HIGHER REAL K-THEORIES AND TOPOLOGICAL AUTOMORPHIC FORMS

M. BEHRENS[1] AND M.J. HOPKINS[2]

ABSTRACT. Given a maximal finite subgroup G of the nth Morava stabilizer group at a prime p, we address the question: is the associated higher real K-theory EO_n a summand of the $K(n)$-localization of a TAF-spectrum associated to a unitary similitude group of type $U(1, n-1)$? We answer this question in the affirmative for $p \in \{2, 3, 5, 7\}$ and $n = (p-1)p^{r-1}$ for a maximal finite subgroup containing an element of order p^r. We answer the question in the negative for all other odd primary cases. In all odd primary cases, we to give an explicit presentation of a global division algebra with involution in which the group G embeds unitarily.

CONTENTS

1

1. Introduction

For a prime p, let E_n denote the Morava E-theory spectrum associated with the Honda formal group H_n of height n over $\bar{\mathbb{F}}_p$, so that

$$\pi_* E_n = W(\bar{\mathbb{F}}_p)[[u_1, \ldots, u_{n-1}]].$$

The second author, with P. Goerss and H. Miller, showed that E_n is an E_∞ ring spectrum, and that the nth Morava stabilizer group

$$\mathbb{S}_n = \mathrm{Aut}(H_n)$$

acts on E_n by E_∞ ring maps [Rez98], [GH04].

One of the original motivations for producing this action was that, given a maximal finite subgroup G of $\mathbb{S}_n$, the spectrum

$$EO_n := E_n^{hG}$$

would more effectively detect v_n-periodic homotopy groups of spheres, generalizing the phenomenon that the spectrum KO detects the 2-primary image of J more effectively than the spectrum KU. In fact, for $p = 2$, there is an equivalence

$$(1.1) \qquad KO_{K(1)} \simeq EO_1^{h\,\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}.$$

It is for this reason that the spectra EO_n are regarded as "higher real K-theories."

For the primes 2 and 3, there are equivalences

$$(1.2) \qquad \mathrm{TMF}_{K(2)} \simeq EO_2^{h\,\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}$$

where TMF denotes the spectrum of topological modular forms. Using a theorem of J. Lurie, the first author and T. Lawson constructed p-complete spectra $\mathrm{TAF}_{GU}(K)$ of topological automorphic forms associated to unitary similitude groups over $\mathbb{Q}$ of signature $(1, n-1)$ and compact open subgroups $K \subset GU(\mathbb{A}^{p,\infty})$ [BLa]. The spectrum $\mathrm{TAF}_{GU}(K)$ arises from a Shimura stack $\mathrm{Sh}(K)$, in the same manner that the spectrum TMF arises from the moduli stack of elliptic curves. The spectra $\mathrm{TAF}_{GU}(K)$ detect $E(n)$-local phenomena in the same sense that the spectrum $\mathrm{TMF}_p^\wedge$ detects $E(2)$-local phenomena. This is made precise as follows: there is an equivalence

$$\mathrm{TAF}_{GU}(K)_{K(n)} \simeq \left(\prod_{x \in \mathrm{Sh}^{[n]}(K)(\bar{\mathbb{F}}_p)} E_n^{h\,\mathrm{Aut}(x)} \right)^{h\,\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}$$

where $\mathrm{Sh}^{[n]}(K)$ is the (non-empty) finite 0-dimensional substack of $\mathrm{Sh}(K)$ where the associated formal group has height n, and the automorphism groups $\mathrm{Aut}(x)$ are finite subgroups of $\mathbb{S}_n$ [BLa, Cor. 14.5.6]. Given equivalences (1.1) and (1.2) it is natural to ask:

> For a given prime p and chromatic level n, does there exist a pair (GU, K) so that there exists an $x \in \mathrm{Sh}^{[n]}(K)$ for which $\mathrm{Aut}(x)$ is a maximal finite subgroup of $\mathbb{S}_n$?

The purpose of this paper is to provide answers to this question.

For large n, the notation EO_n is ambiguous, because there exist multiple non-isomorphic choices of maximal finite subgroups G. Hewett [Hew95] determined precisely the collection of maximal finite subgroups of $\mathbb{S}_n$. In particular, he showed that if r is the largest exponent so that G contains an element of order p^r, then the isomorphism class of G is determined by the pair (n, r). If p is odd and G is non-abelian, then as a subgroup of the group of units of the associated division algebra, it is unique up to conjugation [Hew95, Prop. 6.11]. In this paper, we will denote such a subgroup G_r. We summarize our results in the following theorem.

Theorem 1.3. Suppose that p is odd and $n = (p-1)p^{\alpha-1}m$ for a positive integer m. Then there exists a pair (GU, K) whose associated Shimura stack has a height $n \bmod p$ point with automorphism group G_α if and only if $p \in \{3, 5, 7\}$ and $m = 1$. If $p = 2$, and $n = 2^{r-1}$ for $r > 2$, we can also realize G_{r-1} as an automorphism group.

Remark 1.4. In the above theorem, the case of $p = 2$ and $n = 1$ is handled by KO, and the case of $p = 2$ and $n = 2$ is the TMF case. However, both of these cases may also be viewed as instances of TAF: see [BLa, Ch. 15] for the $n = 1$ case, and [BLb] for the $n = 2$ case.

We also prove the following algebraic theorem, which could be regarded as a kind of global analog of Hewett's results.

Theorem 1.5. Suppose that p is odd, and that $n = (p-1)p^{\alpha-1}m$. Then there exists a global division algebra D with positive involution $\dagger$ of the second kind, so that:

(1) we have $[D : F] = n^2$, where F is the center of D,
(2) there is a prime x of the fixed field $F^{\dagger=1}$ which splits as $yy^\dagger$ in F, so that $\mathrm{Inv}_y D = 1/n$,
(3) there is a $\dagger$-unitary embedding of the maximal finite subgroup $G_\alpha \subset \mathbb{S}_n$ in $D^\times$.

Since G_α is a maximal finite subgroup in the completion $D_y^\times$, it is necessarily a maximal finite subgroup in $D^\times$.

As we point out in Section 9.2, using the theorem above, one can adapt our methods to argue that for *every* odd prime p and chromatic height $n = (p-1)p^{\alpha-1}m$, there exists a unitary Shimura stack with a mod p point with G_α as its automorphism group. The associated unitary group is defined over a totally real field F^+. However, unless $p \leq 7$, this totally real field is *not* $\mathbb{Q}$. As [BLa] only associates TAF-spectra to Shimura stacks of certain unitary groups over $\mathbb{Q}$, such global manifestations of Hewett subgroups have no obvious topological realization.

Organization of the paper.

In Section 2, we give an overview of unitary Shimura varieties of type $(1, n-1)$, and the associated spectra of topological automorphic forms. We explain how the

automorphism groups of height n mod p points can be computed using division algebras with involution.

In Section 3, we give an overview of presentations of division algebras in terms of cohomological data. In the case of a division algebra over a local number field, we explain how to make these presentations explicit using local class field theory. The material in this section is essentially well known.

In Section 4, we use the explicit presentations of Section 3 to simultaneously review and give a new perspective on Hewett's maximal finite subgroups G_α in $\mathbb{S}_n$.

In Section 5, we give one direction of Theorem 1.3, by showing that G_α cannot be an automorphism group of a height n mod p point for p odd and $n = (p-1)p^{\alpha-1}m$ unless $p \leq 7$ and $m = 1$.

In Section 6, we use global class field theory to give global analogs of the explicit presentations of division algebras given in Section 3. We use these explicit presentations to embed the Hewett subgroups G_α into global division algebras.

In Section 7, we produce involutions on the division algebras of Section 6 which act on the finite subgroup G_α by inversion. The existence of these involutions completes the proof of Theorem 1.5.

In Section 8, we assume that $p \in \{3, 5, 7\}$ and $n = (p-1)p^{r-1}$, and show that there is a simple choice of hermitian form of signature $(1, n-1)$ whose associated Shimura stack has a height n mod p point with automorphism group G_r. This completes the odd primary cases of Theorem 1.3.

In Section 9, we give some concluding remarks.

- We explain how the results of this paper relate the Hopkins-Gorbounov-Mahowald approach to EO_{p-1} to the theory of topological automorphic forms.
- We explain that for odd primes, our results also allow one to realize all of the groups G_α as automorphism groups of some unitary Shimura stack — but these Shimura stacks do not have known topological applications (i.e., they are not of type $(1, n-1)$).
- We suggest that our explicit global division algebras could shed light on EO_n-resolutions of the $K(n)$-local sphere.
- We explain the applicability of our results to the problem of producing connective analogs of EO_n.
- We explain that our results combine with a theorem of Mark Hovey to prove that, at least in some cases, the TAF-spectra do not admit an orientation for *any* connective cover of O.
- We show that for any prime p, and $n = (p-1)p^{r-1}$, there exists a unitary Shimura stack of type $(1, n-1)$ with a height n mod p point whose automorphism group contains an element of order p^r.
- Specializing the previous observation to the prime 2, we explain how this gives an automorphism group isomorphic to G_r, in the case where $p = 2$ and $n = 2^{r-1}$. This completes the proof of Theorem 1.3.

Conventions.

In this paper, we shall use the following notation.

- ζ_n = primitive nth root of unity.
- $K[p^n]$ = cyclotomic $\mathbb{Z}/p^n$-extension of K (i.e. the fixed field of $K(\zeta_{p^{n+1}})$ by the subgroup of $(\mathbb{Z}/p^{n+1})^\times = \mathrm{Gal}(K(\zeta_{p^{n+1}})/K)$ of order $p-1$). Here, we are assuming K satisfies $[K(\zeta_{p^{n+1}}) : K] = (p-1)p^n$.
- Art denotes the local/global Artin map.
- $H^*(L/K)$ = the Galois cohomology group $H^*(\mathrm{Gal}(L/K), L^\times)$.
- $\mathbb{A}$ = the rational adeles. If S is a set of places, $\mathbb{A}^S$ denotes the adeles away from S, whereas $\mathbb{A}_S$ denotes the adeles at S. For a global number field K, $\mathbb{A}_K$ denotes the K-adeles.
- $\mathbb{I}_\mathbb{K}$ = the K-ideles $\mathbb{A}_K^\times$.

Acknowledgments.

2. Overview of topological automorphic forms

We review the theory of topological automorphic forms presented in [BLa]. (The p-integral models of the Shimura varieties discussed here are special cases of those constructed and studied in [Kot92].)

Fix a prime p and consider the following initial data:

$$F = \text{quadratic imaginary extension of } \mathbb{Q} \text{ in which } p \text{ splits as } u\bar{u},$$
$$B = \text{central simple } F\text{-algebra of dimension } n^2 \text{ which splits at } u \text{ and } \bar{u},$$
$$* = \text{positive involution of the second kind on } B,$$
$$\mathcal{O}_{B,(p)} = *\text{-invariant maximal } \mathcal{O}_{F,(p)}\text{-order of } B,$$
$$V = B \text{ module of rank } 1,$$
$$\langle -, - \rangle = \mathbb{Q}\text{-valued } *\text{-hermitian alternating form of signature } (1, n-1),$$
$$\epsilon = \text{rank 1 idempotent of } \mathcal{O}_{B,u} \cong M_n(\mathbb{Z}_p).$$

Let ι denote the involution on $\mathrm{End}_B(V)$, defined by

$$\langle \alpha v, w \rangle = \langle v, \alpha^\iota w \rangle.$$

Let $GU = GU_V$ be the associated unitary similitude group over $\mathbb{Q}$, with R-points

$$GU(R) = \{g \in \mathrm{End}_B(V) \otimes_\mathbb{Q} R \ : \ \langle gv, gw \rangle = \nu(g)\langle v, w \rangle, \ \nu(g) \in R^\times \}$$
$$= \{g \in \mathrm{End}_B(V) \otimes_\mathbb{Q} R \ : \ g^\iota g \in R^\times \}$$

(so that $\nu(g) = g^\iota g \in R^\times$).

We let $V^{p,\infty}$ denote $V \otimes \mathbb{A}^{p,\infty}$. For every compact open subgroup

$$K \subset GU(\mathbb{A}^{p,\infty})$$

there is a Deligne-Mumford stack $\mathrm{Sh}(K)/\mathrm{Spec}(\mathbb{Z}_p)$. For a locally noetherian connected $\mathbb{Z}_p$-scheme S, and a geometric point s of S, the S-points of $\mathrm{Sh}(K)$ are the groupoid whose objects are tuples $(A, i, \lambda, [\eta]_K)$, with:

$A,$	an abelian scheme over S of dimension n^2,
$\lambda : A \to A^\vee,$	a $\mathbb{Z}_{(p)}$-polarization,
$i : \mathcal{O}_{B,(p)} \hookrightarrow \mathrm{End}(A)_{(p)},$	an inclusion of rings, such that the λ-Rosati involution is compatible with conjugation,
$[\eta]_K,$	a $\pi_1(S, s)$-invariant K-orbit of B-linear similitudes:

$$\eta : (V^{p,\infty}, \langle -, - \rangle) \xrightarrow{\cong} (V^p(A_s), \langle -, - \rangle_\lambda),$$

subject to the following condition:

(2.1)   the coherent sheaf $\mathrm{Lie}\, A \otimes_{\mathcal{O}_{F,p}} \mathcal{O}_{F,u}$ is locally free of rank n.

Here, since S is a $\mathbb{Z}_p$-scheme, the action of $\mathcal{O}_{F,(p)}$ on $\mathrm{Lie}\, A$ factors through the p-completion $\mathcal{O}_{F,p}$.

The morphisms

$$(A, i, \lambda, \eta) \to (A', i', \lambda', \eta')$$

of the groupoid of S-points of $\mathrm{Sh}(K)$ are the prime-to-p quasi-isogenies of abelian schemes

$$\alpha : A \xrightarrow{\simeq} A'$$

such that

$$\lambda = r\alpha^\vee \lambda' \alpha, \quad r \in \mathbb{Z}_{(p)}^\times,$$
$$i'(z)\alpha = \alpha i(z), \quad z \in \mathcal{O}_{F,(p)},$$
$$[\eta']_K = [\eta \circ \alpha_*]_K.$$

Remark 2.2. If the algebra B is split, then the moduli interpretation of the points of $\mathrm{Sh}(K)$ may be simplified. Namely, the idempotent ϵ may be extended to a rank 1 idempotent on B, and the moduli of B-linear abelian schemes of dimension n^2 becomes Morita equivalent to the moduli of F-linear abelian schemes of dimension n. Thus, in this case, the S-points of $\mathrm{Sh}(K)$ could instead be taken to be a groupoid of tuples $(A, i, \lambda, [\eta]_K)$, with (A, i) an abelian scheme of dimension n with complex multiplication by F.

The p-completion $\mathrm{Sh}(K)_p^\wedge / \mathrm{Spf}(\mathbb{Z}_p)$ is determined by the S-points of $\mathrm{Sh}(K)$ on which p is locally nilpotent. On such schemes, the abelian scheme A has an n^2-dimensional p-divisible group $A(p)$ of height $2n^2$. The composite

$$\mathcal{O}_{B,(p)} \xrightarrow{i} \mathrm{End}(A)_{(p)} \to \mathrm{End}(A(p))$$

factors through the p-completion

$$\mathcal{O}_{B,p} \cong \mathcal{O}_{B,u} \times \mathcal{O}_{B,\bar{u}} \cong M_n(\mathbb{Z}_p) \times M_n(\mathbb{Z}_p).$$

Therefore, the action of $\mathcal{O}_B$ naturally splits $A(p)$ into two summands, $A(u)$ and $A(\bar{u})$, both of height n^2. For such schemes S, Condition (2.1) is equivalent to the condition that $A(u)$ is n-dimensional. This forces the formal group of A to split

into n-dimensional and $n(n-1)$-dimensional formal summands. The action of $\mathcal{O}_{B,u}$ on $A(u)$ provides a splitting

$$A(u) = \epsilon A(u)^n$$

where $\epsilon A(u)$ is a 1-dimensional p-divisible group of height n.

A theorem of Jacob Lurie [BLa, Thm. 8.1.4] associates to a 1-dimensional p-divisible group $\mathbb{G}$ over a locally noetherian separated Deligne-Mumford stack $X/\mathrm{Spec}(\mathbb{Z}_p)$ which is locally a universal deformation of all of its mod p points, a (Jardine fibrant) presheaf of E_∞-ring spectra $\mathcal{E}_{\mathbb{G}}$ on the site $(X_p^\wedge)_{et}$. The presheaf $\mathcal{E}_{\mathbb{G}}$ is functorial in $(X, \mathbb{G})$ (the precise statement of this functoriality is given in [BLa, Thm. 8.1.4]).

If $(\mathbf{A}, \mathbf{i}, \boldsymbol{\lambda}, [\boldsymbol{\eta}])$ is the universal tuple over $\mathrm{Sh}(K)$, then the p-divisible group $\epsilon\mathbf{A}(u)$ satisfies the hypotheses of Lurie's theorem [BLa, Sec. 8.3]. The associated sheaf will be denoted

$$\mathcal{E}_{GU} := \mathcal{E}_{\epsilon\mathbf{A}(u)}.$$

The E_∞-ring spectrum of topological automorphic forms is obtained by taking the homotopy global sections:

$$\mathrm{TAF}_{GU}(K) := \mathcal{E}_{GU}(\mathrm{Sh}(K)_p^\wedge).$$

Let $\epsilon A(u)^0$ denote the formal subgroup of the p-divisible group $\epsilon A(u)$. Let $\mathrm{Sh}(K)_{\mathbb{F}_p}$ denote the reduction mod p of $\mathrm{Sh}(K)$, and let

$$\mathrm{Sh}(K)^{[n]} \subseteq \mathrm{Sh}(K)_{\mathbb{F}_p}$$

denote the 0-dimensional substack where the height of the formal group $\epsilon A(u)^0$ is equal to n.

Picking a point $\mathbf{A}_0 = (A_0, i_0, \lambda_0, [\eta_0]_K) \in \mathrm{Sh}(K)^{[n]}(\bar{\mathbb{F}}_p)$, the ring of prime-to-$p$ $\mathcal{O}_B$-linear quasi-endomorphisms of A_0 is the unique maximal $\mathcal{O}_{F,(p)}$-order in a division algebra D with center F:

$$\mathrm{End}_{\mathcal{O}_{B,(p)}}(A_0)_{(p)} = \mathcal{O}_{D,(p)} \subset D.$$

We have, for x a finite place of F,

$$\mathrm{Inv}_x D = \begin{cases} \mathrm{Inv}_x B, & x \nmid p, \\ \frac{1}{n}, & x = u, \\ \frac{n-1}{n}, & x = \bar{u}. \end{cases}$$

The prime-to-p polarization λ_0 of A_0 gives rise to an associated Rosati involution $\dagger$ on D. The Rosati involution is a positive involution of the second kind. Define the associated unitary similitude group $GU_{\mathbf{A}_0}/\mathbb{Z}_{(p)}$ by

$$GU_{\mathbf{A}_0}(R) = \{g \in \mathcal{O}_{D,(p)} \otimes_{\mathbb{Z}_{(p)}} R \; : \; g^\dagger g \in R^\times\}.$$

Fixing a representative η_0 of $[\eta_0]$ gives a B-linear isomorphism

$$\eta_0 : V^{p,\infty} \to V^p(A_0).$$

The induced B-linear action of $\mathcal{O}_{D,(p)}$ on $V^{p,\infty}$ is an action by similitudes, and induces an isomorphism

$$\xi_{\eta_0} : GU_{\mathbf{A}_0}(\mathbb{A}^{p,\infty}) \xrightarrow{\cong} GU(\mathbb{A}^{p,\infty}).$$

Under this isomorphism, the subgroup $K \subset GU(\mathbb{A}^{p,\infty})$ may be regarded as a subgroup of $GU_{\mathbf{A}_0}(\mathbb{A}^{p,\infty})$. We define

$$\Gamma(K) = GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}) \cap K \subset D^\times.$$

Since K is open, the group $\Gamma(K)$ is finite. Since $GU_{\mathbf{A}_0}(\mathbb{Z}_p) = \mathcal{O}_{D,u}^\times = \mathbb{S}_n$, each of the finite groups $\Gamma(K)$ are finite subgroups of the Morava stabilizer group.

Lemma 2.3 ([BLa, Prop. 14.1.2]). *The automorphism group of the point $\mathbf{A}_0$ is given by*

$$\mathrm{Aut}(\mathbf{A}_0) = \Gamma(K).$$

Let E_n be the Morava E-theory associated to a height n formal group over $\bar{\mathbb{F}}_p$.

Theorem 2.4 ([BLa, Cor. 14.5.6]). *There is an equivalence*

$$\mathrm{TAF}_{GU}(K)_{K(n)} \simeq \left(\prod_{[g] \in GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}) \backslash GU(\mathbb{A}^{p,\infty})/K} E_n^{h\Gamma(gKg^{-1})} \right)^{h\,\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}.$$

Therefore, the problem of realizing EO_n's in the $K(n)$-localization of a TAF-spectrum amounts to determining which maximal finite subgroups of $\mathbb{S}_n$ arise as a $\Gamma(K)$ for some choice of F, form of GU, and subgroup K.

3. Explicit division algebras

Let K be a local or global number field. Following Serre [Ser], we make explicit the isomorphism

$$\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(\bar{K}/K); \bar{K}^\times).$$

We will regard elements of $H^2(G, A)$ as corresponding to extensions

$$1 \to A \to E \to G \to 1.$$

Since we have

$$H^2(\mathrm{Gal}(\bar{K}/K); \bar{K}^\times) = \operatornamewithlimits{colim}_{\substack{M/K \\ [M:K]<\infty}} H^2(\mathrm{Gal}(M/K); M^\times),$$

every element of $H^2(\mathrm{Gal}(\bar{K}/K); \bar{K}^\times)$ originates in $H^2(\mathrm{Gal}(M/K), M^\times)$ for some finite extension M of K.

Given a central simple algebra B/K with $[B : K] = n^2$, we choose a maximal subfield $M \subseteq B$ containing K, so that $[M : K] = n$. Define a group E by

$$E = \{x \in B^\times : xMx^{-1} = M\}.$$

Then the short exact sequence

$$1 \to M^\times \to E \to \mathrm{Gal}(M/K) \to 1$$

gives the desired class in $H^2(\mathrm{Gal}(M/K); M^\times)$.

Conversely, suppose that we are given an element of $H^2(\mathrm{Gal}(M/K), M^\times)$ corresponding to an extension

$$1 \to M^\times \to E \to \mathrm{Gal}(M/K) \to 1,$$

we may express the corresponding central simple algebra as

$$B = \mathbb{Z}[E] \otimes_{\mathbb{Z}[M^\times]} M.$$

We explain how to make this construction explicit in the case where K is a finite extension of $\mathbb{Q}_p$ and M is a cyclic extension of K. Let

$$\mathrm{Art}_{M/K} : K^\times/N(M^\times) \xrightarrow{\cong} \mathrm{Gal}(M/K)$$

be the local Artin map.

Proposition 3.1. Let K be a finite extension of $\mathbb{Q}_p$, and suppose that M is a degree n cyclic extension of K. Fix an injection

$$\chi : \mathrm{Gal}(M/K) \hookrightarrow \mathbb{Q}/\mathbb{Z},$$

and let $\sigma \in \mathrm{Gal}(M/K)$ be the unique element satisfying

$$\chi(\sigma) = 1/n.$$

Then for each element $a \in K^\times$ there is an extension

$$1 \to M^\times \xrightarrow{i} E_a \xrightarrow{j} \mathrm{Gal}(M/K) \to 1$$

such that

(1) there is a lift of σ to $\widetilde{\sigma} \in E_a$ such that $\widetilde{\sigma}^n = i(a)$, and
(2) the corresponding central simple algebra $B_{[a]}$ has invariant

$$\mathrm{Inv}\, B_{[a]} = \chi(\mathrm{Art}_{M/K}(a)).$$

Proof. Let $G = \mathrm{Gal}(M/K)$. Consider the cup product pairing

$$H^0(G, M^\times) \times H^2(G, \mathbb{Z}) \xrightarrow{\cup} H^2(G, M^\times) \xrightarrow[\cong]{\mathrm{Inv}} \mathbb{Q}/\mathbb{Z},$$

and let δ denote the connecting homomorphism in the long exact sequence

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}).$$

Then we have the following formula [Mil97, Prop. 4.1]:

(3.2) $$\chi(\mathrm{Art}(a)) = \mathrm{Inv}(a \cup \delta(\chi)).$$

We may explicitly compute a cochain representative for $\delta(\chi)$. Let

$$\widetilde{\chi} : G \to \mathbb{Q}$$

be the unique lift of χ such that the values of $\widetilde{\chi}$ lie in the interval $[0, 1)$. Then the cohomology element $\delta(\chi)$ is represented by the normalized $\mathbb{Z}$-valued 2-cochain

$$\phi(g_1, g_2) = \widetilde{\chi}(g_2) - \widetilde{\chi}(g_1 g_2) + \widetilde{\chi}(g_1).$$

In particular, we have

$$\phi(\sigma^i, \sigma^j) = 0 \quad \text{if } i + j < n,$$
$$\phi(\sigma^{n-1}, \sigma) = 1.$$

The cup product $a \cup \delta(\chi)$ is represented by the normalized $M^\times$-valued 2-cochain

$$\phi_a(g_1, g_2) = a^{\phi(g_1, g_2)}.$$

Associated to the 2-cochain ϕ_a is the extension

$$E_a = M^\times \times G$$

with multiplication

$$(x_1, g_1) \cdot (x_2, g_2) = (x_1 \cdot {}^{g_1}x_2 a^{\phi_{g_1,g_2}}, g_1 g_2)$$

We define

$$\widetilde{\sigma} = (1, \sigma) \in E_a$$

and compute:

$$\begin{aligned}
\widetilde{\sigma}^n &= (1,\sigma)^{n-1}(1,\sigma) \\
&= (1, \sigma^{n-1})(1,\sigma) \\
&= (a^{\phi(\sigma^{n-1},\sigma)}, \sigma^n) \\
&= (a, 1).
\end{aligned}$$

By (3.2), the associated central simple algebra has invariant

$$\mathrm{Inv}(B_{[a]}) = \chi(\mathrm{Art}(a)).$$

$\square$

Remark 3.3. The algebra $B_{[a]}$ admits the presentation (as a non-commutative K-algebra)

$$B_{[a]} = M\langle S \rangle / (S^n = a, Sx = x^\sigma S, x \in M).$$

Remark 3.4. The analog of Proposition 3.1 holds in the archimedean case as well. The only non-trivial case to discuss is the case where $K = \mathbb{R}$, $M = \mathbb{C}$, and $n = 2$. The character χ and the element σ are uniquely determined. The algebra $B_{[a]}$ is either $\mathbb{H}$ or $M_2(\mathbb{C})$, depending on whether a is negative or positive, that is to say, depending on the image of a under the Artin map

$$\mathrm{Art}_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^\times/N(\mathbb{C}^\times) \xrightarrow{\cong} \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2.$$

Example 3.5. Let $K = \mathbb{Q}_p$ and let $M = \mathbb{Q}_{p^n}$ denote the unique unramified extension of $\mathbb{Q}_p$ of degree n. We have.

$$\mathrm{Gal}(\mathbb{Q}_{p^n}/\mathbb{Q}_p) = C_n = \langle \sigma \rangle$$

where we fix a generator $\sigma = \mathrm{Art}(p)$. The Artin map is normalized so that σ is a lift of the Frobenius on $\mathbb{F}_{p^n}$. Then the central simple algebra $B_{[p^i]}$ has invariant i/n, and presentation:

$$B_{[p^i]} = \mathbb{Q}_{p^n}\langle S \rangle / (S^n = p^i, Sx = x^\sigma S, x \in \mathbb{Q}_{p^n}).$$

This may be compared to [Rav86, A2.2.16].

We end this section by giving a canonical presentation of $M_k(B_{[a]})$ given our presentation of $B_{[a]}$. Let

$$(M^\times)^k \cong \mathrm{Ind}_{C_n}^{C_{nk}} M^\times$$

be the induced C_{nk}-module. The isomorphism above is given so that for a generator σ' of C_{nk}, and $\sigma = (\sigma')^k$ a corresponding generator of the subgroup $C_k \leq C_{nk}$, we have, for $(m_i) \in (M^\times)^k$,

$$\sigma' \cdot (m_1, \ldots, m_k) = (m_2, \ldots, m_k, m_1^\sigma).$$

Then the algebra $M_k(B_{[a]})$ admits a presentation

$$M_k(B_{[a]}) \cong M\langle S \rangle / (S^{nk} = (a, \ldots, a), Sx = x^{\sigma'} S, x \in M^k).$$

The subring M^k is a maximal commutative subalgebra in $B_{[a]}$. Letting E' denote the normalizer of $(M^\times)^k \subseteq M_k(B_{[a]})^\times$, we have a short exact sequence

$$1 \to (M^\times)^k \to E' \to C_{nk} \to 1.$$

The extension E' is classified by the image of the cohomology class $[E_a]$ under the Shapiro isomorphism

$$H^2(C_n, M^\times) \cong H^2(C_{nk}, \mathrm{Ind}_{C_n}^{C_{nk}} M^\times) \cong H^2(C_{nk}, (M^\times)^k).$$

4. Elementary presentation of Hewett subgroups

In this section we explain how the theory of the previous section may be used to understand the finite subgroups of local division algebras studied by Hewett [Hew95].

Let B be a central division algebra over K. Throughout this paper, our technique for constructing finite subgroups of $B^\times$ will be construct extensions G of finite subgroups N of the group of units of a maximal subfield M containing K of the following form.

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & 1 \\
& & \big\downarrow\rotatebox{90}{$\subseteq$} & & \big\downarrow\rotatebox{90}{$\subseteq$} & & \big\downarrow\rotatebox{90}{$\subseteq$} & & \\
1 & \longrightarrow & M^\times & \longrightarrow & E & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & 1
\end{array}
$$

Here $E \le B^\times$ is the normalizer of $M^\times$, as in Section 3.

Let p be an odd prime, fix $r > 0$, and let

$$n = (p-1)p^{r-1}k$$

with k coprime to p. Let D be the central division algebra over $\mathbb{Q}_p$ of invariant $1/n$. Let $\mathcal{O}_D$ be the unique maximal order of D, and let

$$\mathbb{S}_n = \mathcal{O}_D^\times$$

denote the nth Morava stabilizer group.

Hewett [Hew95] showed that the isomorphism classes of finite subgroups of $\mathbb{S}_n$ are given by

$$\{G_\alpha : 0 \le \alpha \le r\}$$

such that G_α contains an element of maximal p-power order p^α. We give an elementary construction of these subgroups.

For $\alpha = 0$, the group G_0 is cyclic of order $p^n - 1$. Explicitly it can be taken to be the embedding

$$G_0 \cong \mathbb{F}_{p^n}^\times \hookrightarrow \mathbb{Z}_{p^n}^\times \hookrightarrow \mathcal{O}_D^\times.$$

Here $\mathbb{Z}_{p^n} = W(\mathbb{F}_{p^n})$ is the ring of integers of $\mathbb{Q}_{p^n}$.

For $0 < \alpha \leq r$, the group G_α is metacyclic, with presentation

$$G_\alpha = \langle a, b \; : \; a^{p^\alpha(p^m-1)} = 1, bab^{-1} = a^t, b^{p-1} = a^{p^\alpha} \rangle,$$

where

(1) t is an integer whose image in $(\mathbb{Z}/p^\alpha)^\times$ has order $p-1$, and
(2) $m = kp^{r-\alpha}$.

The group G_α fits into a short exact sequence

$$1 \to C_{p^\alpha(p^m-1)} \to G_\alpha \to C_{p-1} \to 1$$

where the group $C_{p^\alpha(p^m-1)}$ is generated by a, and the group C_{p-1} is generated by the image of b.

We now give an explicit, elementary embedding of G_α into $\mathcal{O}_D^\times$. Consider the following tower of abelian Galois extensions.

$$M = \mathbb{Q}_{p^m}(\zeta_{p^\alpha})$$
$$\Big| \, C_{p-1}$$
$$L = \mathbb{Q}_{p^m}[p^{\alpha-1}]$$
$$\Big| \, C_m \times \mathbb{Z}/p^{\alpha-1}$$
$$\mathbb{Q}_p$$

Note that $n = [M : \mathbb{Q}_p]$, so M embeds in D as a maximal subfield. Fix such an embedding. As in Section 3, there is an associated short exact sequence

(4.1) $$1 \to M^\times \overset{i}{\to} E \overset{j}{\to} \mathrm{Gal}(M/\mathbb{Q}_p) \to 1$$

where E is the normalizer of M in $D^\times$. The cohomology class $[E]$ of the extension (4.1) corresponds to the Brauer group class of D under the map

$$H^2(M/\mathbb{Q}_p) \to \mathrm{Br}(\mathbb{Q}_p)$$

and hence we have

$$\mathrm{Inv}([E]) = \frac{1}{(p-1)p^{\alpha-1}m} \in \mathbb{Q}/\mathbb{Z}.$$

Since we have $[L : \mathbb{Q}_p] = p^{\alpha-1}m$, we deduce that the image $[E']$ of $[E]$ under the map

$$H^2(M/\mathbb{Q}_p) \to H^2(M/L)$$

has invariant

$$\mathrm{Inv}([E']) = \frac{1}{p-1}.$$

The cohomology class $[E']$ classifies the extension E' given by the pullback:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & M^\times & \overset{i'}{\longrightarrow} & E' & \overset{j'}{\longrightarrow} & \mathrm{Gal}(M/L) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \Big\uparrow & & \\
1 & \longrightarrow & M^\times & \overset{i}{\longrightarrow} & E & \overset{j}{\longrightarrow} & \mathrm{Gal}(M/\mathbb{Q}_p) & \longrightarrow & 1
\end{array}
$$

Let $\omega \in \mathbb{Q}_{p^m} \subset L$ be a primitive $(p^m - 1)$st root of unity.

Lemma 4.2. The image of ω under the local Artin map

$$\mathrm{Art}_L : L^\times \to \mathrm{Gal}(M/L) = C_{p-1}$$

is a generator.

Proof. The following diagram summarizes the relationship of Art_L to $\mathrm{Art}_{\mathbb{Q}_p}$.

$$
\begin{array}{ccccccc}
\mu_{p^m-1} & \hookrightarrow & L^\times & \xrightarrow{\mathrm{Art}_L} & \mathrm{Gal}(M/L) & =\!=\!= & C_{p-1} \\
{\scriptstyle(-)^{p^{\alpha-1}}}\Big\downarrow{\scriptstyle\cong} & & \Big\downarrow{\scriptstyle N_{L/\mathbb{Q}_{p^m}}} & & \Big\downarrow & & \Big\downarrow \\
\mu_{p^m-1} & \hookrightarrow & \mathbb{Q}_{p^m}^\times & \xrightarrow{\mathrm{Art}_{\mathbb{Q}_{p^m}}} & \mathrm{Gal}(M/\mathbb{Q}_{p^m}) & =\!=\!= & (\mathbb{Z}/p^\alpha)^\times \\
{\scriptstyle(-)^{\frac{p^m-1}{p-1}}}\Big\downarrow & & \Big\downarrow{\scriptstyle N_{\mathbb{Q}_{p^m}/\mathbb{Q}_p}} & & \Big\downarrow & & \Big\downarrow \\
\mu_{p-1} & \hookrightarrow & \mathbb{Q}_p^\times & \xrightarrow{\mathrm{Art}_{\mathbb{Q}_p}} & \mathrm{Gal}(M/\mathbb{Q}_p) & =\!=\!= & C_m \times (\mathbb{Z}/p^\alpha)^\times
\end{array}
$$

The lemma follows from the fact that

$$\mathrm{Art}_{\mathbb{Q}_p}(\mu_{p-1}) = \mathrm{Gal}(M/L) \subset \mathrm{Gal}(M/\mathbb{Q}_p).$$

$\square$

Using Proposition 3.1, we deduce the following.

Corollary 4.3. The group E' contains an element b such that $j'(b)$ generates $\mathrm{Gal}(M/L)$, and $b^{p-1} = i'(\omega)$.

We deduce that there is a map of short exact sequences

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & C_{p^\alpha(p^m-1)} & \longrightarrow & G_\alpha & \longrightarrow & C_{p-1} & \longrightarrow & 1 \\
& & \Big\downarrow & & \Big\downarrow & & \Big\downarrow{\scriptstyle\cong} & & \\
1 & \longrightarrow & M^\times & \xrightarrow{i'} & E' & \xrightarrow{j'} & \mathrm{Gal}(M/L) & \longrightarrow & 1
\end{array}
$$

Since E' is a subgroup of E, which in turn is a subgroup of $D^\times$, we have given an embedding of G_α into $D^\times$.

5. Negative results

Let p be odd, and $n = (p-1)p^{\alpha-1}m$. In this section we will make the following observation, which shows that there are only a limited number of cases where all of G_α can be realized as an automorphism group of a height n mod p point of a unitary Shimura stack of type $(1, n-1)$.

Proposition 5.1. Suppose that there is a choice of F, GU, and K such that $\Gamma(K)$ is isomorphic to G_α. Then $p \le 7$ and $m = 1$.

Proof. Suppose that $G_\alpha = \Gamma(K)$ for some F, GU, and K. Then in particular G_α is a subgroup of the units of the algebra D of Section 2 of dimension n^2 over F. There is an element $a \in G_\alpha$ which has order $p^\alpha(p^m - 1)$. Therefore there is an embedding

$$M = F(\zeta_{p^\alpha(p^m-1)}) \hookrightarrow D^\times.$$

Depending on F, we have

$$[M : F] \in \{(p-1)p^{\alpha-1}\varphi(p^m - 1), (p-1)p^{\alpha-1}\varphi(p^m - 1)/2\}.$$

Here, φ is Euler's phi function. Since $[D : F] = n^2$, this is only possible if

$$\varphi(p^m - 1) \in \{m, 2m\}.$$

It is easily checked, using the inequality $\phi(n) \geq \sqrt{n/2}$ and checking a few cases, that this can only happen if $p \in \{3, 5, 7\}$ and $m = 1$. $\square$

6. Constructions of global division algebras

Having established our negative results, we now begin the work necessary to prove our positive results. We wish to construct explicit global division algebras which contain Hewett's subgroups in their groups of units. The tool we will use is the following global analog of Proposition 3.1.

Proposition 6.1. Let K be a finite extension of $\mathbb{Q}$, and suppose that M is a degree n cyclic extension of K. Fix an injection

$$\chi : \mathrm{Gal}(M/K) \hookrightarrow \mathbb{Q}/\mathbb{Z},$$

and let $\sigma \in \mathrm{Gal}(M/K)$ be the unique element satisfying

$$\chi(\sigma) = 1/n.$$

Then for each element $a \in K^\times$ there is an extension

$$1 \to M^\times \xrightarrow{i} E_a \xrightarrow{j} \mathrm{Gal}(M/K) \to 1$$

such that

  (1) there is a lift of σ to $\widetilde{\sigma} \in E$ such that $\widetilde{\sigma}^n = i(a)$, and
  (2) the corresponding central simple algebra $B_{[a]}$ has invariant

  $$\mathrm{Inv}_v B_{[a]} = \chi(\mathrm{Art}_{M/K}(a_v))$$

  at every place v of K.

Proof. The extension E_a may simply be defined by the presentation

$$E_a = M^\times \langle \widetilde{\sigma} \rangle / \langle \widetilde{\sigma}^n = a, \widetilde{\sigma}x = x^\sigma \widetilde{\sigma}, x \in M^\times \rangle.$$

We just need to compute the local invariants of the associated global division algebra. For a place v of K, we have

$$(B_{[a]})_v = B_{[a_v]},$$

thus we have $\mathrm{Inv}_v \, B_{[a_v]} = \mathrm{Inv} \, B_{[a_v]}$. Let v' be a place of M dividing v. We make use of the compatibility of the local and global Artin maps, given by the following diagram.

$$
\begin{array}{ccc}
K_v^\times & \xrightarrow{\mathrm{Art}_{M_{v'}/K_v}} & \mathrm{Gal}(M_{v'}/K_v) \\
\downarrow & & \downarrow \\
\mathbb{I}_K & \xrightarrow{\mathrm{Art}_{M/K}} & \mathrm{Gal}(M/K)
\end{array}
$$

Let k be the number of places of M dividing v. Then

$$[\mathrm{Gal}(M/K) : \mathrm{Gal}(M_{v'}/K_v)] = k.$$

The element σ^k generates $\mathrm{Gal}(M_{v'}/K_v) \cong C_m$, where $m = n/k$. We have $\chi(\sigma^k) = 1/m$. Since we have

$$M_v \cong \mathrm{Ind}_{C_m}^{C_n} M_{v'} \cong M_{v'}^k,$$

we may apply Proposition 3.1 (Remark 3.4 if v is archimedean) together with the discussion following Example 3.5 to deduce that

$$\mathrm{Inv} \, B_{[a_v]} = \chi(\mathrm{Art}_{M_{v'}/K_v}(a_v)) = \chi(\mathrm{Art}_{M/K}(a)).$$

$\square$

Fix an odd prime p. Let $n = (p-1)p^{\alpha-1}m$. If $p = 3$ we will assume that $m > 1$. The case of $p = 3$ and $m = 1$ will be treated separately. In this section we show that there exist some natural choices of global division algebras D with center F, a global CM field, in which G_α embeds, such that there exists a place $y|p$ of F with $\mathrm{Inv}_y \, D = 1/n$.

Let ω be a primitive $(p^m - 1)$st root of unity. Consider the tower of field extensions

$$
\begin{array}{c}
\mathbb{Q}(\omega) \\
C_m \Big| \\
F \qquad (\mathbb{Z}/(p^m-1))^\times \\
\Big| \\
\mathbb{Q}
\end{array}
$$

Here the Galois group $\mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$ is identified by the isomorphism

$$(\mathbb{Z}/(p^m - 1))^\times \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}),$$
$$s \mapsto ([s] : \omega \mapsto \omega^s),$$

the subgroup $C_m \leq (\mathbb{Z}/(p^m-1))^\times$ is the subgroup generated by the element p mod $p^m - 1$, and the field F is the subfield of $\mathbb{Q}(\omega)$ fixed by C_m. The key property of F is that p splits completely in it. The field F is a CM field. This is because $\mathbb{Q}(\omega)$ is a CM field, with conjugation given by the element $[-1] \in (\mathbb{Z}/(p^m - 1))^\times$, and for $p > 3$, or $p = 3$ and $m > 1$, the conjugation element $[-1]$ is not contained in the subgroup C_m generated by p. We will write

$$[-1](x) = \bar{x}$$

for $x \in \mathbb{Q}(\omega)$.

Let F^+ be the totally real subfield of F given by taking $[-1]$-fixed points. Let $\{x_i\}$ be the set of primes of F^+ dividing p. Each prime x_i splits as $y_i\bar{y}_i$ in F. The extension $\mathbb{Q}(\omega)/F$ is totally unramified at the primes y_i and $\bar{y}_i$. Let (t_i) be a finite sequence of integers coprime to $p^m - 1$, with $t_1 = 1$, such that the images $[t_i]$ in $(\mathbb{Z}/(p^m - 1))^\times \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ satisfy

$$[t_i](y_1) = y_i.$$

Theorem 6.2. Let D be a central division algebra over F whose non-trivial local invariants satisfy:

$$p^{\alpha-1}m \, \mathrm{Inv}_{y_i} D \cong t_i/(p-1) \in \mathbb{Q}/\mathbb{Z},$$
$$p^{\alpha-1}m \, \mathrm{Inv}_{\bar{y}_i} D \cong -t_i/(p-1) \in \mathbb{Q}/\mathbb{Z}.$$

Then the group G_α embeds in $D^\times$ as a maximal finite subgroup.

In order to prove Theorem 6.2, we will need to introduce some additional field extensions. Let ζ be a primitive (p^α)th root of unity, and consider the following field diagram.

$$
\begin{array}{ccc}
M = \mathbb{Q}(\omega,\zeta) & & \\
& \diagdown^{C_{p-1}} & \\
(\mathbb{Z}/p^\alpha)^\times \Big| & & \mathbb{Q}(\omega)[p^{\alpha-1}] = L \\
& \diagup_{\mathbb{Z}/p^{\alpha-1}} & \\
\mathbb{Q}(\omega) & & \\
C_m \Big| & & \\
F & & \\
2 \Big| & & \\
F^+ & & \\
\Big| & & \\
\mathbb{Q} & &
\end{array}
$$

The extension $M/\mathbb{Q}(\omega)$ is totally ramified over each of the primes y_i and $\bar{y}_i$. Let ω_{y_i} denote the image of ω under the inclusion

$$L^\times \hookrightarrow L_{y_i}^\times \hookrightarrow \mathbb{I}_L.$$

Define

$$\sigma = \mathrm{Art}_{M/L}(\omega_{y_1}) \in \mathrm{Gal}(M/L) \cong C_{p-1}.$$

We shall need the following lemma.

Lemma 6.3. We have

$$\mathrm{Art}_{M/L}(\omega_{y_i}) = \sigma^{t_i}.$$

The element σ (and hence each of the elements σ^{t_i}) is a generator of $\mathrm{Gal}(M/L)$.

Proof. Consider the following diagram.

$$
\begin{array}{ccccc}
\mathbb{I}_L & \xrightarrow{\mathrm{Art}_{M/L}} & \mathrm{Gal}(M/L) & = & C_{p-1} \\
{\scriptstyle N_{L/\mathbb{Q}(\omega)}}\downarrow & & \downarrow & & \downarrow \\
\mathbb{I}_{\mathbb{Q}(\omega)} & \xrightarrow{\mathrm{Art}_{M/\mathbb{Q}(\omega)}} & \mathrm{Gal}(M/\mathbb{Q}(\omega)) & = & (\mathbb{Z}/p^\alpha)^\times \\
{\scriptstyle N_{\mathbb{Q}(\omega)/F}}\downarrow & & \downarrow & & \downarrow \\
\mathbb{I}_F & \xrightarrow{\mathrm{Art}_{M/F}} & \mathrm{Gal}(M/F) & = & (\mathbb{Z}/p^\alpha)^\times \times C_m \\
{\scriptstyle N_{F/\mathbb{Q}}}\downarrow & & \downarrow & & \downarrow \\
\mathbb{I}_{\mathbb{Q}} & \xrightarrow{\mathrm{Art}_{M/\mathbb{Q}}} & \mathrm{Gal}(M/\mathbb{Q}) & = & (\mathbb{Z}/p^\alpha)^\times \times (\mathbb{Z}/p^m - 1)^\times
\end{array}
$$

Viewing $\sigma = \mathrm{Art}_{M/L}(\omega_{y_1})$ as an element of $\mathrm{Gal}(M/\mathbb{Q})$ under the inclusion

$$\mathrm{Gal}(M/L) \hookrightarrow \mathrm{Gal}(M/\mathbb{Q}),$$

it suffices to show that

$$\mathrm{Art}_{M/\mathbb{Q}}(N_{L/\mathbb{Q}}(\omega_{y_i})) = \sigma^{t_i}.$$

Note that by the definition of σ, we have

$$\mathrm{Art}_{M/\mathbb{Q}}(N_{L/\mathbb{Q}}(\omega_{y_1})) = \sigma.$$

We compute:

$$
\begin{aligned}
N_{L/\mathbb{Q}}(\omega_{y_i}) &= N_{F/\mathbb{Q}}N_{\mathbb{Q}(\omega)/F}N_{L/\mathbb{Q}(\omega)}(\omega_{y_i}) \\
&= N_{F/\mathbb{Q}}N_{\mathbb{Q}(\omega)/F}(\omega_{y_i}^{p^{\alpha-1}}) \\
&= N_{F/\mathbb{Q}}\left(\omega_{y_i}^{\frac{p^{m-1}-1}{p-1}p^{\alpha-1}}\right) \\
&= N_{F/\mathbb{Q}}(\omega_{y_1})^{\frac{p^{m-1}-1}{p-1}p^{\alpha-1}t_i}.
\end{aligned}
$$

Here, the last norm computation comes from the fact that under the composite

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q}) \xrightarrow{\cong} \mathrm{Emb}(F, \mathbb{Q}_p)$$

the element $[t_i]$ maps ω to ω^{t_i}. We have shown that

$$N_{L/\mathbb{Q}}(\omega_{y_i}) = N_{L/\mathbb{Q}}(\omega_{y_1})^{t_i}.$$

Now apply $\mathrm{Art}_{M/\mathbb{Q}}$ to the equation above. $\qquad\square$

Proof of Theorem 6.2. Since G_α is maximal in $D_{y_1}^\times$, if it embeds in $D^\times$, it must be maximal in $D^\times$. We therefore just must show it embeds.

Since each prime y_i does not split in M, we have $[L_{y_i} : F_{y_i}] = p^{\alpha-1}m$, and $[M_{y_i} : F_{y_i}] = (p-1)p^{\alpha-1}m$, which implies that we have

$$
\begin{aligned}
\mathrm{Inv}_{y_i} L \otimes_F D &= t_i/(p-1), \\
\mathrm{Inv}_{\bar{y}_i} L \otimes_F D &= -t_i/(p-1), \\
\mathrm{Inv}_{y_i} L \otimes_F D &= 0, \\
\mathrm{Inv}_{\bar{y}_i} L \otimes_F D &= 0.
\end{aligned}
$$

In particular, M splits D, and therefore M embeds into D as a maximal commutative subfield [Swa70, Thm. 9.18]. Since M embeds into D, the element $[D] \in \mathrm{Br}(F)$ is in the image of the map

$$H^2(M/F) \hookrightarrow \mathrm{Br}(F),$$

and is therefore corresponds to an extension

$$1 \to M^\times \to E \to (\mathbb{Z}/p^\alpha)^\times \times C_{p^m-1} \to 1.$$

We let $[E]$ denote the corresponding cohomology class in $H^2(M/F)$. Using the diagram

$$
\begin{array}{ccc}
H^2(M/F) & \hookrightarrow & \mathrm{Br}(F) \\
{\scriptstyle \mathrm{Res}}\downarrow & & \downarrow \\
H^2(M/L) & \hookrightarrow & \mathrm{Br}(L)
\end{array}
$$

together with with the local invariants of $L \otimes_F D$ computed above, we deduce that the cohomology class

$$\mathrm{Res}[E] \in H^2(M/L)$$

has

$$\mathrm{Inv}_{y_i}[E] = t_i/(p-1),$$
$$\mathrm{Inv}_{\bar{y}_i}[E] = -t_i/(p-1).$$

The class $\mathrm{Res}[E]$ is represented by the pullback E' in the following diagram.

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & M^\times & \xrightarrow{i'} & E' & \xrightarrow{j'} & C_{p-1} & \longrightarrow & 1 \\
& & \| & & \downarrow & & \hookuparrow & & \\
1 & \longrightarrow & M^\times & \xrightarrow{i} & E & \xrightarrow{j} & (\mathbb{Z}/p^\alpha)^\times \times C_{p^m-1} & \longrightarrow & 1
\end{array}
$$

Let

$$\sigma = \mathrm{Art}_{M/L}(\omega_{y_1}) \in \mathrm{Gal}(M/L) \cong C_{p-1}$$

be the generator considered earlier. Choose

$$\chi : \mathrm{Gal}(M/L) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

so that $\chi(\sigma) = 1/(p-1)$. We compute (using Lemma 6.3)

$$\chi(\mathrm{Art}_L(\omega_{y_i})) = t_i/(p-1).$$

By Proposition 6.1, the extension E' contains an element T so that $j'(T) = \sigma$ and $T^{p-1} = i'(\omega)$. We deduce that there is a map of short exact sequences

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & C_{p^\alpha(p^m-1)} & \longrightarrow & G_\alpha & \longrightarrow & C_{p-1} & \longrightarrow & 1 \\
& & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & M^\times & \longrightarrow & E' & \longrightarrow & C_{p-1} & \longrightarrow & 1
\end{array}
$$

which maps a to $\omega\zeta$ and b to T. Since E' is contained in E, which in turn is a subgroup of $D^\times$, we have embedded G_α in $D^\times$. $\square$

Remark 6.4. If $p = 3$ and $m = 1$, then the proof of Theorem 6.2 goes through verbatim with the following modifications. Take F to be *any* quadratic imaginary extension in which the prime 3 splits. Replace all occurrences of $\mathbb{Q}(\omega)$ with F, and replace the element ω with -1. In this case, $L = F[3^{\alpha-1}]$, and $M = F(\zeta_{3^\alpha})$.

7. Involutions

Let $n = (p-1)p^\alpha m$, and let F, L, M, ω, ζ, σ, and D be as in Section 6. Let $m \mapsto \bar{m}$ denote the conjugation on the CM field M. This conjugation automorphism is characterized by

$$\bar{\omega} = \omega^{-1},$$
$$\bar{\zeta} = \zeta^{-1}.$$

Let D' be the division algebra associated to the extension

$$1 \to M^\times \to E' \to C_{p-1} \to 1$$

where $E' = E_\omega$, in the notation of Proposition 6.1. The algebra D' is the subalgebra of D which centralizes the subfield L under the fixed embedding $M \subseteq D$. Explicitly, D' admits the presentation

(7.1) $$D' = M\langle T\rangle/(T^{p-1} = \omega, Tx = x^\sigma T, x \in M).$$

We will express elements of D' as

$$\sum_{i=0}^{p-2} x_i T^i$$

for $x_i \in M$.

In this section we will show that D' admits a positive involution of the second kind so that the subgroup G_α is contained in the unitary group associated to the involution. The involution we are interested in is given by the following lemma.

Lemma 7.2. There is a unique involution $\dagger'$ on D' satisfying:

(1) $x^{\dagger'} = \bar{x}, \qquad x \in M,$
(2) $T^{\dagger'} = T^{-1} = \omega^{-1}T^{p-2}.$

Proof. We just need to check that the relations in the presentation (7.1) are compatible with $\dagger'$. We check

$$(Tx)^{\dagger'} = (x^\sigma T)^{\dagger'} = T^{\dagger'}(x^\sigma)^{\dagger'} = \omega^{-1}T^{p-2}\bar{x}^\sigma = \bar{x}\omega^{-1}T^{p-2} = x^{\dagger'}T^{\dagger'}$$

and

$$(T^{p-1})^{\dagger'} = (\omega^{-1}T^{p-2})^{p-1} = \omega^{p-2} = \bar{\omega} = \omega^{\dagger'}.$$

$\square$

By definition, the involution $\dagger'$ is an involution of the second kind.

Lemma 7.3. The involution $\dagger'$ is positive.

Proof. Let $x = \sum_{i=0}^{p-2} x_i T^i$ be a non-zero element of D'. We must show that $\mathrm{Tr}_{D/L}(xx^{\dagger'})$ is a positive real number under all of the complex embeddings of L.

For a general $y = \sum y_i T^i$ in D', we consider the M-linear transformation:
$$R_y : D' \to D',$$
$$z \mapsto z \cdot y.$$

Giving D' the M-basis $\{T^i\}_{i=1}^{p-2}$, we may represent R_y by the following matrix.

$$R_y = \begin{bmatrix} y_0 & \omega^{-1}y_{p-2}^{\sigma} & \omega^{-1}y_{p-3}^{\sigma^2} & \cdots & \omega^{-1}y_1^{\sigma^{p-2}} \\ y_1 & y_0^{\sigma} & \omega^{-1}y_{p-2}^{\sigma^2} & & \vdots \\ y_2 & y_1^{\sigma} & y_0^{\sigma^2} & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ y_{p-2} & y_{p-3}^{\sigma} & \cdots & \cdots & y_0^{\sigma^{p-2}} \end{bmatrix}$$

In particular, we find that
$$\mathrm{Tr}_{D'/L}(y) = \mathrm{Tr}_{M/L}(y_0).$$

We compute
$$xx^{\dagger'} = (x_0 + x_1 T + \cdots + x_{p-2}T^{p-2})(\bar{x}_0 + \omega^{-1}T^{p-2}\bar{x}_1 + \cdots + \omega^{-1}T\bar{x}_{p-2})$$
$$= (x_0\bar{x}_0 + x_1\bar{x}_1 + \cdots + x_{p-2}\bar{x}_{p-2}) + \text{terms involving } T.$$

We deduce that
$$\mathrm{Tr}_{D'/L}(xx^{\dagger'}) = \mathrm{Tr}_{M/L}(x_0\bar{x}_0 + x_1\bar{x}_1 + \cdots + x_{p-2}\bar{x}_{p-2}),$$

under each complex embedding of L, is a sum of positive real numbers, hence positive. $\square$

For a central simple algebra B over a CM field K with involution $*$ of the second kind, we shall denote the associated unitary and unitary similitude groups $U_{(B,*)}$ and $GU_{(B,*)}$. These algebraic groups (over $\mathbb{Q}$) are given explicitly by
$$U_{(B,*)}(\mathbb{Q}) = \{(B \times_{\mathbb{Q}} R)^{\times} : x^*x = 1\},$$
$$GU_{(B,*)}(\mathbb{Q}) = \{(B \times_{\mathbb{Q}} R)^{\times} : x^*x = R^{\times}\},$$

for every $\mathbb{Q}$-algebra R.

Lemma 7.4. For each element $g \in G_{\alpha} \subset (D')^{\times}$, we have
$$g \in U_{(D',\dagger')}(\mathbb{Q}).$$

Proof. We just need to check on generators. The subgroup G_{α}, as constructed in Theorem 6.2, is generated by T and ω. We have
$$T^{\dagger}T = \omega^{-1}T^{p-2}T = \omega^{-1}\omega = 1$$
and
$$\omega^{\dagger}\omega = \bar{\omega}\omega = \omega^{-1}\omega = 1.$$
$\square$

Proposition 7.5. There exists a positive involution of the second kind † on D which extends the involution †$'$ on D'. For any such extension †, we have

$$G_\alpha \subseteq U_{(D,\dagger)}(\mathbb{Q}).$$

Proof. It suffices to show that the involution †$'$ on D' extends as a positive involution of the second kind to D. This is established by duplicating the argument of [Kot92, Lem. 9.2]. The second statement is immediate from Lemma 7.4.   □

8. POSITIVE RESULTS

Let p be an odd prime. Proposition 5.1 indicates that if G_α is going to be the automorphism group of a mod p point of the height n locus of one of the unitary Shimura stacks of type $(1, n-1)$ under consideration, with $n = (p-1)p^{\alpha-1}m$, then $p \leq 7$ and $m = 1$.

In this section we will assume $p \in \{3, 5, 7\}$, and that $n = (p-1)p^{r-1}$, and show that the finite group G_r is the automorphism group of such a mod p point of a Shimura stack.

For $p \in \{5, 7\}$, let $F = \mathbb{Q}(\omega)$, where, as in Section 6, ω is a $(p-1)$st root of unity. For $p = 3$, we can choose F more freely: for concreteness choose $F = \mathbb{Q}(\sqrt{-2})$ in this case. Note that for these primes, F is a quadratic imaginary extension of $\mathbb{Q}$ which splits at p. In each of these cases, $F = \mathbb{Q}(\delta)$ where, for $p = 3, 5, 7$ we have $\delta = \sqrt{-2}, \sqrt{-1}, \sqrt{-3}$, respectively.

We fix the rest of our defining Shimura data as follows:

$$
\begin{aligned}
B &= M_n(F), \\
* &= \text{conjugate transpose involution on } B, \\
\mathcal{O}_{B,(p)} &= M_n(\mathcal{O}_{F,(p)}), \\
V &= B,
\end{aligned}
$$

$$\langle x, y \rangle = \text{Tr}_{F/\mathbb{Q}} \text{Tr}_{B/F}(x\beta y^*), \quad \text{for} \quad \beta = \begin{bmatrix} 2\delta & & & \\ & -2\delta & & \\ & & \ddots & \\ & & & -2\delta \end{bmatrix} \in B.$$

Thus, the pairing $\langle -, - \rangle$ is the alternating hermitian form associated (see [BLa, Lem. 5.1.2]) to the symmetric hermitian form on F^n given by the matrix

$$\xi = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{bmatrix}.$$

We denote

$$C = B^{op} = \text{End}_B(V)$$

and let ι be the involution on C induced from $\langle -, - \rangle$. Let GU be the associated unitary similitude group over $\mathbb{Q}$, with R-points

$$GU(R) = \{g \in C \otimes_{\mathbb{Q}} R \,:\, g^\iota g \in R^\times\}.$$

The goal of this section is to prove the following theorem.

Theorem 8.1. For $p \in \{3, 5, 7\}$, and the group GU described above, there exists a maximal compact open subgroup

$$K \subset GU(\mathbb{A}^{p,\infty})$$

such that in the associated Shimura stack $\mathrm{Sh}(K)$, there exists a point

$$\mathbf{A}_0 = (A_0, i_0, \lambda_0, [\eta_0]_K) \in \mathrm{Sh}(K)^{[n]}(\bar{\mathbb{F}}_p)$$

with

$$\mathrm{Aut}(\mathbf{A}_0) \cong G_r.$$

Under the map

$$\mathrm{Aut}(\mathbf{A}_0) \to \mathrm{Aut}(\epsilon\mathbf{A}_0(u)) \cong \mathbb{S}_n$$

the group G_r embeds as a maximal finite subgroup with maximal p-order.

Remark 8.2. Theorem 8.1 merely asserts that there exists a point with the desired automorphism group. It is not, in general, the case that every mod p point of the height n locus has isomorphic automorphism group. The desired mod p point is globally determined by the (rather arbitrary) local choices of the maximal compact subgroups K_ℓ of (8.9).

In order to prove Theorem 8.1, we will need several lemmas. Let K_0 be any compact open subgroup of $GU(\mathbb{A}^{p,\infty})$, and choose an $\bar{\mathbb{F}}_p$-point

$$\mathbf{A}_0 = (A_0, i_0, \lambda_0, [\eta_0]_{K_0}) \in \mathrm{Sh}(K_0)^{[n]}(\bar{\mathbb{F}}_p).$$

(By [BLa, Prop. 14.3.2], the set $\mathrm{Sh}(K_0)^{[n]}(\bar{\mathbb{F}}_p)$ is non-empty.) Let $(D, \dagger)$ be the corresponding quasi-endomorphism ring with Rosati involution, as in Section 2.

Let ζ, M, and L be as in Section 6. Let L^+ be the fixed field under the CM-involution of L. Note that in the notation of Section 6, $F = \mathbb{Q}(\omega)$ ($F = \mathbb{Q}(\sqrt{-2})$ if $p = 3$), $m = 1$, and $\alpha = r$. Furthermore, $L = F[p^{r-1}]$ and $L^+ = \mathbb{Q}[p^{r-1}]$. Note that the division algebra D satisfies the hypotheses of Theorem 6.2, and therefore there exists an embedding of G_r in D. We need to show that an embedding exists so that there is a containment

$$G_r \subset GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}),$$

and that there exists a compact open subgroup $K \subset GU(\mathbb{A}^{p,\infty})$, so that there is a containment

$$G_r \subset \Gamma(K) = GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}) \cap K = \mathrm{Aut}(A_0, i_0, \lambda_0, [\eta_0]_K).$$

We pause to recollect the essential facts concerning the classification of involutions of the second kind on a central simple algebra E over K, a quadratic extension of K_0, a local or global number field (see, for instance, [Sch85], or [BLa, Ch. 5], though

the latter only treats the case where $K_0 = \mathbb{Q}$ or $\mathbb{Q}_v$). Suppose that $\dim_K E = d^2$. Fix a positive involution $*$ on E of the second kind. There are bijections

$$H^1(K_0, GU_{(E,*)}) \cong \left\{ \begin{array}{c} \text{Similitude classes of non-degenerate} \\ *\text{-hermitian }*\text{-symmetric forms:} \\ E \otimes E \to K \end{array} \right\}$$

$$\cong \left\{ \begin{array}{c} \text{Equivalence classes of involutions} \\ \text{of the second kind on } E \end{array} \right\}.$$

In the case where K is a global field, if d is even, the group $GU_{(E,*)}$ satisfies the Hasse principle [Kot92, Sec. 7]: the map

$$H^1(K_0, GU_{(E,*)}) \to \prod_v H^1((K_0)_v, GU_{(E,*)})$$

is an injection, and an involution $(-)^\#$ of the second kind on E is determined by the involution it induces on E_v for each place v. Using the Noether-Skolem theorem and Hilbert Theorem 90 to express an involution $(-)^\#$ on E by

$$x^\# = \xi^{-1} x^* \xi$$

for $\xi \in E$ with $\xi^* = \xi$, the associated hermitian form is given by

$$(x, y) = \mathrm{Tr}_{E/K}(x \xi y^*).$$

More precisely, the involution is determined by the discriminant of the associated hermitian form

$$\mathrm{disc}_{(-,-)} := N_{E/F}(\xi) \in K_0^\times / N(K^\times)$$

and the (unordered) signature of the form $(-,-)$ at each of the real places of K_0 which do not split in K. The local Galois cohomology $H^1((K_0)_v, GU_{(E,*)})$ is only nontrivial for places v of K_0 which do not split in K.

Assume now that K is a non-archimedean local number field, and that $E \cong M_d(K)$. If $d > 2$, the existence of the involution $*$ actually forces E to be split. Assume that $*$ is the involution on $M_d(K)$ given by conjugate transpose. The associated hermitian form $(-,-)$ may be regarded as the hermitian form on K^d, associated to the matrix ξ. The isometry class of $(-,-)$ is classified by its discriminant

$$\mathrm{disc}_{(-,-)} := \det \xi \in K_0^\times / N(K^\times) \cong \mathbb{Z}/2.$$

If d is odd, any two hermitian forms lie in the same similitude class (see [BLa, Cor. 3.5.4]). If d is even, then if two forms are in the same similitude class, they are isometric. Therefore, the invariant disc is an invariant of the involution associated to the hermitian form. When d is even, the similitude class of the form is determined by its Witt index, the dimension of a maximal totally isotropic subspace of K^d for $(-,-)$. We have [BLa, Sec. 12.3]

$$\mathrm{disc}_{(-,-)} = (-1)^{d/2} \in K_0^\times / N(K^\times) \Leftrightarrow \text{Witt index} = d/2,$$
$$\mathrm{disc}_{(-,-)} \neq (-1)^{d/2} \in K_0^\times / N(K^\times) \Leftrightarrow \text{Witt index} = d/2 - 1.$$

If the form arises from the completion of a global form, the local discriminant is simply the image of the global discriminant under the completion map, *provided the global involution $*$ is equivalent to conjugate transpose after completion.*

The following lemmas give some useful local presentations of the conjugate transpose involution on a local matrix algebra. We will use these lemmas later in this section to compute the local invariants of the involution $\dagger'$ constructed in Lemma 7.2.

Lemma 8.3. Let K/K_0 be an unramified quadratic extension of local nonarchimedean number fields. Suppose that K'/K is the unramified extension of degree n, so that $\mathrm{Gal}(K'/K) = C_n = \langle \sigma \rangle$. Let $\overline{(-)}$ denote the unique element of $\mathrm{Gal}(K'/K_0) \cong C_{2n}$ of order 2. Let E be the (split) central simple algebra over K associated to the split exact sequence

$$1 \to (K')^\times \to (K')^\times \rtimes C_n \to C_n \to 1.$$

Let $\#$ be the unique involution on E such that

$$x^\# = \bar{x} \qquad \text{for } x \in K',$$
$$\sigma^\# = \sigma^{-1}.$$

Then the pair $(E, \#)$ is isomorphic to $M_n(K)$ with the conjugate-transpose involution.

Proof. Observe that there is a natural way to identify E with $\mathrm{End}_K(K')$: embed K' in $\mathrm{End}_K(K')$ via its action by multiplication, and regard σ as a K-linear endomorphism of K'. Consider the hermitian form

$$(-, -) : K' \times K' \to K,$$
$$(x, y) \mapsto \mathrm{Tr}_{K'/K}(x\bar{y}).$$

Observe that for $a, x, y \in K'$, we have

$$(ax, y) = (x, \bar{a}y)$$
$$(\sigma(x), y) = (x, \sigma^{-1}(y))$$

which implies that the involution $\#$ on E is precisely the involution associated to the form $(-, -)$. We need to show that $\mathrm{disc}_{(-,-)} \equiv 1 \in K_0^\times / N(K^\times)$.

Choose a basis $(e_1, \ldots, e_n)$ of K'/K so that the hermitian form $(-, -)$ is represented by a matrix of the form

$$\xi = \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix}$$

for $a_i \in K_0^\times$. Consider the symmetric bilinear form

$$\mathrm{Tr}_{K/K_0}(-, -) : K' \times K' \to K_0.$$

Write $K = K_0(\delta)$ for $\delta^2 = -d \in K_0$. With respect to the basis

$$(e_1, \delta e_1, e_2, \delta e_2, \ldots, e_n, \delta e_n)$$

the symmetric bilinear form $\mathrm{Tr}_{K/K_0}(-, -)$ is represented by the following matrix.

$$\xi_0 = \begin{bmatrix} 2a_1 & & & & & \\ & 2da_1 & & & & \\ & & \ddots & & & \\ & & & 2a_n & \\ & & & & 2da_n \end{bmatrix}$$

We deduce that

$$\det \xi_0 = (4d)^n \det \xi.$$

Since K/K_0 is unramified, $d \equiv 1$ in $K_0^\times/N(K^\times)$. Since $4 \in N(K^\times) \subset K_0^\times$, we deduce that

$$\mathrm{disc}_{(-,-)} = \det \xi \equiv \det \xi_0 \in K_0^\times/N(K^\times).$$

Now, the trace pairing

$$(-,-)_{K'/K_0} : K' \times K' \to K_0,$$
$$(x,y) \mapsto \mathrm{Tr}_{K'/K_0}(xy)$$

is represented by the matrix $\xi_0 \cdot c$ where c is the K_0-linear endomorphism of K' corresponding to $\overline{(-)}$. Note that since $c^2 = \mathrm{Id}$, we have $\det c \in \{\pm 1\}$. Since K/K_0 is unramified, Corollary 1 of Section III.5 of [Ser79] implies that

$$\det(\xi_0 \cdot c) \not\equiv \pi \in K_0^\times/(K_0^\times)^2,$$

where π is a uniformizer of K_0. Since K/K_0 is unramified, π generates the group $K_0^\times/N(K^\times)$ and we deduce that

$$\mathrm{disc}_{(-,-)} \equiv \det(\xi \cdot c) \equiv 1 \in K_0^\times/N(K^\times),$$

as desired. $\square$

Lemma 8.4. Let K_0, K, K', n, $\overline{(-)}$, and σ be as in Lemma 8.3. Let E_m be the (split) central simple algebra over K associated to the split exact sequence

$$1 \to ((K')^\times)^m \to ((K')^\times)^m \rtimes C_{nm} \to C_{nm} \to 1,$$

where C_{nm} acts on $((K')^\times)^m$ through the isomorphism

$$((K')^\times)^m \cong \mathrm{Ind}_{C_n}^{C_{mn}}(K')^\times,$$

as in the discussion following Example 3.5. Let S be an element of E_m corresponding to a generator of C_{nm}. Let $\#_m$ be the unique involution on E_m such that

$$(x_1,\ldots,x_m)^{\#_m} = (\bar{x}_1,\ldots,\bar{x}_m) \qquad \text{for } (x_i) \in (K')^m,$$
$$S^{\#_m} = S^{-1}.$$

Then the pair $(E_m, \#_m)$ is isomorphic to $M_{nm}(K)$ with the conjugate-transpose involution.

Proof. Note that the case of $m = 1$ is precisely the content of Lemma 8.3. Using Lemma 8.3, fix an isomorphism

$$(E_1, \#_1) \cong (M_n(K), (-)^*),$$

where $(-)^*$ denotes conjugate-transpose. Under this isomorphism, we may represent elements of K', as well as σ, as giving $n \times n$ matrices. Consider the diagonal embedding

$$((K')^\times)^m \hookrightarrow M_{nm}(K)^\times,$$
$$(x_1,\ldots,x_m) \mapsto \begin{bmatrix} x_1 & & \\ & \ddots & \\ & & x_m \end{bmatrix}$$

where here, and elsewhere in this proof, $nm \times nm$ matrices are represented by $m \times m$ matrices of blocks, with each block corresponding to an $n \times n$ matrix. Under this embedding, the conjugate transpose involution $(-)^*$ on $M_{nm}(K)$ restricts to

$$(x_1, \ldots, x_m) \mapsto (\bar{x}_1, \ldots, \bar{x}_m).$$

We may extend this embedding to an embedding

$$((K')^\times)^m \rtimes C_{nm} \hookrightarrow (M_{nm}(K))^\times$$

by sending S to the matrix

$$\begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ \sigma & & & & 0 \end{bmatrix}.$$

It is easily checked that the transpose of this matrix is the matrix corresponding to S^{nm-1}.   □

We now determine the invariants of our involution ι on $C \cong M_n(F)$ which defines the group GU.

Lemma 8.5. For each prime ℓ which does not split in F, the Witt index of $GU(\mathbb{Q}_\ell)$ is $n/2$, except in the case of $p = 5$ and $\ell = 2$, for which the Witt index is $n/2 - 1$.

Proof. The discriminant of ι is $(-1)^{n-1}$. Since

$$n = (p-1)p^{r-1},$$

and p is odd, $n - 1$ is odd, and disc $= -1$. If ℓ is unramified, then disc is zero in $\mathbb{Q}_\ell / N(F_\ell^\times)$. If $p = 3, 7$, the quantity $(p-1)/2$ is odd, and hence disc $= (-1)^{n/2}$. However, if $p = 5$, $n/2$ is even, and disc $\neq (-1)^{n/2}$.   □

Lemma 8.6. There exists an embedding $M \hookrightarrow D$ so that † restricts to the conjugation on M.

Proof. By [PR, Thm. 3.2], it suffices to prove that there are local embeddings

$$(M_v, \overline{(-)}) \hookrightarrow (D_v, \dagger)$$

for each place v of $\mathbb{Q}$. Since M is a CM field, the case where v is the infinite place is easily verified. If v is a finite place which splits in F, the local embedding follows from [PR96, Prop. A.3]. If v is finite and unramified in F, then the isomorphism

$$(C_v, \iota) \cong (D_v, \dagger)$$

induced from the level structure η_0 implies that, using Lemma 8.5, except in the case of $p = 5$ and $\ell = 2$, the Witt index of † is $n/2$. The local embeddability of $(M_v, \overline{(-)})$ then follows from [PR94, p. 340].

We are left with the case of $p = 5$ and $\ell = 2$. In this case, $F = \mathbb{Q}(i)$ and the Witt index of † is $n/2 - 1$. It suffices to prove that $(M, \overline{(-)})$ embeds in $(M_n(F_2), \tau)$ for any involution τ of Witt index $n/2 - 1$, since Witt index determines the equivalence

class of an involution. Let τ_0 be an involution of $M_n(F_2)$ with Witt index $n/2$, and use [PR94, p. 340] to produce an embedding

$$(M_2, \overline{(-)}) \hookrightarrow (M_n(F_2), \tau_0).$$

Since $n \equiv 0 \mod 4$, we deduce that

$$\mathrm{disc}_{\tau_0} = 1 \in \mathbb{Q}_2^\times / N(F_2^\times) = (\mathbb{Z}/4)^\times.$$

Define, for $x \in M_n(F_2)$

$$x^\tau = \xi^{-1} x^{\tau_0} \xi$$

for

$$\xi = (1+i)\zeta + (1-i)\zeta^{-1} \in M_2 \subset M_n(F_2).$$

Note that since we have

$$\xi^{\tau_0} = \overline{\xi} = \xi,$$

the transformation $(-)^\tau$ defines an involution of the second kind on $M_n(F_2)$. Since $\xi \in M$, we easily see that $x^\tau = \overline{x}$ for $x \in M$. In particular, we have an embedding

$$(M_2, \overline{(-)}) \hookrightarrow (M_n(F_2), \tau).$$

Using the fact that $n \equiv 4 \mod 8$, together with $(i+1)^2 = 2i$, we compute

$$\mathrm{disc}_\tau = \det(\xi)$$
$$= N_{M_2/F_2}((1+i)\zeta + (1-i)\zeta^{-1})$$
$$= -2^{n/2}.$$

Since $2 = N_{F_2/\mathbb{Q}_2}(1+i)$, we deduce that

$$-2^{n/2} \equiv -1 \in \mathbb{Q}_2^\times / N(F_2^\times)$$

and therefore that the Witt index of τ is $n/2 - 1$. We have therefore produced the desired local embedding. $\qquad\square$

Fix an embedding

$$(M, \overline{(-)}) \hookrightarrow (D, \dagger)$$

as in Lemma 8.6. Let $D' \subset D$ be the subalgebra which centralizes the subfield $L \subset M$. Since $\dagger$ restricts to an involution of M, we deduce that $\dagger$ restricts to D'. Let $\dagger'$ be the involution of D' constructed in Lemma 7.2.

Lemma 8.7. The involution $\dagger$ restricted to D' is equivalent to the involution $\dagger'$.

In order to prove Lemma 8.7, we shall need the following.

Lemma 8.8. Let v be a finite place of L^+ which is inert in L. Then we have

$$\mathrm{disc}_v(\dagger') \equiv 1 \in (L_v^+)^\times / N(L_v^\times).$$

Proof. Let (v_i) be the collection of places of M which lie over v, so that M_v splits into a product

$$M_v = \prod_i M_{v_i}$$

of (isomorphic) field extensions of L_v. Since v is inert in L, v cannot lie over p, and therefore each of the extensions M_{v_i}/L_v is unramified. Let $d = [M_{v_i} : L_v]$. The division algebra D'_v corresponds to the extension

$$1 \to \prod_i M_{v_i}^\times \to E'_v \to C_{p-1} \to 1$$

where there exists an element $T \in E'_v$ which maps to a generator σ of C_{p-1}, and for which

$$T^{p-1} = (\omega_{v_i}) \in \prod M_{v_i}^\times.$$

Note ω_{v_i} is contained in the subfield $L_v \subset M_{v_i}$, so we will simply denote the corresponding element $\omega_v \in L_v$. Since M_{v_i}/L_v is inert, the element ω_v must lie in $N(M_{v_i}^\times)$. Let $\beta_1 \in M_{v_1}$ be chosen such that

$$N_{M_{v_1}/L_v}(\beta_1) = \omega_{v_1}.$$

We then have

$$N_{M_{\sigma^i v_1}/L_v}(\beta_1^{\sigma^i}) = \omega_{\sigma^i v_1}.$$

Set $\beta = (\beta_1, 1, \ldots, 1) \in \prod M_{v_i}^\times$. Define

$$S = \beta^{-1} T \in D'.$$

We compute

$$\begin{aligned}
S^{p-1} &= \beta^{-1} T \beta^{-1} T \cdots \beta^{-1} T \\
&= \beta^{-1} \beta^{-\sigma} \cdots \beta^{-\sigma^{p-2}} T^{p-1} \\
&= \omega_v^{-1} \omega_v \\
&= 1.
\end{aligned}$$

The effect of the involution $\dagger'$ on S is given by

$$\begin{aligned}
S^{\dagger'} &= (\beta^{-1} T)^{\dagger'} \\
&= \omega_v^{-1} T^{p-2} \bar{\beta}^{-1} \\
&= S^{p-2} \beta^{-1} \bar{\beta}^{-1}.
\end{aligned}$$

By Lemma 8.4, to finish the proof, we must show that the element $\beta_1 \in M_{v_1}$ may be chosen such that $\bar{\beta}_1 = \beta_1^{-1}$. Let t and ℓ be such that $L_v = \mathbb{Q}_{\ell^t}$. The extension M_{v_1} must be isomorphic to $\mathbb{Q}_{\ell^{dt}}$. Since ω_v is a root of unity, it must be contained in

$$\mu_{\ell^t - 1} \subset L_v^\times.$$

Under the norm map

$$N_{M_{v_1}/L_v} : M_{v_1}^\times \to L_v^\times$$

the subgroup $\mu_{\ell^{dt} - 1} \subset M_{v_1}^\times$ surjects onto the subgroup $\mu_{\ell^t - 1} \subset L_v^\times$. Therefore, we may take β_1 to be a root of unity in M_{v_1}. For such a choice of β_1, we have $\bar{\beta}_1 = \beta_1^{-1}$, as desired. $\qquad\square$

Proof of Lemma 8.7. Since n is even, the group $GU_{(D', \dagger')}$ satisfies the Hasse principle [Kot92, Sec. 7], and therefore it suffices to show that the involution $\dagger'$ has the same local invariants as the involution $\dagger$. Since both involutions are positive, we just need to show that the local invariants agree at the finite places of L^+.

Expressing $\dagger'$ as

$$x^{\dagger'} = \xi^{-1} x^\dagger \xi$$

for $x \in D'$, where $\xi = \xi^\dagger$, define

$$\Delta = N_{D/L}(\xi) \in (L^+)^\times / N(L^\times).$$

It suffices to show that

$$\Delta_v \equiv 1 \in (L_v^+)^\times / N(L_v^\times)$$

for every finite place v of L'. Note that F has the property that there is precisely one prime ℓ of $\mathbb{Q}$ which ramifies in F ($\ell = 2$ if $p \in \{3,5\}$ and $\ell = 3$ if $p = 7$). Since in each of these cases, ℓ is a generator of $\mathbb{Z}_p^\times$, we deduce that the extension $L^+/\mathbb{Q}$ is inert at ℓ, and therefore (ℓ) is prime in L^+, and is the unique prime of L^+ which ramifies in L. Since $\dagger'$ is positive, Δ is positive at every archimedean place of L^+. In light of the fundamental exact sequence

$$0 \to (L^+)^\times / N(L^\times) \to \bigoplus_v (L_v^+)^\times / N(L_v^\times) \to \mathbb{Z}/2 \to 0,$$

we see that it suffices for us to verify that $\delta_v \equiv 1$ for only the places v of L^+ which are inert in L. Let v be such a place, and let ℓ' be the rational prime lying under v. We have the following field diagram of unramified extensions
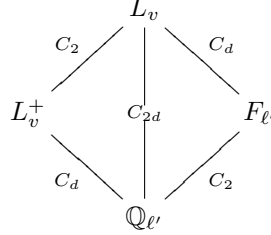
where $d = [L_v^+ : \mathbb{Q}_\ell]$ divides p^{r-1}, and is therefore odd. Under the embedding $GU_{(D',\dagger)} \hookrightarrow GU_{(D,\dagger)}$, the local discriminants give the following commutative diagram.

$$
\begin{array}{ccc}
H^1(L_v^+, GU_{(D',\dagger)}) & \longrightarrow & H^1(\mathbb{Q}_{\ell'}, GU_{(D,\dagger)}) \\
{\scriptstyle \mathrm{disc}_v} \downarrow {\scriptstyle \cong} & & {\scriptstyle \cong} \downarrow {\scriptstyle \mathrm{disc}_{\ell'}} \\
(L_v^+)^\times / N(L_v^\times) & \xrightarrow{\; N_{L_v^+/\mathbb{Q}_{\ell'}} \;} & \mathbb{Q}_{\ell'}^\times / N(F_{\ell'}^\times)
\end{array}
$$

Since all of the extensions are unramified, the compatibility of the local Artin maps allows us to verify that the map

$$(L_v^+)^\times / N(L_v^\times) \xrightarrow{\; N_{L_v^+/\mathbb{Q}_{\ell'}} \;} \mathbb{Q}_{\ell'}^\times / N(F_{\ell'}^\times)$$

is an isomorphism. The level structure η_0 gives an isomorphism

$$GU_{(D,\dagger)}(\mathbb{Q}_{\ell'}) \cong GU(\mathbb{Q}_{\ell'}).$$

Since ℓ' is unramified in F, Lemma 8.5 implies that we have

$$\mathrm{disc}_{\ell'}(\iota) = -1 \equiv 1 \in \mathbb{Q}_{\ell'}^\times / N(F_{\ell'}^\times).$$

We deduce that

$$\mathrm{disc}_v(\dagger) \equiv 1 \in (L_v^+)^\times / N(L_v^\times).$$

By Lemma 8.8, we have
$$\mathrm{disc}_v(\dagger') \equiv \mathrm{disc}_v(\dagger).$$
We conclude that $\Delta_v \equiv 1$, as desired.   □

Proof of Theorem 8.1. By Lemma 8.7, the involution $\dagger$ is equivalent to the involution $\dagger'$. Thus we get an isomorphism $GU_{(D',\dagger')} \cong GU_{(D',\dagger)}$. By Lemma 7.4, G_r embeds in $GU_{(D',\dagger')}(\mathbb{Q})$. We may therefore have an embedding
$$G_r \hookrightarrow GU_{(D',\dagger')}(\mathbb{Q}) \cong GU_{(D',\dagger)}(\mathbb{Q}) \hookrightarrow GU_{(D,\dagger)}(\mathbb{Q}) = GU_{\mathbf{A}_0}(\mathbb{Q}).$$
Since we have
$$GU_{\mathbf{A}_0}(\mathbb{Q}_p) \cong D_u^\times,$$
the group of units in a central division algebra of invariant $1/n$ over $\mathbb{Q}_p$, the group $GU_{\mathbf{A}_0}(\mathbb{Z}_p)$ is the unique maximal compact subgroup. Since G_r is compact, it must be contained in $GU_{\mathbf{A}_0}(\mathbb{Z}_p)$, and we deduce
$$G_r \subset GU_{\mathbf{A}_0}(\mathbb{Z}_p) \cap GU_{\mathbf{A}_0}(\mathbb{Q}) = GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}).$$
Using the level structure η_0 to give an isomorphism
$$GU_{\mathbf{A}_0}(\mathbb{A}^{p,\infty}) \cong GU(\mathbb{A}^{p,\infty})$$
we may regard G_r as a subgroup of $GU(\mathbb{A}^{p,\infty})$. For each prime $\ell \neq p$, choose a maximal compact subgroup
(8.9) $K_\ell \subset GU(\mathbb{Q}_\ell)$
which contains the image of G_r. Let
$$K = \prod_\ell K_\ell \subset GU(\mathbb{A}^{p,\infty})$$
be the associated compact open subgroup. We have
$$G_r \subseteq GU_{\mathbf{A}}(\mathbb{Z}_{(p)}) \cap K = \Gamma(K).$$
Under the completion map
$$GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}) \hookrightarrow GU_{\mathbf{A}_0}(\mathbb{Z}_p) \cong \mathbb{S}_n$$
the finite group $\Gamma(K)$ embeds into $\mathbb{S}_n$. Since G_r is a maximal finite subgroup of $\mathbb{S}_n$, we conclude that
$$G_r = \Gamma(K).$$
However, as discussed in Section 2, the group $\Gamma(K)$ is the automorphism group of the point
$$(A_0, i_0, \lambda_0, [\eta_0]_K) \in \mathrm{Sh}(K)^{[n]}(\bar{\mathbb{F}}_p).$$
The theorem is therefore proven.   □

9. Concluding remarks

In this final section we give a brief discussion of the relationship of the results in this paper to some topics in homotopy theory, as well as sketch some potential extensions.

9.1. **Relationship to Hopkins-Gorbounov-Mahowald theory.** Let $p \geq 3$. In [GM00], the cohomology theory

$$EO_{p-1} = E_2^{hG_1}$$

is related to liftings to characteristic zero of certain curves in characteristic p.

To summarize their work, let $C/\mathbb{F}_p$ be the curve given by

$$C : y^{p-1} = x^p - x.$$

The curve C has genus $(p-1)(p-2)/2$. Therefore the Jacobian $J(C)$ is an abelian variety of dimension $(p-1)(p-2)/2$, and is also acted upon by G_1. The action of the subgroup $\mu_{p-1} < G_1$ induces a splitting of the formal completion $\widehat{J}(C)$ into $p-2$ summands, according to the weights of the action:

$$\widehat{J}(C) = \widehat{J}(C)[1] \oplus \widehat{J}(C)[2] \oplus \cdots \oplus \widehat{J}(C)[p-2].$$

The dimensions of the summand $\widehat{J}(C)$ is i. Each summand has height $p-1$. In particular, $\widehat{J}(C)[1]$ is 1 dimensional and of height $p-1$, and there is an induced embedding

$$G_1 \hookrightarrow \mathrm{Aut}(\widehat{J}(C)[1] \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p) \cong \mathbb{S}_{p-1}$$

as a maximal finite subgroup.

The second author, with Gorbounov and Mahowald, constructed a lift $\widetilde{C}$ of the curve C over the ring

$$E = \mathbb{Z}_p[[u_1, \ldots, u_{p-2}]]$$

such that the action of G_1 lifts to an action on $\widetilde{C}$. Here, the group G_1 acts nontrivially on the ring E, but the subgroup μ_{p-1} acts trivially. The authors prove that the deformation $\widehat{J}(\widetilde{C})[1]$ of $\widehat{J}(C)[1]$ is a universal deformation. This gives a G_1-equivariant isomorphism from E to the Lubin-Tate universal deformation ring of $\widehat{J}(C)[1]$. This gives explicit formulas for the action of G_1 on $\pi_0(E_{p-1})$.

We explain how this set-up relates to the results of this paper. Assume that $p \geq 5$. Let $F = \mathbb{Q}(\omega)$ where ω is a primitive $(p-1)$st root of unity. The action of μ_{p-1} on $\widetilde{C}$ gives the $(p-1)(p-2)/2$-dimensional abelian variety $J(C)$ an action (through quasi-endomorphisms) by the ring $\mathbb{Q}[z]/(z^{p-1} - 1)$. Factorize

$$z^{p-1} - 1 = f_1(z) \cdots f_d(z)$$

as a product of irreducible polynomials, so that f_1 is of degree $\phi(p-1)$. Then there is a product decomposition

$$\mathbb{Q}(z)/(z^{p-1} - 1) \cong F_1 \times \cdots \times F_d$$

where $F_1 \cong F$. The abelian variety $J(C)$ is then quasi-isogenous to a product

$$J(C) \simeq J(C)_1 \times \cdots \times J(C)_d$$

where the factor $J(C)_i$ has complex multiplication by the field F_i. In particular, $J_1(C)$ has complex multiplication by F: we get

$$i_C : F \to D_C := \mathrm{End}^0(J(C)_1).$$

Taking the formal completion, the summands of $\widehat{J}(C)$ which show up in $\widehat{J}(C)_1$ correspond to the weights i for $i \in (\mathbb{Z}/(p-1))^\times$. We therefore have a decomposition

$$\widehat{J}(C)_1 = \bigoplus_{i \in (\mathbb{Z}/(p-1))^\times} \widehat{J}(C)[i].$$

Let $(t_1, \ldots, t_k)$ be a sequence of integers with $k = \phi(p-1)/2$ such that $0 < t_j < p-1$, $t_1 = 1$, and the sequence

$$(t_1, \ldots, t_k, (p-1) - t_1, \ldots, (p-1) - t_k)$$

gives a complete list of the elements of $(\mathbb{Z}/(p-1))^\times$ when reduced mod $(p-1)$. The prime p splits completely in F, and we write

$$(p) = y_1 \ldots y_k \bar{y}_1 \ldots \bar{y}_k$$

where, regarding $(\mathbb{Z}/(p-1))^\times = \mathrm{Gal}(F/\mathbb{Q})$, we have

$$[t_j](y_1) = y_j$$
$$[-t_j](y_1) = \bar{y}_j.$$

The decomposition

$$F_p = \prod_j F_{y_j} \times F_{\bar{y}_j}$$

gives a splitting

$$\widehat{J}(C)_1 = \bigoplus_j [\widehat{J}(C)_1]_{y_j} \oplus [\widehat{J}(C)_1]_{\bar{y}_j},$$

and we fix our labeling of the prime y_1 so that

$$[\widehat{J}(C)_1]_{y_1} = \widehat{J}(C)[1].$$

We then have

$$[\widehat{J}(C)_1]_{y_j} = \widehat{J}(C)[t_j],$$
$$[\widehat{J}(C)_1]_{\bar{y}_j} = \widehat{J}(C)[(p-1) - t_j].$$

By the Honda-Tate classification (see, for instance, [BLa, Ch.2]), we deduce from the slopes of $\widehat{J}(C)$ that $J(C)_1$ is simple, and hence

$$D_C = \mathrm{End}^0(J(C)_1)$$

is a central division algebra over F whose only non-trivial invariants are given by

$$\mathrm{Inv}_{y_j} D_C = t_j/(p-1),$$
$$\mathrm{Inv}_{\bar{y}_j} D_C = -t_j/(p-1).$$

Thus we see that D_C is isomorphic to the division algebra D constructed in Section 6.

Moreover, in the notation of Section 7, the subalgebra D' is equal to D. The involution $\dagger'$ is *characterized* by the property that G_1 is contained in $U_{(D,\dagger')}(\mathbb{Q})$. The abelian variety $J(C)$ possesses a canonical polarization λ_C coming from the Jacobian structure. Since the action of G_1 on $J(C)$ is induced from an action on C, the action of G_1 preserves the polarization. In particular, the polarization restricts to a polarization

$$\lambda_C : J(C)_1 \to J(C)_1^\vee.$$

Letting $\dagger_C$ be the associated Rosati involution on D_C, we conclude that G_1 is contained in $U_{(D_C, \dagger_C)}(\mathbb{Q})$. We therefore deduce that there is an isomorphism

$$(9.1) \qquad\qquad (D, \dagger) \cong (D_C, \dagger_C).$$

Specializing to the case of $p \in \{5, 7\}$, the field F is a quadratic imaginary extension of $\mathbb{Q}$. We have $k = 1$, $(p) = y_1 \bar{y}_1$, and

$$\widehat{J}(C)_1 = \widehat{J}(C)[1] \oplus \widehat{J}(C)[p-2].$$

Fixing the Shimura data as in Section 8, it follows from Theorem 8.1 and (9.1) that there exists a compact open subgroup $K \subset GU(\mathbb{A}^{p,\infty})$ and a level structure η_0 so that C gives rise to a point

$$(J(C)_1, i_C, \lambda_C, [\eta_0]_K) \in \mathrm{Sh}^{[n]}(\mathbb{F}_p)$$

in height n locus of the Shimura stack $\mathrm{Sh}(K)$.

9.2. More Shimura stacks.

In Section 5, we showed that if p is odd, $n = (p-1)mp^{\alpha-1}$ and G_α is an automorphism group of a height n point of a Shimura stack $\mathrm{Sh}(K)$, then we must have $m = 1$ and $p \leq 7$. However this analysis was restricted to the class of Shimura stacks considered in [BLa] that give rise to cohomology theories TAF. If one removes the restriction that the Shimura stack has an associated cohomology theory, one can extend the analysis of Section 8 to show that there do exist Shimura stacks with a mod p point whose associated quasi-endomorphism ring with involution does correspond to the pair $(D, \dagger)$ of Proposition 7.5.

Specifically, using the notation of Section 6, for arbitrary p, m, and α, let $B = M_n(F)$. Then there exists an involution ι on B whose signatures at the real places of F^+ are given by $(t_i, n - t_i)$, and a compact open subgroup $K \subset GU_{(B,\iota)}(\mathbb{A}^{p,\infty})$ such that the associated Shimura stack has G_α as the automorphism group of a mod p point of the associated Shimura stack $\mathrm{Sh}_{(B,\iota)}(K)$ over $\mathcal{O}_{F^+, x_1}$.

The reduction $\mathrm{Sh}_{(B,\iota)}(K) \otimes \bar{k}_{x_1}$ (where k_{x_1} is the residue field of F^+ at x_1) possesses a stratification governed by the Newton polygons of the associated p-divisible groups. It is possible that if one chooses a suitable stratum, one could associate to it a cohomology theory via Lurie's theorem. If this is the case, setting $\alpha = 1$, one could use the deformation theory of points in this stratum to give deformations of the Jacobians of the Artin-Schreier curves studied by Ravenel in [Rav08].

9.3. Potential Applications to EO_n-resolutions.

In [GHMR05], a resolution of the $K(2)$-local sphere at the prime 3 is constructed

$$* \to S_{K(2)} \to X_0 \to \cdots \to X_4 \to *$$

where the spectra X_i are wedges of spectra of the form E_2^{hG} for various finite subgroups of the extended Morava stabilizer group. In [Hen07, Thm. 26], Henn extends this to show that for p odd and $n = p - 1$, there is a similar resolution of $S_{K(p-1)}$ involving the spectra EO_{p-1}.

In [Beh06], the first author gave a moduli theoretic description of *half* of the resolution of [GHMR05]. In [Beh07], the resolution of [Beh06] is shown to $K(2)$-locally arise strictly from the structure of the quaternion algebra of quasi-endomorphisms

of a supersingular elliptic curve. These constructions are further generalized in [BLa]. Even in the cases where there is no Shimura stack giving rise to the groups G_α, the results of Section 6 and Section 7 still produce a very explicit presentation of a global division algebra with involution $(D, \dagger)$ containing the groups G_α. The buildings associated to the groups

$$GU_{(D,\dagger)}(F_\lambda^+) \cong GL_n(F_\lambda^+)$$

for primes λ of F^+ not dividing p which split in F will therefore produce length n resolutions involving $E_n^{hG_\alpha}$. Analogs of the density results of [BL06], [Nau08] should help analyze to what degree these resolutions approximate $S_{K(p-1)}$.

9.4. Connective covers of EO_n. One of the benefits to the equivalence

$$\mathrm{tmf}_{K(2)} \simeq EO_2^{h\,\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}$$

is that the connective spectrum tmf_p serves as a well-behaved connective cover for EO_2 for $p \in \{2, 3\}$. The connective spectrum tmf in turn comes from the compactification of the moduli stack of elliptic curves.

One of the original motivations of the authors to investigate the results of this paper was to try to give similar connective covers for EO_n. The Shimura stacks associated to the group GU of Section 8 possess similar compactifications. In fact, these compactifications involve adding only finitely many points in the locus where the associated formal group has height 1. Therefore, like the case of TMF, the construction of connective forms of the associated TAF spectra is basically a $K(1)$-local problem. The main difficulty lies in the fact that in the equivalence

$$\mathrm{TAF}_{GU}(K)_{K(n)} \simeq \left(\prod_{[g] \in GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}) \backslash GU(\mathbb{A}^{p,\infty})/K} E_n^{h\Gamma(gKg^{-1})} \right)^{h\,\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}.$$

the number of terms in the product could be greater than 1. The computation of the cardinality of

$$GU_{\mathbf{A}_0}(\mathbb{Z}_{(p)}) \backslash GU(\mathbb{A}^{p,\infty})/K$$

is a class number question for the group GU. Unfortunately, preliminary calculations of this cardinality by the first author, using the mass formulas of [GHY01], seem to indicate that, even in the case of $p = 5$ and $n = 4$, this class number is quite large.

9.5. Non-orientability of TAF-spectra. Atiyah, Bott, and Shapiro [ABS64] showed that $Spin$-bundles are KO-orientable, thus giving an orientation

$$\widehat{A} : MSpin \to KO.$$

refining the $\widehat{A}$-genus. The second author, with Ando and Rezk [AHR], showed that the Witten genus refines to an orientation

$$MString \to \mathrm{tmf}.$$

One can ask the following question: is there a natural topological group G over O for which there exists an orientation

$$MG \to \mathrm{TAF}_{GU}(K)?$$

Naïvely, since

$$BSpin = BO\langle 4 \rangle,$$
$$BString = BO\langle 8 \rangle,$$

one might expect that one can take G so that $BG = BO\langle N \rangle$ for N sufficiently large. However, at least if $p \in \{5, 7\}$, $n = p - 1$, and GU and K are as in Theorem 8.1, the existence of a hypothetical $MO\langle N \rangle$-orientation of $\mathrm{TAF}_{GU}(K)$ would result in a composite of maps of ring spectra

$$MO\langle N \rangle \to \mathrm{TAF}_{GU}(K) \to EO_{p-1}.$$

Hovey showed that no such composite can exist, for any N and $p \geq 5$ [Hov97, Prop 2.3.2]. Thus, the results of this paper imply that, at least in some cases, the spectrum $\mathrm{TAF}_{GU}(K)$ is *not* orientable by a any connective cover of O.

Remark 9.2. Hovey's non-orientability result relies only on the spectrum detecting the p-primary α_1 for $p > 3$ in its Hurewitz image. Thus, the comments in the following section actually imply the non-orientability of a much larger class of TAF-spectra by connective covers of O.

9.6. **p-torsion in automorphism groups at other primes.** Fix p odd and set $n = (p-1)p^{\alpha-1}m$. The results of Section 5 imply that in most cases, the maximal finite group G_α cannot be realized as an automorphism group of a mod p point of height n in one of the Shimura stacks under consideration. This does not preclude the possibility that these automorphism groups could contain large p-torsion. The main interest in the groups G_α in homotopy theory is not that they are maximal, but rather that they contain an element of order p^α.

Indeed, fix p to be any prime, and set $n = (p-1)p^{r-1}$. Let F be any quadratic imaginary extension of $\mathbb{Q}$ in which p splits as $u\bar{u}$, and let $M = F(\zeta)$, where ζ is a primitive p^rth root of unity. We necessarily have $[M : F] = n$. Let $A_0/\bar{\mathbb{F}}_p$ be an abelian variety of dimension n with complex multiplication

$$i_0 : F \to \mathrm{End}^0(A) := D$$

with associated p-divisible summand $A(u)$ of slope $1/n$ (such an abelian variety exists by Honda-Tate theory). Embed the extension M of F in D. This gives A_0 complex multiplication by M. Pick a polarization λ_0 compatible with this M-linear structure: one exists by [Kot92, Lem. 9.2]. By the definition of compatibility, the λ_0-Rosati involution restricts to the CM involution on M. In particular there is an inclusion

$$\mu_{p^r} \hookrightarrow \mathrm{Aut}(A_0, i_0, \lambda_0).$$

Let $(\widetilde{A}_0, \widetilde{i}_0, \widetilde{\lambda}_0)/\mathbb{C}$ be the base-change to the complex numbers of a lift of (A_0, i_0, λ_0) to characteristic 0. Following the argument of [BLa, 14.3.2], the tuple $(\widetilde{A}_0, \widetilde{i}_0, \widetilde{\lambda}_0)$ arises as a point of a complex Shimura stack $\mathrm{Sh}_{\mathbb{C}}$ associated to a group $GU_{(C,\iota)}$ where $C = M_n(F)$ and ι is an involution associated to a hermitian form of signature $(1, n-1)$. Let Sh be the p-integral model of $\mathrm{Sh}_{\mathbb{C}}$: by construction the point (A_0, i_0, λ_0) is a mod p point, with an automorphism group containing an element of order p^r. We therefore have established the following proposition.

Proposition 9.3. Suppose that p is any prime, and that $n = (p-1)p^{r-1}$. Then for each quadratic imaginary extension F of $\mathbb{Q}$ in which p splits, there exists an n-dimensional hermitian form of signature $(1, n-1)$, with associated unitary similitude group GU, and a compact open subgroup $K \subset GU(\mathbb{A}^{p,\infty})$, so that the associated Shimura stack contains a point

$$(A_0, i_0, \lambda_0, [\eta_0]_K) \in \mathrm{Sh}^{[n]}(K)(\bar{\mathbb{F}}_p)$$

whose automorphism group contains an element of order p^r.

9.7. **The prime** 2. Suppose now that $p = 2$, and that $n = 2^{r-1}$ with $r > 2$. By [Hew95, Cor. 1.5], every maximal finite subgroup of $\mathbb{S}_n$ is cyclic. Let $\mu_{2^r} \subset \mathbb{S}_n$ be the cyclic subgroup of order 2^r arising from embedding the field $\mathbb{Q}_2(\zeta_{2^r})$ in the division algebra $D_{1/n}$ over $\mathbb{Q}_2$ of invariant $1/n$. Let G be a maximal finite subgroup in $\mathbb{S}_n$ containing μ_{2^r}. Since G is cyclic, there must be a corresponding cyclotomic extension of $\mathbb{Q}_2$ containing $\mathbb{Q}_2(\mu_{2^r})$ which embeds in $D_{1/n}$. Since $\mathbb{Q}_2(\zeta_{2^r})$ is a maximal subfield, we conclude that $G = \mu_{2^r}$, and that μ_{2^r} is a maximal finite subgroup. Using Proposition 9.3, we therefore have the following 2-primary version of Theorem 8.1.

Proposition 9.4. Suppose that $p = 2$ and that $n = 2^{r-1}$ with $r > 2$. Then for each quadratic imaginary extension F of $\mathbb{Q}$ in which 2 splits, there exists an n-dimensional hermitian form of signature $(1, n-1)$, with associated unitary similitude group GU, and a compact open subgroup $K \subset GU(\mathbb{A}^{2,\infty})$, so that the associated Shimura stack contains a point

$$(A_0, i_0, \lambda_0, [\eta_0]_K) \in \mathrm{Sh}^{[n]}(K)(\bar{\mathbb{F}}_2)$$

whose automorphism group is the maximal subgroup $\mu_{2^r} \subset \mathbb{S}_n$.

References

[ABS64]   M. F. Atiyah, R. Bott, and A. Shapiro, *Clifford modules*, Topology **3** (1964), no. suppl. 1, 3–38.

[AHR]   Matthew Ando, Michael J. Hopkins, and Charles Rezk, *Multiplicative orientations of KO-theory and of the spectrum of topological modular forms*, Preprint. Available at http://www.math.uiuc.edu/~mando/node1.html.

[Beh06]   Mark Behrens, *A modular description of the $K(2)$-local sphere at the prime 3*, Topology **45** (2006), no. 2, 343–402.

[Beh07]   ———, *Buildings, elliptic curves, and the $K(2)$-local sphere*, Amer. J. Math. **129** (2007), no. 6, 1513–1563.

[BLa]   Mark Behrens and Tyler Lawson, *Topological automorphic forms*, To appear in *Memoirs of the American Mathematical Society*.

[BLb]   ———, *Topological automorphic forms on $U(1,1)$*, Preprint. Available at http://arxiv.org/abs/0901.1838.

[BL06]   ———, *Isogenies of elliptic curves and the Morava stabilizer group*, J. Pure Appl. Algebra **207** (2006), no. 1, 37–49.

[GH04]   P. G. Goerss and M. J. Hopkins, *Moduli spaces of commutative ring spectra*, Structured ring spectra, London Math. Soc. Lecture Note Ser., vol. 315, Cambridge Univ. Press, Cambridge, 2004, pp. 151–200.

[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), no. 2, 777–822.

[GHY01]   Wee Teck Gan, Jonathan P. Hanke, and Jiu-Kang Yu, *On an exact mass formula of Shimura*, Duke Math. J. **107** (2001), no. 1, 103–133.

[GM00]   V. Gorbounov and M. Mahowald, *Formal completion of the Jacobians of plane curves and higher real K-theories*, J. Pure Appl. Algebra **145** (2000), no. 3, 293–308.

[Hen07]   Hans-Werner Henn, *On finite resolutions of $K(n)$-local spheres*, Elliptic cohomology, London Math. Soc. Lecture Note Ser., vol. 342, Cambridge Univ. Press, Cambridge, 2007, pp. 122–169.

[Hew95]   Thomas Hewett, *Finite subgroups of division algebras over local fields*, J. Algebra **173** (1995), no. 3, 518–548.

[Hov97]   Mark A. Hovey, *v_n-elements in ring spectra and applications to bordism theory*, Duke Math. J. **88** (1997), no. 2, 327–356.

[Kot92]   Robert E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), no. 2, 373–444.

[Mil97]   J. S. Milne, *Class field theory*, http://www.jsmilne.org/math, 1997.

[Nau08]   Niko Naumann, *Arithmetically defined dense subgroups of Morava stabilizer groups*, Compos. Math. **144** (2008), no. 1, 247–270.

[PR]   Gopal Prasad and Andrei S. Rapinchuk, *Local-global principles for embedding of fields with involution into simple algebras with involution*, Commentarii Math. Helv. 85(2010), to appear.

[PR94]   Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.

[PR96]   Gopal Prasad and Andrei S. Rapinchuk, *Computation of the metaplectic kernel*, Inst. Hautes Études Sci. Publ. Math. (1996), no. 84, 91–187 (1997).

[Rav86]   Douglas C. Ravenel, *Complex cobordism and stable homotopy groups of spheres*, Pure and Applied Mathematics, vol. 121, Academic Press Inc., Orlando, FL, 1986.

[Rav08]   ———, *Toward higher chromatic analogs of elliptic cohomology. II*, Homology, Homotopy Appl. **10** (2008), no. 3, 335–368.

[Rez98]   Charles Rezk, *Notes on the Hopkins-Miller theorem*, Homotopy theory via algebraic geometry and group representations (Evanston, IL, 1997), Contemp. Math., vol. 220, Amer. Math. Soc., Providence, RI, 1998, pp. 313–366.

[Sch85]   Winfried Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 270, Springer-Verlag, Berlin, 1985.

[Ser]   J-P. Serre, *Applications algébriques de la cohomologie des groupes, I, II*, Séminaire Henri Cartan, 1950/51.

[Ser79]   Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Swa70]   Richard G. Swan, *K-theory of finite groups and orders*, Lecture Notes in Mathematics, Vol. 149, Springer-Verlag, Berlin, 1970.

Dept. of Mathematics, M.I.T., Cambridge, MA 02139, U.S.A.

Dept. of Mathematics, Harvard University, Cambridge, MA 02138, U.S.A.