Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Pure and Applied Algebra 207 (2006) 37–49

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Isogenies of elliptic curves and the Morava stabilizer group

Mark Behrens*, Tyler Lawson

Department of Mathematics, MIT, Cambridge, MA 02139, USA

Received 27 January 2005; received in revised form 3 August 2005
Available online 2 December 2005
Communicated by E.M. Friedlander

Abstract

Let $\mathbb{S}_2$ be the p-primary second Morava stabilizer group, C a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, $\mathcal{O}$ the ring of endomorphisms of C, and ℓ a topological generator of $\mathbb{Z}_p^\times$ (or $\mathbb{Z}_2^\times/\{\pm 1\}$ if $p = 2$). We show that for $p > 2$ the group $\Gamma \subseteq \mathcal{O}[1/\ell]^\times$ of quasi-endomorphisms of degree a power of ℓ is dense in $\mathbb{S}_2$. For $p = 2$, we show that Γ is dense in an index 2 subgroup of $\mathbb{S}_2$.

MSC: primary 11R52; secondary 14H52, 55Q51

Keywords: Morava stabilizer group; Supersingular elliptic curves; Quaternion algebras

0. Introduction

Fix a prime p. Let F_n be the Honda height n formal group over $\mathbb{F}_{p^n}$. The endomorphism ring $\mathcal{O}_p = \mathrm{End}(F_n)$ is the unique maximal order of the $\mathbb{Q}_p$-division algebra D_p of Hasse invariant $1/n$ [17], and the Morava stabilizer group $\mathbb{S}_n$ is the automorphism group $\mathrm{Aut}\,(F_n) = \mathcal{O}_p^\times$. This group is a p-adic analytic group of dimension n^2, and is of interest to topologists because it is intimately related to the nth layer of the chromatic filtration on

* Corresponding author.
E-mail address: mbehrens@math.mit.edu (M. Behrens).

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2005.09.007

the stable homotopy groups of spheres. We wish to understand the group $\mathbb{S}_n$ for $n = 2$ from the point of view of elliptic curves.

Throughout this paper we let C be a fixed supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $\mathcal{O} = \mathrm{End}(C)$ be the ring of endomorphisms of the curve C defined over $\overline{\mathbb{F}}_p$, and let $D = \mathcal{O} \otimes \mathbb{Q}$ be the ring of quasi-endomorphisms. Because C is supersingular, it is known that D is the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞ [12], and that $\mathcal{O}$ is a maximal order of D [22, 3.1], [4]. The reduced norm

$$N : D \to \mathbb{Q}_p^{\times}$$

gives the degree of the quasi-endomorphism. Let $\widehat{C}$ be the formal completion of C at the identity. Because C is supersingular, the formal group $\widehat{C}$ is isomorphic to the Honda formal group F_2 over $\overline{\mathbb{F}}_p$. In fact, Tate proved that the natural map

$$\rho : \mathrm{End}(C) \otimes \mathbb{Z}_p \to \mathrm{End}(\widehat{C})$$

is an isomorphism [24]. The isomorphism ρ extends to an isomorphism

$$\rho' : D \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\cong} D_p,$$

making explicit the fact that D is ramified at p. The map ρ' is compatible with the reduced norm map on the division algebras D and D_p.

Fix $\ell \geq 2$ to be coprime to p. As the notation suggests, we intend ℓ to be another prime, but this is unnecessary for the results of this paper. Define a monoid

$$\Gamma = \{x \in \mathcal{O}[1/\ell] : N(x) \in \ell^{\mathbb{Z}}\} \subseteq \mathcal{O}[1/\ell]^{\times}.$$

Then Γ is actually a group: given an endomorphism ϕ of degree ℓ^k, the quasi-endomorphism $\ell^{-k}\widehat{\phi}$ is its inverse, where $\widehat{\phi}$ is the dual isogeny. Note that if ℓ is prime, then $\Gamma = \mathcal{O}[1/\ell]^{\times}$. The group Γ may be regarded as being contained in the group $\mathbb{S}_2$ using the map ρ. The purpose of this note is to prove the following theorem.

Theorem 0.1. *Suppose that ℓ is a topological generator of the group $\mathbb{Z}_p^{\times}$ (or the group $\mathbb{Z}_2^{\times}/\{\pm 1\}$ for $p = 2$). For $p > 2$, the group Γ is dense in $\mathbb{S}_2$. For $p = 2$, the group Γ is dense in the index 2 subgroup $\widetilde{\mathbb{S}}_2$, which is the kernel of the composite*

$$\mathbb{S}_2 \xrightarrow{N} \mathbb{Z}_2^{\times} \to (\mathbb{Z}/8)^{\times}/\{1, \ell\}.$$

Let $\mathbb{S}l_2$ be the kernel of the reduced norm, so that there is an exact sequence

$$1 \to \mathbb{S}l_2 \to \mathbb{S}_2 \xrightarrow{N} \mathbb{Z}_p^{\times} \to 1.$$

Similarly, let Γ^1 be the corresponding subgroup of Γ, so that there is an exact sequence

$$1 \to \Gamma^1 \to \Gamma \xrightarrow{N} \ell^{\mathbb{Z}} \to 1.$$

(We will see in the proof of Theorem 0.1 that N is indeed surjective.) We denote by $\mathbb{S}_2^0$ the p-Sylow subgroup of $\mathbb{S}_2$, so that there is a short exact sequence

$$1 \to \mathbb{S}_2^0 \to \mathbb{S}_2 \to \mathbb{F}_{p^2-1}^{\times} \to 1.$$

Similarly we let $\mathbb{S}l_2^0$ be the subgroup of $\mathbb{S}_2^0$ of elements of norm 1. Define Λ to be the subgroup $\Gamma^1 \cap \mathbb{S}l_2^0$. Theorem 0.1 will follow from the following norm 1 versions. Note that in the following theorem and corollary, ℓ is only assumed to be relatively prime to p.

Theorem 0.2. *The group Λ is dense in $\mathbb{S}l_2^0$.*

Corollary 0.3. *The group Γ^1 is dense in $\mathbb{S}l_2$.*

We pause to explain why these theorems are interesting from the point of view of homotopy theory. The p-component of the stable homotopy groups of spheres admits an especially rich filtration known as the chromatic filtration [18]. Work of Morava, Hopkins, Miller, Goerss, and Devinatz [13,19,8,5] shows that the group $\mathbb{S}_n$ acts on the Morava E-theory spectrum E_n, and the nth layer of the chromatic filtration is described by the homotopy fixed points $E_n^{h\mathbb{S}_n}$ of this action. The first chromatic layer is completely understood. The second chromatic layer is currently the subject of intensive study. Goerss et al. [7] produced a decomposition of $E_2^{h\mathbb{S}_2}$ at the prime 3 in terms of finite homotopy fixed point spectra. The first author gave an interpretation of their work in terms of the moduli space of elliptic curves in [2]. In that paper, a spectrum $Q(\ell)$ was introduced which was a shown to be a good approximation to $E_2^{h\mathbb{S}_2}$ for $p = 3$ and $\ell = 2$. In future work [3], we will show that the spectrum $Q(\ell)$ is the homotopy fixed point spectrum $E^{h\Gamma}$. In particular, Theorem 0.1 shows that, in some sense, the spectrum $Q(\ell)$ is a good approximation for $E_2^{h\mathbb{S}_2}$ for all p and suitable ℓ.

Gorbounov et al. [9] studied dense subgroups of $\mathbb{S}l_n^0$ ($\mathbb{S}l$ in their notation), and we prove Theorem 0.2 using their methods. In particular, it is shown in [9] that if $p = 3$, then there is a dense subgroup $\mathbb{Z}/3 * \mathbb{Z}/3$ contained in $\mathbb{S}l_2^0$. In [3], it will be shown that for $\ell = 2$, the group Λ is $\mathbb{Z}/3 * \mathbb{Z}/3$. More generally, the groups Λ and Γ^1 admit explicit presentations as finite amalgamations for any p and ℓ.

The authors were alerted by the referee to the related work of Baker [1]. Baker studies, for primes $p \geq 5$, the category whose objects are supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and whose morphisms are the morphisms of the associated formal groups. He then proves an analog of Morava's change of rings theorem: roughly speaking, he shows that the continuous cohomology of this category of supersingular curves computes the E_2-term of the $K(2)$-local Adams–Novikov spectral sequence converging to $\pi_*(S_{K(2)})$. The chief difference between this paper and the work of Baker is that we insist on working only with the actual rings of isogenies, and not their p-completions.

In Section 1, we recall the relationship between maximal orders of D and the endomorphism rings of supersingular curves at p. In Section 2, we recall the homological criterion that is employed in [9] to detect dense subgroups of $\mathbb{S}l_2^0$ for $p > 2$. We then extend these methods to give an explicit criterion for density at the prime 2. We use these criteria in Section 3 to prove Theorems 0.1 and 0.2, and Corollary 0.3.

The first author would like to thank Hans-Werner Henn for pointing out to him that Theorem 0.1 is true in the case of $p = 3$ and $\ell = 2$. Thanks also go to Johan de Jong and Catherine O'Neil for helpful discussions related to this paper.

1. Supersingular curves and endomorphism rings

In this section we recall the correspondence between endomorphism rings of supersingular curves and maximal orders of D. Any two supersingular elliptic curves C_1 and C_2 over $\overline{\mathbb{F}}_p$ are isogenous. In fact, Kohel proves the following proposition.

Proposition 1.1 (*Kohel [11, Corollary 77]*). *Let C_1 and C_2 be supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Then for all $k \gg 0$, there exists an isogeny $\phi : C_1 \to C_2$ of degree ℓ^k.*

Let X^{ss} be the collection of isomorphism classes of supersingular curves C' over $\overline{\mathbb{F}}_p$. Given an isogeny $\phi : C \to C'$ of degree N, we define a map

$$\iota_\phi : \mathrm{End}(C') \to \mathrm{End}(C) \otimes \mathbb{Z}[1/N] \subset D$$

by

$$\iota_\phi(\alpha) = \frac{1}{N} \cdot \widehat{\phi} \circ \alpha \circ \phi.$$

The map ι_ϕ is a ring homomorphism and its image is a maximal order in D. If $\phi' : C \to C'$ is another choice of isogeny then it is easily seen that the maximal order $\iota_{\phi'}(\mathrm{End}(C'))$ is conjugate to $\iota_\phi(\mathrm{End}(C'))$. Let $\mathcal{M}_D$ be the collection of conjugacy classes of maximal orders of D. Consider the map

$$\xi : X^{ss} \to \mathcal{M}_D$$

given by $\xi([C']) = [\iota_\phi(\mathrm{End}(C'))]$.

Theorem 1.2 (*Deuring [4], Kohel [12]*). *The map ξ is a surjection and the preimage of a conjugacy class $[\mathcal{O}']$ of maximal orders consists of either a single class represented by a curve with j-invariant in $\mathbb{F}_p$, or two classes represented by curves with distinct Galois-conjugate j-invariants in $\mathbb{F}_{p^2}$.*

In the former case, the elliptic curve can be defined over $\mathbb{F}_p$, and in the latter case it can only be defined over $\mathbb{F}_{p^2}$.

We choose a preferred set of representatives of conjugacy classes in $\mathcal{M}_D$ for the remainder of this note. Fix a choice of representative C' of each isomorphism class $[C'] \in X^{ss}$. Using Proposition 1.1, choose for each C' an isogeny

$$\phi_{C'} : C \to C'$$

of degree $\ell^{e(C')}$. Define $\mathcal{O}_{C'}$ to be the maximal order $\iota_{\phi_{C'}}(\mathrm{End}(C'))$. By letting C be the representative of its isomorphism class, and fixing $\phi_C = \mathrm{Id}_C$, we can arrange that $\mathcal{O}_C = \mathrm{End}(C)$. The following is immediate from Theorem 1.2.

Corollary 1.3. *Every maximal order $\mathcal{O}'$ of D is conjugate to one of the form $\mathcal{O}_{C'}$ for some $C' \in X^{ss}$.*

Let $\mathcal{O}'$ be a maximal order of D. Then by Corollary 1.3, $c_y(\mathcal{O}') = y^{-1}\mathcal{O}'y$ is equal to $\mathcal{O}_{C'}$ for some $y \in D$ and some supersingular elliptic curve C'. The map $\iota_{\widehat{\phi}} \circ c_y : \mathcal{O}' \to$

$\mathrm{End}(C) \otimes \mathbb{Z}[1/\ell]$ extends to a norm-preserving ring isomorphism

$$\iota_{\widehat{\phi}} \circ c_y : \mathcal{O}' \otimes \mathbb{Z}[1/\ell] \to \mathcal{O} \otimes \mathbb{Z}[1/\ell]$$

with inverse $c_{y^{-1}} \circ \iota_\phi$. In particular, we have the following.

Corollary 1.4. *Suppose that x' is contained in a maximal $\mathbb{Z}[1/\ell]$-order $\mathcal{O}'[1/\ell]$ of D. Then there exists an element $x \in \mathcal{O}[1/\ell]$ with the same minimal polynomial as x'.*

2. A cohomological criterion for density

In this section we recall some material from [9], but we give this material a slightly different treatment. Our reason is that the authors of [9] use results of Riehm [20] on the structure of the commutator subgroups of $\mathbb{S}l_n$. Riehm's analysis, however, excludes the case of $n = 2$ and $p = 2$, and it turns out that this case has different behavior.

The maximal order $\mathcal{O}_p$ of D_p admits a presentation [17, Appendix 2]

$$\mathcal{O}_p = \mathbb{W}\langle S\rangle/(S^2 = p, Sa = \overline{a}S). \tag{2.1}$$

Here $\mathbb{W} = \mathbb{W}(\mathbb{F}_{p^2})$ is the Witt ring with residue field $\mathbb{F}_{p^2}$, and $\overline{a}$ denotes the Galois conjugate (lift of the Frobenius on $\mathbb{F}_{p^2}$) of an element $a \in \mathbb{W}$. Every element of $\mathcal{O}_p$ can then be written uniquely in the form

$$a + bS$$

for $a, b \in \mathbb{W}$. The group $\mathbb{S}_2 = \mathcal{O}_p^\times$ consists of all such elements where $a \not\equiv 0 \pmod p$.

Let $\mathbb{S}_2^0$ be the p-Sylow subgroup of $\mathbb{S}_2$. The group $\mathbb{S}_2^0$ consists of all elements $a + bS$ where $a \equiv 1 \pmod p$. The subgroup $\mathbb{S}l_2^0$ of elements of $\mathbb{S}_2^0$ of norm 1 is the p-Sylow subgroup of $\mathbb{S}l_2$.

Suppose that G is a pro-p-group. Let G^* be the Frattini subgroup of G, which is the minimal closed normal subgroup that contains G^p and $[G, G]$. Then we have the following theorem.

Theorem 2.1 (*Koch [10], Serre [21]*). *Suppose that H is a subgroup of a pro-p-group G. Then H is dense in G if and only if the composite*

$$H \hookrightarrow G \to G/G^* = H_1^c(G; \mathbb{F}_p)$$

is surjective.

Corollary 2.2. *Let $\{\alpha_i\}$ form an $\mathbb{F}_p$-basis of the continuous group homomorphisms $\mathrm{Hom}^c(G, \mathbb{F}_p) = H_c^1(G; \mathbb{F}_p)$. Then H is a dense subgroup of G if and only if the composite*

$$H \to G \xrightarrow{\bigoplus_i \alpha_i} \bigoplus_i \mathbb{F}_p$$

is surjective.

Every element $x \in \mathbb{S}_2^0$ may be written uniquely in the form

$$x = (1 + pt_2 + p^2 t_4 + \cdots) + (t_1 + pt_3 + p^2 t_5 + \cdots)S, \tag{2.2}$$

where $t_i = t_i(x)$ are Teichmüller lifts of elements of $\mathbb{F}_{p^2}$ in $\mathbb{W}$. This is equivalent to saying that the elements t_i satisfy $t_i^{p^2} = t_i$. The coefficients t_i give rise to continuous functions

$$t_i : \mathbb{S}_2^0 \to \mathbb{F}_{p^2}.$$

Ravenel [15] uses this presentation to express $\mathbb{S}_2^0$ as the $\mathbb{F}_{p^2}$-points of a pro-affine group scheme Spec $S(2)$, where $S(2)$ is the Morava stabilizer algebra

$$S(2) = \mathbb{F}_p[t_1, t_2, t_3, \ldots]/(t_i^{p^2} = t_i).$$

The algebra $S(2)$ is a Hopf algebra. Eq. (2.2) gives an isomorphism of groups

$$\mathbb{S}_2^0 \cong \text{Spec } S(2)(\mathbb{F}_{p^2}).$$

Ravenel shows that this isomorphism gives an isomorphism in cohomology:

$$\begin{aligned} H_c^*(\mathbb{S}_2^0; \mathbb{F}_{p^2}) &= H^*(S(2)) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2} \\ &= \mathrm{Ext}_{S(2)}(\mathbb{F}_p, \mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}. \end{aligned}$$

The Ext group is taken in the category of $S(2)$-comodules.

For an arbitrary element $x \in \mathbb{S}_2^0$ expressed as in Eq. (2.2), express the norm $N(x) \in \mathbb{Z}_p^\times$ by

$$N(x) = 1 + ps_1 + p^2 s_2 + \cdots,$$

where the elements $s_i = s_i(t_1, t_2, \ldots)$ are polynomial functions of the t_i, and $s_i^p = s_i$ are Teichmüller lifts of elements of $\mathbb{F}_p$ (compare with the discussion preceding Theorem 6.3.12 of [17]). Then we may define a quotient Hopf algebra

$$Sl(2) = S(2)/(s_i(t_1, t_2, \ldots)),$$

whose $\mathbb{F}_{p^2}$ points give the subgroups $\mathbb{S}l_2^0$ and for which

$$H_c^*(\mathbb{S}l_2^0; \mathbb{F}_{p^2}) = H^*(Sl(2)) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}.$$

The following computation is obtained from combining Theorems 6.2.7 and 6.3.12 of [17].

Lemma 2.3. *For $p > 2$, we have*

$$H^1(Sl(2)) = \mathbb{F}_p\{h_{1,0}, h_{1,1}\},$$

where $h_{1,i}$ is represented by the element $[t_1^{p^i}]$ in the cobar complex for $Sl(2)$.

Corollary 2.4. *For $p > 2$, the group*

$$H_c^1(\mathbb{S}l_2^0; \mathbb{F}_{p^2}) \cong \mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_{p^2})$$

has an $\mathbb{F}_{p^2}$-basis consisting of the continuous homomorphisms

$$t_1, t_1^p : \mathbb{S}_2^0 \to \mathbb{F}_{p^2}.$$

Corollary 2.5 (*Gorbounov–Mahowald–Symonds [9]*). *For $p > 2$, a subgroup H of $\mathbb{S}l_2^0$ is dense if and only if the composite*

$$H \hookrightarrow \mathbb{S}_2^0 \xrightarrow{t_1} \mathbb{F}_{p^2}$$

is surjective.

Proof. Let $\omega \in \mathbb{F}_{p^2}$ be a primitive $p^2 - 1$ root of unity. We may compute the cohomology with $\mathbb{F}_p$ coefficients by taking $\mathrm{Gal} = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ fixed points, and obtain

$$\mathrm{Hom}^c(\mathbb{S}_2^0, \mathbb{F}_p) = \mathrm{Hom}^c(\mathbb{S}_2^0, \mathbb{F}_{p^2})^{\mathrm{Gal}}.$$

(The Galois group only acts on the coefficient group and not on $\mathbb{S}_2^0$.) Here the Frobenius $\sigma \in \mathrm{Gal}$ acts by $\sigma(t_1^{p^i}) = t_1^{p^{i+1}}$ for $i \in \mathbb{Z}/2$. An $\mathbb{F}_p$-basis for this fixed-point module is given by the pair of homomorphisms

$$t_1 + t_1^p, \omega t_1 + \omega^p t_1^p : \mathbb{S}_2^0 \to \mathbb{F}_{p^2}.$$

The result now follows from Corollary 2.2. $\square$

We now address the case where $p = 2$.

Lemma 2.6. *Let $p = 2$. Then we have*

$$H^1(Sl(2)) = \mathbb{F}_2\{h_{1,0}, h_{1,1}, h_{3,0}, h_{3,1}\},$$

where the generators are represented in the cobar complex for $Sl(2)$ by

$$h_{1,i} = [t_1^{2^i}],$$
$$h_{3,i} = [(t_3 + t_1 t_2)^{2^i}].$$

Proof. We follow the same approach of [17, 6.3] using the May spectral sequence. (It is important to refer to the second edition of [17]; the previous version, as well as [16], had an error in the restriction formula in the restricted Lie algebras $\widetilde{L}(n)$.) The May spectral sequence for $Sl(2)$ takes the form

$$E_2^{s,*} = H^s(E^0 Sl(2)) \Rightarrow H^s(Sl(2)).$$

The E_1-term may be regarded as the Koszul complex for $(E^0 Sl(2))^*$

$$E_1^{*,*} = \mathbb{F}_2[h_{i,j} : i \geq 1, j \in \mathbb{Z}/2]/(h_{2k,j} + h_{2k,j+1}),$$

with differential

$$d_1(h_{i,j}) = \begin{cases} \sum_{i_1+i_2=i} h_{i_1,j} h_{i_2,j+i_1} & i \leq 4, \\ h_{i-2,j+1}^2 & i > 4. \end{cases}$$

We see that the only elements of $E_1^{1,*}$ that persist to $E_2^{1,*}$ are $h_{1,0}$, $h_{1,1}$, $h_{3,0}$, and $h_{3,1}$.

We will show that these elements are permanent cycles in the May spectral sequence by explicitly producing cocycles in the cobar complex that they detect. By taking the images of the formulas for the coproduct on BP_*BP in [6], we arrive at the following formulas for the coproduct in $Sl(2)$:

$$\Delta(t_1) = t_1 \otimes 1 + 1 \otimes t_1,$$
$$\Delta(t_2) = t_2 \otimes 1 + t_1 \otimes t_1^2 + 1 \otimes t_2,$$
$$\Delta(t_3) = t_3 \otimes 1 + t_1 \otimes t_2^2 + t_2 \otimes t_1 + t_1^2 \otimes t_1^2 + 1 \otimes t_3.$$

Using the relation

$$s_1 = t_2 + t_2^2 + t_1^3 = 0,$$

these formulas may be used to verify that the cobar expressions in the statement of the lemma are permanent cycles. □

Corollary 2.7. *For $p = 2$, the group*

$$H_c^1(\mathbb{S}l_2^0; \mathbb{F}_4) \cong \mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_4)$$

has an $\mathbb{F}_4$-basis given by the continuous homomorphisms

$$t_1, t_1^2, t_3 + t_1t_2, (t_3 + t_1t_2)^2 : \mathbb{S}l_2^0 \to \mathbb{F}_4.$$

Corollary 2.8. *For $p = 2$, a subgroup H of $\mathbb{S}l_2^0$ is dense if and only if the composite*

$$H \hookrightarrow \mathbb{S}_2^0 \xrightarrow{t_1 \oplus (t_3 + t_1t_2)} \mathbb{F}_4 \oplus \mathbb{F}_4$$

is surjective.

Proof. Let $\omega \in \mathbb{F}_4$ be a primitive 3rd root of unity. Just as in Corollary 2.5, we compute the cohomology with $\mathbb{F}_2$ coefficients by taking $\mathrm{Gal} = \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$ fixed points, and obtain

$$\mathrm{Hom}^c(\mathbb{S}_2^0, \mathbb{F}_2) = \mathrm{Hom}^c(\mathbb{S}_2^0, \mathbb{F}_4)^{\mathrm{Gal}}.$$

(As before, the Galois group only acts on the coefficient group.) An $\mathbb{F}_2$-basis for this fixed-point module is given by the homomorphisms $t_1 + t_1^2$, $\omega t_1 + \omega^2 t_1^2$, $t_3 + t_1t_2 + (t_3 + t_1t_2)^2$, and $\omega(t_3 + t_1t_2) + \omega^2(t_3 + t_1t_2)^2$. □

3. Proof of Theorems 0.1 and 0.2, and Corollary 0.3

We will make use of the following proposition, which is a special case of Proposition 9.19 of [23].

Proposition 3.1. *Suppose that $f(x) = x^2 + a_1x + a_2$ is a monic polynomial over $\mathbb{Q}$ that is irreducible over $\mathbb{Q}_p$ and $\mathbb{R}$. Then there exists an α in D with $f(\alpha) = 0$. If the elements a_i are integral over $R \subset \mathbb{Q}$, then α lies in a maximal R-order of D.*

Proof of Theorem 0.2 for $p > 2$. We will use Proposition 3.1 to produce elements x_1, x_2 in Λ so that $t_1(x_1), t_1(x_2)$ form an $\mathbb{F}_p$ basis of $\mathbb{F}_{p^2}$. Corollary 2.5 then yields the result.

Choose integers r_1 and r_2 such that $r_i \not\equiv 0 \pmod p$, and so that r_1 is a square and r_2 is not a square in $\mathbb{F}_p$. Let

$$\alpha_i = \frac{-pr_i - 2}{\ell^{m_i p(p-1)}},$$

where the integers m_i are chosen sufficiently large so that

$$\alpha_i^2 < 4. \tag{3.1}$$

We claim that the polynomials

$$f_i(x) = x^2 + \alpha_i x + 1$$

are irreducible over $\mathbb{R}$ and $\mathbb{Q}_p$. It suffices to check that the discriminants $\Delta_i = \alpha_i^2 - 4$ are not squares in each of these fields. Condition (3.1) guarantees that Δ_i is not a square in $\mathbb{R}$. Over $\mathbb{Q}_p$ we note that Δ_i lies in $\mathbb{Z}_p$, so it suffices to check that Δ_i is not a square in $\mathbb{Z}/p^2$. Because $\ell^{p(p-1)}$ is congruent to 1 in $\mathbb{Z}/p^2$, we have

$$\Delta_i \equiv 4pr_i \pmod{p^2}.$$

As r_i is not congruent to 0 (mod p), Δ_i is not a square in $\mathbb{Z}/p^2$.

Applying Proposition 3.1, we see that there exist $\widetilde{x}_i$ in D so that $f_i(\widetilde{x}_i) = 0$. The elements $\widetilde{x}_i$ satisfy monic quadratics over $\mathbb{Z}[1/\ell]$, and so these elements are contained in maximal $\mathbb{Z}[1/\ell]$-orders $\mathcal{O}_i[1/\ell]$ of D. Applying Corollary 1.4, there exist elements $x_i \in \mathcal{O}[1/\ell]$ such that

$$f_i(x_i) = x_i^2 + \alpha_i x_i + 1 = 0. \tag{3.2}$$

The x_i satisfy $N(x_i) = 1$. Therefore, we conclude that the elements x_i are contained in the group Γ^1.

The images of the α_i in $\mathbb{Q}_p$ lie in $\mathbb{Z}_p$, so the images of the x_i in D_p lie in $\mathcal{O}_p$. Write x_i in the form

$$x_i = a_i + b_i S$$

for $a_i, b_i \in \mathbb{W}$. Reducing Eq. (3.2) modulo the ideal (S), we see that

$$x_i^2 - 2x_i + 1 \equiv a_i^2 - 2a_i + 1 \equiv 0 \pmod{S}.$$

We conclude that $a_i \equiv 1 \pmod{p}$. This implies that the elements x_i actually lie in Λ, and their images in $\mathcal{O}_p$ are of the form

$$x_i = (1 + pa_i' + b_i S)$$

for $a_i' \in \mathbb{W}$.

Eq. (3.2) implies that the reduced trace of x_i is given by

$$\mathrm{Tr}(x_i) = 2 + p\mathrm{Tr}(a_i') = -\alpha_i, \tag{3.3}$$

whereas the reduced norm is given by

$$N(x_i) = 1 + p\mathrm{Tr}(a_i') + p^2 N(a_i') - pN(b_i) = 1. \tag{3.4}$$

Substituting the expression for $\mathrm{Tr}(a_i')$ given by Eq. (3.3) gives

$$N(b_i) = pN(a_i') - \frac{\alpha_i + 2}{p}. \tag{3.5}$$

Note that $\alpha_i \equiv -2 \pmod{p}$. Reducing Eq. (3.5) modulo p yields

$$N(t_1(x_i)) \equiv N(b_i) \equiv r_i \in \mathbb{F}_p.$$

If $t_1(x_1)$ and $t_1(x_2)$ were $\mathbb{F}_p$ linearly dependent in $\mathbb{F}_{p^2}$, their norms would lie in the same quadratic residue class. The r_i were chosen so that this does not happen, so we conclude that $\{t_1(x_1), t_1(x_2)\}$ forms a basis of $\mathbb{F}_{p^2}$. Therefore, by Corollary 2.5, the subgroup Λ is dense in $\mathbb{S}l_2^0$. $\square$

Proof of Theorem 0.2 for $p = 2$**.** The proof is similar to the proof for $p > 2$, but more involved. There is precisely one isomorphism class of supersingular elliptic curve C at $p = 2$. It follows that D has one conjugacy class of maximal order. By checking the invariants of the division algebra D, it can be shown [14] that D is of the form of the rational quaternions

$$\mathbb{Q}\langle i, j\rangle/(i^2 = j^2 = -1, ij = -ji).$$

We may therefore assume that $\mathrm{End}(C) \subset D$ is the maximal order $\mathcal{O}$ generated by

$$\{\omega, i, j, k\},$$

where $k = ij$ and $\omega = \frac{1+i+j+k}{2}$. Note that $\omega^3 = 1$. The automorphism group $\mathrm{Aut}C = \mathrm{End}(C)^\times$ is the binary tetrahedral group $\tilde{A}_4$ of order 24 given by the semidirect product $Q_8 \rtimes C_3$. The cyclic group C_3 is generated by ω and the quaternion group Q_8 is generated by i and j. We have $\omega i \omega^2 = j$ and $\omega j \omega^2 = k$.

Let T be the element $i - j \in \mathcal{O}$. Then we have $T^2 = -2$ and $T\omega = \omega^2 T$. The Witt ring $\mathbb{W} = \mathbb{W}(\mathbb{F}_4)$ will be identified with the subring

$$\mathbb{Z}_2[\omega] \subset \mathcal{O} \otimes \mathbb{Z}_2 = \mathcal{O}_2.$$

Let $z \in \mathbb{W}$ be an element of norm -1. Then the element $S = zT$ in $\mathcal{O}_2$ has the property $S^2 = 2$ and $Sa = \bar{a}S$ for $a \in \mathbb{W}$. This makes explicit the presentation of $\mathcal{O}_2$ in terms of S and $\mathbb{W}$ given in Eq. (2.1).

Claim 1: Let $a, b, \in \mathbb{W}$ be such that $x = (1 + a) + bS \in \mathcal{O}_2$ has minimal polynomial $x^2 + 1$. Then we must have $a \equiv 0 \pmod{2}$ and $\nu_2(b) = 0$.

Proof of Claim 1: In order for x to have this minimal polynomial, we must have the following:

$$\mathrm{Tr}(x) = 2 + \mathrm{Tr}(a) = 0, \tag{3.6}$$

$$N(x) = 1 + \mathrm{Tr}(a) + N(a) - 2N(b) = 1. \tag{3.7}$$

Reducing Eq. (3.6) mod 4, we see that

$$\mathrm{Tr}(a) \equiv 2 \pmod{4}.$$

Substituting this into Eq. (3.7) and reducing mod 2, we see that $N(a) \equiv 0 \pmod{2}$. Write $a = 2a'$. Then we have $N(a) = 4N(a')$. Therefore, when we reduce Eq. (3.7) modulo 4, we get $N(b) \equiv 1 \pmod{2}$, and we conclude that $\nu_2(b) = 0$.

Claim 2: Suppose $a, b \in \mathbb{W}$ and $\alpha \in \mathbb{Z}_2$ are such that $x = (1+a) + bS \in \mathcal{O}_2$ has minimal polynomial $x^2 + \alpha x + 1$. Then if α satisfies $\alpha \equiv 6 \pmod{16}$, we must have $a \equiv 0 \pmod 2$ and $\nu_2(b) = 1$.

Proof of Claim 2: Because $\alpha \equiv 6 \pmod{16}$, we can write $2 + \alpha = 4\gamma$, where $\gamma \equiv 2 \pmod 4$.

In order for x to have this minimal polynomial, we must have $\mathrm{Tr}(x) = -\alpha$ and $N(x) = 1$. As a result, we have the following:

$$\mathrm{Tr}(a) = -4\gamma, \tag{3.8}$$

$$N(a) = 2N(b) + 4\gamma. \tag{3.9}$$

Reducing Eq. (3.9), we find that

$$N(a) \equiv 2N(b) \pmod 4. \tag{3.10}$$

This shows that $N(a) \equiv 0 \pmod 2$. Writing $a = 2a'$ and substituting back into Eq. (3.10), we find that $N(b) \equiv 0 \pmod 2$, so $b = 2b'$.

Re-expanding Eqs. (3.8) and (3.9) gives the following:

$$\mathrm{Tr}(a') = -2\gamma, \tag{3.11}$$

$$N(a') = 2N(b') + \gamma. \tag{3.12}$$

From Eq. (3.11), we find $\mathrm{Tr}(a') \equiv 0 \pmod 2$. Write $a' = a_1 + a_2\omega \in \mathbb{W}$. Because $\mathrm{Tr}(a') = 2a_1 - a_2 \equiv 0 \pmod 2$, we find $a_2 \equiv 0 \pmod 2$. As a result we can write $a' = u + vd$ for $u, v \in \mathbb{Z}_2$ and $d = \sqrt{-3} = 2\omega + 1$. We then have $N(a') = u^2 + 3v^2$. Therefore, Eq. (3.12) can be reduced as follows:

$$u^2 - v^2 \equiv 2N(b') + 2 \pmod 4. \tag{3.13}$$

However, the equation $u^2 - v^2 \equiv 2 \pmod 4$ has no integer solutions. In order for Eq. (3.13) to hold, we must have $N(b') \equiv 1 \pmod 2$, or equivalently $\nu_2(b) = 1 + \nu_2(b') = 1$.

Claim 3: Given $x \in \mathbb{S}l_2^0$, let $x' = \omega^2 x \omega$. Then x' is in $\mathbb{S}l_2^0$ and we have

$$t_i(x') = \begin{cases} t_i(x) & i \text{ even}, \\ \omega t_i(x) & i \text{ odd}. \end{cases}$$

This claim is immediate from the definition of the functions t_i given in Section 2.

We now complete the proof of Theorem 0.2 for the case $p = 2$. Consider the polynomial

$$f(x) = x^2 + \frac{6}{\ell^4}x + 1$$

with discriminant $\Delta = 4(9/\ell^8 - 1)$. We have that $\Delta < 0$, so the polynomial f is irreducible over $\mathbb{R}$, and f is irreducible over $\mathbb{Z}_2$ because $\nu_2(\Delta)$ is odd. By Proposition 3.1 and Corollary 1.4 there exists an element y of $\mathcal{O}[1/\ell]$ so that $f(y) = 0$. Because $N(y) = 1$, the element y lies in Γ^1.

In order to show that Λ satisfies the hypotheses of Corollary 2.8, we claim that the elements

$$i, k, y, y' = \omega^2 y \omega$$

lie in Λ, and their images under the homomorphism

$$t_1 \oplus (t_3 + t_1 t_2) : \mathbb{S}l_2^0 \to \mathbb{F}_4 \oplus \mathbb{F}_4$$

form an $\mathbb{F}_2$-basis of $\mathbb{F}_4 \oplus \mathbb{F}_4$. Claims 1, 2, and 3 imply that these elements do lie in Λ, and the functions t_i evaluated on them satisfy

$$\begin{aligned}
&t_1(i) \neq 0,\\
&t_1(k) = \omega t_1(i),\\
&t_1(y) = 0,\\
&t_1(y') = 0,\\
&t_3(y) \neq 0,\\
&t_3(y') = \omega t_3(y).
\end{aligned}$$

These conditions are sufficient for concluding that their images give a basis. Corollary 2.8 now implies that Λ is dense in $\mathbb{S}l_2^0$. $\square$

Proof of Corollary 0.3. There is a short exact sequence

$$1 \to \mathbb{S}l_2^0 \to \mathbb{S}l_2 \to C_{p+1} \to 1,$$

where the cyclic group C_{p+1} is the group of elements of $\mathbb{F}_{p^2}^\times = (\mathcal{O}_p/(S))^\times$ of $\mathbb{F}_p$-norm 1. It therefore suffices to show that we can lift the generator of C_{p+1} to an element of Γ^1. Let $\overline{y} \in \mathbb{F}_{p^2}^\times$ be a generator of the norm 1 subgroup, with minimal polynomial

$$\overline{f}(x) = x^2 + ax + 1$$

over $\mathbb{F}_p$. Let $\tilde{a}$ be an integer that reduces to a modulo p, and define $\alpha = \tilde{a}/\ell^{m(p-1)}$ where m is chosen sufficiently large that $\alpha^2 < 4$. Then the polynomial

$$f(x) = x^2 + \alpha x + 1$$

is irreducible over $\mathbb{Q}_p$ and $\mathbb{R}$. Just as in the proof of Theorem 0.2, Proposition 3.1 and Corollary 1.4 may be used to show that there exists an element $y \in \mathcal{O}[1/\ell]$ so that y reduces to a generator of C_{p+1}. Because y has norm 1, it lies in Γ^1. $\square$

Proof of Theorem 0.1. Assume that $p > 2$. In the light of Corollary 0.3 and the short exact sequence

$$1 \to \mathbb{S}l_2 \to \mathbb{S}_2 \xrightarrow{N} \mathbb{Z}_p^\times \to 1,$$

we must show that there exists an element x of Γ so that $N(x)$ is a topological generator of $\mathbb{Z}_p^\times$. Because ℓ was assumed to be a topological generator, it suffices to show there exists an x so that $N(x) = \ell$. By Proposition 1.1, for m sufficiently large there exists an endomorphism $\alpha \in \mathrm{End}(C)$ of degree ℓ^{2m+1}. Then the element $x = \ell^{-m}\alpha \in \Gamma$ has norm ℓ. The argument for $p = 2$ is identical, except that we use the short exact sequence

$$1 \to \mathbb{S}l_2 \to \widetilde{\mathbb{S}}_2 \xrightarrow{N} \mathbb{Z}_2^\times/\{\pm 1\} \to 1. \quad \square$$

Acknowledgement

Behrens and Lawson were supported by the NSF.

References

[1] A. Baker, Isogenies of supersingular elliptic curves over finite fields and operations in elliptic cohomology, Glasgow University Mathematics Department. Preprint 98/39.

[2] M. Behrens, A modular description of the $K(2)$-local sphere at the prime 3, Topology 45 (2) (2006) 343–402.

[3] M. Behrens, Buildings, elliptic curves, and the $K(2)$-local sphere (preprint).

[4] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272.

[5] E.S. Devinatz, M.J. Hopkins, Homotopy fixed point spectra for closed subgroups of the Morava stabilizer groups, Topology 43 (1) (2004) 1–47.

[6] V. Giambalvo, Some tables for formal groups and BP, in: Geometric applications of homotopy theory (Proc. Conf., Evanston, Ill., 1977), II, in: Lecture Notes in Math., vol. 658, Springer, Berlin, 1978, pp. 169–176.

[7] P. Goerss, H.-W. Henn, M. Mahowald, C. Rezk, A resolution of the $K(2)$-local sphere at the prime 3, Ann. of Math. 162 (2005) 777–822.

[8] P.G. Goerss, M.J. Hopkins, Moduli spaces of commutative ring spectra. Structured ring spectra, in: London Math. Soc. Lecture Note Ser., vol. 315, Cambridge Univ. Press, Cambridge, 2004, pp. 151–200.

[9] V. Gorbounov, M. Mahowald, P. Symonds, Infinite subgroups of the Morava stabilizer groups, Topology 37 (6) (1998) 1371–1379.

[10] H. Koch, Galoissche Theorie der p-Erweiterungen, in: Mit einem Geleitwort von I. R. Šafarevič, Springer-Verlag, Berlin–New York, VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.

[11] D.R. Kohel, Endomorphism rings of elliptic curves over finite fields, Ph.D. Thesis, University of California at Berkeley.

[12] D.R. Kohel, Hecke module structure of quaternions, in: Class Field Theory—its Centenary and Prospect (Tokyo, 1998), in: Adv. Stud. Pure Math., vol. 30, Math. Soc., Japan, Tokyo, 2001, pp. 177–195.

[13] J. Morava, Noetherian localisations of categories of cobordism comodules, Ann. of Math. (2) 121 (1) (1985) 1–39.

[14] A. Pizer, An algorithm for computing modular forms on $\Gamma_0(N)$, J. Algebra 64 (2) (1980) 340–390.

[15] D.C. Ravenel, The structure of Morava stabilizer algebras, Invent. Math. 37 (2) (1976) 109–120.

[16] D.C. Ravenel, The cohomology of the Morava stabilizer algebras, Math. Z. 152 (3) (1977) 287–297.

[17] D.C. Ravenel, Complex cobordism and stable homotopy groups of spheres, 2nd edition, AMS Chelsea Publishing, Amer. Math. Soc., Providence, RI, 2004.

[18] D.C. Ravenel, Nilpotence and periodicity in stable homotopy theory, Appendix C by Jeff Smith, in: Annals of Mathematics Studies, vol. 128, Princeton University Press, Princeton, NJ, 1992.

[19] C. Rezk, Notes on the Hopkins–Miller theorem, in: Homotopy theory via algebraic geometry and group representations (Evanston, IL, 1997), in: Contemp. Math., vol. 220, Amer. Math. Soc., Providence, RI, 1998, pp. 313–366.

[20] C. Riehm, The norm 1 group of a $\mathfrak{p}$-adic division algebra, Amer. J. Math. 92 (1970) 499–523.

[21] J.P. Serre, Cohomologie galoisienne, Cours au Collège de France, 1962–1963 (With a contribution by Jean-Louis Verdier), seconde édition, in: Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, Heidelberg, New York, 1964.

[22] J.H. Silverman, The arithmetic of elliptic curves, in: Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[23] R.G. Swan, K-theory of finite groups and orders, in: Lecture Notes in Mathematics, vol. 149, Springer-Verlag, Berlin, New York, 1970.

[24] W.C. Waterhouse, J.S. Milne, Abelian varieties over finite fields, Proc. Sympos. Pure Math. XX (1971) 53–64.