

Finite generation properties of the pro- p Iwahori–Hecke Ext-algebra

Emanuele Bodon

May 3, 2024

Abstract

The pro- p Iwahori–Hecke Ext-algebra E^* is a graded algebra that has been introduced and studied by Ollivier–Schneider, with the long-term goal of investigating the category of smooth mod- p representations of p -adic reductive groups and its derived category. Its 0^{th} graded piece is the pro- p Iwahori–Hecke algebra studied by Vignéras and others.

In the present article, we first show that the Ext-algebra E^* associated with the group $\mathrm{SL}_2(\mathfrak{F})$, $\mathrm{PGL}_2(\mathfrak{F})$ or $\mathrm{GL}_2(\mathfrak{F})$, where $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ with $p \neq 2, 3$, is finitely generated as a (non-commutative) algebra.

We then specialize to the case of the group $\mathrm{SL}_2(\mathbb{Q}_p)$, with $p \neq 2, 3$, and we show that in this case the natural multiplication map from the tensor algebra $T_{E^0}^* E^1$ to E^* is surjective and that its kernel is finitely generated as a two-sided ideal. Using this fact as main input, we then show that E^* is finitely presented as an algebra. We actually compute an explicit presentation.

Contents

1	Introduction	2
1.1	Context	2
1.2	Main results	4
1.3	Acknowledgements	5
2	Setting and background	6
2.1	Notation and assumptions	6
2.2	The apartment	7
2.3	Affine roots and the length function	8
2.4	The pro- p Iwahori–Weyl group $\tilde{W}$ and the subgroups I_w	10
2.5	The Iwahori decomposition	10
2.6	The pro- p Iwahori–Hecke algebra	11
2.7	The Ext-algebra E^*	11
2.8	A few results on cohomology of pro- p groups	13

3	The first graded piece E^1 is finitely generated as an E^0-bimodule	14
4	The subalgebra generated by E^0 and E^1 in some special cases	22
5	The Ext-algebra E^* is finitely generated in some special cases	32
6	The Ext-algebra E^* is finitely presented when $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$	33
6.1	The Ext-algebra in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$: notation and recollection of and results	34
6.2	Outline of the strategy for the first main result	45
6.3	The tensor algebra	46
6.4	The 2 nd graded piece of the kernel	49
6.5	The 3 rd graded piece of the kernel	64
6.6	The 4 th graded piece of the kernel	74
6.7	First main result: finite presentation over the tensor algebra of E^1	74
6.8	Second main result: finite presentation as a k -algebra	75
	References	86

1 Introduction

1.1 Context

In the framework of the local Langlands program, a fundamental problem is to obtain an understanding of categories of representations of p -adic reductive groups G , such as $G = \mathrm{GL}_n(\mathbb{Q}_p)$ or $G = \mathrm{SL}_n(\mathbb{Q}_p)$. In particular, in the case of representations over fields of characteristic p , such an understating is still far from complete.

Let us introduce the setting: let p be a prime number, let $\mathfrak{F}$ be a finite extension of $\mathbb{Q}_p$ or the field of formal Laurent series $\mathbb{F}_q((X))$, where q is a power of p . Let G be the group of $\mathfrak{F}$ -rational points of a connected split reductive group defined over $\mathfrak{F}$ (for example, $G = \mathrm{GL}_n(\mathfrak{F})$ or $G = \mathrm{SL}_n(\mathfrak{F})$). It is naturally endowed with the structure of a locally profinite topological group. Let k be a field of characteristic p , and let $\mathrm{Rep}_k^\infty(G)$ be the category of smooth representations of G on k -vector spaces.

Let I be a pro- p Iwahori subgroup of G . For example, in the case that $G = \mathrm{GL}_2(\mathbb{Q}_p)$ or $\mathrm{SL}_2(\mathbb{Q}_p)$ we may choose

$$I = \begin{pmatrix} 1 + p\mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & 1 + p\mathbb{Z}_p \end{pmatrix}.$$

(with the understanding that matrices have determinant 1 if we are considering $\mathrm{SL}_2(\mathbb{Q}_p)$).

A fundamental tool to try to study the category $\mathrm{Rep}_k^\infty(G)$ is the pro- p Iwahori–Hecke algebra defined by

$$H := \mathrm{End}_{\mathrm{Rep}_k^\infty(G)}(k[G/I])^{\mathrm{op}}.$$

Here, $k[G/I]$ is the free k -vector space generated by the left cosets, endowed with the natural action of G (in this way $k[G/I]$ is a smooth representation, that can be described more abstractly as the compact induction $\text{c-ind}_I^G k$ of the trivial representation k). Furthermore, $\text{End}_{\text{Rep}_k^\infty(G)}(k[G/I])$ denotes the ring of endomorphisms and R^{op} denotes the opposite ring of a ring R . The ring H is a (not necessarily commutative) k -algebra that has been studied in particular by Vignéras (see for example [Vig16]).

The link between H and the category $\text{Rep}_k^\infty(G)$ is the following functor:

$$\begin{aligned} \text{Rep}_k^\infty(G) &\longrightarrow \text{Mod}(H) \\ V &\longmapsto V^I \cong \text{Hom}_{\text{Rep}_k^\infty(G)}(k[G/I], V). \end{aligned} \tag{1}$$

Here, $\text{Mod}(H)$ denotes the category of left modules over H and H acts on $\text{Hom}_{\text{Rep}_k^\infty(G)}(k[G/I], V)$ by composition (defining a left action since we considered the opposite ring in the definition of H).

If k , instead of being of characteristic p , were the field of complex numbers, then the functor (1) would be exact and, if furthermore I were a Iwahori subgroup of G , then a fundamental result of Bernstein [BD84, Corollary 3.9.ii] would show that the functor induces an equivalence of categories when restricted to the full subcategory $\text{Rep}_k^{\infty, I}(G)$ of those smooth representations that are generated by their I -invariant vectors.

In our case instead, the functor (1) is only left exact. The advantage of considering a pro- p group when k has characteristic p is that a non-zero smooth representation V is sent to a non-zero module V^I by the functor (1). In particular, the subcategory $\text{Rep}_k^{\infty, I}(G)$ contains all irreducible representations. The specific choice of a pro- p Iwahori subgroup is done in order for the algebra H to be “as simple as possible”.

In this setting, the functor (1) restricted to $\text{Rep}_k^{\infty, I}(G)$ defines an equivalence of categories only in a few special cases (see [Oll09, OS11, Koz16] and, in particular, [Koz16, Corollary 5.3]). Schneider [Sch15], however, proved that the situation does improve when one constructs a derived version

$$D(\text{Rep}_k^\infty(G)) \longrightarrow D(\text{DGMod}(\mathcal{H}^\bullet)). \tag{2}$$

of the functor (1). Here, $D(\text{Rep}_k^\infty(G))$ denotes the derived category of $\text{Rep}_k^\infty(G)$, while $\mathcal{H}^\bullet$ denotes a certain differential-graded algebra that plays the role of H (more precisely it is the Hom complex $\text{Hom}^\bullet(\mathcal{J}^\bullet, \mathcal{J}^\bullet)^{\text{op}}$, where $k[G/K] \rightarrow \mathcal{J}^\bullet$ is a fixed injective resolution) and $D(\text{DGMod}(\mathcal{H}^\bullet))$ denotes the derived category of the category of differential-graded modules over $\mathcal{H}^\bullet$. The main result of [Sch15] is that, under the assumption that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free, the functor (2) defines an equivalence of triangulated categories (without the need to restrict to any subcategory).

The objects involved in (2) are much more complicated than those in (1), and an explicit description of the differential graded algebra $\mathcal{H}^\bullet$ is not known.

As an intermediate step, one may try to study instead the Ext-algebra

$$E^* := \text{Ext}^*(k[G/I], k[G/I])^{\text{op}}.$$

This is the cohomology algebra of $\mathcal{H}^\bullet$, and its 0^{th} graded piece is of course H . Such idea is pursued in the work of Ollivier–Schneider [OS19, OS22]. They describe E^* via a certain isomorphism of k -vector spaces

$$E^* \cong \bigoplus_{w \in \widetilde{W}} H^*(I \cap wIw^{-1}, k). \quad (3)$$

Here $\widetilde{W}$ is a certain subquotient of G called the pro- p Iwahori–Weyl group, and $H^*(I \cap wIw^{-1}, k)$ denotes the cohomology of the profinite group $I \cap wIw^{-1}$ with respect to the trivial module k . This decomposition generalizes the Iwahori–Matsumoto basis of $H = E^0$ studied in [Vig16].

Some of the main results by Ollivier–Schneider are the following: a description of the multiplication on E^* via cohomological operations on the right hand side of (3) [OS19, Proposition 5.3]; a more detailed description of the (left) action of E^0 on E^* [OS19, Proposition 5.6]; the existence of an involutive anti-automorphism [OS19, Proposition 6.1]; a duality theorem in the case that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and I is torsion-free [OS19, Proposition 7.18]; a complete description of the structure of E^* as an E^0 -bimodule in the case that $G = \text{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ [OS22, §7]. As an interesting consequence, under the latter assumptions they show that an irreducible representation V is supersingular if and only if its cohomology $H^*(I, V)$ is supersingular as a left H -module [OS22, Corollary 8.12].

1.2 Main results

The present paper is devoted to the study of finite generation properties of the Ext-algebra E^* , especially in the case $G = \text{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$.

In §3, we study the 1^{st} graded piece E^1 as an E^0 -bimodule, and we prove the following result, under quite general assumptions.

Proposition (Proposition 3.5). *Assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$. One has that E^1 is finitely generated as an E^0 -bimodule.*

To prove statements on the whole algebra E^* , in §4 and §5 we specialize to the case of “small G ” (as will be made precise in the statements below), and we study the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$, where $T_{E^0}^* E^1$ denotes the tensor algebra of the E^0 -bimodule E^1 . We first prove the following result.

Proposition (Proposition 4.8, Remark 4.9). *Assume that $p \neq 2, 3$, that $\mathfrak{F}$ is a (finite) unramified extension of $\mathbb{Q}_p$ and that G is either $\text{SL}_2(\mathfrak{F})$ or $\text{PGL}_2(\mathfrak{F})$. One has the image of the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$ has finite codimension in E^* . If instead $G = \text{GL}_2(\mathfrak{F})$, an analogous more technical result holds.*

The two propositions above allow us to prove, with very little effort, that the Ext-algebra is finitely generated as a k -algebra in the above cases. This is the first main result of the paper.

Theorem (Theorem 5.1). *Assume that $p \neq 2, 3$, that $\mathfrak{F}$ is a (finite) unramified extension of $\mathbb{Q}_p$ and that G is one of $\mathrm{SL}_2(\mathfrak{F})$, $\mathrm{PGL}_2(\mathfrak{F})$ or $\mathrm{GL}_2(\mathfrak{F})$. One has that the Ext-algebra E^* is finitely generated as a k -algebra.*

The longest part of the paper (namely, §6) deals with the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. Under this assumption, the explicit description of the Ext-algebra of [OS22] becomes available, and we exploit such description to obtain more precise results.

We first show that the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$ is surjective, and then, with quite a long computation, we explicitly determine its kernel. We prove the following result.

Theorem (Theorem 6.21). *Assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. The multiplication map*

$$\mathcal{M}: T_{E^0}^* E^1 \rightarrow E^*$$

is surjective and its kernel is generated by its 2nd and 3rd graded pieces as a two-sided ideal. Furthermore, the kernel is finitely generated as a two-sided ideal.

We will actually compute an explicit finite list of generators (see again Theorem 6.21).

Starting from the “presentation” of E^* determined by the above theorem, we then compute a presentation of E^* as a (non-commutative) k -algebra. This is achieved by computing a presentation of E^0 (the pro- p Iwahori–Hecke algebra) as a k -algebra and a presentation of E^1 as an E^0 -bimodule. Combining these two presentations with the above theorem, one then readily obtains a presentation of E^* as a k -algebra. In this way, we obtain the following result.

Theorem (Theorem 6.26). *Assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. The Ext-algebra E^* is finitely presented as a k -algebra.*

We stress the fact that we obtain this result by explicitly computing a finite presentation (see again Theorem 6.26).

1.3 Acknowledgements

A large portion of the material in this article was part of the author’s PhD thesis [Bod22] under the direction of Peter Schneider. I thank him for the invaluable help and support, his fruitful and precise comments, and for suggesting such a research topic.

I am indebted with Claudius Heyer for the extremely useful discussions and his great interest in my work. I thank Rachel Ollivier for very interesting discussions and her support during the write-up of this article.

I acknowledge funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy EXC 2044 – 390685587, Mathematics Münster: Dynamics – Geometry – Structure, and under the CRC 1442 Geometry: Deformations and Rigidity (Project Number 427320536).

2 Setting and background

2.1 Notation and assumptions

We fix the following data throughout the paper.

We consider a non-archimedean local field $\mathfrak{F}$. We denote by $p > 0$ its residue characteristic and by $q = p^f$ its residue cardinality. We recall that $\mathfrak{F}$ is either a finite extension of $\mathbb{Q}_p$ or the field of Laurent series $\mathbb{F}_q((X))$. Almost everywhere in this paper we will exclude the second case, but we nevertheless allow such case in this section and in a few lemmas later on for consistency with [OS19], for sake of generality, and to point out a case in which our first result fails (Example 3.6). We denote by $\mathfrak{O}$ the ring of integers of $\mathfrak{F}$, and by $\mathfrak{M}$ the maximal ideal of $\mathfrak{O}$. We also fix a uniformizer π .

Let $\mathbf{G}$ be a split connected reductive group over $\mathfrak{F}$. Many results in this paper will only be valid for special choices of $\mathbf{G}$, as will be explained later. We will always use the convention of denoting linear algebraic groups over $\mathfrak{F}$ with boldface letters, and we will denote the associated group of $\mathfrak{F}$ -rational points with the corresponding non-boldface letter (e.g., in the case of $\mathbf{G}$, we will have $G = \mathbf{G}(\mathfrak{F})$). Such groups will be understood as locally profinite groups, with respect to the topology induced by $\mathfrak{F}$.

Let us choose a split maximal torus $\mathbf{T}$ of $\mathbf{G}$. Let T^0 be the unique maximal compact subgroup of T (isomorphic to $(\mathfrak{O}^\times)^{\dim \mathbf{T}}$), and let T^1 be the unique maximal pro- p subgroup of T (isomorphic to $(1 + \mathfrak{M})^{\dim \mathbf{T}}$).

Let $\mathbf{N}$ be the normalizer of $\mathbf{T}$ in $\mathbf{G}$. We define the (discrete) groups

$$W_0 := N/T, \quad W := N/T^0, \quad \widetilde{W} := N/T^1.$$

The group W_0 is the usual Weyl group, the group W is sometimes called extended affine Weyl group or Iwahori–Weyl group, and the group $\widetilde{W}$ is sometimes called pro- p Iwahori–Weyl group.

Let us consider the semisimple (or adjoint) building associated with $\mathbf{G}$ (see [Vig16, Definition 3.12]) and the apartment corresponding to the choice of $\mathbf{T}$. Let us choose a chamber $\mathfrak{C}$ in such apartment. Let J be the Iwahori subgroup of G corresponding to the choice of $\mathfrak{C}$ (see [HR08] for some possible, and equivalent, definitions), and let I be the corresponding pro- p Iwahori subgroup, i.e., the pro- p radical of J .

We fix a field k of characteristic p (i.e., the same characteristic as the residue field of $\mathfrak{F}$), which will be the coefficient field of the algebras that we will consider.

Warning on the assumptions. Many results in the paper will be stated under stronger assumptions than those above. For §3, §4 and §5, any further assumption will be made explicit in every single statement. In §6, instead, the assumptions will be made explicit only at the beginning and will hold throughout.

2.2 The apartment

In this section and the next ones, we will recall a few notions from Bruhat–Tits theory. We will only need a few facts from the treatise [BT72, BT84]. For a more in-depth recollection of the what is needed in the context of the pro- p Iwahori–Hecke algebra (or its Ext-version) see for example [Vig16, §3]. The present summary is partially inspired by those in [OS19] and [Hey19].

The pair $(\mathbf{G}, \mathbf{T})$ defines a root datum $(X^*(\mathbf{T}), \Phi, X_*(\mathbf{T}), \Phi^\vee)$, where $X^*(\mathbf{T})$ is the group of characters, Φ is the set of roots, $X_*(\mathbf{T})$ is the group of cocharacters, and $\Phi^\vee$ is the set of coroots.

Associated with every root $\alpha \in \Phi$ one has an additive subgroup $\mathbf{U}_\alpha$ of $\mathbf{G}$. We fix a Chevalley system $(x_\alpha: \mathbb{G}_a \rightarrow \mathbf{U}_\alpha)_{\alpha \in \Phi}$ according to the definition given in [BT84, 3.2.1 and 3.2.2]. For all $\alpha \in \Phi$, we denote by $\varphi_\alpha: \mathrm{SL}_2 \rightarrow \mathbf{G}$ the associated morphism defined in [BT84, 3.2.1]. In particular, we recall from loc. cit. that for all $\alpha \in \Phi$ and all $u \in \mathfrak{F}$ one has

$$x_\alpha(u) = \varphi_\alpha \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \quad x_{-\alpha}(u) = \varphi_\alpha \begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix}.$$

For all $\alpha \in \Phi$, the homomorphism of algebraic groups

$$\begin{aligned} \check{\alpha}: \mathbb{G}_m &\longrightarrow \mathbf{G} \\ x &\longmapsto \varphi_\alpha \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \end{aligned}$$

has values in $\mathbf{T}$ (i.e., $\check{\alpha} \in X_*(\mathbf{T})$). It is called the *coroot* associated with α , and seeing $\mathbb{R} \otimes_{\mathbb{Z}} X_*(\mathbf{T})$ as the dual of $\mathbb{R} \otimes_{\mathbb{Z}} X^*(\mathbf{T})$, the coroot $\check{\alpha}$ is indeed the coroot associated with α in the sense of abstract root systems (and hence we will write $\check{\alpha} \in \Phi^\vee$).

The apartment $\mathcal{A}$ corresponding to $\mathbf{T}$ of the semisimple building of $\mathbf{G}$ is a real affine space whose underlying vector space is

$$V_{\mathcal{A}} := (X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)) \otimes_{\mathbb{Z}} \mathbb{R},$$

where $\mathbf{C}^\circ$ denotes the connected centre of $\mathbf{G}$. We fix the valuation x_0 (in the sense of Bruhat–Tits) associated with the Chevalley system $(x_\alpha)_{\alpha \in \Phi}$ (see [BT72, Examples (6.2.3) b])). It is an element of $\mathcal{A}$, and one actually has

$$\mathcal{A} = x_0 + V_{\mathcal{A}}.$$

We assume that the closure of the chamber $\mathfrak{C}$ chosen in §2.1 contains x_0 . Then the choice of $\mathfrak{C}$ is equivalent to the choice of a set of positive roots $\Phi^+ \subseteq \Phi$. We denote by Φ^- the corresponding set of negative roots.

Let us consider the perfect pairing $\langle -, - \rangle: X_*(\mathbf{T}) \times X^*(\mathbf{T}) \rightarrow \mathbb{Z}$. It is W_0 -equivariant for the left actions of W_0 on $X_*(\mathbf{T})$ and $X^*(\mathbf{T})$ (defined via the conjugation action of W_0 on T). For all $t \in T$ there exists a unique cocharacter $\mu(t) \in X_*(\mathbf{T})$ satisfying the condition

$$\langle \mu(t), \chi \rangle = -\mathrm{val}_{\mathfrak{F}}(\chi(t)) \quad \text{for all } \chi \in X^*(\mathbf{T}).$$

The map $\mu: T \longrightarrow X_*(\mathbf{T})$ obtained in this way is thus a surjective group homomorphism, it is W_0 -equivariant and it induces an isomorphism $T/T^0 \longrightarrow X_*(\mathbf{T})$. We will actually use more often the induced surjective group homomorphism

$$\nu: T/T^0 \longrightarrow X_*(\mathbf{T})/X_*(\mathbf{C}^\circ) \subseteq V_{\mathcal{A}}.$$

We will often write $\nu(t)$ not only for $t \in T/T^0$ but also for $t \in T/T^1$.

We also consider the following perfect pairing, induced by the one above:

$$\langle -, - \rangle : (X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)) \times \text{span}_{\mathbb{Z}} \Phi \longrightarrow \mathbb{Z}.$$

In particular, with this notation we have that $\langle \nu(t), \alpha \rangle = -\text{val}_{\mathfrak{F}}(\alpha(t))$ for all $t \in T/T^0$ and all $\alpha \in \Phi$.

By [SFW67, Lemma 56], the surjection $N \longrightarrow W_0$ becomes split after one quotients out the subgroup of T generated by $\check{\alpha}(-1)$ for α running over Φ , and moreover an explicit splitting is obtained by sending, for all $\alpha \in \Phi$, the reflection defined by α to (the class of) $\varphi_\alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (note that the result in loc. cit. is stated for split semisimple groups, but it might be applied to general split reductive groups by working with the derived subgroup). It thus follows that the exact sequence

$$1 \longrightarrow T/T^0 \longrightarrow W \longrightarrow W_0 \longrightarrow 1$$

is split: therefore we write $W = T/T^0 \rtimes W_0$ and we view W_0 as a subgroup of W , fixing once and for all the splitting determined by the above rule.

The group W acts on the apartment (or equivalently, on its supporting vector space) by the following rule:

$$\begin{aligned} W \times V_{\mathcal{A}} &\longrightarrow V_{\mathcal{A}} \\ (w_0 t, x) &\longmapsto w_0 \cdot (x + \nu(t)). \\ \text{(for } w_0 \in W_0, t \in T/T^0) \end{aligned}$$

where the action of w_0 on $V_{\mathcal{A}}$ is defined via the usual action of the Weyl group on cocharacters.

2.3 Affine roots and the length function

We continue recalling a few notions from the literature, following in particular [OS19, §2.1.3].

We define the set of affine roots, the set of positive affine roots and the set of negative affine roots respectively as

$$\Phi_{\text{aff}} := \Phi \times \mathbb{Z}, \quad \Phi_{\text{aff}}^+ := (\Phi \times \mathbb{Z}_{\geq 1}) \cup (\Phi^+ \times \{0\}), \quad \Phi_{\text{aff}}^- := \Phi_{\text{aff}} \setminus \Phi_{\text{aff}}^+.$$

The group W acts on the set of affine roots via the following rule:

$$\begin{aligned} W \times \Phi_{\text{aff}} &\longrightarrow \Phi_{\text{aff}} \\ (w_0 t, (\alpha, \mathfrak{h})) &\longmapsto (w_0 \alpha, \mathfrak{h} - \langle \nu(t), \alpha \rangle) = (w_0 \alpha, \mathfrak{h} + \text{val}_{\mathfrak{F}}(\alpha(t))). \\ \text{(for } w_0 \in W_0, t \in T/T^0) \end{aligned}$$

The length function on W is defined as

$$\begin{aligned} \ell: W &\longrightarrow \mathbb{Z}_{\geq 0} \\ w &\longmapsto \# \{(\alpha, \mathfrak{h}) \in \Phi_{\text{aff}}^+ \mid w(\alpha, \mathfrak{h}) \in \Phi_{\text{aff}}^-\} \end{aligned}$$

(see [Lus89, §1.4]). It satisfies the property $\ell(wv) \leq \ell(w) + \ell(v)$ for all $w, v \in W$. Further properties will be recalled in a moment.

Let $(\alpha, \mathfrak{h}) \in \Phi_{\text{aff}}$. The class of the element $s_{(\alpha, \mathfrak{h})} := \varphi_\alpha \begin{pmatrix} 0 & \pi \mathfrak{h} \\ -\pi - \mathfrak{h} & 0 \end{pmatrix}$ acts on the apartment as the reflection through the hyperplane

$$\{x \in V_{\mathcal{A}} \mid \langle x, \alpha \rangle + \mathfrak{h} = 0\}.$$

We define W_{aff} as the subgroup of W generated by the elements $\varphi_\alpha \begin{pmatrix} 0 & \pi \mathfrak{h} \\ -\pi - \mathfrak{h} & 0 \end{pmatrix}$ for $(\alpha, \mathfrak{h})$ running over Φ_{aff} . This group can be identified with the group generated by the reflections through the above hyperplanes. It forms a Coxeter system $(W_{\text{aff}}, S_{\text{aff}})$, where

$$S_{\text{aff}} := \{s_{(\alpha, \mathfrak{h})} \mid (\alpha, \mathfrak{h}) \in (\Pi \times \{0\}) \cup (\Pi_{\min} \times \{1\})\},$$

and where Π denotes the basis of Φ corresponding to the choice of Φ^+ and $\Pi_{\min}$ denotes the set of minimal roots with respect to the partial order $\leq$ on Φ defined by the rule $\alpha \leq \beta$ if and only if $\beta - \alpha$ is a linear combination with positive coefficients of elements of Π .

Recall from [OS19, §2.1.3] that the group W admits a semidirect product decomposition

$$W = W_{\text{aff}} \rtimes \Omega,$$

where Ω is the subgroup of elements of length zero. Moreover, the length is constant on double cosets $(\Omega w \Omega)_{w \in W_{\text{aff}}}$. When restricted to W_{aff} , the length ℓ actually becomes the length function of the Coxeter system $(W_{\text{aff}}, S_{\text{aff}})$.

The explicit formulas to compute the length are the following:

$$\ell(tw_0) = \sum_{\alpha \in \Phi^+ \cap w_0 \Phi^+} |\langle \nu(t), \alpha \rangle| + \sum_{\alpha \in \Phi^+ \cap w_0 \Phi^-} |\langle \nu(t), \alpha \rangle - 1|, \quad (4)$$

$$\ell(w_0 t) = \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^+} |\langle \nu(t), \alpha \rangle| + \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^-} |\langle \nu(t), \alpha \rangle + 1|, \quad (5)$$

for all $w_0 \in W_0 \subseteq W$ and all $t \in T/T^0$ (see [Vig16, Corollary 5.10]). In particular, for all $t \in T/T^0$ one has

$$\ell(t) = \sum_{\alpha \in \Phi^+} |\langle \nu(t), \alpha \rangle| = \frac{1}{2} \sum_{\alpha \in \Phi} |\langle \nu(t), \alpha \rangle|. \quad (6)$$

For our purposes it will be fundamental to work with the already defined group $\widetilde{W} := N/T^1$ instead of W . We will slightly abuse notation and write $\ell(w)$ not only for $w \in W$ but also for $w \in \widetilde{W}$. For a subgroup $X \subseteq W$ we will write $\widetilde{X}$ for the preimage of X in $\widetilde{W}$. In particular, we will write $\widetilde{\Omega}$ and $\widetilde{W}_0$ (recall that we view $W_0 \subseteq W$).

2.4 The pro- p Iwahori–Weyl group $\widetilde{W}$ and the subgroups I_w

Recall the definition $\widetilde{W} := N/T^1$ of the pro- p Iwahori–Weyl group from §2.1. Its importance stems from the following Bruhat decomposition:

$$G = \coprod_{w \in \widetilde{W}} IwI \quad (7)$$

(see [Vig16, Proposition 3.35]), where we have not distinguished between elements of $\widetilde{W}$ and their representatives in N since $T^1 \subseteq I$, as we will recall in §2.5.

For all $w \in \widetilde{W}$ we define the following subgroup of I :

$$I_w := I \cap wIw^{-1}.$$

Here, again, we have not distinguished between elements of $\widetilde{W}$ and their representatives in N . Actually, since T^0 normalizes I , this definition makes sense also for $w \in W$. The group I_w is useful in the context of the Bruhat decomposition (7) because of the I -equivariant bijection

$$\begin{aligned} IwI/I &\longrightarrow I/I_w \\ iwI &\longmapsto iI_w. \end{aligned} \quad (8)$$

2.5 The Iwahori decomposition

Recall our fixed Chevalley system $(x_\alpha : \mathbb{G}_a \rightarrow \mathbf{U}_\alpha)_{\alpha \in \Phi}$. For all $\alpha \in \Phi$ let us consider the filtration $(\mathcal{U}_{(\alpha, m)})_{m \in \mathbb{Z}}$ of U_α defined by

$$\mathcal{U}_{(\alpha, m)} := x_\alpha(\pi^m \mathfrak{D}).$$

The groups $\mathcal{U}_{(\alpha, 1)}$ for $\alpha \in \Phi^-$, the group T^1 and the groups $\mathcal{U}_{(\alpha, 0)}$ for $\alpha \in \Phi^+$ are all contained in the pro- p Iwahori subgroup I and furthermore the multiplication map

$$\prod_{\alpha \in \Phi^-} \mathcal{U}_{(\alpha, 1)} \times T^1 \times \prod_{\alpha \in \Phi^+} \mathcal{U}_{(\alpha, 0)} \longrightarrow I$$

is bijective (see [SS97, Proposition I.2.2] and [OS14, Lemma 4.8 and its proof]; here the factors in the products are ordered in some arbitrarily chosen way). It is actually a homeomorphism, because it is a continuous bijection between compact Hausdorff spaces.

There is an analogous Iwahori decomposition for the subgroups I_w : for all $\alpha \in \Phi$ let us define

$$g_w(\alpha) := \min \{ m \in \mathbb{Z} \mid (\alpha, m) \in \Phi_{\text{aff}}^+ \cap w\Phi_{\text{aff}}^+ \}. \quad (9)$$

Then the multiplication map induce a bijection (actually, a homeomorphism)

$$\prod_{\alpha \in \Phi^-} \mathcal{U}_{(\alpha, g_w(\alpha))} \times T^1 \times \prod_{\alpha \in \Phi^+} \mathcal{U}_{(\alpha, g_w(\alpha))} \longrightarrow I_w, \quad (10)$$

where, again, the factors in the products are ordered in some arbitrarily chosen way (see [OS19, Lemma 2.3 and Remark 2.4]). Also note that the indices $g_w(\alpha)$ (and hence I_w) only depend on the image of w in W (and so we will sometimes use the notation $g_v(\alpha)$ for $v \in W$).

2.6 The pro- p Iwahori–Hecke algebra

As in the introduction, we consider the compact induction $\text{c-ind}_I^G k$ from I to G of the trivial representation k . Concretely, the compact induction $\text{c-ind}_I^G k$ can be described as the vector space $k[G/I]$ endowed with the action defined by $g \cdot g'I := gg'I$ (for all $g, g' \in G$).

As in [OS19, §2.2], we define the pro- p Iwahori–Hecke algebra to be

$$H := \text{End}_{\text{Rep}_k^\infty(G)}(k[G/I])^{\text{op}},$$

where R^{op} denotes the opposite ring of a ring R . This definition can readily be seen to be equivalent to the one given in [Vig16, §4.1], where H is defined as $\text{End}_{\text{Rep}_k^\infty(G)}(k[I \backslash G])$.

The Bruhat decomposition (7) makes clear that one has a k -basis $(\tau_w)_{w \in \widetilde{W}}$ where τ_w is the characteristic function of the double coset IwI . This is called *Iwahori–Matsumoto basis*.

A fundamental property is the following *braid relation* (see [Vig16, Theorem 2.2]):

$$\tau_v \cdot \tau_w = \tau_{vw} \quad \text{for } v, w \in \widetilde{W} \text{ such that } \ell(vw) = \ell(v) + \ell(w).$$

In the case that $\ell(vw) \neq \ell(v) + \ell(w)$, the formula is more complicated, but it is completely determined by the above braid relation and the *quadratic relations* (see [Vig16, Proposition 4.4 and Theorem 2.2]). We will only introduce the quadratic relations in the case $\mathbf{G} = \text{SL}_2$ (see (51)), since we will not need them in the general case.

2.7 The Ext-algebra E^*

We now introduce the *pro- p Iwahori–Hecke Ext-algebra* E^* following [OS19, §3]. The definition, as anticipated in the introduction is:

$$E^* := \text{Ext}^*(k[G/I], k[G/I])^{\text{op}},$$

where, this time, R^{op} denotes the opposite a graded ring R .

There is a canonical identification of k -vector spaces

$$E^* \cong H^*(I, k[G/I]),$$

where H^* denotes cohomology of profinite groups. Indeed, the abelian category $\text{Rep}_k^\infty(G)$ has enough injective objects (see [Vig96, I.5.9]), and so we can fix an injective resolution $k[G/I] \rightarrow J^\bullet$ in $\text{Rep}_k^\infty(G)$ and compute

$$\begin{aligned} E^* &= \text{Ext}_{\text{Rep}_k^\infty(G)}^*(k[G/I], k[G/I]) \\ &\cong H^*(\text{Hom}(k[G/I], J^\bullet)) \\ &\cong H^*((J^\bullet)^I) \\ &\cong H^*(I, k[G/I]), \end{aligned}$$

where we have used Frobenius reciprocity for the compact induction and the fact that restriction functor from $\text{Rep}_k^\infty(G)$ to $\text{Rep}_k^\infty(I)$ preserves injective objects (see [Vig96, Chapitre I, 5.9 d]).

Then, similarly to H , the Bruhat decomposition (7) induces a k -vector space decomposition

$$E^* \cong \bigoplus_{w \in \widetilde{W}} H^*(I, \mathbf{X}(w)), \quad \text{where } \mathbf{X}(w) := k[IwI/I],$$

since the functor $H^*(I, -)$ commutes with arbitrary direct sums (see [Ser02, Chapter I, Proposition 8]).

Let $w \in \widetilde{W}$. From (8) we have a fixed isomorphism of I -representations $k[IwI/I] \cong k[I/I_w]$. Composing the induced isomorphism between cohomology spaces with the Shapiro isomorphism $H^j(I, k[I/I_w]) \cong H^j(I_w, k)$, we thus obtain an isomorphism

$$\text{Sh}_w: H^*(I, \mathbf{X}(w)) \xrightarrow{\cong} H^*(I, k[I/I_w]) \xrightarrow{\cong} H^*(I_w, k),$$

which we will still call *Shapiro isomorphism*.

One of the main results of [OS19] consists in the description of the multiplication on E^* in terms of cohomological operations on $\bigoplus_{w \in \widetilde{W}} H^*(I, \mathbf{X}(w))$ (equivalently, on $\bigoplus_{w \in \widetilde{W}} H^*(I_w, k)$), see [OS19, Proposition 5.3]. Except in the case $G = \text{SL}_2(\mathbb{Q}_p)$, we will not use the full multiplicative structure of E^* , and so below, after a brief discussion on the needed cohomological operations, we will only state a partial (but interesting) result.

For all $w \in \widetilde{W}$ the cohomology space $H^*(I_w, k)$ has the structure of a graded-commutative k -algebra with respect to the cup product $\smile$. On the other side, the G -equivariant bilinear map $k[G/I] \times k[G/I] \rightarrow k[G/I]$ gives rise to a cup product on the cohomology space $H^*(I, k[G/I])$ (see [NSW13, Chapter I, §4]). This cup product is associative and graded-commutative but in general not unital. The two cup products are compatible in the following sense: if we transport the cup product from $H^*(I, k[G/I])$ to $\bigoplus_{w \in \widetilde{W}} H^*(I_w, k)$, the resulting product is zero when we multiply two elements lying in distinct direct summands, and, when restricted to $H^*(I_w, k)$, coincides with the natural cup product (see [OS19, §3.3]).

We also recall the conjugation on cohomology of profinite groups (with trivial coefficients). Let H be a locally profinite group, let K be a compact subgroup

and let $h \in H$. The conjugation map by h^{-1}

$$\begin{aligned} hKh^{-1} &\longrightarrow K \\ x &\longmapsto h^{-1}xh \end{aligned}$$

defines a map

$$h_*: H^i(K, k) \longrightarrow H^i(hKh^{-1}, k)$$

for all $i \in \mathbb{Z}_{\geq 0}$.

We can now state the above-mentioned partial result about the multiplication in E^* (see [OS19, Corollary 5.5]): let us consider $v, w \in \widetilde{W}$ such that $\ell(vw) = \ell(v) + \ell(w)$, let $i, j \in \mathbb{Z}_{\geq 0}$, let $\alpha \in H^i(I, \mathbf{X}(v))$ and let $\beta \in H^j(I, \mathbf{X}(w))$. One has

$$\alpha \cdot \beta = (\alpha \cdot \tau_w) \smile (\tau_v \cdot \beta) \quad (11)$$

Moreover, one has

$$\begin{aligned} \alpha \cdot \tau_w &\in H^i(I, \mathbf{X}(vw)), \\ \text{Sh}_{vw}(\alpha \cdot \tau_w) &= \text{res}_{I_{vw}}^{I_v}(\text{Sh}_v(\alpha)), \\ \tau_v \cdot \beta &\in H^i(I, \mathbf{X}(vw)), \\ \text{Sh}_{vw}(\tau_v \cdot \beta) &= \text{res}_{I_{vw}}^{vI_w v^{-1}}(v_* \text{Sh}_w(\beta)). \end{aligned} \quad (12)$$

2.8 A few results on cohomology of pro- p groups

Let K be a pro- p group. Let us consider the *Frattini subgroup* $\overline{[K, K]K^p}$, i.e., the smallest closed subgroup of K containing the commutator subgroup and the p -powers of the elements of K . We consider the *Frattini quotient*

$$(K)_{\Phi} := K / \overline{[K, K]K^p}.$$

The first cohomology with trivial coefficients can then be computed as

$$H^1(K, k) \cong \text{Hom}_{\text{TopGps}}(K, k) \cong \text{Hom}_{\text{TopGps}}((K)_{\Phi}, k),$$

where $\text{Hom}_{\text{TopGps}}(-, -)$ denotes continuous group homomorphisms. If furthermore $(K)_{\Phi}$ is finite, then we obtain

$$H^1(K, k) \cong \text{Hom}_{\text{Vect}(\mathbb{F}_p)}((K)_{\Phi}, k),$$

where $\text{Hom}_{\text{Vect}(\mathbb{F}_p)}(-, -)$ denotes homomorphisms of $\mathbb{F}_p$ -vector spaces.

In our situation we consider the case $K = I_w$ for $w \in \widetilde{W}$. Then the Iwahori decomposition (10) induces a surjective homomorphism of topological groups

$$\begin{aligned} \Psi_w: (T^1 / (T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D} / p\mathfrak{D} &\longrightarrow (I_w)_{\Phi} \\ (\bar{t}, (\overline{u_{\alpha}})_{\alpha \in \Phi}) &\longmapsto \bar{t} \cdot \prod_{\alpha \in \Phi} \overline{x_{\alpha}(\pi^{g_w(\alpha)} u_{\alpha})}. \end{aligned} \quad (13)$$

If $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ we have that both $\mathfrak{D}/p\mathfrak{D}$ and $1 + \mathfrak{M}/(1 + \mathfrak{M})^p$ (and hence also $T^1/(T^1)^p$) are finite. Therefore,

$$H^1(I_w, k) \cong \text{Hom}_{\text{Vect}(\mathbb{F}_p)}((I_w)_\Phi, k) \quad \text{if } \mathfrak{F} \text{ is a finite extension of } \mathbb{Q}_p. \quad (14)$$

For the general structure of the cup-product algebra $H^*(K, k)$ of a pro- p group K , we will use some results due to Lazard and Serre. Let K be a torsion-free analytic pro- p group of dimension n as an analytic manifold over $\mathbb{Q}_p$. One has that K is a Poincaré group of dimension n (see [SW00, Theorem 5.1.9 and the following lines]), meaning that the following conditions are satisfied: $H^n(K, k)$ is a one-dimensional k -vector space; for all $i > n$ the space $H^i(K, k)$ is zero; for all $i \in \{0, \dots, n\}$ the pairing

$$\cup: H^i(K, k) \times H^{n-i}(K, k) \longrightarrow H^n(K, k)$$

is non-degenerate. In the literature the definition of Poincaré pro- p group is usually given only in the case $k = \mathbb{F}_p$, but for a general k of characteristic p , the same properties follow because of the natural isomorphism $H^*(-, k) \cong H^*(-, \mathbb{F}_p) \otimes_{\mathbb{F}_p} k$.

A pro- p group K is called *uniform* if it is topologically finitely generated, torsion-free and powerful (see [DDSMS03, Theorem 4.5]); by definition, powerful means that $\overline{[K, K]} \subseteq \overline{K^p}$ if p is odd and $\overline{[K, K]} \subseteq \overline{K^4}$ if $p = 2$. Under these assumptions, a result by Lazard (see [SW00, Theorem 5.1.5]) states that one has natural isomorphisms of k -algebras

$$H^*(K, k) \cong \bigwedge^* (H^1(K, k)) \cong \bigwedge^* (\text{Hom}_{\text{Vect}(\mathbb{F}_p)}((K)_\Phi, k)),$$

where $\bigwedge^*(-)$ denotes the exterior algebra. Note that under the above assumptions $(K)_\Phi$ is finite (see [DDSMS03, 1.14 Proposition]).

3 The first graded piece E^1 is finitely generated as an E^0 -bimodule

In this section we will prove that E^1 is finitely generated as an E^0 -bimodule in the case that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ (Proposition 3.5). For the moment we do not make such assumption, and we start with a lemma on the generalized affine Weyl group W . The proof is inspired by the arguments in [Vig14, Lemma 2.11] (which the author already reused in [Bod22, Lemma 3.2.1]).

Lemma 3.1. *Let $w_0 \in W_0 \subseteq W$, let $r \in \mathbb{Z}_{\geq 0}$, let $\bar{\tau}$ be a closed Weyl chamber in $V_{\mathcal{A}} = (X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)) \otimes_{\mathbb{Z}} \mathbb{R}$, let $x_1, \dots, x_r \in T/T^0 \subseteq W$ be such that $\nu(x_i)$ lies in $\bar{\tau}$ for all $i \in \{1, \dots, r\}$, let $n_1, \dots, n_r \in \mathbb{Z}_{\geq 0}$ and let $m_1, \dots, m_r \in \mathbb{Z}_{\geq 0}$ with the property that if $m_i > 0$, then $n_i > 0$ (for all $i \in \{1, \dots, r\}$). One has that*

$$\ell(w_0 x_1^{n_1+m_1} \dots x_r^{n_r+m_r}) = \ell(w_0 x_1^{n_1} \dots x_r^{n_r}) + \ell(x_1^{m_1} \dots x_r^{m_r}).$$

Proof. Recall the notations in §2.3. Let $x := x_1^{n_1} \dots x_r^{n_r}$ and let $y := x_1^{m_1} \dots x_r^{m_r}$. Looking at the length formula (5), we see that

$$\begin{aligned}
\ell(w_0xy) &= \sum_{\alpha \in \Phi^+ \cap w_0^{-1}\Phi^+} |\langle \nu(xy), \alpha \rangle| + \sum_{\alpha \in \Phi^+ \cap w_0^{-1}\Phi^-} |\langle \nu(xy), \alpha \rangle + 1| \\
&\leq \sum_{\alpha \in \Phi^+ \cap w_0^{-1}\Phi^+} (|\langle \nu(x), \alpha \rangle| + |\langle \nu(y), \alpha \rangle|) \\
&\quad + \sum_{\alpha \in \Phi^+ \cap w_0^{-1}\Phi^-} (|\langle \nu(x), \alpha \rangle + 1| + |\langle \nu(y), \alpha \rangle|) \\
&= \ell(w_0x) + \ell(y),
\end{aligned}$$

and that one has equality if and only if the following two conditions hold:

- (i) For all $\alpha \in \Phi^+ \cap w_0^{-1}\Phi^+$ the signs of $\langle \nu(x), \alpha \rangle$ and of $\langle \nu(y), \alpha \rangle$ are compatible, meaning that their product is bigger or equal than zero;
- (ii) For all $\alpha \in \Phi^+ \cap w_0^{-1}\Phi^-$ the signs of $\langle \nu(x), \alpha \rangle + 1$ and of $\langle \nu(y), \alpha \rangle$ are compatible.

The condition (i) is satisfied because $\nu(x)$ and $\nu(y)$ lie in a common closed Weyl chamber. To check the thesis of the lemma, it remains to show that condition (ii) is satisfied.

Let us consider $\alpha \in \Phi^+ \cap w_0^{-1}\Phi^-$. Since all the $\nu(x_i)$'s lie in a common closed Weyl chamber, we have either that $\langle \nu(x_i), \alpha \rangle \geq 0$ for all $i \in \{1, \dots, r\}$ or that $\langle \nu(x_i), \alpha \rangle \leq 0$ for all $i \in \{1, \dots, r\}$. In the first case both $\langle \nu(x), \alpha \rangle + 1$ and $\langle \nu(y), \alpha \rangle$ are bigger or equal than 0, and so condition (ii) is satisfied. Now, let us assume that we are in the second case. If furthermore there exists $i_0 \in \{1, \dots, r\}$ such that $\langle \nu(x_{i_0}), \alpha \rangle < 0$ and $m_{i_0} > 0$ (and so also $n_{i_0} > 0$, by assumption), we obtain:

$$\begin{aligned}
\langle \nu(x), \alpha \rangle + 1 &\leq n_{i_0} \cdot \langle \nu(x_{i_0}), \alpha \rangle + 1 \\
&\leq 0, \\
\langle \nu(y), \alpha \rangle &\leq m_{i_0} \cdot \langle \nu(x_{i_0}), \alpha \rangle \\
&< 0,
\end{aligned}$$

Hence, in this case condition (ii) is satisfied. Therefore, it remains to consider the case that $\langle \nu(x_i), \alpha \rangle \leq 0$ for all $i \in \{1, \dots, r\}$ and that $m_i = 0$ for all $i \in \{1, \dots, r\}$ such that $\langle \nu(x_i), \alpha \rangle < 0$. These conditions force $\langle \nu(y), \alpha \rangle$ to be 0, and so condition (ii) is satisfied. $\square$

Recall from (9) the indices $g_w(\alpha)$ that appear in the Iwahori decomposition (10). In the following lemma we will study a certain property of these indices that will be crucial to prove Proposition 3.5. The lack of symmetry in the two conditions below reflect the lack of symmetry in the formulas (12) (where in one case only restriction appears and in the other case restriction and conjugation appear). The proof of the lemma is similar to [Bod22, Lemma 3.2.5].

Lemma 3.2. *Let $w_0 \in W_0 \subseteq W$, let $r \in \mathbb{Z}_{\geq 0}$, let $\bar{\tau}$ be a closed Weyl chamber in $V_{\mathcal{A}} = (X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)) \otimes_{\mathbb{Z}} \mathbb{R}$, let $x_1, \dots, x_r \in T/T^0 \subseteq W$ be such that $\nu(x_i)$ lies in $\bar{\tau}$ for all $i \in \{1, \dots, r\}$, let $n_1, \dots, n_r \in \mathbb{Z}_{\geq 0}$ and let $m_1, \dots, m_r \in \mathbb{Z}_{\geq 0}$ with the property that if $m_i > 0$, then $n_i > 0$ (for all $i \in \{1, \dots, r\}$). Finally, let $\alpha \in \Phi$. One has that at least one of the following two conditions is true:*

- $g_{w_0 x_1^{n_1+m_1} \dots x_r^{n_r+m_r}}(\alpha) = g_{w_0 x_1^{n_1} \dots x_r^{n_r}}(\alpha);$
- $g_{w_0 x_1^{n_1+m_1} \dots x_r^{n_r+m_r}}(\alpha) = g_{w_0 x_1^{n_1} \dots x_r^{n_r}}(\alpha) - \langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle.$

Proof. For brevity, let us define

$$\begin{aligned} a &:= g_{w_0 x_1^{n_1+m_1} \dots x_r^{n_r+m_r}}(\alpha), \\ b &:= g_{w_0 x_1^{n_1} \dots x_r^{n_r}}(\alpha), \\ c &:= g_{w_0 x_1^{n_1} \dots x_r^{n_r}}(\alpha) - \langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle. \end{aligned}$$

We have to check that either $a = b$ or $a = c$.

For all $\beta \in \Phi$ let us set

$$\varepsilon_\beta := \begin{cases} 0 & \text{if } \beta \in \Phi^+, \\ 1 & \text{if } \beta \in \Phi^-. \end{cases}$$

Recalling the definition of $g_{(-)}(\alpha)$ from (9), for all $x \in T/T^0$ we compute:

$$\begin{aligned} g_{w_0 x}(\alpha) &= \min \{ m \in \mathbb{Z} \mid (\alpha, m) \in \Phi_{\text{aff}}^+ \cap w_0 x \Phi_{\text{aff}}^+ \} \\ &= \min \left\{ m \in \mathbb{Z} \mid \begin{array}{l} (\alpha, m) \in \Phi_{\text{aff}}^+, \\ (w_0^{-1} \alpha, m + \langle \nu(x), w_0^{-1} \alpha \rangle) \in \Phi_{\text{aff}}^+ \end{array} \right\} \\ &= \max \left\{ \varepsilon_\alpha, \varepsilon_{w_0^{-1} \alpha} - \langle \nu(x), w_0^{-1} \alpha \rangle \right\}. \end{aligned}$$

Plugging in, we obtain

$$\begin{aligned} a &= \max \left\{ \varepsilon_\alpha, \varepsilon_{w_0^{-1} \alpha} - \langle \nu(x_1^{n_1+m_1} \dots x_r^{n_r+m_r}), w_0^{-1} \alpha \rangle \right\}, \\ b &= \max \left\{ \varepsilon_\alpha, \varepsilon_{w_0^{-1} \alpha} - \langle \nu(x_1^{n_1} \dots x_r^{n_r}), w_0^{-1} \alpha \rangle \right\}, \\ c &= \max \left\{ \varepsilon_\alpha, \varepsilon_{w_0^{-1} \alpha} - \langle \nu(x_1^{n_1} \dots x_r^{n_r}), w_0^{-1} \alpha \rangle \right\} - \langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle. \end{aligned}$$

We distinguish three cases on the basis of the sign of $\langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle$.

- Let us consider the case $\langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle < 0$. Using the fact that the $\nu(x_i)$'s lie in a common closed Weyl chamber, we deduce that $\langle \nu(x_i), w_0^{-1} \alpha \rangle \leq 0$ for all $i \in \{1, \dots, r\}$ and that $\langle \nu(x_{i_0}), w_0^{-1} \alpha \rangle < 0$ and $m_{i_0} > 0$ for at least one $i_0 \in \{1, \dots, r\}$. By assumption, this implies that $n_{i_0} > 0$. We thus see that $\langle \nu(x_1^{n_1} \dots x_r^{n_r}), w_0^{-1} \alpha \rangle < 0$. Of course, we also have that $\langle \nu(x_1^{n_1+m_1} \dots x_r^{n_r+m_r}), w_0^{-1} \alpha \rangle < 0$, and we conclude that

$$\begin{aligned} a &= \varepsilon_{w_0^{-1} \alpha} - \langle \nu(x_1^{n_1+m_1} \dots x_r^{n_r+m_r}), w_0^{-1} \alpha \rangle, \\ c &= \varepsilon_{w_0^{-1} \alpha} - \langle \nu(x_1^{n_1} \dots x_r^{n_r}), w_0^{-1} \alpha \rangle - \langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle, \end{aligned}$$

and hence that $a = c$.

- Let us consider the case $\langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle > 0$. With the same argument as before, we see that $\langle \nu(x_1^{n_1} \dots x_r^{n_r}), w_0^{-1} \alpha \rangle > 0$, and, of course, also that $\langle \nu(x_1^{n_1+m_1} \dots x_r^{n_r+m_r}), w_0^{-1} \alpha \rangle > 0$. We thus conclude that

$$a = \varepsilon_\alpha = b.$$

- It remains to consider the case $\langle \nu(x_1^{m_1} \dots x_r^{m_r}), w_0^{-1} \alpha \rangle = 0$, but under such assumption we clearly have $a = b = c$. $\square$

Before stating the main result of this section, we will need the following two elementary lemmas.

Lemma 3.3. *Let $r \in \mathbb{Z}_{\geq 0}$, let F be a finite set, and let $\varphi: \mathbb{Z}_{\geq 0}^r \rightarrow F$ be a map of sets. One has that there exists a finite subset $N \subseteq \mathbb{Z}_{\geq 0}^r$ such that for all $(n_1, \dots, n_r) \in \mathbb{Z}_{\geq 0}^r$ there exists $(m_1, \dots, m_r) \in N$ with the property that:*

- $\varphi(m_1, \dots, m_r) = \varphi(n_1, \dots, n_r)$,
- for all $i \in \{1, \dots, r\}$ one has $m_i \leq n_i$,
- for all $i \in \{1, \dots, r\}$ such that $n_i > 0$, one has $m_i > 0$.

Proof. Omitted. $\square$

Lemma 3.4. *Let V be a finite-dimensional vector space over a field. Let ρ and λ be endomorphisms of V such that there exists $n \in \mathbb{Z}_{\geq 1}$ satisfying the following properties:*

$$\begin{aligned} \rho^{n+1} &= \rho^n, \\ \ker(\rho^n) \cap \ker(\lambda) &= 0, \\ \rho^n \circ \lambda &= \lambda \circ \rho^n, \end{aligned}$$

One has that the subspace $\text{Image}(\rho) + \text{Image}(\lambda)$ is the full V .

Proof. Let us choose a complement V' of $\ker(\rho^n)$ in V . It suffices to prove that the endomorphism

$$\begin{aligned} V = \ker(\rho^n) \oplus V' &\longrightarrow V \\ (x, y) &\longmapsto \lambda(x) + \rho(y) \end{aligned}$$

is injective (hence surjective). So, let (x, y) be in the kernel. Using the first and third assumptions of the lemma, we obtain

$$\begin{aligned} 0 &= \rho^n(\lambda(x)) + \rho^{n+1}(y) \\ &= \lambda(\rho^n(x)) + \rho^n(y) \\ &= \rho^n(y). \end{aligned}$$

Therefore, $y \in \ker(\rho^n) \cap V'$ and so $y = 0$. But now $x \in \ker(\rho^n) \cap \ker(\lambda) = 0$, and so we conclude that also $x = 0$. $\square$

We are now able to prove the main result of §3.

Proposition 3.5. *Assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$. One has that E^1 is finitely generated as an E^0 -bimodule.*

Proof. We consider the Weyl chambers of $(T/T^0) \otimes_{\mathbb{Z}} \mathbb{R} \cong X_*(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{R}$ (note that in Lemmas 3.1 and 3.2 we have instead considered the Weyl chambers of $V_{\mathcal{A}}$).

For all closed Weyl chambers $\bar{\tau}$ in $(T/T^0) \otimes_{\mathbb{Z}} \mathbb{R}$ we fix a finite set of generators $x_{\bar{\tau},1}, \dots, x_{\bar{\tau},r}$ of the monoid $(T/T^0) \cap \bar{\tau}$ (as we can do by Gordan's Lemma; moreover, we choose r to be independent of $\bar{\tau}$, as we can, just to simplify the notation). We also fix representatives $\dot{x}_{\bar{\tau},1}, \dots, \dot{x}_{\bar{\tau},r} \in \widetilde{W}$ for $x_{\bar{\tau},1}, \dots, x_{\bar{\tau},r}$.

Let $w \in \widetilde{W}$. Recall from (13) the map

$$\begin{aligned} \Psi_w: (T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D} &\longrightarrow (I_w)_{\Phi} \\ (\bar{t}, (\overline{u_{\alpha}})_{\alpha \in \Phi}) &\longmapsto \bar{t} \cdot \prod_{\alpha \in \Phi} \overline{x_{\alpha}(\pi^{g_w(\alpha)} u_{\alpha})}. \end{aligned}$$

We argued that, since $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, the map Ψ_w is a surjective homomorphism of *finite-dimensional* $\mathbb{F}_p$ -vector spaces. We also consider the induced isomorphism

$$\overline{\Psi_w}: \frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{\ker(\Psi_w)} \longrightarrow (I_w)_{\Phi}$$

and the dual isomorphism

$$\overline{\Psi_w}^{\vee}: H^1(I, \mathbf{X}(w)) \longrightarrow \mathrm{Hom}_{\mathrm{Vect}(\mathbb{F}_p)} \left(\frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{\ker(\Psi_w)}, k \right)$$

(compare (14)).

Let $\widetilde{W}_0$ denote the preimage of W_0 via the quotient map $\widetilde{W} \longrightarrow W$ (recall that we view W_0 as a subgroup of W). For all $w_0 \in \widetilde{W}_0$ and all closed Weyl chambers $\bar{\tau}$ in $(T/T^0) \otimes_{\mathbb{Z}} \mathbb{R}$ we consider the function

$$\begin{aligned} \mathbb{Z}_{\geq 0}^r &\longrightarrow \left\{ \text{sub-}\mathbb{F}_p\text{-vector spaces of } \right. \\ &\quad \left. (T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D} \right\} \\ (n_1, \dots, n_r) &\longmapsto \ker(\Psi_{w_0 \dot{x}_{\bar{\tau},1}^{n_1} \dots \dot{x}_{\bar{\tau},r}^{n_r}}). \end{aligned}$$

By Lemma 3.3, there exists a finite set $N_{w_0, \bar{\tau}}$ with the property that, for all $(n_1, \dots, n_r) \in \mathbb{Z}_{\geq 0}^r$, there exists $(m_1, \dots, m_r) \in N_{w_0, \bar{\tau}}$ such that:

$$\ker(\Psi_{w_0 \dot{x}_{\bar{\tau},1}^{m_1} \dots \dot{x}_{\bar{\tau},r}^{m_r}}) = \ker(\Psi_{w_0 \dot{x}_{\bar{\tau},1}^{n_1} \dots \dot{x}_{\bar{\tau},r}^{n_r}}), \quad (15)$$

$$\text{for all } i \in \{1, \dots, r\} \text{ one has } m_i \leq n_i, \quad (16)$$

$$\text{for all } i \in \{1, \dots, r\} \text{ such that } n_i > 0, \text{ one has } m_i > 0. \quad (17)$$

We consider the following *finite* set:

$$\mathcal{G} := \left\{ w_0 \dot{x}_{\bar{\epsilon},1}^{m_1} \cdots \dot{x}_{\bar{\epsilon},r}^{m_r} \left| \begin{array}{l} w_0 \in \widetilde{W}_0, \\ \bar{\epsilon} \subseteq (T/T^0) \otimes_{\mathbb{Z}} \mathbb{R} \text{ closed Weyl chamber,} \\ (m_1, \dots, m_r) \in N_{w_0, \bar{\epsilon}} \end{array} \right. \right\}.$$

To prove the proposition, it suffices to show that the subspace

$$\bigoplus_{v \in \mathcal{G}} H^1(I, \mathbf{X}(v))$$

generates E^1 as an E^0 -bimodule, as we said that $\mathcal{G}$ is finite and that $H^1(I, \mathbf{X}(v))$ is finite-dimensional over k .

Let $w \in \widetilde{W}$. We can write it in the form $w = w_0 \dot{x}_{\bar{\epsilon},1}^{n_1} \cdots \dot{x}_{\bar{\epsilon},r}^{n_r}$ for some $w_0 \in \widetilde{W}_0$, some closed Weyl chamber $\bar{\epsilon} \subseteq (T/T^0) \otimes_{\mathbb{Z}} \mathbb{R}$ and some r -tuple $(n_1, \dots, n_r) \in \mathbb{Z}_{\geq 0}^r$. Let us pick an r -tuple $(m_1, \dots, m_r) \in N_{w_0, \bar{\epsilon}}$ satisfying properties (15), (16) and (17). By (16), for all $i \in \{1, \dots, r\}$ we have that $n_i - m_i \in \mathbb{Z}_{\geq 0}$, and from (17) we see that if $n_i - m_i > 0$ then $m_i > 0$. Therefore, Lemma 3.1 yields that

$$\ell(w_0 \dot{x}_{\bar{\epsilon},1}^{n_1} \cdots \dot{x}_{\bar{\epsilon},r}^{n_r}) = \ell(w_0 \dot{x}_{\bar{\epsilon},1}^{m_1} \cdots \dot{x}_{\bar{\epsilon},r}^{m_r}) + \ell(\dot{x}_{\bar{\epsilon},1}^{n_1-m_1} \cdots \dot{x}_{\bar{\epsilon},r}^{n_r-m_r}).$$

To ease notation, let us set $v := w_0 \dot{x}_{\bar{\epsilon},1}^{m_1} \cdots \dot{x}_{\bar{\epsilon},r}^{m_r}$ and $y := \dot{x}_{\bar{\epsilon},1}^{n_1-m_1} \cdots \dot{x}_{\bar{\epsilon},r}^{n_r-m_r}$. Note that $v \in \mathcal{G}$. With the new notation, the above equation becomes

$$\ell(w) = \ell(vy) = \ell(v) + \ell(y). \quad (18)$$

Since $y \in T/T^1$, we have that $\ell(y) = \ell(vyv^{-1})$ (as can be seen from (6)), and so the above equation can also be rewritten as

$$\ell(w) = \ell(vyv^{-1}v) = \ell(vyv^{-1}) + \ell(v). \quad (19)$$

Although we will need this only at a much later point, we also apply Lemma 3.2 (whose assumptions are satisfied, again by (16) and (17)). It tells us that for all $\alpha \in \Phi$ at least one of the following two equalities must be true:

$$\begin{aligned} g_{w_0 x_1^{n_1} \dots x_r^{n_r}}(\alpha) &= g_{w_0 x_1^{m_1} \dots x_r^{m_r}}(\alpha), \\ g_{w_0 x_1^{n_1} \dots x_r^{n_r}}(\alpha) &= g_{w_0 x_1^{m_1} \dots x_r^{m_r}}(\alpha) - \langle \nu(x_1^{n_1-m_1} \dots x_r^{n_r-m_r}), w_0^{-1} \alpha \rangle. \end{aligned}$$

With the simplified notation we have introduced, these two equalities can be rewritten as

$$\begin{aligned} g_w(\alpha) &= g_v(\alpha), \\ g_w(\alpha) &= g_v(\alpha) - \langle \nu(y), w_0^{-1} \alpha \rangle = g_v(\alpha) - \langle \nu(vyv^{-1}), \alpha \rangle. \end{aligned} \quad (20)$$

Now let us consider an element $\beta_v \in H^1(I, \mathbf{X}(v))$. By (18) and (19), we can apply formulas (12) to compute the following products:

$$\begin{aligned} \beta_v \cdot \tau_y &\in H^1(I, \mathbf{X}(vy)) = H^1(I, \mathbf{X}(w)) \\ \text{Sh}_w(\beta_v \cdot \tau_y) &= \text{res}_{I_w}^{I_v} (\text{Sh}_v(\beta_v)). \\ \tau_{vyv^{-1}} \cdot \beta_v &\in H^1(I, \mathbf{X}(vyv^{-1}v)) = H^1(I, \mathbf{X}(w)) \\ \text{Sh}_w(\tau_{vyv^{-1}} \cdot \beta_v) &= \text{res}_{I_w}^{vyv^{-1}I_v(vyv^{-1})^{-1}} ((vyv^{-1})_* \text{Sh}_v(\beta_v)). \end{aligned} \quad (21)$$

If we prove that the elements of the form $\beta_v \cdot \tau_y$ and $\tau_{vyv^{-1}} \cdot \beta_v$, for β_v running over $H^1(I, \mathbf{X}(v))$, generate the full k -vector space $H^1(I, \mathbf{X}(w))$, then the thesis of the proposition is proved.

From (21) we see that for all $\beta_v \in H^1(I, \mathbf{X}(v))$ and for all $\alpha \in \Phi$ we have that

$$\begin{aligned}
\text{Sh}_w(\beta_v \cdot \tau_y)|_{T^1} &= \text{Sh}_v(\beta_v)|_{T^1}, \\
\text{Sh}_w(\beta_v \cdot \tau_y)|_{\mathcal{U}_{\alpha, g_w(\alpha)}} &= \text{Sh}_v(\beta_v)|_{\mathcal{U}_{\alpha, g_w(\alpha)}}, \\
\text{Sh}_w(\tau_{vyv^{-1}} \cdot \beta_v)|_{T^1} &= \text{Sh}_v(\beta_v)((vyv^{-1})^{-1} \cdot - \cdot vyv^{-1})|_{T^1} \\
&= \text{Sh}_v(\beta_v)|_{T^1}, \\
\text{Sh}_w(\tau_{vyv^{-1}} \cdot \beta_v)|_{\mathcal{U}_{\alpha, g_w(\alpha)}} &= \text{Sh}_v(\beta_v)((vyv^{-1})^{-1} \cdot - \cdot vyv^{-1})|_{\mathcal{U}_{\alpha, g_w(\alpha)}} \\
&= \text{Sh}_v(\beta_v)(\alpha(vyv^{-1})^{-1} \cdot -)|_{\mathcal{U}_{\alpha, g_w(\alpha)}}.
\end{aligned} \tag{22}$$

To ease notation, we set $(-)^{\vee} := \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(-, k)$ and $K := \ker(\Psi_v) = \ker(\Psi_w)$. We consider the following picture:

$$\begin{array}{ccc}
H^1(I, \mathbf{X}(v)) & \xrightarrow[\tau_{vyv^{-1}} \cdot -]{-\cdot \tau_y} & H^1(I, \mathbf{X}(w)) \\
\cong \downarrow \overline{\Psi_v}^{\vee} & & \cong \downarrow \overline{\Psi_w}^{\vee} \\
\left(\frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K} \right)^{\vee} & \xrightarrow[\lambda]{\rho} & \left(\frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K} \right)^{\vee}.
\end{array}$$

We want to describe explicitly the map ρ (respectively, the map λ) making the square with the map $-\cdot \tau_y$ (respectively, with the map $\tau_{vyv^{-1}} \cdot -$) commute. Once we do this, to prove the proposition it remains to prove that the subspace $\text{Image}(\rho) + \text{Image}(\lambda)$ is the full space. Let us consider

$$\gamma \in \left(\frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K} \right)^{\vee},$$

and let us compute $\rho(\gamma)$ and $\lambda(\gamma)$. To ease notation, we set $\beta_v := (\overline{\Psi_v}^{\vee})^{-1}(\gamma)$, getting that

$$\begin{aligned}
\gamma &= \overline{\Psi_v}^{\vee}(\beta_v) = \overline{\text{Sh}_v(\beta_v)} \circ \overline{\Psi_v}, \\
\rho(\gamma) &= \overline{\Psi_w}^{\vee}(\beta_v \cdot \tau_y) = \overline{\text{Sh}_w(\beta_v \cdot \tau_y)} \circ \overline{\Psi_w}, \\
\lambda(\gamma) &= \overline{\Psi_w}^{\vee}(\tau_{vyv^{-1}} \cdot \beta_v) = \overline{\text{Sh}_w(\tau_{vyv^{-1}} \cdot \beta_v)} \circ \overline{\Psi_w}.
\end{aligned} \tag{23}$$

Here, by $\overline{\text{Sh}_v(\beta_v)}$ we mean the element of $((I_v)_{\Phi})^{\vee}$ corresponding to the element $\text{Sh}_v(\beta_v) \in H^1(I_v, k)$ (and similarly in the other two lines).

Let $t \in T^1$ and let $\bar{t}$ be its image in $\frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K}$. By (23) we have

$$\begin{aligned}
\gamma(\bar{t}) &= \text{Sh}_v(\beta_v)(t), \\
\rho(\gamma)(\bar{t}) &= \text{Sh}_w(\beta_v \cdot \tau_y)(t), \\
\lambda(\gamma)(\bar{t}) &= \text{Sh}_w(\tau_{vyv^{-1}} \cdot \beta_v)(t).
\end{aligned}$$

From (22) we then see that

$$\begin{aligned}\rho(\gamma)(\bar{t}) &= \gamma(\bar{t}), \\ \lambda(\gamma)(\bar{t}) &= \gamma(\bar{t}).\end{aligned}\tag{24}$$

Now let $\alpha \in \Phi$ and let $u_\alpha \in \mathfrak{D}$. Let us denote by $\overline{u_\alpha}$ be the image of u_α in $\frac{(T^1/(T^1)^p) \oplus \bigoplus_{\alpha' \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K}$, when $\mathfrak{D}/p\mathfrak{D}$ is embedded in $\bigoplus_{\alpha' \in \Phi} \mathfrak{D}/p\mathfrak{D}$ via the inclusion on the summand indexed by α . By (23) we have

$$\begin{aligned}\gamma(\overline{u_\alpha}) &= \text{Sh}_v(\beta_v)(x_\alpha(\pi^{g_v(\alpha)}u_\alpha)), \\ \rho(\gamma)(\overline{u_\alpha}) &= \text{Sh}_w(\beta_v \cdot \tau_y)(x_\alpha(\pi^{g_w(\alpha)}u_\alpha)), \\ \lambda(\gamma)(\overline{u_\alpha}) &= \text{Sh}_w(\tau_{vyv^{-1}} \cdot \beta_v)(x_\alpha(\pi^{g_w(\alpha)}u_\alpha)).\end{aligned}$$

Combining this with (22), we then see that

$$\begin{aligned}\rho(\gamma)(\overline{u_\alpha}) &= \text{Sh}_v(\beta_v)(x_\alpha(\pi^{g_w(\alpha)}u_\alpha)) \\ &= \gamma(\pi^{g_w(\alpha)-g_v(\alpha)}\overline{u_\alpha}), \\ \lambda(\gamma)(\overline{u_\alpha}) &= \text{Sh}_v(\beta_v)(\alpha(vyv^{-1})^{-1} \cdot x_\alpha(\pi^{g_w(\alpha)}u_\alpha)) \\ &= \gamma(\alpha(vyv^{-1})^{-1}\pi^{g_w(\alpha)-g_v(\alpha)}\overline{u_\alpha}).\end{aligned}\tag{25}$$

For all $\alpha \in \Phi$, we set $r_\alpha := \pi^{g_w(\alpha)-g_v(\alpha)}$ and $l_\alpha := \alpha(vyv^{-1})^{-1}\pi^{g_w(\alpha)-g_v(\alpha)}$. We have obtained that the following diagrams are commutative:

$$\begin{array}{ccc} \left(\frac{(T^1/(T^1)^p) \times \prod_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K} \right)^\vee & \xrightarrow[\lambda]{\rho} & \left(\frac{(T^1/(T^1)^p) \times \prod_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K} \right)^\vee \\ \downarrow & & \downarrow \\ (T^1/(T^1)^p)^\vee \oplus \bigoplus_{\alpha \in \Phi} (\mathfrak{D}/p\mathfrak{D})^\vee & \xrightarrow[\tilde{\lambda} := \text{id} \oplus \bigoplus_{\alpha \in \Phi} (l_\alpha \cdot -)^\vee]{\tilde{\rho} := \text{id} \oplus \bigoplus_{\alpha \in \Phi} (r_\alpha \cdot -)^\vee} & (T^1/(T^1)^p)^\vee \oplus \bigoplus_{\alpha \in \Phi} (\mathfrak{D}/p\mathfrak{D})^\vee \end{array}$$

If we check that there exists $n \in \mathbb{Z}_{\geq 1}$ such that

$$\begin{aligned}\rho^{n+1} &= \rho^n, \\ \ker(\rho^n) \cap \ker(\lambda) &= 0, \\ \rho^n \circ \lambda &= \lambda \circ \rho^n,\end{aligned}$$

then the assumptions of Lemma 3.4 are satisfied and so $\text{Image}(\rho) + \text{Image}(\lambda)$ is the full space $\left(\frac{(T^1/(T^1)^p) \times \prod_{\alpha \in \Phi} \mathfrak{D}/p\mathfrak{D}}{K} \right)^\vee$, as we wanted to show to conclude the proof of the proposition. But if we check that there exists $n \in \mathbb{Z}_{\geq 1}$ satisfying the above properties for $\tilde{\rho}$ in place of ρ and for $\tilde{\lambda}$ in place of λ , then a fortiori the above properties remain true for ρ and λ .

The property $\tilde{\rho}^n \circ \tilde{\lambda} = \tilde{\lambda} \circ \tilde{\rho}^n$ is completely trivial for all $n \in \mathbb{Z}_{\geq 1}$. The property $\tilde{\rho}^{n+1} = \tilde{\rho}^n$ is true for n big enough because, for all $\alpha \in \Phi$, the constant

r_α is either 1 or a positive power of π , from which it follows that the sequence $(r_\alpha^n)_{n \in \mathbb{Z}_{\geq 1}}$ is either definitely 1 or 0 in $\mathfrak{D}/p\mathfrak{D}$.

It remains to check the property $\ker(\tilde{\rho}^n) \cap \ker(\tilde{\lambda}) = 0$ (we will actually check it for all $n \in \mathbb{Z}_{\geq 1}$). Let us consider an arbitrary element

$$f = (t^\vee, (u_\alpha^\vee)_{\alpha \in \Phi}) \in (T^1/(T^1)^p)^\vee \oplus \bigoplus_{\alpha \in \Phi} (\mathfrak{D}/p\mathfrak{D})^\vee;$$

we have to check either $\tilde{\rho}^n(f)$ or $\tilde{\lambda}(f)$ is non-zero. If $t^\vee$ is non-zero, then actually both $\tilde{\rho}^n(f)$ and $\tilde{\lambda}(f)$ are non-zero. So we can now assume that $u_\alpha^\vee$ is nonzero for some $\alpha \in \Phi$. Recall from (20) that at least one of the following equalities is true:

$$\begin{aligned} g_w(\alpha) &= g_v(\alpha), \\ g_w(\alpha) &= g_v(\alpha) - \langle \nu(vyv^{-1}), \alpha \rangle. \end{aligned}$$

The first equality means that $r_\alpha = 1$ (and hence that $r_\alpha^n = 1$), while the second equality means that $l_\alpha \in \mathfrak{D}^\times$, because

$$\begin{aligned} \text{val}_{\mathfrak{F}}(l_\alpha) &= \text{val}_{\mathfrak{F}}(\alpha(vyv^{-1})^{-1}) + g_w(\alpha) - g_v(\alpha) \\ &= \langle \nu(vyv^{-1}), \alpha \rangle + g_w(\alpha) - g_v(\alpha). \end{aligned}$$

In particular, we get that either $\tilde{\rho}^n(f)$ or $\tilde{\lambda}(f)$ is non-zero. $\square$

Example 3.6. Assume that $\mathfrak{F} = \mathbb{F}_q((X))$ and that $\mathbf{G} = \mathbb{G}_m$. We show that E^1 is not finitely generated as an E^0 -bimodule.

Proof. Since $\mathbf{G} = \mathbb{G}_m$, the length function on $\widetilde{W}$ is constantly zero and any conjugation by an element of G is trivial. Therefore, looking at the formulas (11) and (12) for the multiplication on E^* we see that we have an isomorphism of graded k -algebras

$$E^* \cong E^0 \otimes_k H^*(I, k),$$

where the multiplication on $H^*(I, k)$ is the cup product. Since left and right action of E^0 are the same, saying that E^1 is finitely generated as an E^0 -bimodule is the same as saying that $H^1(I, k)$ is finitely generated as a k -vector space. This is not the case: indeed, since $\mathfrak{F} = \mathbb{F}_q((X))$, the pro- p group $1 + \mathfrak{M}$ is isomorphic to $\prod_{i \in \mathbb{Z}_{\geq 0}} \mathbb{Z}_p$ (see [FV02, Chapter I, (6.2), Proposition]), and therefore

$$H^1(I, k) = H^1(1 + \mathfrak{M}, k) \cong H^1\left(\prod_{i \in \mathbb{Z}_{\geq 0}} \mathbb{Z}_p, k\right),$$

which has infinite dimension as a k -vector space. $\square$

4 The subalgebra generated by E^0 and E^1 in some special cases

The purpose of this section is to prove Proposition 4.8, i.e., to prove that, when G is “small”, the multiplication map

$$T_{E^0}^* E^1 \longrightarrow E^*$$

is “almost surjective” (for the precise statement see the proposition as well as Remark 4.9). To prove the proposition, we need to specialize the setting introduced in Section 2 to the case that $\mathbf{G}$ has semisimple rank 1.

Let us assume that $\mathbf{G}$ has semisimple rank 1, or, equivalently, that the root system is of type A_1 . Let α_0 denote the positive root. Recalling the notation and facts on the Chevalley system reviewed in §2.2 and on the structure of the group W in §2.3, we define

$$s_0 := \overline{\varphi_{\alpha_0} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}, \quad s_1 := \overline{\varphi_{-\alpha_0} \begin{pmatrix} 0 & \pi \\ -\pi^{-1} & 0 \end{pmatrix}}, \quad (26)$$

where $\overline{\cdot}$ denotes the image of $\cdot$ in $\widetilde{W}$. Strictly speaking this definition is not compatible with the one we will give at the beginning of §6 (see there for details), but this will not cause problems.

With this definition, we have $S_{\text{aff}} = \{\overline{s_0}, \overline{s_1}\}$, where $\overline{s_i}$ denotes the image of s_i in W and every element of W_{aff} can be expressed as a string of the elements $\overline{s_0}$ and $\overline{s_1}$, with no two identical letters one after the other. This representation is actually unique and we have

$$\begin{aligned} \ell((\overline{s_0} \cdot \overline{s_1})^i) &= i, & \ell((\overline{s_1} \cdot \overline{s_0})^i) &= i, \\ \ell(\overline{s_0} \cdot (\overline{s_1} \cdot \overline{s_0})^i) &= i, & \ell(\overline{s_1} \cdot (\overline{s_0} \cdot \overline{s_1})^i) &= i, \end{aligned}$$

for all $i \in \mathbb{Z}_{\geq 0}$ (compare [OS18, §3.1] in the case $\mathbf{G} = \text{SL}_2$). Note that in the above list the string representation of the elements of W is not really unique, the trivial element being repeated twice.

We also deduce that every element of W can be represented in a unique way as a product of an element of Ω and a string of the elements $\overline{s_0}$ and $\overline{s_1}$, without repetitions as above, and every element of $\widetilde{W}$ can be represented in a unique way as a product of an element of $\widetilde{\Omega}$ and a string of the elements s_0 and s_1 , with no two identical letters one after the other.

Lemma 4.1. *Assume that $\mathbf{G}$ has semisimple rank 1. With notation as above, for all $w \in \widetilde{W}$ the following facts hold.*

- If $\ell(s_0 w) = \ell(w) + 1$, then the multiplication map defines a homeomorphism

$$x_{-\alpha_0}(\mathfrak{M}^{\ell(w)+1}) \times T^1 \times x_{\alpha_0}(\mathfrak{D}) \xrightarrow{\cong} I_w.$$

- If $\ell(s_1 w) = \ell(w) + 1$, then the multiplication map defines a homeomorphism

$$x_{-\alpha_0}(\mathfrak{M}) \times T^1 \times x_{\alpha_0}(\mathfrak{M}^{\ell(w)}) \xrightarrow{\cong} I_w.$$

Proof. This is a variation of [OS18, Equations (25) and (26)], which only deals with the case $\mathbf{G} = \text{SL}_2$. Recall from §2.4 that I_w only depends on the image of w in W , so we consider $w \in W$ rather than $w \in \widetilde{W}$. Moreover, for all $v \in W_{\text{aff}}$ and all $\omega \in \Omega$ one has $I_{v\omega} = I_v$ (see [OS19, §2.1.5]), and the condition

$\ell(\overline{s_i}vw) = \ell(vw) + 1$ is satisfied if and only if the condition $\ell(\overline{s_i}v) = \ell(v) + 1$ is. Therefore, by the above argument, one only has to consider the cases $w = (s_0 \cdot s_1)^i$, $w = (s_1 \cdot s_0)^i$, $w = s_0 \cdot (s_1 \cdot s_0)^i$, $w = s_1 \cdot (s_0 \cdot s_1)^i$ for some $i \in \mathbb{Z}_{\geq 0}$, and those cases can be dealt with explicitly as in [OS18, Equations (25) and (26)]. $\square$

Lemma 4.2. *Assume that $p \not\equiv 2$ and that $\mathbf{G}$ has semisimple rank 1. With notation as above, for all $w \in W$ the following facts hold.*

- If $\ell(s_0w) = \ell(w) + 1$, then the following equalities hold:

$$\begin{aligned} \overline{[I_w, I_w]} &= [I_w, I_w] \\ &= \varphi_{\alpha_0} \left(\begin{pmatrix} 1 + \mathfrak{M}^{\ell(w)+1} & \mathfrak{M} \\ \mathfrak{M}^{\ell(w)+2} & 1 + \mathfrak{M}^{\ell(w)+1} \end{pmatrix} \cap \mathrm{SL}_2(\mathfrak{F}) \right) \\ &= x_{-\alpha_0}(\mathfrak{M}^{\ell(w)+2}) \cdot \check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1}) \cdot x_{\alpha_0}(\mathfrak{M}). \end{aligned}$$

- If $\ell(s_1w) = \ell(w) + 1$, then the following equalities hold:

$$\begin{aligned} \overline{[I_w, I_w]} &= [I_w, I_w] \\ &= \varphi_{\alpha_0} \left(\begin{pmatrix} 1 + \mathfrak{M}^{\ell(w)+1} & \mathfrak{M}^{\ell(w)+1} \\ \mathfrak{M}^2 & 1 + \mathfrak{M}^{\ell(w)+1} \end{pmatrix} \cap \mathrm{SL}_2(\mathfrak{F}) \right) \\ &= x_{-\alpha_0}(\mathfrak{M}^2) \cdot \check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1}) \cdot x_{\alpha_0}(\mathfrak{M}^{\ell(w)+1}). \end{aligned}$$

Proof. This is a straightforward variation of [OS18, Proposition 3.62], which only deals with the case $\mathbf{G} = \mathrm{SL}_2$. $\square$

Lemma 4.3. *Assume that $p \not\equiv 2$ and that $\mathbf{G}$ has semisimple rank 1. With notation as above, for all $w \in W$ the following facts hold.*

- If $\ell(s_0w) = \ell(w) + 1$, then one has the group isomorphism

$$\begin{aligned} \mathfrak{O}/\mathfrak{M} \times \frac{T^1}{\check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1}) \cdot (T^1)^p} \times \mathfrak{O}/\mathfrak{M} &\longrightarrow (I_w)_{\Phi} \\ (\bar{c}, \bar{t}, \bar{b}) &\longmapsto \overline{x_{-\alpha_0}(-\pi^{\ell(w)+1}c) \cdot t \cdot x_{\alpha_0}(b)}. \end{aligned}$$

- If $\ell(s_1w) = \ell(w) + 1$, then one has the group isomorphism

$$\begin{aligned} \mathfrak{O}/\mathfrak{M} \times \frac{T^1}{\check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1}) \cdot (T^1)^p} \times \mathfrak{O}/\mathfrak{M} &\longrightarrow (I_w)_{\Phi} \\ (\bar{c}, \bar{t}, \bar{b}) &\longmapsto \overline{x_{-\alpha_0}(-\pi c) \cdot t \cdot x_{\alpha_0}(\pi^{\ell(w)}b)}. \end{aligned}$$

Proof. This follows from the previous lemma. The minus signs in “ $-\pi^{\ell(w)+1}c$ ” and “ $-\pi c$ ” are of course completely inessential but we keep them as they seem more natural (for example, this choice is compatible with [OS18, Proposition 3.62.ii] and $x_{-\alpha_0}(-u) = \varphi_{\alpha_0}(\begin{smallmatrix} 1 & 0 \\ u & 1 \end{smallmatrix})$). $\square$

Remark 4.4. Assume that $p \neq 2$ and that $\mathbf{G}$ has semisimple rank 1. For all $w \in \widetilde{W}$ let us define

$$T_w^1 := \frac{T^1}{\check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1}) \cdot (T^1)^p}.$$

Fixing the isomorphism

$$\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} \cong (I_w)_\Phi$$

defined in the previous lemma, and using the notation $(-)^{\vee} := \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(-, k)$, we have an induced isomorphism

$$(-, -, -)_w : (\mathfrak{O}/\mathfrak{M})^{\vee} \oplus (T_w^1)^{\vee} \oplus (\mathfrak{O}/\mathfrak{M})^{\vee} \longrightarrow H^1(I, \mathbf{X}(w)). \quad (27)$$

For the next lemma, recall from §2.8 the definition of Poincaré pro- p group and of uniform pro- p group.

Lemma 4.5. *Assume that $p \neq 2, 3$, that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ and that $\mathbf{G}$ has semisimple rank 1. One has that I is torsion-free (and so I , as well as all the subgroup I_w with $w \in \widetilde{W}$ are Poincaré pro- p groups) and that I_w is a uniform pro- p group for all $w \in \widetilde{W}$ such that $\ell(w) \geq 1$.*

Proof. We claim that G is p -torsion-free and that I_w is a powerful pro- p group for all $w \in \widetilde{W}$ such that $\ell(w) \geq 1$. Taking these two claims for granted, the two theses of the lemma follow: indeed I is p -torsion-free and hence torsion-free, and furthermore, if $\ell(w) \geq 1$, saying that the pro- p group I_w is uniform amounts to saying that it is topologically finitely generated, powerful and torsion-free. We have the last two properties, and the fact that it is topologically finitely generated follows from the fact $\mathfrak{O}$ and $1 + \mathfrak{M}$ are topologically finitely generated (since $\mathfrak{F}$ is an extension of $\mathbb{Q}_p$) and from the Iwahori decomposition of I_w .

Let us consider the derived group $\mathbf{G}'$ of $\mathbf{G}$ (which must be isomorphic either to SL_2 or to PGL_2) and the semisimple cover SL_2 of $\mathbf{G}'$: we have central isogenies

$$\mathbb{G}_m^{\dim \mathbf{C}^\circ} \times \text{SL}_2 \cong \mathbf{C}^\circ \times \text{SL}_2 \longrightarrow \mathbf{C}^\circ \times \mathbf{G}' \longrightarrow \mathbf{G}.$$

Let μ be the kernel of the composite central isogeny; it must be isomorphic a central subgroup of SL_2 : i.e., either to the trivial group or to the group of 2-units μ_2 . Considering the exact sequence induced by Galois cohomology, we obtain an exact sequence

$$\mu(\mathfrak{F}) \longrightarrow (\mathfrak{F}^\times)^{\dim \mathbf{C}^\circ} \times \text{SL}_2(\mathfrak{F}) \longrightarrow G \longrightarrow H^1(\text{Gal}(\overline{\mathbb{Q}_p}/\mathfrak{F}), \mu(\overline{\mathbb{Q}_p})).$$

The group $(\mathfrak{F}^\times)^{\dim \mathbf{C}^\circ} \times \text{SL}_2(\mathfrak{F})$ does not have p -torsion because $\mathfrak{F}$ is an extension of $\mathbb{Q}_p$ without nontrivial p -th roots of unity and because $p \neq 2, 3$ (an element of $\text{SL}_2(\mathfrak{F})$ of order p would have characteristic polynomial divisible by the p -th cyclotomic polynomial, which is absurd). The groups $\mu(\mathfrak{F})$ and

$H^1(\text{Gal}(\overline{\mathbb{Q}_p}/\mathfrak{F}), \boldsymbol{\mu}(\overline{\mathbb{Q}_p}))$ are (finite) 2-groups. It then follows formally that G is p -torsion-free: indeed, assume by contradiction that we have a non-trivial p -torsion element $x \in G$: it lifts to an element of $y \in (\mathfrak{F}^\times)^{\dim \mathbf{C}^\circ} \times \text{SL}_2(\mathfrak{F})$ since $H^1(\text{Gal}(\overline{\mathbb{Q}_p}/\mathfrak{F}), \boldsymbol{\mu}(\overline{\mathbb{Q}_p}))$ is p -torsion free. The element y^p must lift to an element $z \in \boldsymbol{\mu}(\mathfrak{F})$. Since $z^{2^r} = 1$ for some $r \in \mathbb{Z}_{\geq 1}$, it follows that y^{2^r} is a p -torsion element in $(\mathfrak{F}^\times)^{\dim \mathbf{C}^\circ} \times \text{SL}_2(\mathfrak{F})$. It cannot be trivial, because it maps to x^{2^r} .

Now it remains to prove that I_w is a powerful pro- p group for all $w \in \widetilde{W}$ such that $\ell(w) \geq 1$. We refer to the description of I_w and of $\overline{[I_w, I_w]}$ we gave, respectively, in Lemmas 4.1 4.2 and for brevity we only consider the case $\ell(s_0 w) = \ell(w) + 1$. It is enough to check that the elements of the form $\varphi_{\alpha_0}(\mathfrak{M}^{\ell(w)+2} \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$, of the form $\check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1})$ and of the form $\varphi_{\alpha_0}(\begin{smallmatrix} 1 & \mathfrak{M} \\ 0 & 1 \end{smallmatrix})$ are contained in the subgroup topologically generated by the p -powers (we will actually show that all such elements are p -powers). Since $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, we have that

$$\varphi_{\alpha_0} \left(\mathfrak{M}^{\ell(w)+2} \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right) = \left(\varphi_{\alpha_0} \left(\mathfrak{M}^{\ell(w)+1} \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right) \right)^p,$$

and so we see that the elements in $\varphi_{\alpha_0}(\mathfrak{M}^{\ell(w)+2} \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$ are p -powers of elements in I_w . The same argument shows that the elements in $\varphi_{\alpha_0}(\begin{smallmatrix} 1 & \mathfrak{M} \\ 0 & 1 \end{smallmatrix})$ are p -powers of elements in I_w . It remains to work with $\check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1})$. Since $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ with $p \neq 2$, the p -adic logarithm induces an isomorphism $1 + \mathfrak{M} \cong \mathfrak{M}$, under which $1 + \mathfrak{M}^2$ corresponds to $\mathfrak{M}^2$ (which is equal to $p\mathfrak{M}$, using again that $\mathfrak{F}$ is unramified). Therefore the elements in $1 + \mathfrak{M}^2$ are p -powers of elements in $1 + \mathfrak{M}$ and so, since $\ell(w) \geq 1$, the elements in $\check{\alpha}_0(1 + \mathfrak{M}^{\ell(w)+1})$ are p -powers of elements in $\check{\alpha}_0(1 + \mathfrak{M}) \subseteq I_w$. This concludes the proof that I_w is a powerful pro- p group. $\square$

Remark 4.6. Let $n \in \mathbb{Z}_{\geq 1}$ and let $w_1, \dots, w_n \in \widetilde{W}$ with the propriety that $\ell(w_1 \cdots w_n) = \ell(w_1) + \dots + \ell(w_n)$. For all $i \in \{1, \dots, n\}$ let $j_i \in \mathbb{Z}_{\geq 0}$ and let $\beta_i \in H^{j_i}(I, \mathbf{X}(w_i))$. The following formula holds:

$$\beta_1 \cdots \beta_n = (\beta_1 \cdot \tau_{w_2 \cdots w_n}) \cup \cdots \cup (\tau_{w_1 \cdots w_{i-1}} \cdot \beta_i \cdot \tau_{w_{i+1} \cdots w_n}) \cup \cdots \cup (\tau_{w_1 \cdots w_{n-1}} \cdot \beta_n).$$

Proof. Applying the formula relating (the opposite of) the Yoneda product with the cup product (11), we have

$$\beta_1 \cdots \beta_n = (\beta_1 \cdots \beta_{n-1} \cdot \tau_{w_n}) \cup (\tau_{w_1 \cdots w_{n-1}} \cdot \beta_n).$$

So, by induction on n , it suffices to check that the map

$$- \cdot \tau_{w_n} : H^*(I, \mathbf{X}(w_1 \cdots w_{n-1})) \longrightarrow H^*(I, \mathbf{X}(w_1 \cdots w_n))$$

commutes with cup products. Recall from (12) that we have a commutative diagram

$$\begin{array}{ccc} H^*(I, \mathbf{X}(w_1 \cdots w_{n-1})) & \xrightarrow{- \cdot \tau_{w_n}} & H^*(I, \mathbf{X}(w_1 \cdots w_n)) \\ \cong \downarrow \text{Sh}_{w_1 \cdots w_{n-1}} & & \cong \downarrow \text{Sh}_{w_1 \cdots w_n} \\ H^*(I_{w_1 \cdots w_{n-1}}, k) & \xrightarrow{\text{res}_{I_{w_1 \cdots w_n}}^{I_{w_1 \cdots w_{n-1}}}} & H^*(I_{w_1 \cdots w_n}, k), \end{array}$$

and the claim follows since restriction and Shapiro isomorphism commute with cup products. $\square$

Lemma 4.7. *Assume that $p \neq 2$ and that $\mathbf{G}$ has semisimple rank 1. Let $w \in \widetilde{W}$, let $c^-, c^+ \in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(\mathfrak{D}/\mathfrak{M}, k)$ and let $c^0 \in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(T_w^1, k)$. With notation as at the beginning of this subsection and as in Remark 4.4, the following formulas hold.*

(i) *If $v \in \widetilde{W}$ is such that $\ell(v) \geq 1$ and $\ell(s_0 wv) = 1 + \ell(w) + \ell(v)$, one has*

$$(c^-, c^0, c^+)_w \cdot \tau_v = (0, c^0(\text{pr}(-)), c^+)_{wv},$$

where $\text{pr}: T_{wv}^1 \rightarrow T_w^1$ is the quotient map.

(ii) *If $\ell(s_0 w) = \ell(w) + 1$, one has*

$$\tau_{s_0} \cdot (c^-, c^0, c^+)_w = (0, c^0(w_0^{-1} \text{pr}(-)w_0), -c^-)_{s_0 w},$$

where $\text{pr}: T_{s_0 w}^1 \rightarrow T_w^1$ is the quotient map, and where w_0 is any element of $N \setminus T$.

(iii) *If $v \in \widetilde{W}$ is such that $\ell(v) \geq 1$ and $\ell(s_1 wv) = 1 + \ell(w) + \ell(v)$, one has*

$$(c^-, c^0, c^+)_w \cdot \tau_v = (c^-, c^0(\text{pr}(-)), 0)_{wv},$$

where $\text{pr}: T_{wv}^1 \rightarrow T_w^1$ is the quotient map.

(iv) *If $\ell(s_1 w) = \ell(w) + 1$, one has*

$$\tau_{s_1} \cdot (c^-, c^0, c^+)_w = (-c^+, c^0(w_0^{-1} \text{pr}(-)w_0), 0)_{s_1 w},$$

where $\text{pr}: T_{s_1 w}^1 \rightarrow T_w^1$ is the quotient map, and where w_0 is any element of $N \setminus T$.

Proof. We prove the four statements using the description of the first cohomology of finitely generated pro- p groups as

$$H^1(-, k) \cong \text{Hom}_{\text{Vect}(\mathbb{F}_p)}((-)_{\Phi}, k).$$

and the description of the relevant Frattini quotients given in Lemma 4.3.

(i) Let us assume that $\ell(v) \geq 1$ and $\ell(s_0 wv) = 1 + \ell(w) + \ell(v)$ (in particular, it follows that $\ell(wv) = \ell(w) + \ell(v)$, that $\ell(s_0 wv) = \ell(wv) + 1$ and that $\ell(s_0 w) = \ell(w) + 1$) and let us prove the first formula.

We want to compute $\beta \cdot \tau_v$ where $\beta := (c^-, c^0, c^+)_w$. Since lengths add up, we can apply the formula (12), obtaining

$$\beta \cdot \tau_v \in H^1(I, \mathbf{X}(wv)) \quad \text{and} \quad \text{Sh}_{wv}(\alpha \cdot \tau_v) = \text{res}_{I_{wv}}^{I_w} (\text{Sh}_w(\beta)).$$

Therefore, we have to compute the action of the restriction on cohomology, which corresponds to computing the map induced by the inclusion on the Frattini quotients. Such action can be computed via the following commutative diagram (where we use the description of the Frattini quotients given in Lemma 4.3: note that the conditions $\ell(s_0 w v) = \ell(w v) + 1$ and $\ell(s_0 w) = \ell(w) + 1$ tell us which of the descriptions in Lemma 4.3 we have to consider; also note that the condition $\ell(v) \geq 1$ is used to say that $(\bar{c}, 0, 0)$ is mapped to zero by the map on the left):

$$\begin{array}{ccc}
\mathfrak{O}/\mathfrak{M} \times T_{wv}^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi^{\ell(wv)+1} c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}} & (I_{wv})_{\Phi} \\
\begin{array}{c} (\bar{c}, \bar{t}, \bar{b}) \\ \downarrow \\ (0, \bar{t}, \bar{b}) \end{array} & & \begin{array}{c} \text{ind. by} \\ I_{wv} \hookrightarrow I_w \end{array} \downarrow \\
\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi^{\ell(w)+1} c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}} & (I_w)_{\Phi}.
\end{array}$$

Dualizing (i.e., applying $\text{Hom}_{\text{Vect}(\mathbb{F}_p)}((-)_{\Phi}, k)$), we get the formula in the statement.

- (ii) Now, let us assume that $\ell(s_0 w) = \ell(w) + 1$ and let us prove the second formula.

We first remark that since lengths add up we can apply the formula (12), obtaining

$$\begin{aligned}
\tau_{s_0} \cdot \beta &\in H^i(I, \mathbf{X}(wv)), \\
\text{Sh}_{s_0 w}(\tau_{s_0} \cdot \beta) &= \text{res}_{I_{s_0 w}}^{s_0 I_w s_0^{-1}} ((s_0)_* \text{Sh}_w(\beta)),
\end{aligned}$$

where $\beta := (c^-, c^0, c^+)_w$.

This time we have to compute the action of the inclusion map and of conjugation on the level of the Frattini quotients. We do this via the following commutative diagram (which uses again the description of the Frattini quotients given in Lemma 4.3: note that the description of $(s_0 I_w s_0^{-1})_{\Phi}$ follows from the description of $(I_w)_{\Phi}$):

$$\begin{array}{ccc}
\mathfrak{O}/\mathfrak{M} \times T_{s_0 w}^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & \pi^{\ell(s_0 w)} b \\ 0 & 1 \end{pmatrix}} & (I_{s_0 w})_{\Phi} \\
\begin{array}{c} (\bar{c}, \bar{t}, \bar{b}) \\ \downarrow \\ (0, \bar{t}, \bar{b}) \end{array} & & \begin{array}{c} \text{ind. by} \\ I_{s_0 w} \hookrightarrow s_0 I_w s_0^{-1} \end{array} \downarrow \\
\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & \pi^{\ell(w)+1} b \\ 0 & 1 \end{pmatrix}} & (s_0 I_w s_0^{-1})_{\Phi} \\
\begin{array}{c} (\bar{c}, \bar{t}, \bar{b}) \\ \downarrow \\ (-\bar{b}, w_0^{-1} t w_0, -\bar{c}) \end{array} & & \begin{array}{c} \varphi_{\alpha_0} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \cdot - \cdot \varphi_{\alpha_0} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{array} \downarrow \\
\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi^{\ell(w)+1} c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}} & (I_w)_{\Phi}.
\end{array}$$

Dualizing, we get the formula in the statement.

(iii) The proof is analogous to (i). The commutative diagram in this case is

$$\begin{array}{ccc}
\mathfrak{O}/\mathfrak{M} \times T_{wv}^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & \pi^{\ell(wv)} b \\ 0 & 1 \end{pmatrix}} & (I_{wv})_{\Phi} \\
\downarrow \scriptstyle (\bar{c}, \bar{t}, \bar{b}) \mapsto (\bar{c}, \bar{t}, 0) & & \downarrow \scriptstyle \text{ind. by } I_{wv} \hookrightarrow I_w \\
\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & \pi^{\ell(w)} b \\ 0 & 1 \end{pmatrix}} & (I_w)_{\Phi}.
\end{array}$$

(iv) The proof is analogous to (i). The commutative diagram in this case is

$$\begin{array}{ccc}
\mathfrak{O}/\mathfrak{M} \times T_{s_1 w}^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi^{\ell(s_1 w)+1} c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}} & (I_{s_1 w})_{\Phi} \\
\downarrow \scriptstyle (\bar{c}, \bar{t}, \bar{b}) \mapsto (\bar{c}, \bar{t}, 0) & & \downarrow \scriptstyle \text{ind. by } I_{s_1 w} \hookrightarrow s_1 I_w s_1^{-1} \\
\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi^{\ell(w)+2} c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & \pi^{-1} b \\ 0 & 1 \end{pmatrix}} & (s_1 I_w s_1^{-1})_{\Phi} \\
\downarrow \scriptstyle (\bar{c}, \bar{t}, \bar{b}) \mapsto (-\bar{b}, \overline{w_0^{-1} t w_0}, -\bar{c}) & & \downarrow \scriptstyle \varphi_{\alpha_0} \begin{pmatrix} 0 & -\pi^{-1} \\ \pi & 0 \end{pmatrix}^{-1} \cdot \varphi_{\alpha_0} \begin{pmatrix} 0 & -\pi^{-1} \\ \pi & 0 \end{pmatrix} \\
\mathfrak{O}/\mathfrak{M} \times T_w^1 \times \mathfrak{O}/\mathfrak{M} & \xrightarrow{(\bar{c}, \bar{t}, \bar{b}) \mapsto \varphi_{\alpha_0} \begin{pmatrix} 1 & 0 \\ \pi c & 1 \end{pmatrix} \cdot t \cdot \varphi_{\alpha_0} \begin{pmatrix} 1 & \pi^{\ell(w)} b \\ 0 & 1 \end{pmatrix}} & (I_w)_{\Phi}.
\end{array}$$

□

Proposition 4.8. *Assume that $p \neq 2, 3$, that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ and that $\mathbf{G}$ has semisimple rank 1. Let us denote by f the residue degree of $\mathfrak{F}$ over $\mathbb{Q}_p$. Let us consider the tensor algebra $T_{E^0}^* E^1$ associated with the E^0 -bimodule E^1 and the natural multiplication map $T_{E^0}^* E^1 \rightarrow E^*$. One has that*

$$\text{Image}(T_{E^0}^* E^1 \rightarrow E^*) \supseteq \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \geq f \cdot \dim \mathbf{T}}} H^*(I, \mathbf{X}(w)).$$

Proof. We first note that $f \cdot \dim \mathbf{T} = \dim_{\mathbb{F}_p} T^1 / (T^1)^p$. Indeed, we have

$$T^1 / (T^1)^p \cong (1 + \mathfrak{M} / (1 + \mathfrak{M})^p)^{\oplus \dim \mathbf{T}} \cong (\mathfrak{M} / p\mathfrak{M})^{\oplus \dim \mathbf{T}} \cong (\mathfrak{O} / \mathfrak{M})^{\oplus \dim \mathbf{T}},$$

where in the second step we have used the p -adic logarithm/exponential (which we may apply since $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ and $p \neq 2$) and in the third step we have further used that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. The claimed formula $f \cdot \dim \mathbf{T} = \dim_{\mathbb{F}_p} T^1 / (T^1)^p$ now follows.

Now, for the moment let us consider $a, b, c \in \mathbb{Z}_{\geq 0}$ and arbitrary elements

$$\begin{aligned}
\mathbf{a}_1, \dots, \mathbf{a}_a &\in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(\mathfrak{O} / \mathfrak{M}, k), \\
\mathbf{b}_1, \dots, \mathbf{b}_b &\in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(T^1 / (T^1)^p, k), \\
\mathbf{c}_1, \dots, \mathbf{c}_c &\in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(\mathfrak{O} / \mathfrak{M}, k).
\end{aligned}$$

In the next computations it will be handy to work with the following notation: for all $n \in \mathbb{Z}_{\geq 0}$ we define $s_{\overline{n}}$ to be s_0 if n is even and s_1 if n is odd.

Let $m \in \mathbb{Z}_{\geq 0}$ be an odd number with $m \geq b-1$. With the notation of Remark 4.4, we make the following computation, whose steps will be explained below.

$$\begin{aligned}
& \prod_{i=1}^a (\mathbf{a}_i, 0, 0)_1 \cdot \prod_{i=1}^b (0, \mathbf{b}_i, 0)_{s_{i-1}} \cdot \tau_{s_{\overline{b}} \cdots s_{\overline{m}}} \cdot \prod_{i=1}^c (0, 0, \mathbf{c}_i)_1 \\
&= \bigcup_{i=1}^a ((\mathbf{a}_i, 0, 0)_1 \cdot \tau_{s_{\overline{0}} \cdots s_{\overline{m}}}) \cup \bigcup_{i=1}^b (\tau_{s_{\overline{0}} \cdots s_{i-2}} \cdot (0, \mathbf{b}_i, 0)_{s_{i-1}} \cdot \tau_{s_i \cdots s_{\overline{m}}}) \\
&\quad \cup \tau_{s_{\overline{0}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^c (\tau_{s_{\overline{0}} \cdots s_{\overline{m}}} \cdot (0, 0, \mathbf{c}_i)_1) \\
&= \bigcup_{i=1}^a (\mathbf{a}_i, 0, 0)_{s_{\overline{0}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^b (0, \mathbf{b}_i (w_0^{-(i-1)} - w_0^{i-1}), 0)_{s_{\overline{0}} \cdots s_{\overline{m}}} \\
&\quad \cup \bigcup_{i=1}^c (0, 0, \mathbf{c}_i)_{s_{\overline{0}} \cdots s_{\overline{m}}}.
\end{aligned} \tag{28}$$

Here, $s_{\overline{0}} \cdots s_{\overline{m}}$ means the empty product in the case $m = b-1$. To prove the first equality it suffices to apply the formula of Remark 4.6. Also note that cup product by $\tau_{s_{\overline{0}} \cdots s_{\overline{m}}}$ is the identity on $H^*(I, \mathbf{X}(s_{\overline{0}} \cdots s_{\overline{m}}))$, and so it can be ignored. Regarding the second equality, the fact that $(\mathbf{a}_i, 0, 0)_1 \cdot \tau_{s_{\overline{0}} \cdots s_{\overline{m}}} = (\mathbf{a}_i, 0, 0)_{s_{\overline{0}} \cdots s_{\overline{m}}}$ follows from Lemma 4.7 part (iii); the fact that

$$\tau_{s_{\overline{0}} \cdots s_{i-2}} \cdot (0, \mathbf{b}_i, 0)_{s_{i-1}} \cdot \tau_{s_i \cdots s_{\overline{m}}} = (0, \mathbf{b}_i (w_0^{-(i-1)} - w_0^{i-1}), 0)_{s_{\overline{0}} \cdots s_{\overline{m}}}$$

follows from Lemma 4.7 (applying iteratively parts (ii) and (iv) to compute the action of the left multiplication by $\tau_{s_{\overline{0}} \cdots s_{i-2}}$ and applying a single time parts (i) or (iii), depending on the parity of i , to compute the action of the right multiplication by $\tau_{s_i \cdots s_{\overline{m}}}$. Finally, the fact that $\tau_{s_{\overline{0}} \cdots s_{\overline{m}}} \cdot (0, 0, \mathbf{c}_i)_1 = (0, 0, \mathbf{c}_i)_{s_{\overline{0}} \cdots s_{\overline{m}}}$ follows from Lemma 4.7 (applying iteratively parts (ii) and (iv)): here is the only point where we use that m is odd.

We have thus checked the computation (28). Before deducing some consequences, let us make some completely similar computations.

Let $m \in \mathbb{Z}_{\geq 0}$ be an even number with $m \geq b-1$. The following computation is exactly as (28) except that the factors on the right are different because now m is even (recall that in (28) we have used that m was odd only in the very final step).

$$\begin{aligned}
& \prod_{i=1}^a (\mathbf{a}_i, 0, 0)_1 \cdot \prod_{i=1}^b (0, \mathbf{b}_i, 0)_{s_{i-1}} \cdot \tau_{s_{\overline{b}} \cdots s_{\overline{m}}} \cdot \prod_{i=1}^c (\mathbf{c}_i, 0, 0)_1 \\
&= \bigcup_{i=1}^a (\mathbf{a}_i, 0, 0)_{s_{\overline{0}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^b (0, \mathbf{b}_i (w_0^{-(i-1)} - w_0^{i-1}), 0)_{s_{\overline{0}} \cdots s_{\overline{m}}} \\
&\quad \cup \bigcup_{i=1}^c (0, 0, -\mathbf{c}_i)_{s_{\overline{0}} \cdots s_{\overline{m}}}.
\end{aligned} \tag{29}$$

Now, let $m \in \mathbb{Z}_{\geq 1}$ be an odd number with $m \geq b$. We make the following computation

$$\begin{aligned}
& \prod_{i=1}^a (0, 0, \mathbf{a}_i)_1 \cdot \prod_{i=1}^b (0, \mathbf{b}_i, 0)_{s_{\mathbf{T}} \cdot \tau_{s_{b+1} \cdots s_{\overline{m}}}} \cdot \prod_{i=1}^c (0, 0, \mathbf{c}_i)_1 \\
&= \bigcup_{i=1}^a ((0, 0, \mathbf{a}_i)_1 \cdot \tau_{s_{\mathbf{T}} \cdots s_{\overline{m}}}) \cup \bigcup_{i=1}^b (\tau_{s_{\mathbf{T}} \cdots s_{i-1}} \cdot (0, \mathbf{b}_i, 0)_{s_{\mathbf{T}} \cdot \tau_{s_{i+1} \cdots s_{\overline{m}}}}) \\
&\quad \cup \tau_{s_{\mathbf{T}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^c (\tau_{s_{\mathbf{T}} \cdots s_{\overline{m}}} \cdot (0, 0, \mathbf{c}_i)_1) \\
&= \bigcup_{i=1}^a (0, 0, \mathbf{a}_i)_{s_{\mathbf{T}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^b (0, \mathbf{b}_i (w_0^{-(i-1)} - w_0^{i-1}), 0)_{s_{\mathbf{T}} \cdots s_{\overline{m}}} \\
&\quad \cup \bigcup_{i=1}^c (-\mathbf{c}_i, 0, 0)_{s_{\mathbf{T}} \cdots s_{\overline{m}}}.
\end{aligned} \tag{30}$$

Now, let $m \in \mathbb{Z}_{\geq 1}$ be an even number with $m \geq b$. We make the following computation

$$\begin{aligned}
& \prod_{i=1}^a (0, 0, \mathbf{a}_i)_1 \cdot \prod_{i=1}^b (0, \mathbf{b}_i, 0)_{s_{\mathbf{T}} \cdot \tau_{s_{b+1} \cdots s_{\overline{m}}}} \cdot \prod_{i=1}^c (\mathbf{c}_i, 0, 0)_1 \\
&= \bigcup_{i=1}^a (0, 0, \mathbf{a}_i)_{s_{\mathbf{T}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^b (0, \mathbf{b}_i (w_0^{-(i-1)} - w_0^{i-1}), 0)_{s_{\mathbf{T}} \cdots s_{\overline{m}}} \\
&\quad \cup \bigcup_{i=1}^c (\mathbf{c}_i, 0, 0)_{s_{\mathbf{T}} \cdots s_{\overline{m}}}.
\end{aligned} \tag{31}$$

Now let us go back to (28) and let us draw some consequences from it. Recall that all of a, b, c and all of $\mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i$ were arbitrary, and $m \in \mathbb{Z}_{\geq 0}$ was an odd integer with $m \geq b - 1$.

Let $m \in \mathbb{Z}_{\geq 0}$ be an arbitrary odd natural number. Recall that (since $m + 1 \geq 1$) the pro- p group $I_{s_{\overline{0}} \cdots s_{\overline{m}}}$ is uniform (Lemma 4.5). Therefore, the cup product algebra on $H^*(I, \mathbf{X}(s_{\overline{0}} \cdots s_{\overline{m}})) \cong H^*(I_{s_{\overline{0}} \cdots s_{\overline{m}}}, k)$ is the exterior algebra on H^1 , as recalled in §2.8. The computation (28) tells us that the elements of the following form lie in the image of the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$:

$$\bigcup_{i=1}^a (\mathbf{a}_i, 0, 0)_{s_{\overline{0}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^b (0, \mathbf{b}'_i, 0)_{s_{\overline{0}} \cdots s_{\overline{m}}} \cup \bigcup_{i=1}^c (0, 0, \mathbf{c}_i)_{s_{\overline{0}} \cdots s_{\overline{m}}}, \tag{32}$$

for $a, c \in \mathbb{Z}_{\geq 0}$, for $b \in \mathbb{Z}_{\geq 0}$ with $b \leq m + 1$, for $\mathbf{a}_i, \mathbf{c}_i \in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(\mathfrak{D}/\mathfrak{M}, k)$ and for $\mathbf{b}'_i \in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(T^1/(T^1)^p, k)$. Now let $m \geq f \cdot \dim \mathbf{T} - 1$: in this way, since $T^1/(T^1)^p$ has dimension $f \cdot \dim \mathbf{T}$ as an $\mathbb{F}_p$ -vector space, a k -basis of $\text{Hom}_{\text{Vect}(\mathbb{F}_p)}(T^1/(T^1)^p, k)$ has cardinality less or equal than $m + 1$. Then the elements of the form (32) (with $b \leq m + 1$) span the cup product algebra/exterior algebra $H^*(I, \mathbf{X}(s_{\overline{0}} \cdots s_{\overline{m}}))$.

All in all, this shows that the image of the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$ contains $H^*(I, \mathbf{X}(s_{\overline{0}} \cdots s_{\overline{m}}))$ for $m \in \mathbb{Z}_{\geq 0}$ odd with $m \geq f \cdot \dim \mathbf{T} - 1$. Reasoning

exactly in the same way for the other computations we made, we obtain that the image of the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$ contains the following vector spaces:

$$\begin{aligned} H^*(I, \mathbf{X}(s_{\overline{0}} \cdots s_{\overline{m}})) & \quad \text{for } m \in \mathbb{Z}_{\geq 0} \text{ odd with } m \geq f \cdot \dim \mathbf{T} - 1, \\ H^*(I, \mathbf{X}(s_{\overline{0}} \cdots s_{\overline{m}})) & \quad \text{for } m \in \mathbb{Z}_{\geq 0} \text{ even with } m \geq f \cdot \dim \mathbf{T} - 1, \\ H^*(I, \mathbf{X}(s_{\overline{1}} \cdots s_{\overline{m}})) & \quad \text{for } m \in \mathbb{Z}_{\geq 1} \text{ odd with } m \geq f \cdot \dim \mathbf{T}, \\ H^*(I, \mathbf{X}(s_{\overline{1}} \cdots s_{\overline{m}})) & \quad \text{for } m \in \mathbb{Z}_{\geq 1} \text{ even with } m \geq f \cdot \dim \mathbf{T}. \end{aligned}$$

By the discussion at the beginning of this subsection, every element of $\widetilde{W}$ of length greater or equal than $f \cdot \dim \mathbf{T}$ can be represented as a product ωw , where $\omega \in \widetilde{\Omega}$ (i.e., ω has length zero) and w is of the form $s_{\overline{0}} \cdots s_{\overline{m}}$ or $s_{\overline{1}} \cdots s_{\overline{m}}$ as above.

With this notation, we thus know that the image of the multiplication map $T_{E^0}^* E^1 \rightarrow E^*$ contains $H^*(I, \mathbf{X}(w))$, and to show that it also contains $H^*(I, \mathbf{X}(\omega w))$ it suffices to recall that, since ω has length zero, the formula (12) implies that multiplication on the left by τ_ω induces an isomorphism between $H^*(I, \mathbf{X}(w))$ and $H^*(I, \mathbf{X}(\omega w))$. $\square$

Remark 4.9. Assume that $p \neq 2, 3$, that $\mathbf{G}$ is SL_2 or PGL_2 and that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has that the image of the natural multiplication map $T_{E^0}^* E^1 \rightarrow E^*$ has finite codimension in E^* .

Proof. For all $w \in \widetilde{W}$ the k -vector space $H^*(I, \mathbf{X}(w)) \cong H^*(I_w, k)$ is finite-dimensional since I_w is a Poincaré group (Lemma 4.5). If one shows that, since $\mathbf{G}$ is semisimple, there are only finitely many elements of $\widetilde{W}$ of any given length, then by Proposition 4.8 we conclude.

It suffices to show the claim for W in place of $\widetilde{W}$ by the definition of length and since W is a quotient of $\widetilde{W}$ of finite index. Recall from §2.3 that the length ℓ is constant on double cosets $(\Omega w \Omega)_{w \in W_{\mathrm{aff}}}$. Therefore, it suffices to show that Ω is finite. But Ω is isomorphic to $X_*(\mathbf{T}) / \mathrm{span}_{\mathbb{Z}} \Phi^\vee$ (see [Lus89, §1.5], with the difference that in the construction of W in loc.cit. roots are swapped with coroots and characters with cocaracters with respect to our conventions). Since $\mathbf{G}$ is semisimple, $X_*(\mathbf{T}) / \mathrm{span}_{\mathbb{Z}} \Phi^\vee$ is indeed finite (and isomorphic to the fundamental group). $\square$

5 The Ext-algebra E^* is finitely generated in some special cases

Putting together the results obtained in Proposition 3.5 and Proposition 4.8, we are able to show that, under the assumptions under which those results have been proven, the Ext-algebra E^* is finitely generated as a (non-commutative) k -algebra.

Theorem 5.1. *Assume that $p \neq 2, 3$, that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ and that $\mathbf{G}$ has semisimple rank 1. One has that E^* is finitely generated as a k -algebra.*

Proof. Proposition 4.8 shows that

$$\text{Image}(T_{E^0}^* E^1 \longrightarrow E^*) \supseteq \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \geq f \cdot \dim \mathbf{T}}} H^*(I, \mathbf{X}(w)).$$

Therefore E^* is generated as a k -algebra by E^0 , E^1 and

$$\bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) < f \cdot \dim \mathbf{T}}} H^*(I, \mathbf{X}(w)).$$

By (12), for all $w \in \widetilde{W}$ and all $\omega \in \widetilde{\Omega}$, multiplication on the left by τ_ω induces an isomorphism between $H^*(I, \mathbf{X}(w))$ and $H^*(I, \mathbf{X}(\omega w))$. Furthermore, E^1 is finitely generated as an E^0 -bimodule by Proposition 3.5 (in this setting a more explicit proof could also be provided starting from the formulas in Lemma 4.7).

This shows that E^* is generated as a k -algebra by E^0 , a finite subset of E^1 and

$$\bigoplus_{\substack{w \in \widetilde{W}_{\text{aff}} \\ \text{s.t. } \ell(w) < f \cdot \dim \mathbf{T}}} H^*(I, \mathbf{X}(w)).$$

The last set is finite-dimensional as a k -vector space because there are only finitely many elements of bounded length in $\widetilde{W}_{\text{aff}}$ (and so in $\widetilde{W}$) and because for all $w \in \widetilde{W}$ the k -vector space $H^*(I, \mathbf{X}(w)) \cong H^*(I_w, k)$ is finite-dimensional since I_w is a Poincaré group (Lemma 4.5).

Therefore, to show the thesis of the proposition it suffices to notice that E^0 is finitely generated as a k -algebra. This is clear from the fact that E^0 is a finitely generated module over its centre, which is a finitely generated (commutative) k -algebra (see [Vig14, Theorem 1.3]), but it can also be shown more directly from the braid relations, the fact that $\widetilde{\Omega}$ is a finitely generated group, and the fact that S_{aff} is finite. $\square$

6 The Ext-algebra E^* is finitely presented when $G = \text{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$

Assumptions. For the whole section we make the following assumptions. We consider $\mathfrak{F} := \mathbb{Q}_p$ and $G := \text{SL}_2(\mathbb{Q}_p)$, and we assume that $p \neq 2, 3$. Furthermore, we fix the uniformizer π to be p . We consider the $(\mathbb{Q}_p$ -split maximal) torus $\mathbf{T}$ of diagonal matrices, and we fix the following pro- p Iwahori subgroup I :

$$I = \begin{pmatrix} 1 + p\mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & 1 + p\mathbb{Z}_p \end{pmatrix} \cap \text{SL}_2(\mathbb{Q}_p). \quad (33)$$

(the corresponding choices of the positive root and the Chevalley system will be made explicit in §6.1).

6.1 The Ext-algebra in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$: notation and recollection of and results

Under the current assumptions, the Ext-algebra E^* has been studied extensively in [OS22]. We need to recall quite a few facts from loc. cit. and from [OS19].

First of all, it follows from [OS19, §7.2] that E^* is supported in the following degrees:

$$E^* = E^0 \oplus E^1 \oplus E^2 \oplus E^3.$$

With reference to §2.2, we have a Chevalley system such that, denoting the positive root by α_0 , the map φ_{α_0} is the identity of SL_2 and $\varphi_{-\alpha_0}$ is the inverse transpose. With reference to §2.3, in this setting the group Ω is trivial. Following [OS22, §2.3.1], we define

$$s_0 := \overline{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}, \quad s_1 := \overline{\begin{pmatrix} 0 & -\pi^{-1} \\ \pi & 0 \end{pmatrix}}, \quad (34)$$

where $\bar{?}$ denotes the image of $?$ in $\widetilde{W}$. This is “almost” compatible with the definition we gave in (26), the only difference being that the two definitions of s_1 differ by multiplication by the central element $\overline{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}$. However, this will not cause any problems. For example, in [OS19, Proposition 7.1] some general formulas are stated only for the specific choices (26) (see the comment at the end of the statement), but the only difference being multiplication by a central element, the formulas remain valid for the lifts (34). We make the choice (34) to preserve compatibility of notation with [OS22, §2.3.1].

We also define

$$c_{-1} := \overline{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}} = s_0^2 = s_1^2. \quad (35)$$

Since the group Ω is trivial, every element of $\widetilde{W}$ can be represented in a unique way as a product of an element of T^0/T^1 and a string of the elements s_0 and s_1 , with no two identical letters one after the other (compare the beginning of §4). In other words, the following is a basis of E^0 :

τ_ω	for $\omega \in T^0/T^1$,
$\tau_{\omega s_0 (s_1 s_0)^i}$	for $\omega \in T^0/T^1$ and $i \in \mathbb{Z}_{\geq 0}$,
$\tau_{\omega s_1 (s_0 s_1)^i}$	for $\omega \in T^0/T^1$ and $i \in \mathbb{Z}_{\geq 0}$,
$\tau_{\omega (s_0 s_1)^i}$	for $\omega \in T^0/T^1$ and $i \in \mathbb{Z}_{\geq 1}$,
$\tau_{\omega (s_1 s_0)^i}$	for $\omega \in T^0/T^1$ and $i \in \mathbb{Z}_{\geq 1}$.

As in [OS22, Equation (31)], we parametrize the group $T^0/T^1 \cong \mathbb{F}_p^\times$ as follows: for all $u \in \mathbb{F}_p^\times$ we define

$$\omega_u := \overline{\begin{pmatrix} [u]^{-1} & 0 \\ 0 & [u] \end{pmatrix}}, \quad (36)$$

where $[?]$ denotes the Teichmüller lift of $?$ and $\overline{?}$ denotes the class of $?$ in T^0/T^1 .

In [OS19, §6], it is shown that the map $\mathcal{J}_w$ defined by the commutativity of the diagram

$$\begin{array}{ccc} H^*(I, \mathbf{X}(w)) & \xrightarrow[\cong]{\mathcal{J}_w} & H^*(I, \mathbf{X}(w^{-1})) \\ \text{Sh}_w \downarrow \cong & & \cong \downarrow \text{Sh}_{w^{-1}} \\ H^*(I_w, k) & \xrightarrow[\cong]{(w^{-1})_*} & H^*(I_{w^{-1}}, k). \end{array} \quad (37)$$

gives rise to a map $\mathcal{J} := \bigoplus_{w \in \widetilde{W}} \mathcal{J}_w : E^* \longrightarrow E^*$ that is an involutive anti-automorphism of E^* (anti-automorphism meaning that it is an automorphism of k -vector spaces and that it satisfies the equation $\mathcal{J}(\alpha \cdot \beta) = (-1)^{|\alpha| \cdot |\beta|} \mathcal{J}(\beta) \cdot \mathcal{J}(\alpha)$ for all homogeneous $\alpha \in E^{|\alpha|}$ and $\beta \in E^{|\beta|}$).

In [OS22, §2.2.6] a certain involutive automorphism Γ_ϖ of E^* is constructed as follows. One defines $\varpi := \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \in \text{GL}_2(\mathbb{Q}_p)$ and one considers the map $\Gamma_{\varpi, w}$ defined by the commutativity of the diagram

$$\begin{array}{ccc} H^*(I, \mathbf{X}(w)) & \xrightarrow{\Gamma_{\varpi, w}} & H^*(I, \mathbf{X}(\varpi w \varpi^{-1})) \\ \text{Sh}_w \downarrow \cong & & \cong \downarrow \text{Sh}_{\varpi w \varpi^{-1}} \\ H^*(I_w, k) & \xrightarrow{\varpi_*} & H^*(I_{\varpi w \varpi^{-1}}, k). \end{array}$$

Defining $\Gamma_\varpi := \bigoplus_{w \in \widetilde{W}} \Gamma_{\varpi, w} : E^* \longrightarrow E^*$, one has that Γ_ϖ is an involutive automorphism of E^* (as a graded k -algebra). Moreover, the involutions Γ_ϖ and $\mathcal{J}$ commute (see again [OS22, §2.2.6]):

$$\Gamma_\varpi \circ \mathcal{J} = \mathcal{J} \circ \Gamma_\varpi. \quad (38)$$

The Poincaré duality of §2.8 for the groups I_w implies that there is a duality between $H^i(I, \mathbf{X}(w))$ and $H^{3-i}(I, \mathbf{X}(w))$ for all $i \in \{0, 1, 2, 3\}$ and all $w \in \widetilde{W}$. In [OS19, Proposition 7.18], such duality is extended to a suitably defined “duality” of E^0 -bimodules involving E^i and E^{3-i} . We recall a few details. One fixes (and we will make a specific choice later) an isomorphism of 1-dimensional vector spaces

$$\eta : H^3(I, k) \longrightarrow k \quad (39)$$

as well as the G -equivariant map

$$\begin{array}{ccc} \mathcal{S} : k[G/I] & \longrightarrow & k \\ f & \longmapsto & \sum_{\overline{g} \in G/I} f(g) \end{array} \quad (40)$$

and its induced map

$$\mathcal{S}^i := H^i(I, \mathcal{S}) : E^i = H^i(I, k[G/I]) \longrightarrow H^i(I, k).$$

Furthermore, one defines the *finite twisted dual* ${}^{\mathcal{J}}((E^i)^{\vee, \text{finite}})^{\mathcal{J}}$ of E^i as follows: as a k -vector space it is defined as

$$\bigoplus_{w \in \widetilde{W}} H^i(I, \mathbf{X}(w))^{\vee} \subseteq (E^i)^{\vee},$$

where $(-)^\vee := \text{Hom}_{\text{Vect}(k)}(-, k)$. One may check that this vector space is actually a sub- E^0 -bimodule of the full dual $(E^i)^\vee$, but we endow ${}^{\mathcal{J}}((E^i)^{\vee, \text{finite}})^{\mathcal{J}}$ with the following “twisted” action instead:

$$h \cdot \varphi := \varphi(\mathcal{J}(h) \cdot -), \quad \varphi \cdot h := \varphi(- \cdot \mathcal{J}(h))$$

for all $h \in E^0$ and all $\varphi \in {}^{\mathcal{J}}((E^i)^{\vee, \text{finite}})^{\mathcal{J}}$, thus justifying the complicated notation. Having introduced these notations, we can recall the statement of the above-mentioned duality theorem; namely, the map

$$\begin{aligned} \Delta^i: E^i &\longrightarrow {}^{\mathcal{J}}((E^{3-i})^{\vee, \text{finite}})^{\mathcal{J}} \\ \alpha &\longmapsto \left(\beta \mapsto (\eta \circ S^d)(\alpha \smile \beta) \right) \end{aligned}$$

is a well-defined isomorphism of E^0 -bimodules. The link with Poincaré duality of the groups I_w is as follows: The Poincaré duality of §2.8 defines an isomorphism of k -vector spaces

$$\begin{aligned} \Delta_w^i: H^i(I_w, k) &\longrightarrow (H^{3-i}(I_w, k))^{\vee} \\ \alpha &\longmapsto (\beta \mapsto \eta_w(\alpha \smile \beta)), \end{aligned} \tag{41}$$

once one fixes an isomorphism of 1-dimensional k -vector spaces

$$\eta_w: H^3(I_w, k) \longrightarrow k$$

and we make the choice $\eta_w := \eta \circ \text{cores}_I^{I_w}$ (recalling from [Ser02, Chapter 1, Proposition 30 (4)] that the corestriction is an isomorphism on the top graded piece). With these choices the following diagram of solid arrows commutes (see [OS19, Diagram in the proof of Lemma 7.5]):

$$\begin{array}{ccc} H^i(I_w, k) & \xrightarrow{\Delta_w^i} & H^{3-i}(I_w, k)^{\vee} \\ \cong \downarrow \text{Sh}_w & & \text{Sh}_w^{\vee} \uparrow \cong \\ H^i(I, \mathbf{X}(w)) & \dashrightarrow & H^{3-i}(I, \mathbf{X}(w))^{\vee} \\ \downarrow & & \downarrow \\ E^i & \xrightarrow{\Delta^i} & {}^{\mathcal{J}}((E^{3-i})^{\vee, \text{finite}})^{\mathcal{J}} \end{array} \tag{42}$$

One can thus define a dashed map making the whole diagram commute either as the unique map making the upper square commute or as the restriction of Δ^i .

Following [OS22, §4.2.3], we want to fix k -bases for the graded pieces of E^* “in a compatible way”. Denoting $(-)^{\vee} := \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(-, k)$ let us recall from (27) that for all $w \in \widetilde{W}$ we have fixed a specific isomorphism

$$(-, -, -)_w : (\mathbb{F}_p)^{\vee} \oplus (T_w^1)^{\vee} \oplus \mathbb{F}_p^{\vee} \longrightarrow H^1(I, \mathbf{X}(w)). \quad (43)$$

Using the p -adic logarithm and exponential, one sees that $(1 + \mathfrak{M})^p = 1 + \mathfrak{M}^2$, and therefore

$$\begin{aligned} T_w^1 &\cong (1 + \mathfrak{M}) / ((1 + \mathfrak{M}^{\ell(w)+1}) \cdot (1 + \mathfrak{M})^p) \\ &\cong \begin{cases} \mathbb{F}_p & \text{if } \ell(w) \geq 1, \\ 0 & \text{if } \ell(w) = 0. \end{cases} \end{aligned}$$

Henceforth, in the case that $\ell(w) \geq 1$ we fix the following isomorphism, induced by the p -adic logarithm:

$$\begin{aligned} \iota : T_w^1 &\cong (1 + \mathfrak{M}) / (1 + \mathfrak{M}^2) \longrightarrow \mathfrak{O} / \mathfrak{M} = \mathbb{F}_p \\ \overline{1 + px} &\longmapsto \overline{x}. \end{aligned} \quad (44)$$

Dualizing the isomorphism (43) we obtain an isomorphism

$$H^1(I, \mathbf{X}(w))^{\vee} \xrightarrow{\cong} \mathbb{F}_p \oplus T_w^1 \oplus \mathbb{F}_p$$

We combine the inverse of this isomorphism with the inverse of the isomorphism $H^2(I, \mathbf{X}(w)) \longrightarrow H^1(I, \mathbf{X}(w))^{\vee}$ defined in the diagram (42), obtaining a composite isomorphism

$$\mathbb{F}_p \oplus T_w^1 \oplus \mathbb{F}_p \xrightarrow{\cong} H^1(I, \mathbf{X}(w))^{\vee} \xrightarrow{\cong} H^2(I, \mathbf{X}(w)),$$

for which we will use the notation

$$(-, -, -)_w : \mathbb{F}_p \oplus T_w^1 \oplus \mathbb{F}_p \longrightarrow H^2(I, \mathbf{X}(w))$$

similarly to the isomorphism describing $H^1(I, \mathbf{X}(w))$.

Now, let us fix an element $\mathbf{c} \in \text{Hom}_{\text{Vect}(\mathbb{F}_p)}(\mathbb{F}_p, k)$ and an element $\alpha \in \mathbb{F}_p$ with the property that

$$\mathbf{c}(\alpha) = 1.$$

For all $w \in \widetilde{W}$ we define the following k -basis of $H^1(I, \mathbf{X}(w))$:

$$\begin{aligned} \beta_w^- &:= (\mathbf{c}, 0, 0)_w, \\ \beta_w^+ &:= (0, 0, \mathbf{c})_w, \\ \beta_w^0 &:= (0, \mathbf{c}\iota, 0)_w \quad \text{if } \ell(w) \geq 1, \end{aligned}$$

and for all $w \in \widetilde{W}$ we define the following k -basis of $H^2(I, \mathbf{X}(w))$:

$$\begin{aligned}\alpha_w^- &:= (\boldsymbol{\alpha}, 0, 0)_w, \\ \alpha_w^+ &:= (0, 0, \boldsymbol{\alpha})_w, \\ \alpha_w^0 &:= (0, \iota^{-1}(\boldsymbol{\alpha}), 0)_w \quad \text{if } \ell(w) \geq 1.\end{aligned}$$

Furthermore, we define the basis $(\phi_v)_{v \in \widetilde{W}}$ of E^3 as the dual basis of $(\tau_v)_{v \in \widetilde{W}}$ (dual with respect to the duality isomorphism (41) with $i = 3$), meaning that for all $w \in \widetilde{W}$ the element ϕ_w is characterized by the properties

$$\begin{aligned}(\eta \circ \mathcal{S}^d)(\phi_w \smile \tau_w) &= 1, \\ (\eta \circ \mathcal{S}^d)(\phi_w \smile \tau_v) &= 0 \quad \text{for all } v \in \widetilde{W} \setminus \{w\}.\end{aligned}$$

As anticipated above, we make a specific choice for $\eta: H^3(I, k) \rightarrow k$. In [OS22, Lemma 4.5], it is shown that there exists a (necessarily unique) choice of η such that the following property holds:

$$\beta_w^- \smile \beta_w^0 \smile \beta_w^+ = \phi_w \quad \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geq 1. \quad (45)$$

Henceforth, we will always work with this fixed choice of η .

It is possible to show that the following relations hold (see [OS22, Lemma 5.3]):

$$\begin{aligned}\alpha_w^0 &= \beta_w^+ \smile \beta_w^- & \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geq 1, \\ \alpha_w^- &= \beta_w^0 \smile \beta_w^+ & \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geq 1, \\ \alpha_w^+ &= \beta_w^- \smile \beta_w^0 & \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geq 1.\end{aligned} \quad (46)$$

We have thus fixed the following k -basis of $H^*(I, \mathbf{X}(w))$:

$$\begin{aligned}\tau_w, \\ \beta_w^-, \quad \beta_w^0 \quad (\text{if } \ell(w) \geq 1), \quad \beta_w^+, \\ \alpha_w^-, \quad \alpha_w^0 \quad (\text{if } \ell(w) \geq 1), \quad \alpha_w^+, \\ \phi_w.\end{aligned} \quad (47)$$

It is useful to introduce some idempotent elements of E^0 . We denote by $\widehat{T^0/T^1}$ the group of characters $T^0/T^1 \rightarrow k^\times$. To each $\lambda \in \widehat{T^0/T^1}$ we attach

$$e_\lambda := - \sum_{t \in T^0/T^1} \lambda(t)^{-1} \tau_t. \quad (48)$$

Using the braid relations and that $T^0/T^1 \cong \mathbb{F}_p^\times$, one sees that $(e_\lambda)_{\lambda \in \widehat{T^0/T^1}}$ is a system of orthogonal idempotents, that they form a basis of the subalgebra $\text{span}_k \{\tau_t \mid t \in T^0/T^1\} \cong k[T^0/T^1]$ of E^0 , and that the formula

$$e_\lambda \cdot \tau_t = \tau_t \cdot e_\lambda = \lambda(t) e_\lambda \quad (49)$$

holds for all $\lambda \in \widehat{T^0/T^1}$ and all $t \in T^0/T^1$ (compare [OS19, §2.2.1]). With this notation, e_1 denotes the idempotent associated with the trivial character. Furthermore, we define

$$\begin{aligned} \text{id}: T^0/T^1 &\longrightarrow k^\times \\ \omega_u &\longmapsto u, \end{aligned} \tag{50}$$

where the notation ω_u has been introduced in (36). We may thus write e_{id} for the corresponding idempotent. More generally, every idempotent of the form (48) can be written as e_{id^m} for some uniquely determined $m \in \{0, \dots, p-2\}$.

Using the basis (47), we will now recall the formulas for the multiplication on E^0 , for the left action of E^0 on E^* (and partially, also on the right) as well as the action of the anti-involution $\mathcal{J}$ and of the involutive automorphism Γ_ϖ .

- Braid and quadratic relations on E^0 (see [OS22, Equations (19) and (20)]):

One has:

$$\tau_v \cdot \tau_w = \tau_{vw} \quad \text{for } v, w \in \widetilde{W} \text{ such that } \ell(vw) = \ell(v) + \ell(w), \tag{51}$$

$$\tau_{s_i}^2 = -e_1 \cdot \tau_{s_i} = -\tau_{s_i} \cdot e_1, \quad \text{for } i \in \{0, 1\}. \tag{52}$$

- Action of the anti-involution $\mathcal{J}$ on E^0 (see [OS19, Proposition 6.1]):

For all $w \in \widetilde{W}$ one has:

$$\mathcal{J}(\tau_w) = \tau_{w^{-1}}. \tag{53}$$

- Action of the involutive automorphism Γ_ϖ on E^0 :

For all $w \in \widetilde{W}$ one has that

$$\Gamma_\varpi(\tau_w) = \tau_{\varpi w \varpi^{-1}}$$

(immediate from the definition of Γ_ϖ). With an explicit computation, this can be made explicit as follows:

$$\begin{aligned} \Gamma_\varpi(\tau_\omega) &= \tau_{\omega^{-1}} && \text{for all } \omega \in T^0/T^1, \\ \Gamma_\varpi(\tau_{s_0}) &= \tau_{s_1}, \\ \Gamma_\varpi(\tau_{s_1}) &= \tau_{s_0}. \end{aligned} \tag{54}$$

- Left and right action of τ_ω on E^1 for $\omega \in T^0/T^1$ (see [OS22, Equations (64) and (66)]):

Let $u \in \mathbb{F}_p^\times$ and let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about β_w^0). Recall the notation ω_u from (36). One has:

$$\begin{aligned} \tau_{\omega_u} \cdot \beta_w^- &= u^{-2} \beta_{\omega_u w}^-, \\ \tau_{\omega_u} \cdot \beta_w^0 &= \beta_{\omega_u w}^0, \\ \tau_{\omega_u} \cdot \beta_w^+ &= u^2 \beta_{\omega_u w}^+, \end{aligned} \tag{55}$$

and

$$\begin{aligned}\beta_w^- \cdot \tau_{\omega_u} &= \beta_{w\omega_u}^-, \\ \beta_w^0 \cdot \tau_{\omega_u} &= \beta_{w\omega_u}^0, \\ \beta_w^+ \cdot \tau_{\omega_u} &= \beta_{w\omega_u}^+.\end{aligned}\tag{56}$$

- Action of the idempotents on E^1 :

Let $\lambda \in \widehat{T^0/T^1}$ and let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about β_w^0). Recalling the notation (48) and (50), one has:

$$\begin{aligned}\beta_w^- \cdot e_\lambda &= e_{\lambda(-1)^{\ell(w)} \underline{\text{id}}^{-2}} \cdot \beta_w^-, \\ \beta_w^0 \cdot e_\lambda &= e_{\lambda(-1)^{\ell(w)}} \cdot \beta_w^0, \\ \beta_w^+ \cdot e_\lambda &= e_{\lambda(-1)^{\ell(w)} \underline{\text{id}}^2} \cdot \beta_w^+.\end{aligned}\tag{57}$$

These formulas can be easily computed from formulas (55) and (56), and they are also proven in [OS22, Equation (69)] (for $\lambda = \underline{\text{id}}^m$ for some $m \in \mathbb{Z}$, i.e., for every λ).

- Left action of τ_{s_0} and τ_{s_1} on E^1 when lengths add up:

Let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about β_w^0). One has:

$$\left. \begin{aligned}\tau_{s_0} \cdot \beta_w^- &= -\beta_{s_0 w}^+ \\ \tau_{s_0} \cdot \beta_w^0 &= -\beta_{s_0 w}^0 \\ \tau_{s_0} \cdot \beta_w^+ &= 0\end{aligned} \right\} \quad \text{if } \ell(s_0 w) = \ell(w) + 1,$$

$$\left. \begin{aligned}\tau_{s_1} \cdot \beta_w^- &= 0 \\ \tau_{s_1} \cdot \beta_w^0 &= -\beta_{s_1 w}^0 \\ \tau_{s_1} \cdot \beta_w^+ &= -\beta_{s_1 w}^-\end{aligned} \right\} \quad \text{if } \ell(s_1 w) = \ell(w) + 1.\tag{58}$$

These formulas are proved in [OS22, Proposition 4.9], and they also follow from Lemma 4.7 parts (ii) and (iv).

- Right action of τ_v on E^1 when lengths add up (for $v \in \widetilde{W}$):

Let $w, v \in \widetilde{W}$ such that $\ell(wv) = \ell(w) + \ell(v)$ and such that $\ell(v) \geq 1$ (and furthermore let us assume that $\ell(w) \geq 1$ when we speak about β_w^0). One has:

$$\left. \begin{aligned}\beta_w^- \cdot \tau_v &= \beta_{wv}^- \\ \beta_w^0 \cdot \tau_v &= \beta_{wv}^0 \\ \beta_w^+ \cdot \tau_v &= 0\end{aligned} \right\} \quad \text{if } \ell(s_1 wv) = \ell(wv) + 1,$$

$$\left. \begin{aligned}\beta_w^- \cdot \tau_v &= 0 \\ \beta_w^0 \cdot \tau_v &= \beta_{wv}^0 \\ \beta_w^+ \cdot \tau_v &= \beta_{wv}^+\end{aligned} \right\} \quad \text{if } \ell(s_0 wv) = \ell(wv) + 1.\tag{59}$$

These formulas are proved in [OS22, Lemma 4.12], and they also follow from Lemma 4.7 parts (i) and (iii).

- Left action of τ_{s_0} and τ_{s_1} on E^1 when lengths do not add up:

Let $w \in \widetilde{W}$ be such that $\ell(s_0 w) = \ell(w) - 1$. One has:

$$\begin{aligned}\tau_{s_0} \cdot \beta_w^- &= \begin{cases} -e_1 \beta_w^- - 2e_{\underline{\text{id}}} \beta_w^0 - \beta_{s_0 w}^+ & \text{if } \ell(w) \geq 2, \\ -e_1 \beta_w^- - 2e_{\underline{\text{id}}} \beta_w^0 + e_{\underline{\text{id}}^2} \beta_w^+ - \beta_{s_0 w}^+ & \text{if } \ell(w) = 1, \end{cases} \\ \tau_{s_0} \cdot \beta_w^0 &= \begin{cases} -e_1 \beta_w^0 & \text{if } \ell(w) \geq 2, \\ -e_1 \beta_w^0 + e_{\underline{\text{id}}} \beta_w^+ & \text{if } \ell(w) = 1, \end{cases} \\ \tau_{s_0} \cdot \beta_w^+ &= -e_1 \beta_w^+. \end{aligned} \tag{60}$$

Let $w \in \widetilde{W}$ be such that $\ell(s_1 w) = \ell(w) - 1$. One has:

$$\begin{aligned}\tau_{s_1} \cdot \beta_w^- &= -e_1 \beta_w^- \\ \tau_{s_1} \cdot \beta_w^0 &= \begin{cases} -e_1 \beta_w^0 & \text{if } \ell(w) \geq 2, \\ -e_1 \beta_w^0 - e_{\underline{\text{id}}^{-1}} \beta_w^- & \text{if } \ell(w) = 1, \end{cases} \\ \tau_{s_1} \cdot \beta_w^+ &= \begin{cases} -e_1 \beta_w^+ + 2e_{\underline{\text{id}}^{-1}} \beta_w^0 - \beta_{s_1 w}^- & \text{if } \ell(w) \geq 2, \\ -e_1 \beta_w^+ + 2e_{\underline{\text{id}}^{-1}} \beta_w^0 + e_{\underline{\text{id}}^{-2}} \beta_w^- - \beta_{s_1 w}^- & \text{if } \ell(w) = 1, \end{cases} \end{aligned} \tag{61}$$

This is proved in [OS22, Proposition 4.9].

- Right action of τ_{s_0} and τ_{s_1} on E^1 when lengths do not add up (some cases):

Let $v \in \widetilde{W}$ such that $\ell(s_0 v) = \ell(v) - 1$. One has:

$$\beta_{s_0}^0 \cdot \tau_v = -e_1 \beta_v^0 - e_{\underline{\text{id}}^{-1}} \beta_v^-. \tag{62}$$

Let $v \in \widetilde{W}$ such that $\ell(s_1 v) = \ell(v) - 1$. One has:

$$\beta_{s_1}^0 \cdot \tau_v = -e_1 \beta_v^0 + e_{\underline{\text{id}}} \beta_v^+. \tag{63}$$

This is proved in [OS22, Lemma 4.12].

- Action of the anti-involution $\mathcal{J}$ on E^1 (see [OS22, Lemma 4.7]):

Let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about β_w^0) and let $u_w \in \mathbb{F}_p^\times$ be such that $\omega_{u_w}^{-1} w$ lies in the subgroup of $\widetilde{W}$ generated by s_0 and s_1 (it is easy to see that such u_w exists and, although it is not unique, it has the property that u_w^2 is uniquely determined by w ; for the notation ω ? see (36)). One has:

$$\begin{aligned}\mathcal{J}(\beta_w^-) &= \begin{cases} u_w^2 \beta_{w^{-1}}^- & \text{if } \ell(w) \text{ is even,} \\ -u_w^2 \beta_{w^{-1}}^+ & \text{if } \ell(w) \text{ is odd,} \end{cases} \\ \mathcal{J}(\beta_w^0) &= \begin{cases} \beta_{w^{-1}}^0 & \text{if } \ell(w) \text{ is even,} \\ -\beta_{w^{-1}}^0 & \text{if } \ell(w) \text{ is odd,} \end{cases} \\ \mathcal{J}(\beta_w^+) &= \begin{cases} u_w^{-2} \beta_{w^{-1}}^+ & \text{if } \ell(w) \text{ is even,} \\ -u_w^{-2} \beta_{w^{-1}}^- & \text{if } \ell(w) \text{ is odd.} \end{cases} \end{aligned} \tag{64}$$

- Action of the involutive automorphism Γ_ϖ on E^1 (see [OS22, Lemma 4.4]):

Let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about β_w^0). One has:

$$\begin{aligned}\Gamma_\varpi(\beta_w^-) &= \beta_{\varpi w \varpi^{-1}}^+, \\ \Gamma_\varpi(\beta_w^0) &= -\beta_{\varpi w \varpi^{-1}}^0, \\ \Gamma_\varpi(\beta_w^+) &= \beta_{\varpi w \varpi^{-1}}^-\end{aligned}\tag{65}$$

- Left and right action of τ_ω on E^2 for $\omega \in T^0/T^1$:

Let $u \in \mathbb{F}_p^\times$, let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about α_w^0). Recall the notation ω_u from (36). One has:

$$\begin{aligned}\tau_{\omega_u} \cdot \alpha_w^- &= u^2 \alpha_{\omega_u w}^-, \\ \tau_{\omega_u} \cdot \alpha_w^0 &= \alpha_{\omega_u w}^0, \\ \tau_{\omega_u} \cdot \alpha_w^+ &= u^{-2} \alpha_{\omega_u w}^+\end{aligned}\tag{66}$$

and

$$\begin{aligned}\alpha_w^- \cdot \tau_{\omega_u} &= \alpha_{w \omega_u}^-, \\ \alpha_w^0 \cdot \tau_{\omega_u} &= \alpha_{w \omega_u}^0, \\ \alpha_w^+ \cdot \tau_{\omega_u} &= \alpha_{w \omega_u}^+.\end{aligned}\tag{67}$$

For the proof of the first formula see [OS22, Equation (89)]. The second formula can be proved exactly in the same way using the corresponding formula for E^1 , or from the first formula by using the anti-involution (see (72) later).

- Action of the idempotents on E^2 :

Let $\lambda \in \widehat{T^0/T^1}$ and let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about α_w^0). One has:

$$\begin{aligned}\alpha_w^- \cdot e_\lambda &= e_{\lambda(-1)^{\ell(w)} \cdot \underline{id}^2} \cdot \alpha_w^-, \\ \alpha_w^0 \cdot e_\lambda &= e_{\lambda(-1)^{\ell(w)}} \cdot \alpha_w^0 \quad (\text{if } \ell(w) \geq 1), \\ \alpha_w^+ \cdot e_\lambda &= e_{\lambda(-1)^{\ell(w)} \cdot \underline{id}^{-2}} \cdot \alpha_w^+.\end{aligned}\tag{68}$$

These formulas can be proved using (66) and (67).

- Left action of τ_{s_0} and τ_{s_1} when lengths add up (see [OS22, Proposition 5.5]):

Let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about α_w^0). One has:

$$\left. \begin{aligned}\tau_{s_0} \cdot \alpha_z^- &= 0 \\ \tau_{s_0} \cdot \alpha_z^0 &= 0 \\ \tau_{s_0} \cdot \alpha_z^+ &= -\alpha_{s_0 w}^-\end{aligned} \right\} \quad \text{if } \ell(s_0 w) = \ell(w) + 1,$$

$$\left. \begin{aligned}\tau_{s_1} \cdot \alpha_z^- &= -\alpha_{s_1 w}^+ \\ \tau_{s_1} \cdot \alpha_z^0 &= 0 \\ \tau_{s_1} \cdot \alpha_z^+ &= 0\end{aligned} \right\} \quad \text{if } \ell(s_1 w) = \ell(w) + 1.\tag{69}$$

- Left action of τ_{s_0} and τ_{s_1} when lengths do not add up (see [OS22, Proposition 5.5]):

Let $w \in \widetilde{W}$ be such that $\ell(s_0 w) = \ell(w) - 1$. One has:

$$\begin{aligned} \tau_{s_0} \cdot \alpha_w^- &= -e_1 \alpha_w^- \\ \tau_{s_0} \cdot \alpha_w^0 &= \begin{cases} -e_1 \alpha_w^0 + 2e_{\underline{\text{id}}} \alpha_w^- - \alpha_{s_0 w}^0 & \text{if } \ell(w) \geq 2, \\ -e_1 \alpha_w^0 + 2e_{\underline{\text{id}}} \alpha_w^- & \text{if } \ell(w) = 1, \end{cases} \\ \tau_{s_0} \cdot \alpha_w^+ &= \begin{cases} -e_1 \alpha_w^+ - \alpha_{s_0 w}^- & \text{if } \ell(w) \geq 2, \\ -e_1 \alpha_w^+ - e_{\underline{\text{id}}} \alpha_w^0 + e_{\underline{\text{id}}^2} \alpha_w^- - \alpha_{s_0 w}^- & \text{if } \ell(w) = 1, \end{cases} \end{aligned} \quad (70)$$

Let $w \in \widetilde{W}$ be such that $\ell(s_1 w) = \ell(w) - 1$. One has:

$$\begin{aligned} \tau_{s_1} \cdot \alpha_w^- &= \begin{cases} -e_1 \alpha_w^- - \alpha_{s_1 w}^+ & \text{if } \ell(w) \geq 2, \\ -e_1 \alpha_w^- + e_{\underline{\text{id}}^{-1}} \alpha_w^0 + e_{\underline{\text{id}}^{-2}} \alpha_w^+ - \alpha_{s_1 w}^+ & \text{if } \ell(w) = 1, \end{cases} \\ \tau_{s_1} \cdot \alpha_w^0 &= \begin{cases} -e_1 \alpha_w^0 - 2e_{\underline{\text{id}}^{-1}} \alpha_w^+ - \alpha_{s_1 w}^0 & \text{if } \ell(w) \geq 2, \\ -e_1 \alpha_w^0 - 2e_{\underline{\text{id}}^{-1}} \alpha_w^+ & \text{if } \ell(w) = 1, \end{cases} \\ \tau_{s_1} \cdot \alpha_w^+ &= -e_1 \alpha_w^+ \end{aligned} \quad (71)$$

- Action of the anti-involution $\mathcal{J}$ on E^2 (see [OS22, Equations (86) and (87)]):

Let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about α_w^0) and let $u_w \in \mathbb{F}_p^\times$ as in (64). One has:

$$\begin{aligned} \mathcal{J}(\alpha_w^-) &= \begin{cases} u_w^{-2} \alpha_{w^{-1}}^- & \text{if } \ell(w) \text{ is even,} \\ -u_w^{-2} \alpha_{w^{-1}}^+ & \text{if } \ell(w) \text{ is odd,} \end{cases} \\ \mathcal{J}(\alpha_w^0) &= \begin{cases} \alpha_{w^{-1}}^0 & \text{if } \ell(w) \text{ is even,} \\ -\alpha_{w^{-1}}^0 & \text{if } \ell(w) \text{ is odd,} \end{cases} \\ \mathcal{J}(\alpha_w^+) &= \begin{cases} u_w^2 \alpha_{w^{-1}}^+ & \text{if } \ell(w) \text{ is even,} \\ -u_w^2 \alpha_{w^{-1}}^- & \text{if } \ell(w) \text{ is odd.} \end{cases} \end{aligned} \quad (72)$$

- Action of the involutive automorphism Γ_ϖ on E^2 (see [OS22, Lemma 5.2]):

Let $w \in \widetilde{W}$ (with the understanding that $\ell(w) \geq 1$ when we speak about α_w^0). One has:

$$\begin{aligned} \Gamma_\varpi(\alpha_w^-) &= \alpha_{\varpi w \varpi^{-1}}^+, \\ \Gamma_\varpi(\alpha_w^0) &= -\alpha_{\varpi w \varpi^{-1}}^0, \\ \Gamma_\varpi(\alpha_w^+) &= \alpha_{\varpi w \varpi^{-1}}^-. \end{aligned} \quad (73)$$

- Left and right action of E^0 on E^3 :

For all $\omega \in T^0/T^1$, for all $j \in \{0, 1\}$ and for all $w \in \widetilde{W}$ one has

$$\begin{aligned} \tau_\omega \cdot \phi_w &= \phi_{\omega w}, \\ \phi_w \cdot \tau_\omega &= \phi_{w\omega}, \\ \tau_{s_j} \cdot \phi_w &= \begin{cases} \phi_{s_j w} - e_1 \cdot \phi_w & \text{if } \ell(s_j w) = \ell(w) - 1, \\ 0 & \text{if } \ell(s_j w) = \ell(w) + 1, \end{cases} \\ \phi_w \cdot \tau_{s_j} &= \begin{cases} \phi_{ws_j} - \phi_w \cdot e_1 & \text{if } \ell(ws_j) = \ell(w) - 1, \\ 0 & \text{if } \ell(ws_j) = \ell(w) + 1. \end{cases} \end{aligned} \quad (74)$$

These formulas follow from the general ones in [OS19, Proposition 8.2].

- Action of the anti-involution $\mathcal{J}$ on E^3 (see [OS19, Equation (89)]):

For all $w \in \widetilde{W}$ one has

$$\mathcal{J}(\phi_w) = \phi_{w^{-1}}. \quad (75)$$

- Action of the involutive automorphism Γ_ϖ on E^3 (see [OS22, Lemma 4.1]):

For all $w \in \widetilde{W}$ one has:

$$\Gamma_\varpi(\phi_w) = \phi_{\varpi w \varpi^{-1}}. \quad (76)$$

Recall that E^1 is finitely-generated as an E^0 -bimodule (Proposition 3.5). In the next lemma we compute a (nice) finite set of generators, along with some useful formulas.

Lemma 6.1. *One has the following facts.*

(i) *The following formulas hold:*

$$\beta_1^- \cdot \tau_w = \beta_w^- \quad \text{for } w \in \widetilde{W} \text{ with } \ell(s_1 w) = \ell(w) + 1, \quad (77)$$

$$\beta_1^+ \cdot \tau_w = \beta_w^+ \quad \text{for } w \in \widetilde{W} \text{ with } \ell(s_0 w) = \ell(w) + 1, \quad (78)$$

$$\tau_{(s_1 s_0)^i} \cdot \beta_1^- = \beta_{(s_1 s_0)^i}^- \quad \text{for all } i \in \mathbb{Z}_{\geq 0}, \quad (79)$$

$$\tau_{s_0(s_1 s_0)^i} \cdot \beta_1^- = -\beta_{s_0(s_1 s_0)^i}^+ \quad \text{for all } i \in \mathbb{Z}_{\geq 0}, \quad (80)$$

$$\tau_{(s_0 s_1)^i} \cdot \beta_1^+ = \beta_{(s_0 s_1)^i}^+ \quad \text{for all } i \in \mathbb{Z}_{\geq 0}, \quad (81)$$

$$\tau_{s_1(s_0 s_1)^i} \cdot \beta_1^+ = -\beta_{s_1(s_0 s_1)^i}^- \quad \text{for all } i \in \mathbb{Z}_{\geq 0}, \quad (82)$$

$$\beta_{s_i}^0 \cdot \tau_w = \beta_{s_i w}^0 \quad \text{for } i \in \{0, 1\} \text{ and } w \in \widetilde{W} \text{ with } \ell(s_i w) = \ell(w) + 1, \quad (83)$$

$$\tau_w \cdot \beta_{s_i}^0 = (-1)^{\ell(w)} \beta_{ws_i}^0 \quad \text{for } i \in \{0, 1\} \text{ and } w \in \widetilde{W} \text{ with } \ell(ws_i) = \ell(w) + 1. \quad (84)$$

(ii) *The following elements generate E^1 as an E^0 -bimodule:*

$$\beta_1^-, \quad \beta_1^+, \quad \beta_{s_0}^0, \quad \beta_{s_1}^0.$$

Proof. Let us prove the two statements.

- (i) Formulas (77), (78) and (83) are immediate consequence of the formulas describing the right action of E^0 when lengths add up (namely, formulas (59) in the case that $\ell(w) \geq 1$ and formulas (56) in the case that $\ell(w) = 0$). Formulas (79), (80), (81) and (82) can be shown using the formulas describing the left action of E^0 when lengths add up (namely, formulas (58)). The same is true for formula (84), also recalling the left action of τ_ω for $\omega \in T^0/T^1$ of formula (55).
- (ii) This is a consequence of part (i). More precisely, for all $v \in \widetilde{W}$ we want to show that the elements β_v^- , β_v^+ and β_v^0 (the last one if $\ell(v) \geq 1$) lie in the sub- E^0 bimodule generated by the four elements in the statement. For β_v^0 this is clear from formula (83) (or from formula (84)). For β_v^- and β_v^+ , using (56) (or (55)), we might assume that v is of the form $(s_1 s_0)^i$, $s_0(s_1 s_0)^i$, $(s_0 s_1)^i$ or $s_1(s_0 s_1)^i$ for some $i \in \mathbb{Z}_{\geq 0}$. Then we can apply the formulas in part (i) to conclude. $\square$

6.2 Outline of the strategy for the first main result

Let us consider the multiplication map

$$\mathcal{M}: T_{E^0}^* E^1 \longrightarrow E^*,$$

where the left hand side is the tensor algebra generated by the E^0 -bimodule E^1 . Proposition 4.8 can be used to prove surjectivity of $\mathcal{M}$, even if it does not directly imply such property (see Lemmas 6.3 and 6.15). The “first main result” we want to prove is the computation of the kernel of $\mathcal{M}$ (Theorem 6.21), hence obtaining a “presentation” of E^* .

This computation will be quite long and will require many intermediate statements, and we now outline the strategy of the proof, working in a general abstract setting to simplify the notation.

Let A be an associative k -algebra with 1 (in our case $A = E^0$); let M and N be A -bimodules (in our case, at first, $M = E^1 \otimes_{E^0} E^1$ and $N = E^2$) and let $\mathcal{M}: M \longrightarrow N$ be a surjective homomorphism of A -bimodules (in our case $\mathcal{M}$ will be the above multiplication map, at first restricted to $E^1 \otimes_{E^0} E^1$). To compute the kernel of $\mathcal{M}$ we fix the following:

- generators $(a_i)_{i \in \mathbf{I}}$ of A as a k -algebra (for a suitable index set $\mathbf{I}$);
- generators $(m_j)_{j \in \mathbf{J}}$ of M as an A -bimodule (for a suitable index set $\mathbf{J}$);
- a basis $(n_l)_{l \in \mathbf{L}}$ of N as a k -vector space (for a suitable index set $\mathbf{L}$).

We fix a splitting $\mathcal{R}$ of $\mathcal{M}$ as a map of k -vector spaces:

$$\begin{array}{ccc} M & \xrightarrow{\mathcal{M}} & N \\ & \nwarrow \mathcal{R} & \nearrow \end{array}$$

Let M' be the sub- A -bimodule of M generated by the elements $\mathcal{R}(a_i n_l) - a_i \mathcal{R}(n_l)$ and by the elements $\mathcal{R}(n_l a_i) - \mathcal{R}(n_l) a_i$ for $i \in \mathbf{I}$ and $l \in \mathbf{L}$. The maps $\mathcal{M}$ and $\mathcal{R}$ define maps $\overline{\mathcal{M}}$ and $\overline{\mathcal{R}}$:

$$\begin{array}{ccc} M/M' & \xrightarrow[\overline{m} \mapsto \mathcal{M}(m)]{\overline{\mathcal{M}}} & N, \\ & \nwarrow \overline{\mathcal{R}} \nearrow & \\ & \overline{\mathcal{R}(n)} \leftarrow n & \end{array}$$

with $\overline{\mathcal{R}}$ being a splitting of $\overline{\mathcal{M}}$, this time not only as a homomorphism of k -vector spaces, but as a homomorphism of A -bimodules. It follows that the A -bimodule $\ker \overline{\mathcal{M}}$ (i.e., $(\ker \mathcal{M})/M'$) is generated by the elements $m_j - (\mathcal{R} \circ \mathcal{M})(m_j)$ for $j \in \mathbf{J}$, and we thus conclude that $\ker \mathcal{M}$ is the sub- A -bimodule of M generated by the following elements:

- $\mathcal{R}(a_i n_l) - a_i \mathcal{R}(n_l)$, for $i \in \mathbf{I}$ and $l \in \mathbf{L}$;
- $\mathcal{R}(n_l a_i) - \mathcal{R}(n_l) a_i$, for $i \in \mathbf{I}$ and $l \in \mathbf{L}$;
- $m_j - (\mathcal{R} \circ \mathcal{M})(m_j)$, for $j \in \mathbf{J}$.

6.3 The tensor algebra

As explained, we work with the tensor algebra $T_{E^0}^* E^1$ and the multiplication map $\mathcal{M}: T_{E^0}^* E^1 \rightarrow E^*$. We denote its graded pieces by

$$\mathcal{M}_i: T_{E^0}^i E^1 \rightarrow E^i.$$

Let us define maps Γ_ϖ and $\mathcal{J}$ on $T_{E^0}^* E^1$ that are compatible with the name-sake maps on E^* . We start by defining a map

$$\begin{aligned} \Gamma_\varpi: \quad T_{E^0}^* E^1 &\longrightarrow T_{E^0}^* E^1 \\ E^0 \ni x &\longmapsto \Gamma_\varpi(x), \\ \beta_1 \otimes \cdots \otimes \beta_i &\longmapsto \Gamma_\varpi(\beta_1) \otimes \cdots \otimes \Gamma_\varpi(\beta_i). \end{aligned}$$

extending the map Γ_ϖ defined on E^0 and E^1 . We see that it is an involutive automorphism the graded k -algebra $T_{E^0}^* E^1$. Similarly, we define the map

$$\begin{aligned} \mathcal{J}: \quad T_{E^0}^* E^1 &\longrightarrow T_{E^0}^* E^1 \\ E^0 \ni x &\longmapsto \mathcal{J}(x), \\ \beta_1 \otimes \cdots \otimes \beta_i &\longmapsto (-1)^{\frac{(i-1)i}{2}} \mathcal{J}(\beta_i) \otimes \cdots \otimes \mathcal{J}(\beta_1). \end{aligned}$$

Note that the sign $(-1)^{\frac{(i-1)i}{2}}$ is the sign of the permutation $(\begin{smallmatrix} 1 & \cdots & i \\ i & \cdots & 1 \end{smallmatrix})$. The map $\mathcal{J}$ that we have just defined is an involutive anti-automorphism on $T_{E^0}^* E^1$.

The above definitions are given in such a way that the following diagrams commute:

$$\begin{array}{ccc}
T_{E^0}^* E^1 & \xrightarrow{\mathcal{M}} & E^* \\
\Gamma_\varpi \downarrow & & \downarrow \Gamma_\varpi \\
T_{E^0}^* E^1 & \xrightarrow{\mathcal{M}} & E^*
\end{array}
\quad
\begin{array}{ccc}
T_{E^0}^* E^1 & \xrightarrow{\mathcal{M}} & E^* \\
\mathcal{J} \downarrow & & \downarrow \mathcal{J} \\
T_{E^0}^* E^1 & \xrightarrow{\mathcal{M}} & E^*
\end{array}
\quad (85)$$

As explained in the outline of the strategy in §6.2, we want to compute a (quite simple) set of generators of $T_{E^0}^2 E^1$ as an E^0 -bimodule.

We recall that the following are generators of E^1 as an E^0 -bimodule (see Lemma 6.1):

$$\beta_1^-, \quad \beta_1^+, \quad \beta_{s_0}^0, \quad \beta_{s_1}^0.$$

It follows that $E^1 \otimes_{E^0} E^1$ is generated by the following elements as a left E^0 -module (in particular also as an E^0 -bimodule):

$$\begin{aligned}
& \beta_1^- \otimes \beta_w^\sigma, \quad \beta_1^+ \otimes \beta_w^\sigma, \quad \beta_{s_0}^0 \otimes \beta_w^\sigma, \quad \beta_{s_1}^0 \otimes \beta_w^\sigma \quad (86) \\
& \text{for } w \in \widetilde{W} \text{ and } \sigma \in \{-, 0, +\} \text{ (with } \ell(w) \geq 1 \text{ in the case } \sigma = 0).
\end{aligned}$$

In the next lemma, we compute a simpler set of E^0 -bimodule generators.

Lemma 6.2. *The following elements generate $E^1 \otimes_{E^0} E^1$ as an E^0 -bimodule:*

$$\begin{aligned}
& \beta_1^- \otimes \beta_1^-, \quad \beta_1^+ \otimes \beta_1^-, \quad \beta_{s_0}^0 \otimes \beta_1^-, \quad \beta_{s_1}^0 \otimes \beta_1^-, \\
& \beta_1^- \otimes \beta_1^+, \quad \beta_1^+ \otimes \beta_1^+, \quad \beta_{s_0}^0 \otimes \beta_1^+, \quad \beta_{s_1}^0 \otimes \beta_1^+, \\
& \beta_1^- \otimes \beta_{s_0}^0, \quad \beta_1^+ \otimes \beta_{s_0}^0, \quad \beta_{s_0}^0 \otimes \beta_{s_0}^0, \quad \beta_{s_1}^0 \otimes \beta_{s_0}^0, \\
& \beta_1^- \otimes \beta_{s_1}^0, \quad \beta_1^+ \otimes \beta_{s_1}^0, \quad \beta_{s_0}^0 \otimes \beta_{s_1}^0, \quad \beta_{s_1}^0 \otimes \beta_{s_1}^0, \\
& \beta_1^+ \otimes \beta_{(s_1 s_0)^i}^- = \beta_{(s_1 s_0)^i}^+ \otimes \beta_1^- \quad \text{for } i \in \mathbb{Z}_{\geq 1}, \\
& \beta_1^+ \otimes \beta_{s_1(s_0 s_1)^i}^- = -\beta_{s_1(s_0 s_1)^i}^+ \otimes \beta_1^+ \quad \text{for } i \in \mathbb{Z}_{\geq 0}, \\
& \beta_1^- \otimes \beta_{(s_0 s_1)^i}^+ = \beta_{(s_0 s_1)^i}^- \otimes \beta_1^+ \quad \text{for } i \in \mathbb{Z}_{\geq 1}, \\
& \beta_1^- \otimes \beta_{s_0(s_1 s_0)^i}^+ = -\beta_{s_0(s_1 s_0)^i}^- \otimes \beta_1^- \quad \text{for } i \in \mathbb{Z}_{\geq 0}.
\end{aligned}$$

Note that the equalities in the last four lines follow from Lemma 6.1.

Proof. We start from the generators in (86), and we recall from Lemma 6.1 that

$$\begin{aligned}
\beta_w^- &= \beta_1^- \cdot \tau_w & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_1 w) = \ell(w) + 1, \\
\beta_w^+ &= \beta_1^+ \cdot \tau_w & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\
\beta_{s_1 w}^0 &= \beta_{s_1}^0 \cdot \tau_w & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_1 w) = \ell(w) + 1, \\
\beta_{s_0 w}^0 &= \beta_{s_0}^0 \cdot \tau_w & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1.
\end{aligned}$$

From this (and from the behaviour of multiplication by τ_ω for $\omega \in T^0/T^1$, see (56)), we obtain that the following elements generate $E^1 \otimes_{E^0} E^1$ as an E^0 -bimodule:

$$\begin{array}{ll}
\gamma \otimes \beta_1^- & \text{for } \gamma \in \{\beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}, \\
\gamma \otimes \beta_1^+ & \text{for } \gamma \text{ as above,} \\
\gamma \otimes \beta_{s_0}^0 & \text{for } \gamma \text{ as above,} \\
\gamma \otimes \beta_{s_1}^0 & \text{for } \gamma \text{ as above.} \\
\gamma \otimes \beta_{(s_1 s_0)^i}^- & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}, \\
\gamma \otimes \beta_{s_1(s_0 s_1)^i}^- & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}, \\
\gamma \otimes \beta_{(s_0 s_1)^i}^+ & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}, \\
\gamma \otimes \beta_{s_0(s_1 s_0)^i}^+ & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}.
\end{array}$$

The first four of these lines consist exactly of the first four lines of the claimed generators in the statement of the lemma. Now, let us look at the remaining four lines: we certainly get the families of generators in the remaining four lines of the statement of the lemma, and we have to argue that the remaining generators are superfluous. Up to changing signs if necessary, using the formulas of Lemma 6.1, we can rewrite the last four lines as:

$$\begin{array}{ll}
(\gamma \cdot \tau_{(s_1 s_0)^i}) \otimes \beta_1^- & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}, \\
(\gamma \cdot \tau_{s_1(s_0 s_1)^i}) \otimes \beta_1^+ & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}, \\
(\gamma \cdot \tau_{(s_0 s_1)^i}) \otimes \beta_1^+ & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}, \\
(\gamma \cdot \tau_{s_0(s_1 s_0)^i}) \otimes \beta_1^- & \text{for } \gamma \text{ as above and for } i \in \mathbb{Z}_{\geq 1}.
\end{array}$$

From Lemma 6.1, one has

$$\beta_1^- \cdot \tau_{(s_1 s_0)^i} = 0, \quad \beta_1^- \cdot \tau_{s_1(s_0 s_1)^i} = 0, \quad \beta_1^+ \cdot \tau_{(s_0 s_1)^i} = 0, \quad \beta_1^+ \cdot \tau_{s_0(s_1 s_0)^i} = 0.$$

This shows that some of the remaining generators are superfluous, and now it remains to study the cases where $\gamma \in \{\beta_{s_0}^0, \beta_{s_1}^0\}$.

Let us start with the following case:

$$\begin{aligned}
(\beta_{s_0}^0 \cdot \tau_{(s_1 s_0)^i}) \otimes \beta_1^- &= \beta_{s_0(s_1 s_0)^i}^0 \otimes \beta_1^- \\
&= \tau_{(s_0 s_1)^i} \beta_{s_0}^0 \otimes \beta_1^-,
\end{aligned}$$

where we used the formulas (83) and (84). We see that the element $\beta_{s_0}^0 \otimes \beta_1^-$ is a generator already appearing in the list in the statement of the lemma, and so the generator $(\beta_{s_0}^0 \cdot \tau_{(s_1 s_0)^i}) \otimes \beta_1^-$ is superfluous. The other three cases where lengths add up are similar.

Now it remains to prove that the generators

$$\begin{array}{ll}
(\beta_{s_1}^0 \cdot \tau_{(s_1 s_0)^i}) \otimes \beta_1^-, & (\beta_{s_1}^0 \cdot \tau_{s_1(s_0 s_1)^i}) \otimes \beta_1^+, \\
(\beta_{s_0}^0 \cdot \tau_{(s_0 s_1)^i}) \otimes \beta_1^+, & (\beta_{s_0}^0 \cdot \tau_{s_0(s_1 s_0)^i}) \otimes \beta_1^-
\end{array}$$

are superfluous. To this end, we can use the formulas (62) and (63): we spell the details for the first generator, the other three being similar.

$$\begin{aligned} (\beta_{s_1}^0 \cdot \tau_{(s_1 s_0)^i}) \otimes \beta_1^- &= \left(-e_1 \cdot \beta_{(s_1 s_0)^i}^0 + e_{\text{id}} \cdot \beta_{(s_1 s_0)^i}^+ \right) \otimes \beta_1^- \\ &= e_1 \cdot \tau_{(s_1 s_0)^{i-1} s_1} \cdot \beta_{s_0}^0 \otimes \beta_1^- + e_{\text{id}} \cdot \beta_{(s_1 s_0)^i}^+ \otimes \beta_1^-, \end{aligned}$$

where, besides (63), we have also used (84). $\square$

6.4 The 2nd graded piece of the kernel

The multiplication map $\mathcal{M}_2$ is surjective: indeed, Proposition 4.8 shows that $H^2(I, \mathbf{X}(w))$ is contained in its image for all $w \in \widetilde{W}$ with $\ell(w) \geq 1$, and for all $\omega \in T^0/T^1$ (i.e., $\omega \in \widetilde{W}$ with $\ell(\omega) = 0$) one concludes with the following consequence of formulas (70) and (71):

$$\begin{aligned} \tau_{s_0} \cdot \alpha_{s_0^{-1}\omega}^+ + \alpha_\omega^- &\in \bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) = 1}} H^2(I, \mathbf{X}(v)), \\ \tau_{s_1} \cdot \alpha_{s_1^{-1}\omega}^- + \alpha_\omega^+ &\in \bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) = 1}} H^2(I, \mathbf{X}(v)). \end{aligned} \tag{87}$$

The purpose of this subsection is to compute the kernel of $\mathcal{M}_2$, and following the outline in §6.2 we start by constructing a section of $\mathcal{M}_2$ as a homomorphism of k -vector space.

Lemma 6.3. *The multiplication map $\mathcal{M}_2: T_{E^0}^2 E^1 \longrightarrow E^2$ is surjective, and the following is a section of it as a homomorphism of k -vector spaces.*

$$\begin{array}{lll} \mathcal{R}_2: E^2 & \longrightarrow & T_{E^0}^2 E^1 = E^1 \otimes_{E^0} E^1 \\ \alpha_{s_1 v}^- & \longmapsto & -\beta_1^+ \otimes \beta_{s_1 v}^0 & \text{if } \ell(s_1 v) = \ell(v) + 1, \\ \alpha_{s_1 v}^0 & \longmapsto & \beta_1^+ \otimes \beta_{s_1 v}^- & \text{if } \ell(s_1 v) = \ell(v) + 1, \\ \alpha_{s_1 v}^+ & \longmapsto & \beta_{s_1}^0 \otimes \beta_v^+ & \text{if } \ell(s_1 v) = \ell(v) + 1, \\ \alpha_{s_0 w}^- & \longmapsto & -\beta_{s_0}^0 \otimes \beta_w^- & \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \alpha_{s_0 w}^0 & \longmapsto & -\beta_1^- \otimes \beta_{s_0 w}^+ & \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \alpha_{s_0 w}^+ & \longmapsto & \beta_1^- \otimes \beta_{s_0 w}^0 & \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \alpha_\omega^- & \longmapsto & \mathcal{R}_2(\alpha_\omega^- + \tau_{s_0} \cdot \alpha_{s_0^{-1}\omega}^+) - \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0^{-1}\omega}^+) & \text{for } \omega \in T^0/T^1, \\ \alpha_\omega^+ & \longmapsto & \mathcal{R}_2(\alpha_\omega^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}\omega}^-) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}\omega}^-) & \text{for } \omega \in T^0/T^1. \end{array}$$

Note that the last two lines make sense: by (87), on the right hand side of such lines only the values of $\mathcal{R}_2$ on $\bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) = 1}} H^2(I, \mathbf{X}(v))$ are used, and on such subspace $\mathcal{R}_2$ is defined in the preceding lines.

Proof. Combining formula (28) in the proof of Proposition 4.8 with (46), we obtain

$$\begin{aligned}\beta_{(s_0 s_1)^i}^0 \cdot \beta_1^+ &= \beta_{(s_0 s_1)^i}^0 \smile \beta_{(s_0 s_1)^i}^+ = \alpha_{(s_0 s_1)^i}^-, \\ \beta_1^- \cdot \tau_{(s_0 s_1)^i} \cdot \beta_1^+ &= \beta_{(s_0 s_1)^i}^- \smile \beta_{(s_0 s_1)^i}^+ = -\alpha_{(s_0 s_1)^i}^0, \\ \beta_1^- \cdot \beta_{(s_0 s_1)^i}^0 &= \beta_{(s_0 s_1)^i}^- \smile \beta_{(s_0 s_1)^i}^0 = \alpha_{(s_0 s_1)^i}^+, \end{aligned}$$

We rewrite this as follows:

$$\begin{aligned}\alpha_{(s_0 s_1)^i}^- &= \beta_{(s_0 s_1)^i}^0 \cdot \beta_1^+ = \beta_{s_0}^0 \cdot \tau_{s_1(s_0 s_1)^{i-1}} \cdot \beta_1^+ = -\beta_{s_0}^0 \cdot \beta_{s_1(s_0 s_1)^{i-1}}^-, \\ \alpha_{(s_0 s_1)^i}^0 &= -\beta_1^- \cdot \tau_{(s_0 s_1)^i} \cdot \beta_1^+ = -\beta_1^- \cdot \beta_{(s_0 s_1)^i}^+, \\ \alpha_{(s_0 s_1)^i}^+ &= \beta_1^- \cdot \beta_{(s_0 s_1)^i}^0, \end{aligned}$$

where we have used the formulas of Lemma 6.1.

This proves that the map $\mathcal{M}_2 \circ \mathcal{R}_2$ is the identity at $\alpha_{s_0 w}^-$, $\alpha_{s_0 w}^0$, $\alpha_{s_0 w}^+$ for all w of the form $s_1(s_0 s_1)^{i-1}$ for some $i \in \mathbb{Z}_{\geq 1}$. From the formulas (56) it follows that the same is true for w of the form $s_1(s_0 s_1)^{i-1}\omega$ for some $i \in \mathbb{Z}_{\geq 1}$ and some $\omega \in T^0/T^1$. The proof that the same claim is true for all w of the form $(s_1 s_0)^{i-1}\omega$ for some $i \in \mathbb{Z}_{\geq 1}$ and some $\omega \in T^0/T^1$ is similar, and this shows that the map $\mathcal{M}_2 \circ \mathcal{R}_2$ is the identity at $\alpha_{s_0 w}^-$, $\alpha_{s_0 w}^0$, $\alpha_{s_0 w}^+$ for all $w \in \widetilde{W}$ such that $\ell(s_0 w) = \ell(w) + 1$.

Similarly one shows that $\mathcal{M}_2 \circ \mathcal{R}_2$ is the identity at $\alpha_{s_1 v}^-$, $\alpha_{s_1 v}^0$, $\alpha_{s_1 v}^+$ for all $v \in \widetilde{W}$ such that $\ell(s_1 v) = \ell(v) + 1$. Finally, the fact that $\mathcal{M}_2 \circ \mathcal{R}_2$ is the identity at α_{ω}^- and α_{ω}^+ for all $\omega \in \Omega$ follows from the fact that $\mathcal{M}_2 \circ \mathcal{R}_2$ is the identity on $\bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) = 1}} H^2(I, \mathbf{X}(v))$. $\square$

For the next lemma, we use the identification of k -algebras

$$\text{span}_k \{ \tau_{\omega} \mid \omega \in T^0/T^1 \} \cong k[T^0/T^1].$$

Lemma 6.4. *The map $\mathcal{R}_2$ is a homomorphism of $k[T^0/T^1]$ -bimodules.*

Proof. From the definition of $\mathcal{R}_2$ and from the formulas for the right action of $k[T^0/T^1]$ on E^1 and E^2 (see (56) (67)), it is clear that $\mathcal{R}_2$ is a homomorphism of right $k[T^0/T^1]$ -modules.

Regarding the left action, from the formulas (66) and (67) describing the action of $k[T^0/T^1]$ on E^2 , we see that for all $\omega \in T^0/T^1$, for all $\sigma \in \{-, 0, +\}$ and for all $w \in \widetilde{W}$ (of length greater or equal than 1 if $\sigma = 0$) we have

$$\tau_{\omega} \cdot \alpha_w^{\sigma} = c_{\omega, \sigma} \alpha_w^{\sigma} \cdot \tau_{\omega(-1)^{\ell(w)}},$$

for some $c_{\omega, \sigma} \in k^{\times}$. Assume now that $\ell(w) \geq 1$. Looking at the definition of $\mathcal{R}_2$ in Lemma 6.3, and using the formulas (55) and (56) describing the action of $k[T^0/T^1]$ on E^1 , we see that we also have the completely analogous result

$$\tau_{\omega} \cdot \mathcal{R}_2(\alpha_w^{\sigma}) = c'_{\omega, \sigma} \mathcal{R}_2(\alpha_w^{\sigma}) \cdot \tau_{\omega(-1)^{\ell(w)}},$$

for some $c'_{\omega,\sigma} \in k^\times$. Using that $\mathcal{R}_2$ is a homomorphism of right $k[T^0/T^1]$ -modules, we thus see that

$$\tau_\omega \cdot \mathcal{R}_2(\alpha_w^\sigma) = c'_{\omega,\sigma} c_{\omega,\sigma}^{-1} \mathcal{R}_2(\tau_\omega \cdot \alpha_w^\sigma),$$

and by applying $\mathcal{M}_2$ to both sides, we see that the coefficient $c'_{\omega,\sigma} c_{\omega,\sigma}^{-1}$ must be 1.

So far, we have shown that the maps $\tau_\omega \cdot \mathcal{R}_2(-)$ and $\mathcal{R}_2(\tau_\omega \cdot -)$ coincide on the subspace $\bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) \geq 1}} H^2(I, \mathbf{X}(v))$, and looking at the definition of $\mathcal{R}_2$ on the subspace $\bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) = 0}} H^2(I, \mathbf{X}(v))$, we then deduce that the maps $\tau_\omega \cdot \mathcal{R}_2(-)$ and $\mathcal{R}_2(\tau_\omega \cdot -)$ coincide on the whole E^2 . $\square$

Lemma 6.5. *The maps $\mathcal{R}_2$ and Γ_ϖ commute. More precisely, the following diagram is commutative:*

$$\begin{array}{ccc} E^2 & \xrightarrow{\mathcal{R}_2} & E^1 \otimes_{E^0} E^1 \\ \downarrow \Gamma_\varpi & & \downarrow \Gamma_\varpi \\ E^2 & \xrightarrow{\mathcal{R}_2} & E^1 \otimes_{E^0} E^1. \end{array}$$

Proof. Let $v \in \widetilde{W}$ with $\ell(s_1 v) = \ell(v) + 1$. We compute

$$\begin{aligned} \Gamma_\varpi(\mathcal{R}_2(\alpha_{s_1 v}^-)) &= \Gamma_\varpi(-\beta_1^+ \otimes \beta_{s_1 v}^0) \\ &= \beta_1^- \otimes \beta_{s_0 \varpi v \varpi^{-1}}^0, \\ \Gamma_\varpi(\mathcal{R}_2(\alpha_{s_1 v}^0)) &= \Gamma_\varpi(\beta_1^+ \otimes \beta_{s_1 v}^-) \\ &= \beta_1^- \otimes \beta_{s_0 \varpi v \varpi^{-1}}^+, \\ \Gamma_\varpi(\mathcal{R}_2(\alpha_{s_1 v}^+)) &= \Gamma_\varpi(\beta_{s_1}^0 \otimes \beta_v^+) \\ &= -\beta_{s_0}^0 \otimes \beta_{\varpi v \varpi^{-1}}^-. \end{aligned}$$

Here we have used the definition of Γ_ϖ on $T_{E^0}^* E^1$, the formulas for the action of Γ_ϖ on E^1 (65), and the fact that $\varpi s_1 \varpi^{-1} = s_0$. On the other side, we compute

$$\begin{aligned} \mathcal{R}_2(\Gamma_\varpi(\alpha_{s_1 v}^-)) &= \mathcal{R}_2(\alpha_{s_0 \varpi v \varpi^{-1}}^+), \\ \mathcal{R}_2(\Gamma_\varpi(\alpha_{s_1 v}^0)) &= -\mathcal{R}_2(\alpha_{s_0 \varpi v \varpi^{-1}}^0), \\ \mathcal{R}_2(\Gamma_\varpi(\alpha_{s_1 v}^+)) &= \mathcal{R}_2(\alpha_{s_0 \varpi v \varpi^{-1}}^-), \end{aligned}$$

where we have used the formulas for the action of Γ_ϖ on E^2 (73). Comparing the two above computations with the definition of $\mathcal{R}_2$, we see that the maps $\Gamma_\varpi \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \Gamma_\varpi$ coincide at $\alpha_{s_1 v}^-$, $\alpha_{s_1 v}^0$ and $\alpha_{s_1 v}^+$.

We also see that

$$\begin{aligned}
\Gamma_{\varpi}(\mathcal{R}_2(\alpha_{\omega}^+)) &= \Gamma_{\varpi} \left(\mathcal{R}_2(\alpha_{\omega}^+ + \tau_{s_1\omega} \cdot \alpha_{s_1^{-1}\omega}^-) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}\omega}^-) \right) \\
&= \Gamma_{\varpi} \left(\mathcal{R}_2(\alpha_{\omega}^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}\omega}^-) \right) - \tau_{s_0} \cdot \Gamma_{\varpi} \left(\mathcal{R}_2(\alpha_{s_1^{-1}\omega}^-) \right) \\
&= \mathcal{R}_2 \left(\Gamma_{\varpi}(\alpha_{\omega}^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}\omega}^-) \right) - \tau_{s_0} \cdot \mathcal{R}_2 \left(\Gamma_{\varpi}(\alpha_{s_1^{-1}\omega}^-) \right) \\
&\quad \text{(since } \Gamma_{\varpi} \circ \mathcal{R}_2 \text{ and } \mathcal{R}_2 \circ \Gamma_{\varpi} \text{ coincide on } \bigoplus_{\vartheta \in T^0/T^1} H^2(I, \mathbf{X}(s_1\vartheta)) \text{)} \\
&= \mathcal{R}_2(\alpha_{\varpi\omega\varpi^{-1}}^- + \tau_{s_0} \cdot \alpha_{s_0^{-1}\varpi\omega\varpi^{-1}}^+) - \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0^{-1}\varpi\omega\varpi^{-1}}^+) \\
&= \mathcal{R}_2(\alpha_{\varpi\omega\varpi^{-1}}^-) \\
&= \mathcal{R}_2(\Gamma_{\varpi}(\alpha_{\omega}^+)),
\end{aligned}$$

where we have used the same formulas as before (and the fact that $\Gamma_{\varpi}(\tau_{s_1}) = \tau_{s_0}$, see (54)).

So far, we have shown that the maps $\Gamma_{\varpi} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \Gamma_{\varpi}$ coincide on “half” of the elements of the k -basis of E^2 used in the definition of $\mathcal{R}_2$. To conclude the proof, we remark that, since Γ_{ϖ} is an involution, if the maps $\Gamma_{\varpi} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \Gamma_{\varpi}$ coincide on an element $x \in E^2$, then they coincide also on $\Gamma_{\varpi}(x)$. $\square$

Lemma 6.6. *Let us consider the following $\mathcal{J}$ -invariant k -subspace of E^2 :*

$$F^1 E^2 := \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \geq 1}} H^2(I, \mathbf{X}(w)).$$

One has that map $\mathcal{R}_2|_{F^1 E^2}$ commutes with the anti-involution $\mathcal{J}$. More precisely, the following diagram is commutative:

$$\begin{array}{ccc}
F^1 E^2 & \xrightarrow{\mathcal{R}_2|_{F^1 E^2}} & E^1 \otimes_{E^0} E^1 \\
\mathcal{J} \downarrow & & \downarrow \mathcal{J} \\
F^1 E^2 & \xrightarrow{\mathcal{R}_2|_{F^1 E^2}} & E^1 \otimes_{E^0} E^1.
\end{array}$$

$\beta \otimes \beta' \downarrow$
 $-\mathcal{J}(\beta') \otimes \mathcal{J}(\beta) \downarrow$

Proof. We first recall from (38) that the involutions $\mathcal{J}$ and Γ_{ϖ} commute on E^* . Using this property, let us see that if the maps $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ coincide at a certain $\alpha \in E^2$, then they also coincide at $\Gamma_{\varpi}(\alpha)$: indeed, one has

$$\begin{aligned}
(\mathcal{J} \circ \mathcal{R}_2)(\Gamma_{\varpi}(\alpha)) &= (\mathcal{J} \circ \Gamma_{\varpi} \circ \mathcal{R}_2)(\alpha) \quad \text{as } \mathcal{R}_2 \text{ and } \Gamma_{\varpi} \text{ commute (Lemma 6.5)} \\
&= (\Gamma_{\varpi} \circ \mathcal{J} \circ \mathcal{R}_2)(\alpha) \quad \begin{array}{l} \text{as } \mathcal{J} \text{ and } \Gamma_{\varpi} \text{ commute on } E^1 \\ \text{and hence on } E^1 \otimes_{E^0} E^1 \end{array} \\
&= (\Gamma_{\varpi} \circ \mathcal{R}_2 \circ \mathcal{J})(\alpha) \quad \text{by assumption} \\
&= (\mathcal{R}_2 \circ \Gamma_{\varpi} \circ \mathcal{J})(\alpha) \quad \text{as } \mathcal{R}_2 \text{ and } \Gamma_{\varpi} \text{ commute (Lemma 6.5)} \\
&= (\mathcal{R}_2 \circ \mathcal{J})(\Gamma_{\varpi}(\alpha)) \quad \text{as } \mathcal{J} \text{ and } \Gamma_{\varpi} \text{ commute on } E^2.
\end{aligned}$$

Now, let us look at the definition of $\mathcal{R}_2$ in Lemma 6.3. By what we have just remarked, we only need to show that $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ coincide at $\alpha_{s_1 v}^-$, $\alpha_{s_1 v}^0$ and $\alpha_{s_1 v}^+$ for all $v \in \widetilde{W}$ such that $\ell(s_1 v) = \ell(v) + 1$. Since $\mathcal{R}_2$ is a homomorphism of $k[T^0/T^1]$ -bimodules (Lemma 6.4) and since $\mathcal{J}: E^* \rightarrow E^*$ and $\mathcal{J}: T_{E^0}^* E^1 \rightarrow T_{E^0}^* E^1$ are anti-multiplicative, it follows that $\mathcal{J} \circ \mathcal{R}_2 \circ \mathcal{J}$ is a homomorphism of $k[T^0/T^1]$ -bimodules, and so (looking at formulas (67)) we can assume that v is of the form $(s_0 s_1)^i$ or $s_0(s_1 s_0)^i$ for some $i \in \mathbb{Z}_{\geq 0}$. Using the formulas for the action of $\mathcal{J}$ on E^2 (72) as well as the definition of $\mathcal{R}_2$ and recalling the definition of c_{-1} from (35), we compute

$$\mathcal{R}_2(\mathcal{J}(\alpha_{s_1(s_0 s_1)^i}^-)) = -\mathcal{R}_2(\alpha_{s_1(s_0 s_1)^i c_{-1}}^+) = -\beta_{s_1}^0 \otimes \beta_{(s_0 s_1)^i c_{-1}}^+.$$

Similarly, using the formulas for the action of $\mathcal{J}$ on E^1 (64) (together with the definition of $\mathcal{J}$ on $E^1 \otimes_{E^0} E^1$ and the definition of $\mathcal{R}_2$), we compute

$$\mathcal{J}(\mathcal{R}_2(\alpha_{s_1(s_0 s_1)^i}^-)) = -\mathcal{J}(\beta_1^+ \otimes \beta_{s_1(s_0 s_1)^i}^0) = -\beta_{s_1(s_0 s_1)^i c_{-1}}^0 \otimes \beta_1^+.$$

And, using the formulas in Lemma 6.1, we conclude that the two simple tensors we have obtained are equal, and hence that $\mathcal{R}_2 \circ \mathcal{J}$ and $\mathcal{J} \circ \mathcal{R}_2$ coincide at $\alpha_{s_1(s_0 s_1)^i}^-$.

Similarly, one computes that $\mathcal{R}_2 \circ \mathcal{J}$ and $\mathcal{J} \circ \mathcal{R}_2$ coincide at $\alpha_{s_1(s_0 s_1)^i}^0$, $\alpha_{s_1(s_0 s_1)^i}^+$, $\alpha_{(s_1 s_0)^{i+1}}^-$, $\alpha_{(s_1 s_0)^{i+1}}^0$ and $\alpha_{(s_1 s_0)^{i+1}}^+$. $\square$

The above result leaves open the question of whether $\mathcal{R}_2$ and $\mathcal{J}$ could commute on the whole E^2 . This is dealt with in the following lemma and remark.

Lemma 6.7. *One has the following equalities:*

$$\begin{aligned} (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) &= \beta_{s_0}^+ \otimes \beta_{s_0^{-1}}^0 + \beta_{s_0}^0 \otimes \beta_{s_0^{-1}}^- \\ &= -\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0^{-1}} \\ (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^+) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^+) &= -\beta_{s_1}^- \otimes \beta_{s_1^{-1}}^0 - \beta_{s_1}^0 \otimes \beta_{s_1^{-1}}^+ \\ &= \tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 - \beta_{s_1}^0 \otimes \beta_1^+ \cdot \tau_{s_1^{-1}} \end{aligned}$$

Proof. First note that the second formula can be obtained from the first one by applying Γ_ϖ : indeed Γ_ϖ commutes with $\mathcal{R}_2$ (Lemma 6.5) and with $\mathcal{J}$ (see (38)), and $\Gamma_\varpi(\alpha_1^-) = \alpha_1^+$ (see (73)); hence applying Γ_ϖ on $(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-)$ we obtain exactly $(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^+) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^+)$. Using the formulas for the action of Γ_ϖ on E^0 (54) and on E^1 (65), we also see that the terms on the right of the equations correspond.

The equality $\beta_{s_0}^+ \otimes \beta_{s_0^{-1}}^0 + \beta_{s_0}^0 \otimes \beta_{s_0^{-1}}^- = -\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0^{-1}}$ is immediate from the formulas (58) and (59). Therefore, to prove the lemma it remains to check that

$$(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) = -\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0^{-1}}$$

Using (72) and the definition of $\mathcal{R}_2$, we see that

$$\begin{aligned} (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) &= \mathcal{R}_2(\alpha_1^-) \\ &= \mathcal{R}_2(\alpha_1^- + \tau_{s_0} \cdot \alpha_{s_0-1}^+) - \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0-1}^+). \end{aligned}$$

On the other side, using that the maps $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ coincide on $F^1 E^2$, we deduce that

$$\begin{aligned} (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) &= (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^- + \tau_{s_0} \cdot \alpha_{s_0-1}^+) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_{s_0-1}^+) \cdot \tau_{s_0}^{-1} \\ &= (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^- + \tau_{s_0} \cdot \alpha_{s_0-1}^+) - (\mathcal{R}_2 \circ \mathcal{J})(\alpha_{s_0-1}^+) \cdot \tau_{s_0}^{-1} \quad (88) \\ &= \mathcal{R}_2(\alpha_1^- + \mathcal{J}(\tau_{s_0} \cdot \alpha_{s_0-1}^+)) + \mathcal{R}_2(\alpha_{s_0}^-) \cdot \tau_{s_0}^{-1}, \end{aligned}$$

where we have also used that $\mathcal{J}$ is anti-multiplicative, that $\mathcal{J}(\tau_{s_0}) = \tau_{s_0}^{-1}$ by (53) and, again, that $\mathcal{J}(\alpha_1^-) = \alpha_1^-$. We thus deduce that

$$\begin{aligned} (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) &= \mathcal{R}_2(\tau_{s_0} \cdot \alpha_{s_0-1}^+ - \mathcal{J}(\tau_{s_0} \cdot \alpha_{s_0-1}^+)) - \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0-1}^+) - \mathcal{R}_2(\alpha_{s_0}^-) \cdot \tau_{s_0}^{-1} \quad (89) \end{aligned}$$

We now focus on the first term in this sum. Using (70), we compute

$$\tau_{s_0} \cdot \alpha_{s_0-1}^+ = -e_1 \alpha_{s_0-1}^+ - e_{\text{id}} \alpha_{s_0-1}^0 + e_{\text{id}^2} \alpha_{s_0-1}^- - \alpha_1^-.$$

Using formulas (72) and (68) and using the fact that $\mathcal{J}(e_\lambda) = e_{\lambda^{-1}}$ for all $\lambda \in \widehat{T^0/T^1}$ (which follows from (53)), we compute

$$\begin{aligned} \mathcal{J}(\tau_{s_0} \cdot \alpha_{s_0-1}^+) &= \mathcal{J}(-e_1 \alpha_{s_0-1}^+ - e_{\text{id}} \alpha_{s_0-1}^0 + e_{\text{id}^2} \alpha_{s_0-1}^- - \alpha_1^-) \\ &= \alpha_{s_0}^- e_1 + \alpha_{s_0}^0 e_{\text{id}^{-1}} - \alpha_{s_0}^+ e_{\text{id}^{-2}} - \alpha_1^- \\ &= e_{\text{id}^2} \alpha_{s_0}^- + e_{\text{id}} \alpha_{s_0}^0 - e_1 \alpha_{s_0}^+ - \alpha_1^- \\ &= e_{\text{id}^2} \alpha_{s_0}^- - e_{\text{id}} \alpha_{s_0-1}^0 - e_1 \alpha_{s_0-1}^+ - \alpha_1^-. \end{aligned}$$

In the last line we have used the formulas for the left action of $\tau_{c_{-1}}$ on E^2 (see (55) and recall the definition of c_{-1} from (35)) and the fact $e_\lambda \tau_{c_{-1}} = \lambda(c_{-1}) e_\lambda$ for all $\lambda \in \widehat{T^0/T^1}$ (see (49)).

We have shown that $\tau_{s_0} \cdot \alpha_{s_0-1}^+ = \mathcal{J}(\tau_{s_0} \cdot \alpha_{s_0-1}^+)$, and so going back to (89), we obtain

$$\begin{aligned} (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) &= -\tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0-1}^+) - \mathcal{R}_2(\alpha_{s_0}^-) \cdot \tau_{s_0}^{-1} \\ &= -\tau_{s_0} \cdot (\beta_1^- \otimes \beta_{s_0-1}^0) - (-\beta_{s_0}^0 \otimes \beta_1^-) \cdot \tau_{s_0}^{-1} \end{aligned}$$

This is the formula we had to check. $\square$

Remark 6.8. It can be proved that the elements of $E^1 \otimes_{E^0} E^1$ in the previous lemma are nonzero, thus showing that $\mathcal{J} \circ \mathcal{R}_2 \neq \mathcal{R}_2 \circ \mathcal{J}$. For the details see [Bod22, Remark 4.5.8]. Furthermore, in loc.cit. it is shown that one can modify the definition of $\mathcal{R}_2$ on $\bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) = 0}} H^2(I, \mathbf{X}(w))$ in such a way that one gets

a new section $\mathcal{R}'_2$ of $\mathcal{M}_2$ that is a homomorphism of $k[T^0/T^1]$ -bimodules, that commutes with Γ_ϖ and that commutes with $\mathcal{J}$. However, we do not change the definition of $\mathcal{R}_2$ to reduce the amount of computations.

Lemma 6.9. *The sub- E^0 -bimodule of $E^1 \otimes_{E^0} E^1$ generated by the elements of the form*

$$x - \mathcal{R}_2(\mathcal{M}_2(x)) \in \ker(\mathcal{M}_2),$$

where x runs through the set of generators of $E^1 \otimes_{E^0} E^1$ as an E^0 -bimodule computed in Lemma 6.2, is the sub- E^0 -bimodule of $E^1 \otimes_{E^0} E^1$ generated by the following elements.

$$\begin{array}{lll} \beta_1^- \otimes \beta_1^-, & \beta_1^+ \otimes \beta_1^-, & \beta_{s_1}^0 \otimes \beta_1^-, \\ \beta_1^- \otimes \beta_1^+, & \beta_1^+ \otimes \beta_1^+, & \beta_{s_0}^0 \otimes \beta_1^+, \\ \beta_1^+ \otimes \beta_{s_0}^0, & \beta_{s_1}^0 \otimes \beta_{s_0}^0, & \\ \beta_1^- \otimes \beta_{s_1}^0, & \beta_{s_0}^0 \otimes \beta_{s_1}^0, & \\ \beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\text{id}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\text{id}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+, & & \\ \beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\text{id}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\text{id}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-. & & \end{array}$$

In particular, all the above elements lie in $\ker(\mathcal{M}_2)$.

Proof. Let us look at the generators of $E^1 \otimes_{E^0} E^1$ as an E^0 -bimodule computed in Lemma 6.2. From the definition of $\mathcal{R}_2$ (Lemma 6.3), we immediately see that some of these lie in the image of $\mathcal{R}_2$, and so we can discard them immediately, because if x is one of these elements then $x - \mathcal{R}_2(\mathcal{M}_2(x)) = 0$. We are left with the following elements:

$$\begin{array}{llll} \beta_1^- \otimes \beta_1^-, & \beta_1^+ \otimes \beta_1^-, & // // // // & \beta_{s_1}^0 \otimes \beta_1^-, \\ \beta_1^- \otimes \beta_1^+, & \beta_1^+ \otimes \beta_1^+, & \beta_{s_0}^0 \otimes \beta_1^+, & // // // // \\ // // // // & \beta_1^+ \otimes \beta_{s_0}^0, & \beta_{s_0}^0 \otimes \beta_{s_0}^0, & \beta_{s_1}^0 \otimes \beta_{s_0}^0, \\ \beta_1^- \otimes \beta_{s_1}^0, & // // // // & \beta_{s_0}^0 \otimes \beta_{s_1}^0, & \beta_{s_1}^0 \otimes \beta_{s_1}^0. \end{array}$$

We consider these remaining elements.

- The elements $\beta_1^- \otimes \beta_1^-, \beta_1^+ \otimes \beta_1^-, \beta_1^- \otimes \beta_1^+$ and $\beta_1^+ \otimes \beta_1^+$ are all in the kernel of $\mathcal{M}_2$: indeed products are cup products by (11), and then trivially $\beta_1^- \cdot \beta_1^-$ and $\beta_1^+ \cdot \beta_1^+$ are both zero; moreover, the fact that $\beta_1^+ \smile \beta_1^-$ and $\beta_1^- \smile \beta_1^+$ are both zero can be shown with a simple computation using Poincaré duality (see [OS22, Example 4.6]).

In particular, if x is one of the above four elements, then, trivially,

$$x - \mathcal{R}_2(\mathcal{M}_2(x)) = x.$$

- Now let us consider the four elements $\beta_{s_1}^0 \otimes \beta_1^-, \beta_{s_0}^0 \otimes \beta_1^+, \beta_1^+ \otimes \beta_{s_0}^0$ and $\beta_1^- \otimes \beta_{s_1}^0$. To compute the product, one can use the formula (11) relating cup product and (opposite of the) Yoneda product. But then we see that all such products are zero, because

$$\begin{aligned}\tau_{s_0} \cdot \beta_1^+ &= 0, & \beta_1^+ \cdot \tau_{s_0} &= 0, \\ \tau_{s_1} \cdot \beta_1^- &= 0, & \beta_1^- \cdot \tau_{s_1} &= 0\end{aligned}$$

(see formulas (58) and (59)).

So, if x is one of the above four elements, one has $x - \mathcal{R}_2(\mathcal{M}_2(x)) = x$.

- Now let us consider the two elements $\beta_{s_1}^0 \otimes \beta_{s_0}^0$ and $\beta_{s_1}^0 \otimes \beta_{s_0}^0$. We compute the first product using the formula (11) relating cup product and (opposite of the) Yoneda product, and the formulas (58) and (59) for the action of E^0 on E^1 (the other product can be computed exactly in the same way, or alternatively one can use Γ_{ϖ} or $\mathcal{J}$):

$$\begin{aligned}\beta_{s_1}^0 \cdot \beta_{s_0}^0 &= (\beta_{s_1}^0 \cdot \tau_{s_0}) \cup (\tau_{s_1} \cdot \beta_{s_0}^0) \\ &= \beta_{s_1 s_0}^0 \cup (-\beta_{s_1 s_0}^0) \\ &= 0.\end{aligned}$$

So, if x is one of the above two elements, one has $x - \mathcal{R}_2(\mathcal{M}_2(x)) = x$.

- It remains to consider the two elements $\beta_{s_0}^0 \otimes \beta_{s_0}^0$ and $\beta_{s_1}^0 \otimes \beta_{s_1}^0$; we start with the first one and then we use Γ_{ϖ} for the second one. In the end of the proof of [OS22, Proposition 9.5] the following formula is computed:

$$\mathbf{x}_0 \cdot \mathbf{x}_0 = e_1 \cdot \alpha_{s_0}^*,$$

where $\mathbf{x}_0$ is defined as

$$\mathbf{x}_0 := -\beta_{s_0}^0 - e_{\underline{\text{id}}-1} \beta_1^-$$

(see [OS22, Lemma 4.17 and the subsequent lines]) and $\alpha_{s_0}^*$ is a certain element of E^2 (defined in [OS22, Equation (123)]) with the property that

$$\alpha_{s_0}^{0,*} + \alpha_{s_0}^0 \in e_{\{\underline{\text{id}}, \underline{\text{id}}-1\}} E^2$$

(see [OS22, Equation (124)]). Therefore, we deduce that

$$\begin{aligned}-e_1 \cdot \alpha_{s_0}^0 &= (-\beta_{s_0}^0 - e_{\underline{\text{id}}-1} \cdot \beta_1^-) \cdot (-\beta_{s_0}^0 - e_{\underline{\text{id}}-1} \cdot \beta_1^-) \\ &= \beta_{s_0}^0 \cdot \beta_{s_0}^0 + e_{\underline{\text{id}}-1} \cdot \beta_1^- \cdot \beta_{s_0}^0 + \beta_{s_0}^0 \cdot e_{\underline{\text{id}}-1} \cdot \beta_1^- \\ &\quad + e_{\underline{\text{id}}-1} \cdot \beta_1^- \cdot e_{\underline{\text{id}}-1} \cdot \beta_1^- \\ &= \beta_{s_0}^0 \cdot \beta_{s_0}^0 + e_{\underline{\text{id}}-1} \cdot \beta_1^- \cdot \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \cdot \beta_1^- \\ &\quad + e_{\underline{\text{id}}-1} \cdot e_{\underline{\text{id}}-3} \cdot \beta_1^- \cdot \beta_1^- \\ &= \beta_{s_0}^0 \cdot \beta_{s_0}^0 + e_{\underline{\text{id}}-1} \cdot \alpha_{s_0}^+ - e_{\underline{\text{id}}} \cdot \alpha_{s_0}^-\end{aligned}$$

(here we have used the behaviour of the left and right action of the idempotents (57); moreover, in the last step one can compute products explicitly, but actually we have already computed them – see the definition of $\mathcal{R}_2$ in Lemma 6.3). Now we can compute $\mathcal{R}_2(\beta_{s_0}^0 \cdot \beta_{s_0}^0)$:

$$\begin{aligned}\mathcal{R}_2(\beta_{s_0}^0 \cdot \beta_{s_0}^0) &= \mathcal{R}_2(-e_{\underline{\text{id}}^{-1}} \cdot \alpha_{s_0}^+ + e_{\underline{\text{id}}} \cdot \alpha_{s_0}^- - e_1 \cdot \alpha_{s_0}^0) \\ &= -e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 - e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- + e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+\end{aligned}$$

(here we have used that $\mathcal{R}_2$ is a homomorphism of left E^0 -modules, by Lemma 6.4). Hence, the value of $x - \mathcal{R}_2(\mathcal{M}_2(x))$ for $x = \beta_{s_0}^0 \otimes \beta_{s_0}^0$ is

$$\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+.$$

Now it remains to compute the value of $x - \mathcal{R}_2(\mathcal{M}_2(x))$ for $x = \beta_{s_1}^0 \otimes \beta_{s_1}^0$, but since $\Gamma_{\varpi}(\beta_{s_0}^0) = -\beta_{s_1}^0$ and since $\mathcal{R}_2$ is Γ_{ϖ} -invariant (Lemma 6.5), we see that such value can be obtained by applying Γ_{ϖ} to the last displayed equality. Hence we get

$$\beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-$$

(using the formulas for the action of Γ_{ϖ} on E^0 (54) and on E^1 (65)). $\square$

Remark 6.10. Let us define K_2 as the sub- E^0 -bimodule of $E^1 \otimes_{E^0} E^1$ generated by the following elements:

$$\begin{array}{lll}\beta_1^- \otimes \beta_1^-, & \beta_1^+ \otimes \beta_1^-, & \beta_{s_1}^0 \otimes \beta_1^-, \\ \beta_1^- \otimes \beta_1^+, & \beta_1^+ \otimes \beta_1^+, & \beta_{s_0}^0 \otimes \beta_1^+, \\ \beta_1^+ \otimes \beta_{s_0}^0, & \beta_{s_1}^0 \otimes \beta_{s_0}^0, & \\ \beta_1^- \otimes \beta_{s_1}^0, & \beta_{s_0}^0 \otimes \beta_{s_1}^0, & \\ \beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+, & & \\ \beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-, & & \\ \beta_{s_0}^+ \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_{s_0}^0 = -\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0}, & & \\ \beta_{s_1}^- \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_{s_1}^+ = -\tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_1^+ \cdot \tau_{s_1}.\end{array}$$

The first twelve elements were obtained in Lemma 6.9 (in particular, they lie in $\ker(\mathcal{M}_2)$). The last two elements are slight modifications of those obtained in Lemma 6.7: more precisely, recalling the definition of c_{-1} from (35), they are respectively equal to

$$\begin{aligned}(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) \cdot \tau_{c_{-1}} - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) \cdot \tau_{c_{-1}}, \\ -(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^+) \cdot \tau_{c_{-1}} + (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^+) \cdot \tau_{c_{-1}}\end{aligned}$$

(in particular, they lie in $\ker(\mathcal{M}_2)$, too, since $\mathcal{J}$ and $\mathcal{M}_2$ commute by (85)).

We want to prove that K_2 is actually the full $\ker(\mathcal{R}_2)$. Let us start with some lemmas.

Lemma 6.11. *One has that K_2 is Γ_ϖ -invariant and $\mathcal{J}$ -invariant.*

Proof. It suffices to prove that the generators listed in the definition of K_2 (Remark 6.10) are Γ_ϖ -invariant and $\mathcal{J}$ -invariant. From the formulas for the action of Γ_ϖ (65) and of $\mathcal{J}$ (64) on E^1 , it is immediate to see that applying Γ_ϖ or $\mathcal{J}$ to each of the first ten generators we get, up to a sign, again one of such generators. The same is true for the last two generators. It remains to study the behaviour of Γ_ϖ and $\mathcal{J}$ on the following two elements:

$$\begin{aligned} x_0 &:= \beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+, \\ x_1 &:= \beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-. \end{aligned}$$

In the proof of Lemma 6.9, the element x_1 was obtained by applying Γ_ϖ to x_0 : in other words $\Gamma_\varpi(x_0) = x_1$ and hence $\Gamma_\varpi(x_1) = x_0$. Now let us compute $\mathcal{J}(x_0)$, using the formula (64) for the action of $\mathcal{J}$ on E^1 and the formula (57) for the action of the idempotents on E^1 :

$$\begin{aligned} \mathcal{J}(x_0) &= \mathcal{J}(\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+) \\ &= -\beta_{s_0^{-1}}^0 \otimes \beta_{s_0^{-1}}^0 + \beta_{s_0^{-1}}^0 \otimes \beta_1^- \cdot e_{\underline{\text{id}}} + \beta_1^- \otimes \beta_{s_0^{-1}}^0 \cdot e_{\underline{\text{id}}^{-1}} - \beta_{s_0^{-1}}^- \otimes \beta_1^- \cdot e_1 \\ &= -\beta_{s_0}^0 \otimes \beta_{s_0}^0 + \beta_{s_0^{-1}}^0 \otimes e_{\underline{\text{id}}^{-1}} \beta_1^- + \beta_1^- \otimes e_{\underline{\text{id}}} \beta_{s_0^{-1}}^0 - \beta_{s_0^{-1}}^- \otimes e_{\underline{\text{id}}^{-2}} \beta_1^- \\ &= -\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0^{-1}}^0 \otimes \beta_1^- + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 - e_1 \cdot \beta_{s_0^{-1}}^- \otimes \beta_1^- \\ &= -\beta_{s_0}^0 \otimes \beta_{s_0}^0 - e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+ \\ &= -x_0. \end{aligned}$$

Now it remains to treat x_1 : we have already recalled that $x_1 = \Gamma_\varpi(x_0)$. We can use the fact that Γ_ϖ and $\mathcal{J}$ commute (on E^* , as recalled in (38), and hence also on $T_{E^0}^* E^1$), getting that

$$\mathcal{J}(x_1) = \mathcal{J}(\Gamma_\varpi(x_0)) = \Gamma_\varpi(\mathcal{J}(x_0)) = \Gamma_\varpi(-x_0) = -x_1. \quad \square$$

Lemma 6.12. *The two composite maps*

$$\begin{aligned} E^2 &\xrightarrow{\mathcal{R}_2} E^1 \otimes_{E^0} E^1 \xrightarrow{\mathcal{J}} E^1 \otimes_{E^0} E^1 \xrightarrow{\text{quot.}} (E^1 \otimes_{E^0} E^1)/K_2, \\ E^2 &\xrightarrow{\mathcal{J}} E^2 \xrightarrow{\mathcal{R}_2} E^1 \otimes_{E^0} E^1 \xrightarrow{\text{quot.}} (E^1 \otimes_{E^0} E^1)/K_2 \end{aligned}$$

coincide.

Proof. By Lemma 6.6 the two maps coincide on $F^1 E^2$, and by Remark 6.10 they also coincide at α_1^- and at α_1^+ . For $\omega \in T^0/T^1$, both maps transform left multiplication by τ_ω into right multiplication by $\tau_{\omega^{-1}}$ by Lemma 6.4, and so we conclude that the two maps coincide on the whole E^2 . $\square$

Lemma 6.13. *One has that the composite map*

$$E^2 \xrightarrow{\mathcal{R}_2} E^1 \otimes_{E^0} E^1 \xrightarrow{\text{quot. map}} (E^1 \otimes_{E^0} E^1)/K_2$$

is a homomorphism of E^0 -bimodules.

Proof. We will show that the following equalities are true:

- (i) $\mathcal{R}_2(\tau_{s_0} \cdot \alpha_{s_1 v}^\sigma) \equiv \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_1 v}^\sigma)$ modulo K_2 for $v \in \widetilde{W}$ with $\ell(s_1 v) = \ell(v) + 1$ and for $\sigma \in \{-, 0, +\}$ (we will see that in this case we actually have a true equality in $E^1 \otimes_{E^0} E^1$, with no need to consider the quotient modulo K_2);
- (ii) $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^\sigma) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^\sigma)$ modulo K_2 for $v \in \widetilde{W}$ with $\ell(s_1 v) = \ell(v) + 1$ and for $\sigma \in \{-, 0, +\}$;
- (iii) $\mathcal{R}_2(\tau_{s_i} \cdot \alpha_1^+) \equiv \tau_{s_i} \cdot \mathcal{R}_2(\alpha_1^+)$ modulo K_2 for $i \in \{0, 1\}$.

Before checking these three properties, let us show that, if they hold, then the lemma is proved. We saw in Lemma 6.5 that Γ_ϖ commutes with $\mathcal{R}_2$ and in Lemma 6.11 that K_2 is Γ_ϖ -invariant, and so by applying Γ_ϖ to the equalities in (i), (ii) and (iii) (and using (54) and (73)), we get:

- (i') $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_0 w}^\sigma) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_0 w}^\sigma) \pmod{K_2}$ for $w \in \widetilde{W}$ with $\ell(s_0 w) = \ell(w) + 1$ and for $\sigma \in \{-, 0, +\}$ (as before, we already have equality in $E^1 \otimes_{E^0} E^1$);
- (ii') $\mathcal{R}_2(\tau_{s_0} \cdot \alpha_{s_0 w}^\sigma) \equiv \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0 w}^\sigma) \pmod{K_2}$ for $w \in \widetilde{W}$ with $\ell(s_0 w) = \ell(w) + 1$ and for $\sigma \in \{-, 0, +\}$;
- (iii') $\mathcal{R}_2(\tau_{s_i} \cdot \alpha_1^-) \equiv \tau_{s_i} \cdot \mathcal{R}_2(\alpha_1^-) \pmod{K_2}$ for $i \in \{0, 1\}$.

Note that, for $\omega \in T^0/T^1$, in (iii) and (iii') we can consider the analogous congruences with α_ω^+ (respectively, of α_ω^-) in place of α_1^+ (respectively, of α_1^-): the new congruences are still true because $\mathcal{R}_2$ is a homomorphism of left $k[T^0/T^1]$ -modules (by Lemma 6.4, or just by the definition of $\mathcal{R}_2$ in Lemma 6.3).

All in all, this shows that the congruence

$$\mathcal{R}_2(x \cdot \alpha) \equiv x \cdot \mathcal{R}_2(\alpha) \pmod{K_2} \quad (90)$$

is true for α running through a k -basis of E^2 and for $x \in \{\tau_{s_0}, \tau_{s_1}\}$. But since $\mathcal{R}_2$ is a homomorphism of left $k[T^0/T^1]$ -modules, the same congruence is also true for $x = \tau_\omega$ for $\omega \in T^0/T^1$. In other words (90) is true for α running through a k -basis of E^2 and for x running through a set of generators of E^0 as a k -algebra, and hence it follows that it must be true for all $\alpha \in E^2$ and all $x \in E^0$, completing the proof that $\mathcal{R}_2$ becomes a homomorphism of left E^0 -modules after modding out K_2 .

To prove the same claim for the right E^0 -action, since K_2 is $\mathcal{J}$ -invariant by Lemma 6.11, applying $\mathcal{J}$ to (90) we obtain that

$$(\mathcal{J} \circ \mathcal{R}_2)(x \cdot \alpha) \equiv (\mathcal{J} \circ \mathcal{R}_2)(\alpha) \cdot \mathcal{J}(x) \pmod{K_2}$$

for all $x \in E^0$ and all $\alpha \in E^2$. Since the maps $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ coincide after modding out by K_2 (Lemma 6.12), we deduce that

$$\mathcal{R}_2(\mathcal{J}(\alpha) \cdot \mathcal{J}(x)) \equiv \mathcal{R}_2(\mathcal{J}(\alpha)) \cdot \mathcal{J}(x) \pmod{K_2},$$

completing the proof that $\mathcal{R}_2$ becomes a homomorphism of right E^0 -modules after modding out K_2 .

Now, it remains to prove (i), (ii) and (iii).

(i) One has

$$\begin{aligned}
\tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_1 v}^-) &= -\tau_{s_0} \cdot \beta_1^+ \otimes \beta_{s_1 v}^0 \\
&= 0 && \text{by (58)} \\
&= \mathcal{R}_2(\tau_{s_0} \cdot \alpha_{s_1 v}^-) && \text{by (69)}.
\end{aligned}$$

Moreover,

$$\begin{aligned}
\tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_1 v}^0) &= \tau_{s_0} \cdot \beta_1^+ \otimes \beta_{s_1 v}^- \\
&= 0 && \text{by (58)} \\
&= \mathcal{R}_2(\tau_{s_0} \cdot \alpha_{s_1 v}^0) && \text{by (69)}.
\end{aligned}$$

And finally,

$$\begin{aligned}
\tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_1 v}^+) &= \tau_{s_0} \cdot \beta_{s_1}^0 \otimes \beta_v^+ \\
&= -\beta_{s_0 s_1}^0 \otimes \beta_v^+ && \text{by (58)} \\
&= \beta_{s_0}^0 \otimes \beta_{s_1 v}^- && \text{by (59) and (58)} \\
&= -\mathcal{R}_2(\alpha_{s_0 s_1 v}^-) \\
&= \mathcal{R}_2(\tau_{s_0} \cdot \alpha_{s_1 v}^+) && \text{by (69)}.
\end{aligned}$$

(ii-a) Let us prove that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^-) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^-)$ modulo K_2 : we first assume that $\ell(v) \geq 1$, and compute

$$\begin{aligned}
\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^-) &= -e_1 \mathcal{R}_2(\alpha_{s_1 v}^-) - \mathcal{R}_2(\alpha_{c-1 v}^+) \\
&&& \text{by (71) and Lemma 6.4} \\
&= e_1 \beta_1^+ \otimes \beta_{s_1 v}^0 - \beta_1^- \otimes \beta_{c-1 v}^0,
\end{aligned}$$

and

$$\begin{aligned}
\tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^-) &= -\tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1 v}^0 \\
&= \tau_{s_1} \cdot \beta_{s_1}^+ \otimes \beta_v^0 \\
&&& \text{by (58) and (59)} \\
&= -e_1 \beta_{s_1}^+ \otimes \beta_v^0 + 2e_{\underline{\text{id}}-1} \beta_{s_1}^0 \otimes \beta_v^0 \\
&\quad + e_{\underline{\text{id}}-2} \beta_{s_1}^- \otimes \beta_v^0 - \beta_{c-1}^- \otimes \beta_v^0 \\
&&& \text{by (61)} \\
&= e_1 \beta_1^+ \otimes \beta_{s_1 v}^0 + 2e_{\underline{\text{id}}-1} \beta_{s_1}^0 \otimes \beta_{s_0}^0 \cdot \tau_{s_0^{-1} v} \\
&\quad - e_{\underline{\text{id}}-2} \tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_0}^0 \cdot \tau_{s_0^{-1} v} - \beta_1^- \otimes \beta_{c-1 v}^0 \\
&&& \text{by (58), (59), (55) and (56)}.
\end{aligned}$$

Since both $\beta_{s_1}^0 \otimes \beta_{s_0}^0$ and $\beta_1^+ \otimes \beta_{s_0}^0$ lie in the list of generators defining K_2 , we conclude that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^-) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^-)$ modulo K_2 .

We now consider the case $\ell(v) = 0$: by definition of $\mathcal{R}_2$ we have

$$\mathcal{R}_2(\alpha_{c_{-1}v}^+) = \mathcal{R}_2(\alpha_{c_{-1}v}^+ + \tau_{s_1} \cdot \alpha_{s_1v}^-) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1v}^-),$$

and then the claimed congruence is actually an equality in $E^1 \otimes_{E^0} E^1$ by k -linearity of $\mathcal{R}_2$.

(ii-b) Let us prove that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1v}^0) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1v}^0)$ modulo K_2 : we compute

$$\begin{aligned} \mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1v}^0) &= \begin{cases} -e_1 \mathcal{R}_2(\alpha_{s_1v}^0) - 2e_{\underline{\text{id}}-1} \mathcal{R}_2(\alpha_{s_1v}^+) & \text{if } \ell(v) \geq 1 \\ -\mathcal{R}_2(\alpha_{c_{-1}v}^0) & \\ -e_1 \mathcal{R}_2(\alpha_{s_1v}^0) - 2e_{\underline{\text{id}}-1} \mathcal{R}_2(\alpha_{s_1v}^+) & \text{if } \ell(v) = 0 \end{cases} \\ &\quad \text{by (71) and Lemma 6.4} \\ &= \begin{cases} -e_1 \beta_1^+ \otimes \beta_{s_1v}^- - 2e_{\underline{\text{id}}-1} \beta_{s_1}^0 \otimes \beta_v^+ & \text{if } \ell(v) \geq 1 \\ +\beta_1^- \otimes \beta_{c_{-1}v}^+ & \\ -e_1 \beta_1^+ \otimes \beta_{s_1v}^- - 2e_{\underline{\text{id}}-1} \beta_{s_1}^0 \otimes \beta_v^+ & \text{if } \ell(v) = 0, \end{cases} \end{aligned}$$

and

$$\begin{aligned} \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1v}^0) &= \tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1v}^- \\ &= -\tau_{s_1} \cdot \beta_{s_1}^+ \otimes \beta_v^+ \\ &\quad \text{by (58) and (59)} \\ &= e_1 \beta_{s_1}^+ \otimes \beta_v^+ - 2e_{\underline{\text{id}}-1} \beta_{s_1}^0 \otimes \beta_v^+ \\ &\quad - e_{\underline{\text{id}}-2} \beta_{s_1}^- \otimes \beta_v^+ + \beta_{c_{-1}}^- \otimes \beta_v^+ \\ &\quad \text{by (61)} \\ &= -e_1 \beta_1^+ \otimes \beta_{s_1v}^- - 2e_{\underline{\text{id}}-1} \beta_{s_1}^0 \otimes \beta_v^+ \\ &\quad - e_{\underline{\text{id}}-2} \beta_{s_1}^- \otimes \beta_v^+ + \beta_1^- \otimes \beta_{c_{-1}v}^+ \\ &\quad \text{by (58), (59), (55) and (56).} \end{aligned}$$

Now, if $\ell(v) \geq 1$, then using (58) and (59) we see that

$$\beta_{s_1}^- \otimes \beta_v^+ = -(\beta_{s_1}^- \tau_{s_0}) \otimes \beta_{s_0^{-1}v}^- = 0,$$

and hence we conclude that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1v}^0) = \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1v}^0)$.

If instead $\ell(v) = 0$, then using (58) and (56) we see that

$$\begin{aligned} \beta_{s_1}^- \otimes \beta_v^+ &= -\tau_{s_1} \cdot \beta_1^+ \otimes \beta_1^+ \cdot \tau_v \in K_2, \\ \beta_1^- \otimes \beta_{c_{-1}v}^+ &= \beta_1^- \otimes \beta_1^+ \cdot \tau_{c_{-1}v} \in K_2, \end{aligned}$$

and hence we conclude that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1v}^0) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1v}^0)$ modulo K_2 .

(ii-c) Let us prove that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^+) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^+)$ modulo K_2 : we compute

$$\begin{aligned} \mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^+) &= -\mathcal{R}_2(e_1 \alpha_{s_1 v}^+) && \text{by (71)} \\ &= -e_1 \mathcal{R}_2(\alpha_{s_1 v}^+) && \text{by Lemma 6.4} \\ &= -e_1 \beta_{s_1}^0 \otimes \beta_v^+, \end{aligned}$$

and

$$\begin{aligned} \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^+) &= \tau_{s_1} \cdot \beta_{s_1}^0 \otimes \beta_v^+ \\ &= -e_1 \beta_{s_1}^0 \otimes \beta_v^+ - e_{\underline{\text{id}}^{-1}} \beta_{s_1}^- \otimes \beta_v^+ && \text{by (61)}. \end{aligned}$$

If $\ell(v) \geq 1$, we can write v as $s_0 v'$ for some $v' \in \widetilde{W}$ such that lengths add up. Using formulas (58) and (59), we obtain

$$\beta_{s_1}^- \otimes \beta_v^+ = -(\beta_{s_1}^- \cdot \tau_{s_0}) \otimes \beta_v^- = 0.$$

If instead $\ell(v) = 0$, using formulas (58) and (56), we obtain

$$-e_{\underline{\text{id}}^{-1}} \beta_{s_1}^- \otimes \beta_v^+ = e_{\underline{\text{id}}^{-1}} \tau_{s_1} \cdot \beta_1^+ \otimes \beta_1^+ \cdot \tau_v \in K_2.$$

Therefore, both in the case $\ell(v) \geq 1$ and in the case $\ell(v) = 0$, we obtain that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1 v}^+) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1 v}^+)$ modulo K_2 .

(iii-a) Let us prove that $\mathcal{R}_2(\tau_{s_1} \cdot \alpha_1^+) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha_1^+)$ modulo K_2 : we compute

$$\begin{aligned} \tau_{s_1} \cdot \mathcal{R}_2(\alpha_1^+) &= \tau_{s_1} \cdot \left(\mathcal{R}_2(\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^-) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}}^-) \right) \\ &\equiv \mathcal{R}_2(\tau_{s_1} \cdot (\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^-)) - \tau_{s_1}^2 \cdot \mathcal{R}_2(\alpha_{s_1^{-1}}^-) \pmod{K_2} \\ &\quad \text{by (ii), since } \alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^- \in \bigoplus_{\omega \in T^0/T^1} H^2(I, \mathbf{X}(s_1 \omega)) \\ &\equiv \mathcal{R}_2(\tau_{s_1} \cdot (\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^-)) - \mathcal{R}_2(\tau_{s_1}^2 \cdot \alpha_{s_1^{-1}}^-) \pmod{K_2} \\ &\quad \text{again by (ii)} \\ &= \mathcal{R}_2(\tau_{s_1} \cdot \alpha_1^+). \end{aligned}$$

(iii-b) Let us prove that $\mathcal{R}_2(\tau_{s_0} \cdot \alpha_1^+) \equiv \tau_{s_0} \cdot \mathcal{R}_2(\alpha_1^+)$ modulo K_2 . Since K_2 is $\mathcal{J}$ -invariant, this is equivalent to showing that

$$(\mathcal{J} \circ \mathcal{R}_2)(\tau_{s_0} \cdot \alpha_1^+) \equiv (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^+) \cdot \tau_{s_0}^{-1} \pmod{K_2}.$$

Recall from Lemma 6.12 that the maps $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ coincide after post-composing with the quotient map onto $(E^1 \otimes_{E^0} E^1)/K_2$. Therefore our claim is equivalent to showing that

$$(\mathcal{R}_2 \circ \mathcal{J})(\tau_{s_0} \cdot \alpha_1^+) \equiv (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^+) \cdot \tau_{s_0}^{-1} \pmod{K_2}.$$

I.e., using the formula (72) for the action of $\mathcal{J}$ on E^2 , this is equivalent to showing that

$$\mathcal{R}_2(\alpha_1^+ \cdot \tau_{s_0}^{-1}) \equiv \mathcal{R}_2(\alpha_1^+) \cdot \tau_{s_0}^{-1} \pmod{K_2}. \quad (91)$$

By definition of $\mathcal{R}_2$, the right hand side of the above equation is

$$\mathcal{R}_2(\alpha_1^+) \cdot \tau_{s_0^{-1}} = \mathcal{R}_2(\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^-) \cdot \tau_{s_0^{-1}} - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}}^-) \cdot \tau_{s_0^{-1}}. \quad (92)$$

From (i) we know that

$$\tau_{s_0} \cdot \mathcal{R}_2(\alpha) = \mathcal{R}_2(\tau_{s_0} \cdot \alpha)$$

for all $\alpha \in \oplus_{\omega \in T^0/T^1} H^2(I, \mathbf{X}(\omega s_1))$, and therefore for the same α 's we have

$$(\mathcal{J} \circ \mathcal{R}_2)(\alpha) \cdot \tau_{s_0^{-1}} = (\mathcal{J} \circ \mathcal{R}_2)(\tau_{s_0} \cdot \alpha).$$

As explained above, we can replace $\mathcal{J} \circ \mathcal{R}_2$ with $\mathcal{R}_2 \circ \mathcal{J}$ if we content ourselves with a congruence modulo K_2 . As the subspace $\oplus_{\omega \in T^0/T^1} H^2(I, \mathbf{X}(\omega s_1))$ is $\mathcal{J}$ -invariant, we then obtain

$$\mathcal{R}_2(\alpha) \cdot \tau_{s_0^{-1}} \equiv \mathcal{R}_2(\alpha \cdot \tau_{s_0^{-1}}) \pmod{K_2}$$

for all $\alpha \in \oplus_{\omega \in T^0/T^1} H^2(I, \mathbf{X}(\omega s_1))$. Since both $\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^-$ and $\alpha_{s_1^{-1}}^-$ lie in such subspace, applying this latter fact to (92) we obtain

$$\begin{aligned} \mathcal{R}_2(\alpha_1^+) \cdot \tau_{s_0^{-1}} &= \mathcal{R}_2(\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^-) \cdot \tau_{s_0^{-1}} \\ &\quad - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}}^-) \cdot \tau_{s_0^{-1}} \\ &\equiv \mathcal{R}_2(\alpha_1^+ \cdot \tau_{s_0^{-1}} + \tau_{s_1} \cdot \alpha_{s_1^{-1}}^- \cdot \tau_{s_0^{-1}}) \\ &\quad - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}}^- \cdot \tau_{s_0^{-1}}) \pmod{K_2}. \end{aligned} \quad (93)$$

Now, since $\alpha_{s_1^{-1}}^- \cdot \tau_{s_0^{-1}}$ lies in $H^2(I, \mathbf{X}(s_1 s_0))$, by (ii) we have that

$$\tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1}}^- \cdot \tau_{s_0^{-1}}) \equiv \mathcal{R}_2(\tau_{s_1} \cdot \alpha_{s_1^{-1}}^- \cdot \tau_{s_0^{-1}}) \pmod{K_2}.$$

Therefore, continuing the computation in (93), we obtain

$$\mathcal{R}_2(\alpha_1^+) \cdot \tau_{s_0^{-1}} \equiv \mathcal{R}_2(\alpha_1^+ \cdot \tau_{s_0^{-1}}) \pmod{K_2},$$

as we wanted to show in (91). $\square$

Proposition 6.14. *The kernel of the degree 2 multiplication map*

$$\mathcal{M}_2: T_{E^0}^2 E^1 = E^1 \otimes_{E^0} E^1 \longrightarrow E^2$$

is K_2 (defined in Remark 6.10).

Proof. We consider the maps

$$(E^1 \otimes_{E^0} E^1)/K_2 \xrightleftharpoons[\overline{\mathcal{R}_2}]{\overline{\mathcal{M}_2}} E^2,$$

induced by $\mathcal{M}_2$ and $\mathcal{R}_2$ (note that $\overline{\mathcal{M}_2}$ is well defined because in Remark 6.10 we have observed that $K_2 \subseteq \ker(\mathcal{M}_2)$).

To prove the proposition it suffices to show that $\overline{\mathcal{R}_2} \circ \overline{\mathcal{M}_2} = \text{id}_{(E^1 \otimes_{E^0} E^1)/K_2}$: this can be checked on a set of generators of $E^1 \otimes_{E^0} E^1$ as an E^0 -bimodule, since Lemma 6.13 states that $\overline{\mathcal{R}_2}$ is a homomorphism of E^0 -bimodules: then the claim is clear from Lemma 6.9 and the definition of K_2 . $\square$

6.5 The 3rd graded piece of the kernel

To study the kernel of the multiplication map $\mathcal{M}_3: T_{E^0}^3 E^1 \rightarrow E^3$, we follow the same strategy as for the kernel of $\mathcal{M}_2$. Since E^3 admits a somewhat simpler basis than E^2 , some things will be easier.

Lemma 6.15. *The multiplication map $\mathcal{M}_3: T_{E^0}^3 E^1 \rightarrow E^3$ is surjective, and the following is a section of it as a homomorphism of k -vector spaces.*

$$\begin{aligned} \mathcal{R}_3: \quad E^3 &\longrightarrow T_{E^0}^3 E^1 \\ \phi_{(s_1 s_0)^i \omega} &\longmapsto -\beta_1^+ \otimes \beta_{(s_1 s_0)^i}^0 \otimes \beta_1^- \cdot \tau_\omega && \text{for } i \in \mathbb{Z}_{\geq 1}, \omega \in T^0/T^1, \\ \phi_{(s_0 s_1)^i \omega} &\longmapsto \beta_1^- \otimes \beta_{(s_0 s_1)^i}^0 \otimes \beta_1^+ \cdot \tau_\omega && \text{for } i \in \mathbb{Z}_{\geq 1}, \omega \in T^0/T^1, \\ \phi_{s_0(s_1 s_0)^i \omega} &\longmapsto -\beta_1^- \otimes \beta_{s_0(s_1 s_0)^i}^0 \otimes \beta_1^- \cdot \tau_\omega && \text{for } i \in \mathbb{Z}_{\geq 0}, \omega \in T^0/T^1, \\ \phi_{s_1(s_0 s_1)^i \omega} &\longmapsto \beta_1^+ \otimes \beta_{s_1(s_0 s_1)^i}^0 \otimes \beta_1^+ \cdot \tau_\omega && \text{for } i \in \mathbb{Z}_{\geq 0}, \omega \in T^0/T^1, \\ \phi_\omega &\longmapsto (\tau_{s_0} + e_1) \cdot \mathcal{R}_3(\phi_{s_0^{-1} \omega}) && \text{for } \omega \in T^0/T^1. \end{aligned}$$

It can also be rewritten as

$$\begin{aligned} \mathcal{R}_3: \quad E^3 &\longrightarrow T_{E^0}^3 E^1 \\ \phi_{s_1 v} &\longmapsto \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_v^+ && \text{if } \ell(s_1 v) = \ell(v) + 1, \\ \phi_{s_0 w} &\longmapsto -\beta_1^- \otimes \beta_{s_0}^0 \otimes \beta_w^- && \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \phi_\omega &\longmapsto (\tau_{s_0} + e_1) \cdot \mathcal{R}_3(\phi_{s_0^{-1} \omega}) && \text{for } \omega \in T^0/T^1. \end{aligned}$$

Moreover, $\mathcal{R}_3$ is a homomorphism of $k[T^0/T^1]$ -bimodules. Finally, defining

$$F^1 E^3 := \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \geq 1}} H^3(I, \mathbf{X}(w)),$$

one has that the following diagrams are commutative:

$$\begin{array}{ccc} F^1 E^3 & \xrightarrow{\mathcal{R}_3|_{F^1 E^3}} & T_{E^0}^3 E^1 \\ \Gamma_\varpi \downarrow & & \downarrow \Gamma_\varpi \\ F^1 E^3 & \xrightarrow{\mathcal{R}_3|_{F^1 E^3}} & T_{E^0}^3 E^1, \end{array} \quad \begin{array}{ccc} F^1 E^3 & \xrightarrow{\mathcal{R}_3|_{F^1 E^3}} & T_{E^0}^3 E^1 \\ \mathcal{J} \downarrow & \begin{array}{c} \beta \otimes \beta' \\ \downarrow \\ -\mathcal{J}(\beta') \otimes \mathcal{J}(\beta) \end{array} & \downarrow \mathcal{J} \\ F^1 E^3 & \xrightarrow{\mathcal{R}_3|_{F^1 E^3}} & T_{E^0}^3 E^1. \end{array}$$

Note the last line in each of the definitions of $\mathcal{R}_3$ makes sense because $\mathcal{R}_3(\phi_{s_0^{-1} \omega})$ is already defined lines before.

Proof. Let us first check that $\mathcal{R}_3$, defined in the first way, is a section of $\mathcal{M}_3$ (and hence, in particular, $\mathcal{M}_3$ is surjective). Using the computations (28), (29), (30) and (31) in the proof of Proposition 4.8, one obtains

$$\begin{aligned}\beta_1^- \cdot \beta_{s_0(s_1 s_0)^i}^0 \cdot \beta_1^- &= -\beta_{s_0(s_1 s_0)^i}^- \cup \beta_{s_0(s_1 s_0)^i}^0 \cup \beta_{s_0(s_1 s_0)^i}^+, \\ \beta_1^+ \cdot \beta_{s_1(s_0 s_1)^i}^0 \cdot \beta_1^+ &= -\beta_{s_1(s_0 s_1)^i}^+ \cup \beta_{s_1(s_0 s_1)^i}^0 \cup \beta_{s_1(s_0 s_1)^i}^-, \\ \beta_1^- \cdot \beta_{(s_0 s_1)^i}^0 \cdot \beta_1^+ &= \beta_{(s_0 s_1)^i}^- \cup \beta_{(s_0 s_1)^i}^0 \cup \beta_{(s_0 s_1)^i}^+, \\ \beta_1^+ \cdot \beta_{(s_1 s_0)^i}^0 \cdot \beta_1^- &= \beta_{(s_1 s_0)^i}^+ \cup \beta_{(s_1 s_0)^i}^0 \cup \beta_{(s_1 s_0)^i}^-.\end{aligned}$$

Recalling from (45) that $\phi_w = \beta_w^- \cup \beta_w^0 \cup \beta_w^+$ for all $w \in \widetilde{W}$ such that $\ell(w) \geq 1$, we see that $\mathcal{M}_3 \circ \mathcal{R}_3$ is the identity map on $F^1 E^3$. For the last line in the definition of $\mathcal{R}_3$ one uses instead the formula $(\tau_{s_0} + e_1) \cdot \phi_{s_0^{-1}} = \phi_1$ (immediate from (74)), and so we conclude that $\mathcal{R}_3$ is indeed a section of $\mathcal{M}_3$.

The claim about the second description of $\mathcal{R}_3$ follows from the formulas of Lemma 6.1: for example, for all $i \in \mathbb{Z}_{\geq 1}$ and all $\omega \in T^0/T^1$, we have

$$\begin{aligned}-\beta_1^+ \otimes \beta_{(s_1 s_0)^i}^0 \otimes \beta_1^- \cdot \tau_\omega &= -\beta_1^+ \otimes \beta_{s_1}^0 \otimes (\tau_{s_0(s_1 s_0)^{i-1}} \cdot \beta_1^-) \cdot \tau_\omega \\ &= \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_{s_0(s_1 s_0)^{i-1}}^+ \cdot \tau_\omega \\ &= \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_{s_0(s_1 s_0)^{i-1}\omega}^+.\end{aligned}$$

The fact that $\mathcal{R}_3$ is a homomorphism of right $K[T^0/T^1]$ -modules is basically true by construction (using the formula $\phi_{w\omega} = \phi_w \cdot \tau_\omega$ for all $w \in \widetilde{W}$ and all $\omega \in T^0/T^1$, see (74)).

The fact that $\mathcal{R}_3$ is also a homomorphism of left $K[T^0/T^1]$ -modules can be proved exactly as in Lemma 6.4, replacing the references to the formulas involving E^2 with those involving E^3 (namely, (74)).

The fact that the restriction of $\mathcal{R}_3$ to $F^1 E^3$ commutes with $\mathcal{J}$ and Γ_ϖ can be proved in the same way as in Lemmas 6.5 and 6.6, of course replacing the references to the formulas for E^2 with the formulas for E^3 : namely, (76), (75) and (74). Actually, the first description of $\mathcal{R}_3$ makes the computations for $\mathcal{J}$ easier than the analogous proof for $\mathcal{R}_2$. $\square$

Lemma 6.16. *The map*

$$\begin{aligned}\mathcal{R}'_3: E^3 &\longrightarrow T_{E^0}^3 E^1 = E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 \\ \phi_w &\longmapsto \begin{cases} \mathcal{R}_3(\phi_w) & \text{if } \ell(w) \geq 1, \\ \frac{1}{4} \left(\mathcal{R}_3(\phi_w) + (\Gamma_\varpi \circ \mathcal{R}_3 \circ \Gamma_\varpi)(\phi_w) \right. \\ \quad \left. + (\mathcal{J} \circ \mathcal{R}_3 \circ \mathcal{J})(\phi_w) + (\Gamma_\varpi \circ \mathcal{J} \circ \mathcal{R}_3 \circ \mathcal{J} \circ \Gamma_\varpi)(\phi_w) \right) & \text{if } \ell(w) = 0. \\ \quad = \frac{1}{4} \left(\mathcal{R}_3(\phi_1) + \Gamma_\varpi(\mathcal{R}_3(\phi_1)) \right. \\ \quad \left. + \mathcal{J}(\mathcal{R}_3(\phi_1)) + \Gamma_\varpi(\mathcal{J}(\mathcal{R}_3(\phi_1))) \right) \cdot \tau_w \end{cases}\end{aligned}$$

is well defined, is a section of the multiplication map $\mathcal{M}_3$ as a homomorphism of $k[T^0/T^1]$ -bimodules and commutes with Γ_ϖ and with $\mathcal{J}$.

Proof. Let us consider

$$F^1 E^3 := \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \geq 1}} H^3(I, \mathbf{X}(w)),$$

$$F_0 E^3 := \bigoplus_{\omega \in T^0/T^1} H^3(I, \mathbf{X}(\omega)).$$

The fact that $\mathcal{R}'_3|_{F^1 E^3}$ is a homomorphism of $k[T^0/T^1]$ -bimodules, the fact that $\mathcal{M}_3 \circ \mathcal{R}'_3|_{F^1 E^3}$ is the identity and the fact that $\mathcal{R}'_3|_{F^1 E^3}$ commutes with Γ_ϖ and $\mathcal{J}$ are all clear from the previous lemma, and we now have to study what happens on $F_0 E^3$.

We will check in the end that the two definitions of $\mathcal{R}'_3$ on $F_0 E^3$ coincide, but for the moment we stick to the first definition: using that $\mathcal{M}_3 \circ \mathcal{R}_3|_{F_0 E^3}$ is the identity and that $\mathcal{M}_3$ commutes with Γ_ϖ and $\mathcal{J}$, we see that $\mathcal{M}_3 \circ \mathcal{R}'_3|_{F_0 E^3}$ is the identity. Let $\omega \in T^0/T^1$. Since $\mathcal{R}_3|_{F_0 E^3}$ is a homomorphism of $k[T^0/T^1]$ -bimodules, since Γ_ϖ transforms the left (respectively, right) action of τ_ω into the left (respectively, right) action by $\tau_{\omega^{-1}}$ and since $\mathcal{J}$ transforms the left (respectively, right) action of τ_ω into the right (respectively, left) action by $\tau_{\omega^{-1}}$, we conclude that $\mathcal{R}'_3|_{F_0 E^3}$ is a homomorphism of $k[T^0/T^1]$ -bimodules (also using (74)).

The fact that $\mathcal{R}'_3|_{F_0 E^3}$ commutes with Γ_ϖ and $\mathcal{J}$ is clear from the construction and the fact that Γ_ϖ and $\mathcal{J}$ commute by (38) (on E^* and hence on $T_{E^0}^* E^1$).

For $\omega \in T^0/T^1$, the alternative description

$$\mathcal{R}'_3(\phi_\omega) = \frac{1}{4} \left(\mathcal{R}_3(\phi_1) + \Gamma_\varpi(\mathcal{R}_3(\phi_1)) + \mathcal{J}(\mathcal{R}_3(\phi_1)) + \Gamma_\varpi(\mathcal{J}(\mathcal{R}_3(\phi_1))) \right) \cdot \tau_\omega$$

is clear from the fact that $\mathcal{R}'_3|_{F_0 E^3}$ is a homomorphism of right $k[T^0/T^1]$ -modules, together with the fact that both Γ_ϖ and $\mathcal{J}$ fix ϕ_1 (see (76) and (75)). $\square$

Remark 6.17. Using the formulas for the action of Γ_ϖ and $\mathcal{J}$ on E^1 (respectively, (65) and (64)) one readily computes explicitly the four summands in the definition of $\mathcal{R}'_3(\phi_1)$:

$$\begin{aligned} \mathcal{R}_3(\phi_1) &= -(\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-, \\ \Gamma_\varpi(\mathcal{R}_3(\phi_1)) &= (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^+, \\ \mathcal{J}(\mathcal{R}_3(\phi_1)) &= -\beta_1^- \otimes \beta_{s_0}^0 \otimes \beta_1^- \cdot (\tau_{s_0^{-1}} + e_1), \\ \Gamma_\varpi(\mathcal{J}(\mathcal{R}_3(\phi_1))) &= \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1). \end{aligned}$$

Lemma 6.18. *Let $K_{2,3}$ be the sub- E^0 -bimodule of $T_{E^0}^3 E^1$ generated by the kernel of the degree 2 multiplication map, i.e.,*

$$K_{2,3} := \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \subseteq T_{E^0}^3 E^1,$$

where $\overline{(\cdot)}$ denotes the image of $(\cdot)$ in $T_{E^0}^3 E^1$. One has the following congruences:

$$\begin{aligned}\Gamma_{\varpi}(\mathcal{J}(\mathcal{R}_3(\phi_1))) &\equiv \mathcal{R}_3(\phi_1) \pmod{K_{2,3}}, \\ \mathcal{J}(\mathcal{R}_3(\phi_1)) &\equiv \Gamma_{\varpi}(\mathcal{R}_3(\phi_1)) \pmod{K_{2,3}}.\end{aligned}$$

Proof. First of all we note that the second congruence follows from the first one, since $K_{2,3}$ is Γ_{ϖ} -invariant (which is true because the multiplication map commutes with Γ_{ϖ} , see (85)). To show the first congruence, we first compute a couple of useful equalities and congruences: we have

$$\begin{aligned}(\tau_{s_0} + e_1) \cdot \beta_1^- \cdot \tau_{s_0} &= (\tau_{s_0} + e_1) \cdot \beta_{s_0}^- \\ &= -2e_{\text{id}}\beta_{s_0}^0 + e_{\text{id}^2}\beta_{s_0}^+ - \beta_{c_{-1}}^+, \end{aligned}$$

by (59) and (60). Since both $\beta_{s_0}^0 \otimes \beta_{s_1}^0$ and $\beta_{s_0}^+ \otimes \beta_{s_1}^0 = -\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_1}^0$ lie in $\ker(\mathcal{M}_2)$ (see, e.g., Lemma 6.9 and see (60) for the claimed equality), tensoring both sides of the last equality by $\beta_{s_1}^0$ on the right, we get the congruence

$$((\tau_{s_0} + e_1) \cdot \beta_1^- \cdot \tau_{s_0}) \otimes \beta_{s_1}^0 \equiv -\beta_1^+ \otimes \beta_{s_1}^0 \pmod{\ker(\mathcal{M}_2)} \quad (94)$$

(also using the formulas for the left and right action of $\tau_{c_{-1}}$ on E^1 : see (55) and (56)). Now we apply Γ_{ϖ} to the last congruence, obtaining again a congruence since $\ker(\mathcal{M}_2)$ is Γ_{ϖ} -invariant:

$$-((\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot \tau_{s_1}) \otimes \beta_{s_0}^0 \equiv \beta_1^- \otimes \beta_{s_0}^0 \pmod{\ker(\mathcal{M}_2)},$$

where we have used the formulas for the action of Γ_{ϖ} on E^0 and E^1 (see (54) and (73)). Now we apply $\mathcal{J}$ (or rather $-\mathcal{J}$) to the last congruence, obtaining again a congruence since $\ker(\mathcal{M}_2)$ is $\mathcal{J}$ -invariant (by (85)):

$$-\mathcal{J}(\beta_{s_0}^0) \otimes \mathcal{J}((\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot \tau_{s_1}) \equiv \mathcal{J}(\beta_{s_0}^0) \otimes \mathcal{J}(\beta_1^-) \pmod{\ker(\mathcal{M}_2)},$$

i.e.,

$$\beta_{s_0}^0 \otimes (\tau_{s_1}^{-1} \cdot \beta_1^+ \cdot (\tau_{s_1}^{-1} + e_1)) \equiv -\beta_{s_0}^0 \otimes \beta_1^- \pmod{\ker(\mathcal{M}_2)},$$

using the formulas for the action of $\mathcal{J}$ on E^0 and E^1 (see (53) and (64)). Equivalently, using the formulas for the action of $\tau_{c_{-1}}$ ((55) and (56)),

$$\beta_{s_0}^0 \otimes (\tau_{s_1} \cdot \beta_1^+ \cdot (\tau_{s_1} + e_1)) \equiv -\beta_{s_0}^0 \otimes \beta_1^- \pmod{\ker(\mathcal{M}_2)}, \quad (95)$$

We now get the desired congruence $\Gamma_{\varpi}(\mathcal{J}(\mathcal{R}_3(\phi_1))) \equiv \mathcal{R}_3(\phi_1)$ modulo $K_{2,3}$, by putting together (94) and (95): indeed denoting by $\equiv$ congruences modulo $K_{2,3}$,

we have

$$\begin{aligned}
& \Gamma_{\varpi}(\mathcal{J}(\mathcal{R}_3(\phi_1))) \\
&= \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1) && \text{by Remark 6.17} \\
&= \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_1^+ \cdot \tau_{c-1} \cdot (\tau_{s_1} + e_1) \\
&= \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^+ \cdot (\tau_{s_1} + e_1) && \text{by (55) and (56)} \\
&\equiv -((\tau_{s_0} + e_1) \cdot \beta_1^- \cdot \tau_{s_0}) \otimes \beta_{s_1}^0 \otimes \beta_1^+ \cdot (\tau_{s_1} + e_1) && \text{by (94)} \\
&= (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0}^0 \otimes (\tau_{s_1} \cdot \beta_1^+ \cdot (\tau_{s_1} + e_1)) && \text{by (58) and (59)} \\
&\equiv -(\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^- && \text{by (95)} \\
&= \mathcal{R}_3(\phi_1). \quad \square
\end{aligned}$$

Proposition 6.19. *As in the last lemma, let $K_{2,3}$ be the sub- E^0 -bimodule of $T_{E^0}^3 E^1$ generated by the kernel of the degree 2 multiplication map, i.e.,*

$$K_{2,3} := \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \subseteq T_{E^0}^3 E^1,$$

where $\overline{(\cdot)}$ denotes the image of $(\cdot)$ in $T_{E^0}^3 E^1$. Furthermore, let $K_{\text{extra},3}$ be the sub-left- k $[T^0/T^1]$ -module generated by the following element:

$$\begin{aligned}
& \Gamma_{\varpi}(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1) \\
&= (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-.
\end{aligned}$$

One has that the kernel $\ker(\mathcal{M}_3)$ of the multiplication map in degree 3 coincides with $K_{2,3} + K_{\text{extra},3}$. Furthermore, $K_{\text{extra},3}$ is also the sub-right- k $[T^0/T^1]$ -module generated by the above element.

Proof. The last claim is easy to see using that $\mathcal{R}_3$ is a homomorphism of k $[T^0/T^1]$ -bimodules (Lemma 6.16), that Γ_{ϖ} transforms multiplication by τ_{ω} into multiplication by $\tau_{\omega^{-1}}$ and that k $[T^0/T^1]$ centralizes ϕ_1 .

We now turn to the proof of the main claim. Let us define

$$V := K_{2,3} + K_{\text{extra},3} + \text{Image}(\mathcal{R}'_3) \subseteq T_{E^0}^3 E^1,$$

where the map $\mathcal{R}'_3$ was defined in Lemma 6.16. To prove the proposition, it suffices to show that $V = T_{E^0}^3 E^1$ (i.e., the inclusion from right to left): indeed assuming this equality, we obtain

$$K_{2,3} + K_{\text{extra},3} + \text{Image}(\mathcal{R}'_3) = \ker(\mathcal{M}_3) \oplus \text{Image}(\mathcal{R}'_3),$$

and this, together with the “easy inclusion” $K_{2,3} + K_{\text{extra},3} \subseteq \ker(\mathcal{M}_3)$, shows that we have $K_{2,3} + K_{\text{extra},3} = \ker(\mathcal{M}_3)$, as we wanted (for the inclusion $K_{\text{extra},3} \subseteq \ker(\mathcal{M}_3)$, recall from (85) that Γ_{ϖ} commutes with $\mathcal{M}$ and from (76) that Γ_{ϖ} fixes ϕ_1).

To reduce the amount of computations, we first make some preliminary observations.

(a) We remark that one has the congruences

$$\Gamma_{\varpi}(\mathcal{J}(\phi_1)) \equiv \mathcal{R}_3(\phi_1) \equiv \Gamma_{\varpi}(\mathcal{R}_3(\phi_1)) \equiv \mathcal{J}(\mathcal{R}_3(\phi_1)) \pmod{K_{2,3} + K_{\text{extra},3}}.$$

Indeed the first and last congruence follow from Lemma 6.18, while the second congruence holds by definition of $K_{\text{extra},3}$. Looking at the definition of $\mathcal{R}'_3$, this shows that

$$\begin{aligned} \mathcal{R}'_3(\phi_1) &\equiv \mathcal{R}_3(\phi_1) \equiv \Gamma_{\varpi}(\mathcal{R}_3(\phi_1)) \\ &\equiv \mathcal{J}(\mathcal{R}_3(\phi_1)) \equiv \Gamma_{\varpi}(\mathcal{J}(\mathcal{R}_3(\phi_1))) \pmod{K_{2,3} + K_{\text{extra},3}}. \end{aligned} \quad (96)$$

(b) We remark that V is invariant for Γ_{ϖ} and $\mathcal{J}$.

- The term $K_{2,3}$ is invariant for Γ_{ϖ} and $\mathcal{J}$ because both involutions commute with $\mathcal{M}_2$ (see (85)).
- The term $\text{Image}(\mathcal{R}'_3)$ is invariant for Γ_{ϖ} and $\mathcal{J}$ because these involutions commute with $\mathcal{R}'_3$ (Lemma 6.16).
- The term $K_{\text{extra},3}$ is visibly invariant for Γ_{ϖ} . Moreover, applying $\mathcal{J}$ to the difference $\Gamma_{\varpi}(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1)$ and using that Γ_{ϖ} and $\mathcal{J}$ commute on E^* by (38) and hence also on $T_{E^0}^3 E^1$, we obtain the element $\Gamma_{\varpi}(\mathcal{J}(\mathcal{R}_3(\phi_1))) - \mathcal{J}(\mathcal{R}_3(\phi_1))$, which lies in $K_{2,3} + K_{\text{extra},3}$ by part (a). Also considering the behaviour of $\mathcal{J}$ with respect to multiplication by τ_{ω} for $\omega \in T^0/T^1$, we obtain that $\mathcal{J}(K_{\text{extra},3}) \subseteq K_{2,3} + K_{\text{extra},3}$.

(c) We further remark that V is a sub- $k[T^0/T^1]$ -bimodule of $T_{E^0}^3 E^1$: indeed the term $K_{2,3}$ is clearly even a sub- E^0 -bimodule, the term $K_{\text{extra},3}$ is a sub- $k[T^0/T^1]$ -bimodule as already discussed and the term $\text{Image}(\mathcal{R}'_3)$ is a sub- $k[T^0/T^1]$ -bimodule because $\mathcal{R}'_3$ is a homomorphism of $k[T^0/T^1]$ -bimodules (Lemma 6.16).

Now we can start the actual proof of the proposition. Let us consider $x \in T_{E^0}^3 E^1$ and let us prove that $x \in V$. Without loss of generality, we can of course assume that x is of the form $y \otimes z$ for $y \in E^1$ and $z \in E^1 \otimes_{E^0} E^1$. Considering the equality

$$x = y \otimes z = y \otimes (z - \mathcal{R}_2(\mathcal{M}_2(z))) + y \otimes \mathcal{R}_2(\mathcal{M}_2(z)),$$

we see that the first summand on the right hand side lies in $\overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)}$ and hence in V . Therefore, without loss of generality, we can assume that x is of the form $y \otimes z'$ for some $y \in E^1$ and some $z' \in \text{Image}(\mathcal{R}_2)$. From Lemma 6.6 we obtain that $\mathcal{R}_2(F^1 E^2) = \mathcal{J}(\mathcal{R}_2(F^1 E^2))$. Using the formulas for the action of $\mathcal{J}$ on E^1 (64) and looking at the explicit definition of $\mathcal{R}_2$ in Lemma 6.3 we then see that every $z' \in \text{Image}(\mathcal{R}_2)$ can be written as a sum of simple tensors of the following forms:

$$u \otimes \beta_1^-, \quad u \otimes \beta_1^+, \quad u \otimes \beta_{s_0}^0, \quad u \otimes \beta_{s_1}^0,$$

for $u \in E^1$. Hence, without loss of generality, we can assume that z' is of one of those forms. To simplify a little further, we note that since V is invariant for Γ_ϖ , it follows that it suffices to prove that the elements of the following forms lie in V :

- (i) $y \otimes u \otimes \beta_1^-$ for some $u \in E^1$,
- (ii) $y \otimes u \otimes \beta_{s_0}^0$ for some $u \in E^1$,

because by applying Γ_ϖ to such elements we immediately obtain what is left (see (65)). We treat separately elements of the forms (i) and (ii).

- (i) Let us start the proof that every element of the form

$$y \otimes u \otimes \beta_1^- \quad (\text{for some } y, u \in E^1)$$

lies in V . Similarly to what we did before, we can consider the equality

$$y \otimes u \otimes \beta_1^- = (y \otimes u - \mathcal{R}_2(\mathcal{M}_2(y \otimes u))) \otimes \beta_1^- + \mathcal{R}_2(\mathcal{M}_2(y \otimes u)) \otimes \beta_1^-,$$

from which we see that we may consider instead elements of the form $r \otimes \beta_1^-$ for $r \in \text{Image}(\mathcal{R}_2)$, and, looking at the explicit definition of $\mathcal{R}_2$ (Lemma 6.3), we can further assume that $r \otimes \beta_1^-$ is of one of the following forms:

$$\begin{array}{ll} \beta_1^+ \otimes \beta_{s_1 v}^0 \otimes \beta_1^- & \text{for } v \in \widetilde{W} \text{ such that } \ell(s_1 v) = \ell(v) + 1, \\ \beta_1^+ \otimes \beta_{s_1 v}^- \otimes \beta_1^- & \text{for } v \in \widetilde{W} \text{ such that } \ell(s_1 v) = \ell(v) + 1, \\ \beta_{s_1}^0 \otimes \beta_v^+ \otimes \beta_1^- & \text{for } v \in \widetilde{W} \text{ such that } \ell(s_1 v) = \ell(v) + 1, \\ \beta_{s_0}^0 \otimes \beta_w^- \otimes \beta_1^- & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\ \beta_1^- \otimes \beta_{s_0 w}^+ \otimes \beta_1^- & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\ \beta_1^- \otimes \beta_{s_0 w}^0 \otimes \beta_1^- & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\ \tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0^{-1} \omega}^+) \otimes \beta_1^- & \text{for } \omega \in T^0/T^1, \\ \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1} \omega}^-) \otimes \beta_1^- & \text{for } \omega \in T^0/T^1. \end{array}$$

If v is as above, from Lemma 6.1 and from (55) one sees that either $\beta_{s_1 v}^- \in k^\times \tau_{s_1 v} \beta_1^-$ or $\beta_{s_1 v}^- \in k^\times \tau_{s_1 v} \beta_1^+$. This justifies the first line below:

$$\begin{aligned} \beta_{s_1 v}^- \otimes \beta_1^- &\in E^0 \cdot \{\beta_1^- \otimes \beta_1^-, \beta_1^+ \otimes \beta_1^-\}, \\ \beta_v^+ \otimes \beta_1^- &\in E^0 \cdot \{\beta_1^- \otimes \beta_1^-, \beta_1^+ \otimes \beta_1^-\}, \\ \beta_w^- \otimes \beta_1^- &\in E^0 \cdot \{\beta_1^- \otimes \beta_1^-, \beta_1^+ \otimes \beta_1^-\}, \\ \beta_{s_0 w}^+ \otimes \beta_1^- &\in E^0 \cdot \{\beta_1^- \otimes \beta_1^-, \beta_1^+ \otimes \beta_1^-\}, \end{aligned}$$

and the other lines can be justified with a completely analogous argument.

Since the two elements $\beta_1^- \otimes \beta_1^-$ and $\beta_1^+ \otimes \beta_1^-$ lie in $\ker(\mathcal{M}_2)$ (see, e.g., Lemma 6.9), we see that the elements $\beta_1^+ \otimes \beta_{s_1 v}^- \otimes \beta_1^-$, $\beta_{s_1}^0 \otimes \beta_v^+ \otimes \beta_1^-$,

$\beta_{s_0}^0 \otimes \beta_w^- \otimes \beta_1^-$ and $\beta_1^- \otimes \beta_{s_0 w}^+ \otimes \beta_1^-$ in the above list all lie in V . Also recalling that V is a left- $k[T^0/T^1]$ -submodule, we see that we are reduced to showing that the following elements lie in V :

$$\begin{aligned}
& \beta_1^+ \otimes \beta_{(s_1 s_0)^i}^0 \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geq 1}, \\
& \beta_1^+ \otimes \beta_{s_1(s_0 s_1)^i}^0 \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geq 0}, \\
& \beta_1^- \otimes \beta_{(s_0 s_1)^i}^0 \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geq 1}, \\
& \beta_1^- \otimes \beta_{s_0(s_1 s_0)^i}^0 \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geq 0}, \\
& \tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-, \\
& \tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^-.
\end{aligned} \tag{97}$$

Up to a sign, the first line (respectively, the fourth line) is $\mathcal{R}'_3(\phi_{(s_1 s_0)^i})$ (respectively, $\mathcal{R}'_3(\phi_{s_0(s_1 s_0)^i})$), and hence they both lie in V . Moreover, we know that $\beta_{s_1}^0 \otimes \beta_1^- \in \ker(\mathcal{M}_2)$ (see for example Lemma 6.9), from which it follows that

$$\begin{aligned}
& \beta_{(s_0 s_1)^i}^0 \otimes \beta_1^- = -\tau_{(s_0 s_1)^{i-1} s_0} \cdot \beta_{s_1}^0 \otimes \beta_1^- \in \ker(\mathcal{M}_2) && \text{for all } i \in \mathbb{Z}_{\geq 1}, \\
& \beta_{s_1(s_0 s_1)^i}^0 \otimes \beta_1^- = \tau_{(s_1 s_0)^i} \cdot \beta_{s_1}^0 \otimes \beta_1^- \in \ker(\mathcal{M}_2) && \text{for all } i \in \mathbb{Z}_{\geq 0}
\end{aligned}$$

(where we used (84)). Therefore, it follows that also the second, the third and the sixth line in (97) lie in V . It remains to consider the element $\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-$. First of all, we see that there is no harm in considering instead the element $(\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^- = -\mathcal{R}_3(\phi_1)$, since $e_1 \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^- \in \text{Image}(\mathcal{R}'_3) \subseteq V$. But we have seen in formula (96) that $\mathcal{R}_3(\phi_1)$ is congruent to $\mathcal{R}'_3(\phi_1)$ modulo $K_{2,3} + K_{\text{extra},3}$, and hence $\mathcal{R}_3(\phi_1) \in V$, thus completing the proof that all the lines in (97) lie in V .

(ii) We have to consider the elements of the form

$$y \otimes u \otimes \beta_{s_0}^0 = y \otimes u \otimes \beta_{s_0}^0 \quad (\text{for some } y, u \in E^1)$$

and prove that they lie in V . As before, we see that we may only treat the elements of the form $r \otimes \beta_{s_0}^0$ for $r \in \text{Image}(\mathcal{R}_2)$, and, looking at the explicit definition of $\mathcal{R}_2$ (Lemma 6.3), we can further assume that $r \otimes \beta_{s_0}^0$

is of one of the following forms:

$$\begin{array}{ll}
\beta_1^+ \otimes \beta_{s_1 v}^0 \otimes \beta_{s_0}^0 & \text{for } v \in \widetilde{W} \text{ such that } \ell(s_1 v) = \ell(v) + 1, \\
\beta_1^+ \otimes \beta_{s_1 v}^- \otimes \beta_{s_0}^0 & \text{for } v \in \widetilde{W} \text{ such that } \ell(s_1 v) = \ell(v) + 1, \\
\beta_{s_1}^0 \otimes \beta_v^+ \otimes \beta_{s_0}^0 & \text{for } v \in \widetilde{W} \text{ such that } \ell(s_1 v) = \ell(v) + 1, \\
\beta_{s_0}^0 \otimes \beta_w^- \otimes \beta_{s_0}^0 & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\
\beta_1^- \otimes \beta_{s_0 w}^+ \otimes \beta_{s_0}^0 & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\
\beta_1^- \otimes \beta_{s_0 w}^- \otimes \beta_{s_0}^0 & \text{for } w \in \widetilde{W} \text{ such that } \ell(s_0 w) = \ell(w) + 1, \\
\tau_{s_0} \cdot \mathcal{R}_2(\alpha_{s_0^{-1} \omega}^+) \otimes \beta_{s_0}^0 & \text{for } \omega \in T^0/T^1, \\
\tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1^{-1} \omega}^-) \otimes \beta_{s_0}^0 & \text{for } \omega \in T^0/T^1.
\end{array}$$

In part (i) we have proved that all the elements of the form $x \otimes y \otimes \beta_1^-$ (for some $x, y \in E^1$) lie in V . As we have already said that V is $\mathcal{J}$ -invariant and Γ_{ϖ} -invariant, we deduce that the elements of the following forms lie in V :

$$\begin{array}{ll}
\beta_1^- \otimes x \otimes y & \text{for some } x, y \in E^1, \\
\beta_1^+ \otimes x \otimes y & \text{for some } x, y \in E^1.
\end{array}$$

This shows that most of the elements in the above list are in V . For the remaining ones, we first use Lemma 6.1 and (55) as in part (i) to reduce to checking that the following elements lie in V :

$$\begin{array}{ll}
\beta_{(s_1 s_0)^i}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0 & \text{for } i \in \mathbb{Z}_{\geq 1}, \\
\beta_{s_1(s_0 s_1)^i}^0 \otimes \beta_1^+ \otimes \beta_{s_0}^0 & \text{for } i \in \mathbb{Z}_{\geq 0}, \\
\beta_{(s_0 s_1)^i}^0 \otimes \beta_1^+ \otimes \beta_{s_0}^0 & \text{for } i \in \mathbb{Z}_{\geq 1}, \\
\beta_{s_0(s_1 s_0)^i}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0 & \text{for } i \in \mathbb{Z}_{\geq 0}, \\
\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^0, \\
\tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_{s_0}^0.
\end{array}$$

We recall from Lemma 6.9 that $\beta_1^+ \otimes \beta_{s_0}^0 \in \ker(\mathcal{M}_2)$ and that the same is true for $\beta_{s_1}^0 \otimes \beta_{s_0}^0$, and so it only remains to consider the following elements:

$$\beta_{(s_1 s_0)^i}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0 \quad \text{for } i \in \mathbb{Z}_{\geq 1}, \quad (98)$$

$$\beta_{s_0(s_1 s_0)^i}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0 \quad \text{for } i \in \mathbb{Z}_{\geq 0}, \quad (99)$$

$$\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^0. \quad (100)$$

Let us treat the last line, where, multiplying by $\tau_{c_{-1}}$, we can replace s_0^{-1} by s_0 . We consider the following element of $\ker(\mathcal{M}_2)$ (Lemma 6.9):

$$\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\text{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+.$$

Tensoring by $\tau_{s_0} \cdot \beta_1^-$ on the left we get

$$\begin{aligned} & \tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 \otimes \beta_{s_0}^0 + \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\text{id}}^{-1}} \beta_1^- \otimes \beta_{s_0}^0 \\ & + \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\text{id}}} \beta_{s_0}^0 \otimes \beta_1^- - \tau_{s_0} \cdot \beta_1^- \otimes e_1 \beta_1^- \otimes \beta_{s_0}^+ \\ & \in K_{2,3}. \end{aligned}$$

Since $\beta_1^- \otimes \beta_1^-$ lies in $\ker(\mathcal{R}_2)$, we can delete the two terms where this element appears, getting that

$$\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 \otimes \beta_{s_0}^0 + \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\text{id}}} \beta_{s_0}^0 \otimes \beta_1^- \in K_{2,3}.$$

In part (i) we have seen that the element $\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 \otimes \beta_1^-$ lies in V , and so this proves that (100) lies in V .

It remains to prove that the elements in (98) and in (99) lie in V . We claim that $\beta_{s_0}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0$ lies in $K_{2,3}$. If we show this, then we are done because $K_{2,3}$ is a sub- E^0 -bimodule, and using (84) we get that the elements in the lines (98) and (99) lie in $K_{2,3}$ as well and hence also to V . So, let us show that $\beta_{s_0}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0$ lies in $K_{2,3}$.

$$\begin{aligned} \beta_{s_0}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0 &= \mathcal{R}_2(-\alpha_{s_0}^-) \otimes \beta_{s_0}^0 \\ &= \mathcal{R}_2(\tau_{s_0} \cdot \alpha_1^+) \otimes \beta_{s_0}^0 \\ &\quad \text{(by (69))} \\ &\equiv (\tau_{s_0} \cdot \mathcal{R}_2(\alpha_1^+)) \otimes \beta_{s_0}^0 \pmod{K_{2,3}} \end{aligned} \tag{101}$$

We now compute $\mathcal{R}_2(\alpha_1^+)$ explicitly

$$\begin{aligned} \mathcal{R}_2(\alpha_1^+) &= \mathcal{R}_2(\alpha_1^+ + \tau_{s_1} \cdot \alpha_{s_1}^-) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1}^-) \\ &\quad \text{by Lemma 6.3} \\ &= \mathcal{R}_2(-e_1 \alpha_{s_1}^- + e_{\underline{\text{id}}^{-1}} \alpha_{s_1}^0 + e_{\underline{\text{id}}^{-2}} \alpha_{s_1}^+) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha_{s_1}^-) \\ &\quad \text{by (71)} \\ &= e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^0 + e_{\underline{\text{id}}^{-1}} \cdot \beta_1^+ \otimes \beta_{s_1}^- \\ &\quad + e_{\underline{\text{id}}^{-2}} \cdot \beta_{s_1}^0 \otimes \beta_{c-1}^+ + \tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1}^0 \\ &\quad \text{by Lemma 6.3 and Lemma 6.4} \\ &= e_1 \cdot \beta_{c-1}^+ \otimes \beta_{s_1}^0 - e_{\underline{\text{id}}^{-1}} \cdot (\beta_1^+ \cdot \tau_{s_1}^{-1}) \otimes \beta_1^+ \\ &\quad + e_{\underline{\text{id}}^{-2}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ + \tau_{s_1} \cdot \beta_{c-1}^+ \otimes \beta_{s_1}^0 \\ &\quad \text{by (55), (56), (82)} \end{aligned}$$

Going back to (101), and recalling from Lemma 6.9 that both $\beta_1^+ \otimes \beta_{s_0}^0$ and $\beta_{s_1}^0 \otimes \beta_{s_0}^0$ lie in $\ker(\mathcal{M}_2)$, we conclude that $\beta_{s_0}^0 \otimes \beta_1^- \otimes \beta_{s_0}^0$ lies in $K_{2,3}$, as claimed. This concludes the proof that all the elements of the forms (98) and (99) lie in V , and with it the proof that all the elements of the form (ii) lie in V . $\square$

6.6 The 4th graded piece of the kernel

Since $E^4 = 0$, the kernel of the multiplication map $\mathcal{M}_4: T_{E^0}^4 E^1 \rightarrow E^4$ is of course the whole $T_{E^0}^4 E^1$. As we computed generators for $\ker(\mathcal{M}_2)$ as an E^0 -bimodule (Proposition 6.14), and we computed $\ker(\mathcal{M}_3)$ in terms of $\ker(\mathcal{M}_2)$ and an additional generator (Proposition 6.19), we now would like to compute $\ker(\mathcal{M}_4) = T_{E^0}^4 E^1$ in terms of $\ker(\mathcal{M}_3)$ (and, a priori, some other generators). The following result achieves this, showing that no further generators are needed and hence that $\ker(\mathcal{M})$ is generated as a two-sided ideal by its 2nd and 3rd graded pieces.

Proposition 6.20. *Let $\mathcal{M}: T_{E^0}^* E^1 \rightarrow E^*$ be the multiplication map, and let*

$$K_{3,4} := \overline{\ker(\mathcal{M}_3) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_3)} \subseteq T_{E^0}^4 E^1,$$

where $\overline{(\cdot)}$ denotes the image of $(\cdot)$ in $T_{E^0}^4 E^1$. One has that $K_{3,4} = T_{E^0}^4 E^1$.

Proof. We have to prove that every element of $T_{E^0}^4 E^1$ lies in $K_{3,4}$, and clearly it suffices to prove this for “simple tensors” of the form $x \otimes y$ for $x \in E^1$ and $y \in T_{E^0}^3 E^1$. Considering the equality

$$x \otimes y = x \otimes (y - \mathcal{R}_3(\mathcal{M}_3(y))) + x \otimes \mathcal{R}_3(\mathcal{M}_3(y)),$$

we see that it suffices to prove our claim for elements of the form $x \otimes y'$ for $x \in E^1$ and $y' \in \text{Image}(\mathcal{M}_3)$. Now looking at the explicit definition of $\mathcal{R}_3$ in Lemma 6.15, we see that every $y' \in \text{Image}(\mathcal{M}_3)$ can be written as a k -linear combination of tensors of the form $z \otimes t \otimes \beta_1^-$ for some $z, t \in E^1$ and of the form $z \otimes t \otimes \beta_1^+$ for some $z, t \in E^1$ (the presence of τ_ω in the definition of $\mathcal{R}_3$ is irrelevant, since it commutes, up to a scalar, with both β_1^- and β_1^+). We are thus reduced to showing that the elements of the form $u \otimes \beta_1^-$ and $u \otimes \beta_1^+$, for $u \in T_{E^0}^3 E^1$, lie in $K_{3,4}$. With the same trick as before, we see that we can assume that $u \in \text{Image}(\mathcal{M}_3)$. Using the same property of $\text{Image}(\mathcal{M}_3)$ as above, we are thus reduced to showing that the elements of the form

$$\begin{aligned} z \otimes t \otimes \beta_1^- \otimes \beta_1^-, & \quad z \otimes t \otimes \beta_1^+ \otimes \beta_1^-, \\ z \otimes t \otimes \beta_1^- \otimes \beta_1^+, & \quad z \otimes t \otimes \beta_1^+ \otimes \beta_1^+, \end{aligned}$$

(for $z, t \in E^1$) all lie in $K_{3,4}$. This is clear, since all of the elements $\beta_1^- \otimes \beta_1^-$, $\beta_1^+ \otimes \beta_1^-$, $\beta_1^- \otimes \beta_1^+$, and $\beta_1^+ \otimes \beta_1^+$ lie in $\ker(\mathcal{M}_2)$ (see, e.g., Lemma 6.9). $\square$

6.7 First main result: finite presentation over the tensor algebra of E^1

We are now going to state the first main result of this section, consisting in a presentation of the Ext-algebra E^* in terms of the tensor algebra $T_{E^0}^* E^1$.

Theorem 6.21. *Recall the assumptions stated at the beginning of §6. The multiplication map*

$$\mathcal{M}: T_{E^0}^* E^1 \rightarrow E^*$$

is surjective and its kernel is generated by its 2nd and 3rd graded pieces. Furthermore, the kernel is finitely generated as a two-sided ideal and the following is an explicit list of generators:

$$\begin{aligned}
& \beta_1^- \otimes \beta_1^-, \quad \beta_1^+ \otimes \beta_1^-, \quad \beta_{s_1}^0 \otimes \beta_1^-, \quad \beta_1^+ \otimes \beta_{s_0}^0, \quad \beta_{s_1}^0 \otimes \beta_{s_0}^0, \\
& \beta_1^- \otimes \beta_1^+, \quad \beta_1^+ \otimes \beta_1^+, \quad \beta_{s_0}^0 \otimes \beta_1^+, \quad \beta_1^- \otimes \beta_{s_1}^0, \quad \beta_{s_0}^0 \otimes \beta_{s_1}^0, \\
& \beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\text{id}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\text{id}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+, \\
& \beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\text{id}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\text{id}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-, \\
& \beta_{s_0}^+ \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_{s_0}^- = -\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0}, \\
& \beta_{s_1}^- \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_{s_1}^+ = -\tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_1^+ \cdot \tau_{s_1}, \\
& (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-.
\end{aligned}$$

Proof. Surjectivity has been proved in Lemmas 6.3 and 6.15, while the description of the kernel follows from Propositions 6.14, 6.19 and 6.20. $\square$

Remark 6.22. The statement of the theorem does not exclude the possibility that $\ker(\mathcal{M})$ is actually generated by its 2nd graded piece. It is actually possible to show that this is not the case (see [Bod22, §4.9]). However, the proof is quite long and we do not present it here.

6.8 Second main result: finite presentation as a k -algebra

The purpose of this section is to show that the Ext-algebra E^* is finitely presented a k -algebra, and to compute an explicit presentation (Theorem 6.26). For this, besides Theorem 6.21 we will need a presentation of E^0 as a k -algebra and a presentation of E^1 as an E^0 -bimodule (where by E^0 -bimodule we mean $E^0 \otimes_k (E^0)^{\text{op}}$ -left-module and not $E^0 \otimes_{\mathbb{Z}} (E^0)^{\text{op}}$ -left-module). We begin by studying the latter problem.

For later purposes, we fix a generator ω_0 of the cyclic group $T^0/T^1 \cong \mathbb{F}_p^\times$:

$$T^0/T^1 = \{1, \omega_0, \omega_0^2, \dots, \omega_0^{p-2}\}. \quad (102)$$

Lemma 6.23. *Let M be the free $E^0 \otimes_k (E^0)^{\text{op}}$ -left-module of rank 4 generated by the four symbols $\widehat{\beta_1^-}$, $\widehat{\beta_1^+}$, $\widehat{\beta_{s_0}^0}$ and $\widehat{\beta_{s_1}^0}$. Let us consider the submodule N*

generated by the following elements:

$$\tau_{s_1} \cdot \widehat{\beta_1^-}, \quad \tau_{s_0} \cdot \widehat{\beta_1^+}, \quad (103)$$

$$\widehat{\beta_1^+} \cdot \tau_{s_0}, \quad \widehat{\beta_1^-} \cdot \tau_{s_1}, \quad (104)$$

$$\begin{aligned} (\tau_{s_0} + e_1) \cdot \widehat{\beta_1^-} \cdot (\tau_{s_0} + e_1) & \quad (\tau_{s_1} + e_1) \cdot \widehat{\beta_1^+} \cdot (\tau_{s_1} + e_1) \\ + 2e_{\text{id}} \widehat{\beta_{s_0}^0} + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^+}, & \quad - 2e_{\text{id}^{-1}} \widehat{\beta_{s_1}^0} + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^-}, \end{aligned} \quad (105)$$

$$\tau_{s_0} \cdot \widehat{\beta_{s_1}^0} + \widehat{\beta_{s_0}^0} \cdot \tau_{s_1}, \quad \tau_{s_1} \cdot \widehat{\beta_{s_0}^0} + \widehat{\beta_{s_1}^0} \cdot \tau_{s_0}, \quad (106)$$

$$(\tau_{s_0} + e_1) \cdot \widehat{\beta_{s_0}^0} + e_{\text{id}} \tau_{s_0} \cdot \widehat{\beta_1^-}, \quad (\tau_{s_1} + e_1) \cdot \widehat{\beta_{s_1}^0} - e_{\text{id}^{-1}} \tau_{s_1} \cdot \widehat{\beta_1^+}, \quad (107)$$

$$\widehat{\beta_{s_0}^0} \cdot (\tau_{s_0} + e_1) + e_{\text{id}^{-1}} \widehat{\beta_1^-} \cdot \tau_{s_0}, \quad \widehat{\beta_{s_1}^0} \cdot (\tau_{s_1} + e_1) - e_{\text{id}} \widehat{\beta_1^+} \cdot \tau_{s_1}, \quad (108)$$

$$\tau_{\omega_0} \cdot \widehat{\beta_1^-} - u_{\omega_0}^{-2} \widehat{\beta_1^-} \cdot \tau_{\omega_0}, \quad \tau_{\omega_0} \cdot \widehat{\beta_1^+} - u_{\omega_0}^2 \widehat{\beta_1^+} \cdot \tau_{\omega_0}, \quad (109)$$

$$\tau_{\omega_0} \cdot \widehat{\beta_{s_0}^0} - \widehat{\beta_{s_0}^0} \cdot \tau_{\omega_0^{-1}}, \quad \tau_{\omega_0} \cdot \widehat{\beta_{s_1}^0} - \widehat{\beta_{s_1}^0} \cdot \tau_{\omega_0^{-1}}. \quad (110)$$

For $\sigma \in \{\beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}$, we denote by $\tilde{\sigma}$ the image of $\widehat{\sigma}$ in M/N . One has an isomorphism of $E^0 \otimes_k (E^0)^{\text{op}}$ -left-modules

$$\begin{aligned} M/N & \longrightarrow E^1 \\ \tilde{\sigma} & \\ (\text{for } \sigma \in \{\beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}) & \longmapsto \sigma. \end{aligned}$$

Proof. To show that the claimed isomorphism is well-defined, we need to show that the elements of E^1 that we obtain from the elements in (103)-(110) by replacing $\widehat{\sigma}$ with σ (for $\sigma \in \{\beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}$) are all zero. For line (103) the claim follows from (58), for line (104) the claim follows from (59). Regarding line (105), using again such results and also (55), (57) and (60), we compute

$$\begin{aligned} & (\tau_{s_0} + e_1) \cdot \beta_1^- \cdot (\tau_{s_0} + e_1) \\ &= \tau_{s_0} \cdot \beta_1^- \cdot \tau_{s_0} + e_1 \cdot \beta_1^- \cdot \tau_{s_0} + \tau_{s_0} \cdot \beta_1^- \cdot e_1 + e_1 \cdot \beta_1^- \cdot e_1 \\ &= \tau_{s_0} \cdot \beta_{s_0}^- + e_1 \beta_{s_0}^- - e_{\text{id}^2} \beta_{s_0}^+ \\ &= \left(-e_1 \beta_{s_0}^- - 2e_{\text{id}} \beta_{s_0}^0 + e_{\text{id}^2} \beta_{s_0}^+ - \beta_{c-1}^+ \right) + e_1 \beta_{s_0}^- - e_{\text{id}^2} \beta_{s_0}^+ \\ &= -2e_{\text{id}} \beta_{s_0}^0 - \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^+. \end{aligned}$$

This shows the claim for the first part of line (105), and for the second part one can just apply Γ_{ϖ} and use the pertaining formulas.

To show that the elements in line (106) are zero it suffices to use again the formulas (58) and (59). Similarly, for line (107) we use (60) and (61) and for line (108) we use instead (62) and (63). Finally, for lines (109) and (110) we use (55) and (56).

Now, it remains to prove injectivity and surjectivity of our homomorphism. Surjectivity is clear from the fact that the elements $\beta_1^-, \beta_1^+, \beta_{s_0}^0$ and $\beta_{s_1}^0$ generate

E^1 as an E^0 -bimodule (see Lemma 6.1). To prove injectivity, we fix a k -basis $\mathcal{B}$ of E^1 , and, using surjectivity, for all $b \in \mathcal{B}$ we consider a preimage $m_b \in M/N$, to be chosen later. If we prove that the elements m_b generate M/N as a k -vector space then injectivity of P follows.

To pursue the above strategy, let us consider the following table: the elements of M/N in the first column get mapped to the elements of the second column by the formulas in Lemma 6.1 and (56). Moreover, the elements in the second column form a basis of E^1 .

$\widetilde{\beta_{s_1}^0} \cdot \tau_w \longmapsto \beta_{s_1 w}^0$	for $w \in \widetilde{W}$ such that $\ell(s_1 w) = \ell(w) + 1$,
$\widetilde{\beta_{s_0}^0} \cdot \tau_w \longmapsto \beta_{s_0 w}^0$	for $w \in \widetilde{W}$ such that $\ell(s_0 w) = \ell(w) + 1$,
$\widetilde{\beta_1^-} \cdot \tau_w \longmapsto \beta_w^-$	for $w \in \widetilde{W}$ such that $\ell(s_1 w) = \ell(w) + 1$,
$\widetilde{\beta_1^+} \cdot \tau_w \longmapsto \beta_w^+$	for $w \in \widetilde{W}$ such that $\ell(s_0 w) = \ell(w) + 1$,
$\tau_{(s_1 s_0)^j} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega \longmapsto \beta_{(s_1 s_0)^j \omega}^-$	for $\omega \in T^0/T^1$ and $j \in \mathbb{Z}_{\geq 1}$,
$\tau_{s_0(s_1 s_0)^j} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega \longmapsto -\beta_{s_0(s_1 s_0)^j \omega}^+$	for $\omega \in T^0/T^1$ and $j \in \mathbb{Z}_{\geq 0}$,
$\tau_{(s_0 s_1)^j} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega \longmapsto \beta_{(s_0 s_1)^j \omega}^+$	for $\omega \in T^0/T^1$ and $j \in \mathbb{Z}_{\geq 1}$,
$\tau_{s_1(s_0 s_1)^j} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega \longmapsto -\beta_{s_1(s_0 s_1)^j \omega}^-$	for $\omega \in T^0/T^1$ and $j \in \mathbb{Z}_{\geq 0}$.

Therefore, it remains to show that the elements in the first column generate M/N as a k -vector space. For this, it suffices to prove that, for all $v, w \in \widetilde{W}$, the following elements lie in the sub- k -vector space V generated by the first column:

$$\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_w, \quad \tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_w, \quad \tau_v \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w, \quad \tau_v \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w.$$

We are going to prove this claim by induction on $\ell(v) + \ell(w)$.

Let us consider the case $\ell(v) + \ell(w) = 0$. This condition means that v and w lie in T^0/T^1 , and so that they are powers of ω_0 . Using (109), we see that the elements $\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_w$ (respectively, $\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_w$) can be rewritten, up to a coefficient, in the form $\widetilde{\beta_1^-} \cdot \tau_\omega$ (respectively, $\widetilde{\beta_1^+} \cdot \tau_\omega$) for a suitable $\omega \in T^0/T^1$, and so it lies in V , as we wanted to show. In the same way one deals with the elements $\tau_v \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w$ and $\tau_v \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w$, this time using (110).

Now it remains to consider the induction step. We distinguish some cases.

- Let us consider first $\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_w$ and $\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_w$.

Since both $\widetilde{\beta_1^+} \cdot \tau_{s_0}$ and $\widetilde{\beta_1^-} \cdot \tau_{s_1}$ lie in N by (104), we see that it suffices to consider the following cases:

$\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_\omega$	for some $\omega \in T^0/T^1$,
$\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_\omega$	for some $\omega \in T^0/T^1$,
$\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0 w'}$	for some $w' \in \widetilde{W}$ such that $\ell(s_0 w') = \ell(w') + 1$,
$\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1 w'}$	for some $w' \in \widetilde{W}$ such that $\ell(s_1 w') = \ell(w') + 1$.

Let us look at the first two elements. Since both $\tau_{s_1} \cdot \widehat{\beta_1^-}$ and $\tau_{s_0} \cdot \widehat{\beta_1^+}$ lie in N by (103), it suffices to consider the following cases:

$$\begin{aligned} \tau_{(s_1 s_0)^j \omega'} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega & \quad \text{for some } j \in \mathbb{Z}_{\geq 0} \text{ and some } \omega, \omega' \in T^0/T^1, \\ \tau_{s_0(s_1 s_0)^j \omega'} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega & \quad \text{for some } j \in \mathbb{Z}_{\geq 0} \text{ and some } \omega, \omega' \in T^0/T^1, \\ \tau_{(s_0 s_1)^j \omega'} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega & \quad \text{for some } j \in \mathbb{Z}_{\geq 0} \text{ and some } \omega, \omega' \in T^0/T^1, \\ \tau_{s_1(s_0 s_1)^j \omega'} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega & \quad \text{for some } j \in \mathbb{Z}_{\geq 0} \text{ and some } \omega, \omega' \in T^0/T^1. \end{aligned}$$

If $\omega' = 1$ then these elements are in V because they are in the list of generators of V , and in the general case we can reduce to this situation exactly as we did in the case $\ell(v) + \ell(w) = 0$.

Now we have to consider the elements

$$\begin{aligned} \tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0} \cdot \tau_{w'} & \quad \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_0 w') = \ell(w') + 1, \\ \tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1} \cdot \tau_{w'} & \quad \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_1 w') = \ell(w') + 1. \end{aligned}$$

If $\ell(v) = 0$, we reduce as usual to the case $v = 1$, in which case we see that the above elements are in the list of generators of V . So we might assume that $\ell(v) \geq 1$. In this case, using again that both $\tau_{s_1} \cdot \widehat{\beta_1^-}$ and $\tau_{s_0} \cdot \widehat{\beta_1^+}$ lie in N , we are reduced to considering elements of the following forms:

$$\begin{aligned} \tau_{v'} \cdot \tau_{s_0} \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0} \cdot \tau_{w'}, \\ \tau_{v'} \cdot \tau_{s_1} \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1} \cdot \tau_{w'}, \end{aligned}$$

where v' and w' are elements of $\widetilde{W}$ such that lengths add up in the corresponding multiplications (i.e., $\tau_{v'} \cdot \tau_{s_0}$ and $\tau_{s_0} \cdot \tau_{w'}$ in the case of the first line). Now, looking at (105), we see that we can write these two elements as linear combinations of elements of the form

$$\tau_{v''} \cdot \widetilde{\beta_1^-} \cdot \tau_{w''}, \quad \tau_{v''} \cdot \widetilde{\beta_1^+} \cdot \tau_{w''}, \quad \tau_{v''} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_{w''}, \quad \tau_{v''} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_{w''}$$

for $v'', w'' \in \widetilde{W}$ such that $\ell(v'') + \ell(w'') < \ell(v) + \ell(w)$. The induction hypothesis then allow us to conclude that the elements $\tau_{v' s_0} \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0 w'}$ and $\tau_{v' s_1} \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1 w'}$ lie in V .

- Now we consider the elements $\tau_v \cdot \widetilde{\beta_{s_i}^0} \cdot \tau_w$ (for $i \in \{0, 1\}$) under the additional assumption that $\ell(v s_i) = \ell(v) + 1$ and $\ell(s_i w) = \ell(w) + 1$.

Making v explicit, we see that we are dealing with the following elements:

$$\begin{aligned} \tau_{(s_0 s_1)^i \omega} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w & \quad \text{for } i \in \mathbb{Z}_{\geq 0}, \omega \in T^0/T^1, w \in \widetilde{W} \text{ with } \ell(s_0 w) = \ell(w) + 1, \\ \tau_{s_1(s_0 s_1)^i \omega} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w & \quad \text{for } i \in \mathbb{Z}_{\geq 0}, \omega \in T^0/T^1, w \in \widetilde{W} \text{ with } \ell(s_0 w) = \ell(w) + 1, \\ \tau_{(s_1 s_0)^i \omega} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w & \quad \text{for } i \in \mathbb{Z}_{\geq 0}, \omega \in T^0/T^1, w \in \widetilde{W} \text{ with } \ell(s_1 w) = \ell(w) + 1, \\ \tau_{s_0(s_1 s_0)^i \omega} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w & \quad \text{for } i \in \mathbb{Z}_{\geq 0}, \omega \in T^0/T^1, w \in \widetilde{W} \text{ with } \ell(s_1 w) = \ell(w) + 1. \end{aligned}$$

As before, we see that we can assume without loss of generality that $\omega = 1$, and then, using (106) repeatedly, we see that, up to a sign, the above elements can be rewritten in the form $\widetilde{\beta}_{s_i}^0 \cdot \tau_v$ for some $i \in \{0, 1\}$ and some $v \in \widetilde{W}$ such that $\ell(s_i v) = \ell(v) + 1$.

- Now we consider the elements $\tau_v \cdot \widetilde{\beta}_{s_i}^0 \cdot \tau_w$ (for $i \in \{0, 1\}$) under the additional assumption that $\ell(s_i w) = \ell(w) - 1$.

We only deal with the case $i = 0$, the other case being completely analogous. Using (108), we see that

$$\begin{aligned} \tau_v \cdot \widetilde{\beta}_{s_0}^0 \cdot \tau_w &= \tau_v \cdot \widetilde{\beta}_{s_0}^0 \cdot \tau_{s_0} \cdot \tau_{s_0^{-1}w} \\ &= \tau_v \cdot \left(-\widetilde{\beta}_{s_0}^0 \cdot e_1 - e_{\underline{\text{id}}-1} \widetilde{\beta}_1^- \cdot \tau_{s_0} \right) \cdot \tau_{s_0^{-1}w} \\ &= -\tau_v \cdot \widetilde{\beta}_{s_0}^0 \cdot \tau_{s_0^{-1}w} e_1 - \tau_v e_{\underline{\text{id}}-1} \cdot \widetilde{\beta}_1^- \cdot \tau_w. \end{aligned}$$

The first term in the last line is a linear combination of terms of the form $\tau_{v'} \cdot \widetilde{\beta}_{s_0}^0 \cdot \tau_{w'}$ for $v', w' \in \widetilde{W}$ such that $\ell(v') + \ell(w') = \ell(v) + \ell(w) - 1$, and so by inductive hypothesis it lies in V . On the other hand, the second term is a linear combination of terms of the form $\tau_{v'} \cdot \widetilde{\beta}_1^- \cdot \tau_{w'}$ for $v', w' \in \widetilde{W}$ such that $\ell(v') + \ell(w') = \ell(v) + \ell(w)$, and these also lie in V , as already proved.

- Now it remains to consider the elements $\tau_v \cdot \widetilde{\beta}_{s_i}^0 \cdot \tau_w$ (for $i \in \{0, 1\}$) under the additional assumption that $\ell(v s_i) = \ell(v) - 1$. This case is completely analogous to the previous one, using (107) in place of (108). $\square$

In the next lemma we compute a presentation of the Hecke algebra $E^0 = H$. This is straightforward (and probably well-known) under our assumptions. Also compare the finite presentation of H in the case $G = \text{GL}_n(\mathfrak{F})$ determined in [GK20, §2.1]. The following lemma does not use anything about the Ext-algebra, and it is actually valid in the case $G = \text{SL}_2(\mathfrak{F})$, without assumptions on $\mathfrak{F}$ or p , but replacing the occurrences of p with q .

Lemma 6.24. *The pro- p Iwahori–Hecke algebra $H = E^0$ can be expressed by generators and relations as follows. Let*

$$k \langle \widehat{\tau}_{\omega_0}, \widehat{\tau}_{s_0}, \widehat{\tau}_{s_1} \rangle$$

be the ring of non-commutative polynomials in three indeterminates called $\widehat{\tau}_{\omega_0}$, $\widehat{\tau}_{s_0}$ and $\widehat{\tau}_{s_1}$. Furthermore, let I be the two-sided ideal of $k \langle \widehat{\tau}_{\omega_0}, \widehat{\tau}_{s_0}, \widehat{\tau}_{s_1} \rangle$ generated by the following elements

$$\widehat{\tau}_{\omega_0}^{p-1} - 1, \tag{111}$$

$$\widehat{\tau}_{\omega_0} \cdot \widehat{\tau}_{s_0} - \widehat{\tau}_{s_0} \cdot \widehat{\tau}_{\omega_0}^{p-2}, \quad \widehat{\tau}_{\omega_0} \cdot \widehat{\tau}_{s_1} - \widehat{\tau}_{s_1} \cdot \widehat{\tau}_{\omega_0}^{p-2}, \tag{112}$$

$$\widehat{\tau}_{s_0}^2 - \sum_{i=0}^{p-2} \widehat{\tau}_{\omega_0}^i \cdot \widehat{\tau}_{s_0}, \quad \widehat{\tau}_{s_1}^2 - \sum_{i=0}^{p-2} \widehat{\tau}_{\omega_0}^i \cdot \widehat{\tau}_{s_1}. \tag{113}$$

Let $\widetilde{\tau_{\omega_0}}$, $\widetilde{\tau_{s_0}}$ and $\widetilde{\tau_{s_1}}$ be respectively the images of $\widehat{\tau_{\omega_0}}$, $\widehat{\tau_{s_0}}$ and $\widehat{\tau_{s_1}}$ in the quotient algebra $k\langle\widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}\rangle/I$. One has an isomorphism of k -algebras

$$\begin{array}{ccc} k\langle\widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}\rangle/I & \longrightarrow & H = E^0 \\ \widetilde{\tau_{\omega_0}} & \longmapsto & \tau_{\omega_0}, \\ \widetilde{\tau_{s_0}} & \longmapsto & \tau_{s_0}, \\ \widetilde{\tau_{s_1}} & \longmapsto & \tau_{s_1}. \end{array}$$

Proof. The braid relations, the quadratic relations and the properties of the group $\widetilde{W}$ imply that the homomorphism in the statement is indeed well-defined and surjective.

To show injectivity, we proceed as in Lemma 6.23. Let us consider the following table, where the elements in the first column are mapped to the elements on the right column by our k -algebra homomorphism $k\langle\widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}\rangle/I \longrightarrow E^0$, and where the elements in the right column form a k -basis of E^0 :

$$\begin{array}{ll} \widetilde{\tau_{\omega_0}}^i \longmapsto \tau_{\omega_0}^i & \text{for } i \in \{0, \dots, p-2\}, \\ \widetilde{\tau_{\omega_0}}^i \cdot \widetilde{\tau_{s_1}} \cdot (\widetilde{\tau_{s_0}} \cdot \widetilde{\tau_{s_1}})^j \longmapsto \tau_{\omega_0^i s_1 (s_0 s_1)^j} & \text{for } i \in \{0, \dots, p-2\} \text{ and } j \in \mathbb{Z}_{\geq 0}, \\ \widetilde{\tau_{\omega_0}}^i \cdot \widetilde{\tau_{s_0}} \cdot (\widetilde{\tau_{s_1}} \cdot \widetilde{\tau_{s_0}})^j \longmapsto \tau_{\omega_0^i s_0 (s_1 s_0)^j} & \text{for } i \in \{0, \dots, p-2\} \text{ and } j \in \mathbb{Z}_{\geq 0}, \\ \widetilde{\tau_{\omega_0}}^i \cdot (\widetilde{\tau_{s_0}} \cdot \widetilde{\tau_{s_1}})^j \longmapsto \tau_{\omega_0^i (s_0 s_1)^j} & \text{for } i \in \{0, \dots, p-2\} \text{ and } j \in \mathbb{Z}_{\geq 1}, \\ \widetilde{\tau_{\omega_0}}^i \cdot (\widetilde{\tau_{s_1}} \cdot \widetilde{\tau_{s_0}})^j \longmapsto \tau_{\omega_0^i (s_1 s_0)^j} & \text{for } i \in \{0, \dots, p-2\} \text{ and } j \in \mathbb{Z}_{\geq 1}. \end{array}$$

As in Lemma 6.23, to show injectivity of our homomorphism, it suffices to show that the k -vector space V generated by the elements in the left column is the full $k\langle\widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}\rangle/I$. So, it suffices to prove that every element of the form

$$\widetilde{\tau_{w_1}} \cdots \widetilde{\tau_{w_n}},$$

for $n \in \mathbb{Z}_{\geq 0}$ and $w_1, \dots, w_n \in \{\omega_0, s_0, s_1\}$, lies in V . Using the relations (111) and (112), we see that we may further reduce to elements of the form

$$\widetilde{\tau_{\omega_0}}^i \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_m}}}$$

for $i \in \{0, \dots, p-2\}$, for $m \in \mathbb{Z}_{\geq 0}$ and for $l_1, \dots, l_m \in \{0, 1\}$. We now prove that an element of this form lies in V by induction on m . If $m = 0$, then the result is clear. Furthermore, for general m the result is clear in the case that there are no consecutive indices l_j and l_{j+1} both equal to 0 or both equal to 1. If instead there is at least one such pair of indices, then we use (113) (together with (111) and (112) again) to reduce to the case of smaller m . $\square$

Lemma 6.25. *Let A^* be a positively graded algebra over a field F (associative, with 1, not necessarily commutative) such that the natural map $T_{A^0}^* A^1 \longrightarrow A^*$ is surjective. Let us consider generators the kernel of the above map (as a two-sided ideal), obtaining a presentation*

$$\frac{T_{A^0}^* A^1}{(a_i)_{i \in \mathbf{I}}} \longrightarrow A^*.$$

Let us consider a presentation of A^1 as an $A^0 \otimes_k (A^0)^{\text{op}}$ -left module

$$\frac{\bigoplus_{j \in \mathbf{J}} (A^0 \otimes_k (A^0)^{\text{op}}) X_j}{(b_k)_{k \in \mathbf{K}}} \longrightarrow A^1,$$

and let us consider a presentation of A^0 as a k -algebra

$$\frac{F\langle Y_l \rangle_{l \in \mathbf{L}}}{(c_m)_{m \in \mathbf{M}}} \longrightarrow A^0.$$

For all $i \in \mathbf{I}$ (respectively, for all $k \in \mathbf{K}$) let us choose a lift $\dot{a}_i$ (respectively, $\dot{b}_k$) of a_i (respectively, of b_k) in $F\langle X_j, Y_l \rangle_{j \in \mathbf{J}, l \in \mathbf{L}}$.

One then has an induced presentation of A^* as a k -algebra

$$\frac{F\langle X_j, Y_l \rangle_{j \in \mathbf{J}, l \in \mathbf{L}}}{\left(\dot{a}_i, \dot{b}_k, c_m \mid i \in \mathbf{I}, k \in \mathbf{K}, m \in \mathbf{M} \right)} \longrightarrow A^*.$$

Proof. For the moment let us not assume that the map $T_{A^0}^* A^1 \longrightarrow A^*$ is surjective.

Let $\iota_0: A^0 \longrightarrow T_{A^0}^* A^1$ and $\iota_1: A^1 \longrightarrow T_{A^0}^* A^1$ be the canonical inclusions. It is easy to check that the triple $(T_{A^0}^* A^1, \iota_0, \iota_1)$ enjoys the following universal property: for all triples (R, ξ_0, ξ_1) consisting of a F -algebra R (associative, not necessarily commutative), a homomorphism of F -algebras $\xi_0: A^0 \longrightarrow R$ and a homomorphism of left $A^0 \otimes_F (A^0)^{\text{op}}$ -modules $\xi_1: A^1 \longrightarrow R$ (where R is a left $A^0 \otimes_F (A^0)^{\text{op}}$ -module via ξ_0), there exists a unique homomorphism of F -algebras $\eta: T_{A^0}^* A^1 \longrightarrow R$ making the following diagrams commute:

$$\begin{array}{ccc} & T_{A^0}^* A^1 & \\ \iota_0 \nearrow & \downarrow \eta & \searrow \iota_1 \\ A^0 & & A^1 \\ \xi_0 \searrow & & \searrow \xi_1 \\ & R & \end{array}$$

This universal property provides an inverse to the obvious map

$$\frac{F\langle X_j, Y_l \rangle_{j \in \mathbf{J}, l \in \mathbf{L}}}{\left(\dot{b}_k, c_m \mid k \in \mathbf{K}, m \in \mathbf{M} \right)} \longrightarrow T_{A^0}^* A^1,$$

and the claim of the lemma follows (assuming that the map $T_{A^0}^* A^1 \longrightarrow A^*$ is surjective). $\square$

The preceding lemma directly allows us to compute a presentation of E^* , since we have already computed the three presentations required in the statement of the lemma, in Theorem 6.21, Lemma 6.24 and Lemma 6.23 respectively.

Let us work with the ring of noncommutative polynomials in seven indeterminates $k \langle \widehat{\tau}_{\omega_0}, \widehat{\tau}_{s_0}, \widehat{\tau}_{s_1}, \widehat{\beta}_1^-, \widehat{\beta}_1^+, \widehat{\beta}_{s_0}^0, \widehat{\beta}_{s_1}^0 \rangle$ (where the indeterminates have been labelled in accordance with the notation of Lemma 6.23 and Lemma 6.24).

For all $\lambda \in \widehat{T^0/T^1}$, let us give the following definition, mimicking the definition of e_λ :

$$\varepsilon_\lambda := - \sum_{i=0}^{p-1} \lambda(\omega_0^{-i}) \widehat{\tau_{\omega_0}}^i \in k[\widehat{\tau_{\omega_0}}].$$

Let us consider the following elements of $k \langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \rangle$:

$$\begin{aligned} & \widehat{\beta_1^-} \cdot \widehat{\beta_1^-}, & \widehat{\beta_1^+} \cdot \widehat{\beta_1^-}, & \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^-}, \\ & \widehat{\beta_1^-} \cdot \widehat{\beta_1^+}, & \widehat{\beta_1^+} \cdot \widehat{\beta_1^+}, & \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^+}, \\ & \widehat{\beta_1^+} \cdot \widehat{\beta_{s_0}^0}, & \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_{s_0}^0}, & \\ & \widehat{\beta_1^-} \cdot \widehat{\beta_{s_1}^0}, & \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_{s_1}^0}, & \\ & \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_{s_0}^0} + \varepsilon_{\underline{\text{id}}^{-1}} \cdot \widehat{\beta_1^-} \cdot \widehat{\beta_{s_0}^0} + \varepsilon_{\underline{\text{id}}} \cdot \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^-} + \varepsilon_1 \cdot \widehat{\beta_1^-} \cdot \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^-}, & (114) \\ & \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_{s_1}^0} - \varepsilon_{\underline{\text{id}}} \cdot \widehat{\beta_1^+} \cdot \widehat{\beta_{s_1}^0} - \varepsilon_{\underline{\text{id}}^{-1}} \cdot \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^+} + \varepsilon_1 \cdot \widehat{\beta_1^+} \cdot \widehat{\tau_{s_1}} \cdot \widehat{\beta_1^+}, \\ & \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^-} \cdot \widehat{\tau_{s_0}} - \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^-} \cdot \widehat{\beta_{s_0}^0}, \\ & \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^+} \cdot \widehat{\tau_{s_1}} - \widehat{\tau_{s_1}} \cdot \widehat{\beta_1^+} \cdot \widehat{\beta_{s_1}^0}, \\ & (\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_1^+} \cdot \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^+} + (\widehat{\tau_{s_0}} + \varepsilon_1) \cdot \widehat{\beta_1^-} \cdot \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^-}. \end{aligned}$$

We claim that this is a set of lifts to $k \langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \rangle$ of a set of generators of the kernel of the multiplication map $\mathcal{M}: T_{E^0}^* E^1 \rightarrow E^*$ (as a two-sided ideal). Indeed, this list has been obtained in the following way from the list of generators of the $\ker(\mathcal{M})$ given in Theorem 6.21: the occurrences of β_1^- have been replaced by $\widehat{\beta_1^-}$, the occurrences of β_1^+ have been replaced by $\widehat{\beta_1^+}$, the occurrences of $\beta_{s_i}^0$ have been replaced by $\widehat{\beta_{s_i}^0}$ for $i \in \{0, 1\}$, the occurrences of τ_{s_i} have been replaced by $\widehat{\tau_{s_i}}$ for $i \in \{0, 1\}$ and the occurrences of e_λ have been replaced by ε_λ for $\lambda \in \{1, \underline{\text{id}}, \underline{\text{id}}^{-1}\}$. Furthermore, the occurrences of $\beta_{s_i}^\pm$ (for $i \in \{0, 1\}$) have first been replaced according to the following rules (see the formulas in Lemma 6.1):

$$\begin{aligned} \beta_{s_0}^+ &= -\tau_{s_0} \cdot \beta_1^-, & \beta_{s_1}^- &= -\tau_{s_1} \cdot \beta_1^+, \\ \beta_{s_0}^- &= \beta_1^- \cdot \tau_{s_0}, & \beta_{s_1}^+ &= \beta_1^+ \cdot \tau_{s_1}, \end{aligned}$$

and then, of course, according to the rules above. Finally, as regards the generator $(\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1-1}^0 \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0-1}^0 \otimes \beta_1^-$, for simplicity we have also deleted the exponent “ -1 ” (which can be achieved up to multiplying by $\tau_{c_{-1}}$, thus not affecting the fact that we are dealing with a set of generators). This shows that (114) is a set of lifts to $k \langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \rangle$ of a set of generators of $\ker(\mathcal{M})$, as claimed. In the notation of the previous lemma, the list (114) corresponds to the family $(\dot{a}_i)_{i \in \mathbf{I}}$.

Furthermore, let consider the following list of elements, obtaining from the list in Lemma 6.23 by replacing τ_{ω_0} with $\widehat{\tau_{\omega_0}}$, by replacing $\tau_{\omega_0^{-1}} = \tau_{\omega_0}^{p-2}$ with $\widehat{\tau_{\omega_0}^{p-2}}$ by replacing τ_{s_i} with $\widehat{\tau_{s_i}}$ for $i \in \{0, 1\}$ and by replacing e_λ by ε_λ for $\lambda \in \{1, \underline{\text{id}}, \underline{\text{id}}^{-1}\}$:

$$\begin{array}{ll}
\widehat{\tau_{s_1}} \cdot \widehat{\beta_1^-}, & \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^+}, \\
\widehat{\beta_1^+} \cdot \widehat{\tau_{s_0}}, & \widehat{\beta_1^-} \cdot \widehat{\tau_{s_1}}, \\
(\widehat{\tau_{s_0}} + \varepsilon_1) \cdot \widehat{\beta_1^-} \cdot (\widehat{\tau_{s_0}} + \varepsilon_1) & (\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_1^+} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) \\
+ 2\varepsilon_{\underline{\text{id}}} \widehat{\beta_{s_0}^0} + \widehat{\tau_{\omega_0}^{\frac{p-1}{2}}} \cdot \widehat{\beta_1^+}, & -2\varepsilon_{\underline{\text{id}}^{-1}} \widehat{\beta_{s_1}^0} + \widehat{\tau_{\omega_0}^{\frac{p-1}{2}}} \cdot \widehat{\beta_1^-}, \\
\widehat{\tau_{s_0}} \cdot \widehat{\beta_{s_1}^0} + \widehat{\beta_{s_0}^0} \cdot \widehat{\tau_{s_1}}, & \widehat{\tau_{s_1}} \cdot \widehat{\beta_{s_0}^0} + \widehat{\beta_{s_1}^0} \cdot \widehat{\tau_{s_0}}, \\
(\widehat{\tau_{s_0}} + \varepsilon_1) \cdot \widehat{\beta_{s_0}^0} + \varepsilon_{\underline{\text{id}}} \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^-}, & (\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_{s_1}^0} - \varepsilon_{\underline{\text{id}}^{-1}} \widehat{\tau_{s_1}} \cdot \widehat{\beta_1^+}, \\
\widehat{\beta_{s_0}^0} \cdot (\widehat{\tau_{s_0}} + \varepsilon_1) + \varepsilon_{\underline{\text{id}}^{-1}} \widehat{\beta_1^-} \cdot \widehat{\tau_{s_0}}, & \widehat{\beta_{s_1}^0} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) - \varepsilon_{\underline{\text{id}}} \widehat{\beta_1^+} \cdot \widehat{\tau_{s_1}}, \\
\widehat{\tau_{\omega_0}} \cdot \widehat{\beta_1^-} - u_{\omega_0}^{-2} \widehat{\beta_1^-} \cdot \widehat{\tau_{\omega_0}}, & \widehat{\tau_{\omega_0}} \cdot \widehat{\beta_1^+} - u_{\omega_0}^2 \widehat{\beta_1^+} \cdot \widehat{\tau_{\omega_0}}, \\
\widehat{\tau_{\omega_0}} \cdot \widehat{\beta_{s_0}^0} - \widehat{\beta_{s_0}^0} \cdot \widehat{\tau_{\omega_0}^{p-2}}, & \widehat{\tau_{\omega_0}} \cdot \widehat{\beta_{s_1}^0} - \widehat{\beta_{s_1}^0} \cdot \widehat{\tau_{\omega_0}^{p-2}}.
\end{array} \tag{115}$$

In the notation of the previous lemma, this list corresponds to the family $(\dot{b}_k)_{k \in \mathbf{K}}$.

Furthermore, let us recall the list of elements Lemma 6.24 (which we simply rewrite using the notation ε_1):

$$\begin{array}{ll}
\widehat{\tau_{\omega_0}^{p-1}} - 1, & \\
\widehat{\tau_{\omega_0}} \cdot \widehat{\tau_{s_0}} - \widehat{\tau_{s_0}} \cdot \widehat{\tau_{\omega_0}^{p-2}}, & \widehat{\tau_{\omega_0}} \cdot \widehat{\tau_{s_1}} - \widehat{\tau_{s_1}} \cdot \widehat{\tau_{\omega_0}^{p-2}}, \\
\widehat{\tau_{s_0}}^2 + \varepsilon_1 \widehat{\tau_{s_0}}, & \widehat{\tau_{s_1}}^2 + \varepsilon_1 \widehat{\tau_{s_1}}.
\end{array} \tag{116}$$

In the notation of the previous lemma, this list corresponds to the family $(c_m)_{m \in \mathbf{M}}$.

Theorem 6.26. *Recall the assumptions stated at the beginning of the current §6. The Ext-algebra E^* is finitely presented as a k -algebra. More precisely, it can be expressed as the quotient of the ring of non-commutative polynomials in seven indeterminates $k\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \rangle$ by the two-sided ideal generated by the elements in the lists (114), (115) and (116).*

Proof. This follows from Lemma 6.25 and the subsequent discussion (which relied on the presentations obtained in Theorem 6.21, Lemma 6.24 and Lemma 6.23). $\square$

Remark 6.27. The relation

$$(\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot (\tau_{s_1} + e_1) - 2e_{\underline{\text{id}}^{-1}} \beta_{s_1}^0 + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^- = 0$$

(which we used in to produce the corresponding element in the list (115)) allows us to express β_1^- in terms of β_1^+ , $\beta_{s_1}^0$, τ_{s_1} and τ_{ω_0} . This shows that E^* is actually generated by τ_{ω_0} , τ_{s_0} , τ_{s_1} , β_1^+ , $\beta_{s_0}^0$ and $\beta_{s_1}^0$ as a k -algebra, without the need to add β_1^- . Using the presentation we obtained in the last theorem, it is then immediate (but cumbersome) to obtain a presentation of E^* as a quotient of $k\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \rangle$ by replacing $\widehat{\beta_1^-}$ with

$$-\widehat{\tau_{\omega_0}}^{\frac{p-1}{2}} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_1^+} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) + 2\widehat{\tau_{\omega_0}}^{\frac{p-1}{2}} \cdot \varepsilon_{\text{id}^{-1}} \widehat{\beta_{s_1}^0}$$

wherever it appears in the lists (114), (115) and (116).

References

- [BD84] Joseph N. Bernstein and Pierre Deligne. Le “centre” de Bernstein. In *Representations des groupes réductifs sur un corps local, travaux en cours*, pages 1–32. Hermann, 1984.
- [Bod22] Emanuele Bodon. *On the structure of the pro- p Iwahori-Hecke Ext-algebra*. PhD thesis, Westfälische Wilhelms-Universität Münster, 2022.
- [BT72] François Bruhat and Jacques Tits. Groupes réductifs sur un corps local: I. Données radicielles valuées. *Publications Mathématiques de l’IHÉS*, 41:5–251, 1972.
- [BT84] François Bruhat and Jacques Tits. Groupes réductifs sur un corps local: II. Schémas en groupes. Existence d’une donnée radicielle valuée. *Publications Mathématiques de l’IHÉS*, 60:5–184, 1984.
- [DDSMS03] John D. Dixon, Marcus P.F. Du Sautoy, Avinoam Mann, and Dan Segal. *Analytic pro- p groups*, volume 61 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2003.
- [FV02] Ivan B. Fesenko and Sergei V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of mathematical monographs*. American Mathematical Society, 2nd edition, 2002.
- [GK20] Elmar Grosse-Klönne. Supersingular Hecke modules as Galois representations. *Algebra & Number Theory*, 14(1):67–118, 2020.
- [Hey19] Claudius Heyer. *Applications of parabolic Hecke algebras: parabolic induction and Hecke polynomials*. PhD thesis, Humboldt-Universität zu Berlin, 2019.
- [HR08] Thomas Haines and Michael Rapoport. On parahoric subgroups. *Advances in Mathematics*, 219(1):188–198, 2008.

- [Koz16] Karol Koziol. Pro- p -Iwahori invariants for SL_2 and L -packets of Hecke modules. *International Mathematics Research Notices*, 2016(4):1090–1125, 2016.
- [Lus89] George Lusztig. Affine Hecke algebras and their graded version. *Journal of the American Mathematical Society*, 2(3):599–635, 1989.
- [NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer, 2nd edition, 2013.
- [Oll09] Rachel Ollivier. Le foncteur des invariants sous l’action du pro- p -Iwahori de $\mathrm{SL}_2(F)$. *Journal für die reine und angewandte Mathematik*, 635:149–185, 2009.
- [OS11] Rachel Ollivier and Vincent Sécherre. Modules universels de GL_3 sur un corps p -adique en caractéristique p . Available as arXiv preprint arXiv:1105.2957, 2011.
- [OS14] Rachel Ollivier and Peter Schneider. Pro- p Iwahori–Hecke algebras are Gorenstein. *Journal of the Institute of Mathematics of Jussieu*, 13(4):753–809, 2014.
- [OS18] Rachel Ollivier and Peter Schneider. A canonical torsion theory for pro- p Iwahori–Hecke modules. *Advances in Mathematics*, 327:52–127, 2018.
- [OS19] Rachel Ollivier and Peter Schneider. The modular pro- p Iwahori–Hecke Ext-algebra. *Proceedings of Symposia in Pure Mathematics*, 101:255–308, 2019.
- [OS22] Rachel Ollivier and Peter Schneider. On the pro- p Iwahori Hecke Ext-algebra of $\mathrm{SL}_2(\mathbb{Q}_p)$. *Mémoires de la Société mathématique de France*, 175, 2022.
- [Sch15] Peter Schneider. Smooth representations and Hecke modules in characteristic p . *Pacific Journal of Mathematics*, 279(1):447–464, 2015.
- [Ser02] Jean-Pierre Serre. *Galois cohomology*. Monographs in mathematics. Springer, 2002. Corrected second printing.
- [SFW67] Robert Steinberg, John Faulkner, and Robert Wilson. *Lectures on Chevalley groups*. Yale University New Haven, 1967.
- [SS97] Peter Schneider and Ulrich Stuhler. Representation theory and sheaves on the Bruhat-Tits building. *Publications Mathématiques de l’Institut des Hautes Études Scientifiques*, 85(1):97–191, 1997.

- [SW00] Peter Symonds and Thomas Weigel. Cohomology of p -adic analytic groups. In *New horizons in pro- p groups*, volume 184 of *Progress in mathematics*, pages 349–410. Birkhäuser, 2000.
- [Vig96] Marie-France Vignéras. *Représentations l -modulaires d’un groupe réductif p -adique avec $l \neq p$* , volume 137 of *Progress in mathematics*. Birkhäuser, 1996.
- [Vig14] Marie-France Vignéras. The pro- p -Iwahori–Hecke algebra of a reductive p -adic group II. *Münster Journal of Mathematics*, 7(1):363–379, 2014.
- [Vig16] Marie-France Vignéras. The pro- p -Iwahori Hecke algebra of a reductive p -adic group I. *Compositio Mathematica*, 152(4):693–753, 2016.

UNIVERSITY OF BRITISH COLUMBIA,
 MATHEMATICS DEPARTMENT,
 1984 MATHEMATICS ROAD,
 VANCOUVER, BC V6T 1Z2, CANADA
 E-mail address: e.bodon@math.ubc.ca