Astérisque
312, 2007, p. 25–47

5. THE GENUS OF THE ENDOMORPHISMS OF A SUPERSINGULAR ELLIPTIC CURVE

by

Torsten Wedhorn

***Abstract.* —** We describe the genus of the quadratic space $\mathrm{Hom}(E', E)$ of homomorphisms of two supersingular elliptic curves E and E' and study the map $(E', E) \mapsto \mathrm{Hom}(E', E)$ from the set of pairs of supersingular elliptic curves over $\bar{\mathbb{F}}_p$ to the set of proper classes in this genus. We show that this map is surjective and determine its fibres. In the last section we use the Minkowski-Siegel formula to express the mean value of the representation of a ternary quadratic form in this genus by local representation densities.

***Résumé* (Le genre des endomorphismes d'une courbe elliptique supersingulière)**

Nous décrivons le genre de l'espace quadratique $\mathrm{Hom}(E', E)$ des homomorphismes de deux courbes elliptiques supersingulières E et E' et nous étudions l'application $(E', E) \mapsto \mathrm{Hom}(E', E)$ de l'ensemble des paires de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ vers l'ensemble des classes propres dans ce genre. Dans le dernier paragraphe, on utilise la formule de Minkowski-Siegel pour exprimer la moyenne de la représentation d'une forme quadratique ternaire dans ce genre en termes de densités de représentation locales.

Introduction

Let $p > 0$ be a prime and let D be the unique quaternion division algebra with center $\mathbb{Q}$ which is ramified precisely at p and at infinity. The reduced norm Nrd is a quadratic form on D. We will study lattices and maximal orders in D. Recall that two lattices Λ and Λ' are said to be in the same proper class if there exists a $g \in \mathrm{SO}(D, \mathrm{Nrd})$ such that $g\Lambda = \Lambda'$.

We will relate the lattices and the maximal orders in D to supersingular elliptic curves. Many of these results, although formulated somewhat differently, can already be found in [**Do**] (see also [**GZ**]).

2000 ***Mathematics Subject Classification.* —** 11E08, 14K07, 11E12.
***Key words and phrases.* —** Supersingular elliptic curve, quaternion algebra, genus, Minkowski-Siegel formula.

Fix a supersingular elliptic curve E_0 over $\overline{\mathbb{F}}_p$ set $O = \mathrm{End}(E_0)$. Then O is a maximal order in the quadratic space $O \otimes_{\mathbb{Z}} \mathbb{Q}$, where the quadratic form is given by the degree, and we can and will identify the rational quadratic spaces $O \otimes_{\mathbb{Z}} \mathbb{Q}$ with D.

The first result is the following (proved in sections 2.9 and 2.15):

Theorem. — *Consider isomorphism classes of pairs (E, φ) where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and $\varphi\colon E \to E_0$ is a quasi-isogeny.*

(1) *The map $(E, \varphi) \mapsto \varphi \mathrm{Hom}(E_0, E)$ induces a bijection of the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and the set of right ideal classes of O.*

(2) *The map $(E, \varphi) \mapsto \varphi \mathrm{End}(E)\varphi^{-1}$ induces a surjection from the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ to the set of conjugacy classes of maximal orders in D. Two supersingular elliptic curves E and E' are sent to the same conjugacy class if and only if there exists a $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ such that $E' \cong E^{(\sigma)}$.*

For all pairs (E', E) of supersingular elliptic curves it is possible to choose quasi-isogenies $\varphi\colon E \to E_0$ and $\varphi'\colon E' \to E_0$ with $\deg(\varphi) = \deg(\varphi')$. Then $\varphi \mathrm{Hom}(E', E)\varphi'^{-1}$ is a lattice in D whose proper class is independent of the choice of φ and φ'. In this way we can consider $\mathrm{Hom}(E', E)$ as a proper class of lattices in D.

The second theorem describes these proper classes (see sections 3.1 and Proposition 3.2).

Theorem. — *Let Λ be a lattice in D. Then the proper class $[\Lambda]$ of Λ is the proper class associated to $\mathrm{Hom}(E', E)$ if and only if Λ is in the same genus as O.*

It follows that the map $((E, \varphi), (E', \varphi')) \mapsto \varphi \mathrm{Hom}(E', E)\varphi'^{-1}$ induces a surjection $(E, E') \mapsto [\mathrm{Hom}(E', E)]$ from the set of pairs of isomorphism classes of supersingular elliptic curves onto the set of proper classes of lattices in D which are locally isomorphic to O. The next theorem describes the fibres of this map and number of automorphisms of the quadratic space $\mathrm{Hom}(E, E')$ (see Proposition 3.3 and Corollary 3.5).

Theorem

(1) *Two pairs (E, E') and (F, F') are sent to the same proper class if and only if there exists a $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ such that $F = E^{(\sigma)}$ and $F' = E'^{(\sigma)}$.*

(2) *For all (E, E')*

$$\#\mathrm{SO}([\mathrm{Hom}(E', E)]) = \begin{cases} \#\mathrm{Aut}(E)\#\mathrm{Aut}(E'), & E,\ E' \text{ both defined over } \mathbb{F}_p; \\ \frac{1}{2}\#\mathrm{Aut}(E)\#\mathrm{Aut}(E'), & \text{otherwise.} \end{cases}$$

Now fix a positive definite ternary quadratic form Q over $\mathbb{Z}$. By the theorems above we can consider the expression

$$2\left(\sum_{E}\frac{1}{\#\operatorname{Aut}(E)}\right)^{-2}\sum_{(E',E)}\frac{R_{\operatorname{Hom}(E',E)}(Q)}{\#\operatorname{Aut}(E')\#\operatorname{Aut}(E)}$$

as the mean value of the representation of Q by the genus of $\operatorname{End}(E_0)$ (here E and E' run through all isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and $R_{\operatorname{Hom}(E',E)}(Q)$ denotes the number of isometries $Q \to \operatorname{Hom}(E',E)$). Hence it can be expressed as a product of local representation densities $\alpha_l(Q,\operatorname{End}(E_0))$ (see 4.3) by the Minkowski-Siegel formula. We obtain (theorem 4.3):

Theorem. — *The mean value is given by*

$$\sum_{(E',E)}\frac{R_{\operatorname{Hom}(E',E)}(Q)}{\#\operatorname{Aut}(E')\#\operatorname{Aut}(E)}=2\left(\frac{p-1}{12}\right)^2\frac{\pi^4}{p^3}\prod_l\alpha_l(Q,\operatorname{End}(E_0)),$$

where l runs through all prime numbers l.

This article is organized as follows. In the first section some definitions and results on quadratic spaces and quaternion algebras are recalled. The second section addresses the correspondence between supersingular elliptic curves, right ideal classes, and conjugacy classes of maximal orders. In the third section the above results on the quadratic spaces $\operatorname{Hom}(E',E)$ are proved. The Minkowski-Siegel formula is applied in the last section.

Acknowledgements. — I am very grateful to S. Kudla for his helpful remarks and to M. Rapoport, T. Yang and the referee for their comments.

1. Preliminaries on quadratic spaces and quaternion algebras

1.1. In this section we recall some definitions and results on quadratic spaces.

If R is a commutative ring, a *quadratic space over* R is a free R-module M together with a map $Q\colon M \to R$, such that

(a) $Q(rm) = r^2Q(m)$ for all $r \in R$ and $m \in M$.

(b) The form $b_Q(x,y) = Q(x+y) - Q(x) - Q(y)$ is R-bilinear and nondegenerate (*i.e.*, the R-linear map $M \to M^*$ corresponding to b_Q is injective).

The map Q is called the *quadratic form* of the quadratic space (M,Q).

Two quadratic spaces (M,Q) and (M',Q') over R are said to be *isomorphic* if there exists an R-linear isomorphism $f\colon M \to M'$ such that $Q'(f(m)) = Q(m)$ for all $m \in M$. We then write $(M,Q) \cong (M',Q')$.

The group of automorphisms of a quadratic space will be denoted by $\mathrm{O}(M,Q)$, the subgroup of automorphisms $g \in \mathrm{O}(M,Q)$ with $\det(g) = 1$ is denoted by $\mathrm{SO}(M,Q)$.

1.2. In the sequel we will only consider quadratic spaces (M, Q) over integral domains R whose field of fractions has characteristic not equal to 2. Then we write $\mathrm{Sym}_n(R)^\vee$ for the set of symmetric matrices n by n matrices $A = (a_{ij})$ with coefficients in $\mathrm{Quot}(R)$ such that $a_{ii} \in R$ for all i and such that $2a_{ij} \in R$ for all i, j. Moreover, we denote by B_Q the $\mathrm{Quot}(R)$-valued bilinear form

$$B_Q \colon M \times M \longrightarrow \mathrm{Quot}(R), \qquad (x, y) \longmapsto \frac{1}{2}(Q(x+y) - Q(x) - Q(y)).$$

Let $\mathcal{B} = (e_1, \ldots, e_n)$ be an R-basis of M. The matrix

$$S_Q = (B_Q(e_i, e_j)) \in \mathrm{Sym}_n(R)^\vee$$

is called the matrix associated to $(M, Q, \mathcal{B})$.

We denote by $\det(M) = \det((M, Q))$ the class of $\det(S_Q)$ modulo $(R^\times)^2$. This is independent of the choice of $\mathcal{B}$.

1.3. Very often we will consider quadratic spaces which arise as follows: Let (V, Q) be a quadratic space over $\mathbb{Q}$ and let Λ be a $\mathbb{Z}$-lattice of V (*i.e.*, a finitely generated $\mathbb{Z}$-submodule Λ such that $\Lambda\mathbb{Q} = V$). If $Q(\Lambda) \subset \mathbb{Z}$, the restriction of Q to Λ defines a quadratic form on Λ over $\mathbb{Z}$.

If l is a finite place of $\mathbb{Q}$, $\Lambda_l = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a lattice in the $\mathbb{Q}_l$-vector space $V_l = V \otimes \mathbb{Q}_l$. Recall that to give a $\mathbb{Z}$-lattice Λ in V is the same as to give a $\mathbb{Z}_l$-lattice Λ_l for all l such that there exists a $\mathbb{Z}$-lattice Γ of V with $\Lambda_l = \Gamma_l$ for almost all l.

Denote by $\mathbb{A}_f$ the ring of finite adeles of $\mathbb{Q}$. An element $g \in GL(V \otimes \mathbb{A}_f)$ is an element $(g_l) \in \prod_l GL(V_l)$ where l runs over all finite places of $\mathbb{Q}$ such that $g_l(\Lambda_l) = \Lambda_l$ for almost all l (this condition is independent of Λ). Hence $g = (g_l)$ acts on the set of lattices by setting

$$g(\Lambda) = \bigcap_l (V \cap g_l(\Lambda_l)).$$

We obtain an action of $GL(V \otimes \mathbb{A}_f)$ on the set of lattices in V and in particular an action of the subgroups $\mathrm{O}(V \otimes \mathbb{A}_f)$ and $\mathrm{SO}(V \otimes \mathbb{A}_f)$.

Definition 1.1. — We say that two quadratic spaces M and M' over $\mathbb{Z}$ are *related* if M and M' are isomorphic over $\mathbb{Z}_l$ for all places l of $\mathbb{Q}$ (with the convention $\mathbb{Z}_\infty = \mathbb{R}$).

1.4. If M and M' are related, they are of course also isomorphic over $\mathbb{Q}_l$ for all places l and hence they are isomorphic over $\mathbb{Q}$ by the weak approximation theorem for quadratic spaces. If we choose an isomorphism of rational quadratic spaces $M \otimes \mathbb{Q} \cong M' \otimes \mathbb{Q}$, we can consider M and M' both as lattices in the same quadratic space V over $\mathbb{Q}$. Moreover, the fact that M and M' are related just means that there exists a $g \in \mathrm{O}(V)(\mathbb{A}_f)$ with $g(M) = M'$. This leads us to the following definition:

Definition 1.2. — Let V be a quadratic space over $\mathbb{Q}$. We say that two lattices Λ and Λ' in V are *related* if there exists a $g \in \mathrm{O}(V)(\mathbb{A}_f)$ such that $g(\Lambda) = \Lambda'$.

An $\mathrm{O}(V)(\mathbb{A}_f)$-orbit of lattices in V is called a *genus*.

Lemma 1.3. — *Let l be a prime number and let (M, Q) be a quadratic space over $\mathbb{Z}_l$. Then there exists a reflection in $\mathrm{O}(M, Q)$.*

Proof. — Let $x \in M$ be an element such that the l-adic valuation of $Q(x)$ is minimal among the elements in M. Then an easy calculation shows that the reflection associated to x preserves M. □

Corollary 1.4. — *Let V be a quadratic space over $\mathbb{Q}$. Two lattices Λ and Λ' in V are in the same genus if and only if there exists a $g \in \mathrm{SO}(V \otimes \mathbb{A}_f)$ such that $g(\Lambda) = \Lambda'$.*

Definition 1.5. — Let V be a quadratic space over $\mathbb{Q}$. Two lattices Λ and Λ' in V are said to be in the same *proper class* or to be *properly equivalent* if there exists a $g \in \mathrm{SO}(V)$ such that $g(\Lambda) = \Lambda'$.

They are in the same *class* or *equivalent* if there exists a $g \in \mathrm{O}(V)$ such that $g(\Lambda) = \Lambda'$.

Obviously, every genus of a lattice is the disjoint union of classes and every class is the disjoint union of one or two proper classes. Moreover, it is well known (*e.g.*, [**Ki**, 6.1.2]) that in each genus there are only finitely many proper classes.

The class of a lattice Λ is equal to the proper class of Λ if and only if there exists a $g \in \mathrm{O}(V)$ with $\det(g) = -1$ such that $g(\Lambda) = \Lambda$, *i.e.*, if and only if $\mathrm{SO}(\Lambda) \neq \mathrm{O}(\Lambda)$.

1.5. We will be mostly interested in quadratic spaces which arise from quaternion algebras: By a quaternion algebra over a field F we mean a central simple algebra D over F of dimension 4. We write Trd and Nrd for the reduced trace and the reduced norm on D, respectively, and we denote by $x \mapsto \bar{x} := \mathrm{Trd}(x) - x$ the canonical involution on D.

Assume that F is the field of fractions of Dedekind domain A (*e.g.*, $A = \mathbb{Z}$ or $A = \mathbb{Z}_l$). Let Λ be some A-lattice of D. Then we set

$$O_l(\Lambda) = \{\, d \in D \mid d\Lambda \subset \Lambda \,\}, \tag{1.1}$$

$$O_r(\Lambda) = \{\, d \in D \mid \Lambda d \subset \Lambda \,\}. \tag{1.2}$$

These are orders in D. We call them the *left order* (resp. *right order*) of Λ. We say that Λ is *normal* if $O_l(\Lambda)$ and $O_r(\Lambda)$ are maximal orders.

Lemma 1.6. — *Let F be a field with $\mathrm{char}(F) \neq 2$ and let D be a quaternion algebra over F. We set*

$$S(D) := \{\, (d, d') \in D^\times \times D^\times \mid \mathrm{Nrd}(d) = \mathrm{Nrd}(d') \,\}.$$

Consider the group homomorphism

$$\begin{aligned} \alpha \colon S(D) &\longrightarrow \mathrm{O}(D, \mathrm{Nrd}), \\ (d, d') &\longmapsto (\delta \longmapsto d\delta d'^{-1}). \end{aligned}$$