



ELSEVIER

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



Selectivity in quaternion algebras

Benjamin Linowitz

Department of Mathematics, 6188 Kemeny Hall, Dartmouth College, Hanover, NH 03755, USA

ARTICLE INFO

Article history:

Received 14 October 2009

Revised 2 June 2011

Accepted 13 January 2012

Available online 3 March 2012

Communicated by Kenneth A. Ribet

Keywords:

Quaternion algebra

Order

ABSTRACT

We prove an integral version of the classical Albert–Brauer–Hasse–Noether theorem regarding quaternion algebras over number fields. Let K be a number field with ring of integers \mathcal{O}_K , and let \mathfrak{A} be a quaternion algebra over K satisfying the Eichler condition. Let Ω be a commutative, quadratic \mathcal{O}_K -order and let $\mathcal{R} \subset \mathfrak{A}$ be an order of full rank. Assume that there exists an embedding of Ω into \mathcal{R} . We describe a number of criteria which imply that every order in the genus of \mathcal{R} admits an embedding of Ω . In the case that the relative discriminant ideal of Ω is coprime to the level of \mathcal{R} and the level of \mathcal{R} is coprime to the discriminant of \mathfrak{A} , we give necessary and sufficient conditions for an order in the genus of \mathcal{R} to admit an embedding of Ω . We explicitly parameterize the isomorphism classes of orders in the genus of \mathcal{R} which admit an embedding of Ω . In particular, we show that the proportion of the genus of \mathcal{R} admitting an embedding of Ω is either 0, $1/2$ or 1. Analogous statements are proven for optimal embeddings.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

The study of non-commutative algebras has a long and rich history with applications in class field theory, modular forms and geometry. One of the high points of this history came in 1932, when much of the field's foundational work was being done, with the publication of the Brauer–Hasse–Noether theorem. Although his name did not appear on the publication, many of the results contained in the Brauer–Hasse–Noether theorem were proven independently by Adrian Albert in 1931. We are interested in the quaternionic version of their theorem:

E-mail address: Benjamin.D.Linowitz@dartmouth.edu.

Theorem 1.1 (Albert–Brauer–Hasse–Noether). *Let \mathfrak{A} be a quaternion algebra over a number field K and let L be a quadratic field extension of K . Then there is an embedding of L into \mathfrak{A} if and only if no prime of K which ramifies in \mathfrak{A} splits in L .*

In this paper we consider an integral refinement of the Albert–Brauer–Hasse–Noether theorem. Let \mathfrak{A} be a quaternion algebra defined over a number field K which satisfies the Eichler condition; that is, there exists an archimedean prime of K which does not ramify in \mathfrak{A} . Let L be a quadratic field extension of K and Ω a quadratic order of L . Finally, let $\mathcal{R} \subset \mathfrak{A}$ be an \mathcal{O}_K -order of full rank. We are interested in the question of when there exists an embedding of Ω into \mathcal{R} .

Chinburg and Friedman considered a special case of this question in their paper [4], where they determined the maximal orders into which Ω can be embedded. We now state a simplified version of their main theorem (see [4] for notation):

Theorem 1.2 (Chinburg–Friedman). *Let L be a quadratic field extension of K which embeds into the quaternion algebra \mathfrak{A} , and assume that \mathfrak{A} satisfies the Eichler condition. Then a quadratic \mathcal{O}_K -order $\Omega \subset L$ can be embedded into either all of the maximal \mathcal{O}_K -orders $\mathcal{D} \subset \mathfrak{A}$, or into all those belonging to exactly half of the isomorphism types of maximal \mathcal{O}_K -orders in \mathfrak{A} . In the latter case the maximal orders admitting an embedding of Ω may be described as follows. If \mathcal{R} and \mathcal{S} are maximal orders and \mathcal{R} admits an embedding of Ω , then \mathcal{S} admits an embedding of Ω if and only if the image by the reciprocity map $\text{Frob}_{L/K}$ of the distance ideal $\rho(\mathcal{R}, \mathcal{S})$ is the trivial element of $\text{Gal}(L/K)$.*

Theorem 1.2 is especially significant because of its applications, particularly its applications to differential geometry. As our results will have similar applications, we give a brief sketch of the relevant construction. Suppose that $K \neq \mathbb{Q}$ is totally real and that \mathfrak{A} is unramified at a unique real place of K . Let $\mathcal{R}_1, \mathcal{R}_2$ be two orders of \mathfrak{A} which lie in the same genus (i.e. have locally isomorphic completions at all finite primes of K) but represent distinct isomorphism classes. Vigneras [10] used \mathcal{R}_1 and \mathcal{R}_2 to construct compact, non-isometric hyperbolic 2-manifolds M_1 and M_2 . Further, she showed that M_1 and M_2 are isospectral (have the same spectra with respect to the Laplace–Beltrami operator) if there did not exist a quadratic \mathcal{O}_K -order Ω which could be embedded into exactly one of the \mathcal{R}_i . When \mathcal{R}_1 and \mathcal{R}_2 are taken to be maximal orders, Theorem 1.2 can be used to determine necessary and sufficient conditions for M_1 and M_2 to be isospectral.

Chinburg and Friedman’s theorem was later generalized to Eichler orders independently by Guo and Qin [5] and Chan and Xu [2]. It is interesting to note that whereas Guo and Qin make use of tree-theoretic techniques (as Chinburg and Friedman did) in their generalization, Chan and Xu instead use the representation theory of spinor genera.

In this paper we obtain a number of generalizations of Chinburg and Friedman’s theorem. Central to our arguments will be the class field $K(\mathcal{R})$ associated to the order \mathcal{R} (defined in Section 3 immediately after the proof of Theorem 3.3). The class field $K(\mathcal{R})$ is an abelian extension of K whose degree is the number of isomorphism classes in the genus of \mathcal{R} , whose Galois group is of exponent 2 and whose conductor is divisible only by the prime divisors of the level ideal $N_{\mathcal{R}}$ of \mathcal{R} (defined in Section 2); that is, the primes ν of K for which \mathcal{R}_{ν} is not maximal.

In Section 5.1 we consider arbitrary orders $\mathcal{R} \subset \mathfrak{A}$ and describe a number of criteria which, if satisfied, imply that every order in the genus of \mathcal{R} admits an embedding of a given commutative, quadratic \mathcal{O}_K -order Ω . The main result of the section is

Theorem 1.3. *Let L be a maximal subfield of \mathfrak{A} , $\Omega \subset L$ a quadratic \mathcal{O}_K -order and assume that an embedding of Ω into \mathcal{R} exists.*

- (1) *If $L \not\subset K(\mathcal{R})$, then every order in the genus of \mathcal{R} admits an embedding of Ω .*
- (2) *If $L \subset K(\mathcal{R})$, then the proportion of isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω is at least $1/2$.*

An easy consequence of Theorem 1.3 is that if Ω embeds into an order \mathcal{R} , then every representative of at least half of the isomorphism classes in the genus of \mathcal{R} admits an embedding of Ω . Another

consequence is that if any prime of K which does not divide the level ideal $N_{\mathcal{R}}$ ramifies in L then every order in the genus of \mathcal{R} admits an embedding of Ω . This is especially nice in applications because in practice the computation of $K(\mathcal{R})$ can be quite difficult. In a future publication we will apply Theorem 1.3 in order to construct *isospectral towers* of hyperbolic manifolds; that is, pairs of infinite towers $\{M_i\}, \{N_i\}$ of finite covers of hyperbolic manifolds M and N such that the covers M_j and N_j are isospectral, but not isometric for every j .

In Section 5.2 we constrain slightly the class of orders $\mathcal{R} \subset \mathfrak{A}$ that we consider and provide necessary and sufficient conditions for an order Ω to embed into some, but not all, orders in the genus of \mathcal{R} . The main result of Section 5.2 is:

Theorem 1.4. *Assume that an embedding of Ω into \mathcal{R} exists. Assume as well that the relative discriminant ideal d_{Ω/\mathcal{O}_K} of Ω is coprime to the level ideal $N_{\mathcal{R}}$ of \mathcal{R} and that the set of primes dividing $N_{\mathcal{R}}$ is disjoint from the set of primes ramifying in \mathfrak{A} . Then every order in the genus of \mathcal{R} admits an embedding of Ω except when the following conditions hold:*

- (1) Ω is an integral domain whose quotient field L is a quadratic field extension of K which is contained in \mathfrak{A} .
- (2) There is a containment of fields $L \subset K(\mathcal{R})$.
- (3) All primes of K which divide the relative discriminant ideal d_{Ω/\mathcal{O}_K} of Ω split in L/K .

Suppose now that (1)–(3) hold. Then the isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω comprise exactly half of the isomorphism classes. If \mathcal{R} admits an embedding of Ω and \mathcal{E} is another order in the genus of \mathcal{R} , then \mathcal{E} admits an embedding of Ω if and only if $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is the trivial element of $\text{Gal}(L/K)$.

The proof of Theorem 1.4 makes extensive use of the tree of maximal orders of $M_2(k)$ (for k a local field), allowing us to parameterize explicitly the orders in the genus of \mathcal{R} admitting an embedding of Ω , explicit enough to specify them via the local–global correspondence.

In Section 6 we consider the related question of when there exists an *optimal embedding* of Ω into \mathcal{R} . Maclachlan [8] considered Eichler orders of square-free level and proved that the proportion of isomorphism classes of orders in the genus of \mathcal{R} admitting an optimal embedding of Ω is equal to 0, $\frac{1}{2}$ or 1. We show that Theorems 1.3 and 1.4 hold not only for embeddings but for optimal embeddings as well. These theorems are of independent interest however, in part because of the ubiquity of optimal embeddings in number theory. For example, optimal embeddings play an important role in Hijikata’s [6] formula for the trace of Hecke operators acting on spaces of \mathcal{R}^\times -automorphic cusp forms.

2. Notation

In this section we fix the notation concerning quaternion algebras and their orders that will be used throughout this paper.

Let K be a number field with ring of integers \mathcal{O}_K . Let \mathfrak{A} be a quaternion algebra over K with reduced norm n . We denote by K_ν the completion of K at a prime ν of K . If ν is a non-archimedean prime, we let \mathcal{O}_{K_ν} be the valuation ring of K_ν and π_ν a fixed uniformizer. When there will be no confusion we will write \mathcal{O}_ν in place of \mathcal{O}_{K_ν} . We denote by \mathfrak{A}_ν the K_ν -algebra $\mathfrak{A} \otimes_K K_\nu$ and by \mathfrak{A}^1 (resp. \mathfrak{A}_ν^1) the elements of \mathfrak{A} (resp. \mathfrak{A}_ν) having reduced norm equal to 1. We let J_K denote the idele group of K and $J_{\mathfrak{A}}$ the idele group of \mathfrak{A} .

Given an \mathcal{O}_K -order $\mathcal{R} \subset \mathfrak{A}$ (having maximal rank) and a prime ν of K , we define the completions $\mathcal{R}_\nu \subset \mathfrak{A}_\nu$ by:

$$\mathcal{R}_\nu = \begin{cases} \mathcal{R} \otimes_{\mathcal{O}_K} \mathcal{O}_\nu & \text{if } \nu \text{ is non-archimedean,} \\ \mathcal{R} \otimes_{\mathcal{O}_K} K_\nu = \mathfrak{A}_\nu & \text{if } \nu \text{ is archimedean.} \end{cases}$$

For almost all finite primes ν of K , $\mathfrak{A}_\nu \cong M_2(K_\nu)$ and $\mathcal{R}_\nu \cong M_2(\mathcal{O}_\nu)$, so we will identify \mathfrak{A}_ν with $M_2(K_\nu)$. Define the normalizer of \mathcal{R}_ν in \mathfrak{A}_ν^\times to be $N(\mathcal{R}_\nu) = \{x \in \mathfrak{A}_\nu^\times : x\mathcal{R}_\nu x^{-1} = \mathcal{R}_\nu\}$. This

normalizer, along with its image under the reduced norm, is central to determining whether the class field associated to \mathcal{R} admits finite ramification. We therefore note that whenever ν is a finite prime of K which is unramified in \mathfrak{A} and \mathcal{R}_ν is a maximal order of \mathfrak{A}_ν , its normalizer is conjugate to $GL_2(\mathcal{O}_\nu)K_\nu^\times$ and hence, $n(N(\mathcal{R}_\nu)) = \mathcal{O}_\nu^\times K_\nu^{\times 2}$.

We define the *level ideal* $N_{\mathcal{R}}$ of \mathcal{R} to be the order-ideal [9, p. 49] of the \mathcal{O}_K -module \mathcal{M}/\mathcal{R} , where \mathcal{M} is any maximal order of \mathfrak{A} containing \mathcal{R} . This definition is independent of the choice of maximal order \mathcal{M} .

3. The class field associated to an order

Let \mathfrak{A} be a quaternion algebra over a number field K satisfying the Eichler condition; that is, there exists an archimedean prime of K which splits in \mathfrak{A} . The reason for this assumption, as will soon be made clear, is that it is only in this context that the Strong Approximation theorem may be applied.

We say that two orders \mathcal{R}_1 and \mathcal{R}_2 are of the same *genus* if $\mathcal{R}_{1\nu}$ is \mathcal{O}_ν -isomorphic to $\mathcal{R}_{2\nu}$ for all finite primes ν of K . The *type number* $t(\mathcal{R})$ of an order \mathcal{R} is defined to be the number of isomorphism classes of orders in the genus of \mathcal{R} .

Example 3.1. Let $\mathcal{M} \subset \mathfrak{A}$ be a maximal order (of full rank). For every finite prime ν of K , \mathcal{M}_ν is a maximal order of \mathfrak{A}_ν . If ν is a finite prime splitting in \mathfrak{A} , then it is well known that every maximal order of \mathfrak{A}_ν is conjugate to \mathcal{M}_ν . If ν is a finite prime ramifying in \mathfrak{A} , then \mathcal{M}_ν is the unique maximal order of \mathfrak{A}_ν . It follows that the collection of all maximal orders of \mathfrak{A} comprise the genus of \mathcal{M} .

Example 3.2. Let $\mathcal{E} \subset \mathfrak{A}$ be an Eichler order of level \mathfrak{N} (where \mathfrak{N} is coprime to the discriminant of \mathfrak{A}). Recall that this means that \mathcal{E} is an order of \mathfrak{A} (of full rank) with the property that \mathcal{E}_ν is maximal if ν ramifies in \mathfrak{A} , and if ν splits in \mathfrak{A} then \mathcal{E}_ν is conjugate to

$$\begin{pmatrix} \mathcal{O}_\nu & \mathcal{O}_\nu \\ \mathfrak{N}\mathcal{O}_\nu & \mathcal{O}_\nu \end{pmatrix}.$$

It follows that the genus of \mathcal{E} is the collection of all Eichler orders of level \mathfrak{N} .

Let $\mathcal{R} \subset \mathfrak{A}$ be an order (of maximal rank). The isomorphism classes of orders in the genus of \mathcal{R} are in one-to-one correspondence with points in the double coset space $\mathfrak{A}^\times \backslash J_{\mathfrak{A}} / \mathfrak{N}(\mathcal{R})$, where $\mathfrak{N}(\mathcal{R}) = J_{\mathfrak{A}} \cap \prod_\nu N(\mathcal{R}_\nu)$. This bijection is induced by the map sending an order \mathcal{E} belonging to the genus of \mathcal{R} to the double coset $\mathfrak{A}^\times \tilde{x}_{\mathcal{E}} \mathfrak{N}(\mathcal{R})$, where $\tilde{x}_{\mathcal{E}} = (x_{\mathcal{E}_\nu})$ is an element of $J_{\mathfrak{A}}$ such that $x_{\mathcal{E}_\nu} \mathcal{E}_\nu x_{\mathcal{E}_\nu}^{-1} = \mathcal{R}_\nu$ for all ν .

Theorem 3.3. *The reduced norm induces a bijection of sets*

$$n : \mathfrak{A}^\times \backslash J_{\mathfrak{A}} / \mathfrak{N}(\mathcal{R}) \longrightarrow K^\times \backslash J_K / n(\mathfrak{N}(\mathcal{R})).$$

Proof. The induced map is defined in the obvious way: $n(\mathfrak{A}^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R})) = K^\times n(\tilde{\alpha} n(\mathfrak{N}(\mathcal{R})))$.

We first show that n is surjective. Let $\tilde{\beta} \in J_K$. We may assume, by the weak approximation theorem, that $\beta_\nu > 0$ for every infinite prime ν ramifying in \mathfrak{A} . The reduced norm is locally surjective at all finite primes and at the infinite primes not ramifying in \mathfrak{A} . At the infinite primes ramifying in \mathfrak{A} the image of the reduced norm consists of the non-negative reals. We construct an idele $\tilde{\alpha} \in J_{\mathfrak{A}}$ such that $n(\mathfrak{A}^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R})) = K^\times \tilde{\beta} n(\mathfrak{N}(\mathcal{R}))$. For all but finitely many non-archimedean primes ν of K , $\beta_\nu \in \mathcal{O}_\nu^\times$ and $\mathcal{R}_\nu \cong M_2(\mathcal{O}_\nu)$. For each such prime ν , let α_ν be the conjugate of the diagonal matrix $\text{diag}(\beta_\nu, 1)$ lying in \mathcal{R}_ν . For the other primes, define α_ν to be any element in the preimage of β_ν . The constructed element $\tilde{\alpha} = (\alpha_\nu)_\nu$ is easily seen to lie in $J_{\mathfrak{A}}$ and establishes surjectivity.

We now show that n is injective. Denote by $J_{\mathfrak{A}}^1$ the kernel of the reduced norm map $n : J_{\mathfrak{A}} \rightarrow J_K$. We show that $\mathfrak{A}^\times J_{\mathfrak{A}}^1 \mathfrak{N}(\mathcal{R})$ is the preimage of $K^\times n(\mathfrak{N}(\mathcal{R}))$. It is obvious that $\mathfrak{A}^\times J_{\mathfrak{A}}^1 \mathfrak{N}(\mathcal{R})$ is contained

in the preimage. Let $\tilde{\gamma} \in J_{\mathfrak{A}}$ be such that $n(\mathfrak{A}^\times \tilde{\gamma} \mathfrak{N}(\mathcal{R})) = K^\times n(\mathfrak{N}(\mathcal{R}))$. Then $n(\tilde{\gamma}) = k \cdot n(\tilde{r})$ where $k \in K^\times$ and $\tilde{r} \in \mathfrak{N}(\mathcal{R})$. If ν is an infinite prime ramifying in \mathfrak{A} then $n(\tilde{\gamma}_\nu), n(\tilde{r}_\nu) > 0$. Thus $k_\nu > 0$ as well. The Hasse–Schilling–Maass theorem (Theorem 33.15 of [9]) implies that there exists $b \in \mathfrak{A}^\times$ such that $n(b) = k$ and $n(\tilde{\gamma}) = n(b)n(\tilde{r})$, hence $n(b^{-1})n(\tilde{\gamma})n(\tilde{r}^{-1}) = (1) \in J_K$. This shows that $\mathfrak{A}^\times \tilde{\gamma} \mathfrak{N}(\mathcal{R}) = \mathfrak{A}^\times b^{-1} \tilde{\gamma} \tilde{r}^{-1} \mathfrak{N}(\mathcal{R}) \in \mathfrak{A}^\times J_{\mathfrak{A}}^1 \mathfrak{N}(\mathcal{R})$ as claimed.

We now continue with our proof of injectivity. Suppose that there exist $\tilde{\alpha}, \tilde{\beta} \in J_{\mathfrak{A}}$ such that $n(\mathfrak{A}^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R})) = n(\mathfrak{A}^\times \tilde{\beta} \mathfrak{N}(\mathcal{R}))$. Then $n(\tilde{\alpha}^{-1} \tilde{\beta}) \in K^\times n(\mathfrak{N}(\mathcal{R}))$ and by the above claim $\tilde{\alpha}^{-1} \tilde{\beta} \in \mathfrak{A}^\times J_{\mathfrak{A}}^1 \mathfrak{N}(\mathcal{R})$. Making use of the fact that $\mathfrak{A}^\times J_{\mathfrak{A}}^1$ is a normal subgroup of $J_{\mathfrak{A}}$, we see that $\tilde{\beta} \in \tilde{\alpha} \mathfrak{A}^\times J_{\mathfrak{A}}^1 \mathfrak{N}(\mathcal{R}) = \mathfrak{A}^\times J_{\mathfrak{A}}^1 \tilde{\alpha} \mathfrak{N}(\mathcal{R})$.

Let S be the set of archimedean places of K and define $\mathfrak{A}_S^1 = \prod_{\nu \in S} \mathfrak{A}_\nu^1$. Recall the Strong Approximation theorem [11, Theorem 4.3]: if \mathfrak{A}_S^1 is not compact, then $\mathfrak{A}^1 \mathfrak{A}_S^1$ is dense in $J_{\mathfrak{A}}^1$. Recalling that \mathfrak{A}_ν^1 is compact if and only if ν ramifies in \mathfrak{A} , our assumption that \mathfrak{A} satisfy the Eichler condition implies that there exists an archimedean prime ν of K such that \mathfrak{A}_ν^1 is not compact. It follows that \mathfrak{A}_S^1 is not compact. For any $\tilde{\gamma} \in J_{\mathfrak{A}}$, $\tilde{\gamma} \mathfrak{N}(\mathcal{R}) \tilde{\gamma}^{-1}$ contains a neighborhood of the identity and is therefore an open subgroup of $J_{\mathfrak{A}}$ containing \mathfrak{A}_S^1 , hence $J_{\mathfrak{A}}^1 \subset \mathfrak{A}^\times \tilde{\gamma} \mathfrak{N}(\mathcal{R}) \tilde{\gamma}^{-1}$. Choosing $\tilde{\gamma} = \tilde{\alpha}$, we have

$$\tilde{\beta} \in \mathfrak{A}^\times J_{\mathfrak{A}}^1 \tilde{\alpha} \mathfrak{N}(\mathcal{R}) \subset \mathfrak{A}^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R}).$$

Therefore $\mathfrak{A}^\times \tilde{\beta} \mathfrak{N}(\mathcal{R}) \subset \mathfrak{A}^\times \tilde{\alpha} \mathfrak{N}(\mathcal{R})$, and by symmetry, we have equality. \square

We have shown that the isomorphism classes comprising the genus of a fixed order $\mathcal{R} \subset \mathfrak{A}$ are in one-to-one correspondence with the double cosets of the group $K^\times \backslash J_K / n(\mathfrak{N}(\mathcal{R}))$. Set $H_{\mathcal{R}} = K^\times n(\mathfrak{N}(\mathcal{R}))$ and $G_{\mathcal{R}} = J_K / H_{\mathcal{R}}$. As J_K is abelian, $G_{\mathcal{R}} \cong K^\times \backslash J_K / n(\mathfrak{N}(\mathcal{R}))$. Since $H_{\mathcal{R}}$ is an open subgroup of J_K , associated to it is a class field $K(\mathcal{R})$ whose arithmetic is intimately related to the arithmetic of \mathcal{R} in \mathfrak{A} . The basic properties of $K(\mathcal{R})$ are given by the standard theorems of class field theory (see for example Chapter 11 of [7]). In particular, we note that the conductor of $K(\mathcal{R})$ is divisible only by prime divisors of the level ideal $N_{\mathcal{R}}$ of \mathcal{R} .

We now prove that $G_{\mathcal{R}}$ can be generated by elements having a very simple form and that in fact, $G_{\mathcal{R}}$ is an elementary abelian group of exponent 2.

Lemma 3.4. *$G_{\mathcal{R}}$ is generated by cosets having representatives of the form $e_{v_i} = (1, \dots, 1, \pi_{v_i}, 1, \dots)$. If S is any finite set of primes of K , then the representatives $\{e_{v_i}\}$ can be taken so that $v_i \notin S$ for all i .*

Proof. The Chebotarev density theorem guarantees that every element of $\text{Gal}(K(\mathcal{R})/K)$ has infinitely many prime ideals in its preimage under the Artin map. As these prime ideals correspond to ideals of the form $(1, 1, \dots, 1, \pi_{v_i}, 1, \dots)$, $G_{\mathcal{R}}$ can be generated by cosets having representatives of the form e_{v_i} . Only finitely many primes of K lie in S and a given element of $G_{\mathcal{R}}$ has infinitely many prime ideals in its preimage, so each v_i can be chosen so that $v_i \notin S$. \square

Proposition 3.5. *The group $G_{\mathcal{R}}$ is an elementary abelian group of exponent 2.*

Proof. This is clear since $J_K^2 \subset n(\mathfrak{N}(\mathcal{R}))$. \square

Given orders \mathcal{D}, \mathcal{E} in the genus of \mathcal{R} , we define the distance $\rho(\mathcal{D}, \mathcal{E})$ as follows. Let $\tilde{x}_{\mathcal{D}}, \tilde{x}_{\mathcal{E}}$ be defined as in the paragraph preceding Theorem 3.3. We define $\rho(\mathcal{D}, \mathcal{E})$ to be the coset $n(\tilde{x}_{\mathcal{D}}^{-1} \tilde{x}_{\mathcal{E}}) H_{\mathcal{R}}$ in $G_{\mathcal{R}}$. By Proposition 3.5 this is the same coset as $n(\tilde{x}_{\mathcal{D}} \tilde{x}_{\mathcal{E}}) H_{\mathcal{R}}$. It is not difficult to see that our definition of $\rho(-, -)$ is well-defined. Indeed, let $\tilde{x}'_{\mathcal{D}}, \tilde{x}'_{\mathcal{E}}$ be another pair of ideles such that $x'_{\mathcal{D}_\nu} \mathcal{D}_\nu (x'_{\mathcal{D}_\nu})^{-1} = \mathcal{R}_\nu = x'_{\mathcal{E}_\nu} \mathcal{E}_\nu (x'_{\mathcal{E}_\nu})^{-1}$ for all ν . It is clear from Theorem 3.3 and the paragraph preceding it that this implies $\mathfrak{A}^\times \tilde{x}'_{\mathcal{D}} \mathfrak{N}(\mathcal{R}) = \mathfrak{A}^\times \tilde{x}_{\mathcal{D}} \mathfrak{N}(\mathcal{R})$ and $\mathfrak{A}^\times \tilde{x}'_{\mathcal{E}} \mathfrak{N}(\mathcal{R}) = \mathfrak{A}^\times \tilde{x}_{\mathcal{E}} \mathfrak{N}(\mathcal{R})$, hence $n(\tilde{x}'_{\mathcal{D}} \tilde{x}'_{\mathcal{E}}) H_{\mathcal{R}} = n(\tilde{x}_{\mathcal{D}} \tilde{x}_{\mathcal{E}}) H_{\mathcal{R}}$. Similar arguments show that the following elementary properties are satisfied.

Proposition 3.6. *Let $\mathcal{D}, \mathcal{E}, \mathcal{E}'$ lie in the genus of \mathcal{R} .*

- (1) $\rho(\mathcal{D}, \mathcal{E}) = \rho(\mathcal{E}, \mathcal{D})$.
- (2) $\rho(\mathcal{D}, \mathcal{E})$ is trivial if and only if $\mathcal{D} \cong \mathcal{E}$.
- (3) If $\mathcal{E} \cong \mathcal{E}'$ then $\rho(\mathcal{D}, \mathcal{E}) = \rho(\mathcal{D}, \mathcal{E}')$.

Let L be a quadratic field extension of K . We have shown that $G_{\mathcal{R}}$ is an elementary abelian group of exponent 2 with generators $\overline{e_{v_i}} = e_{v_i} H_{\mathcal{R}}$. We now show that the generators $\{\overline{e_{v_i}}\}$ can be chosen so that the primes v_i have certain splitting properties in L/K .

Lemma 3.7. *Let notation be as above.*

- (1) If $L \not\subset K(\mathcal{R})$, then $G_{\mathcal{R}}$ is generated by elements $\{\overline{e_{v_i}}\}$ where v_i splits in L for all i .
- (2) If $L \subset K(\mathcal{R})$, then $G_{\mathcal{R}}$ is generated by elements $\{\overline{e_{v_i}}\}$ where v_i splits in L for all $i > 1$, and v_1 is inert in L .

Proof. We first suppose that $L \not\subset K(\mathcal{R})$. By the Chebotarev density theorem we may generate $\text{Gal}(K(\mathcal{R})L/L)$ with the Frobenius elements associated to primes of L having degree one over K (since the set of primes of L with degree greater than one over K has density zero). As $\text{Gal}(K(\mathcal{R})L/L)$ is isomorphic to $\text{Gal}(K(\mathcal{R})/K)$ via restriction to $K(\mathcal{R})$, we may generate the latter group with Frobenius elements associated to primes of K splitting completely in L/K . These automorphisms correspond, via the Artin map, to the generators $\{\overline{e_{v_i}}\}_{i=1}^m$ of $G_{\mathcal{R}}$. We have therefore proven the first assertion.

Suppose now that $L \subset K(\mathcal{R})$. Let λ be a prime of K which is inert in the extension L/K and set $v_1 = \lambda$. Indeed, viewing $\text{Gal}(K(\mathcal{R})/L)$ as a subgroup of $\text{Gal}(K(\mathcal{R})/K)$, consider the set $\{(\lambda, K(\mathcal{R})/K), \{(v_j, K(\mathcal{R})/K)\}_{j=2}^m\}$ where $\{(v_j, K(\mathcal{R})/K)\}_{j=2}^m$ is an $m - 1$ element generating set of $\text{Gal}(K(\mathcal{R})/L)$. We claim that this set generates $\text{Gal}(K(\mathcal{R})/K)$. As $\text{Gal}(K(\mathcal{R})/K)$ and $\text{Gal}(K(\mathcal{R})/L)$ are elementary abelian groups of exponent 2, they are \mathbb{F}_2 -vector spaces. The set $\{(v_j, K(\mathcal{R})/K)\}_{j=2}^m$ is therefore a basis of $\text{Gal}(K(\mathcal{R})/L)$, hence linearly independent. To show that $\{(\lambda, K(\mathcal{R})/K), \{(v_j, K(\mathcal{R})/K)\}_{j=2}^m\}$ is a basis for $\text{Gal}(K(\mathcal{R})/K)$, it suffices to show that $(\lambda, K(\mathcal{R})/K)$ is not an \mathbb{F}_2 -linear combination of elements of $\{(v_j, K(\mathcal{R})/K)\}_{j=2}^m$. But this is clear as all of the elements of $\{(v_j, K(\mathcal{R})/K)\}_{j=2}^m$ restrict to the trivial element of $\text{Gal}(L/K)$ while $(\lambda, K(\mathcal{R})/K)$ does not. \square

4. Parameterizing the genus of \mathcal{R}

Let $\{e_{v_i}\}_{i=1}^m \subset J_K$ be such that $\{\overline{e_{v_i}}\}_{i=1}^m$ generate $G_{\mathcal{R}} = J_K/K^\times n(\mathfrak{N}(\mathcal{R})) \cong (\mathbb{Z}/2\mathbb{Z})^m$. By Lemma 3.4 one may choose this generating set so that each v_i is non-archimedean and split in \mathfrak{A} and so that \mathcal{R}_{v_i} is maximal for $1 \leq i \leq m$. Throughout the remainder of this paper we will only consider generating sets $\{\overline{e_{v_i}}\}_{i=1}^m$ of $G_{\mathcal{R}}$ which satisfy these properties. For each $1 \leq i \leq m$, let \mathcal{R}'_{v_i} be a maximal order of \mathfrak{A}_{v_i} which is adjacent to \mathcal{R}_{v_i} in the tree of maximal orders of $\mathfrak{A}_{v_i} \cong M_2(K_{v_i})$. For the basic definitions and properties concerning the tree of maximal orders of $M_2(k)$ (for k a local field) we refer the reader to Section 2.2 of [11].

Given $\gamma = (\gamma_i) \in (\mathbb{Z}/2\mathbb{Z})^m$, we define the order D^γ (via the local–global correspondence) as having the following local factors

$$D_v^\gamma = \begin{cases} \mathcal{R}_{v_i} & \text{if } v = v_i \text{ and } \gamma_i = 0, \\ \mathcal{R}'_{v_i} & \text{if } v = v_i \text{ and } \gamma_i = 1, \\ \mathcal{R}_v & \text{otherwise.} \end{cases}$$

We will show that the set $\{D^\gamma\}_{\gamma \in (\mathbb{Z}/2\mathbb{Z})^m}$ consists of representatives of all 2^m isomorphism classes in the genus of \mathcal{R} . We therefore call $\{D^\gamma\}_{\gamma \in (\mathbb{Z}/2\mathbb{Z})^m}$ a *parameterization* of the genus of \mathcal{R} . Note that by construction, if $\gamma = (0, 0, \dots)$, D^γ is \mathcal{R} .

Proposition 4.1. *Let notation be as above. The orders of $\{\mathcal{D}^\gamma\}_{\gamma \in (\mathbb{Z}/2\mathbb{Z})^m}$ are pairwise non-isomorphic and represent all isomorphism classes of the genus of \mathcal{R} . In particular, $\mathcal{D}^\gamma \cong \mathcal{D}^{\gamma'}$ if and only if $\gamma = \gamma'$.*

Proof. It follows from [11, Section 2.2] that if $1 \leq i \leq m$ and $x \in \mathfrak{A}_{v_i}^\times$ is such that $x\mathcal{R}'_{v_i}x^{-1} = \mathcal{R}_{v_i}$ then $\text{ord}_{v_i}(n(x)) \equiv 1 \pmod{2}$. Using this, it is easy to see that $\rho(\mathcal{D}^\gamma, \mathcal{D}^{\gamma'}) = \prod_{i=1}^m \bar{e}_{v_i}^{\gamma_i + \gamma'_i \pmod{2}}$. By Proposition 3.6, $\mathcal{D}^\gamma \cong \mathcal{D}^{\gamma'}$ if and only if $\rho(\mathcal{D}^\gamma, \mathcal{D}^{\gamma'})$ is trivial. As there are 2^m non-isomorphic orders \mathcal{D}^γ and 2^m isomorphism classes in the genus of \mathcal{R} , the proposition follows. \square

5. Selectivity

Let Ω be a commutative, quadratic \mathcal{O}_K -order and assume that an embedding of Ω into \mathcal{R} exists. We are interested in determining the proportion of isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω . As in [4], we shall say that Ω is *selective* for the genus of \mathcal{R} if Ω does not embed into every order in the genus of \mathcal{R} .

Remark 5.1. Suppose that \mathcal{E} is an order in the genus of \mathcal{R} , Ω is an integral domain and φ is an embedding of Ω into \mathcal{E} . Then φ extends to an embedding of the quotient field of Ω into \mathfrak{A} . Such an embedding is, by the Skolem–Noether theorem, given by conjugation by an element of \mathfrak{A}^\times . Thus an order \mathcal{E} in the genus of \mathcal{R} admits an embedding of Ω if and only if it contains a conjugate of Ω .

5.1. *Obstructions to selectivity*

In this section we describe several easy to check criteria that, if satisfied, preclude the possibility of selectivity. In order to show that in these cases Ω can be embedded into every order in the genus of \mathcal{R} , we employ the following strategy.

Let $\{e_{v_i}\}_{i=1}^m \subset J_K$ be such that $\{\bar{e}_{v_i}\}$ generate $G_{\mathcal{R}} = J_K/K^\times \cdot n(\mathfrak{N}(\mathcal{R}))$. Note that by Lemma 3.4 we may assume that each v_i is non-archimedean, that no v_i ramifies in \mathfrak{A} and that \mathcal{R}_{v_i} is maximal for all i . For each v_i , we will construct two distinct local maximal orders \mathcal{D}_{v_i} and \mathcal{D}'_{v_i} which both contain Ω (that is, $\Omega \subset \mathcal{D}_{v_i} \cap \mathcal{D}'_{v_i}$ for all v_i) and are adjacent in the tree of maximal orders of $\mathfrak{A}_{v_i} \cong M_2(K_{v_i})$. By hypothesis \mathcal{R} also contains Ω . Then for each $\gamma \in (\mathbb{Z}/2\mathbb{Z})^m$, let \mathcal{D}^γ be the global order defined by the local factors

$$\mathcal{D}_v^\gamma = \begin{cases} \mathcal{D}_{v_i} & \text{if } v = v_i \text{ and } \gamma_i = 0, \\ \mathcal{D}'_{v_i} & \text{if } v = v_i \text{ and } \gamma_i = 1, \\ \mathcal{R}_v & \text{otherwise.} \end{cases}$$

As Ω is contained in every completion of \mathcal{D}^γ (for each $\gamma \in (\mathbb{Z}/2\mathbb{Z})^m$), Ω is contained in \mathcal{D}^γ as well. These 2^m orders represent all isomorphism classes of orders in the genus of \mathcal{R} and each contains a conjugate of Ω . Hence Ω can be embedded into all orders in the genus of \mathcal{R} .

Remark 5.2. The strategy outlined above was used in [4] by Chinburg and Friedman in order to prove the theorem in the case that \mathcal{R} was a maximal order. The same strategy was used by Guo and Qin in [5] to extend the theorem to Eichler orders of arbitrary level.

Proposition 5.3. *If Ω is not an integral domain then every order in the genus of \mathcal{R} admits an embedding of Ω .*

Proof. If Ω is not an integral domain then $\mathfrak{A} \cong M_2(K)$ and Ω is conjugate to a subring of

$$\Omega_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathcal{O}_K \right\} \quad \text{or} \quad \Omega_J = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathcal{O}_K, b \in J \right\}$$

for J a fractional ideal of K .

We may, without loss of generality, assume that $\Omega \subset \Omega_0$ or $\Omega \subset \Omega_J$.
 If $\Omega \subset \Omega_0$, set

$$\mathcal{D}_{v_i} = \begin{pmatrix} \mathcal{O}_{v_i} & \mathcal{O}_{v_i} \\ \mathcal{O}_{v_i} & \mathcal{O}_{v_i} \end{pmatrix}, \quad \mathcal{D}'_{v_i} = \begin{pmatrix} \mathcal{O}_{v_i} & \pi_{v_i}^{-1} \mathcal{O}_{v_i} \\ \pi_{v_i} \mathcal{O}_{v_i} & \mathcal{O}_{v_i} \end{pmatrix}.$$

If $\Omega \subset \Omega_J$ for a fractional ideal J of K , set

$$\mathcal{D}_{v_i} = \begin{pmatrix} \mathcal{O}_{v_i} & J\mathcal{O}_{v_i} \\ J^{-1}\mathcal{O}_{v_i} & \mathcal{O}_{v_i} \end{pmatrix}, \quad \mathcal{D}'_{v_i} = \begin{pmatrix} \mathcal{O}_{v_i} & \pi_{v_i}^{-1} J\mathcal{O}_{v_i} \\ \pi_{v_i} J^{-1}\mathcal{O}_{v_i} & \mathcal{O}_{v_i} \end{pmatrix}.$$

In both cases \mathcal{D}_{v_i} is conjugate to \mathcal{D}'_{v_i} by $\begin{pmatrix} 1 & 0 \\ 0 & \pi_{v_i} \end{pmatrix}$ and $\Omega \subset \mathcal{D}_{v_i} \cap \mathcal{D}'_{v_i}$. As this holds for all i and $\Omega \subset \mathcal{D}_v$ for all $v \neq v_i$ for any i by definition of \mathcal{D} , we have, for every γ , $\Omega \subset \bigcap_v (\mathfrak{A} \cap \mathcal{D}'_v) = \mathcal{D}^\gamma$. Thus Ω can be embedded into representatives of every isomorphism class in the genus of \mathcal{R} . \square

In light of Proposition 5.3 we henceforth assume that Ω is an integral domain with quotient field L .

Proposition 5.4. *If $L \not\subset K(\mathcal{R})$, then every order in the genus of \mathcal{R} admits an embedding of Ω .*

Proof. By Lemma 3.7 we can choose primes v_i of K which split in L such that $\{\overline{e_{v_i}}\}$ generate $G_{\mathcal{R}}$. Let $\lambda = v_i$ for some i . As λ splits in L/K , \mathfrak{A}_λ must be split (this is immediate from the Albert–Brauer–Hasse–Noether theorem), so there is a K_λ -isomorphism $f_\lambda : \mathfrak{A}_\lambda \rightarrow M_2(K_\lambda)$ such that

$$f_\lambda(L) \subset \begin{pmatrix} K_\lambda & 0 \\ 0 & K_\lambda \end{pmatrix}$$

by Lemma 2.2 of [1]. Then

$$f_\lambda(\Omega) \subset f_\lambda(\mathcal{O}_L) \subset \begin{pmatrix} \mathcal{O}_{K_\lambda} & 0 \\ 0 & \mathcal{O}_{K_\lambda} \end{pmatrix}.$$

Choose \mathcal{D}_λ and \mathcal{D}'_λ so that

$$\mathcal{D}_\lambda = f_\lambda^{-1} \left(\begin{pmatrix} \mathcal{O}_{K_\lambda} & \mathcal{O}_{K_\lambda} \\ \mathcal{O}_{K_\lambda} & \mathcal{O}_{K_\lambda} \end{pmatrix} \right), \quad \mathcal{D}'_\lambda = f_\lambda^{-1} \left(\begin{pmatrix} \mathcal{O}_{K_\lambda} & \pi_\lambda^{-1} \mathcal{O}_{K_\lambda} \\ \pi_\lambda \mathcal{O}_{K_\lambda} & \mathcal{O}_{K_\lambda} \end{pmatrix} \right).$$

As λ ranges over all v_i , we see that $\Omega \subset \mathcal{D}_{v_i} \cap \mathcal{D}'_{v_i}$ for all i . By the strategy outlined in the beginning of this section, Ω can be embedded into representatives of every isomorphism class in the genus of \mathcal{R} . \square

Recalling that the conductor of $K(\mathcal{R})$ is divisible only by the prime divisors of the level ideal $N_{\mathcal{R}}$ of \mathcal{R} , we have the following immediate corollary to Proposition 5.4.

Corollary 5.5. *If any finite prime of K not dividing $N_{\mathcal{R}}$ ramifies in L , then every order in the genus of \mathcal{R} admits an embedding of Ω .*

That Corollary 5.5 allows one to preclude the possibility of selectivity without computing the class field $K(\mathcal{R})/K$ is especially nice, as in practice such a computation may be quite difficult.

Having dealt with the case that $L \not\subset K(\mathcal{R})$, we now suppose that $L \subset K(\mathcal{R})$.

Proposition 5.6. *If $L \subset K(\mathcal{R})$, then the proportion of isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω is at least $1/2$.*

Proof. Identify Ω with its image in \mathcal{R} so that $\Omega \subset \mathcal{R}$. We may choose, by Lemma 3.7, a generating set $\{\overline{e_{v_i}}\}_{i=1}^m$ of $G_{\mathcal{R}}$ for which v_1 is inert in L/K , and v_i splits in L/K whenever $i > 1$. Let $\{\mathcal{D}^\gamma\}$ be a parameterization of the genus of \mathcal{R} associated to this generating set. The proof of Proposition 5.4 shows that the parameterization $\{\mathcal{D}^\gamma\}$ can be constructed so that for all γ , Ω is contained in $\mathcal{D}_{v_i}^\gamma$ whenever $i > 1$. As the set of orders $\{\mathcal{D}^\gamma: \mathcal{D}_{v_1}^\gamma = \mathcal{R}_{v_1}\}$ represent half of the isomorphism classes in the genus of \mathcal{R} and each of these orders contains Ω , we're done. \square

We summarize Propositions 5.4 and 5.6 as a theorem.

Theorem 5.7. *Assume that an embedding of Ω into \mathcal{R} exists.*

- (1) *If $L \not\subset K(\mathcal{R})$, then every order in the genus of \mathcal{R} admits an embedding of Ω .*
- (2) *If $L \subset K(\mathcal{R})$, then the proportion of isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω is at least $1/2$.*

5.2. A selectivity theorem

In this section we constrain slightly the class of orders $\mathcal{R} \subset \mathfrak{A}$ that we consider and provide necessary and sufficient conditions for an order Ω to be selective for the genus of \mathcal{R} . In the case that Ω is selective for the genus of \mathcal{R} , we shall see that representatives of exactly $1/2$ of the isomorphism classes of the genus of \mathcal{R} admit an embedding of Ω . The constraints which we shall impose on \mathcal{R} are the following:

- (5.1) The relative discriminant ideal d_{Ω/\mathcal{O}_K} of Ω is coprime to the level ideal $N_{\mathcal{R}}$ of \mathcal{R} .
- (5.2) The set of primes dividing $N_{\mathcal{R}}$ is disjoint from the set of primes ramifying in \mathfrak{A} .

Theorem 5.8. *Assume that an embedding of Ω into \mathcal{R} exists. Then every order in the genus of \mathcal{R} admits an embedding of Ω except when the following conditions hold:*

- (1) Ω is an integral domain whose quotient field L is a quadratic field extension of K which is contained in \mathfrak{A} .
- (2) There is a containment of fields $L \subset K(\mathcal{R})$.
- (3) All primes of K which divide the relative discriminant ideal d_{Ω/\mathcal{O}_K} of Ω split in L/K .

Suppose now that (1)–(3) hold. Then the isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω comprise exactly half of the isomorphism classes. If \mathcal{R} admits an embedding of Ω and \mathcal{E} is another order in the genus of \mathcal{R} , then \mathcal{E} admits an embedding of Ω if and only if $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is the trivial element of $\text{Gal}(L/K)$.

Remark 5.9. Although our condition (2) is not the same as that which appears in [2,4,5], it is equivalent whenever \mathcal{R} is an Eichler order. Indeed, this equivalence plays an important role in the proofs of the aforementioned theorems.

Example 5.10. Let K be a number field and \mathfrak{A} be a quaternion algebra over K which satisfies the Eichler condition and has no finite ramification. Let L be a maximal subfield of \mathfrak{A} and $\Omega = \mathcal{O}_L$. If \mathcal{R} is any quaternion order in \mathfrak{A} containing Ω for which assumption (5.1) holds, then by Theorem 5.8, the proportion of isomorphism classes in the genus of \mathcal{R} whose representatives admit an embedding of Ω is $[K(\mathcal{R}) \cap L : K]^{-1}$. This generalizes the $n = 2$ case of a theorem of Chevalley [3], who showed that if L is a maximal subfield of $M_n(K)$ then the ratio of the isomorphism classes of maximal orders

of $M_n(K)$ into which \mathcal{O}_L can be embedded to the total number of isomorphism classes of maximal orders is $[H_K \cap L : K]^{-1}$, where H_K is the Hilbert class field of K .

We prove Theorem 5.8 as a series of propositions. We have seen in Propositions 5.3 and 5.4 that if either (1) or (2) fail to hold then every order in the genus of \mathcal{R} admits an embedding of \mathcal{R} . We henceforth assume that conditions (1) and (2) hold.

Proposition 5.11. *Both L/K and \mathfrak{A} are unramified at all finite primes of K and ramify at the same (possibly empty) set of real primes.*

Proof. If a finite prime ν of K ramifies in \mathfrak{A} then by assumption (5.2), \mathcal{R}_ν must be maximal, hence $n(N(\mathcal{R}_\nu)) = K_\nu^\times$. It follows that ν splits completely in $K(\mathcal{R})$ and thus in L/K as well. As L embeds into \mathfrak{A} we obtain a contradiction to the Albert–Brauer–Hasse–Noether theorem. If ν is a finite prime of K which ramifies in L/K then ν ramifies in $K(\mathcal{R})/K$ and thus divides the level ideal $N_{\mathcal{R}}$. As ν also divides d_{Ω/\mathcal{O}_K} we have a contradiction to assumption (5.1). That L/K is ramified at every real prime which ramifies in \mathfrak{A} follows from the Albert–Brauer–Hasse–Noether theorem. If ν is a real prime of K which is unramified in \mathfrak{A} then $n(N(\mathcal{R}_\nu)) = \mathbb{R}^\times$, hence ν splits completely in $K(\mathcal{R})/K$ and thus in L/K as well. \square

Remark 5.12. That L/K and \mathfrak{A} are unramified at all finite primes and ramify at exactly the same set of real primes appeared as condition (2) in [4,5] and may very well be a necessary condition for selectivity to occur at all in \mathfrak{A} .

Proposition 5.13. *If condition (3) does not hold, then every order in the genus of \mathcal{R} admits an embedding of Ω .*

Proof. If condition (3) does not hold, there exists a finite prime λ of K with $\lambda \mid d_{\Omega/\mathcal{O}_K}$ and which does not split in L/K . By Proposition 5.11, λ is unramified in L/K , so λ is inert in L . By assumption (5.1), $(d_{\Omega/\mathcal{O}_K}, N_{\mathcal{R}}) = 1$ and since $\lambda \mid d_{\Omega/\mathcal{O}_K}$, we have $\lambda \nmid N_{\mathcal{R}}$ which implies that \mathcal{R}_λ is maximal. Finally, since λ is finite, Proposition 5.11 implies that $\mathfrak{A}_\lambda \cong M_2(K_\lambda)$.

Because condition (2) holds, $L \subset K(\mathcal{R})$ and by Lemma 3.7 we may choose ν_2, \dots, ν_m such that $\{\overline{e_\lambda}, \overline{e_{\nu_2}}, \dots, \overline{e_{\nu_m}}\}$ generate $G_{\mathcal{R}}$, where ν_i splits in L/K for $i = 2, \dots, m$. We also assume that the ν_i are chosen so that \mathcal{R}_{ν_i} is maximal for all i . As the ν_i all split in L , for each i we may pick two adjacent maximal orders of \mathfrak{A}_{ν_i} containing Ω (as in the proof of Proposition 5.4).

Since L_λ/K_λ is a quadratic unramified extension and λ divides d_{Ω/\mathcal{O}_K} , $\Omega \subset \Omega \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\lambda} \subset \mathcal{O}_{K_\lambda} + \pi_\lambda \mathcal{O}_{L_\lambda}$. Let \mathcal{D}_λ be some maximal order of \mathfrak{A}_λ containing \mathcal{O}_{L_λ} and consequently, Ω . All maximal orders of \mathfrak{A}_λ are conjugate, so we may assume that $\mathcal{D}_\lambda = \begin{pmatrix} \mathcal{O}_{K_\lambda} & \mathcal{O}_{K_\lambda} \\ \mathcal{O}_{K_\lambda} & \mathcal{O}_{K_\lambda} \end{pmatrix}$. Now consider the maximal order $\mathcal{D}'_\lambda = \begin{pmatrix} \mathcal{O}_{K_\lambda} & \pi_\lambda^{-1} \mathcal{O}_{K_\lambda} \\ \pi_\lambda \mathcal{O}_{K_\lambda} & \mathcal{O}_{K_\lambda} \end{pmatrix}$. It is clear that $\pi_\lambda \mathcal{D}_\lambda \subset \mathcal{D}'_\lambda$ (viewed as \mathcal{O}_{K_λ} -modules), so $\pi_\lambda \mathcal{O}_{L_\lambda} \subset \mathcal{D}'_\lambda$. Then $\Omega \subset \mathcal{D}'_\lambda$.

Hence $\Omega \subset \mathcal{D}_\nu \cap \mathcal{D}'_\nu$ for all $\nu \in \{\lambda, \nu_2, \dots, \nu_m\}$ and thus can be embedded into representatives of every isomorphism class in the genus of \mathcal{R} . \square

We now assume that conditions (1)–(3) hold.

Proposition 5.14. *Let notation be as above and suppose that conditions (1)–(3) hold. Then the orders in the genus of \mathcal{R} admitting an embedding of Ω represent exactly half of the isomorphism classes. If \mathcal{E} is another order in the genus of \mathcal{R} , then \mathcal{E} admits an embedding of Ω if and only if $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is the trivial element of $\text{Gal}(L/K)$.*

Proof. By assumption, Ω is contained in \mathcal{R} . Let \mathcal{E} be an order in the genus of \mathcal{R} . We may choose, by Lemma 3.7, a generating set $\{\overline{e_{\nu_i}}\}_{i=1}^m$ of $G_{\mathcal{R}}$ for which ν_1 is inert in L/K , and ν_i splits in L/K

whenever $i > 1$. Let $\{\mathcal{D}^\gamma\}$ be the parameterization of the genus of \mathcal{R} associated to this generating set. As the $\{\mathcal{D}^\gamma\}$ span the isomorphism classes in the genus of \mathcal{R} , there exists a γ such that $\mathcal{E} \cong \mathcal{D}^\gamma$. Then \mathcal{E} contains a conjugate of Ω if and only if \mathcal{D}^γ contains a conjugate of Ω , so we may suppose without loss of generality that $\mathcal{E} = \mathcal{D}^\gamma$.

The proof of Proposition 5.4 shows that the parameterization $\{\mathcal{D}^\gamma\}$ can be constructed so that for all γ , Ω is contained in $\mathcal{D}_{v_i}^\gamma$ whenever $i > 1$. Suppose that $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{D}^\gamma))$ is trivial in $\text{Gal}(L/K)$. Since $\rho(\mathcal{R}, \mathcal{D}^\gamma) = \prod_{i=1}^m \overline{e_{v_i}^{\gamma_i}}$, this implies that $\text{Frob}_{L/K}(\overline{e_{v_1}^{-\gamma_1}})$ is trivial (as v_1 splits in L/K whenever $i > 1$). As $\text{Frob}_{L/K}(\overline{e_{v_1}})$ is the non-trivial element of $\text{Gal}(L/K)$, we deduce that $\gamma_1 = 0$. Therefore $\Omega \subset \mathcal{D}_{v_1}^\gamma$ and $\Omega \subset \mathcal{D}_v^\gamma$ for all primes v of K , hence $\Omega \subset \mathcal{D}^\gamma$.

In order to prove the converse we will need a lemma.

Lemma 5.15. *If v is a finite prime of K which is inert in L , then \mathcal{O}_{L_v} is contained in a unique maximal order of \mathfrak{A}_v .*

Proof. By Proposition 5.11, v is unramified in \mathfrak{A} so that we may identify \mathfrak{A}_v with $M_2(K_v)$. Suppose that \mathcal{O}_{L_v} is contained in distinct maximal orders $\mathcal{M}_1, \mathcal{M}_2$ of \mathfrak{A}_v . All of the maximal orders of $M_2(K_v)$ are conjugate, so there exists an element $x \in \mathfrak{A}_v^\times$ such that $\mathcal{M}_2 = x\mathcal{M}_1x^{-1}$. Because v is inert in L/K we may write $\mathcal{O}_{L_v} = \mathcal{O}_{K_v}[\alpha]$ for some $\alpha \in \mathcal{O}_{L_v}^\times$. Because $\alpha \in \mathcal{M}_1^\times \cap \mathcal{M}_2^\times$, conjugation by α fixes both \mathcal{M}_1 and \mathcal{M}_2 and hence every vertex in the unique path joining \mathcal{M}_1 and \mathcal{M}_2 in the tree of maximal orders of \mathfrak{A}_v . Thus α fixes an edge in the tree of maximal orders of \mathfrak{A}_v . But this contradicts Lemma 2.2 of [4], proving the lemma. \square

We now continue the proof of Proposition 5.14 and suppose now that \mathcal{E} contains a conjugate of Ω but $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is not trivial. By conjugating \mathcal{E} we may assume that Ω is contained in \mathcal{E} , as $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is unchanged if \mathcal{E} is replaced with a conjugate order (by Proposition 3.6). We claim that there is a finite prime v which is inert in L/K and for which \mathcal{R}_v and \mathcal{E}_v are not equal. Suppose to the contrary that $\mathcal{E}_\mu = \mathcal{R}_\mu$ for all primes μ that are inert in L/K . Let $y = \tilde{y}_\mathcal{E} \in J_\mathfrak{A}$ be such that $\mathcal{E}_\lambda = y_\lambda \mathcal{R}_\lambda y_\lambda^{-1}$ for all primes λ of K . By hypothesis we may take $y_\mu = 1$ for all primes μ which are inert in L/K . We may also take $y_\mu = 1$ for all archimedean primes μ of K . Consider the element $\rho(\mathcal{R}, \mathcal{E}) = n(y)H_\mathcal{R}$ of $G_\mathcal{R}$. Its image under $\text{Frob}_{L/K}$ is clearly trivial since $n(y_\mu) = 1$ whenever μ is inert in L/K (here we have used the fact that by Proposition 5.11, L/K is unramified at all finite primes). This contradicts our assumption that $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ be non-trivial and proves our claim.

Let v be a finite prime which is inert in L/K and such that $\mathcal{R}_v \neq \mathcal{E}_v$. By Proposition 5.11 v is unramified in \mathfrak{A} . Because condition (3) holds, $\Omega_v = \mathcal{O}_{L_v}$. Locally we see that $\Omega_v \subset \mathcal{R}_v \subset \mathcal{M}_v$ for some maximal order \mathcal{M}_v of \mathfrak{A}_v . Writing $\mathcal{E}_v = y_v \mathcal{R}_v y_v^{-1}$, we have $\Omega_v \subset \mathcal{E}_v \subset y_v \mathcal{M}_v y_v^{-1}$. By Lemma 5.15, $\mathcal{M}_v = y_v \mathcal{M}_v y_v^{-1}$, so that \mathcal{M}_v is fixed by y_v . An element of \mathfrak{A}_v whose reduced norm has odd valuation fixes no maximal order, so it must be the case that $\text{ord}_v(n(y_v))$ is even. If this holds for every inert prime v for which $\mathcal{R}_v \neq \mathcal{E}_v$, then $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ would be trivial. This contradiction finishes the proof. \square

6. An optimal embedding theorem

Let Ω be an integral domain whose quotient field L is a quadratic extension of K . Recall that an embedding $\sigma : L \rightarrow \mathfrak{A}$ is an optimal embedding of Ω into \mathcal{R} if $\sigma(L) \cap \mathcal{R} = \sigma(\Omega)$. Given a finite prime v of K and an embedding $\sigma : L \rightarrow \mathfrak{A}$, extension of scalars yields an embedding $\sigma_v : L_v \rightarrow \mathfrak{A}_v$. The following lemma makes clear the relationship between the optimality of an embedding σ and the optimality of the induced embeddings $\{\sigma_v\}$, where v ranges over the finite primes of K .

Lemma 6.1. *Let notation be as above. Then σ is an optimal embedding of Ω into \mathcal{R} if and only if for every finite prime v of K , σ_v is an optimal embedding of Ω_v into \mathcal{R}_v .*

Proof. Identify L and Ω with their images in \mathfrak{A} under σ . We must show that $L \cap \mathcal{R} = \Omega$ if and only if $L_\nu \cap \mathcal{R}_\nu = \Omega_\nu$ for all $\nu < \infty$. This follows from the Corollary on p. 85 of [12], which implies that $(L \cap \mathcal{R})_\nu = L_\nu \cap \mathcal{R}_\nu$ for all finite primes ν of K . \square

All of the results in Section 5 hold for optimal embeddings as well. We begin by proving a few general results in which there are no restrictions on the orders Ω or \mathcal{R} . Assume there is an optimal embedding σ of Ω into \mathcal{R} .

Proposition 6.2. *If $L \not\subset K(\mathcal{R})$, then every order in the genus of \mathcal{R} admits an optimal embedding of Ω .*

Proof. If $L \not\subset K(\mathcal{R})$, we may choose a generating set $\{\overline{e}_{v_i}\}_{i=1}^m$ of $G_{\mathcal{R}}$ such that both \mathcal{R}_{v_i} and Ω_{v_i} are maximal for all i . As in the proof of Proposition 5.4, we may construct a parameterization $\{\mathcal{D}^\gamma\}$ of the genus of \mathcal{R} such that each $\mathcal{D}_{v_i}^\gamma$ contains $\sigma_{v_i}(\Omega_{v_i})$. However every embedding of a maximal quadratic order into a quaternion order is optimal. In particular, σ_{v_i} is an optimal embedding of Ω_{v_i} into $\mathcal{D}_{v_i}^\gamma$ for all γ and for $i = 1, \dots, m$. As σ is an optimal embedding of Ω into \mathcal{R} , Lemma 6.1 implies that σ_ν is an optimal embedding of Ω_ν into \mathcal{R}_ν for all ν . As $\mathcal{D}_\nu^\gamma = \mathcal{R}_\nu$ whenever $\nu \notin \{v_i\}$, we conclude from Lemma 6.1 that σ is an optimal embedding of Ω into \mathcal{D}^γ . \square

Proposition 6.3. *If $L \subset K(\mathcal{R})$, then the proportion of isomorphism classes in the genus of \mathcal{R} whose representatives admit an optimal embedding of Ω is at least $1/2$.*

Proof. Let $\{\mathcal{D}^\gamma\}$ be a parameterization of the genus of \mathcal{R} and let $\mathcal{D}^{\gamma_0} \in \{\mathcal{D}^\gamma\}$ contain $\sigma(\Omega)$ (i.e. σ is an embedding of Ω into \mathcal{D}^{γ_0}). We show that for every finite prime ν of K , σ_ν is an optimal embedding of Ω_ν into $\mathcal{D}_\nu^{\gamma_0}$. If $\nu \notin \{v_i\}$ then $\mathcal{D}_\nu^{\gamma_0} = \mathcal{R}_\nu$ and σ_ν is optimal by Lemma 6.1. As Ω_{v_i} can be taken to be the maximal order of L_{v_i} (by suitably choosing the generators $\{\overline{e}_{v_i}\}$ of $G_{\mathcal{R}}$) and every embedding of a maximal quadratic order into a quaternion order is optimal, we see that the embeddings $\{\sigma_{v_i}\}_{i=1}^m$ are optimal as well. By Lemma 6.1 σ is an optimal embedding of Ω into \mathcal{D}^{γ_0} , finishing our proof. \square

We now adopt the assumptions outlined in the beginning Section 5.2 and prove an analog of Theorem 5.8 for optimal embeddings.

Theorem 6.4. *Let notation be as above and suppose that assumptions (5.1) and (5.2) are satisfied. If an optimal embedding of Ω into \mathcal{R} exists then every order in the genus of \mathcal{R} admits an optimal embedding of Ω except when the following conditions hold:*

- (1) We have a containment of fields $L \subset K(\mathcal{R})$.
- (2) All primes of K which divide the relative discriminant ideal d_{Ω/\mathcal{O}_K} of Ω split in L/K .

Suppose now that (1) and (2) hold. Then the isomorphism classes in the genus of \mathcal{R} whose representatives admit an optimal embedding of Ω comprise exactly half of the isomorphism classes. If \mathcal{R} admits an optimal embedding of Ω and \mathcal{E} is another order in the genus of \mathcal{R} , then \mathcal{E} admits an optimal embedding of Ω if and only if $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is the trivial element of $\text{Gal}(L/K)$.

Proof. If condition (1) fails then Proposition 6.2 shows that every order in the genus of \mathcal{R} admits an optimal embedding of Ω .

If condition (1) is satisfied and condition (2) fails, then we may choose a generating set $\{\overline{e}_{v_i}\}_{i=1}^m$ of $G_{\mathcal{R}}$ such that both \mathcal{R}_{v_i} and Ω_{v_i} are maximal for all i . The proof of Theorem 5.8 again proceeds by constructing a parameterization $\{\mathcal{D}^\gamma\}$ of the genus of \mathcal{R} such that for every i , $\sigma(\Omega_{v_i}) \subset \mathcal{R}_{v_i} \cap \mathcal{R}'_{v_i}$, where $\mathcal{D}_{v_i}^\gamma$ equals either \mathcal{R}_{v_i} or \mathcal{R}'_{v_i} , depending on the parity of γ_i . The argument used to prove Proposition 6.2 shows that σ is an optimal embedding of Ω into every order in the genus of \mathcal{R} .

We now assume that (1) and (2) are both satisfied and show that the orders in the genus of \mathcal{R} admitting an optimal embedding of Ω represent exactly one half of the isomorphism classes.

Proposition 6.3 shows that the representatives of at least half of the isomorphism classes of orders in the genus of \mathcal{R} admit an optimal embedding of Ω . By Theorem 5.8, the orders \mathcal{E} in the genus of \mathcal{R} admitting an embedding of Ω are precisely those for which $\text{Frob}_{L/K}(\rho(\mathcal{R}, \mathcal{E}))$ is the trivial element of $\text{Gal}(L/K)$ and represent exactly half of the isomorphism classes. An order in the genus of \mathcal{R} cannot admit an optimal embedding of Ω if it admits no embedding of Ω , so the isomorphism classes whose representatives admit an optimal embedding of Ω are precisely those whose representatives admit an embedding of Ω , finishing our proof. \square

Acknowledgments

It is a pleasure to thank Tom Shemanske, my advisor, for his encouragement and for patiently reading and commenting on drafts of this paper. I would also like to thank Ted Chinburg for useful conversations regarding the proof of Theorem 3.3 of [4].

References

- [1] J. Brzezinski, On two classical theorems in the theory of orders, *J. Number Theory* 34 (1) (1990) 21–32.
- [2] W.K. Chan, F. Xu, On representations of spinor genera, *Compos. Math.* 140 (2) (2004) 287–300.
- [3] C. Chevalley, *L'arithmétique dans les algèbres de matrices*, Hermann, Paris, 1936.
- [4] T. Chinburg, E. Friedman, An embedding theorem for quaternion algebras, *J. Lond. Math. Soc.* (2) 60 (1) (1999) 33–44.
- [5] X. Guo, H. Qin, An embedding theorem for Eichler orders, *J. Number Theory* 107 (2) (2004) 207–214.
- [6] H. Hijikata, Explicit formula of the traces of Hecke operators for $T_0(N)$, *J. Math. Soc. Japan* 26 (1974) 56–82.
- [7] S. Lang, *Algebraic Number Theory*, second edition, *Grad. Texts in Math.*, vol. 110, Springer-Verlag, New York, 1994.
- [8] C. Maclachlan, Optimal embeddings in quaternion algebras, *J. Number Theory* 128 (10) (2008) 2852–2860.
- [9] I. Reiner, *Maximal Orders*, *London Math. Soc. Monogr. Ser.*, vol. 5, Academic Press, London–New York, 1975.
- [10] M.-F. Vignéras, Variétés riemanniennes isospectrales et non isométriques, *Ann. of Math.* (2) 112 (1) (1980) 21–32.
- [11] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, *Lecture Notes in Math.*, vol. 800, Springer, Berlin, 1980.
- [12] A. Weil, *Basic Number Theory*, reprint of the second (1973) edition, *Classics Math.*, Springer-Verlag, Berlin, 1995.