$ of K so that the $\{\overline{e}_{\nu_i}\}$ generate $G_{\mathcal{R}}$, where ν_i splits completely in L for $i > 1$ and where ν_1 is inert in L. Parametrize the isomorphism classes of maximal orders as in Equation (3.1), using $\mathcal{R}$ and in each completion B_{ν_i} assigning the types by using the vertices in a fixed chamber containing $\mathcal{R}_{\nu_i}$ in the $SL_p(K_\nu)$ building. Thus every maximal order is isomorphic to exactly one order $\mathcal{D}^\gamma$, for $\gamma \in (\mathbb{Z}/p\mathbb{Z})^m$. We have $\mathcal{R} = \mathcal{D}^{(0)}$. Let γ be fixed with $\mathcal{E} \cong \mathcal{D}^\gamma$. To establish our claim, we need only show that $\Omega \subset \mathcal{D}^\gamma$. By Proposition 3.3, $\rho(\mathcal{R},\mathcal{E}) = \rho(\mathcal{R},\mathcal{D}^\gamma)$ so $(\rho(\mathcal{R},\mathcal{D}^\gamma), L/K) = 1$. Recall that $\mathcal{D}^\gamma_\nu = R_\nu$ for all $\nu \neq \nu_i$ and the primes $\nu_2, \ldots, \nu_m$ all split completely in L. Thus $(\rho(\mathcal{R},\mathcal{D}^\gamma), L/K) = (\nu_1^{td_{\nu_1}(\mathcal{R}_{\nu_1},\mathcal{D}^\gamma_{\nu_1})}, L/K) = 1$. Since the Artin symbol $(\nu_1, L/K)$ has order p in $Gal(L/K)$, we have that $td_{\nu_1}(\mathcal{R}_{\nu_1},\mathcal{D}^\gamma_{\nu_1}) \equiv 0 \pmod{p}$. But given that the parametrization used the vertices in a fixed chamber of the building, this is only possible if $\mathcal{D}^\gamma_{\nu_1} = R_{\nu_1}$, so of course $\Omega \subset \mathcal{D}^\gamma_{\nu_1}$. That $\Omega \subset \mathcal{D}^\gamma_{\nu_i}$ for $i = 2, \ldots, m$ follows in exactly the same way as in the proof of Proposition 3.4. Finally for $\nu \neq \nu_i$, $\Omega \subset \mathcal{R}_\nu = \mathcal{D}^\gamma_\nu$. Thus $\Omega \subset \mathcal{D}^\gamma_\nu$ for all primes ν, and the argument is complete. □

References

1. Peter Abramenko and Kenneth S. Brown, *Buildings*. Graduate Texts in Mathematics, vol. **248**, Springer, New York, 2008, Theory and applications. MR MR2439729
2. Luis Arenas-Carmona, *Applications of spinor class fields: embeddings of orders and quaternionic lattices*. Ann. Inst. Fourier (Grenoble) **53** (2003), no. 7, 2021–2038. MR MR2044166 (2005b:11044)
3. Kenneth S. Brown, *Buildings*. Springer-Verlag, New York, 1989. MR MR969123 (90e:20001)
4. J. Brzezinski, *On two classical theorems in the theory of orders*. J. Number Theory **34** (1990), no. 1, 21–32. MR MR1039764 (91d:11142)
5. Wai Kiu Chan and Fei Xu, *On representations of spinor genera*. Compos. Math. **140** (2004), no. 2, 287–300. MR MR2027190 (2004j:11035)
6. C. Chevalley, *Algebraic number fields*. L'arithmétique dans les algèbres de matrices, Herman, Paris, 1936.
7. Ted Chinburg and Eduardo Friedman, *An embedding theorem for quaternion algebras*. J. London Math. Soc. (2) **60** (1999), no. 1, 33–44. MR MR1721813 (2000j:11173)
8. A. Fröhlich, *Locally free modules over arithmetic orders*. J. Reine Angew. Math. **274/275** (1975), 112–124, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. MR MR0376619 (51 #12794)
9. Paul Garrett, *Buildings and classical groups*. Chapman & Hall, London, 1997. MR 98k:20081
10. Xuejun Guo and Hourong Qin, *An embedding theorem for Eichler orders*. J. Number Theory **107** (2004), no. 2, 207–214. MR MR2072384 (2005c:11141)
11. P. J. Higgins, *Introduction to topological groups*. Cambridge University Press, London, 1974, London Mathematical Society Lecture Note Series, No. **15**. MR MR0360908 (50 #13355)
12. Serge Lang, *Algebraic number theory*, second ed. Graduate Texts in Mathematics, vol. **11**, Springer-Verlag, New York, 1994. MR MR1282723 (95f:11085)

13. B. Linowitz, *Selectivity in quaternion algebras*. J. of Number Theory **132** (2012), 1425–1437.
14. C. Maclachlan, *Optimal embeddings in quaternion algebras*. J. Number Theory **128** (2008), 2852–2860.
15. Władysław Narkiewicz, *Elementary and analytic theory of algebraic numbers*, second ed. Springer-Verlag, Berlin, 1990. MR MR1055830 (91h:11107)
16. Jürgen Neukirch, *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. **322**, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR MR1697859 (2000m:11104)
17. Richard S. Pierce, *Associative algebras*. Graduate Texts in Mathematics, vol. **88**, Springer-Verlag, New York, 1982, , Studies in the History of Modern Science, **9**. MR MR674652 (84c:16001)
18. I. Reiner, *Maximal orders*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975, London Mathematical Society Monographs, No. **5**. MR MR0393100 (52 #13910)
19. Mark Ronan, *Lectures on buildings*. Academic Press Inc., Boston, MA, 1989. MR 90j:20001
20. Thomas R. Shemanske, *Split orders and convex polytopes in buildings*. J. Number Theory **130** (2010), no. 1, 101–115. MR MR2569844

Benjamin Linowitz
Department of Mathematics
6188 Kemeny Hall
Dartmouth College
Hanover, NH 03755
E-mail: benjamin.linowitz@dartmouth.edu
URL: http://www.math.dartmouth.edu/~linowitz/

Thomas R. Shemanske
Department of Mathematics
6188 Kemeny Hall
Dartmouth College
Hanover, NH 03755
E-mail: thomas.r.shemanske@dartmouth.edu
URL: http://www.math.dartmouth.edu/~trs/