Compositio Math. 144 (2008) 247–270
doi:10.1112/S0010437X07003181

Arithmetically defined dense subgroups of Morava stabilizer groups

Niko Naumann

Abstract

For every prime p and integer $n \geqslant 3$ we explicitly construct an abelian variety $A/\mathbb{F}_{p^n}$ of dimension n such that for a suitable prime l the group of quasi-isogenies of $A/\mathbb{F}_{p^n}$ of l-power degree is canonically a dense subgroup of the nth Morava stabilizer group at p. We also give a variant of this result taking into account a polarization. This is motivated by the recent construction by Behrens and Lawson of topological automorphic forms which generalizes topological modular forms. For this, we prove some arithmetic results of independent interest: a result about approximation of local units in maximal orders of global skew fields which also gives a precise solution to the problem of extending automorphisms of the p-divisible group of a simple abelian variety over a finite field to quasi-isogenies of the abelian variety of degree divisible by as few primes as possible.

1. Introduction

One of the most fruitful ways of studying the stable homotopy category is the chromatic approach. After localizing, in the sense of Bousfield, at a prime p, one is left with an infinite hierarchy of primes corresponding to the Morava K-theories $K(n)$, $n \geqslant 0$; see [Rav92]. The successive layers in the resulting filtration are the $K(n)$-local categories [HS99], the structure of which is governed to a large extent by (the continuous cohomology of) the nth Morava stabilizer group $\mathbb{S}_n$, i.e. the automorphism group of the one-dimensional commutative formal group of height n over $\overline{\mathbb{F}}_p$. A fundamental problem in this context is to generalize the fibration

$$L_{K(1)}S^0 \longrightarrow E_1^{hF} \longrightarrow E_1^{hF},$$

cf. the introduction of [GHMR05], to a resolution of the $K(n)$-local sphere for $n \geqslant 2$. Substantial progress on this problem for $n = 2$ and in many other cases as well has been achieved by clever use of homological algebra for $\mathbb{S}_n$-modules [GHMR05, Hen07]. Recently, pursuing a question of Mahowald and Rezk, Behrens [Beh06] was able to give a modular interpretation of one such resolution in the case $n = 2$.

A basic observation is that $\mathbb{S}_2$ is the automorphism group of the p-divisible group of a supersingular elliptic curve E over a finite field k. Hence it seemed plausible, and was established in [Beh06], that the morphisms in a resolution of a spectrum closely related to $L_{K(2)}S^0$ should have a description in terms of suitable endomorphisms of E. A key result for seeing this was to observe that, for suitable primes l,

$$\left(\mathrm{End}_k(E)\left[\frac{1}{l}\right]\right)^* \subseteq \mathbb{S}_2 \tag{1}$$

is a dense subgroup [BL06, Theorem 0.1].

Received 20 August 2006, accepted in final form 29 June 2007, published online 23 January 2008.
2000 Mathematics Subject Classification 55P42 (primary), 14L05 (secondary).
Keywords: Morava stabilizer group, maximal orders, p-divisible groups, unitary groups.
This journal is © Foundation Compositio Mathematica 2008.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

One of our main results, Theorem 25, is the direct generalization of (1) to arbitrary chromatic level $n \geqslant 3$ in which E is replaced by an abelian variety of dimension n which is known to be the minimal dimension possible.

In Corollary 21 we give a variant of the arithmetic result underlying Theorem 25 in which on the left-hand side of (1) we only allow endomorphisms which are unitary with respect to a given Rosati involution. The motivation for this stems from recent work of Behrens and Lawson [BL07] bringing the arithmetic of suitable (derived) Shimura varieties to bear on homotopy theoretic problems of arbitrary chromatic level, generalizing the role of topological modular forms for problems of chromatic level at most two; cf. [BL07, Theorem 15.2.1].

This paper is organized as follows. In § 2.1 we record a well-known result about generically trivial torsors for later reference. In § 2.2 we determine the structure of certain naturally occurring integral models for forms of SL_d; see Theorems 2 and 7. As a first application, in § 3, we consider the problem of approximating local units of maximal orders in finite-dimensional skew fields over $\mathbb{Q}$ (carrying a positive involution of the second kind) by global (unitary) units with as few denominators as possible. This is naturally an approximation problem for specific integral models of the general linear (certain unitary) group(s) and will be reduced to a similar problem for $\mathbb{G}_m$ (a specific integral model T' of a one-dimensional anisotropic torus) in Theorems 9 and 14. In § 4 we can solve the approximation problem for $\mathbb{G}_m$ using class field theory and settle a special case for T'; see Theorems 17 and 19. In § 5.1 we explain the application of the results obtained so far to the following problem: given a simple abelian variety A over a finite field one would like to extend an automorphism of the p-divisible group $A[p^\infty]$ of A to a quasi-isogeny of A the degree of which should be divisible by as few primes as possible. Finally, § 5.2 contains the proof of Theorem 25 reviewed above.

2. Arithmetic

2.1 Triviality of torsors

The following result is well known but we wish to state it in the form most suitable for later references.

Proposition 1. *Let k be a number field with ring of integers $\mathcal{O}_k$, $\emptyset \neq U \subseteq \mathrm{Spec}(\mathcal{O}_k)$ an open subscheme and G/U an affine smooth group scheme. Assume that G/U has connected fibers, that the generic fiber $G_k = G \times_U \mathrm{Spec}(k)$ is k-simple, semi-simple and simply connected and that there is a place v of k outside U such that G is isotropic at v. Then the canonical map of pointed sets*

$$\mathrm{H}^1(U, G) \to \mathrm{H}^1(\mathrm{Spec}(k), G)$$

has trivial kernel.

Proof. We use a result of Nisnevich, see [Gil02, Théorème 5.1]. Since G/U has connected fibers we have $\mathrm{H}^1_{\mathrm{fppf}}(\hat{\mathcal{O}}_x, G) = 0$ in the notation of [Gil02]. It is thus sufficient to see that for every finite set Σ of closed points of U we have

$$\left| \left(\prod_{\mathfrak{p} \in \Sigma} G(\mathcal{O}_{k,\mathfrak{p}}) \setminus G(k_\mathfrak{p}) \right) \Big/ G(U - \Sigma) \right| = 1. \tag{2}$$

Here $\mathcal{O}_{k,\mathfrak{p}}$ is the completion of $\mathcal{O}_k$ at $\mathfrak{p}$ and $k_\mathfrak{p}$ is the field of fractions of $\mathcal{O}_{k,\mathfrak{p}}$. The proof of (2) using strong approximation is very similar to the proof of Proposition 11 and is therefore left to the reader. □

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

2.2 The geometry of some groups

In this section we consider forms of SL_d. These can be described in terms of skew fields (with involution). The choice of a maximal order in the skew field determines an integral model of the algebraic group and we will study the geometry of these group schemes. The referee pointed out that some of these results, notably Theorem 2 and Theorem 7, part (ii), are part of Bruhat and Tits theory; cf. [BT84b, § 5] and [BT84a, Théorème 4.6.32].

2.2.1 *Type* A_{d-1}. Let D be a finite-dimensional skew field over $\mathbb{Q}$ and $\mathcal{O} \subseteq D$ a maximal order [Deu68, Kapitel VI]. The center of D, denoted k, is a number field and we denote by d the reduced dimension of D, i.e. $\dim_k D = d^2$. We denote by $\mathcal{O}_k \subseteq k$ the ring of integers and note that $k \cap \mathcal{O} = \mathcal{O}_k$ as an immediate consequence of [Deu68, Kapitel VI, § 11, Satz 7].

Recall that D is determined by its local invariants as follows [PR94, § 1.5.1]. Writing Σ_k for the set of places of k, for every $v \in \Sigma_k$ there is a local invariant $\mathrm{inv}_v(D) \in (1/d)\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$ and $\mathrm{inv}_v(D) = 0$ for almost all v. For a given place v, we denote by k_v the completion of k with respect to v. Then $D_v := D \otimes_k k_v$ is a central simple k_v-algebra which determines a class $[D_v] \in \mathrm{Br}(k_v)$ in the Brauer group of k_v. There are specific isomorphisms

$$\tau_v : \mathrm{Br}(k_v) \xrightarrow{\sim} \begin{cases} \mathbb{Q}/\mathbb{Z}, & v \text{ finite}, \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z}, & v \text{ real}, \\ 0, & v \text{ complex}, \end{cases}$$

such that $\mathrm{inv}_v(D) = \tau_v([D_v])$. Note that, for every $v \in \Sigma_k$, D_v is a skew field if and only if the order of $\mathrm{inv}_v(D)$ is d.

The group-valued functor G on $\mathcal{O}_k$-algebras R

$$G(R) := (\mathcal{O} \otimes_{\mathcal{O}_k} R)^*$$

is representable by an affine group scheme of finite type $G/\mathrm{Spec}(\mathcal{O}_k)$. The reduced norm induces a morphism of group schemes $\mathrm{N} : G \longrightarrow \mathbb{G}_m$ over $\mathrm{Spec}(\mathcal{O}_k)$ and writing $G' := \ker(\mathrm{N})$ gives an exact sequence of representable fppf-sheaves on $\mathrm{Spec}(\mathcal{O}_k)$:

$$1 \longrightarrow G' \longrightarrow G \xrightarrow{\mathrm{N}} \mathbb{G}_m \longrightarrow 1. \tag{3}$$

To see that N is fppf-surjective, note that the inclusion $R^* \subseteq (\mathcal{O} \otimes_{\mathcal{O}_k} R)^*$ defines a closed immersion $i : \mathbb{G}_m \longrightarrow G$ such that $\mathrm{N} \circ i$ is multiplication by d as can be checked on the generic fiber.

Theorem 2. *The groups G and G' are smooth with connected fibers over* $\mathrm{Spec}(\mathcal{O}_k)$.

For the proof, we will need the following result which might be compared with [DG70, Exposé VI_B, Proposition 9.2(xi)].

Proposition 3. *Let S be a scheme, $G, H/S$ group schemes of finite presentation with affine fibers and G/S flat, and let $\phi : G \longrightarrow H$ be a morphism of S-group schemes. Then the following are equivalent and imply that H/S is flat:*

(i) *ϕ is faithfully flat*

(ii) *ϕ is an epimorphism of fppf-sheaves*

(iii) *for every geometric point $\mathrm{Spec}(\Omega) \longrightarrow S$, ϕ_Ω is an epimorphism of fppf-sheaves.*

Proof. Since ϕ is of finite presentation, the implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are trivial, so assume that part (iii) holds true. Then, for every geometric point $\mathrm{Spec}(\Omega) \longrightarrow S$, the morphism of Ω-Hopf algebras corresponding to ϕ_Ω is injective, which follows from the existence of an fppf-local section of ϕ_Ω, and thus faithfully flat [Wat79, Theorem 4.1]. This shows that ϕ is surjective and the fiber-wise criterion for flatness [Gro66, Corollaire 11.3.11, (a) $\Rightarrow$ (b)] implies that ϕ and H/S are flat. □

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

Proof of Theorem 2. To see that $G/\mathrm{Spec}(\mathcal{O}_k)$ is smooth we use the lifting criterion [Gro67, Remarques 17.1.2,i) and 17.5.4]: if $A \longrightarrow A/I$ is the quotient of an Artinian $\mathcal{O}_k$-algebra A by an ideal $I \subseteq A$ of square zero, the surjectivity of $G(A) \longrightarrow G(A/I)$ is clear from the definition of G, hence $G/\mathrm{Spec}(\mathcal{O}_k)$ is smooth. By Proposition 3, (ii) $\Rightarrow$ (i), $\mathrm{N} : G \longrightarrow \mathbb{G}_m$ is (faithfully) flat, hence so is its base change $G'/\mathrm{Spec}(\mathcal{O}_k)$.

We shall now show that all geometric fibers of G (respectively G') are smooth and connected of dimension d^2 (respectively d^2-1). This will also imply that $G'/\mathrm{Spec}(\mathcal{O}_k)$ is smooth by the fiber-wise criterion [Gro67, Théorème 17.5.1] and thus conclude the proof.

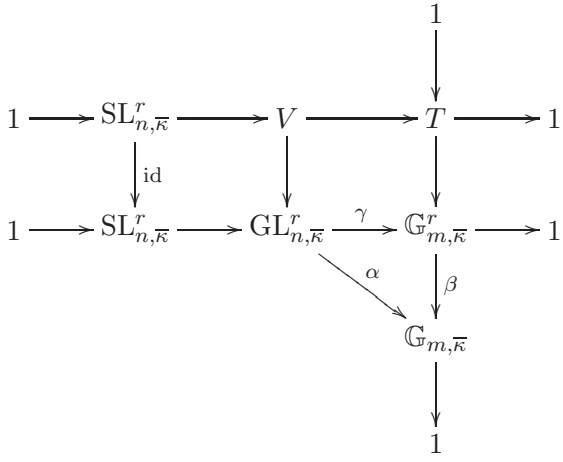
Geometric fibers of G (respectively G') in characteristic zero are isomorphic to GL_d (respectively SL_d). Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ be a prime, $\kappa := \mathcal{O}_k/\mathfrak{p}$ and $\overline{\kappa}$ be an algebraic closure of κ. We have $D_{\mathfrak{p}} \simeq \mathrm{M}_n(\mathcal{D})$ for a central skew field $\mathcal{D}$ over $k_{\mathfrak{p}}$. Denoting by r the reduced dimension of $\mathcal{D}$, we have $d = nr$. Since $\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathfrak{p}} \subseteq D_{\mathfrak{p}}$ is a maximal order [Rei03, Corollary 11.2], we have $\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathfrak{p}} \simeq \mathrm{M}_n(\mathcal{O}_{\mathcal{D}})$ as $\mathcal{O}_{k,\mathfrak{p}}$-algebras by [Rei03, Theorem 17.3] where $\mathcal{O}_{\mathcal{D}} \subseteq \mathcal{D}$ is the unique maximal order [Rei03, Theorem 12.8].

Let $\Pi \in \mathcal{O}_{\mathcal{D}}$ and $\pi \in \mathcal{O}_{k,\mathfrak{p}}$ be uniformizers. Then $\overline{A} := (\mathcal{O}_{\mathcal{D}}/\pi\mathcal{O}_{\mathcal{D}}) \otimes_{\kappa} \overline{\kappa}$ is a $\overline{\kappa}$-algebra with radical $\overline{\mathcal{R}} = (\Pi\mathcal{O}_{\mathcal{D}}/\pi\mathcal{O}_{\mathcal{D}}) \otimes_{\kappa} \overline{\kappa}$ and maximal semi-simple quotient $\overline{A}/\overline{\mathcal{R}} \simeq \overline{\kappa}^r$. Since $G_{\overline{\kappa}} = \mathrm{GL}_n(\overline{A})$, we have an extension

$$1 \longrightarrow U \longrightarrow G_{\overline{\kappa}} \longrightarrow (\mathrm{GL}_{n,\overline{\kappa}})^r \longrightarrow 1,$$

where U is a unipotent group of dimension $n^2(r-1)r$ (recall that $\pi\mathcal{O}_{\mathcal{D}} = \Pi^r\mathcal{O}_{\mathcal{D}}$ and $(\Pi^i\mathcal{O}_{\mathcal{D}}/\Pi^{i+1}\mathcal{O}_{\mathcal{D}}) \otimes_{\kappa} \overline{\kappa} \simeq \overline{\kappa}^r$). So $G_{\overline{\kappa}}$ is connected and smooth of dimension $n^2r + n^2(r-1)r = d^2$.

Since the reduced norm $\mathrm{N}_{\overline{\kappa}} : G_{\overline{\kappa}} \longrightarrow \mathbb{G}_{m,\overline{\kappa}}$ is trivial on U it factors over some $\alpha : (\mathrm{GL}_{n,\overline{\kappa}})^r \longrightarrow \mathbb{G}_{m,\overline{\kappa}}$. We have $\alpha(g_1, \ldots, g_r) = \prod_{i=1}^r \det(g_i)$ as an immediate consequence of [Kle00, Lemma 3.8]. This exhibits $G'_{\overline{\kappa}}$ as an extension of $V := \ker(\alpha)$ by U. We can factor $\alpha = \beta \circ \gamma$ with $\gamma : (\mathrm{GL}_{n,\overline{\kappa}})^r \longrightarrow \mathbb{G}^r_{m,\overline{\kappa}}$, $\gamma(g_1, \ldots, g_r) := (\det(g_i))_i$ and $\beta : \mathbb{G}^r_{m,\overline{\kappa}} \longrightarrow \mathbb{G}_{m,\overline{\kappa}}$, $\beta(x_1, \ldots, x_r) := x_1 \ldots x_r$ and thus obtain the following diagram, with $T := \ker(\beta)$.



Looking at character groups, for example, one sees that $T \simeq \mathbb{G}^{r-1}_{m,\overline{\kappa}}$ and hence V is connected and smooth of dimension $\dim(T) + \dim(\mathrm{SL}^r_n) = n^2r - 1$ and $G'_{\overline{\kappa}}$ is connected and smooth of dimension $\dim(V) + \dim(U) = d^2 - 1$. □

Remark 4. The maximal locus inside $\mathrm{Spec}(\mathcal{O}_k)$ over which G (respectively G') is reductive (respectively semi-simple) is obtained by inverting the discriminant of D, i.e. by removing all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_k)$ such that $\mathrm{inv}_{\mathfrak{p}}(D) \neq 0$.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

2.2.2 *Type* ${}^2A_{d-1}$. Let D be a finite-dimensional skew field of reduced dimension d over $\mathbb{Q}$ carrying a positive involution of the second kind $*$, i.e. for all $x \in D^*$ we have $\mathrm{tr}^D_{\mathbb{Q}}(^*xx) > 0$ (positivity) and $*$ restricted to the center L of D is non-trivial. Then L is a CM-field with $k := \{x \in L \mid x =^* x\} \subseteq L$ as its maximal real subfield [Mum70, p. 194]. Note that $*$ is k-linear. We assume that $\mathcal{O} \subseteq D$ is a maximal order which is invariant under $*$. The existence of such an order is claimed without proof in [Hid04, 7.1.1]. Then $\mathcal{O} \cap L = \mathcal{O}_L$ and $\mathcal{O} \cap k = \mathcal{O}_k$ are the rings of integers of L and k. We consider the affine group schemes of finite type U and T over $\mathrm{Spec}(\mathcal{O}_k)$ whose groups of points are given for every $\mathcal{O}_k$-algebra R by

$$\mathrm{U}(R) = \{g \in (\mathcal{O} \otimes_{\mathcal{O}_k} R)^* \mid {}^*gg = 1\},$$
$$\mathrm{T}(R) = \{g \in (\mathcal{O}_L \otimes_{\mathcal{O}_k} R)^* \mid \mathrm{N}^L_k(g) = 1\}.$$

There is a homomorphism $\mathrm{N} : \mathrm{U} \longrightarrow \mathrm{T}$ over $\mathrm{Spec}(\mathcal{O}_k)$ given on points by the reduced norm of D and we put $\mathrm{SU} := \ker(\mathrm{N})$. Over $\mathrm{Spec}(k)$ we have an exact sequence

$$1 \to \mathrm{SU}_1(D,1) = \mathrm{SU} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(k) \longrightarrow$$
$$\mathrm{U}_1(D,1) = \mathrm{U} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(k) \xrightarrow{\mathrm{N}_k} \mathrm{Res}^L_k(\mathbb{G}_{m,L})^{(1)} \longrightarrow 1,$$

where '1' denotes the standard rank one Hermitian form on D and

$$\mathrm{Res}^L_k(\mathbb{G}_{m,L})^{(1)} := \ker(\mathrm{Res}^L_k(\mathbb{G}_{m,L}) \xrightarrow{\mathrm{N}^L_k} \mathbb{G}_{m,k})$$

is a one-dimensional anisotropic torus over k; cf. [PR94, § 2.3] for notation and general background on unitary groups.

We first study the integral model $\mathrm{T}/\mathrm{Spec}(\mathcal{O}_k)$ of $\mathrm{Res}^L_k(\mathbb{G}_{m,L})^{(1)}$. We define the open subscheme $\mathcal{U} \subseteq \mathrm{Spec}(\mathcal{O}_k)$ by

$$\mathcal{U} := \mathrm{Spec}(\mathcal{O}_k) - \{0 \neq \mathfrak{p} \subseteq \mathcal{O}_k \text{ is a prime of residue characteristic 2 and ramified in } L/k\}.$$

The following result makes [CTS87, Proposition 5.2] slightly more precise in the present special case.

PROPOSITION 5. *We have that* $\mathrm{T}/\mathrm{Spec}(\mathcal{O}_k)$ *is an affine flat group scheme such that*

$$\mathrm{T}_k \simeq \mathrm{Res}^L_k(\mathbb{G}_{m,L})^{(1)}.$$

For a prime $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ *we have*

$$\mathrm{T}_{\kappa(\mathfrak{p})} \simeq \begin{cases} \mathbb{G}_{m,\kappa(\mathfrak{p})}, & \text{if } \mathfrak{p} \text{ splits in } L/k, \\ \mathrm{Res}^{\kappa(\mathfrak{p})^{(2)}}_{\kappa(\mathfrak{p})}(\mathbb{G}_{m,\kappa(\mathfrak{p})^{(2)}})^{(1)}, & \text{if } \mathfrak{p} \text{ is inert in } L/k, \\ \mathbb{G}_{a,\kappa(\mathfrak{p})} \times \mu_{2,\kappa(\mathfrak{p})}, & \text{if } \mathfrak{p} \text{ is ramified in } L/k. \end{cases}$$

In particular, the maximal locus inside $\mathrm{Spec}(\mathcal{O}_k)$ *over which* T *is smooth equals* $\mathcal{U}$. *Here,* $\kappa(\mathfrak{p}) := \mathcal{O}_k/\mathfrak{p}$ *and* $\kappa(\mathfrak{p})^{(2)}$ *is the unique quadratic extension of* $\kappa(\mathfrak{p})$.

Proof. We know that $\mathrm{Res}^{\mathcal{O}_L}_{\mathcal{O}_k}(\mathbb{G}_{m,\mathcal{O}_L})/\mathrm{Spec}(\mathcal{O}_k)$ is an affine and smooth group scheme from [BLR90, 7.6, proof of Theorem 4 and Proposition 5,h)]. There is an obvious subgroup $i : \mathbb{G}_{m,\mathcal{O}_k} \hookrightarrow \mathrm{Res}^{\mathcal{O}_L}_{\mathcal{O}_k}(\mathbb{G}_{m,\mathcal{O}_L})$ such that $\mathrm{N}^L_k \circ i$ is multiplication by 2, hence $\mathrm{N}^L_k : \mathrm{Res}^{\mathcal{O}_L}_{\mathcal{O}_k}(\mathbb{G}_{m,\mathcal{O}_L}) \longrightarrow \mathbb{G}_{m,\mathcal{O}_k}$ is an fppf-epimorphism and the first assertion follows from Proposition 3 since by definition $\mathrm{T} = \ker(\mathrm{N}^L_k)$. Since restriction commutes with base change, for every $\mathcal{O}_k$-algebra R we have

$$\mathrm{T}_R = \ker(\mathrm{Res}^{\mathcal{O}_L \otimes_{\mathcal{O}_k} R}_R(\mathbb{G}_{m,R}) \longrightarrow \mathbb{G}_{m,R}),$$

which makes the assertions concerning the generic fiber and the fibers over split and inert primes obvious.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

For ramified $\mathfrak{p}$ we have $\mathcal{O}_L \otimes_{\mathcal{O}_k} \kappa(\mathfrak{p}) \simeq \mathcal{O}_{L,\mathfrak{q}}/\mathfrak{q}^2\mathcal{O}_{L,\mathfrak{q}}$ for $\mathfrak{q}$ the unique prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. There exists $\alpha \in \mathcal{O}_{L,\mathfrak{q}}$ with $\mathcal{O}_{L,\mathfrak{q}} = \mathcal{O}_{k,\mathfrak{p}}[\alpha]$ and α satisfies an Eisenstein polynomial $x^2 - ax + b \in \mathcal{O}_{k,\mathfrak{p}}[x]$. Since $a \in \mathfrak{p}\mathcal{O}_{k,\mathfrak{p}} \subseteq \mathfrak{q}^2\mathcal{O}_{L,\mathfrak{q}}$, the non-trivial automorphism σ of $\mathcal{O}_{L,\mathfrak{q}}$ over $\mathcal{O}_{k,\mathfrak{p}}$ satisfies

$$\sigma(\alpha) = a - \alpha \equiv -\alpha \quad \text{in } \mathcal{O}_{L,\mathfrak{q}}/\mathfrak{q}^2\mathcal{O}_{L,\mathfrak{q}}.$$

As $\mathcal{O}_{L,\mathfrak{q}}/\mathfrak{q}^2\mathcal{O}_{L,\mathfrak{q}} \simeq \kappa(\mathfrak{p})[\alpha]/(\alpha^2)$ we conclude that for every $\kappa(\mathfrak{p})$-algebra R

$$\mathrm{T}_{\kappa(\mathfrak{p})}(R) \simeq \{x + y\alpha \in (R[\alpha]/(\alpha^2))^* \mid 1 = (x + y\alpha)\sigma(x + y\alpha) = (x + y\alpha)(x - y\alpha) = x^2\}$$

and we have an exact sequence

$$1 \longrightarrow \mathbb{G}_{a,\kappa(\mathfrak{p})}(R) \longrightarrow \mathrm{T}_{\kappa(\mathfrak{p})}(R) \longrightarrow \mu_{2,\kappa(\mathfrak{p})}(R) \longrightarrow 1,$$
$$x + y\alpha \longmapsto x,$$

which is split by $x \mapsto x + 0\alpha$. □

We will need the following proposition.

Proposition 6. *Let k be a commutative ring, B_1 and B_2 k-algebras and τ an involution on $B := B_1 \times B_2$ such that $\tau(x, y) = (y, x)$ for all $x, y \in k$. Then there is an isomorphism of k-algebras with involution*

$$(B, \tau) \simeq (B_1 \times B_1^{\mathrm{opp}}, (x, y) \mapsto (y, x)).$$

Proof. The proof of [KMRT98, Proposition 2.14] carries over without any change. □

Now let C be the set of non-zero primes $\mathfrak{p} \in \mathcal{U}$ such that $\mathrm{U}_{\overline{\kappa(\mathfrak{p})}}$ is an extension of a *symplectic* group. We will see during the proof of Theorem 7 that this set only contains primes which are ramified in L/k. Let $\mathrm{T}' \subseteq \mathrm{T}$ be the open subscheme obtained by removing from T the non-identity component of $\mathrm{T}_{\kappa(\mathfrak{p})}$ for all $\mathfrak{p} \in C$, cf. Proposition 5. Clearly, $\mathrm{T}' \subseteq \mathrm{T}$ is a subgroup scheme.

Theorem 7. (i) *The morphism $\mathrm{N}_{\mathcal{U}} : \mathrm{U}_{\mathcal{U}} \longrightarrow \mathrm{T}_{\mathcal{U}}$ factors through $\mathrm{T}'_{\mathcal{U}} \subseteq \mathrm{T}_{\mathcal{U}}$ and the resulting sequence of fppf-sheaves on $\mathcal{U}$*

$$1 \longrightarrow \mathrm{SU}_{\mathcal{U}} \longrightarrow \mathrm{U}_{\mathcal{U}} \xrightarrow{\mathrm{N}_{\mathcal{U}}} \mathrm{T}'_{\mathcal{U}} \longrightarrow 1$$

is exact.

(ii) *The group $\mathrm{U}/\mathcal{U}$ (respectively $\mathrm{SU}/\mathcal{U}$) is smooth (respectively smooth with connected fibers).*

Remark 8. It is easy to give examples of the situation in Theorem 7 in which $C \neq \emptyset$, i.e. $\mathrm{T}' \neq \mathrm{T}$. From case (3′.2) in the proof of Theorem 7 it will however be clear that $C = \emptyset$ if d is odd.

Proof of Theorem 7. Fix $\mathfrak{p} \in \mathcal{U}$. We will study the group schemes

$$\mathrm{U}_{\mathfrak{p}} := \mathrm{U} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}}),$$
$$\mathrm{SU}_{\mathfrak{p}} := \mathrm{SU} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$$

over $\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$. For this, we need to understand the $\mathcal{O}_{k,\mathfrak{p}}$-algebra with involution

$$\mathcal{O}_{\mathfrak{p}} := \mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathfrak{p}}.$$

We distinguish three cases.

(1) *The prime $\mathfrak{p}$ is inert in L/k.* For the unique prime $\mathfrak{q} \subseteq \mathcal{O}_L$ lying above $\mathfrak{p}$ we have $\mathrm{inv}_{\mathfrak{q}}(D) = 0$ (see [Mum70, (B) on page 199]) and

$$\mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} k_{\mathfrak{p}} \simeq D \otimes_L L_{\mathfrak{q}} \simeq \mathrm{M}_d(L_{\mathfrak{q}})$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

is a maximal order, hence $\mathcal{O}_{\mathfrak{p}} \simeq \mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}})$ as $\mathcal{O}_{k,\mathfrak{p}}$-algebras. Denote by σ the non-trivial automorphism of $\mathcal{O}_{L,\mathfrak{q}}$ over $\mathcal{O}_{k,\mathfrak{p}}$. We obtain for every $\mathcal{O}_{L,\mathfrak{q}}$-algebra R:

$$(\mathrm{U}_{\mathfrak{p}} \times_{\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})} \mathrm{Spec}(\mathcal{O}_{L,\mathfrak{q}}))(R) = \mathrm{U}_{\mathfrak{p}}(R) \simeq \{g \in \mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} R) \,|\, {}^*gg = 1\}.$$

Since $\mathfrak{p}$ is unramified we have $\mathcal{O}_{L,\mathfrak{q}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} \mathcal{O}_{L,\mathfrak{q}} \simeq \mathcal{O}_{L,\mathfrak{q}} \times \mathcal{O}_{L,\mathfrak{q}}$ and under this isomorphism $(\sigma \otimes 1)$ switches the factors. Since by Proposition 6 we have an isomorphism of $\mathcal{O}_{L,\mathfrak{q}}$-algebras with involution

$$(\mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}}) \otimes_{\mathcal{O}_{k,\mathfrak{p}}} \mathcal{O}_{L,\mathfrak{q}}, *) \simeq (\mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}}) \times \mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}})^{\mathrm{opp}}, (x,y) \mapsto ({}^{\mathrm{t}}y, {}^{\mathrm{t}}x)),$$

where ${}^{\mathrm{t}}$ denotes the transpose of a matrix, we find that

$$\mathrm{U}_{\mathfrak{p}}(R) \simeq \{(x,y) \in \mathrm{M}_d(R \times R) \simeq \mathrm{M}_d(R) \times \mathrm{M}_d(R) \mid ({}^{\mathrm{t}}y, {}^{\mathrm{t}}x)(x,y) = 1\} \simeq \mathrm{GL}_d(R).$$

We have thus shown that $\mathrm{U}_{\mathfrak{p}} \times_{\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})} \mathrm{Spec}(\mathcal{O}_{L,\mathfrak{q}}) \simeq \mathrm{GL}_{d,\mathcal{O}_{L,\mathfrak{q}}}$. By descent, we conclude that $\mathrm{U}_{\mathfrak{p}}/\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$ is smooth. Furthermore, the special fiber $\mathrm{U}_{\kappa(\mathfrak{p})} := \mathrm{U}_{\mathfrak{p}} \times_{\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})} \mathrm{Spec}(\kappa(\mathfrak{p}))$ is a $\overline{\kappa(\mathfrak{p})}/\kappa(\mathfrak{p})$-form of $\mathrm{GL}_{d,\kappa(\mathfrak{p})}$ and since $\mathrm{H}^1(\mathrm{Spec}(\kappa(\mathfrak{p})), \mathrm{PGL}_d) = 1$ we have $\mathrm{U}_{\kappa(\mathfrak{p})} \simeq \mathrm{GL}_{d,\kappa(\mathfrak{p})}$.

(2) *The prime* $\mathfrak{p}$ *splits in* L/k. In this case we have

$$\mathcal{O}_{\mathfrak{p}} \simeq \mathcal{O}_{\mathfrak{q}} \times \mathcal{O}_{\mathfrak{q}'},$$

where $\mathfrak{q}$ and $\mathfrak{q}'$ are the primes of $\mathcal{O}_L$ lying above $\mathfrak{p}$ and $\mathcal{O}_{\mathfrak{q}} := \mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O}_{L,\mathfrak{q}}$ and similarly for $\mathfrak{q}'$. By Proposition 6 we have an isomorphism of $\mathcal{O}_{k,\mathfrak{p}}$-algebras with involution

$$(\mathcal{O}_{\mathfrak{p}}, *) \simeq (\mathcal{O}_{\mathfrak{q}} \times \mathcal{O}_{\mathfrak{q}}^{\mathrm{opp}}, (x,y) \mapsto (y,x))$$

and thus $\mathrm{U}_{\mathfrak{p}} \simeq \mathrm{GL}_1(\mathcal{O}_{\mathfrak{q}})$ and this group is trivially smooth over $\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$.

(3) *The prime* $\mathfrak{p}$ *is ramified in* L/k. As in case (1) we have

$$\mathcal{O}_{\mathfrak{p}} \simeq \mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}})$$

as $\mathcal{O}_{k,\mathfrak{p}}$-algebras with $\mathfrak{q} \subseteq \mathcal{O}_L$ the unique prime lying above $\mathfrak{p}$. We check the smoothness of $\mathrm{U}_{\mathfrak{p}}/\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$ using the lifting criterion. Let A be an Artinian $\mathcal{O}_{k,\mathfrak{p}}$-algebra and $I \subseteq A$ an ideal with $I^2 = 0$. Given

$$x \in \mathrm{U}_{\mathfrak{p}}(A/I) = \{g \in (\mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} A/I)^* \mid {}^*gg = 1\},$$

there is some $y \in \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} A$ lifting x and we have

$${}^*yy = 1 + z \quad \text{for some } z \in \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} I \subseteq \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} A$$

with ${}^*z = z$ because ${}^*({}^*yy) = {}^*yy$. As $\mathfrak{p} \in \mathcal{U}$ we have $2 \in A^*$ and can define

$$y' := y(1 - \tfrac{1}{2}z) \in \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} A,$$

which still lifts x and satisfies

$${}^*y'y' = (1 - \tfrac{1}{2}{}^*z)^*yy(1 - \tfrac{1}{2}z) = (1 - \tfrac{1}{2}{}^*z)(1+z)(1 - \tfrac{1}{2}z) \overset{(I^2=0,\,{}^*z=z)}{=} 1.$$

Hence we have found $y' \in \mathrm{U}_{\mathfrak{p}}(A)$ lifting x.

At this point we have established that $\mathrm{U}/\mathcal{U}$ is smooth and we now proceed to study $\mathrm{SU}/\mathcal{U}$. We first consider the geometric fibers, showing in particular that they are all connected and smooth.

Let $\mathrm{Spec}(\Omega) \longrightarrow \mathcal{U}$ be a geometric point. If the characteristic of Ω is zero, we have $\mathrm{SU}_\Omega \simeq \mathrm{SL}_{d,\Omega}$, and hence we can assume that $\Omega = \overline{\kappa(\mathfrak{p})}$ for some $\mathfrak{p} \in \mathcal{U}$. We again have to distinguish three cases as above.

(1′) *The prime* $\mathfrak{p}$ *is inert in* L/k. From (1) above we have $\mathrm{U}_\Omega \simeq \mathrm{GL}_{d,\Omega}$ and from Proposition 5 we know that $\mathrm{T}_\Omega \simeq \mathbb{G}_{m,\Omega}$. Under these isomorphisms, N_Ω is identified with the determinant, hence $\mathrm{SU}_\Omega \simeq \mathrm{SL}_{d,\Omega}$.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

(2′) *The prime* $\mathfrak{p}$ *splits in* L/k. From (2) above and Proposition 5 we know that $\mathrm{U}_\Omega \simeq \mathrm{GL}_1(\overline{A})$ and $\mathrm{T}_\Omega \simeq \mathbb{G}_{m,\Omega}$ for the Ω-algebra $\overline{A} := \mathcal{O}_\mathfrak{q} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} \Omega$ where $\mathfrak{q} \subseteq \mathcal{O}_L$ is a prime lying above $\mathfrak{p}$. This is the situation studied in Theorem 2 from which we read off that $\mathrm{SU}_\Omega/\mathrm{Spec}(\Omega)$ is connected and smooth (and, in fact, also the dimensions of the semi-simple, toric and unipotent parts of SU_Ω in terms of the order of $\mathrm{inv}_\mathfrak{q}(D)$).

(3′) *The prime* $\mathfrak{p}$ *is ramified in* L/k. Recall from (3) above that $\mathcal{O}_\mathfrak{p} \simeq \mathrm{M}_d(\mathcal{O}_{L,\mathfrak{q}})$. We have to study the involution induced by $*$ on

$$\mathcal{O}_\mathfrak{p} \otimes_{\mathcal{O}_{k,\mathfrak{p}}} \Omega \simeq \mathrm{M}_d(\Omega(\epsilon)).$$

Recall that $\Omega(\epsilon) := \Omega[\epsilon]/(\epsilon^2)$ and that the involution $*$ on $\mathrm{M}_d(\Omega(\epsilon))$ satisfies ${}^*\epsilon = -\epsilon$ as established during the proof of Proposition 5. Denoting by $\sigma \in \mathrm{Aut}_{\Omega\text{-alg}}(\Omega(\epsilon))$ the element determined by $\sigma(\epsilon) = -\epsilon$ and by $+$ the involution on $\mathrm{M}_d(\Omega(\epsilon))$ defined by

$${}^+(x_{i,j}) := (\sigma(x_{j,i})),$$

the theorem of Skolem and Noether [Mil80, ch. IV, Proposition 1.4] shows that there exists a $g \in \mathrm{GL}_d(\Omega(\epsilon))$ such that

$${}^*x = g\,{}^+x g^{-1} \quad \text{for all } x \in \mathrm{M}_d(\Omega(\epsilon)). \tag{4}$$

From ${}^{**}x = x$ one sees that

$$g = \alpha^+ g \tag{5}$$

for some $\alpha \in \Omega(\epsilon)^*$. This gives ${}^+g = \sigma(\alpha)g$ and by multiplying we obtain $g^+g = \alpha\sigma(\alpha)^+gg$, which using (5) implies that $\alpha\sigma(\alpha) = 1$.

Writing $\alpha = x + y\epsilon$ with $x, y \in \Omega$ we get

$$1 = \alpha\sigma(\alpha) = x^2 - y^2\epsilon^2 = x^2$$

and hence

$$\alpha = \pm 1 + y\epsilon \quad \text{for some } y \in \Omega. \tag{6}$$

Replacing g by βg for $\beta := 1 \mp \frac{1}{2}y\epsilon \in \Omega(\epsilon)^*$ (the sign opposite to the one occurring in (6)) does not affect (4) and replaces α by

$$\begin{aligned}\alpha\beta\sigma(\beta)^{-1} &\overset{(6)}{=} (\pm 1 + y\epsilon)(1 \mp \tfrac{1}{2}y\epsilon)(1 \pm \tfrac{1}{2}y\epsilon)^{-1} = (\pm 1 + y\epsilon)(1 \mp \tfrac{1}{2}y\epsilon)^2 \\ &= (\pm 1 + y\epsilon)(1 \mp y\epsilon) = \pm 1.\end{aligned}$$

Hence we can assume that

$$\alpha = \pm 1. \tag{7}$$

To further simplify the involution, note that, for every $h \in \mathrm{GL}_d(\Omega(\epsilon))$, $(\mathrm{M}_d(\Omega(\epsilon)), *)$ is isomorphic, via conjugation with h, to $(\mathrm{M}_d(\Omega(\epsilon)), \tau)$ with

$${}^\tau x = h^*(h^{-1}xh)h^{-1} = hg^+(h^{-1}xh)g^{-1}h^{-1} = hg^+h^+x(hg^+h)^{-1},$$

i.e. we have the following.

$$\text{For every } h \in \mathrm{GL}_d(\Omega(\epsilon)) \text{ we can replace } g \text{ in (4) by } hg\,{}^+h. \tag{8}$$

We now distinguish two cases according to (7).

(3′.1) Assume that $\alpha = 1$. Writing $g = A + B\epsilon$ with $A \in \mathrm{GL}_d(\Omega), B \in \mathrm{M}_d(\Omega)$ we have

$$A + B\epsilon = g \overset{((5),\alpha=1)}{=} {}^+g = {}^{\mathrm{t}}A - {}^{\mathrm{t}}B\epsilon,$$

hence $A = {}^{\mathrm{t}}A, B = -{}^{\mathrm{t}}B$ and there exists some $S \in \mathrm{GL}_d(\Omega)$ with $A = S\,{}^{\mathrm{t}}S$. Using (8) with $h = S^{-1}$ we can replace g by

$$hg^+h = S^{-1}(A + B\epsilon)\,{}^{\mathrm{t}}S^{-1} = 1 + S^{-1}B\,{}^{\mathrm{t}}S^{-1}\epsilon.$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

Put $T := S^{-1}B\,{}^{\mathrm{t}}S^{-1}$ and note that $B = -\,{}^{\mathrm{t}}B$ implies that ${}^{\mathrm{t}}T = -T$. Using (8) again with $h = 1 - \frac{1}{2}T\epsilon$ replaces g by

$$hg^{+}h = (1 - \tfrac{1}{2}T\epsilon)(1 + T\epsilon)(1 + \tfrac{1}{2}\,{}^{\mathrm{t}}T\epsilon) = 1,$$

i.e. we can assume that ${}^{*}x = {}^{+}x$ for all $x \in \mathrm{M}_d(\Omega(\epsilon))$. For every Ω-algebra R we thus obtain

$$\begin{aligned}\mathrm{U}_\Omega(R) \simeq \{x = X + Y\epsilon \in \mathrm{M}_d(R(\epsilon)) \mid 1 = {}^{+}xx = ({}^{\mathrm{t}}X - {}^{\mathrm{t}}Y\epsilon)(X + Y\epsilon)\\ = {}^{\mathrm{t}}XX + (-\,{}^{\mathrm{t}}YX + {}^{\mathrm{t}}XY)\epsilon\}\end{aligned}$$

and hence an exact sequence

$$\begin{aligned}1 \longrightarrow F(R) := \{1 + Y\epsilon \in \mathrm{M}_d(\Omega(\epsilon)) \mid Y = {}^{\mathrm{t}}Y\} \longrightarrow \mathrm{U}_\Omega(R) &\longrightarrow \mathrm{O}_d(R) \longrightarrow 1,\\ X + Y &\longmapsto X,\end{aligned}$$

O_d denoting the orthogonal group, which is split by $X \mapsto X + 0 \cdot \epsilon$. Evidently, $F \simeq \mathbb{G}_{a,\Omega}^{\frac{1}{2}d(d+1)}$. We have the following diagram with exact rows and columns.

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & F' & \longrightarrow & \mathrm{SU}_\Omega & \xrightarrow{\alpha} & \mathrm{SO}_{d,\Omega} & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & F & \xrightarrow{\iota} & \mathrm{U}_\Omega & \longrightarrow & \mathrm{O}_{d,\Omega} & \longrightarrow & 1\\
 & & \downarrow{\scriptstyle \mathrm{tr}} & & \downarrow{\scriptstyle \mathrm{N}_\Omega} & & \downarrow{\scriptstyle \det} & & \\
1 & \longrightarrow & \mathbb{G}_{a,\Omega} & \longrightarrow & \mathrm{T}_\Omega & \xrightarrow{\pi} & \mu_{2,\Omega} & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array} \tag{9}$$

This is obtained as follows. The lower row is taken from Proposition 5. The reduced norm induces the determinant on $\mathrm{M}_d(\Omega(\epsilon))$. This shows that $\pi\mathrm{N}_\Omega\iota$ is trivial and $\mathrm{N}_\Omega\iota$ factors through some $F \longrightarrow \mathbb{G}_a$. As $\det(1 + Y\epsilon) = 1 + \mathrm{tr}(Y)\epsilon$, the map $F \longrightarrow \mathbb{G}_a$ is in fact the trace and $F' := \ker(\mathrm{tr})$. This also shows that the map $\mathrm{O}_{d,\Omega} \longrightarrow \mu_2$ induced by N_Ω is the determinant which is visibly fppf-surjective; in fact, it is surjective as a morphism of pre-sheaves as is the trace tr. It is also clear that $F' \simeq \mathbb{G}_a^{\frac{1}{2}d(d+1)-1}$. Now the fppf-surjectivity of α and N_Ω follows from a 5-lemma argument (which does not use commutativity). In particular, SU_Ω is connected and smooth.

(3′.2) Assume that $\alpha = -1$. Writing $g = A + B\epsilon$ with $A \in \mathrm{GL}_d(\Omega), B \in \mathrm{M}_d(\Omega)$ we have

$$A + B\epsilon = g \overset{((5),\alpha=-1)}{=} -\,{}^{+}g = -\,{}^{\mathrm{t}}A + {}^{\mathrm{t}}B\epsilon,$$

i.e. $A = -\,{}^{\mathrm{t}}A$ and $B = {}^{\mathrm{t}}B$. The conditions on A force d to be even, say $d = 2m$. Let

$$J := \begin{pmatrix} 0 & 1_m \\ -1_m & 0 \end{pmatrix} \in \mathrm{GL}_d(\Omega)$$

be the standard alternating matrix. Then there exists an $S \in \mathrm{GL}_d(\Omega)$ such that $SA\,{}^{\mathrm{t}}S = J$. Using (8) with $h = S$ we can replace g by

$$hg\,{}^{+}h = S(A + B\epsilon)\,{}^{\mathrm{t}}S = J + SB\,{}^{\mathrm{t}}S\epsilon.$$

Put $T := SB\,{}^{\mathrm{t}}S$ and note that $B = {}^{\mathrm{t}}B$ implies that $T = {}^{\mathrm{t}}T$. Using (8) again with $h = 1 + \frac{1}{2}TJ\epsilon$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

replaces g by

$$hg^+h = (1+\tfrac{1}{2}TJ\epsilon)(J+T\epsilon)(1-\tfrac{1}{2}{}^{\mathrm{t}}J\,{}^{\mathrm{t}}T\epsilon) = J + (\tfrac{1}{2}TJ^2 + T - \tfrac{1}{2}J\,{}^{\mathrm{t}}J\,{}^{\mathrm{t}}T)\epsilon$$
$$= J + (\tfrac{1}{2}T(-1) + T - \tfrac{1}{2}{}^{\mathrm{t}}T) \overset{({}^{\mathrm{t}}T=T)}{=} J,$$

i.e. we can assume that $g = J$.

For every Ω-algebra R we thus obtain, using ${}^{\mathrm{t}}J = J^{-1}$,

$$\mathrm{U}_\Omega(R) \simeq \{x = X + Y\epsilon \in \mathrm{M}_d(\Omega(\epsilon)) \mid 1 = {}^*xx = J^+(X+Y\epsilon)\,{}^{\mathrm{t}}J(X+Y\epsilon)$$
$$= J({}^{\mathrm{t}}X - {}^{\mathrm{t}}Y\epsilon)\,{}^{\mathrm{t}}J(X+Y\epsilon) = J\,{}^{\mathrm{t}}X\,{}^{\mathrm{t}}JX + (-J\,{}^{\mathrm{t}}Y{}^{\mathrm{t}}JX + J\,{}^{\mathrm{t}}X\,{}^{\mathrm{t}}JY)\epsilon\}.$$

Note that $1 = J\,{}^{\mathrm{t}}X\,{}^{\mathrm{t}}JX$ if and only if ${}^{\mathrm{t}}XJX = J$, and hence we get an exact sequence

$$1 \longrightarrow F(R) := \{1 + Y\epsilon \in \mathrm{M}_d(\Omega(\epsilon)) \mid Y = J{}^{\mathrm{t}}Y\,{}^{\mathrm{t}}J\} \longrightarrow \mathrm{U}_\Omega(R) \longrightarrow \mathrm{Sp}_{2m}(R) \longrightarrow 1,$$
$$X + Y\epsilon \longmapsto X,$$

where Sp_{2m} denotes the symplectic group, which is split by $X \mapsto X + 0\epsilon$. Writing

$$Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \mathrm{M}_m(\Omega)$ one obtains

$$F(R) \simeq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_{2m}(R) \,|\, {}^{\mathrm{t}}a = d,\ {}^{\mathrm{t}}b = -b,\ {}^{\mathrm{t}}c = -c \right\},$$

hence $F \simeq \mathbb{G}_a^{2m^2-m}$. The analog of diagram (9) in this case reads as follows.

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & F' & \longrightarrow & \mathrm{SU}_\Omega & \xrightarrow{\alpha} & \mathrm{Sp}_{2m} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & F & \longrightarrow & \mathrm{U}_\Omega & \longrightarrow & \mathrm{Sp}_{2m} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{tr}} & \nearrow & \downarrow{\scriptstyle \mathrm{N}_\Omega} & & \downarrow{\scriptstyle \det(\equiv 1)} & & \\
1 & \longrightarrow & \mathbb{G}_{a,\Omega} & \longrightarrow & \mathrm{T}_\Omega & \longrightarrow & \mu_{2,\Omega} & \longrightarrow & 1 \\
 & & \downarrow & & & & & & \\
 & & 1 & & & & & &
\end{array} \tag{10}$$

Note that, since the determinant of every symplectic matrix equals 1, N_Ω factors as indicated in diagram (10). In particular, $\mathrm{N}_\Omega : \mathrm{U}_\Omega \longrightarrow \mathrm{T}_\Omega$ is not an fppf-epimorphism but has image the connected component $\mathbb{G}_{a,\Omega} \simeq \mathrm{T}_\Omega^0 \subseteq \mathrm{T}_\Omega$. Since $F' \simeq \mathbb{G}_a^{2m^2-m-1}$ we conclude that SU_Ω is connected and smooth.

We now establish the exactness of the sequence

$$1 \longrightarrow \mathrm{SU}_\mathcal{U} \longrightarrow \mathrm{U}_\mathcal{U} \xrightarrow{\mathrm{N}_\mathcal{U}} \mathrm{T}'_\mathcal{U} \longrightarrow 1$$

over $\mathcal{U}$. Since $\mathrm{T}' \subseteq \mathrm{T}$ is an open subscheme, the fact that $\mathrm{N}_\mathcal{U}$ factors through $\mathrm{T}'_\mathcal{U}$ can be checked on fibers where it follows from what has been shown above: since the determinant is trivial on Sp_{2m} in diagram (10), N_Ω factors through $\mathbb{G}_{a,\Omega} = \mathrm{T}'_\Omega \subseteq \mathrm{T}_\Omega$. We now need to see that the resulting morphism $\mathrm{N}_\mathcal{U} : \mathrm{U}_\mathcal{U} \longrightarrow \mathrm{T}'_\mathcal{U}$ is an fppf-epimorphism and we will show that it is in fact faithfully flat. By Proposition 3, it is enough to see that $\mathrm{U}_\Omega \longrightarrow \mathrm{T}'_\Omega$ is an fppf-epimorphism for every geometric point

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

$\mathrm{Spec}(\Omega) \longrightarrow \mathcal{U}$ which follows again from what has been proved above. The flatness of $\mathrm{U}_{\mathcal{U}} \longrightarrow \mathrm{T}'_{\mathcal{U}}$ implies that $\mathrm{SU}/\mathcal{U}$ is flat, hence smooth by the fiber-wise criterion.

The proof of Theorem 7 is now complete. □

3. Approximation of local units

In this section we study the problem of p-adically approximating local units of a maximal order (with involution) by global (unitary) units of bounded denominators. Using the results of §§ 2.1 and 2.2.1 (2.2.2) this problem will be reduced in § 3.1 (3.2) to an approximation problem for tori which will be solved in § 4.1 (solved in a special case in § 4.2).

3.1 Type A_{d-1}

In this section we consider the problem of p-adically approximating local units of a maximal order $\mathcal{O} \subseteq D$ where D is a finite-dimensional skew field over $\mathbb{Q}$. We denote by k the center of D and by d its reduced dimension. We fix a prime $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ at which we wish to approximate. There is a unique prime $\mathfrak{P} \subseteq \mathcal{O}$ lying above $\mathfrak{p}$ (see [Deu68, VI, § 12, Satz 1]) and we denote by $\mathcal{O}_{\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of $\mathcal{O}$; cf. [Deu68, Kapitel VI, § 11].

To describe the denominators that we allow the approximating global units to have, we fix a finite set of places S of k such that

$$\mathfrak{p} \notin \mathrm{S} \text{ and there exists a place } v_0 \in \mathrm{S} \text{ such that } D_{v_0} \text{ is not a skew field.}$$

We write $\mathrm{S}^{\mathrm{fin}}$ for the set of finite places contained in S and consider the ring $\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}$ of $\mathrm{S}^{\mathrm{fin}}$-integers

$$\mathcal{O}_k \subseteq \mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}} := \{x \in k \mid v(x) \geqslant 0 \text{ for all finite } v \notin \mathrm{S}\} \subseteq k.$$

Since $\mathfrak{p} \notin \mathrm{S}$ we have $\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}} \subseteq \mathcal{O}_{k,\mathfrak{p}}$. We define

$$X = \{x \in \mathcal{O}^*_{k,\mathrm{S}^{\mathrm{fin}}} \mid v(x) > 0 \text{ for all archimedean } v \text{ with } \mathrm{inv}_v(D) = \tfrac{1}{2}\} \subseteq \mathcal{O}^*_{k,\mathfrak{p}}. \tag{11}$$

Note that we have

$$(\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}})^* \subseteq \mathcal{O}^*_{\mathfrak{P}}.$$

Recall that N denotes the reduced norm of D.

Theorem 9. *The closure of* $(\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}})^*$ *inside* $\mathcal{O}^*_{\mathfrak{P}}$ *equals*

$$\{x \in \mathcal{O}^*_{\mathfrak{P}} \mid \mathrm{N}_{\mathfrak{p}}(x) \in \mathcal{O}^*_{k,\mathfrak{p}} \text{ lies in the closure of } X\}.$$

Example 10. (1) For $k = \mathbb{Q}$ and D a definite quaternion algebra, i.e. $d = 2$ and $\mathrm{inv}_v(D) = \frac{1}{2}$ for the unique infinite place v of $\mathbb{Q}$, we can choose $\mathrm{S} = \{l\}$ for any prime $l \neq p$ at which D splits, i.e. $\mathrm{inv}_l(D) = 0$. Then $\mathcal{O}^*_{k,\mathrm{S}^{\mathrm{fin}}} = \{\pm 1\} \times l^{\mathbb{Z}}$ and $X = l^{\mathbb{Z}} \subseteq \mathcal{O}^*_{k,\mathfrak{p}} = \mathbb{Z}_p^*$. For $p \neq 2$ we can choose l as above such that in addition $X \subseteq \mathbb{Z}_p^*$ is dense and conclude that in this case $\mathcal{O}[1/l]^* \subseteq \mathcal{O}^*_{\mathfrak{P}}$ is dense. For $p = 2$ we can choose l such that the closure of X in $\mathbb{Z}_2^*$ equals $1 + 4\mathbb{Z}_2$ and conclude that the closure of $\mathcal{O}[1/l]^*$ inside $\mathcal{O}^*_{\mathfrak{P}}$ equals

$$\ker(\mathcal{O}^*_{\mathfrak{P}} \xrightarrow{\mathrm{N}} \mathbb{Z}_2^* \longrightarrow \mathbb{Z}_2^*/(1 + 4\mathbb{Z}_2) \simeq \{\pm 1\}),$$

cf. Remark 24. In the special case in which D is the endomorphism algebra of a super-singular elliptic curve in characteristic p, i.e. $\mathrm{inv}_v(D) = 0$ for all $v \neq p, \infty$, this result has been established by different means in [BL06, Theorem 0.1].

(2) See Theorem 17 in § 4.1 for a further discussion of the closure of $X \subseteq \mathcal{O}^*_{k,\mathfrak{p}}$.

The rest of this section is devoted to the proof of Theorem 9.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

Remember the groups G and $G'/\mathrm{Spec}(\mathcal{O}_k)$ defined by $G(R) = (\mathcal{O} \otimes_{\mathcal{O}_k} R)^*$ and $G'(R) = \{g \in G(R) \,|\, \mathrm{N}(g) = 1\}$.

PROPOSITION 11. *The subgroup $G'(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) \subseteq G'(\mathcal{O}_{k,\mathfrak{p}})$ is dense.*

Proof. First note that $G'/\mathrm{Spec}(\mathcal{O}_k)$ is representable by an affine group scheme; hence the injectivity of the homomorphism $G'(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) \longrightarrow G'(\mathcal{O}_{k,\mathfrak{p}})$ follows from the injectivity of $\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}} \hookrightarrow \mathcal{O}_{k,\mathfrak{p}}$. Secondly, $G'(\mathcal{O}_{k,\mathfrak{p}})$ is canonically a topological group [Wei82, ch. I] and we claim density with respect to this topology. We know that $G'_k := G' \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(k) = \mathrm{SL}_1(D)$ [PR94, § 2.3] is an inner form of $\mathrm{SL}_{d,k}$ and thus is k-simple, semi-simple and simply connected. Furthermore, $G'_k \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k_{v_0}) = \mathrm{SL}_n(\tilde{D})$ for some central skew field $\tilde{D}$ over k_{v_0} and some $n \geqslant 1$. Since D_{v_0} is not a skew field by assumption, we have $n \geqslant 2$ and $\mathrm{rk}_{k_{v_0}}(G'_k \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k_{v_0})) = n - 1 \geqslant 1$ (see [PR94, Proposition 2.12]), i.e. G'_k is isotropic at v_0. From strong approximation [Spr94, Theorem 5.1.8] we conclude that

$$G'(k) \cdot G'(k_{v_0}) \subseteq G'(\mathbb{A}_k) \text{ is dense,} \tag{12}$$

where $\mathbb{A}_k$ denotes the adèle ring of k. Fix $x \in G'(\mathcal{O}_{k,\mathfrak{p}})$ and an open subgroup $U_{\mathfrak{p}} \subseteq G'(\mathcal{O}_{k,\mathfrak{p}})$. Denote by $\tilde{x} \in G'(\mathbb{A}_k)$ the adèle having $\mathfrak{p}$-component x and all other components equal to 1. Then

$$U := U_{\mathfrak{p}} \times \prod_{v \neq \mathfrak{p} \text{ finite}} G'(\mathcal{O}_{k,v}) \times \prod_{v \text{ infinite}} G'(k_v) \subseteq G'(\mathbb{A}_k)$$

is an open subgroup and by (12) there exist $\gamma \in G'(k)$ and $\delta \in G'(k_{v_0})$ such that $\gamma\delta \in \tilde{x}U$. Since $\mathfrak{p} \neq v_0$ this implies that $\gamma_{\mathfrak{p}} \in \tilde{x}_{\mathfrak{p}} U_{\mathfrak{p}} = xU_{\mathfrak{p}}$, where $\gamma_{\mathfrak{p}}$ is the $\mathfrak{p}$-component of the principal adèle γ, equivalently, the image of γ under the inclusion $G'(k) \subseteq G'(k_{\mathfrak{p}})$. Since x and $U_{\mathfrak{p}}$ are arbitrary, we will be done if we can show that $\gamma \in G'(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) \subseteq G'(k)$, i.e. that for every finite place $v \notin \mathrm{S}$ we have $\gamma_v \in G'(\mathcal{O}_{k,v})$. For $v = \mathfrak{p}$ this is clear since $xU_{\mathfrak{p}} \subseteq G'(\mathcal{O}_{k,\mathfrak{p}})$ whereas for $v \neq \mathfrak{p}$ we have, using that $\delta_v = 1$ since $v \neq v_0 \in \mathrm{S}$,

$$(\gamma\delta)_v = \gamma_v \in (\tilde{x}U)_v = \tilde{x}_v \cdot G'(\mathcal{O}_{k,v}) = G'(\mathcal{O}_{k,v}). \qquad \square$$

To proceed, we apply (3) to the inclusion $\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}} \hookrightarrow \mathcal{O}_{k,\mathfrak{p}}$ to obtain the following commutative diagram.

$$\begin{array}{ccccccc} 1 & \longrightarrow & G'(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) & \longrightarrow & G(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) & \xrightarrow{\mathrm{N}} & \mathcal{O}^*_{k,\mathrm{S}^{\mathrm{fin}}} \\ & & \downarrow & & \downarrow \iota & & \downarrow \\ 1 & \longrightarrow & G'(\mathcal{O}_{k,\mathfrak{p}}) & \longrightarrow & G(\mathcal{O}_{k,\mathfrak{p}}) & \xrightarrow{\mathrm{N}_{\mathfrak{p}}} & \mathcal{O}^*_{k,\mathfrak{p}} \end{array} \tag{13}$$

By definition, $G(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) = (\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}})^*$ and $G(\mathcal{O}_{k,\mathfrak{p}}) = (\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathfrak{p}})^* = \mathcal{O}^*_{\mathfrak{P}}$ (see [Deu68, Kapitel VI, § 11, Satz 6]), so Theorem 9 is concerned with the closure of the image of ι. Recall the subgroup $X \subseteq \mathcal{O}^*_{k,\mathrm{S}^{\mathrm{fin}}}$ from (11).

PROPOSITION 12. *In diagram (13) we have* $\mathrm{im}(\mathrm{N}) = X \subseteq \mathcal{O}^*_{k,\mathrm{S}^{\mathrm{fin}}}$.

Proof. Eichler's norm theorem [PR94, Theorem 1.13] states that

$$\mathrm{im}(\mathrm{N}_k : G(k) \longrightarrow k^*) = \{\alpha \in k^* \mid v(x) > 0 \text{ for all archimedean } v \text{ with } \mathrm{inv}_v(D) = \tfrac{1}{2}\}, \tag{14}$$

and the inclusion $\mathrm{im}(\mathrm{N}) \subseteq X$ is trivial by the definition of X.

From the cohomology sequence associated with (3) we have the following diagram.

$$\begin{array}{ccccc} G(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) & \xrightarrow{\mathrm{N}} & \mathcal{O}^*_{k,\mathrm{S}^{\mathrm{fin}}} & \longrightarrow & \mathrm{H}^1(\mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}), G') \\ \downarrow & & \downarrow & & \downarrow \iota \\ G(k) & \longrightarrow & k^* & \longrightarrow & \mathrm{H}^1(\mathrm{Spec}(k), G') \end{array}$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

Now, $G'/\mathrm{Spec}(\mathcal{O}_k)$ is smooth with connected fibers by Theorem 2, and the generic fiber G'_k is an inner form of SL_d and is thus k-simple, semi-simple and simply connected. Finally, the place v_0 is outside $U := \mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}})$ and, since D_{v_0} is not a skew field, G'_k is isotropic at v_0 (see [PR94, Proposition 2.12]). We can thus apply Proposition 1 to G'/U to conclude that ι has trivial kernel. This, jointly with (14), implies that $X \subseteq \mathrm{im}(\mathrm{N})$. □

We know that $\mathrm{H}^1(\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}}), G') = 0$ from the fact that $G' \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})/\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$ is smooth with connected fibers and Lang's theorem. Hence, in (13), $N_{\mathfrak{p}}$ is surjective and we can, using Proposition 12, rewrite (13) as follows.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G'(\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}}) & \longrightarrow & (\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}})^* & \xrightarrow{\mathrm{N}} & X & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \iota} & & \downarrow & & \\ 1 & \longrightarrow & G'(\mathcal{O}_{k,\mathfrak{p}}) & \longrightarrow & \mathcal{O}^*_{\mathfrak{P}} & \xrightarrow{\mathrm{N}_{\mathfrak{p}}} & \mathcal{O}^*_{k,\mathfrak{p}} & \longrightarrow & 1 \end{array} \tag{15}$$

Since the image of α is dense by Proposition 11 and $\mathcal{O}^*_{\mathfrak{P}}$ is compact, all that remains to be done to conclude the proof of Theorem 9 is to apply Proposition 13 below to (15).

For a subset Y of a topological space X we denote by $\overline{Y}^X$ the closure of Y in X.

Proposition 13. *Let*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H' & \longrightarrow & H & \xrightarrow{\rho} & H'' & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & G' & \longrightarrow & G & \xrightarrow{\pi} & G'' & \longrightarrow & 1 \end{array}$$

be a commutative diagram of first countable topological groups with exact rows, G compact, and such that $H' \subseteq G'$ is dense. Then

$$\overline{H}^G = \pi^{-1}(\overline{H''}^{G''}).$$

Proof. Assume that $g \in \overline{H}^G$. Then $g = \lim_n h_n$ for suitable $h_n \in H$ and $\pi(g) = \lim_n \pi(h_n) \in \overline{H''}^{G''}$. Conversely, given $g \in G$ with $\pi(g) = \lim_n h''_n$ for suitable $h''_n \in H''$, choose $h_n \in H$ with $\rho(h_n) = h''_n$. The sequence $(h_n g^{-1})_n$ in G has a convergent subsequence, $\tilde{g} := \lim_i h_{n_i} g^{-1} \in G$. Then $\pi(\tilde{g}) = 1$, i.e. $\tilde{g} \in G'$ and we have $\tilde{g} = \lim_i h'_i$ for suitable $h'_i \in H'$. The sequence $((h'_i)^{-1} h_{n_i})_i$ in H satisfies $\lim_i (h'_i)^{-1} h_{n_i} = \tilde{g}^{-1}\tilde{g}g = g$, hence $g \in \overline{H}^G$. □

3.2 Type ${}^2A_{d-1}$

Let D be a finite-dimensional skew field of reduced dimension $d > 1$ over $\mathbb{Q}$ carrying a positive involution of the second kind $*$ and assume that $\mathcal{O} \subseteq D$ is a maximal order which is stable under $*$. In § 2.2.2 we associated with these data group schemes $\mathrm{SU} \subseteq \mathrm{U}$ and $\mathrm{T}' \subseteq \mathrm{T}$ over $\mathrm{Spec}(\mathcal{O}_k)$ and an open subscheme $\mathcal{U} \subseteq \mathrm{Spec}(\mathcal{O}_k)$.

To formulate our approximation problem, we fix a prime $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ at which we wish to approximate and a finite set of finite places S of k such that

$$\begin{gathered} \mathfrak{p} \notin \mathrm{S}, \mathrm{S} \text{ contains all primes of residue characteristic two ramified in } L/k \text{ and} \\ \mathrm{S} \text{ contains a place } v_0 \text{ split in } L/k \text{ such that for } w_0|v_0 \ D_{w_0} \text{ is not a skew field.} \end{gathered}$$

This implies in particular that $\mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathcal{U}$. Note that we do not really restrict generality by insisting that S consists of finite place because, unlike the case treated in § 3.1, the group SU is anisotropic at every infinite place of k.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

THEOREM 14. *The closure of* $\mathrm{U}(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathrm{U}(\mathcal{O}_{k,\mathfrak{p}})$ *equals*

$$\{g \in \mathrm{U}(\mathcal{O}_{k,\mathfrak{p}}) \mid \mathrm{N}_{\mathfrak{p}}(g) \text{ lies in the closure of } \mathrm{T}'(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathrm{T}'(\mathcal{O}_{k,\mathfrak{p}})\}.$$

See Corollary 20 for the computation of the closure of $\mathrm{T}'(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathrm{T}'(\mathcal{O}_{k,\mathfrak{p}})$ in a special case.

Note that

$$\mathrm{U}(\mathcal{O}_{k,\mathrm{S}}) = \{g \in (\mathcal{O} \otimes_{\mathcal{O}_k} \mathcal{O}_{k,\mathrm{S}})^* \mid {}^*gg = 1\}$$

by definition but the structure of $\mathrm{U}(\mathcal{O}_{k,\mathfrak{p}})$ depends on the splitting behavior of $\mathfrak{p}$ in L; cf. the proof of Theorem 7. In particular, if $\mathfrak{p}$ splits in L/k then

$$G(\mathcal{O}_{k,\mathfrak{p}}) \simeq \mathcal{O}_{D_{\mathfrak{q}}}^* \simeq \mathcal{O}_{D_{\mathfrak{q}'}}^*$$

where $\mathfrak{q}$ and $\mathfrak{q}'$ are the primes of L lying above k.

In the rest of this section we give the proof of Theorem 14.

PROPOSITION 15. *We have that* $\mathrm{SU}(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathrm{SU}(\mathcal{O}_{k,\mathfrak{p}})$ *is a dense subgroup.*

Proof. Since $\mathrm{SU}_k := \mathrm{SU} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(k)$ is an outer form of $\mathrm{SL}_{d,k}$, it is k-simple, semi-simple and simply connected. In the proof of Theorem 7 we saw that $\mathrm{SU}_{k_{v_0}} \simeq \mathrm{SL}_1(D_{w_0})$ and, since D_{w_0} is not a skew field by assumption, SU_k is isotropic at v_0. Now one proceeds as in the proof of Proposition 11. □

Recall from Theorem 7 that we have an exact sequence

$$1 \longrightarrow \mathrm{SU}_{\mathcal{U}} \longrightarrow \mathrm{U}_{\mathcal{U}} \xrightarrow{\mathrm{N}_{\mathcal{U}}} T'_{\mathcal{U}} \longrightarrow 1 \tag{16}$$

over $\mathcal{U} \supseteq \mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}})$.

PROPOSITION 16. *The diagram obtained by applying (16) to* $\mathcal{O}_{k,\mathrm{S}} \hookrightarrow \mathcal{O}_{k,\mathfrak{p}}$,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{SU}(\mathcal{O}_{k,\mathrm{S}}) & \longrightarrow & \mathrm{U}(\mathcal{O}_{k,\mathrm{S}}) & \xrightarrow{\mathrm{N}} & \mathrm{T}'(\mathcal{O}_{k,\mathrm{S}}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{SU}(\mathcal{O}_{k,\mathfrak{p}}) & \longrightarrow & \mathrm{U}(\mathcal{O}_{k,\mathfrak{p}}) & \xrightarrow{\mathrm{N}_{\mathfrak{p}}} & \mathrm{T}'(\mathcal{O}_{k,\mathfrak{p}}) & \longrightarrow & 1 \end{array} \tag{17}$$

fulfills the assumptions of Proposition 13.

This finishes the proof of Theorem 14 by applying Proposition 13 to (17).

Proof of Proposition 16. Clearly, diagram (17) is made up of first-countable groups and is commutative, $\mathrm{SU}(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathrm{SU}(\mathcal{O}_{k,\mathfrak{p}})$ is dense by Proposition 15 and $\mathrm{U}(\mathcal{O}_{k,\mathfrak{p}})$ is compact. It remains to prove the exactness of the rows, i.e. the surjectivity of N and $\mathrm{N}_{\mathfrak{p}}$. Since $\mathrm{SU}_{\mathfrak{p}}/\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}})$ is smooth with connected fibers by Theorem 7, Lang's theorem implies that $\mathrm{H}^1(\mathrm{Spec}(\mathcal{O}_{k,\mathfrak{p}}), \mathrm{SU}_{\mathfrak{p}}) = 0$ and thus $\mathrm{N}_{\mathfrak{p}}$ is surjective. We now show that $\mathrm{N}_k : \mathrm{U}(k) \longrightarrow \mathrm{T}'(k)$ is surjective: we have a commutative diagram with exact rows as follows.

$$\begin{array}{ccccc} \mathrm{U}(k) & \xrightarrow{\mathrm{N}_k} & \mathrm{T}'(k) & \longrightarrow & \mathrm{H}^1(\mathrm{Spec}(k), \mathrm{SU}) \\ \downarrow & & \downarrow & & \downarrow \simeq \\ \prod_{v \in \Sigma_k^\infty} \mathrm{U}(k_v) & \xrightarrow{\prod \mathrm{N}_v} & \prod_{v \in \Sigma_k^\infty} \mathrm{T}'(k_v) & \longrightarrow & \prod_{v \in \Sigma_k^\infty} \mathrm{H}^1(\mathrm{Spec}(k_v), \mathrm{SU}) \end{array}$$

Here, Σ_k^∞ denotes the set of infinite places of k and the right-most vertical arrow is an isomorphism by the Hasse principle for $\mathrm{SU} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}(k)$ (see [PR94, Theorem 6.6]). Hence the surjectivity

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

of N_k will follow from the surjectivity of N_v for all $v \in \Sigma_k^\infty$, which is easy to see: for $v \in \Sigma_k^\infty$ we have, using [Mum70, Step IV on page 199],

$$\begin{array}{ccc} \mathrm{U}(k_v) & \xrightarrow{\mathrm{N}_v} & \mathrm{T}'(k_v) = \mathrm{T}(k_v) \\ \downarrow \simeq & & \downarrow \simeq \\ \{(x_{i,j}) \in \mathrm{GL}_d(\mathbb{C}) \mid (\overline{x_{i,j}})(x_{j,i}) = 1\} & \xrightarrow{\det} & \{\alpha \in \mathbb{C}^* \mid \alpha\overline{\alpha} = 1\} \end{array}$$

where a bar denotes complex conjugation, and the lower horizontal arrow is surjective since it is split by $\alpha \mapsto \mathrm{diag}(\alpha, 1, \ldots, 1)$. Next we look at the commutative diagram with exact rows.

$$\begin{array}{ccccc} \mathrm{U}(\mathcal{O}_{k,\mathrm{S}}) & \xrightarrow{\mathrm{N}} & \mathrm{T}'(\mathcal{O}_{k,\mathrm{S}}) & \longrightarrow & \mathrm{H}^1(\mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}}), \mathrm{SU}) \\ \downarrow & & \downarrow & & \downarrow \iota \\ \mathrm{U}(k) & \xrightarrow{\mathrm{N}_k} & \mathrm{T}'(k) & \longrightarrow & \mathrm{H}^1(\mathrm{Spec}(k), \mathrm{SU}) \end{array}$$

We need to see that ι has trivial kernel for then the desired surjectivity of N will follow from the already proved surjectivity of N_k. Since $\mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}}) \subseteq \mathcal{U}$ we know that $\mathrm{SU}/\mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}})$ is smooth with connected fibers from Theorem 7, SU_k is k-simple, semi-simple and simply connected and the place v_0 lies outside $\mathrm{Spec}(\mathcal{O}_{k,\mathrm{S}})$ and SU_k is isotropic at v_0 as explained in the proof of Proposition 15. Hence the kernel of ι is indeed trivial by Proposition 1. □

4. The commutative case

4.1 Type A_{d-1}

In § 3.1 the problem of approximating a local unit in a maximal order of a finite-dimensional skew field over $\mathbb{Q}$ was reduced to the following problem involving solely number fields. Let k be a number field, $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ a prime dividing the rational prime p and Σ a possibly empty set of real places of k. For a finite set of finite places S of k not containing $\mathfrak{p}$ we consider

$$X_{\mathrm{S}} := \{x \in \mathcal{O}_{k,\mathrm{S}}^* \mid v(x) > 0 \text{ for all } v \in \Sigma\} \subseteq \mathcal{O}_{k,\mathrm{S}}^*$$

and wish to understand when $X_{\mathrm{S}} \subseteq \mathcal{O}_{k,\mathfrak{p}}^* =: U_{\mathfrak{p}}$ is a dense subgroup. The principal units

$$U_{\mathfrak{p}}^{(1)} := 1 + \mathfrak{p}\mathcal{O}_{k,\mathfrak{p}} \subseteq U_{\mathfrak{p}}$$

are canonically a finitely generated $\mathbb{Z}_p$-module and $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$ is a finite abelian group.

It follows from Nakayama's lemma that a subgroup $Y \subseteq U_{\mathfrak{p}}$ is dense if and only if the composition $Y \hookrightarrow U_{\mathfrak{p}} \longrightarrow U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$ is surjective: since $U_{\mathfrak{p}}$ is pro-finite, $Y \subseteq U_{\mathfrak{p}}$ is dense if and only if it surjects onto every finite quotient of $U_{\mathfrak{p}}$. Assume that Y does surject onto $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$ and $V \subseteq U_{\mathfrak{p}}$ is arbitrary of finite index. In order to see that Y surjects onto $U_{\mathfrak{p}}/V$ we can assume that $V \subseteq U_{\mathfrak{p}}^{(1)^p}$. Then the image of Y in $U_{\mathfrak{p}}/V = \mu_{q-1} \times U_{\mathfrak{p}}^{(1)}/V$ surjects onto μ_{q-1} and $U_{\mathfrak{p}}^{(1)}/V$ is a finitely generated $\mathbb{Z}_p$-module which modulo p is generated by the image of Y. By Nakayama's lemma, Y surjects onto $U_{\mathfrak{p}}/V$.

For an infinite place v of k we write $k_v^{*,+}$ for the connected component of 1 inside k_v^*, i.e. $k_v^{*,+} \simeq \mathbb{R}^+$ (respectively $k_v^{*,+} \simeq \mathbb{C}^*$) if v is real (respectively complex).

We denote by

$$E^+ := \ker\left(\mathcal{O}_k^* \overset{\mathrm{diag}}{\hookrightarrow} \bigoplus_{v\in\Sigma} k_v^* \longrightarrow \bigoplus_{v\in\Sigma} k_v^*/k_v^{*,+}\right)$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

the group of global units of k which are positive at all places in Σ. We write

$$\psi : E^+ \subseteq \mathcal{O}_k^* \hookrightarrow U_\mathfrak{p}$$

for the inclusion. Then $U_\mathfrak{p}/\psi(E^+)U_\mathfrak{p}^{(1)^p}$ is a finite abelian group the minimal number of generators of which we denote by $g(\mathfrak{p}, \Sigma)$.

THEOREM 17. *In the above situation the following hold.*

(i) *If $X_\mathrm{S} \subseteq U_\mathfrak{p}$ is dense then $|\mathrm{S}| \geqslant g(\mathfrak{p}, \Sigma)$.*

(ii) *Given a set T of places of k of density 1, there exists S as above such that $X_\mathrm{S} \subseteq U_\mathfrak{p}$ is dense, $|\mathrm{S}| = g(\mathfrak{p}, \Sigma)$ and $\mathrm{S} \subseteq \mathrm{T}$.*

(iii) *We have*

$$g(\mathfrak{p}, \Sigma) \leqslant \begin{cases} [k_\mathfrak{p} : \mathbb{Q}_p], & \text{if } \mu_{p^\infty}(k_\mathfrak{p}) = \{1\}, \\ 1 + [k_\mathfrak{p} : \mathbb{Q}_p], & \text{if } \mu_{p^\infty}(k_\mathfrak{p}) \neq \{1\}. \end{cases}$$

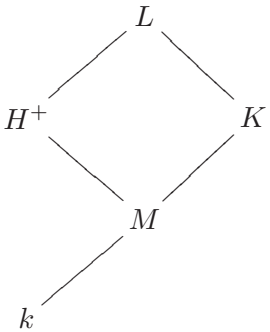
Remark 18. (1) In general, the inequalities in (iii) are strict: for $k = \mathbb{Q}(\sqrt{2})$, $\mathfrak{p}$ dividing 7 and $\Sigma = \emptyset$ one can check that $g(\mathfrak{p}, \Sigma) = 0$, i.e. $\mathcal{O}_k^* \subseteq U_\mathfrak{p}$ is dense.

(2) The proof of Theorem 17(ii) is rather constructive: one has to find principal prime ideals (λ) of $\mathcal{O}_k$ with λ positive at all places in Σ (this corresponds to being trivial in $\mathrm{Gal}(M/k)$ in the notation of the proof) and determine the image of λ in $U_\mathfrak{p}/\psi(E^+)U_\mathfrak{p}^{(1)^p}$.

Proof of Theorem 17. We consider the following subgroups of I_k, the idèles of k:

$$\begin{aligned} U_K &:= \prod_{v\nmid\infty, v\neq\mathfrak{p}} U_v \times U_\mathfrak{p}^{(1)^p} \times \prod_{v\in\Sigma} k_v^{*,+} \times \prod_{v\mid\infty, v\notin\Sigma} k_v^*, \\ U_M &:= \prod_{v\nmid\infty} U_v \times \prod_{v\in\Sigma} k_v^{*,+} \times \prod_{v\mid\infty, v\notin\Sigma} k_v^*, \\ U_+ &:= \prod_{v\nmid\infty} U_v \times \prod_{v\mid\infty} k_v^{*,+}. \end{aligned}$$

Then $U_K \subseteq U_M$ and $k^*U_K \subseteq I_k$ is of finite index. Class field theory, e.g. [Neu99, ch. VI], yields finite abelian extensions $k \subseteq M \subseteq K$ and the upper part of diagram (18) below. The field corresponding to k^*U_+ is the big Hilbert class field of k which we denote by H^+. Since $k^*U_K \cdot k^*U_+ = k^*U_M$ we have $H^+ \cap K = M$ and we put $L := H^+K$. We have the following diagram of fields.



https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

Some of the occurring Galois groups are identified as follows.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K/M) & \xrightarrow{\iota} & \mathrm{Gal}(K/k) & \xrightarrow{\pi} & \mathrm{Gal}(M/k) & \longrightarrow & 1 \\ & & \beta\uparrow\simeq & & \uparrow\simeq & & \uparrow\simeq & & \\ 1 & \longrightarrow & k^*U_M/k^*U_K & \longrightarrow & I_k/k^*U_K & \longrightarrow & I_k/k^*U_M & \longrightarrow & 1 \\ & & \alpha\uparrow\simeq & & & & & & \\ & & U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p} & & & & & & \end{array} \tag{18}$$

The isomorphism α is induced by the inclusion $U_{\mathfrak{p}} \hookrightarrow k^*U_M$: one has $k^*U_M = k^*U_{\mathfrak{p}}U_K$, hence

$$k^*U_M/k^*U_K = k^*U_{\mathfrak{p}}U_K/k^*U_K \xleftarrow{\simeq} U_{\mathfrak{p}}/(U_{\mathfrak{p}} \cap k^*U_K)$$

and $U_{\mathfrak{p}} \cap k^*U_K = k^*U_{\mathfrak{p}} \cap U_K = \psi(E^+)U_{\mathfrak{p}}^{(1)^p}$.

To prove part (i), assume that $X_{\mathrm{S}} \subseteq U_{\mathfrak{p}}$ is dense. Then $X_{\mathrm{S}} \subseteq U_{\mathfrak{p}} \longrightarrow U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$ is surjective, hence so is $X_{\mathrm{S}}/E^+ \longrightarrow U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$. The group X_{S}/E^+ is easily seen to be torsion-free and Dirichlet's unit theorem determines its rank, hence $X_{\mathrm{S}}/E^+ \simeq \mathbb{Z}^{|\mathrm{S}|}$ and $|\mathrm{S}| \geqslant g(\mathfrak{p}, \Sigma)$.

To prove part (ii), fix generators $x_i \in U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$ $(1 \leqslant i \leqslant g(\mathfrak{p}, \Sigma))$. Let $\sigma_i \in \mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/k)$ be the unique element such that $\sigma_i|_{H^+} = \mathrm{id}$ and $\sigma_i|_K = (\iota\beta\alpha)(x_i)$. Note that $(\iota\beta\alpha)(x_i)|_M = (\pi\iota\beta\alpha)(x_i) = \mathrm{id}$ by (18). By Chebotarev's density theorem [Neu99, ch. VII, Theorem 13.4], there is a finite place $v_i \in \mathrm{T}$, unramified in L/k such that $\sigma_i = \mathrm{Frob}_{v_i}^{-1}$, where Frob_{v_i} denotes the Frobenius at the place v_i, in $\mathrm{Gal}(L/k)$. Then $(\iota\beta\alpha)(x_i) = \mathrm{Frob}_{v_i}^{-1}$ in $\mathrm{Gal}(K/k)$. Since $\mathrm{Frob}_{v_i}|_{H^+} = \sigma_i^{-1}|_{H^+} = \mathrm{id}$, the prime ideal $\mathfrak{p}_i \subseteq \mathcal{O}_k$ corresponding to v_i is principal, generated by a totally positive element $\pi_i \in \mathcal{O}_k$ (see [Neu99, ch. VI, Theorem 7.3]). We claim that the image of π_i in $U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$ equals x_i. To see this, we apply the Artin map $(-, K/k) : I_k \longrightarrow \mathrm{Gal}(K/k)$ to the identity $\pi_i = \pi_{i,\mathfrak{p}} \cdot (\pi_i/\pi_{i,\mathfrak{p}})$ in I_k, where $\pi_{i,\mathfrak{p}}$ denotes the idèle having π_i as its $\mathfrak{p}$-component and all other components equal to 1. By Artin reciprocity we obtain $1 = (\pi_{i,\mathfrak{p}}, K/k)(\pi_i/\pi_{i,\mathfrak{p}}, K/k)$. Denoting $y := \pi_i/\pi_{i,\mathfrak{p}}$ we have $(y, K/k) = \prod_v (y_v, K_v/k_v)$ (see [Neu99, ch. VI, Theorem 5.6]) and evaluate the local terms $(y_v, K_v/k_v)$ as follows.

For $v = \mathfrak{p}$ we obtain 1 since $y_{\mathfrak{p}} = 1$; for $v \neq \mathfrak{p}, v_i$ finite, we obtain 1 since $y_v \in \mathcal{O}_{k,v}^*$ and v is unramified in K/k; for $v = v_i$ we obtain Frob_{v_i} since K/k is unramified at v_i and $y_{v_i} \in \mathcal{O}_{k,v_i}$ is a local uniformizer; finally, for $v|\infty$ we obtain 1 since $y_v > 0$ because π_i is totally positive.

Hence $(\pi_{i,\mathfrak{p}}, K/k) = \mathrm{Frob}_{v_i}^{-1} = (\iota\beta\alpha)(x_i)$ in $\mathrm{Gal}(K/k)$. Denoting by $\tau : U_{\mathfrak{p}} \longrightarrow U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$ the projection we have $(\pi_{i,\mathfrak{p}}, K/k) = (\iota\beta\alpha\tau)(\pi_{i,\mathfrak{p}})$ by construction, hence $x_i = \tau(\pi_{i,\mathfrak{p}})$ by the injectivity of $\iota\beta\alpha$. This establishes the above claim saying that the global elements $\pi_i \in \mathcal{O}_k$ have the prescribed image x_i in $U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$. To conclude the proof of (ii), put $\mathrm{S} := \{v_i \mid 1 \leqslant i \leqslant g(\mathfrak{p}, \Sigma)\}$ and note that $\pi_i \in X_{\mathrm{S}}$ with this choice of S, hence $X_{\mathrm{S}} \longrightarrow U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$ is surjective and since $E^+ \subseteq X_{\mathrm{S}}$, so is $X_{\mathrm{S}} \longrightarrow U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$, i.e. $X_{\mathrm{S}} \subseteq U_{\mathfrak{p}}$ is dense and by construction we have $\mathrm{S} \subseteq \mathrm{T}$ and $|\mathrm{S}| = g(\mathfrak{p}, \Sigma)$.

To see part (iii) we use

$$U_{\mathfrak{p}} = \mu_{q-1} \times U_{\mathfrak{p}}^{(1)} \simeq \mu_{q-1} \times \mu_{p^\infty}(k_{\mathfrak{p}}) \times \mathbb{Z}_p^{[k_{\mathfrak{p}}:\mathbb{Q}_p]},$$

where $q = |\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}}|$ (see [Neu99, ch. II, Theorem 5.7(i)]), which implies that the upper bound claimed in (iii) is in fact the minimal number of generators of $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$, which obviously is greater than or equal to the minimal number of generators of $U_{\mathfrak{p}}/\psi(E^+)U_{\mathfrak{p}}^{(1)^p}$, i.e. $g(\mathfrak{p}, \Sigma)$. □

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

4.2 Type ${}^2A_{d-1}$

In Theorem 14 we reduced the problem of approximating a local unit of a maximal order carrying a positive involution of the second kind by global *unitary* units to an approximation problem for a specific integral model T' of a one-dimensional anisotropic torus over a totally real number field. Here, we will only consider the following special case of this.

Let k be an imaginary quadratic field in which the rational prime p splits, $p\mathcal{O}_k = \mathfrak{p}\overline{\mathfrak{p}}$, and put

$$\mathrm{T} := \ker(\mathrm{Res}^{\mathcal{O}_k}_{\mathbb{Z}}(\mathbb{G}_{m,\mathcal{O}_k}) \xrightarrow{\mathrm{N}^k_{\mathbb{Q}}} \mathbb{G}_{m,\mathbb{Z}}).$$

THEOREM 19. *In the above situation, there exist infinitely many rational primes $l \neq p$ which split in $k/\mathbb{Q}$ and are such that $\mathrm{T}(\mathbb{Z}[1/l]) \subseteq \mathrm{T}(\mathbb{Z}_p)$ is a dense subgroup.*

Proof. Note that, for every rational prime $l \neq p$,

$$\mathrm{T}(\mathbb{Z}[1/l]) = \{\alpha \in \mathcal{O}_k[1/l]^* \mid \alpha\overline{\alpha} = 1\} \subseteq \mathrm{T}(\mathbb{Z}_p) = U_{\mathfrak{p}} \simeq \mathbb{Z}_p^*, \tag{19}$$

the local units of k at $\mathfrak{p}$, the final equalities following from the fact that p splits in k. Here, $^-$ denotes complex conjugation. The following proof is similar to the argument of Theorem 17(ii) but extra care is needed to deal with the norm condition $\alpha\overline{\alpha} = 1$.

Consider the following subgroups of the idèles of k:

$$U_K := \prod_{v \neq \mathfrak{p},\overline{\mathfrak{p}} \text{ finite}} U_v \times U_{\mathfrak{p}}^{(1)^p} \times U_{\overline{\mathfrak{p}}}^{(1)^p} \times \prod_{v|\infty} k_v^*$$

$$U_H := \prod_{v \text{ finite}} U_v \times \prod_{v|\infty} k_v^*.$$

We have a corresponding tower of abelian extensions $k \subseteq H \subseteq K$ and, since U_K is stable under $\mathrm{Gal}(k/\mathbb{Q})$, the extension $K/\mathbb{Q}$ is Galois, though rarely abelian. We have an isomorphism

$$\phi : U_{\mathfrak{p}}U_{\overline{\mathfrak{p}}}/U_{\mathfrak{p}}^{(1)^p}U_{\overline{\mathfrak{p}}}^{(1)^p}\mathcal{O}_k^* \simeq \frac{U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p} \times U_{\overline{\mathfrak{p}}}/U_{\overline{\mathfrak{p}}}^{(1)^p}}{\mathcal{O}_k^*} \xrightarrow{\simeq} \mathrm{Gal}(K/H)$$

induced by the Artin map, where $\mathcal{O}_k^*$ is embedded diagonally. Since p splits in k we have $U_{\mathfrak{p}} \simeq \mathbb{Z}_p^*$, $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}\mathcal{O}_k^*$ is cyclic and we fix a generator x of this group. By Chebotarev's theorem applied to $K/\mathbb{Q}$ there exist infinitely many rational primes $l \neq p$, unramified in $K/\mathbb{Q}$ and such that for a suitable prime Λ of K lying above l we have

$$\mathrm{Frob}_{\Lambda|l}^{-1} = \phi([(x,1)]) \text{ in } \mathrm{Gal}(K/H) \subseteq \mathrm{Gal}(K/\mathbb{Q}).$$

We claim that every such l satisfies the conclusion of Theorem 19.

Put $\lambda := \Lambda|_k$. Since $(\mathrm{Frob}_{\Lambda|l})|_H = \mathrm{id}$, l is split in $k/\mathbb{Q}$ and λ is a principal ideal of $\mathcal{O}_k$ a generator of which we denote by π. Then

$$\beta := \frac{\pi}{\overline{\pi}} \in \{\alpha \in \mathcal{O}_k[1/l]^* \mid \alpha\overline{\alpha} = 1\} = T(\mathbb{Z}[1/l]),$$

and we claim that β goes to x under the map induced by (19). As in the proof of Theorem 17(ii) one sees that

$$(\pi_{\mathfrak{p}}, \pi_{\overline{\mathfrak{p}}}) = [(x,1)]$$

and similarly

$$((\overline{\pi})_{\mathfrak{p}}, (\overline{\pi})_{\overline{\mathfrak{p}}}) = [(1,x)] \text{ in } \frac{U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p} \times U_{\overline{\mathfrak{p}}}/U_{\overline{\mathfrak{p}}}^{(1)^p}}{\mathcal{O}_k^*},$$

hence indeed

$$(\beta_{\mathfrak{p}}, \beta_{\overline{\mathfrak{p}}}) = [(x, x^{-1})],$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

and *a fortiori* $\beta_{\mathfrak{p}} = x$ in $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}\mathcal{O}_k^*$. Since we have $\mathcal{O}_k^* \subseteq \mathrm{T}(\mathbb{Z}[1/l])$ because $\mathcal{O}_k^*$ consists of roots of unity which have norm 1, we are done. □

To use Theorem 14 we must study approximation for the open subgroup scheme $\mathrm{T}' \subseteq \mathrm{T}$ obtained from T by removing the non-identity components of finitely many special fibers of T; cf. § 2.2.2. Let $\mu \subseteq \mathcal{O}_k^*$ denote the group of roots of unity. While we have $\mu \subseteq \mathrm{T}(\mathbb{Z})$, and this was used at the end of the proof of Theorem 19, in general we also have $-1 \notin \mathrm{T}'(\mathbb{Z}[1/l])$.

Corollary 20. *In the above situation there exist infinitely many rational primes $l \neq p$ which split in $k/\mathbb{Q}$ and are such that the closure of $\mathrm{T}'(\mathbb{Z}[1/l]) \subseteq \mathrm{T}'(\mathbb{Z}_p) = \mathrm{T}(\mathbb{Z}_p)$ has index at most $|\mu|$.*

Proof. We have $\mathrm{T}' \times_{\mathrm{Spec}\mathbb{Z}} \mathrm{Spec}(\mathbb{Z}_p) \xrightarrow{\simeq} \mathrm{T} \times_{\mathrm{Spec}\mathbb{Z}} \mathrm{Spec}(\mathbb{Z}_p)$ by the construction of T' and the fact that p is unramified (in fact, split) in $k/\mathbb{Q}$. Now observe that the element $\beta \in \mathrm{T}(\mathbb{Z}[1/l])$ constructed in the proof of Theorem 19 satisfies $\beta \in \mathrm{T}'(\mathbb{Z}[1/l])$. □

Corollary 21. *Let D be a finite-dimensional skew field over $\mathbb{Q}$ of reduced dimension $d > 1$ with a positive involution of the second kind $*$ and $\mathcal{O} \subseteq D$ a maximal order, stable under $*$. Assume that the center of D is an imaginary quadratic field k and let $p \neq 2$ be a rational prime which splits in k and $\mathfrak{P} \subseteq \mathcal{O}$ a prime lying above p. Then there exists a rational prime $l \neq p$ such that the closure of*

$$\left\{ g \in \mathcal{O}\left[\frac{1}{2l}\right] \;\middle|\; {}^*gg = 1 \right\} \subseteq \mathcal{O}_{\mathfrak{P}}^*$$

has index at most $|\mu|$.

Proof. From the data $(D, *)$ and $\mathcal{O} \subseteq D$ we construct group schemes $\mathrm{SU} \subseteq \mathrm{U}$ and $\mathrm{T}' \subseteq \mathrm{T}$ over $\mathrm{Spec}(\mathbb{Z})$ as in § 2.2.2. Using Corollary 20 we choose a prime $l \neq 2, p$ which splits in $k/\mathbb{Q}$ such that the closure of $\mathrm{T}'(\mathbb{Z}[1/l]) \subseteq \mathrm{T}'(\mathbb{Z}_p)$ has index at most $|\mu|$ and such that for every place λ of k lying above l we have $\mathrm{inv}_\lambda(D) = 0$. We apply Theorem 14 with $\mathrm{S} := \{2, l\}$ to conclude that the index of the closure of $\mathrm{U}(\mathbb{Z}[1/2l]) \subseteq \mathrm{U}(\mathbb{Z}_p)$ equals the index of the closure of $\mathrm{T}'(\mathbb{Z}[1/2l]) \subseteq \mathrm{T}'(\mathbb{Z}_p)$ and is thus bounded above by $|\mu|$. It remains to recall that

$$\mathrm{U}\left(\mathbb{Z}\left[\frac{1}{2l}\right]\right) = \left\{ g \in \mathcal{O}\left[\frac{1}{2l}\right] \;\middle|\; {}^*gg = 1 \right\}$$

and, since p splits in $k/\mathbb{Q}$,

$$\mathrm{U}(\mathbb{Z}_p) \simeq \mathcal{O}_{\mathfrak{P}}^*.$$

□

Remark 22. The conclusion of Corollary 21 can be sharpened in special cases. For example, if the reduced dimension of D is odd and 2 is unramified in $k/\mathbb{Q}$, then ($p = 2$ being allowed) there is a rational prime $l \neq p$ such that $\{\alpha \in \mathcal{O}[1/l] \mid {}^*\alpha\alpha = 1\} \subseteq \mathcal{O}_{\mathfrak{P}}^*$ is dense. This is because d being odd implies that $\mathrm{T}' = \mathrm{T}$ and 2 being unramified implies that $\mathcal{U} = \mathrm{Spec}(\mathbb{Z})$.

5. Applications

5.1 Extending automorphisms of p-divisible groups

Here we explain the application of some of the above results to the following problem.

Let k be a finite field of characteristic p and A/k a simple abelian variety such that $\mathrm{End}_k(A)$ is a maximal order in the skew field $D := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. The center K of D is a number field and $K \cap \mathrm{End}_k(A) = \mathcal{O}_K$ is its ring of integers.

The p-divisible group of A/k [Tat66] splits as

$$A[p^\infty] = \prod_{\mathfrak{p}|p} A[\mathfrak{p}^\infty], \tag{20}$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

the product extending over all primes $\mathfrak{p}$ of $\mathcal{O}_K$ dividing p. According to Tate, cf. [MW69, Theorem 6], the canonical homomorphism

$$\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\simeq} \mathrm{End}_k(A[p^\infty]) \tag{21}$$

is an isomorphism. We have

$$\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \prod_{\mathfrak{p}|p} \mathrm{End}_k(A) \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}} \simeq \prod_{\mathfrak{p}|p} \mathrm{End}_k(A)_{\mathfrak{P}}$$

with $\mathfrak{P}$ the unique prime of $\mathrm{End}_k(A)$ lying above $\mathfrak{p}$. Similarly, (20) implies that

$$\mathrm{End}_k(A[p^\infty]) \simeq \prod_{\mathfrak{p}|p} \mathrm{End}_k(A[\mathfrak{p}^\infty]).$$

These decompositions are compatible with (21), i.e. the canonical homomorphism

$$\mathrm{End}_k(A) \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}} \xrightarrow{\simeq} \mathrm{End}_k(A[\mathfrak{p}^\infty])$$

is an isomorphism for every $\mathfrak{p}|p$. We fix some $\mathfrak{p}|p$ and ask for a finite set S of finite primes of K such that $\mathfrak{p} \notin \mathrm{S}$ and

$$(\mathrm{End}_k(A) \otimes_{\mathcal{O}_K} \mathcal{O}_{K,S})^* \hookrightarrow \mathrm{Aut}_k(A[\mathfrak{p}^\infty]) \tag{22}$$

is a dense subgroup. Note that this density is equivalent to the following assertion.

For every $\alpha \in \mathrm{Aut}_k(A[\mathfrak{p}^\infty])$ and integer $n \geqslant 1$ there is an isogeny $\phi \in \mathrm{End}_k(A)$ of degree divisible by primes in S only and some $x \in \mathcal{O}_{K,S}^*$ such that

$$\phi x|_{A[\mathfrak{p}^n]} = \alpha|_{A[\mathfrak{p}^n]},$$

i.e. the quasi-isogeny ϕx of A extends the truncation at arbitrary finite level n of α.

By Theorem 9, the inclusion (22) is dense if and only if $X \subseteq U_{\mathfrak{p}}$ is dense where $X \subseteq \mathcal{O}_K^*$ is the subgroup of global units which are positive at all real places of K at which D does not split and $U_{\mathfrak{p}} := \mathcal{O}_{K,\mathfrak{p}}^*$ are the local units of K at $\mathfrak{p}$. The density of $X \subseteq U_{\mathfrak{p}}$ in turn is firmly controlled by Theorem 17. We would like to illustrate all of this with some examples.

According to the Albert classification [Mum70, Theorem 2, p. 201] (note that types I and II do not occur over finite fields) there are two possibilities.

Type III. Here, K is a totally real number field and D/K is a totally definite quaternion algebra. The simplest such case occurs if A/k is a super-singular elliptic curve with $\mathrm{End}_k(A) = \mathrm{End}_{\overline{k}}(A)$. In this case, it follows from Example 10(2) that, in case the characteristic of k is different from 2, for a suitable prime l

$$\left(\mathrm{End}_k(A)\left[\frac{1}{l}\right]\right)^* \hookrightarrow \mathrm{Aut}_k(A[p^\infty])$$

is dense.

To see another example of this type, let $A/\mathbb{F}_p$ correspond to a p-Weil number π with $\pi^2 = p$. Then $\dim(A) = 2$ and $A \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is isogeneous to the square of a super-singular elliptic curve. We have $K = \mathbb{Q}(\sqrt{p})$ and $\mathfrak{p} = (\sqrt{p})\mathcal{O}_K$, hence $A[\mathfrak{p}^\infty] = A[p^\infty]$. Furthermore, $\mathcal{O}_K^* = \{\pm 1\} \times \epsilon^{\mathbb{Z}}$ for a fundamental unit ϵ and $X \subseteq \mathcal{O}_K^*$ is of index 4. To find a small set S such that (22) is dense one first needs to compute the minimal number of generators of $U_{\mathfrak{p}}/XU_{\mathfrak{p}}^{(1)^p}$, denoted $g(\mathfrak{p}, \Sigma)$ in Theorem 17, where, in the present situation, Σ consists of both the infinite places of K. For $p = 2$ one can choose $\epsilon = 1 + \sqrt{2}$, then $X = \epsilon^{2\mathbb{Z}}$. Since $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^2} \simeq \mathbb{F}_2^3$ and $\epsilon^2 \notin U_{\mathfrak{p}}^{(1)^2}$, one gets $g(\mathfrak{p}, \Sigma) = 2$.

For $p = 3$ we may take $\epsilon = 2 + \sqrt{3}$, then $X = \epsilon^{2\mathbb{Z}}$ again. Since now $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^3} = \mu_2 \times \mathbb{F}_3^2 \simeq \mathbb{Z}/6 \times \mathbb{Z}/3$ the fact that $\epsilon^2 \notin U_{\mathfrak{p}}^{(1)^3}$ is not enough to conclude that $g(\mathfrak{p}, \Sigma) = 1$. However, one checks in addition that $\epsilon^2 \in U_{\mathfrak{p}}^{(1)}$, and concludes that $U_{\mathfrak{p}}/XU_{\mathfrak{p}}^{(1)^3} \simeq \mathbb{Z}/6$ and hence indeed $g(\mathfrak{p}, \Sigma) = 1$.

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

For $p \geqslant 5$ one has $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p} = \mu_{p-1} \times \mathbb{F}_p^2$ and since $\mu_{p-1} \not\subseteq K$ the image of a generator of X in $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p}$ will have non-trivial projection to $\mathbb{F}_p^2$ and one concludes that $g(\mathfrak{p}, \Sigma) = 1$.

Type IV. In this case, K is a CM-field and $X = \mathcal{O}_K^*$. The easiest such example occurs for an ordinary elliptic curve and we give two examples.

A solution of $\pi^2 + 5 = 0$ is a 5-Weil number to which there corresponds an elliptic curve $E/\mathbb{F}_5$ with $K = D = \mathbb{Q}(\sqrt{5})$. For $\mathfrak{p} = (\sqrt{5})\mathcal{O}_K$ one has $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)^p} = \mu_4 \times \mathbb{F}_5^2$ and since $\mathcal{O}_K^* = \{\pm 1\}$ one gets $U_{\mathfrak{p}}/XU_{\mathfrak{p}}^{(1)^p} \simeq \mathbb{Z}/10 \times \mathbb{Z}/5$, hence $g(\mathfrak{p}, \Sigma) = 2$.

Similarly, a solution of $\pi^2 - 4\pi + 5 = 0$ gives an elliptic curve over $\mathbb{F}_5$ with $D = K = \mathbb{Q}(i)$ and since 5 splits in K one has $U_{\mathfrak{p}}/XU_{\mathfrak{p}}^{(1)^p} \simeq \mathbb{Z}/10$, hence $g(\mathfrak{p}, \Sigma) = 1$ in this case.

Finally, we leave it as an easy exercise to an interested reader to check that for every prime p and integer $N \geqslant 1$ there exists a simple abelian variety $A/\mathbb{F}_p$ such that every set S for which (22) is dense necessarily satisfies $|S| \geqslant N$.

5.2 A dense subgroup of quasi-isogenies in the Morava stabilizer group

Let p be a prime and $n \geqslant 1$ an integer. The nth Morava stabilizer group $\mathbb{S}_n$ is the group of units of the maximal order of the central skew field over $\mathbb{Q}_p$ of Hasse invariant $1/n$.

In this section we will construct an abelian variety A/k over a finite field k of characteristic p such that for a suitable prime l the group $(\mathrm{End}_k(A)[1/l])^*$ is canonically a dense subgroup of $\mathbb{S}_n$. We will completely ignore the case $n = 1$ as it is very well understood. In the case $n = 2$ one can take for A a super-singular elliptic curve [BL06] and the resulting dense subgroup of $\mathbb{S}_2$ has been used to great advantage in the construction of a modular resolution of the $K(2)$-local sphere [Beh06].

For general n we remark that, since $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathrm{End}_k(A[p^\infty])$, in order that $\mathrm{End}_k(A)$ have a relation with $\mathbb{S}_n$ one needs $A[p^\infty] \otimes_k \overline{k}$ to have an isogeny factor of type $G_{1,n-1}$ (see [Man63, IV, § 2,2]). By the symmetry of p-divisible groups of abelian varieties [Man63, IV, § 3, Theorem 4.1], there must then also be a factor of type $G_{n-1,1}$ which shows that $n = 2$ is somewhat special since $(1, n-1) = (n-1, 1)$ in this case. For $n \geqslant 3$ the above considerations imply that the sought for abelian variety must be of dimension at least n, as already remarked by D. Ravenel [Rav07, Corollary 2.4(ii)]. Following suggestions of M. Behrens and T. Lawson we will be able to construct A having this minimal possible dimension. We start by constructing a suitable isogeny class as follows.

Proposition 23. *Let p be a prime and $n \geqslant 3$ an integer. Then there is a simple abelian variety $A/\mathbb{F}_{p^n}$ such that the center of $\mathrm{End}_{\mathbb{F}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field in which p splits into, say, $\mathfrak{p}$ and $\mathfrak{p}'$ such that $\mathrm{inv}_{\mathfrak{p}}(\mathrm{End}_{\mathbb{F}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}) = 1/n$, $\mathrm{inv}_{\mathfrak{p}'}(\mathrm{End}_{\mathbb{F}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}) = -1/n$ and $\dim(A) = n$. Furthermore, A is geometrically simple with $\mathrm{End}_{\overline{\mathbb{F}}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}_{\mathbb{F}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Proof. We use Honda–Tate theory; see [MW69] for an exposition. Let $\pi \in \overline{\mathbb{Q}}$ be a root of $f := x^2 - px + p^n \in \mathbb{Z}[x]$. Since the discriminant of f is negative, π is a p^n-Weil number and we choose $A/\mathbb{F}_{p^n}$ simple associated with the conjugacy class of π. Then $\mathbb{Q}(\pi)$ is an imaginary quadratic field and is the center of $\mathrm{End}_{\mathbb{F}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Since $n \geqslant 3$ the Newton polygon of f at p has different slopes 1 and $n-1$ which shows that f is reducible over $\mathbb{Q}_p$ (see [Neu99, ch. II, Theorem 6.4]), hence p splits in $\mathbb{Q}(\pi)$ into $\mathfrak{p}$ and $\mathfrak{p}'$ and, exchanging π and $\overline{\pi}$ if necessary, we can assume that $v_{\mathfrak{p}}(\pi) = 1$ and $v_{\mathfrak{p}}(\overline{\pi}) = n - 1$. Then [MW69, Theorem 8, 4]

$$\mathrm{inv}_{\mathfrak{p}}(\mathrm{End}_{\mathbb{F}_{p^n}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}) = \frac{v_{\mathfrak{p}}(\pi)}{v_{\mathfrak{p}}(p^n)}[\mathbb{Q}(\pi)_{\mathfrak{p}} : \mathbb{Q}_p] = \frac{1}{n}$$

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

and similarly

$$\mathrm{inv}_{\mathfrak{p}'}(\mathrm{End}_{\mathbb{F}_{p^n}}(A)\otimes_{\mathbb{Z}}\mathbb{Q}) = \frac{n-1}{n} = \frac{-1}{n}.$$

Furthermore [MW69, Theorem 8, 3], $2\cdot\dim(A) = [\mathrm{End}_{\mathbb{F}_{p^n}}(A)\otimes_{\mathbb{Z}}\mathbb{Q} : \mathbb{Q}(\pi)]^{1/2}\cdot[\mathbb{Q}(\pi):\mathbb{Q}] = 2n$. The final statement follows easily from the fact that $\pi^k \notin \mathbb{Q}$ for all $k \geqslant 1$, cf. [HZ02, Proposition 3(2)], which in turn is evident since $v_{\mathfrak{p}}(\pi) \neq v_{\mathfrak{p}}(\overline{\pi})$. □

Since the properties of $A/\mathbb{F}_{p^n}$ listed in Proposition 23 are invariant under $\mathbb{F}_{p^n}$-isogenies, we can, and do, choose $A/\mathbb{F}_{p^n}$ having these properties such that in addition $\mathrm{End}_{\mathbb{F}_{p^n}}(A) \subseteq \mathrm{End}_{\mathbb{F}_{p^n}}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ is a maximal order [Wat69, proof of Theorem 3.13]. Denoting by $\mathfrak{P} \subseteq \mathrm{End}_{\mathbb{F}_{p^n}}(A)$ the unique prime lying above the prime $\mathfrak{p}$ constructed in Proposition 23, we have $(\mathrm{End}_{\mathbb{F}_{p^n}}(A))^*_{\mathfrak{P}} = \mathbb{S}_n$ since $\mathrm{inv}_{\mathfrak{p}}(\mathrm{End}^0_{\mathbb{F}^{p^n}}(A)\otimes_{\mathbb{Z}}\mathbb{Q}) = 1/n$. We choose a prime l as follows: if $p \neq 2$ we take l to be a topological generator of $\mathbb{Z}_p^*$; for $p = 2$ we take $l = 5$.

Remark 24. Note that for $p \neq 2$ a prime $l \neq p$ topologically generates $\mathbb{Z}_p^*$ if and only if $(l \bmod p^2)$ generates $(\mathbb{Z}/p^2)^*$. Hence, by Dirichlet's theorem on primes in arithmetic progressions, the set of all such l has a density equal to $((p-1)\phi(p-1))^{-1} > 0$ and is thus infinite. Such an l can be found rather effectively: given $l \neq p$, compute $\alpha_k := (l^{p(p-1)/k} \bmod p^2)$ for all primes k dividing $p(p-1)$. If for all k, $\alpha_k \not\equiv 1\,(p^2)$, then l is suitable.

Theorem 25. *In the above situation,*

$$(\mathrm{End}_{\mathbb{F}_{p^n}}(A)[1/l])^* \hookrightarrow (\mathrm{End}_{\mathbb{F}_{p^n}}(A))^*_{\mathfrak{P}} = \mathbb{S}_n$$

is a dense subgroup.

Proof. We apply Theorem 9 with $\mathcal{O} := \mathrm{End}_{\mathbb{F}_{p^n}}(A)$, $k := \mathbb{Q}(\pi)$, $\mathfrak{p}$ the prime of $\mathcal{O}_k$ constructed in Proposition 23 and $\mathrm{S} := \{\infty, l\}$ the set consisting of the unique infinite place ∞ of k and all places dividing l. Clearly, $\mathfrak{p} \notin \mathrm{S}$ and $D := \mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}$ is not a skew field at ∞ since $k_\infty \simeq \mathbb{C}$ and $n > 1$. Using the notation of Theorem 9 we have $\mathcal{O}_{k,\mathrm{S}^{\mathrm{fin}}} = \mathcal{O}_k[1/l]$ and $X = (\mathcal{O}_k[1/l])^*$ since k has no real place. Theorem 9 shows that the claim of Theorem 25 is equivalent to the density of $(\mathcal{O}_k[1/l])^* \subseteq \mathcal{O}^*_{k,\mathfrak{p}} \simeq \mathbb{Z}_p^*$. Since $l \in (\mathcal{O}_k[1/l])^*$, this density is clear for $p \neq 2$ by our choice of l whereas for $p = 2$ we have that $\{\pm 1\}\times 5^{\mathbb{Z}} \subseteq \mathbb{Z}_2^*$ is dense and $-1, 5 \in (\mathcal{O}_k[1/5])^*$. □

Acknowledgements

I would like to thank U. Jannsen and A. Schmidt for useful discussions concerning § 4.1 and M. Behrens and T. Lawson for pointing out to me the abelian varieties used in § 5.2. Furthermore, I thank M. Behrens for pointing out a gap in the first version of this paper and J. Heinloth for his help to fix it. Finally, I am grateful to one referee for suggesting stylistic improvements and to the other for a very careful report which led to substantial simplifications.

References

Beh06 M. Behrens, *A modular description of the $K(2)$-local sphere at the prime 3*, Topology **45** (2006), 343–402.

BL06 M. Behrens and T. Lawson, *Isogenies of elliptic curves and the Morava stabilizer group*, J. Pure Appl. Algebra **207** (2006), 37–49.

BL07 M. Behrens and T. Lawson, *Topological automorphic forms*, http://front.math.ucdavis.edu/math.AT/0702719.

BLR90 S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21 (Springer, Berlin, 1990).

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

BT84a F. Bruhat and J. Tits, *Groupes réductifs sur un corps local II, Schémas en groupes, Existence d'une donnée radicielle valuée*, Publ. Math. Inst. Hautes Études Sci. **60** (1984), 197–376.

BT84b F. Bruhat and J. Tits, *Schémas en groupes et immeubles des groupes classiques sur un corps local*, Bull. Soc. Math. France **112** (1984), 259–301.

CTS87 J.-L. Colliot-Thélène and J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: applications*, J. Algebra **106** (1987), 148–205.

DG70 M. Demazure and A. Grothendieck, *Schémas en groupes I: Propriétés générales des schémas en groupes*, in *Séminaire de Géométrie Algébrique du Bois Marie 1962/64*, Lecture Notes in Mathematics, vol. 151 (Springer, Berlin, 1970).

Deu68 M. Deuring, *Algebren*, second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 41 (Springer, Berlin, 1968).

Gil02 P. Gille, *Torseurs sur la droite affine*, Transform. Groups **7** (2002), 231–245.

GHMR05 P. Goerss, H.-W. Henn, M. Mahowald and C. Rezk, *A resolution of the $K(2)$-local sphere at the prime 3*, Ann. of Math. (2) **162** (2005), 777–822.

Gro66 A. Grothendieck, *Éléments de géométrie algébrique, IV, Étude locale des schémas et des morphismes de schémas III*, Publ. Math. Inst. Hautes Études Sci. **28** (1966).

Gro67 A. Grothendieck, *Éléments de géométrie algébrique IV, Étude locale des schémas et des morphismes de schémas IV*, Publ. Math. Inst. Hautes Études Sci. **32** (1967).

Hen07 H.-W. Henn, *On finite resolutions of $K(n)$-local spheres*, in *Elliptic cohomology*, London Mathematical Society Lecture Note Series, vol. 342 (Cambridge University Press, Cambridge, 2007) 122–169.

Hid04 H. Hida, *p-adic automorphic forms on Shimura varieties*, Springer Monographs in Mathematics (Springer, New York, 2004).

HS99 M. Hovey and N. Strickland, *Morava K-theories and localisation*, Mem. Amer. Math. Soc. **139** (1999), no. 666.

HZ02 E. Howe and H. Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory **92** (2002), 139–163.

Kle00 E. Kleinert, *Units in skew fields*, Progress in Mathematics, vol. 186 (Birkhäuser, Basel, 2000).

KMRT98 M. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44 (American Mathematical Society, Providence, RI, 1998).

Man63 J. Manin, *Theory of commutative formal groups over fields of finite characteristic*, Uspekhi Mat. Nauk **18** (1963), no. 6 (114), 3–90.

Mil80 J. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33 (Princeton University Press, Princeton, NJ, 1980).

MW69 J. Milne and W. Waterhouse, *Abelian varieties over finite fields*, Proc. Sympos. Pure Math. **XX** (1969), 53–64.

Mum70 D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, no. 5 (Oxford University Press, London, 1970).

Neu99 J. Neukirch, *Algebraic number theory*, Fundamental Principles of Mathematical Sciences, vol. 322 (Springer, Berlin, 1999).

PR94 V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139 (Academic Press, Boston, MA, 1994).

Rav92 D. Ravenel, *Nilpotence and periodicity in stable homotopy theory*, Annals of Mathematics Studies, vol. 128 (Princeton University Press, Princeton, NJ, 1992).

Rav07 D. Ravenel, *Preprint of part I*, http://www.math.rochester.edu/people/faculty/doug/preprints.html.

Rei03 I. Reiner, *Maximal orders*, London Mathematical Society Monographs, New Series, vol. 28 (Clarendon Press, Oxford, 2003).

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press

Spr94 T. Springer, *Linear algebraic groups*, in *Algebraic geometry IV*, Encyclopaedia of Mathematical Sciences, vol. 55 (Springer, Berlin, 1994).

Tat66 J. Tate, *p-divisible groups*, in *1967 Proc. Conf. Local Fields*, Driebergen, 1966, pp. 158–183.

Wat69 W. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

Wat79 W. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66 (Springer, Berlin, 1979).

Wei82 A. Weil, *Adèles and algebraic groups*, Progress in Mathematics, vol. 23 (Birkhäuser, Boston, MA, 1982).

Niko Naumann niko.naumann@mathematik.uni-regensburg.de
NWF I – Mathematik, Universität Regensburg, 93040 Regensburg, Germany

https://doi.org/10.1112/S0010437X07003181 Published online by Cambridge University Press