Vol. 91, No. 3 DUKE MATHEMATICAL JOURNAL

CENTRALIZERS OF ELEMENTARY ABELIAN p-SUBGROUPS AND MOD-p COHOMOLOGY OF PROFINITE GROUPS

HANS-WERNER HENN

1. Introduction

1.1. Let G be a profinite group and p be a fixed prime. In this paper we will be concerned with $H_c^*(G;\mathbb{F}_p)$, the continuous cohomology of G with coefficients in the trivial module $\mathbb{F}_p$. We will abbreviate $H_c^*(G;\mathbb{F}_p)$ by $H^*(G;\mathbb{F}_p)$, or simply by H^*G if p is understood from the context. We recall that if G is the (inverse) limit of finite groups G_i, then $H^*G = \operatorname{colim} H^*G_i$.

Throughout this paper we will assume that H^*G is finitely generated as an $\mathbb{F}_p$-algebra. By work of Lazard [La], it is known that this holds for many interesting groups, for example, for profinite p-adic analytic groups like $GL(n,\mathbb{Z}_p)$, the general linear groups over the p-adic integers. In case H^*G is finitely generated as an $\mathbb{F}_p$-algebra, Quillen has shown [Q1] that there are only finitely many conjugacy classes of elementary abelian p-subgroups of G (i.e., groups isomorphic to $(\mathbb{Z}/p)^n$ for some natural number n). In other words, the following category $\mathscr{A}(G)$ is equivalent to a finite category: objects of $\mathscr{A}(G)$ are all elementary abelian p-subgroups of G; if E_1 and E_2 are elementary abelian p-subgroups of G, then the set of morphisms from E_1 to E_2 in $\mathscr{A}(G)$ consists precisely of those homomorphisms $\alpha : E_1 \to E_2$ of abelian groups for which there exists an element $g \in G$ with $\alpha(e) = geg^{-1}$ for all e in E_1. The category $\mathscr{A}(G)$ plays an important role both in Quillen's results and in the work presented here.

This category entered into Quillen's work as follows. The assignment $E \mapsto H^*E$ extends to a functor from the opposite category $\mathscr{A}(G)^{op}$ to graded $\mathbb{F}_p$-algebras and the restriction homomorphisms $H^*G \to H^*E$ (for E running through the elementary abelian p-subgroups of G) induce a canonical map of algebras $q : H^*G \to \lim_{\mathscr{A}(G)^{op}} H^*E$.

THEOREM 1.2 [Q1]. *Let G be a profinite group and assume that H^*G is a finitely generated $\mathbb{F}_p$-algebra. Then the canonical map $q : H^*G \to \lim_{\mathscr{A}(G)^{op}} H^*E$ is an F-isomorphism; in other words, q has the following properties.*

- *If $x \in \operatorname{Ker} q$, then x is nilpotent.*
- *If $y \in \lim_{\mathscr{A}(G)^{op}} H^*E$, then there exists an integer n with $y^{p^n} \in \operatorname{Im} q$.*

1.3. In our main result we use the full subcategory $\mathscr{A}_*(G)$ of $\mathscr{A}(G)$ whose objects are all elementary abelian p-subgroups except the trivial subgroup. The

Received 24 March 1995. Revision received 18 December 1996.

centralizer $C_G(E)$ of an elementary abelian p-subgroup E is a closed subgroup, and hence it inherits a natural profinite structure from G. The assignment $E \mapsto H^*C_G(E)$ extends to a functor from $\mathscr{A}_*(G)$ to graded $\mathbb{F}_p$-algebras, and the restriction homomorphisms $H^*G \to H^*C_G(E)$ (for E running through the nontrivial elementary abelian p-subgroups of G) induce a canonical map $\rho : H^*G \to \lim_{\mathscr{A}_*(G)} H^*C_G(E)$. Our main result reads as follows.

THEOREM 1.4. *Let G be a profinite group and assume that H^*G is a finitely generated $\mathbb{F}_p$-algebra. Then the canonical map $\rho : H^*G \to \lim_{\mathscr{A}_*(G)} H^*C_G(E)$ has finite kernel and cokernel.*

1.5. Remarks/Questions. (a) The map ρ of Theorem 1.4 is an actual isomorphism if G is a finite group or a compact Lie group (in the latter case H^*G has to be interpreted as the mod-p cohomology of the classifying space BG) provided G contains any elements of order p. This was first proved by Jackowski and McClure [JM] and then reproved and extended to certain classes of unstable algebras over the Steenrod algebra by Dwyer and Wilkerson [DW]. One's first reaction might be that because the continuous cohomology of a profinite group is the colimit of the cohomology of finite groups, the profinite case should be a direct consequence of the finite case by passing to appropriate (co)limits. However, one gets confronted with a subtle problem of interchanging limits and colimits, and this has the effect that ρ need not be an isomorphism for a profinite group.

In fact, our proof requires a different approach: in [He] we investigated an appropriately defined map ρ for any unstable algebra K over the Steenrod algebra which is finitely generated as an $\mathbb{F}_p$-algebra and showed that this map always has a finite kernel and cokernel (see Theorem 2.5). In Section 2 we explain this algebraic result and show how Theorem 1.4 can be deduced from it. We emphasize that we do not know any proof of Theorem 1.4 which does not use the Steenrod algebra, in particular, Lannes' T-functor, in a crucial way.

(b) Obviously, Theorem 1.4 gives more precise information than Theorem 1.2, but on the other hand, its applicability is more limited. For example, a major reason for working with $\mathscr{A}_*(G)$ instead of $\mathscr{A}(G)$ was to avoid the appearance of H^*G in the limit. However, if G contains central elements of order p, then H^*G does appear in the limit anyway, and Theorem 1.4 is not very useful. In other cases the functor $E \mapsto H^*C_G(E)$ may be too complicated to be evaluated. However, in these cases Theorem 1.4 may still be of some theoretical interest (see Sections 2.10 and 2.11 for examples).

(c) Theorem 1.4 says, in particular, that there is a minimal integer d such that ρ is an isomorphism in cohomological degrees greater than d. It would be interesting to have effective upper bounds for d in group-theoretical terms. For profinite p-analytic groups, the work of Lazard [La] suggests the dimension of such a group as a candidate for an upper bound for the number d. In fact, if such a group does not contain any elements of order p, as well as in the examples discussed in Sections 4 and 5, this actually gives a correct upper bound.

1.6. If G does not contain elements of order p, then the target of ρ is the trivial algebra, and Theorem 1.4 says that H^*G is a finite algebra. Of course, this could have also been directly deduced from Theorem 1.2.

However, Theorem 1.4 may already be quite interesting in case the p-rank of G is equal to one. We recall that the p-rank $r_p(G)$ of G is defined as the supremum of all natural numbers n such that G contains an elementary abelian p-subgroup E of rank n, that is, $E \cong (\mathbb{Z}/p)^n$. In the case $r_p(G) = 1$, the inverse limit simplifies substantially because $\mathscr{A}_*(G)$ is equivalent to the following discrete category: objects are in one-to-one correspondence with conjugacy classes of subgroups $E \cong \mathbb{Z}/p$; the only morphisms of this category are automorphisms and the automorphism group of an object E identifies with $N_G(E)/C_G(E)$, with $N_G(E)$ denoting the normalizer of E in G. In particular, we get the following corollary.

COROLLARY 1.7. *Let G be a profinite group and assume that H^*G is a finitely generated $\mathbb{F}_p$-algebra and $r_p(G) = 1$. Then the restriction maps induce a map*

$$\rho : H^*G \to \prod_{(E)} (H^*C_G(E))^{N_G(E)}$$

with finite kernel and cokernel. (Here the product is taken over conjugacy classes of elementary abelian p-subgroups of rank 1.) $\square$

Note that the group $N_G(E)/C_G(E)$ is of order prime to p if E is of rank 1. Therefore the invariants $(H^*C_G(E))^{N_G(E)}$ are isomorphic to $H^*N_G(E)$ and Corollary 1.7 can be considered as a "profinite analogue" of Brown's result [B] on the Farell cohomology of discrete groups of p-rank 1. In this case, the number d introduced in Section 1.5(c) above corresponds to the virtual cohomological dimension of G.

1.8. As mentioned above, Section 2 will be concerned with the proof of Theorem 1.4 and related results. In Sections 3 and 4 we will study certain subgroups of the group of units in p-adic division algebras, and in Section 5 we will touch upon the general linear group over the p-adic integers.

To get more explicit, we fix a prime p and a natural number n. Consider $\mathbb{D}_n$, the division algebra with invariant $1/n$ over the field of p-adic numbers $\mathbb{Q}_p$ and $\mathcal{O}_n$, the maximal compact subring of $\mathbb{D}_n$. $\mathcal{O}_n$ is a local ring and reducing modulo its maximal ideal gives a homomorphism from $\mathcal{O}_n$ to the finite field $\mathbb{F}_q$ with $q = p^n$. Let $\mathcal{O}_n^\times$ denote the units of $\mathcal{O}_n$, and let S_n denote the kernel of the map $\mathcal{O}_n^\times \to \mathbb{F}_q^\times$. In stable homotopy theory these groups are known as Morava stabilizer groups, and their cohomology is known to play a central role in the chromatic theory of stable homotopy (see [M], [Ra2], [Ra3], [D], and [HG], for example).

It is well known that $r_p(S_n) = r_p(\mathcal{O}_n^\times) \leqslant 1$ and equality holds if and only if $n \equiv 0 \bmod (p-1)$. Our results give new insight if $n \equiv 0 \bmod (p-1)$. Using standard facts about division algebras, we determine the categories $\mathscr{A}_*(\mathcal{O}_n^\times)$ and $\mathscr{A}_*(S_n)$ for $n \equiv 0 \bmod (p-1)$ and describe the structure of the centralizers of the elementary abelian p-subgroups (Theorem 3.2.2). Furthermore, for $n = p-1$ the centralizers turn out to be abelian, and we can compute the target of ρ explicitly; hence H^*S_n up to finite ambiguity. In particular, we obtain in Section 3.3 the following result in which $E(-)$ denotes an exterior algebra over $\mathbb{F}_p$ on the specified elements. The elements y_i are of degree 2 and the elements x_i and $a_{i,j}$ are of degree 1. For more details about the definition of these elements the reader is referred to Sections 3.3 and 3.4.

THEOREM 1.9. *Let p be an odd prime, $n = p-1$, and $s = (p^n-1)/(p-1)^2$. Then there is a homomorphism*

$$\rho : H^*S_n \to \prod_{i=1}^{s} \mathbb{F}_p[y_i] \otimes E(x_i) \otimes E(a_{i,1}, \ldots, a_{i,n})$$

with finite kernel and cokernel.

We remark that previously the mod-p cohomology of S_n was computed by Ravenel [Ra1] in the following cases: H^1S_n and H^2S_n for all n and p, all of H^*S_n if either $n \leqslant 2$ and p arbitrary, or if $n = 3$ and $p \geqslant 5$. So the only overlap between Ravenel's computation and Theorem 1.9 occurs for $p = 3$ and $n = 2$ [Ra1, Thm 3.3]. In Section 4 we use Theorem 1.9 together with some more detailed group-theoretical analysis of S_2 to give an independent computation of H^*S_n if $p = 3$ and $n = 2$. In this case, we find that ρ is injective, and we use this to describe H^*S_2 as an explicit subalgebra of $\prod_{i=1}^{2} \mathbb{F}_3[y_i] \otimes E(x_i) \otimes E(a_{i,1}, a_{i,2})$ (Theorem 4.2). The multiplicative structure of the result derived here differs from that of Ravenel, although additively the two results agree. Ravenel has informed me that he now believes that there is a mistake in his calculation. Finally, we remark that Gorbounov, Siegel, and Symonds [GSS] have independently and with very different methods confirmed the calculation in Theorem 4.2.

The calculations of H^*S_2 for primes $p > 3$ have been used by Shimomura and Yabe [SY] to determine the stable homotopy groups of $L_2S_p^0$, the second stage in the chromatic tower of the p-local sphere. The computation of H^*S_2 at the prime 3 will be relevant for understanding $L_2S_p^0$ if $p = 3$, and for this reason we have decided to give a rather detailed presentation in Section 4. In fact, Shimomura [S] has already used the corrected computation of H^*S_2 to compute the homotopy groups of the L_2-localization of the Toda-Smith complex $V(1)$ at the prime 3 up to a certain ambiguity. This ambiguity will be settled in a joint work with Mahowald [HM] using the approach towards H^*S_2 via centralizers of elementary abelian p-subgroups that we introduce in this paper.

1.10. Our second application concerns the mod-p cohomology of the general linear groups $GL(n, \mathbb{Z}_p)$. The following result should be compared with Ash's computations [A] of the Farrell cohomology of $GL(n, \mathbb{Z})$. As above, the element y has degree 2 while all other elements are of degree 1.

THEOREM 1.10. *Let p be an odd prime and let $n = p - 1$. Then there is a homomorphism*

$$\rho : H^*GL(n, \mathbb{Z}_p) \to (\mathbb{F}_p[y] \otimes E(x) \otimes E(a_1, \ldots, a_n))^{\mathbb{Z}/n}$$

with finite kernel and cokernel. (Here $(-)^{\mathbb{Z}/n}$ denotes the invariants with respect to the following action of $\mathbb{Z}/n$ by algebra homomorphisms. After choosing a suitable isomorphism $\tau : \mathbb{Z}/n \to \mathbb{F}_p^\times$, this action is given by $gy = \tau(g)y$, $gx = \tau(g)x$, and $ga_j = \tau(g)^j a_j$ for $j = 1, \ldots, n$ if $g \in \mathbb{Z}/n$.)

This result looks very similar to Theorem 1.9. In fact, the similarity becomes even stronger if one compares (for $n = p - 1$) the groups $\mathcal{O}_n^\times$ and $GL(n, \mathbb{Z}_p)$. In this case, the targets of the two maps ρ agree (cf. Thm 3.2.2 and Thm 5.2).

As in the case of S_n, we give the complete computation for $p = 3$ and $n = 2$ (Proposition 5.5).

Acknowledgements. The author was partially supported by a Heisenberg fellowship of the Deutsche Forschungsgemeinschaft. The origin of this paper can be traced back to a one-month visit to Aarhus in the fall of 1990. This work was then pushed further during a three-month visit at the Mittag Leffler Institute in the fall of 1993. I would like to thank the staff at both institutions for providing such pleasant and stimulating working conditions. It is a pleasure to express special thanks to Bob Oliver on both occassions.

2. The proof of Theorem 1.4 and related results. As already indicated in the introduction, Theorem 1.4 is deduced from a general result about certain unstable algebras over the Steenrod algebra A (see [He]). We will begin by recalling some facts about Lannes' T functor that are necessary to explain the main algebraic result of [He] and to deduce Theorem 1.4 from it.

2.1. Let $\mathcal{U}$ (resp., $\mathcal{K}$) denote the category of unstable modules (resp., unstable algebras) over the mod-p Steenrod algebra A (see [L1]). The cohomology of a space is an unstable algebra; in particular, the cohomology of any finite group and then also the cohomology of any profinite group is such an algebra. The Steenrod algebra is actually a Hopf algebra, and its diagonal gives rise to a tensor product on the categories $\mathcal{U}$ (resp., $\mathcal{K}$).

Now let V be an elementary abelian p-group with mod-p cohomology H^*V. Lannes [L1] has introduced the functor $T_V : \mathcal{U} \to \mathcal{U}$. It is left adjoint to tensoring with H^*V, that is, $\mathrm{Hom}_{\mathcal{U}}(T_V M, N) \cong \mathrm{Hom}_{\mathcal{U}}(M, H^*V \otimes N)$ for all unstable modules M and N. T_V has a number of remarkable properties. In particular, T_V lifts to a functor from $\mathcal{K}$ to itself, and the adjunction relation continues to hold in $\mathcal{K}$: $\mathrm{Hom}_{\mathcal{K}}(T_V K, L) \cong \mathrm{Hom}_{\mathcal{K}}(K, H^*V \otimes L)$ for all unstable algebras K and L.

2.2. Now let G be a finite group. The following computation of $T_V H^*G$ in [L2] (for a more accessible reference see also [L1, 3.4]) is quite crucial for the proof of Theorem 1.4.

Denote by $\operatorname{Rep}(V,G)$ the set of G-conjugacy classes of homomorphisms from V to G. For each conjugacy class choose a representative φ and denote the centralizer of $\operatorname{Im}\varphi$ in G by $C_G(\varphi)$. The homomorphism $c_\varphi : V \times C_G(\varphi) \to G$, $(v,g) \mapsto v\varphi(g)$ induces a map of unstable algebras $c_\varphi^* : H^*G \to H^*V \otimes H^*C_G(\varphi)$ that is adjoint to a map of unstable algebras $\operatorname{ad}(c_\varphi^*) : T_V H^*G \to H^*C_G(\varphi)$.

THEOREM 2.2 [L2]. *The homomorphism of unstable algebras*

$$T_V H^*G \to \prod_{\varphi \in \operatorname{Rep}(V,G)} H^*C_G(\varphi)$$

whose components are the maps $\operatorname{ad}(c_\varphi^*)$ *is an isomorphism for each finite group* G. □

Note that the theorem shows in particular that the natural map from $\operatorname{Rep}(V,G)$ to $\operatorname{Hom}_{\mathscr{K}}(H^*G, H^*V)$, which sends φ to its induced map φ^*, is a bijection.

We also see that the terms in the inverse limit occuring in Theorem 1.4 appear in the computation of $T_V H^*G$. Dwyer and Wilkerson [DW] noticed that this allows a purely algebraic approach to the map ρ of Theorem 1.4 which makes sense for a much larger class of unstable algebras. In order to explain this, we need some more preparations (see [DW] and [HLS, I.4 and I.5]).

2.3. To an unstable algebra K we associate a category $\mathscr{R}(K)$ as follows. Its objects are the morphisms of unstable algebras $\varphi : K \to H^*V$, V an elementary abelian p-group for which H^*V becomes a finitely generated K-module via φ; sometimes it will be convenient to denote such an object by the pair (V,φ). Then the set of morphisms from (V_1,φ_1) to (V_2,φ_2) are all homomorphisms $V_1 \xrightarrow{\alpha} V_2$ of abelian groups such that $\varphi_1 = \alpha^*\varphi_2$. If K is Noetherian, the opposite of this category was first investigated by Rector [Rc]. The full subcategory of $\mathscr{R}(K)$ having as objects all (V,φ) with V nontrivial will be denoted by $\mathscr{R}_*(K)$.

If $K = H^*BG$, then $\mathscr{R}(K)$ is equivalent to Quillen's category $\mathscr{A}(G)$ and $\mathscr{R}_*(K)$ is equivalent to $\mathscr{A}_*(G)$. In fact, in this case, the computation of $\operatorname{Hom}_{\mathscr{K}}(H^*G, H^*V)$ (see Section 2.2 above) can be used to identify the objects of $\mathscr{R}(K)$ with the monomorphic representations of elementary abelian p-groups in G, and an equivalence between $\mathscr{R}(K)$ and a skeleton of $\mathscr{A}(G)$ is induced by associating to a homomorphism $\varphi : V \to G$ the unique object in the skeleton of $\mathscr{A}(G)$ that is isomorphic to the image of φ (see [HLS, I.5.3]).

2.4. Now consider the unstable algebra $T_V K$. For a morphism $\varphi : K \to H^*V$ we obtain a connected component $T_V(K;\varphi)$ of $T_V K$; it is defined as $T_V(K;\varphi) := \mathbb{F}_p(\varphi) \otimes_{T_V^0 K} T_V K$, where $\mathbb{F}_p(\varphi)$ denotes $\mathbb{F}_p$ considered as a module over $T_V^0 K$, the subalgebra of elements of degree 0 in $T_V K$, via the adjoint of φ.

More generally, we can consider the category $K - \mathscr{U}$ whose objects are unstable A-modules M with A-linear K-module structure maps $K \otimes M \to M$, and whose morphisms are all A-linear maps which are also K-linear. The full subcategory of $K - \mathcal{U}$ consisting of those objects which are finitely generated as K-modules is denoted by $K_{fg} - \mathcal{U}$.

If M is in $K - \mathcal{U}$, then $T_V M$ is in $T_V K - \mathcal{U}$, and one can define components $T_V(M;\varphi) := \mathbb{F}_p(\varphi) \otimes_{T_V^0 K} T_V M$ that are modules over the corresponding components $T_V(K;\varphi)$. From the adjoint of the identity of $T_V K$, we obtain canonical algebra morphisms $\rho_{K,(V,\varphi)}$ from K to $T_V(K;\varphi)$. Hence, $T_V(M;\varphi)$ can be considered as a K-module, and the assignment $(V,\varphi) \mapsto T_V(M;\varphi)$ gives rise to a functor from $\mathcal{R}(K)$ to $K - \mathcal{U}$. Furthermore, the adjoint of the identity of $T_V M$ gives rise to maps $\rho_{M,(V,\varphi)}$ from M to $T_V(M;\varphi)$ that are all K-linear, and we obtain a natural transformation between the constant functor from $\mathcal{R}(K)$ to $K - \mathcal{U}$ with value M and the functor $(V,\varphi) \mapsto T_V(M;\varphi)$.

If G is a finite group and $K = M = H^*G$, then Theorem 2.2 implies that the functor $(V,\varphi) \mapsto T_V(M;\varphi)$ corresponds via the equivalence between $\mathcal{R}(K)$ and $\mathcal{A}(G)$ to the functor $E \mapsto H^*C_G(E)$ that appears in Theorem 1.4. Furthermore, the maps $\rho_{M,(V,\varphi)}$ correspond to the restriction maps $H^*G \to H^*C_G(\varphi)$.

Now we are ready to formulate the general algebraic theorem from which Theorem 1.4 is deduced.

THEOREM 2.5 [He, Cor. 3.10]. *Let K be a Noetherian unstable algebra, and let M be an object in $K_{fg} - \mathcal{U}$. Then the maps $\rho_{M,(V,\varphi)}$ induce a map*

$$\rho : M \to \lim_{\mathcal{R}_*(K)} T_V(M;\varphi)$$

that has finite kernel and cokernel. □

In fact, it is shown in [He] that this map is localization away from finite objects in $K_{fg} - \mathcal{U}$.

Theorem 2.5 together with Theorem 2.2 yields Theorem 1.4 in the case of a finite group (in which case ρ is even an isomorphism by [JM] and [DW]). To prove Theorem 1.4 for profinite groups G for which H^*G is a finitely generated $\mathbb{F}_p$-algebra, it suffices to extend Theorem 2.2 to this setting. We recall that a profinite group G is given as the (inverse) limit $\lim_i G_i$ of finite groups G_i along a directed partially ordered set $(\mathcal{I}, \leqslant)$, which we think of as a category (denoted $\mathcal{I}$ for simplicity) in the usual way. Then H^*G can be identified with $\operatorname{colim}_i H^*G_i$. Here is the extension of Theorem 2.2.

THEOREM 2.6. *Assume that G is a profinite group such that H^*G is a finitely generated $\mathbb{F}_p$-algebra. Then the homomorphism of unstable algebras*

$$T_V H^*G \to \prod_{\varphi \in \operatorname{Rep}(V,G)} H^*C_G(\varphi),$$

whose components are the maps $\operatorname{ad}(c_\varphi^*)$, is an isomorphism.

In this result, the set $\operatorname{Rep}(V, G)$ of representations is defined as before, that is, the topology on G does not play any role. However, the centralizer of an elementary abelian p-subgroup of a profinite group inherits a natural structure of a profinite group, and this structure is used in Theorem 2.6.

Proof. We deduce Theorem 2.6 from Theorem 2.2. For this we note that T_V commutes with arbitrary colimits, that is, we get

$$T_V H^* G = \operatorname*{colim}_i T_V H^* G_i \cong \operatorname*{colim}_i \prod_{\varphi \in \operatorname{Rep}(V, G_i)} H^* C_{G_i}(\varphi).$$

Let us look more carefully at the maps in the inverse system. For a morphism $\lambda : i \to j$ in $\mathscr{I}$, we use the same letter for the associated maps from G_j to G_i and from $C_{G_j}(\varphi)$ to $C_{G_i}(\lambda\varphi)$ (with $\varphi \in \operatorname{Rep}(V, G_j)$). If we identify $T_V H^* G_i$ as in Theorem 2.2, then the map $T_V\lambda^* : T_V H^* G_i \to T_V H^* G_j$ is given as follows: the φth component of it ($\varphi \in \operatorname{Rep}(V, G_j)$) sends the family $\{x_{\varphi'}\} \in \prod_{\varphi' \in \operatorname{Rep}(V, G_i)} H^* C_{G_i}(\varphi')$ to the element $\lambda^*(x_{\lambda\varphi}) \in H^* C_{G_j}(\varphi)$. Here, λ^* is the induced map from $H^* C_{G_i}(\lambda\varphi)$ to $H^* C_{G_j}(\varphi)$. In fact, in the same way, we get maps $T_V \pi_i^*$ from $\prod_{\varphi' \in \operatorname{Rep}(V, G_i)} H^* C_{G_i}(\varphi')$ to $\prod_{\varphi \in \operatorname{Rep}(V, G)} H^* C_G(\varphi)$ if π_i denotes the canonical map from G to G_i. These maps fit together and thus give a map

$$\operatorname*{colim}_i \prod_{\varphi' \in \operatorname{Rep}(V, G_i)} H^* C_{G_i}(\varphi') \to \prod_{\varphi \in \operatorname{Rep}(V, G)} H^* C_G(\varphi),$$

which we denote $T_V \pi^*$ by abuse of notation, and which we claim to be an isomorphism. In order to show this, we need the following lemmas.

LEMMA 2.7. *Let $G = \lim G_i$ be any profinite group.*

(a) *Then the maps $\pi_i : G \to G_i$ induce a bijection* $\operatorname{Rep}(V, G) \to \lim_i \operatorname{Rep}(V, G_i)$ *of profinite sets for each elementary abelian p-group V.*

(b) *For any homomorphism φ from an elementary abelian p-group V into G, the maps $\pi_i : G \to G_i$ induce an isomorphism $C_G(\varphi) \to \lim_i C_{G_i}(\pi_i\varphi)$ of profinite groups.*

LEMMA 2.8. *Let G be any profinite group for which $H^* G$ is a finitely generated $\mathbb{F}_p$-algebra. Then the set* $\operatorname{Rep}(V, G)$ *is finite for each elementary abelian p-group V.*

We postpone the proofs of Lemmas 2.7 and 2.8 and continue with the proof of Theorem 2.6.

First we show that $T_V \pi^*$ is epi. Let $x = \{x_\varphi\} \in \prod_{\varphi \in \operatorname{Rep}(V, G)} H^* C_G(\varphi)$ be given. For each $\varphi \in \operatorname{Rep}(V, G)$ we find by Lemma 2.7(b) an object $i = i(\varphi)$ of $\mathscr{I}$ and an element $y_i \in H^* C_{G_i}(\pi_i\varphi)$ such that $x_\varphi = (\pi_i)^* y_i$. By Lemma 2.8 there are only finitely many φ, and therefore we can assume that i is independent of φ. Furthermore, by Lemmas 2.7(a) and 2.8, we can choose i such that, in addition, the natural map $\operatorname{Rep}(V, G) \to \operatorname{Rep}(V, G_i)$ is injective. For such an i and any $\varphi' \in \operatorname{Rep}(V, G_i)$, let $z_{\varphi'} \in H^*C_{G_i}(\varphi')$ be equal to $y_{i(\varphi)}$ if $\varphi' = \pi_i\varphi$ for some (necessarily unique) φ, and arbitrarily choose elements $z_{\varphi'}$ if there is no φ such that $\varphi' = \pi_i\varphi$. Then the family $z = \{z_{\varphi'}\} \in \prod_{\varphi' \in \operatorname{Rep}(V,G_i)} H^*C_{G_i}(\varphi')$ satisfies $T_V\pi_i^*(z) = x$, and hence $T_V\pi^*$ is epi.

To see that $T_V\pi^*$ is mono, we show that for any element $z = \{z_{\varphi'}\} \in \prod_{\varphi' \in \operatorname{Rep}(V,G_i)} H^*C_{G_i}(\varphi')$ with $T_V\pi^*(z) = 0$, there is $\mu : i \to j$ in $\mathscr{I}$ such that $T_V\mu^*(z) = 0$. Now $T_V\pi^*(z) = 0$ implies by Lemma 2.7(b) that for each φ' there is $\lambda_{\varphi'} : i \to j(\varphi')$ such that for each lift φ of φ' to $\operatorname{Rep}(V, G_{j(\varphi')})$, which further lifts to $\operatorname{Rep}(V, G)$, we get $(\lambda_{\varphi'})^*(z_{\varphi'}) = 0$ in $H^*C_{G_{j(\varphi')}}(\varphi)$. As there are only finitely many φ', we can choose a common $\lambda : i \to j$ such that $\lambda^*(z_{\varphi'}) = 0$ in $H^*C_{G_j}(\varphi)$ for each φ' and each lift φ of φ' to $\operatorname{Rep}(V, G_j)$, which further lifts to $\operatorname{Rep}(V, G)$. Furthermore, by Lemma 2.7(a), we can find $\lambda' : j \to j'$ such that each element $\varphi \in \operatorname{Rep}(V, G_j)$ that does not lift to $\operatorname{Rep}(V, G)$ does not lift to $\operatorname{Rep}(V, G_{j'})$ either. If $\mu = \lambda'\lambda : i \to j'$, then it is clear that $T_V\mu^*(z) = 0$. □

Proof of Lemma 2.7. The proof is an exercise in elementary point set topology. We sketch part (a) and leave part (b) to the reader.

Let us first show surjectivity. So assume we have a compatible family of elements $\varphi_i \in \operatorname{Rep}(V, G_i)$. For a subset $\mathscr{J}$ of $\mathscr{I}$ let $\operatorname{Rep}_{\mathscr{J}}$ be the set of families of homomorphisms $\{\phi_i\} \in \prod_{i \in \mathscr{I}} \operatorname{Hom}(V, G_i)$ such that the conjugacy class of ϕ_i is equal to φ_i whenever $i \in \mathscr{J}$ and such that the ϕ_i are compatible as long as $i \in \mathscr{J}$. We have to show that $\operatorname{Rep}_{\mathscr{I}}$ is nonempty. Because any two elements of $\mathscr{I}$ have an upper bound, it is clear that $\operatorname{Rep}_{\mathscr{J}}$ is nonempty whenever $\mathscr{J}$ is finite. Furthermore, $\operatorname{Rep}_{\mathscr{J}}$ is easily seen to be closed for any $\mathscr{J}$. Now we use that the intersection of closed sets in a compact space is nonempty if every finite intersection is nonempty, and we are done.

Next assume that we have two elements φ and φ' in $\operatorname{Rep}(V, G)$ represented by homomorphisms ϕ and ϕ' such that $\pi_i\phi$ and $\pi_i\phi'$ are conjugate for each i; that is, there is an element $g_i \in G_i$ with $\pi_i\phi(v) = g_i\pi_i\phi'(v)g_i^{-1}$ for all $v \in V$. For injectivity in (a), it is enough to show that the family g_i can be chosen to be compatible. Again, this is easy for any finite subset of $\mathscr{I}$, and the general case follows again from the fact that an intersection of closed sets in a compact space is nonempty if every finite intersection is nonempty. □

Proof of Lemma 2.8. For any profinite G, we have by Theorem 2.2 and Lemma 2.7(a)

$$\operatorname{Rep}(V, G) \cong \lim_i \operatorname{Rep}(V, G_i) \cong \lim_i \operatorname{Hom}_{\mathscr{K}}(H^*G_i, H^*V).$$

Furthermore, we can identify $\lim_i \operatorname{Hom}_{\mathscr{K}}(H^*G_i, H^*V)$ with $\operatorname{Hom}_{\mathscr{K}}(H^*G, H^*V)$. Finally, if H^*G is a finitely generated $\mathbb{F}_p$-algebra, then the set $\operatorname{Hom}_{\mathscr{K}}(H^*G, H^*V)$ is clearly finite, and hence we are done. □

2.9. We would like to point out that Theorem 2.2 can be used to derive numerous qualitative results on cohomology of finite groups. Among them are results concerning detection of H^*G on certain subgroups, results giving bounds for the nilpotence degree of elements in H^*G and results on the existence of elements in H^*G with particular restriction behavior to elementary abelian p-subgroups (cf. [HLS, I.5] and [CH]). Because of Theorem 2.6, all these results have anologues for continuous cohomology of profinite groups G as long as H^*G is a finitely generated $\mathbb{F}_p$-algebra. We list here only the following result which is a special case of the profinite analogue of Theorem 2 of [CH].

PROPOSITION 2.10. *Let G be profinite with p-rank 1 and assume that H^*G is finitely generated as an $\mathbb{F}_p$-algebra. Then the map*

$$\rho : H^*G \to \prod_{(E)} (H^*C_G(E))^{N_G(E)}$$

(cf. Cor. 1.7) is a monomorphism if and only if H^*G is free over a polynomial subalgebra of H^*G with one generator.

Proof. Assume that H^*G is free over a polynomial subalgebra on one generator. Then the same is true for any nontrivial ideal in H^*G, in particular for the kernel of the map ρ. However, by Corollary 1.7, this ideal is finite; hence, it must be trivial.

Conversely, assume that ρ is a monomorphism. Take any element x in H^*G that restricts to a nonnilpotent element on all nontrivial elementary abelian p subgroups of rank 1. Such an x exists by Theorem 1.2. We can consider the cohomology of $H^*C_G(E)$ as a module over the polynomial subalgebra of H^*G generated by x (again via a restriction homomorphism). Now the proof of Theorem 1.1 in [BH] (see also Remark 2.3 in the same paper) shows that $H^*C_G(E)$ is free over this polynomial subalgebra. By assumption, H^*G is a submodule of the free module $\prod_{(E)} H^*C_G(E)$, and hence it is also free. □

2.11. Finally we want to point out that Theorem 1.4 can also be used to get information on cohomology with nontrivial coefficients. For example, assume M is a finite continuous G-module with a composition series for which all successive subquotients are trivial modules. (Such composition series exist always if G is a pro-p group.) Furthermore, assume that the p-rank of G is 1 and $\rho : H^*G \to \prod_{(E)}(H^*C_G(E))^{N_G(E)}$ is an isomorphism in degrees greater than d. Then playing with the long exact sequences in cohomology associated to short exact sequences of coefficient modules shows that the map $\rho : H^*(G;M) \to \prod_{(E)}(H^*(C_G(E);M))^{N_G(E)}$ is an isomorphism in all degrees greater than $d+1$.

3. The case of the stabilizer groups

3.1. In this section we will apply our general results to certain subgroups of p-adic division algebras that play an important role in stable homotopy theory.

We begin by recalling the definition and basic properties of these groups. The reader is referred to [Rn, Chaps. 3 and 7] and [Ha, 20.2.16 and 23.1.4] for background information on division algebras.

3.1.1. Let p be a prime. For each integer n let $\mathbb{W}_n$ be the ring of Witt vectors of the finite field $\mathbb{F}_q$ with $q = p^n$ elements, and let $\sigma : \mathbb{W}_n \to \mathbb{W}_n$, $w \mapsto w^\sigma$ be the lift of the Frobenius automorphism $x \mapsto x^p$ on $\mathbb{F}_q$. Adjoin an element S to $\mathbb{W}_n$ subject to the relations $S^n = p$, $Sw = w^\sigma S$ for each $w \in \mathbb{W}_n$. The resulting non-commutative ring will be denoted by $\mathcal{O}_n$. It is the maximal order in the central division algebra $\mathbb{D}_n$ over the field $\mathbb{Q}_p$ of p-adic numbers with invariant $1/n$ and is a free module over $\mathbb{W}_n$ of rank n with generators the elements $S^i, 0 \leqslant i < n$. An important property of $\mathbb{D}_n$ that we will use below is that the degree (over $\mathbb{Q}_p$) of each commutative subfield of $\mathbb{D}_n$ divides n, and each extension of $\mathbb{Q}_p$ whose degree divides n can be embedded as a commutative subfield of $\mathbb{D}_n$.

We recall that $\mathcal{O}_n$ can be identified with the endomorphism ring of a certain formal group law over $\mathbb{F}_q$ of height n [Ha, Thm. 20.2.13]. Its group of units $\mathcal{O}_n^\times$ is often called the nth (full) Morava stabilizer group. The element S generates a two-sided maximal ideal $\mathfrak{m}$ in $\mathcal{O}_n$ with quotient $\mathcal{O}_n/\mathfrak{m} = \mathbb{F}_q$. The kernel of the resulting epimorphism of groups $\mathcal{O}_n^\times \to (\mathbb{F}_q)^\times$ will be denoted by S_n and is also called the (strict) Morava stabilizer group; it can be identified with the group of strict automorphisms of the same formal group law over $\mathbb{F}_q$ height n.

3.1.2. The groups $\mathcal{O}_n^\times$ and S_n have natural profinite structures which can be described as follows. The valuation v on $\mathbb{Q}_p$ (normalized such that $v(p) = 1$) extends uniquely to a valuation on $\mathbb{D}_n$ such that $v(S) = 1/n$ and $\mathcal{O}_n = \{x \in \mathbb{D}_n | v(x) \geqslant 0\}$. The two-sided maximal ideal $\mathfrak{m}$ is given by $\mathfrak{m} = \{x \in \mathbb{D}_n | v(x) > 0\}$. The valuation gives subgroups

$$F_i S_n := \{x \in S_n | v(1-x) \geqslant i\} = \{x \in S_n | x \equiv 1 \operatorname{mod} S^{ni}\}$$

for positive multiples i of $1/n$ with

$$S_n = F_{1/n} S_n \supset F_{2/n} S_n \cdots .$$

The intersection of all these subgroups contains only the element 1 and S_n is complete with respect to this filtration, that is, we have $S_n = \lim_i S_n / F_i S_n$. Furthermore, we have canonical isomorphisms

$$F_i S_n / F_{i+1/n} S_n \cong \mathbb{F}_q$$

induced by

$$x = 1 + aS^i \mapsto \bar{a}.$$

Here a is an element in $\mathcal{O}_n$, that is, $x \in F_i S_n$ and $\bar{a}$ is the residue class of a in

$\mathcal{O}_n/\mathfrak{m} = \mathbb{F}_q$ In particular, all the quotients S_n/F_iS_n are finite p-groups, and hence S_n is a profinite p-group which is the p-Sylow subgroup of the profinite group $\mathcal{O}_n^\times$.

3.1.3. The associated graded object $\operatorname{gr} S_n$ with $\operatorname{gr}_i S_n = F_iS_n/F_{i+1/n}S_n$ becomes a graded Lie algebra with Lie bracket $[\bar{a}, \bar{b}]$ induced by the commutator $xyx^{-1}y^{-1}$ in S_n. Furthermore, if we define a function φ from the positive real numbers to itself by $\varphi(i) := \min\{i+1, pi\}$, then the pth power map on S_n induces maps $P : \operatorname{gr}_i S_n \to \operatorname{gr}_{\varphi(i)} S_n$ that define on $\operatorname{gr} S_n$ the structure of a mixed Lie algebra in the sense of Lazard [La, Chap. II.1]. If we identify the filtration quotients with $\mathbb{F}_q$ as in Section 3.1.2 above, then the Lie bracket and the map P are explicitly given as follows.

LEMMA 3.1.4. *(a) Let $\bar{a} \in \operatorname{gr}_i S_n$, $\bar{b} \in \operatorname{gr}_j S_n$. Then*

$$[\bar{a}, \bar{b}] = \bar{a}\bar{b}^{p^{ni}} - \bar{b}\bar{a}^{p^{nj}} \in \operatorname{gr}_{i+j} S_n.$$

(b) Let $\bar{a} \in \operatorname{gr}_i S_n$. Then

$$P\bar{a} = \begin{cases} \bar{a}^{1+p^{ni}+\cdots+p^{(p-1)ni}} & \text{if } i < (p-1)^{-1}, \\ \bar{a} + \bar{a}^{1+p^{ni}+\cdots+p^{(p-1)ni}} & \text{if } i = (p-1)^{-1}, \\ \bar{a} & \text{if } i > (p-1)^{-1}. \end{cases}$$

Proof. (a) Write $i = k/n$, $j = l/n$ and choose representatives $x = 1 + aS^k \in F_iS_n$, $y = 1 + bS^l \in F_jS_n$. Then $x^{-1} = 1 - aS^k \bmod S^{k+1}$, $y^{-1} = 1 - bS^l \bmod S^{l+1}$, and the formula

$$xyx^{-1}y^{-1} = 1 + ((x-1)(y-1) - (y-1)(x-1))x^{-1}y^{-1}$$

shows

$$xyx^{-1}y^{-1} = 1 + (aS^kbS^l - bS^laS^k) \bmod S^{k+l+1}.$$

Because $\mathcal{O}_n/\mathfrak{m} \cong \mathbb{W}_n/(p)$, we can choose a and b from $\mathbb{W}_n$. Then $Sw = w^\sigma S$ and $w^\sigma \equiv w^p \bmod (p)$ give the stated formula.

(b) Again we write $i = k/n$ and choose a representative $x = 1 + aS^k$ with $a \in \mathbb{W}_n$. Consider the expression $x^p = \sum_r \binom{p}{r}(aS^k)^r$. Because $\binom{p}{r}$ is divisible by p for $0 < r < p$, and because $S^n = p$, we get

$$x^p \equiv 1 + aS^{n+k} + \cdots + (aS^k)^p \bmod S^{2k+n}.$$

Furthermore,

$$(aS^k)^p = aa^{\sigma^k} \cdots a^{\sigma^{(p-1)k}} S^{pk} \equiv aa^{p^k} \cdots a^{p^{(p-1)k}} S^{pk} \equiv a^{1+p^k+\cdots+p^{(p-1)k}} S^{pk} \bmod S^{pk+1}.$$

Now we only have to determine whether pk is smaller (resp., equal; resp., larger) than $n+k$, that is, whether pi is smaller (resp., equal; resp., larger) than $1+i$. These cases are equivalent to $i<(p-1)^{-1}$ (resp., $i=(p-1)^{-1}$; resp., $i>(p-1)^{-1}$), and hence we are done. □

Remark. One can use Lemma 3.1.4 to compute $H^1(F_iS_n)$, respectively, $H_1(F_iS_n)$. (Coefficients are, as always, in $\mathbb{F}_p$.) For example, by using [La, III.2.1; in particular, III.2.1.8] we can derive the following. If $i>(p-1)^{-1}$, then the quotient map $F_iS_n \to F_iS_n/F_{i+1}S_n$ induces an isomorphism on H_1. Furthermore, if $i \geqslant 1$, then $F_iS_n/F_{i+1}S_n$ is elementary abelian of rank n^2 and, if p is odd and $i \geqslant 1$, then $H^*F_iS_n$ is an exterior algebra on $H^1F_iS_n$ (see [La, V.2.2.7]). Ravenel claims in [Ra2, Thm 6.3.7] that $H^*F_iS_n$ is exterior on n^2 generators in dimension 1 as soon as $i>p/2(p-1)$. (Note that Ravenel's i corresponds to i/n in our notation!) However, if $p=5$, $n=4$, and $i=3/4$, it is not hard to show (using Lemma 3.1.4) that the abelianization of $F_iS_n/F_{i+1}S_n$ is $F_iS_n/F_{i+((n-1)/n)}S_n$ which is elementary abelian of rank 12. Hence $H_1F_iS_n$ and $H^1F_iS_n$ are also of dimension 12 only.

3.2. The algebras $H^*(\mathcal{O}_n^\times)$ and H^*S_n are known to be finitely generated $\mathbb{F}_p$-algebras (e.g., because they have a finite-index normal subgroup, say F_1S_n, whose cohomology algebra is even finite); hence Theorem 1.4 and its consequences can be applied to both groups. In order to do this we need to determine the categories $\mathscr{A}_*(G)$, $G=\mathcal{O}_n^\times$ or $G=S_n$. The first step to determine these categories is given by the following well-known theorem. For the convenience of the reader we repeat its short proof.

THEOREM 3.2.1. *The groups $\mathcal{O}_n^\times$ (resp., S_n) have elements of order p if and only if $n \equiv 0 \bmod (p-1)$, in which case both groups have p-rank 1.*

Proof. If A is any finite abelian subgroup of $\mathbb{D}_n^\times$, then A generates a commutative subfield K of $\mathbb{D}_n$, and A is a finite subgroup of its roots of unity. However, for any commutative field the roots of unity form a cyclic subgroup, and hence the p-rank is at most 1. Furthermore, the p-rank of the units $\mathbb{D}_n^\times$ is 1 if and only if $\mathbb{D}_n$ contains the cyclotomic field $\mathbb{Q}_p(\zeta_p)$ of degree $p-1$ over $\mathbb{Q}_p$, which happens if and only if n is a multiple of $p-1$. Finally, any element of finite order in $\mathbb{D}_n^\times$ must have valuation zero; that is, it is contained in $\mathcal{O}_n^\times$. Furthermore, if the order of the element is a power of p, it must be in the p-Sylow subgroup S_n. □

Remark. Lemma 3.1.4(b) implies directly that an element of order p can exist in S_n only if $1/(p-1)$ is of the form k/n, that is, if $n=k(p-1)$. In fact, in this case any nontrivial element x of order p is necessarily contained in $F_{1/(p-1)}S_n$, and $x=1+aS^k$ satisfies $\bar{a}+\bar{a}^{1+p^k+\cdots+p^{(p-1)k}}=0$ with $\bar{a}\neq 0$. One can show that for any $\bar{a}\neq 0$ satisfying $\bar{a}+\bar{a}^{1+p^k+\cdots+p^{(p-1)k}}=0$, one can find $a\in\mathcal{O}_n$ such that $1+aS^k$ is of order p.

The following more precise result gives the complete description of the categories $\mathscr{A}_*(G)$ and of the centralizers of each object.

THEOREM 3.2.2. *Let $n = k(p-1)$.*

(a) *Any two subgroups of $\mathcal{O}_n^\times$ which are isomorphic to $\mathbb{Z}/p$ are conjugate in $\mathcal{O}_n^\times$, and each abstract automorphism of such a subgroup E is induced by conjugation by an element in $\mathcal{O}_n^\times$, that is,* $\mathrm{Aut}_{\mathscr{A}_*(\mathcal{O}_n^\times)}(E) \cong \mathrm{Aut}(E) \cong \mathbb{Z}/(p-1)$. *Furthermore, the centralizer $C_{\mathcal{O}_n^\times}(E)$ is given as the group of units in the maximal order in the central division algebra over $\mathbb{Q}_p(\zeta_p)$ of dimension k^2 and invariant $1/k$.*

(b) *There are exactly $(p^n-1)/(p-1)(p^k-1)$ conjugacy classes of subgroups isomorphic to $\mathbb{Z}/p$ in S_n, and for each such subgroup E the group* $\mathrm{Aut}_{\mathscr{A}_*(S_n)}(E)$ *is trivial. Furthermore, the centralizer $C_{S_n}(E)$ is normal in $C_{\mathcal{O}_n^\times}(E)$ with cyclic quotient of order p^k-1.*

Proof. (a) First note that the group of field automorphisms of $\mathbb{Q}_p(\zeta_p)$ maps via restriction isomorphically to the group of all abstract automorphisms of the multiplicative subgroup of order p generated by ζ_p. Furthermore, by the Skolem-Noether theorem, any two embeddings φ, φ' of $\mathbb{Q}_p(\zeta_p)$ in $\mathbb{D}_n$ are conjugate; that is, there exists $u \in \mathbb{D}_n^\times$ such that $\varphi(x) = u\varphi'(x)u^{-1}$ for each $x \in \mathbb{Q}_p(\zeta_p)$. These two facts imply immediately that the assertion on conjugacy classes and automorphisms in part (a) hold if $\mathcal{O}_n^\times$ is replaced by $\mathbb{D}_n^\times$. To show them for $\mathcal{O}_n^\times$ it suffices therefore to show that in the Skolem-Noether theorem one can take u of valuation zero. To see this, it is enough to note that the valuation on $\mathbb{D}_n$ and its restriction to the centralizer $C_{\mathbb{D}_n}(\varphi(\mathbb{Q}_p(\zeta_p)))$ take the same values. Now $C_{\mathbb{D}_n}(\varphi(\mathbb{Q}_p(\zeta_p)))$ is again a division algebra which is a central division algebra over $\mathbb{Q}_p(\zeta_p)$ of dimension k^2 and of invariant $1/k$ (see [Ha, 20.2.16, 23.1.4]). Then the required property of the value groups follows easily from Theorem 14.3 in [Rn].

If $E \cong \mathbb{Z}/p \subset \mathcal{O}_n^\times$, then E generates a subfield which we can identify with $\mathbb{Q}_p(\zeta_p)$. Furthermore, $C_{\mathcal{O}_n^\times}(E)$ is just the intersection $\mathcal{O}_n^\times \cap C_{\mathbb{D}_n}(E) \cong \mathcal{O}_n^\times \cap C_{\mathbb{D}_n}(\mathbb{Q}_p(\zeta_p))$ which is precisely the group of units in the maximal order of $C_{\mathbb{D}_n}(\mathbb{Q}_p(\zeta_p))$. Thus the proof of (a) is complete.

(b) First we observe that for any $E \cong \mathbb{Z}/p$ in S_n the group $\mathrm{Aut}_{\mathscr{A}_*(S_n)}(E)$ is isomorphic to $N_{S_n}(E)/C_{S_n}(E)$, so it is a subquotient of a profinite p-group, and hence a p-group. However, the abstract isomorphism group is of order $p-1$ (i.e., of order prime to p) so we see that $\mathrm{Aut}_{\mathscr{A}_*(S_n)}(E)$ is trivial.

The remaining parts of (b) are now deduced from (a). We know from (a) that $\mathbb{F}_q^\times$ acts transitively on the set of S_n-conjugacy classes of subgroups $E \cong \mathbb{Z}/p$. So in order to determine the number of S_n-conjugacy classes, it suffices to show that the order of the isotropy group of this action is $(p-1)(p^k-1)$. Now the isotropy subgroup of E is equal to the image of the normalizer $N_{\mathcal{O}_n^\times}(E)$ under the quotient map $\mathcal{O}_n^\times \to \mathbb{F}_q^\times$. The image of the centralizer is of order p^k-1 because $C_{\mathbb{D}_n}(E)$ is of dimension k^2 over $\mathbb{Q}_p(\zeta_p)$, and hence the residue field of the maximal order of $C_{\mathbb{D}_n}(E)$ has order p^k. Again by (a), the quotient $N_{\mathcal{O}_n^\times}(E)/C_{\mathcal{O}_n^\times}(E)$ has order $p-1$. We claim that the image of $C_{\mathcal{O}_n^\times}(E)$ in $\mathbb{F}_q^\times$ continues to have index $p-1$ in the image of $N_{\mathcal{O}_n^\times}(E)$, and therefore the isotropy group has order as claimed.

So assume the image of $C_{\mathcal{O}_n^\times}(E)$ in $\mathbb{F}_q^\times$ has index less than $p-1$ in the image of $N_{\mathcal{O}_n^\times}(E)$. By (a) again there would be a nontrivial automorphism α of E induced by conjugation by an element $y \in N_{\mathcal{O}_n^\times}(E)$, and $y = zx$ with $z \in C_{\mathcal{O}_n^\times}(E)$ and $x \in S_n$. However, then we would even have $x \in S_n \cap N_{\mathcal{O}_n^\times}(E) = N_{S_n}(E) = C_{S_n}(E)$; hence $y \in C_{\mathcal{O}_n^\times}(E)$, and this is in contradiction to the nontriviality of α.

Finally, $C_{S_n}(E)$ is normal in $C_{\mathcal{O}_n^\times}(E)$ with cyclic quotient of order p^{k-1} because $C_{S_n}(E)$ is the kernel of the surjective map from the units in $C_{\mathcal{O}_n}(E)$ to the units in the residue field of $C_{\mathcal{O}_n}(E)$, which is of order p^k. □

Remark. We remark that in the case $p = 2$, Theorem 3.2.2 becomes trivial because there is a unique central element of order 2, namely the element $-1 \in \mathcal{O}_n$. However, in this case Proposition 2.10 implies that H^*S_n is finitely generated and free over a polynomial subalgebra on one generator.

If p is odd, the number of conjugacy classes grows quickly with p and n; for example, if $p = 3$ and $n = 2$ we get two classes, and if $p = 5$ and $n = 4$ we get 39 classes. We will see in the remark after the proof of Proposition 4.3 below that for $p > 3$ and $n = p - 1$ the map ρ of Proposition 2.10 is not mono in dimension 2, and hence H^*S_n cannot be free over a polynomial subalgebra on one generator as it was claimed in [Ra2, 6.2.10(b)].

3.3. We will now consider our main theorem for S_n in the case $n = p - 1$, and we will assume that p is odd, the case $p = 2$ being trivial.

Let E be a cyclic subgroup of order p in S_n. By Theorem 3.2.2 we know that $C_{\mathcal{O}_n^\times}(E)$ is given as the group of units in the maximal order of $\mathbb{Q}_p(\zeta_p)$, which is equal to $\mathbb{Z}_p[\zeta_p]$; in particular, $C_{\mathcal{O}_n^\times}(E)$ is abelian. In fact, the units $\mathbb{Z}_p[\zeta_p]^\times$ are well known to be (noncanonically) isomorphic to $\mathbb{Z}/p \times (\mathbb{Z}_p)^n \times \mathbb{Z}/n$, and hence Theorem 3.2.2 yields $C_{S_n}(E) \cong \mathbb{Z}/p \times (\mathbb{Z}_p)^n$ (see also the remark after Proposition 3.4 below). So the cohomology of $C_{S_n}(E)$ is isomorphic to $H^*(\mathbb{Z}/p) \otimes H^*(\mathbb{Z}_p)^{\otimes n}$ and can be written as $\mathbb{F}_p[y] \otimes E(x) \otimes E(a_1, \ldots, a_n)$, where y has degree 2 and x and the elements a_j have degree 1. The following result (Theorem 1.9 of the introduction) is now an immediate consequence of Corollary 1.7 and of Theorem 3.3.2.

THEOREM 3.3. *Let p be an odd prime and $n = p - 1$. Then S_n has $(p^n - 1)/(p - 1)^2$ conjugacy classes of subgroups which are isomorphic to $\mathbb{Z}/p$ and whose centralizers are all isomorphic to $\mathbb{Z}/p \times (\mathbb{Z}_p)^n$. Choose representatives E_i, $i = 1, \ldots, (p^n - 1)/(p - 1)^2$ from each conjugacy class. Then the map*

$$\rho : H^*S_n \to \prod_i H^*C_{S_n}(E_i) \cong \prod_i \mathbb{F}_p[y_i] \otimes E(x_i) \otimes E(a_{i,1}, \ldots, a_{i,n})$$

induced by the restriction maps has finite kernel and cokernel.

3.4. Now assume again that $n = k(p - 1)$ with k arbitrary. The conjugation action of $\mathcal{O}_n^\times$ on S_n induces an action of $(\mathbb{F}_q)^\times$ on H^*S_n, which is important in applications in homotopy theory. The group $(\mathbb{F}_q)^\times$ acts also on $\prod_{(E)} H^*C_{S_n}(E)$ in such a way that the map ρ is $(\mathbb{F}_q)^\times$-linear. This action can be described as follows. Let E_1 be a fixed cyclic subgroup of S_n of order p. The action of $N_{\mathcal{O}_n^\times}(E_1)$ on $H^*C_{S_n}(E_1)$ induces an action of the image of $N_{\mathcal{O}_n^\times}(E_1)$ in $(\mathbb{F}_q)^\times$. We denote this image by $\bar{N}$. The product $\prod_{(E)} H^*C_{S_n}(E)$ can be identified with the representation of $(\mathbb{F}_q)^\times$ which is induced from that of $\bar{N}$ on $H^*C_{S_n}(E_1)$. With this $\mathbb{F}_q^\times$-action on its target the map ρ is linear.

The following result explicitly describes the action of $\bar{N}$ on $C_{S_n}(E_1)$ in case $n = p-1$, and hence it gives an explicit description of the action of $\mathbb{F}_q^\times$ on $\prod_{(E)} H^*C_{S_n}(E)$ in this case. Note that in the case $n = (p-1)$, we have isomorphisms $\bar{N} \cong \mathbb{Z}/n^2$ and $C_{S_n}(E_1) \cong \mathbb{Z}/p \times (\mathbb{Z}_p)^n$.

Proposition 3.4. *Let $n = p-1$. The action of $\bar{N} \cong \mathbb{Z}/n^2$ on $C_{S_n}(E_1)$ factors through an action of the quotient $\mathbb{Z}/n$. With respect to this $\mathbb{Z}/n$-action $C_{S_n}(E_1) \cong \mathbb{Z}/p \times (\mathbb{Z}_p)^n$ splits as the direct sum of $\mathbb{Z}/p$ (with the natural action of $\mathbb{Z}/n \cong \mathrm{Aut}(\mathbb{Z}/p)$) and the n different 1-dimensional representations of $\mathbb{Z}/n$ over the ring $\mathbb{Z}_p$.*

Proof. The first statement follows because the image $\bar{C}$ of $C_{\mathcal{O}_n^\times}(E_1)$ (which is isomorphic to $\mathbb{Z}/n$) acts clearly trivially, and hence the action factors through $\bar{N}/\bar{C} \cong \mathbb{Z}/n$. This action agrees by the Skolem-Noether theorem with the action of the Galois group of the cyclotomic extension which is well understood in number theory (see [W, p. 301]). □

Remark. By Proposition 3.4 it is clear that for a suitable choice of an isomorphism $\tau : \mathbb{Z}/n \to \mathbb{F}_p^\times$ and of elements y, x, and a_j, the action of $\mathbb{Z}/n$ on $H^*(\mathbb{Z}/p \times (\mathbb{Z}_p)^n) \cong \mathbb{F}_p[y] \otimes E(x) \otimes E(a_1, \ldots, a_n)$ is described by the formula given in Theorem 1.10 of the introduction. In the next section we will have to be even more specific with the choice of these generators, so we take the time now to explain this.

The valuation on $\mathbb{D}_n$ restricts to one on $C_{\mathbb{D}_n}(E)$, and, as in Section 3.1.2, we get a filtration on the group $C_{S_n}(E)$. If we identify $C_{\mathbb{D}_n}(E)$ with $\mathbb{Q}_p(\zeta_p)$, then the maximal ideal in the maximal order of $C_{\mathbb{D}_n}(E)$ is generated by the element $\zeta_p - 1$ of valuation $1/(p-1)$. Using the pth power map on the associated graded mixed Lie algebra of this filtration, one sees that a minimal set of topological generators for $C_{S_n}(E)$ is given by the element ζ_p of order p and any choice of elements η_j, $j = 2, \ldots, n+1$ with the property that $\eta_j \equiv 1 + (\zeta_p - 1)^j \bmod (\zeta_p - 1)^{j+1}$. Furthermore, the filtration is $\mathbb{Z}/n$-invariant, and because n is prime to p, the elements η_j can be chosen to generate the different 1-dimensional representations of $\mathbb{Z}/n$ over $\mathbb{Z}_p$. With such a choice, mod p reduction gives a set of generators $\bar{\zeta}_p, \bar{\eta}_2, \ldots, \bar{\eta}_{n+1}$ of $H_1(\mathbb{Z}_p[\zeta_p]^\times)$. If we take for x, $a_2, \ldots, a_n, a_{n+1} =: a_1$ the dual basis in H^1, and for y the Bockstein of x, then the formula given in Theorem 1.10 holds.

4. The case $p = 3$ and $n = 2$

4.1. In this section we will consider the case $p = 3$ and $n = 2$ in fair detail. This is the first nontrivial case where our main theorem can be applied to get information on H^*S_n. By Theorem 3.3 we find two conjugacy classes of $\mathbb{Z}/3$'s in S_2 whose centralizers are isomorphic to $\mathbb{Z}/3 \times (\mathbb{Z}_3)^2$. We will compute H^*S_2; in particular, we will show that the map ρ of Proposition 2.10 is a monomorphism, and we will describe H^*S_2 as a subalgebra of $\prod_{i=1}^2 \mathbb{F}_3[y_i] \otimes E(x_i) \otimes E(a_{i,1}, a_{i,2})$.

First we recall a product decomposition of the group S_n. The algebra $\mathcal{O}_n$ has $\mathbb{Z}_p$ as its center, and hence $\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1) \times \mathbb{Z}_p$ is central in $\mathcal{O}_n^\times$, that is, $\mathbb{Z}_p$ is central in S_n. Furthermore, the reduced norm, which is a homomorphism from $\mathbb{D}_n^\times$ to $\mathbb{Q}_p^\times$, induces a homomorphism from S_n back to $\mathbb{Z}_p$, which is left inverse to the inclusion of the central $\mathbb{Z}_p$ as long as $n \not\equiv 0 \bmod p$. In other words, the group S_n splits as a product $\mathbb{Z}_p \times S_n^1$ of the central $\mathbb{Z}_p$ with the kernel of the reduced norm. Following Ravenel [Ra2] we will call this kernel S_n^1. Similarly, the centralizers $C_{S_n}(E)$, $E \cong \mathbb{Z}/p$, split as $C_{S_n}(E) \cong C_{S_n^1}(E) \times \mathbb{Z}_p$, and $C_{S_n^1}(E) \cong \mathbb{Z}/3 \times \mathbb{Z}_3$ if $n = p - 1 = 2$. The action of the group $\mathbb{Z}/2$ of Proposition 3.4 respects this splitting. In fact, $\mathbb{Z}/2$ acts trivially on the central $\mathbb{Z}_3$ and by -1 on $C_{S_n^1}(E)$.

We need to specify the elements y_i, x_i, $a_{i,1}$, and $a_{i,2}$. For this we pick a representative E_1 of one of the two conjugacy classes and choose elements y_1, x_1, $a_{1,1}$, and $a_{1,2}$ of $H^*C_{S_2}(E_1)$, as in the remark after Proposition 3.4. If ω generates $\mathbb{F}_9^\times$, then ω^2 generates the group $\bar{N}$ of Proposition 3.4 and acts on $H^*C_{S_2}(E_1)$ by $\omega^2(y_1) = -y_1$, $\omega^2(x_1) = -x_1$, $\omega^2(a_{1,1}) = -a_{1,1}$, and $\omega^2(a_{1,2}) = a_{1,2}$. Furthermore, ρ will be linear with respect to the action of $\mathbb{F}_9^\times$ if we choose the classes y_2, x_2, $a_{2,1}$, and $a_{2,2}$ such that $\omega(y_1) = y_2$, $\omega(x_1) = x_2$, $\omega(a_{1,1}) = a_{2,1}$, and $\omega(a_{1,2}) = a_{2,2}$. In $H^*C_{S_2^1}(E_i)$ the class $a_{i,2}$ is missing, but otherwise the same formula holds. In the discussion below we will change notation and write a_i instead of $a_{i,1}$, and a_i' instead of $a_{i,2}$.

With these preparations we can finally formulate the main result of this section.

THEOREM 4.2. *Let $p = 3$ and $n = 2$.*

(a) *Then the map ρ of Proposition 2.10 is a monomorphism and identifies H^*S_2 with the subalgebra of $\prod_{i=1}^2 \mathbb{F}_3[y_i] \otimes E(x_i) \otimes E(a_i, a_i')$ generated by the classes $x_1, x_2, y_1, y_2, a_1' + a_2', x_1a_1 - x_2a_2, y_1a_1$, and y_2a_2.*

(b) *In particular, H^*S_2 is a finitely generated free module over $\mathbb{F}_3[y_1 + y_2] \otimes E(a_1' + a_2')$ with eight generators which we can choose as follows: $1, x_1, x_2, y_1, x_1a_1 - x_2a_2, y_1a_1, y_2a_2$, and $y_1x_1a_1$.*

Before we begin with the proof, we compare this calculation with the one of Ravenel in [Ra1, Thm 3.3]. After extension of scalars to $\mathbb{F}_9$, the two results have to agree. However, they do not. For example, according to Ravenel, H^*S_2 would be multiplicatively generated by classes in degree 1 and 2, while in our computation the classes y_1a_1 and y_2a_2 are indecomposable classes of degree 3. Furthermore, it is easy to see that if one extends scalars to $\mathbb{F}_9$ in Ravenel's calculation, then the resulting algebra cannot be embedded into $\prod_{i=1}^2 \mathbb{F}_9[y_i] \otimes E(x_i) \otimes E(a_i, a_i')$.

The two computations both give the same Poincaré series, however. Furthermore, both computations give free modules over a polynomial generator of degree 2, which means that Ravenel's computation is not compatible with Proposition 2.10.

Because of the decomposition $S_n \cong \mathbb{Z}_p \times S_n^1$ it suffices to prove the following analogous result for the group S_n^1.

PROPOSITION 4.3. *Assume that $p = 3$ and $n = 2$.*

(a) *The map ρ of Proposition 2.10 is a monomorphism and identifies $H^*S_2^1$ with the subalgebra of $\prod_{i=1}^2 \mathbb{F}_3[y_i] \otimes E(x_i) \otimes E(a_i)$ generated by the classes x_1, x_2, y_1, y_2, $x_1a_1 - x_2a_2$, y_1a_1, and y_2a_2.*

(b) *In particular, $H^*S_2^1$ is a finitely generated free module over $\mathbb{F}_3[y_1 + y_2]$ with eight generators which we can choose as follows: 1, x_1, x_2, y_1, $x_1a_1 - x_2a_2$, y_1a_1, y_2a_2, and $y_1x_1a_1$.*

The crucial step in the proof of Proposition 4.3 is given by the following proposition.

PROPOSITION 4.4. *Assume that $p = 3$ and $n = 2$. There is a homomorphism $S_2^1 \to \mathbb{Z}/3$ whose kernel K is torsion free and such that S_2^1 is isomorphic to the semidirect product $K \rtimes \mathbb{Z}/3$. Furthermore, H^*K is a Poincaré duality algebra of dimension 3, and as a $\mathbb{Z}/3$ module, $H^1K \cong (\mathbb{F}_3)^2$ is isomorphic to the augmentation ideal $I(\mathbb{Z}/3)$ in the group algebra $\mathbb{F}_3[\mathbb{Z}/3]$.*

Proof of Proposition 4.4. We will make use of the filtration on S_n^1 which is induced from the filtration on S_n that we discussed in Section 3.1. The central $\mathbb{Z}_p$ in S_n is topologically generated by $1 + p \in F_1S_n$. Furthermore, an inspection of the formula for the reduced norm (cf. [M]) shows that it sends F_iS_n onto $p^{[i]}\mathbb{Z}_p$, where $[i]$ denotes the smallest integer which is bigger than or equal to i, and that it induces the trace map $\mathrm{Tr} : \mathrm{gr}_iS_n \cong \mathbb{F}_q \to \mathbb{F}_p \cong p^{[i]}\mathbb{Z}_p/p^{[i]+1}\mathbb{Z}_p$ if i is an integer. In particular, we obtain

$$\mathrm{gr}_iS_n^1 \cong \begin{cases} \mathbb{F}_q & \text{if } i \notin \mathbb{N}, \\ \mathrm{Ker}\,\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p & \text{if } i \in \mathbb{N}. \end{cases}$$

Furthermore, the Lie bracket as well as the map P are given on $\mathrm{gr}\,S_n^1$ by the formula of Lemma 3.1.4.

So far, p and n were general. Now assume that $p = 3$ and $n = 2$. As we have noted in the remark after the proof of Theorem 3.2.1, all nontrivial elements of order 3 in S_2 have the form $1 + aS$, with $\bar{a} \neq 0$ and $\bar{a} + \bar{a}^{1+3+9} = 0$, that is, $\bar{a}^4 = -1$. (Recall that $\bar{a} \in \mathbb{F}_9$ denotes the residue class of $a \in \mathcal{O}_2$.) In particular, there is no $\bar{a} \in \mathbb{F}_3$ with this property. Therefore, if we identify $\mathbb{F}_9$ with $(\mathbb{Z}/3)^2$, and if we divide out by $\mathbb{F}_3$, we get a homomorphism $S_2^1 \to \mathrm{gr}_{1/2}S_2^1 \to \mathbb{Z}/3$ whose kernel K is torsion free. Furthermore, as S_2^1 contains elements of order 3, the group S_2^1 is isomorphic to the semidirect product $K \rtimes \mathbb{Z}/3$.

The group S_2 is an analytic pro 3-group of dimension 4, and hence S_2^1 and K are analytic pro 3-groups of dimension 3; so by [La, V.2.5.8] H^*K is a Poincaré duality algebra of dimension 3. To finish, it suffices to show that $H_1K \cong (\mathbb{Z}/3)^2$

and that there are elements z_1 and z_2 in K which project to a basis $\bar{z}_1$ and $\bar{z}_2$ of H_1K, and such that, if $x \in S_2^1$ is a suitable nontrivial element of order 3, then $xz_1x^{-1} = z_1z_2 \bmod \Phi(K)$ and $xz_2x^{-1} = z_2 \bmod \Phi(K)$, where Φ denotes the Frattini subgroup.

Now it follows from Lemma 3.1.4 (by using [La, III.2.1.8]) that all elements in $F_2S_2 \cap K$ are third powers, and hence $H_1K \cong H_1\tilde{K}$, where $\tilde{K}$ denotes the group $K/F_2S_2 \cap K$. The filtration of S_2 induces one on $\tilde{K}$, and we obtain

$$\mathrm{gr}_i\tilde{K} \cong \begin{cases} \mathbb{F}_3 & \text{if } i = 1/2, \\ \mathrm{Ker}\,\mathrm{Tr} : \mathbb{F}_9 \to \mathbb{F}_3 & \text{if } i = 1, \\ \mathbb{F}_9 & \text{if } i = 3/2, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, the Lie bracket $\mathrm{gr}_{1/2}\tilde{K} \times \mathrm{gr}_1\tilde{K} \to \mathrm{gr}_{3/2}\tilde{K}$ and the map P : $\mathrm{gr}_{1/2}\tilde{K} \to \mathrm{gr}_{3/2}\tilde{K}$ are given by $[\bar{a}, \bar{b}] = \bar{a}\bar{b}^3 - \bar{b}\bar{a}$ and $P\bar{a} = \bar{a} + \bar{a}^{1+3+9}$. With this it is easy to check that $\mathrm{gr}_{3/2}\tilde{K}$ is generated by commutators and third powers and $H_1K \cong \tilde{K}/\mathrm{gr}_{3/2}\tilde{K} \cong (\mathbb{Z}/3)^2$.

The action of an element $x \in \mathbb{Z}/3$ on H_1K can now be read off from the commutator formula in Lemma 3.1.4. Let $z_1 \in K$ and $z_2 \in K$ be elements in the appropriate filtration which project nontrivially to $\mathrm{gr}_{1/2}K$ (resp., gr_1K). The element x is represented by an element $\bar{x} \in \mathrm{gr}_{1/2}S_2$ with $\bar{x}^4 = -1$. Then $xz_2x^{-1}z_2^{-1} \in K \cap F_{3/2}S_2$, and hence gives zero in H_1K. Furthermore $[\bar{x}, \bar{z}_1] = \bar{x}\bar{z}_1^3 - \bar{z}_1\bar{x}^3$. This is nontrivial and can be made equal to $\bar{z}_2$ if x is chosen appropriately. In other words, $xz_1x^{-1} = z_1z_2 \bmod \Phi(K)$, and we are done. □

Proof of Proposition 4.3. We consider the spectral sequence of the group extension $1 \to K \to S_2^1 \to \mathbb{Z}/3 \to 1$ with E_2-term $E_2^{*,q} \cong H^*(\mathbb{Z}/3; H^qK)$. This is a spectral sequence of modules over $H^*\mathbb{Z}/3$, and the lines $q = 0$ and $q = 3$ are free $H^*\mathbb{Z}/3$-modules on one generator on the vertical edge. Furthermore, $H^2K \cong H^1K$ as $\mathbb{Z}/3$-module by Poincaré duality. The exact sequence $0 \to I(\mathbb{Z}/3) \to \mathbb{F}_3[\mathbb{Z}/3] \to \mathbb{F}_3 \to 0$ shows that for $0 \leqslant q \leqslant 3$ the graded vector space $H^*(\mathbb{Z}/3; H^qK)$ is additively independent of q, and, in fact, this is true even as modules over the polynomial subalgebra of $H^*\mathbb{Z}/3$ generated by the periodicity generator in degree 2. Therefore, the spectral sequence collapses because by Theorem 1.9 we have $H^*S_2^1 \cong \prod_{i=1}^{2} \mathbb{F}_3[y_i] \otimes E(x_i) \otimes E(a_i)$ in large degrees, and a nontrivial differential would give too small a result.

In particular, we see that $H^*S_2^1$ is a free module of rank 8 over the polynomial subalgebra of $H^*\mathbb{Z}/3$ generated in degree 2. The module generators have degree $0, 1, 1, 2, 2, 3, 3, 4$. By Proposition 2.10 we conclude that ρ is a monomorphism, and we compute the Poincaré series of the cokernel of ρ to be $1 + 2t + t^2$. It remains to identify the image of ρ.

Let us first consider H^1; it is 2-dimensional and can be identified with the dual of $\mathrm{gr}_{1/2}S_2^1$. For each $\mathbb{Z}/3 \subset S_2$ the basis element $\bar{\eta}_3$ in $H_1C_{S_2}(\mathbb{Z}/3)$ (which was defined in the remark after Proposition 3.4) maps trivially to $\mathrm{gr}_{1/2}S_2$. Therefore, the image of ρ in dimension 1 is contained in the linear span of the elements x_i and by a dimension argument is equal to this span.

The Bocksteins of x_1 and x_2 give the elements y_1 and y_2. However, $H^2S_2^1$ has dimension 3, so we need one more element. To identify it we consider the action of $\mathbb{F}_9^\times$ on H^*S_2 and $\prod_{i=1}^2 \mathbb{F}_3[y_i] \otimes E(x_i) \otimes E(a_i)$ (as described in Section 4.1) and use the linearity of ρ. The subspace generated by y_1 and y_2 is invariant under this action and because the order of $\mathbb{F}_9^\times$ is prime to the characteristic we can assume that this last element is an eigenvector for the action of the generator $\omega \in \mathbb{F}_9^\times$. Now there are only two eigenspaces of ω, with eigenvalue 1 (resp., -1) and eigenvectors $x_1a_1 + x_2a_2$ (resp., $x_1a_1 - x_2a_2$). By Lemma 4.5 below it is an eigenvector with eigenvalue -1.

Finally, ρ is onto in degrees 3, so we have determined the image of ρ and the missing parts of the proposition follow easily. □

Remark. We have remarked after Theorem 3.2.2 that the map ρ is not a monomorphism if $n = p - 1$ and $p > 3$. In fact, in this case we have again a decomposition $S_n \cong \mathbb{Z}_p \times S_n^1$, and $H^1S_n^1 \cong \mathrm{gr}_{1/n}S_n^1 \cong (\mathbb{Z}/p)^n$. As above, one sees that for any $E \cong \mathbb{Z}/p \subset S_n^1$ the image of the restriction map $H^1S_n^1 \to H^1C_{S_n^1}(E) \cong \mathbb{F}_p[y] \otimes E(x) \otimes E(a_1, \ldots a_{p-1})$ is spanned by the class x. In particular, the product of any two 1-dimensional classes restricts trivially to all centralizers. According to [Ra2, Thm 6.3.14] there are nontrivial products of 1-dimensional classes as soon as $p > 3$, and hence ρ is not injective in degree 2.

LEMMA 4.5. *Let $p = 3$ and $n = 2$. The action of $\mathbb{F}_9^\times$ on $H^2S_2^1 \cong (\mathbb{Z}/3)^3$ decomposes into a direct sum of the subspace generated by y_1 and y_2 with $\omega y_1 = y_2$, $\omega y_2 = -y_1$, and a 1-dimensional subspace on which ω acts by multiplication with -1.*

Proof. The element $\omega \in \mathbb{F}_9^\times$ can be lifted to a primitive 8th root of unity in $\mathbb{W}_2 \subset \mathcal{O}_2$ which we will still call ω. The group extension that we used in Proposition 4.4 to investigate $H^*S_2^1$ is not invariant under the conjugation action $x \mapsto \omega x \omega^{-1}$, and hence is not suited for the problem that we are considering here. Therefore, we consider the subgroup $F_1S_2^1 := S_2^1 \cap F_1S_2$ which is invariant under the action of ω and normal in S_2^1 with quotient $\mathrm{gr}_{1/2}S_2^1 \cong \mathbb{F}_9 \cong (\mathbb{Z}/3)^2$. It follows easily from [La, V.2.2.7] that $H^*F_1S_2^1$ is an exterior algebra on three classes in degree 1. We will prove the lemma by inspecting the spectral sequence

$$E_2^{p,q} \cong H^p((\mathbb{Z}/3)^2, H^qF_1S_2^1) \Rightarrow H^{p+q}S_2^1,$$

and for this we need to understand the action of $(\mathbb{Z}/3)^2$ on $H^*F_1S_2^1$ and the action of $\mathbb{F}_9^\times$ on $(\mathbb{Z}/3)^2$ and on $H^*F_1S_2^1$

The element ω^2 is a primitive 4th root of unity for which we will write i. Together with the unit element, it forms a basis of $\mathbb{F}_9$ as an $\mathbb{F}_3$ vector space. Therefore, the elements $a = 1 + S$ and $b = 1 + iS$ project to a basis $\{\bar{a}, \bar{b}\}$ of $\mathrm{gr}_{1/2}S_n^1$, while the elements $c = 1 + iS^2 = 1 + 3i$, $d = 1 + S^3$, and $e = 1 + iS^3$ project to a basis $\{\bar{c}, \bar{d}, \bar{e}\}$ in $H_1F_1S_2^1$. Furthermore, the relation $S\omega = \omega^3 S$ in $\mathcal{O}_2$ implies that the conjugation action of ω on $\mathrm{gr}_{1/2}S_2^1$ (resp., on $H_1F_1S_2^1$) is given by the following formulas:

$$\omega_*\bar{a} = -\bar{b}, \quad \omega_*\bar{b} = \bar{a}$$

$$\omega_*\bar{c} = \bar{c}, \quad \omega_*\bar{d} = -\bar{e}, \quad \omega_*\bar{e} = \bar{d}.$$

The action of $\bar{a}$ and $\bar{b}$ on $H_1F_1S_2^1$ can be read from the commutator formula of Lemma 3.1.4, and we obtain

$$\bar{a}_*(\bar{d}) = \bar{d}, \quad \bar{a}_*(\bar{e}) = \bar{e}, \quad \bar{a}_*(\bar{c}) = \bar{c} + \bar{e}$$

$$\bar{b}_*(\bar{d}) = \bar{d}, \quad \bar{b}_*(\bar{e}) = \bar{e}, \quad \bar{b}_*(\bar{c}) = \bar{c} - \bar{d}.$$

With this information at hand we can look at the spectral sequence. The important groups for us are $E_2^{1,1}$ and $E_2^{3,0}$ as modules over $\mathbb{F}_9^\times$. A straightforward computation gives $E_2^{1,1} \cong (\mathbb{Z}/3)^3$ and $E_2^{3,0} \cong (\mathbb{Z}/3)^4$. Furthermore, with respect to the ω-action, $E_2^{1,1}$ decomposes as a sum of a 2-dimensional eigenspace with eigenvalue -1 and a 1-dimensional eigenspace with eigenvalue 1, while $E_2^{3,0}$ decomposes into a direct sum of two 2-dimensional eigenspaces with respective eigenvalues 1 and -1.

From the proof of Proposition 4.3, we know already that the classes x_1 and x_2 are represented on $E_2^{1,0}$ and consequently the classes y_1 and y_2 are represented on $E_2^{2,0}$. Because we know already that $H^2S_n^1$ is of dimension 3, it follows that the kernel of the differential $d_2 : E_2^{1,1} \to E_2^{3,0}$ is at most 1-dimensional, and because we also know that the classes x_1y_1 and x_2y_2 in $E_2^{3,0}$ survive to E_∞, the kernel is precisely 1-dimensional and gives the missing class in $H^2S_2^1$. We have to show that this kernel is contained in the -1 eigenspace of ω.

In fact, $E_3^{3,0}$, the quotient of $E_2^{3,0}$ by the image of d_2, is generated by x_1y_1 and x_2y_2 and is a direct sum of two 1-dimensional eigenspaces with eigenvalues 1 (resp., -1). The decomposition of $E_2^{3,0}$ implies that the image of d_2 is also a direct sum of two 1-dimensional eigenspaces with eigenvalues 1 (resp., -1), and hence the decomposition of $E_2^{1,1}$ gives that ω acts by multiplication by -1 on the kernel of d_2. □

5. The case $GL(n, \mathbb{Z}_p)$

5.1. We start with a few general remarks on the continuous cohomology of the groups $GL(n, \mathbb{Z}_p)$. Mod p^r-reduction defines maps from $GL(n, \mathbb{Z}_p)$ to $GL(n, \mathbb{Z}/p^r)$ with kernel $\Gamma(p^r)$. The groups $\Gamma(p^r)$ form a decreasing sequence of closed subgroups with $GL(n, \mathbb{Z}_p) \cong \lim GL(n, \mathbb{Z}_p)/\Gamma(p^r)$. Furthermore, the quotients $\Gamma(p^r)/\Gamma(p^{r+1})$ are elementary abelian p-groups (of rank n^2), and hence $\Gamma(p) \cong \lim \Gamma(p)/\Gamma(p^r)$ is a profinite p-group.

In particular, for a prime $l \neq p$, mod-p reduction induces an isomorphism in continuous cohomology $H^*(GL(n,\mathbb{Z}/p);\mathbb{F}_l) \to H^*(GL(n,\mathbb{Z}_p);\mathbb{F}_l)$, and hence $H^*(GL(n,\mathbb{Z}_p);\mathbb{F}_l)$ is known by the work of Quillen [Q2]. However, if $p = l$, then very little seems to be known about $H^*(GL(n,\mathbb{Z}_p);\mathbb{F}_p) = H^*GL(n,\mathbb{Z}_p)$ (from now on we will omit the coefficients again in our notation). For example, studying mod-p reduction does not lead very far, because the mod-p cohomology of the quotient $GL(n,\mathbb{F}_p)$ is not known unless n is very small.

We will use our centralizer approach to compute $H^*GL(n,\mathbb{Z}_p)$ in large dimensions in case $n = p-1$, p odd. The following result gives the necessary group theoretic information to apply Theorem 1.4 (resp., Corollary 1.7).

THEOREM 5.2. *Let p be odd and $n = p-1$.*

(a) *The p-rank of $GL(n,\mathbb{Z}_p)$ is equal to 1, and, up to conjugacy, there is a unique subgroup E of $GL(n,\mathbb{Z}_p)$ that is isomorphic to $\mathbb{Z}/p$.*

(b) *The centralizer $C_{GL(n,\mathbb{Z}_p)}(E)$ is isomorphic to $\mathbb{Z}_p[\zeta_p]^\times \cong \mathbb{Z}/p \times (\mathbb{Z}_p)^n \times \mathbb{Z}/(p-1)$.*

(c) $\mathrm{Aut}_{\mathscr{A}_*(GL(n,\mathbb{Z}_p))}(E) \cong \mathbb{Z}/n$ *and the action of $\mathbb{Z}/n$ on $C_{GL(n,\mathbb{Z}_p)}(E)$ correspond via the isomorphism of (b) to the Galois action on $\mathbb{Z}_p[\zeta_p]^\times$, which was explicitly described in Section 3.4.*

The crucial input for Theorem 5.2 is the following p-adic version of the theorem of Diederichsen and Reiner [CR, Thm (74.3)]. It can be proved in the same way as the integral version except that some of the details simplify because class group phenomena disappear in the p-adic version.

THEOREM 5.3. *Let $G = \mathbb{Z}/p$ and M be a $\mathbb{Z}_p[G]$-module which is finitely generated and free as a $\mathbb{Z}_p$-module. Let $F = \mathbb{Z}_p[G]$ be the free $\mathbb{Z}_p[G]$-module on one generator, $T \cong \mathbb{Z}_p$ the trivial 1-dimensional module, and $R = \mathbb{Z}_p[\zeta_p]$ the ring of integers in the cyclotomic extension $\mathbb{Q}_p(\zeta_p)$ with action of a generator $g \in G$ given by $gr = \zeta_p r$ for $r \in R$.*

Then

$$M \cong F^k \oplus T^l \oplus R^m$$

for a unique triple (k,l,m) of nonnegative numbers. □

Proof of Theorem 5.2. (a) The $\mathbb{Z}_p[G]$-module R is isomorphic to $(\mathbb{Z}_p)^n$ as a $\mathbb{Z}_p$-module, which shows that there is an embedding of G into $GL(n,\mathbb{Z}_p)$. By Theorem 5.2 there is a unique $\mathbb{Z}_p[G]$-module structure on $(\mathbb{Z}_p)^n$ for which the action is faithful, which means that all subgroups E of order p in $GL(n,\mathbb{Z}_p)$ are conjugate. That the p-rank is not bigger than 1 will follow from part (b) because the p-rank of the centralizer of E is only 1.

(b) We have isomorphisms $C_{GL(n,\mathbb{Z}_p)}(E) \cong \mathrm{Aut}_{\mathbb{Z}_p[E]}(R)$ and because the $\mathbb{Z}_p[E]$-module structure on the ring R is pulled back from the R-module structure, we also get $\mathrm{Aut}_{\mathbb{Z}_p[E]}(R) \cong \mathrm{Aut}_R(R) \cong R^\times$.

(c) The group $\mathrm{Aut}_{\mathscr{A}_*(GL(n,\mathbb{Z}_p))}(E)$ is a subgroup of the group of all abstract automorphisms of E and the Galois group of the cyclotomic extension realizes all of them through conjugations in $GL(n,\mathbb{Z}_p)$. □

Using the notation of Theorem 3.3 and Proposition 3.4, we write $H^*C_{GL(n,\mathbb{Z}_p)}(E) \cong \mathbb{F}_p[y] \otimes E(x) \otimes E(a_1,\dots,a_n)$. The action of the Galois group is determined by Proposition 3.4. Combining Theorem 5.2 with Corollary 1.7 leads to the following result (see Theorem 1.10 of the introduction).

THEOREM 5.4. *Let p be an odd prime, $n = p-1$, and $E \cong \mathbb{Z}/p \subset GL(n,\mathbb{Z}_p)$. Then the restriction map*

$$\rho : H^*GL(n,\mathbb{Z}_p) \to (H^*C_{GL(n,\mathbb{Z}_p)}(E))^{\mathbb{Z}/n} \cong (\mathbb{F}_p[y] \otimes E(x) \otimes E(a_1,\dots,a_n))^{\mathbb{Z}/n}$$

has finite kernel and cokernel. □

As in [A], one can analyze all p-rank 1 cases $p-1 \leqslant n \leqslant 2p-3$ further and reduce the computation of $H^*GL(n,\mathbb{Z}_p)$ in large dimensions to the computation of the cohomology of $GL(n-p+1,\mathbb{Z}_p)$ and of appropriate congruence subgroups thereof. We leave the details to the interested reader.

5.5. We finish with a brief discussion of the case $p=3$ and $n=2$. This case is simple enough that one could do it directly with standard methods. However, we include it here as another example illustrating our theory and how the map ρ of Corollary 1.7 may fail to be an isomorphism in small dimensions.

The situation is very similar to that of the group S_2 for the prime 3 that we discussed in Section 4. Using the same notation as in Section 4.1, we write $H^*C_{GL(2,\mathbb{Z}_3)}(\mathbb{Z}/3) \cong \mathbb{F}_3[y] \otimes E(x) \otimes E(a,a')$, where y is of degree 2, all the other classes are of degree 1, and the action of the nontrivial element g in the Galois group is trivial on a' and multiplies all other generators by -1. In particular, the ring of invariants $(\mathbb{F}_3[y] \otimes E(x) \otimes E(a,a'))^{\mathbb{Z}/2}$ is equal to the subring generated by the elements y^2, yx, ya, xa, and a'. This is a free module of rank 4 over $\mathbb{F}_3[y^2] \otimes E(a')$ on generators $1, yx, ya$, and xa.

PROPOSITION 5.5. *The restriction map*

$$\rho : H^*GL(2,\mathbb{Z}_3) \to (H^*C_{GL(2,\mathbb{Z}_3)}(\mathbb{Z}/3))^{\mathbb{Z}/2} \cong (\mathbb{F}_3[y] \otimes E(x) \otimes E(a,a'))^{\mathbb{Z}/2}$$

is a monomorphism and identifies $H^*GL(2,\mathbb{Z}_3)$ with the subalgebra $\mathbb{F}_3[y^2] \otimes E(yx,ya) \otimes E(a')$ of the invariants.

Proof. First we note that, if $n \not\equiv 0$ mod-p $GL(n,\mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p \times GL^1(n,\mathbb{Z}_p)$, where $GL^1(n,\mathbb{Z}_p)$ denotes the subgroup of $GL(n,\mathbb{Z}_p)$, which is the preimage of $\mathbb{Z}/p-1 \subset \mathbb{Z}_p^\times$ under the determinant map. In fact, $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \mathbb{Z}/p-1$ identifies with the center of $GL(n,\mathbb{Z}_p)$, and the composition with the determinant is multiplication by n, and hence is an isomorphism on the $\mathbb{Z}_p$ summand of $\mathbb{Z}_p^\times$ if $n \not\equiv 0 \bmod p$. Furthermore, $H^*GL^1(n,\mathbb{Z}_p) \cong (H^*SL(n,\mathbb{Z}_p))^{\mathbb{Z}/p-1}$, and hence Proposition 5.5 will follow from the following result for the special linear group. □

First note that if one works with $SL(2,\mathbb{Z}_3)$ instead of $GL(2,\mathbb{Z}_3)$, then one still has a unique subgroup $\mathbb{Z}/3$ up to conjugacy with centralizer $C_{SL(2,\mathbb{Z}_3)} \cong \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}_3$ and $H^*C_{SL(2,\mathbb{Z}_3)}(E) \cong \mathbb{F}_3[y] \otimes E(x) \otimes E(a)$. Furthermore, in this case $\mathrm{Aut}_{\mathscr{A}_*(SL(2,\mathbb{Z}_3))}(\mathbb{Z}/3)$ is the trivial group, so that in large degrees $H^*SL(2,\mathbb{Z}_3) \cong \mathbb{F}_3[y] \otimes E(x) \otimes E(a)$ by Corollary 1.7.

Proposition 5.6. *The restriction map*

$$\rho : H^*SL(2,\mathbb{Z}_3) \to H^*C_{SL(2,\mathbb{Z}_3)}(\mathbb{Z}/3) \cong \mathbb{F}_3[y] \otimes E(x,a)$$

is a monomorphism and identifies $H^*SL(2,\mathbb{Z}_3)$ *with* $\mathbb{F}_3[y] \otimes E(x,ya)$.

Proof. We consider the mod-3 reduction map $SL(2,\mathbb{Z}_3) \to SL(2,\mathbb{F}_3)$. The kernel K is a torsion-free 3-dimensional analytic pro 3-group, and hence H^*K is a 3-dimensional Poincaré duality algebra by [La,V.2.5.8]. Now consider the graded Lie algebra associated to the decreasing filtration of $SL(2,\mathbb{Z}_3)$ by the kernels of mod-3^k reduction, $k = 1,2,\ldots$. It is easy to see from this Lie algebra, say, as in the proof of Proposition 4.4, that $H_1K \cong (\mathbb{F}_3)^3$. Furthermore, using [La,V.2.2.7], we see that H^*K is exterior on the three generators in degree 1.

Now we consider the spectral sequence of the extension

$$1 \to K \to SL(2,\mathbb{Z}_3) \to SL(2,\mathbb{F}_3) \to 1$$

with $E_2^{*,q} \cong H^*(SL(2,\mathbb{F}_3); H^qK)$. The group $SL(2,\mathbb{F}_3)$ acts necessarily trivial on H^3K because there are no nontrivial homomomorphisms from $SL(2,\mathbb{F}_3)$ to $GL(1,\mathbb{F}_3)$. Next, one can check that the invariants of H^1K, with respect to the action of the 2-Sylow subgroup Q_8 of $SL_2(\mathbb{F}_3)$, are trivial. Because Q_8 is normal in $SL(2,\mathbb{F}_3)$, this implies that $H^*(SL(2,\mathbb{F}_3); H^1K) = 0$, and by Poincaré duality we also have $H^*(SL(2,\mathbb{F}_3); H^2K) = 0$. Finally, the restriction map to the 3-Sylow subgroup is well known to induce an isomorphism $H^*SL(2,\mathbb{F}_3) \cong H^*\mathbb{Z}/3$, and so our spectral sequences have just two nontrivial rows at E_2 which are both isomorphic to $H^*\mathbb{Z}/3$. As in the proof of Proposition 4.3, we see now that the spectral sequence has to collapse; a nontrivial differential would lead to a result that is too small to be compatible with Corollary 1.7. Then the spectral sequence shows that $H^*SL(2,\mathbb{Z}_3)$ is free over $\mathbb{F}_3[y]$, and hence ρ is injective. It is clear that the elements x and y are in the image of ρ, and by counting dimensions one sees that ρ is an isomorphism in degrees of 3 and larger; in particular, the image of ρ is $\mathbb{F}_3[y] \otimes E(x,ya)$. □

References

[A] A. Ash, *Farrell Cohomology of GL(n, Z)*, Israel J. Math. **67** (1989), 327–336.

[BH] C. Broto and H.-W. Henn, *Some remarks on central elementary abelian p-subgroups and cohomology of classifying spaces*, Quart. J. Math. Oxford Ser. (2) **44** (1993), 155–163.

[B] K. Brown, *Cohomology of groups*, Grad. Texts in Math. **87**, Springer-Verlag, Berlin, 1982.

[CH] J. Carlson and H.-W. Henn, *Cohomological detection and regular elements in group cohomology*, Proc. Amer. Math. Soc. **124** (1996), 665–670.

[CR] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley and Sons, New York, 1966.

[D] E. Devinatz, "Morava's change of rings theorem" in *The Čech Centenntal (Boston, 1993)*, Contemp. Math. **181** (1995), 83–118.

[DW] W. Dwyer and C. Wilkerson, *A cohomology decomposition theorem*, Topology **31** (1992), 433–443.

[GSS] V. Gorbounov, S. Siegel, and P. Symonds, *The cohomology of the Morava stabilizer group S_2 at the prime 3*, to appear in Proc. Amer. Math. Soc.

[Ha] M. Hazewinkel, *Formal Groups and Applications*, Pure Appl. Math. **78**, Academic Press, New York, 1978.

[He] H.-W. Henn, *Commutative algebra of unstable K-modules, Lannes' T-functor, and equivariant mod-p cohomology*, J. Reine Angew. Math. **478** (1996), 189–215.

[HLS] H.-W. Henn, J. Lannes, and L. Schwartz, *Localizations of unstable A-modules and equivariant mod p cohomology*, Math. Ann. **301** (1995), 23–68.

[HM] H.-W. Henn and M. Mahowald, *The homotopy groups of the L_2-localization of $V(1)$ at the prime 3*, in preparation.

[HG] M. J. Hopkins and B. H. Gross, *The rigid analytic period mapping, Lubin-Tate space, and stable homotopy theory*, Bull. Amer. Math. Soc. **30** (1994), 76–86.

[JM] S. Jackowski and J. McClure, *Homotopy decomposition of classifying spaces via elementary abelian subgroups*, Topology **31** (1992), 113–132.

[L1] J. Lannes, *Sur les espaces fonctionnels dont la source est le classifiant d'un p-groupe abélien élémentaire*, Inst. Hautes Études Sci. Publ. Math. **75** (1992), 135–244.

[L2] ———, *Cohomology of groups and function spaces*, preprint, 1986.

[La] M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603.

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

[Q1] D. Quillen, *The spectrum of an equivariant cohomology ring I*, Ann. of Math. (2) **94** (1971), 549–572; *II*, 573–602.

[Q2] ———, *On the cohomology and K-theory of the general linear groups over finite fields*, Ann. of Math. (2) **96** (1972), 552–586.

[Ra1] D. Ravenel, *The cohomology of the Morava stabilizer algebras*, Math. Z. **152** (1977), 287–297.

[Ra2] ———, *Complex Cobordism and Stable Homotopy Groups of Spheres*, Pure Appl. Math. **121**, Academic Press, Orlando, 1986.

[Ra3] ———, *Nilpotence and Periodicity in Stable Homotopy Theory*, Ann. of Math. Stud. **128**, Princeton Univ. Press, Princeton, 1992.

[Rc] D. Rector, *Noetherian cohomology rings and finite loop spaces with torsion*, J. Pure Appl. Algebra **32** (1984), 191–217.

[Rn] I. Reiner, *Maximal Orders*, London Math. Soc. Monographs (N.S.) **5**, Academic Press, London, 1975.

[S] K. Shimomura, *The homotopy groups of the L_2-localized Toda-Smith spectrum $V(1)$ at the prime 3*, Trans. Amer. Math. Soc. **349** (1997), 1821–1850.

[SY] K. Shimomura and A. Yabe, *The homotopy groups $\pi_*(L_2S^0)$*, Topology **34** (1995), 261–289.

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. **83**, Springer-Verlag, New York, 1982.

Mathematisches Institut der Universität, Im Neuenheimer Feld 288, D-69120 Heidelberg, Germany

Current: Max Planck Institut für Mathematik, Gottfried Claren Straße 26, D-53225 Bonn, Germany