Generators for Maximal Finite Subgroups of the Morava Stabilizer Group
SPUR Final Paper, Summer 2016

Colin Aitken
Mentor: Lyuboslav Panchev
Project Suggested by Haynes Miller

August 3, 2016

Abstract

The Morava stabilizer group $\mathbb{S}_n$ at a prime p is the automorphism group of the Honda formal group law F_n. The maximal finite subgroups of $\mathbb{S}_n$ are central to the construction of higher real K-theories, and were first classified by Hewett. In this paper, we use ideas inspired by Kummer theory to produce an explicit expression for the generators of the largest nonabelian finite subgroup when p is odd.

In this paper we examine generators of the largest nonabelian finite subgroup G_1 of the Morava stabilizer group $\mathbb{S}_n$ at a prime $p > 2$. As a group, G_1 is generated by one generator ζ_p of order p and one of order prime to p. Since the latter is easy to compute, most of the paper is devoted to computing ζ_p.

In the first section, we give a brief overview of formal group laws and their use in chromatic homotopy theory. Technically speaking, only Definition 1.4 and Theorems 1.5 and 1.6 are relevant to the body of the paper, but we include more details to motivate our question and situate it within (a subset of) chromatic homotopy theory. This information is largely from Ravenel's "green book" [8]. We then summarize the contributions of Hewett, Bujard, and Henn and their relevance to our work.

The next section forms the meat of the paper, and is devoted to constructing an embedding of $\mathbb{Q}_p(\zeta_p)$ into the division algebra $\mathrm{End}(F_n)[1/p]$. The meat of this involves constructing a certain element αS^m such that there are $a_1, \cdots, a_{p-2} \in \mathbb{Q}_p$ with

$$\zeta_p = a_0 + a_1\alpha S^m + a_2(\alpha S^m)^2 + \cdots + a_{p-2}(\alpha S^m)^{p-2}.$$

In the the final section, we use this embedding to compute values for the coefficents $a_0, \cdots, a_n$. To do this, we use the fact that the trace of any nontrivial power of αS^m is zero to compute the coefficients in terms of relatively simple trace maps. We end with some examples, listing explicit values of ζ_p when $p = 3, 5$, and 7.

Finally, we include an appendix giving an algorithm based on Hewett's work to produce explicit values of ζ_p at specific primes.

1 Background

One particularly elegant area of modern algebraic topology is *chromatic homotopy theory,* which uses tools from algebraic geometry to study complex-oriented cohomology theories and their applications to stable homotopy theory. The central geometric object of study is a *formal group law,* which is essentially a power series in two variables that behaves like a group operation.

Definition 1.1. A *formal group law* $F(x, y)$ over a nilpotent-free ring R is an element of $R[[x, y]]$ such that:

1. $F(x, y) = x + y +$ terms of higher degree.
2. $F(x, F(y, z)) = F(F(x, y), z)$

It follows (with some effort) from this definition that $F(x, y) = F(y, x)$ and that there is a power series ι such that $F(x, \iota(x)) = 0$, so we have "power series versions" of all the axioms for an abelian group. We can make this more concrete by using F to put an abelian group structure on $R[[x]]$ with operation $+_F$ given by $a +_F b = F(a, b)$. In this paper, however, we're more interested in morphisms between formal group laws.

Definition 1.2. Let F and G be formal group laws over R. A *morphism* from F to G is a power series $h \in R[[x]]$ such that

$$h(F(x,y)) = G(h(x), h(y)).$$

An invertible morphism is called an *isomorphism.* A morphism from F to itself is called an *endomorphism*, and an invertible endomorphism is called an *automorphism.*

Example 1. Let F be a formal group law over R and r any element of R. Then, there is an endomorphism r given by the (rather small) power series rx.

Example 2. Let n be an integer and F a formal group law. Then, there is an endomorphism $[n]$ of F, defined inductively via:

1. $[1]x = x$
2. $[n+1]x = [n]x +_F x$
3. $[-n]x = \iota([n]x)$

The endomorphisms of a given formal group law F turn out to form a ring $\mathrm{End}(F)$, called the *endomorphism ring* of F, with operations given by $+_F$ and composition, and the function $\mathbb{Z} \to \mathrm{End}(F)$ given by $n \mapsto [n]$ is a ring homomorphism!

The main use of formal group laws in algebraic topology arises from their connection with complex-oriented cohomology theories. We can associate a formal group law to each (complex orientation of a)cohomology theory, which allows the geometric tools used to study formal group laws to apply to cohomology theories. Rather than going into the general construction, we're just going to look at specific formal group laws: those defined over $\overline{\mathbb{F}_p}$.

It turns out that there aren't very many distinct formal group laws over $\overline{\mathbb{F}_p}$. In particular, there is an invariant called *height* such that any formal group law of height n over $\overline{\mathbb{F}_p}$ is isomorphic to the following formal group law:

Definition 1.3. The *Honda formal group law* F_n is the unique formal group law over $\mathbb{F}_{p^n}$ satisfying

$$[p]x = x^{p^n}.$$

So if we're working over finite fields, we only need to look at the Honda formal group laws. Just as it's interesting to look at the cohomology operations corresponding to a given spectrum, it turns out to be fruitful to look at automorphisms of a given formal group law. This leads us to make the following definition.

Definition 1.4. The Morava stabilizer group $\mathbb{S}_n$ is the automorphism group of $\mathbb{F}_n$. (Equivalently, $\mathbb{S}_n$ is the group of units in the endomorphism ring $\mathrm{End}(F_n)$.)

The Morava stabilizer group shows up in a variety of contexts related to stable homotopy. One form of the Adams-Novikov spectral sequence takes the form[1]

$$E^2_{r,s} = \mathrm{Ext}^{r,s}_{BP_*BP}(BP_*, BP_*)$$

and converges to (the p-localization of) the stable homotopy groups of spheres. Since this can be difficult to compute, we localize the sphere spectrum S at the Morava K-theory $K(n)$. This lets us restrict our attention from all of BP_*BP to the automorphisms of the single formal group law F_n, arriving at a spectral sequence

$$H^*_c(\mathbb{S}_n, (E_n)_*)^{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)} \Rightarrow \pi_* L_{K(n)} S,$$

where E_n is a certain localization of BP.

The upshot of all this is that understanding the continuous group cohomology of $\mathbb{S}_n$ with coefficients in a certain ring should let us build up approximations to (the p-localization of) the stable homotopy groups of spheres! One key step in this direction is understanding the structure of $\mathbb{S}_n$, which requires us to understand $\mathrm{End}(F_n)$.

Theorem 1.5. *Let $\mathcal{O}_n = \mathbb{Z}_p[\omega]$, where ω is a primitive $(p^n-1)^{th}$ root of unity. Then,* $\mathrm{End}(F_n)$ *can be identified with $\mathcal{O}_n\langle S\rangle$ subject to the relations $S^n = p$ and $S\omega = \omega^p S$.*

The identification works roughly as follows: S corresponds to the power series $x \mapsto x^p$ and ω corresponds to $x \mapsto \omega x$. For each element $a = a_0 + a_1 p + \cdots \in \mathbb{Z}_p$, we have a power series $[a_0] +_F [a_1 p] +_F [a_2 p^2] + \cdots$. (The sum converges in $\mathbb{F}_{p^n}[[x]]$ because the leading term of $[a_k p^k]$ is x^{p^k}.)

However, $\mathbb{S}_n$ remains a very large and complicated group, and its action on $(E_n)_*$ is relatively complicated, so the cohomology remains difficult to compute. We thus have to take another approximation by replacing the (localization of the) sphere spectrum $L_{K(n)}S$ with something else. Given a closed subgroup G of $\mathbb{S}_n$, we can compute the "homotopy fixed points" of G acting on E_n to get a spectrum E_n^{hG}. Of particular interest is the case where G is a maximal finite subgroup of $\mathbb{S}_n$, in which case E_n^{hG} is called a "higher real K-theory" and it is believed that $\pi_*(E_n^{hG})$ is a reasonable approximation to $\pi_*(L_{K(n)}S)$. Then, we have a spectral sequence

$$H^*_c(G, (E_n)_*) \Rightarrow \pi_*(E_n^{hG})$$

In short, we can use maximal finite subgroups $G \subseteq \mathbb{S}_n$ to compute the homotopy groups of the spectrum E_n^{hG}. These are believed to be a reasonable approximation to the homotopy groups of $L_{K(n)}S$, which can be used to approximate the (p-localization of) homotopy groups of spheres.

[1] It is beyond the scope of this paper to properly introduce the various spectra appearing in these calculations, (e.g. BP, $K(n)$, and E_n). The reader will not miss out on anything important by viewing the spectral sequences as black boxes relating $\mathbb{S}_n$ to questions topologists care about.

To compute the cohomology of G with coefficients in $(E_n)_*$, a good first step is to know what G actually is. A complete list of maximal finite subgroups was first computed by Hewett [7], although we will give the list in a form due to Bujard [2].

Theorem 1.6 (Hewett, Bujard)**.** *Let p be an odd prime, and let $n = (p-1)p^{k-1}m$, where m is not divisible by p. Then $\mathbb{S}_n$ has $k+1$ (conjugacy classes of) maximal finite subgroups $G_0, \cdots, G_k$. These groups are given by:*

$$G_0 = C_{p^n-1}$$
$$G_a = C_{p^a} \rtimes C_{(p^{mp^{k-a}}-1)(p-1)} \text{for } 1 \leq a \leq k,$$

where C_r denotes a cyclic group of size r. If n is not divisible by $(p-1)$, then C_0 is the only maximal finite subgroup.

The above cohomology groups have been computed in the case $p = 3, n = 2$ by Goerss et al. [4] using an explicit expression for the generator ζ_3, and we belief that explicit expressions for generators in other cases will similarly aid in further cohomology computations. Some generators are easy: G_0 is simply the group of roots of unity in $\mathbb{Z}_p[\omega]$ and is generated by ω. The $C_{(p^{mp^{k-a}}-1)(p-1)}$ piece of the higher groups is a subgroup of G_0 and is generated by ω to the power of $\frac{p^n-1}{(p^{mp^{k-a}}-1)(p-1)}$. As such, we will restrict our attention to the p-subgroups C_{p^a}. Both Bujard's and Hewett's constructions imply that *any* element of order p^a can be taken to be the generator of C_{p^a}, so our problem reduces to computing elements of order p^a in $\mathbb{S}_n$.

Bujard's construction, as with a similar one by Behrens and Hopkins in [1], depends on the fact that any field F containing $\mathbb{Q}_p$ with $[F : \mathbb{Q}_p] = n$ embeds in any division algebra of dimension n^2 over $\mathbb{Q}_p$. There does not seem to be a general way to compute such an embedding, so Bujard's construction does not give explicit generators.

Hewett's construction similarly depends on such an embedding when $a > 1$. When $a = 1$, it can with a fair amount of effort be turned into an algorithm, using an algorithm of Hanke [5] to construct a key isomorphism of cyclic algebras. Hewett's work was not intended as an explicit algorithm, however, and therefore this "constructive version" of his work runs rather slowly, around $O(pn^5)$. It does not seem to be adaptable to create an explicit formula, and its expressions are quite large, having $O(n^2)$ terms. We give a sketch of this algorithm in the Appendix.

In this paper, we will provide an explicit formula for the p-generator of G_1 at odd primes, which has $O(p)$ terms. The search for this formula relied quite deeply on many aspects of Hewett's paper, although the final form of the proof does not interact with it at all.

I only very recently (after writing the rest of this paper) became aware of an article [6] by Henn examining topological aspects of the case $n = (p-1)$. Henn's Lemma 19 plays much the same role as our Proposition 2.3 for this value of n although his proof is quite different, and he does not go on to compute explicit

coefficients. I have so far not been able to determine whether Henn's work can be generalized to other values of n, or whether an analogue of our Theorem 3.1 can be acheived on Henn's choice of embedding.

As a final note, there is some question as to what an "explicit" representation is. For example, writing ζ_p as a generator of G_1 is clearly insufficient, since it does not tell us how to actually construct ζ_p as an element of $\mathbb{S}_n$ and has simply avoided the problem. On the other hand, it's less clear with something like $\sqrt{2}$: is this "explicit"? For the purposes of this paper, we will take explicit representations to mean polynomials in ω and S with coefficients in $\mathbb{Z}_p$. Thus, for example $\sqrt{2}$ is acceptable when $p = 7$, since it is a 7-adic integer, but not when $p = 3$, when we would ask for an expansion in ω.

1.1 Notation

We collect here some notational choices we use in the rest of the paper.

1. We denote by K_n the unique unramified extension of $\mathbb{Q}_p$ of degree n.
2. We denote by $\mu_\ell(F)$ the group of ℓ^{th} roots of unity in the field F.
3. We denote by ζ_p a primitive p-th root of unity in either an extension of $\mathbb{Q}_p$ or $\mathbb{S}_n$.

2 An Embedding of $\mathbb{Q}_p(\zeta_p)$ into $\mathrm{End}(F_n)[1/p]$.

The finite subgroup $G_1 \subseteq \mathbb{S}_n$ is the largest nonabelian finite subgroup of $\mathbb{S}_n$, and exists whenever $(p-1)$ divides n. For the rest of this paper, therefore, we will set $n = (p-1)m$. We will also find it useful to extend $\mathrm{End}(F_n)$ to the division algebra $\mathrm{End}(F_n)[1/p]$.

In this section, we compute an α so that $\mathbb{Q}_p(\alpha S^m) = \mathbb{Q}_p(\zeta_p)$. We do this by constructing an element $Z(y,r) \in \mathbb{Q}_p(\zeta_p)$ such that $\mathbb{Q}_p(Z(y,r)) = \mathbb{Q}_p(\zeta_p)$ so that the equation $(\alpha S^m)^{p-1} = Z(y,r)^{p-1}$ is solvable for α.

Definition 2.1. If y satisfies $y^{p-1} = 1$ and r is a generator of $(\mathbb{Z}/p)^\times$, we will set:

$$Z(y,r) = \sum_{i=1}^{p-1} y^i \zeta_p^{r^i}$$

Lemma 2.2. *Let σ_r denote the generator of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ induced by $\sigma_r(\zeta_p) = \zeta_p^r$. Then,*

$$\sigma_r(Z(y,r)) = y^{-1} Z(y,r).$$

Proof. More or less by definition, we see that

$$\begin{aligned}\sigma_r(Z(y,r)) &= \sigma_r\left(\sum_{i=1}^{p-1} y^i \zeta_p^{r^i}\right)\\ &= \sum_{i=1}^{p-1} \sigma_r(y^i \zeta_p^{r^i})\\ &= \sum_{i=1}^{p-1} y^i \zeta_p^{r^{i+1}}\\ &= y^{-1}\sum_{i=1}^{p-1} y^i \zeta_p^{r^i}\\ &= y^{-1} Z(y,r).\end{aligned}$$

■

From this, we can see that $Z(y,r)^{p-1}$ is fixed by σ_r, and therefore lies in $\mathbb{Q}_p$.

Proposition 2.3. $\mathbb{Q}_p(Z(y,r)) = \mathbb{Q}_p(\zeta_p)$.

Proof. Since $Z(y,r) \in \mathbb{Q}_p(\zeta_p)$, it suffices to note that $Z(y,r)$ has $p-1$ distinct Galois conjugates under $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ given by $y^{-i}Z(y,r)$ for $0 \le i < p-1$. This implies that $[\mathbb{Q}_p(Z(y,r)) : \mathbb{Q}_p] = (p-1)$, so the result follows. ■

Recall that G_1 only exists if n is divisible by $(p-1)$. Therefore, for the rest of this paper, let $n = (p-1)m$. We want to construct an element of $\mathbb{S}_n$ with the same algebraic properties as $Z(y,r)$. In particular, we're going to look for a value of α satisfying $(\alpha S^m)^{p-1} = Z(y,r)$.

A simple calculation shows that

$$(\alpha S^m)^{p-1} = \alpha^{1+\sigma^m+\sigma^{2m}+\cdots\sigma^{(p-2)m}} p,$$

so we're looking for values of α with $\alpha^{1+\sigma^m+\sigma^{2m}+\cdots\sigma^{(p-2)m}} = Z(y,r)/p$. To get a handle on the left hand side of the equation, we make the following definition:

Definition 2.4. The partial norm $N_m : K_n^\times \to K_m^\times$ is defined as follows:

$$N_m(\alpha) = \alpha^{1+\sigma^m+\sigma^{2m}+\cdots\sigma^{(p-2)m}}$$

In particular, we note that the partial norm is multiplicative and reduces to α^{p-1} if $\alpha \in \mathbb{Q}_p$. The next proposition establishes the existence of the desired α, and will occupy our attention for the next two pages.

Proposition 2.5. *Choose y to be congruent to r^{-1} modulo p. Then, there exists an $\alpha \in K_n$ such that $(\alpha S^m)^{p-1} = Z(y,r)^{p-1}$.*

Before proving this proposition, we note that it would be easy if we knew $Z(y,r)^{p-1}/p$ were congruent to 1 modulo p. Indeed, any $(p-1)^{\text{st}}$ root of $Z(y,r)^{p-1}/p$ would lie in $\mathbb{Q}_p$ by Hensel's lemma, and therefore would be a valid choice of α.

Since not all numbers are congruent to 1 modulo p, we'll need to go to a bit more effort. First, we'll show that $Z(y,r)^{p-1}/p$ lies in $\mathbb{Z}_p^\times$ (so that it makes sense to speak of "mod p" to begin with.) Second, we'll show that the partial norm is surjective on roots of unity, which we will argue is sufficient to finish the proof.

Lemma 2.6. *If y is equivalent to r^{-1} modulo p, then $Z(y,r)^{p-1}/p$ is an element of $\mathbb{Z}_p^\times$.*

Proof. We need to show that $Z(y,r)^{p-1}$ is divisible by p but not p^2. To begin, take $\pi = \zeta_p - 1$ as a uniformizer for $\mathbb{Q}_p(\zeta_p)$. The given condition implies that y is the Teichmuller representative $[r^{-1}]$ of r^{-1}, so that we can write

$$\begin{aligned}
\sum_{i=1}^{p-1} y^i \zeta_p^{r^i} &= \sum_{i=1}^{p-1} [r^{-i}](\pi+1)^{r^i} \\
&= \sum_{\ell=1}^{p-1} [\ell^{-1}](\pi+1)^{\ell} \\
&= \sum_{\ell=1}^{p-1} [\ell^{-1}] \sum_{k=0}^{\ell} \binom{\ell}{k} \pi^k \\
&= \sum_{k=0}^{p-1} \left(\sum_{\ell=k}^{p-1} [\ell^{-1}] \binom{\ell}{k} \right) \pi^k.
\end{aligned}$$

The coefficient of π^0 in this sum is $\sum_{\ell=1}^{p-1}[\ell^{-1}]$, which is the sum of all $(p-1)$st roots of unity and therefore zero. The coefficient of π^1 is $\sum_{\ell=1}^{p-1} \ell[\ell^{-1}]$, which reduces mod p to $\sum_{\ell=1}^{p-1} 1 = -1$. Therefore, we can write

$$\begin{aligned}
Z(y,r) &= (-\pi + O(\pi^2))^{p-1} \\
&= \pi^{p-1} + O(\pi^p) \\
&= up + O(p^{\frac{p}{p-1}})
\end{aligned}$$

for some unit u, as desired. This implies the lemma. ∎

Recall that K_n contains all of its $(p^n-1)^{th}$ roots of unity, which form a cyclic group μ_{p^n-1}. The partial norm maps μ_{p^n-1} in K_n to μ_{p^m-1} in K_m-we will now show that this is surjective.

Lemma 2.7. *The restriction of the partial norm $N_m : \mu_{p^n-1} \to \mu_{p^m-1}$ is surjective.*

Proof. We note that for $\alpha \in \mu_{p^n-1}$, we have:

$$\begin{aligned} N_m(\alpha) &= \alpha^{1+\sigma^m+\sigma^{2m}+\cdots\sigma^{(p-2)m}} \\ &= \alpha^{1+p^m+p^{2m}+\cdots+p^{(p-2)m}} \\ &= \alpha^{\frac{p^n-1}{p^m-1}} \end{aligned}$$

It follows if α has order $p^n - 1$, then $N_m(\alpha)$ must have order $p^m - 1$. But the only subgroup of μ_{p^n-1} of size $p^m - 1$ is μ_{p^m-1}, so $N_m(\alpha)$ must be a generator of μ_{p^m-1}. This implies the partial norm must be surjective, as desired. ■

We now know enough to construct an α to prove Proposition 2.5! (Remember Proposition 2.5? It's at the bottom of page 7.)

Proof of Proposition 2.5. Let $\beta = Z(y,r)^{p-1}/p$, so that the given condition is then $N_m(\alpha) = \beta$. We know from Lemma 2.6 that $\beta \in \mathbb{Z}_p^\times$. Now, let γ be a $(p-1)^{\text{th}}$ root of unity congruent to β modulo p. By Lemma 2.7, we can find $\mu \in \mu_{p^n-1}$ with $N_m(\mu) = \gamma$. Now, $\frac{\beta}{\gamma}$ is congruent to 1 modulo p, so we can set

$$\alpha = \mu \left(\frac{\beta}{\gamma}\right)^{\frac{1}{p-1}}.$$

■

Finally, this gives us the promised embedding! It's not quite clear yet where ζ_p is sent, so we'll have to do a bit more work in the next section.

Corollary 2.8. *There is an embedding $\mathbb{Q}_p(\zeta_p) \to \mathrm{End}(F_n)[1/p]$.*

Proof. We simply identify $\mathbb{Q}_p(\zeta_p)$ with $\mathbb{Q}_p(Z(y,r))$, and send $Z(y,r)$ to αS^m. This extends to a full embedding because αS^m commutes with members of $\mathbb{Q}_p$ and powers of itself. ■

3 Computing Explicit Coefficients

We know from the previous section that $\mathbb{Q}_p(\alpha S^m) = \mathbb{Q}_p(\zeta_p)$, and we have a way of constructing α. All that remains is to actually express ζ_p in terms of αS^m. This is the content of the following theorem:

Theorem 3.1. *The generator ζ_p of the p-part of G_1 can be written as*

$$\zeta_p = \sum_{k=0}^{p-2} \frac{Z(y^k,r)}{(p-1)Z(y,r)^k}(\alpha S^m)^k.$$

The coefficients of $(\alpha S^m)^k$ all lie in $\mathbb{Z}_p$.

The proof of this theorem depends strongly on the following trick we'll use to isolate coefficients:

Lemma 3.2. *The coefficient of $(\alpha S^m)^k$ in the expansion of ζ_p is*

$$\frac{\mathrm{Tr}\left(\frac{\zeta_p}{Z(y,r)^k}\right)}{p-1}$$

Proof. Suppose

$$\zeta_p = a_0 + a_1\alpha S^m + a_2(\alpha S^m)^2 + \cdots + a_{p-2}(\alpha S^m)^{p-2}.$$

We can identify αS^m with $Z(y,r)$, and write:

$$\zeta_p = a_0 + a_1 Z(y,r) + a_2 Z(y,r)^2 + \cdots + a_{p-2}Z(y,r)^{p-2}.$$

We can then divide by $Z(y,r)^k$ to isolate a_k, which gives:

$$\frac{\zeta_p}{Z(y,r)^k} = a_0 Z(y,r)^{-k} + \cdots + a_k + \cdots + a_{p-2}Z(y,r)^{p-2-k}.$$

Since the trace of an element of $\mathbb{Q}_p(\zeta_p)$ is $\mathbb{Q}_p$-linear, we see that:

$$\mathrm{Tr}\left(\frac{\zeta_p}{Z(y,r)^k}\right) = a_0\,\mathrm{Tr}(Z(y,r)^{-k}) + \cdots + \mathrm{Tr}(a_k) + \cdots + a_{p-2}\,\mathrm{Tr}(Z(y,r)^{p-2-k}).$$

But if j is not divisible by $p-1$, we have:

$$\begin{aligned}\mathrm{Tr}(Z(y,r)^j) &= \sum_{i=0}^{p-2} \sigma_r^i(Z(y,r)^j) \\ &= \sum_{i=0}^{p-2} y^{-ij} Z(y,r)^j \\ &= 0.\end{aligned}$$

So almost all of the terms on the right hand side disappear! We're left with

$$\mathrm{Tr}\left(\frac{\zeta_p}{Z(y,r)^k}\right) = \mathrm{Tr}(a_k) = (p-1)a_k,$$

from which the lemma follows. ∎

This reduces the proof of the theorem to computing a couple of traces!

Proof of Theorem 3.1. Using the lemma, we only need to compute $\mathrm{Tr}\left(\frac{\zeta_p}{Z(y,r)^k}\right)$.

We have

$$\begin{aligned}\mathrm{Tr}\left(\frac{\zeta_p}{Z(y,r)^k}\right) &= \sum_{i=0}^{p-1} \frac{\zeta_p^{r^i}}{y^{-ik}Z(y,r)^k} \\ &= \sum_{i=0}^{p-1} \frac{y^{ik}\zeta_p^{r^i}}{Z(y,r)^k} \\ &= \frac{\sum_{i=0}^{p-1} y^{ik}\zeta_p^{r^i}}{Z(y,r)^k} \\ &= \frac{Z(y^k,r)}{Z(y,r)^k},\end{aligned}$$

as desired. It remains to check that the coefficients lie in $\mathbb{Z}_p$ as claimed.

All of these coefficients must lie in $\mathbb{Q}_p$ follows because the image of the trace map does. Now, extend the usual valuation v_p on K_n to $\mathrm{End}(F_n)[1/p]$ by setting $v_p(S) = 1/(p-1)$. We know from Proposition 1.1 of [2] that ζ_p lies in $\mathbb{S}_n$, so in particular it has nonnegative valuation. Now, the valuation of an element of $\mathbb{Q}_p$ is an integer, and $v_p((\alpha S)^k) = k/(p-1)$, so no two terms can share a valuation. Therefore, if any coefficient had negative valuation, it would force the whole sum to. Since this is a contradiction, each coefficient must have nonnegative valuation and lie in $\mathbb{Z}_p$, as desired. ■

Remark 3.3. The first two terms of this expansion take the particularly nice form

$$\zeta_p = \frac{-1}{p-1} + \frac{1}{p-1}\alpha S^m + \cdots.$$

We might guess that this pattern continues and gives nice coefficients the whole time! Sadly, we would be wrong.

Example 3. Below we list some values of ζ_p when $n = (p-1)$ and p is relatively small. Recall that for $k \in \mathbb{F}_{p^n}$, $[k]$ refers to the $(p^n-1)^{\text{th}}$ root of unity in K_n congruent to k mod p.

p	α	ζ_p
3	$[\sqrt{-1}]$	$\frac{-1}{2} + \frac{1}{2}\alpha S$
5	$[\sqrt[8]{2}](4[2] - 3[4])^{1/4}$	$\frac{-1}{4} + \frac{1}{4}\alpha S + \frac{2[3]-1}{4\cdot 5}(\alpha S)^2 + \frac{4[3]+3}{4\cdot 5^2}(\alpha S)^3$
7	$[\sqrt[19608]{2}](-39[6] - 16[4])^{1/6}$	$\frac{-1}{6} + \frac{-1}{6}\alpha S + \frac{[5]+2}{6\cdot 7}(\alpha S)^2 + \frac{-3[5]+8}{6\cdot 7^2}(\alpha S)^3 + \frac{19[5]-18}{6\cdot 7^3}(\alpha S)^4 + \frac{-39[5]+55}{6\cdot 7^4}(\alpha S)^5$

4 Acknowledgments

I would first of all like to thank Lyuboslav Panchev for all of his time, mentorship, and support, which has been invaluable to me throughout this whole

program. I would also like to thank Haynes Miller for proposing this problem, and for many conversations, through which I've learned most of what I know about algebraic topology. I'd also like to thank Slava Gerovitch, Ankur Moitra, and David Jerison for their tremendous effort in organizing SPUR, and particularly Ankur and David for their many helpful conversations and comments. Computations for this project were implemented and run in SageMath [3].

A Algorithms Based on Hewett's Construction

Here we present an algorithm for computing ζ_p based on Hewett's construction of G_1, which is supplanted by the main body of the paper but may be of some interest. This depends on the notion of a *cyclic algebra*, defined here:

Definition A.1. Let L/K be a cyclic field extension of degree n with Galois group generated by σ, and let $y \in K$. The *cyclic algebra* $\langle L/K, \sigma, y\rangle$ is the algebra $L\langle S\rangle$ subject to the restrictions $S^n = y$ and $Sx = \sigma(x)S$ for any $x \in L$.

In particular, we can identify $\mathrm{End}(F_n)[1/p]$ with the maximal order in $\langle K_n/\mathbb{Q}_p, \sigma, y\rangle$. Hewett's Theorem 6.8 produces a pair of cyclic algebras which he argues are isomorphic by non-constructive means.

Theorem A.2 (Hewett)**.** *Let r, σ_r be as in Section 2. Then, there is a $(p-1)^{st}$ root of unity y such that there is an isomorphism*

$$\psi : \langle \mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p, \sigma_r, y\rangle \to \langle K_n/\mathbb{Q}_p, \sigma, y\rangle.$$

Given such an isomorphism, we only need to compute $\psi(\zeta_p)$ to find our desired embedding. The general isomorphism problem for cyclic algebras over the same field has been studied by Hanke, who gives the following algorithm (See algorithms 5 and 7 in [5].)

Theorem A.3 (Hanke)**.** *There exists an isomorphism of cyclic algebras of degree n*

$$A_1 = \langle L_1/K, \sigma_1, b_1\rangle \to \langle L_2/K, \sigma_2, b_2\rangle = A_2$$

if and only if the following steps have a solution.

1. *Compute $x_1 \in L_1L_2$ such that $N_1(x_1) = b_1$.*
2. *Compute $x_2' \in L_1L_2$ such that*
$$\frac{\sigma_1(x_2')}{x_2'} = \frac{x_1}{\sigma_2(x_1)}.$$
3. *Compute $x_2'' \in L_2$ such that $N_2(x_2'') = b_2^{-1}N_2(x_2')$.*

If such an isomorphism exists, it can be computed via the following steps:

1. *Define*

$$\gamma : \langle L_1/K, \sigma_1, b_1\rangle \otimes \langle L_2/K, \sigma_2, b_2^{-1}\rangle \to \langle L_1/K, \sigma_1, 1\rangle \otimes \langle L_2/K, \sigma_2, 1\rangle$$

by sending the S_1 *to* $x_1 S_1$ *and* S_2 *to* $x_2''(x_2')^{-1}S_2$.

2. *For each of* $i = 1, 2$, *compute an isomorphism*

$$\phi_i : \langle L_i/K, \sigma_i, 1\rangle \to M_n(K)$$

via linear algebra.

3. *Use the previous steps to compute injections:*

$$\varphi_i : \langle L_i/K, \sigma_i, b_i\rangle \to \langle L_i/K, \sigma_i, 1\rangle \to M_n(K) \otimes M_n(K) = M_{n^2}(K)$$

4. *Fix a basis and identify* $M_{n^2}(K)$ *with* $\mathrm{End}_K(A_1)$.

5. *Choose a matrix* $X \in M_{n^2}(K)$ *such that* $X\varphi X^{-1} = \lambda$, *the left-regular representation of* A_1.

6. *Set* $\varphi_2' = X\phi_2 X^{-1}$, *and let* ρ *be the right-regular representation of* A_2.

7. *The desired isomorphism is then* $(\varphi_2')^{-1} \circ \rho$.

It is not too hard to compute x_1, x_2', x_2'', and a quick computation confirms the following proposition.

Proposition A.4. *Given* y *and* r *such that* $y \equiv r^{-1}$ *mod* p, *we can construct* x_1, x_2', *and* x_2'', *as follows (again using the notation from section* 2, *above.)*

$$\begin{aligned} x_1 &= y^{\frac{1}{1-p}} \\ x_2' &= Z(y, r) \\ x_2'' &= \alpha \end{aligned}$$

Therefore, an algorithm to compute $\zeta_p \in \mathbb{S}_n$ just needs to follow the above steps, and output $(\varphi_2')^{-1} \circ \rho(\zeta_p)$. We will not discuss this further.

References

[1] Mark Behrens and Michael J. Hopkins. Higher real k-theories and topological automorphic forms. *Journal of Topology*, 2011.

[2] Cedric Bujard. Finite subgroups of extended morava stabilizer groups. *preprint*, 2012. arXiv:1206.1951.

[3] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.2)*, 2016. `http://www.sagemath.org`.

[4] Paul Goerss, Hans-Werner Henn, and Charles Rezk. A resolution of the k(2)-local sphere at the prime 3. *Proceedings of the 2007 international symposium on symbolic and algebraic computation*, 2007.

[5] Timo Hanke. The isomorphism problem for cyclic algebras and an application. *Proceedings of the 2007 international symposium on symbolic and algebraic computation*, 2007.

[6] Hans-Werner Henn. On finite resolutions of k(n)-local spheres. In *Elliptic Cohomology, London Mathematical Society Lecture Note Series vol. 157*, pages 122–169. Cambridge University Press, Cambridge, 2007.

[7] Thomas Hewett. Finite subgroups of division algebras over local fields. *Journal of Algebra*, 173.3:518–548, 1995.

[8] Douglas C. Ravenel. *Complex cobordism and stable homotopy groups of spheres*. American Mathematical Soc., 2003.