On the structure of the pro-p Iwahori–Hecke Ext-algebra

Emanuele Bodon

Advisor:
Prof. Dr. Peter Schneider

Fachbereich 10
Mathematik und
Informatik

Mathematik

On the structure of the pro-p Iwahori–Hecke Ext-algebra

Inaugural-Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften im Fachbereich
Mathematik und Informatik
der Mathematisch-Naturwissenschaftlichen Fakultät
der Westfälischen Wilhelms-Universität Münster

vorgelegt von
Emanuele Bodon
aus Genova, Italien
2021

Dekan:	Prof. Dr. Xiaoyi Jiang
Erster Gutachter:	Prof. Dr. Peter Schneider
Zweiter Gutachter:	Prof. Dr. Eugen Hellmann
Tag der mündlichen Prüfung:	11.03.2022
Tag der Promotion:	11.03.2022

This page was left blank in compliance with university requirements.

To the memory of Davide Curletto.

Abstract

In this work, we study two problems concerning the pro-p Iwahori–Hecke Ext-algebra. This object, introduced by Ollivier and Schneider in [OS19], is a graded algebra which plays an important role in the context of smooth mod p representations of p-adic reductive groups.

The first main aim of this thesis is the study of the centre of the Ext-algebra: we determine it completely for the Ext-algebra associated with the group $\mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. We then describe the 0^{th} and the 1^{st} graded piece of the centre for more general groups.

The second main aim of this thesis is the study of finite generation properties for the Ext-algebra associated with the group $\mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. Under these assumptions, we show that the Ext-algebra is finitely presented.

Contents

Introduction

The broad area of mathematics referred to as the "local Langlands programme" aims at connecting the representation theory of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ of the field of p-adic numbers with the representation theory of $\mathrm{GL}_n(\mathbb{Q}_p)$, or more generally of p-adic reductive groups. A whole series of conjectural statements have been formulated, and much progress has been made in recent years, even leading to proofs of some of the conjectures. However, many aspects of this theory continue to be elusive, and, in particular, the case of mod p representations is still poorly understood.

In light of the local Langlands programme, the study of representations of p-adic reductive groups has acquired a central importance. Let us introduce some notation to talk about a precise setting related to the work in this thesis. Let $\mathfrak{F}$ be a locally compact non-archimedean field (with non-trivial absolute value) of residue characteristic p, i.e., $\mathfrak{F}$ is either a finite extension of $\mathbb{Q}_p$ or the field of formal Laurent series $\mathbb{F}_{p^f}((T))$ for some $f \in \mathbb{Z}_{\geqslant 1}$. We denote by $\mathfrak{O}$ the ring of integers of $\mathfrak{F}$ and by $\mathfrak{M}$ the maximal ideal of $\mathfrak{O}$. Furthermore, let $G = \mathbf{G}(\mathfrak{F})$ be the group of $\mathfrak{F}$-rational points of a split connected reductive group $\mathbf{G}$ defined over $\mathfrak{O}$: for example, we may consider $G = \mathrm{GL}_n(\mathfrak{F})$ or $G = \mathrm{SL}_n(\mathfrak{F})$. We view G as a locally profinite group with respect to the topology induced by $\mathfrak{F}$.

Let l be a field. One can consider different categories of representations of G over l: a possible (interesting) choice is the category of smooth representations $\mathrm{Rep}_l^\infty(G)$: it is defined as the full subcategory of the category of abstract representations V of G over l such that the map $G \times V \longrightarrow V$ is continuous, where V is endowed with the discrete topology. This condition is easily seen to be equivalent to requiring that for all $v \in V$ the stabilizer of v in G is open.

A fundamental tool to understand the category $\mathrm{Rep}_l^\infty(G)$ is the Hecke algebra associated with the pair (G, K), where K is a compact open subgroup of G. To define it, let us first consider the representation $l\,[G/K]$ given by the free l-vector space generated by the set of left cosets G/K endowed with the obvious G-action. It is easy to show that this is a smooth representation. We define

$$H_l(G,K) \coloneqq \mathrm{End}_{\mathrm{Rep}_l^\infty(G)}\left(l\,[G/K]\right)^{\mathrm{op}},$$

i.e., (the opposite ring of) the ring of endomorphisms of the representation $l\,[G/K]$. The choice of the opposite ring instead of the actual ring of endomorphisms is done in order to work with the category of left $H_l(G,K)$-modules and for some other slight advantages.

The main point in considering the Hecke algebra of the pair (G, K) in the setting of smooth representations is the existence of the following two functors:

$$\begin{aligned} \mathfrak{h}\colon \operatorname{Rep}_l^\infty(G) &\longrightarrow H_l(G,K)\text{-mod} \\ V &\longmapsto \operatorname{Hom}_{\operatorname{Rep}_l^\infty(G)}\left(l\left[G/K\right],V\right) \cong V^K, \end{aligned}$$

$$\begin{aligned} \mathfrak{t}\colon H_l(G,K)\text{-mod} &\longrightarrow \operatorname{Rep}_l^\infty(G) \\ M &\longmapsto l\left[G/K\right] \otimes_{H_l(G,K)} M. \end{aligned}$$

It is not difficult to see that the two functors are well defined, that $\mathfrak{t}$ is left adjoint to $\mathfrak{h}$ and that $\mathfrak{h}$ is left exact. However, they behave very differently depending on the field l. Let us explain this in more detail, starting by recalling the following properties in the characteristic 0 case:

(i) It is easy to see that if the characteristic of l does not divide the pro-order of K, then the functor $\mathfrak{h}$ is exact.

(ii) If $l = \mathbb{C}$ and if K is an Iwahori subgroup (i.e., the preimage of $\mathbf{B}(\mathfrak{O}/\mathfrak{M})$ via the reduction map $\mathbf{G}(\mathfrak{O}) \longrightarrow \mathbf{G}(\mathfrak{O}/\mathfrak{M})$, for a choice of a Borel subgroup $\mathbf{B}$ of $\mathbf{G}$), then the functors $\mathfrak{h}$ and $\mathfrak{t}$ induce an equivalence of categories between the full subcategory $\operatorname{Rep}_l^{\infty,K}(G) \subseteq \operatorname{Rep}_l^\infty(G)$ consisting of the smooth representations that are generated by their K-invariant vectors and the category $H_l(G,K)$-mod (see [BD84, Cor. 3.9 (ii)]).

Therefore, especially in the case $l = \mathbb{C}$, the above functors help to shed some light on the category $\operatorname{Rep}_l^\infty(G)$, also taking into account that in case (ii) the Hecke algebra $H_l(G,K)$ can be described very explicitly.

In contrast, let us see some known facts in the opposite situation where l has characteristic equal to the residue characteristic p of $\mathfrak{F}$. In this situation, instead of an Iwahori subgroup, it is better to consider its unique pro-p Sylow subgroup, which is called a pro-p Iwahori subgroup. The reason for this is that a nonzero mod p representation V of a pro-p group K is such that the space of invariants V^K is nonzero. From this it also follows immediately that every irreducible representation in $\operatorname{Rep}_l^\infty(G)$ is contained in $\operatorname{Rep}_l^{\infty,K}(G)$. Given its relevance for this introduction and for the whole thesis, further below we will come back to the definition of pro-p Iwahori subgroups.

(iii) If the characteristic of l divides the pro-order of K, then the functor $\mathfrak{h}$ is not exact (for example, this can be shown by choosing an open subgroup K' of K of index divisible by p, by considering the surjective homomorphism of G-representations $k[G/K'] \longrightarrow k[G/K]$ sending a coset gK' to the corresponding coset gK, and by showing that the K-invariant coset $K \in k[G/K]$ does not lie in the image of the K-invariants $k[G/K']^K = k[K\backslash G/K']$.)

(iv) If $l = k$ is an algebraically closed field of characteristic p, if $G = \mathrm{GL}_2(\mathbb{Q}_p)$ or $G = \mathrm{SL}_2(\mathbb{Q}_p)$ and if K is a pro-p Iwahori subgroup then the functors $\mathfrak{h}$ and $\mathfrak{t}$ (surprisingly) induce an equivalence of categories between the subcategory $\operatorname{Rep}_k^{\infty,K}(G)$ and the category $H_k(G,K)$-mod: for GL_2 see [Oll09, Theorème 1.3 (a)], and for SL_2 see [OS18, Proposition 3.25] (for SL_2 the case $p \neq 2$ was first proved in [Koz16, Corollary 5.3 (1)]).

(v) If $G = \mathrm{GL}_2(\mathfrak{F})$, where $\mathfrak{F}$ is an extension of $\mathbb{Q}_p$ with non-trivial residue degree, and if $l = k$ and K are as above, then the functors $\mathfrak{h}$ and $\mathfrak{t}$ do not induce such equivalence of categories (see [Oll09, Theorème 1.3 (b) and the following lines]).

From now on, we will always assume that l has characteristic p and we will call it k in order to avoid confusion (in accordance with the rest of the thesis). The above observations suggest that, while the Hecke algebra still seems to play an important role in this setting, the situation is much more complicated. The lack of right exactness suggests to look at a "derived setting". In this direction, one has the following fundamental result, proved by Schneider in [Sch15]: assuming that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that K is a torsion-free pro-p group, there exists a derived version of the functors $\mathscr{h}$ and $\mathscr{t}$ that defines an equivalence of derived categories between the derived category of $\mathrm{Rep}_k^\infty(G)$ and the derived category of modules over a certain differential graded algebra $\mathcal{H}_k^\bullet(G,K)$. Note also that here we are considering the full derived category of $\mathrm{Rep}_k^\infty(G)$ and we are not restricting ourselves to representations generated by their K-invariant vectors.

The differential graded algebra $\mathcal{H}_k^\bullet(G,K)$ is constructed as the $\mathrm{Hom}^\bullet$-complex $\mathrm{Hom}^\bullet(\mathcal{J}^\bullet,\mathcal{J}^\bullet)^{\mathrm{op}}$, where $k[G/K] \longrightarrow \mathcal{J}^\bullet$ is a fixed injective resolution (here the $\mathrm{Hom}^\bullet$-complex is as in [Har66, Chapter I, §6], but we consider the opposite product). Note that an injective resolution as above exists because the category $\mathrm{Rep}_k^\infty(G)$ has enough injective objects (see [Vig96, I.5.9]). However, the differential graded algebra $\mathcal{H}_k^\bullet(G,K)$ is independent of the choice of $\mathcal{J}^\bullet$ only up to quasi-isomorphism (see [Sch15, §3]). But its cohomology algebra is

$$H^*\big(\mathcal{H}_k^\bullet(G,K)\big) = \mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(G)}\left(k\left[G/K\right], k\left[G/K\right]\right)^{\mathrm{op}}$$

(see again [Sch15, §3]), and this is of course independent of such choice. Here the product is (the opposite of) the Yoneda product. In particular,

$$H^0\big(\mathcal{H}_k^\bullet(G,K)\big) = H_k(G,K).$$

In light of the above mentioned equivalence of derived categories, it would be desirable to describe explicitly the differential graded algebra $\mathcal{H}_k^\bullet(G,K)$ and to understand it as best as possible. Unfortunately, this seems to be a difficult task (also taking into account that $\mathcal{H}_k^\bullet(G,K)$ depends on the choice of an injective resolution), and as a first step in this direction one may try instead to understand the Ext-algebra.

The study of the above Ext-algebra has been carried out by Ollivier and Schneider in the case that $K = I$ is a pro-p Iwahori subgroup of G. This is a fundamental case as stressed above, although, if $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, the group I may or may not be torsion-free (and hence the above result of Schneider is not applicable in full generality).

From now on we will focus on the case $K = I$, and we will write

$$E^* := \mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(G)}\left(k\left[G/I\right], k\left[G/I\right]\right)^{\mathrm{op}}.$$

This is called the pro-p Iwahori–Hecke Ext-algebra (and we will sometimes call it just Ext-algebra for short). Before dealing with the properties of E^*, let us return to the notion of pro-p Iwahori subgroup, since it is the main object appearing in this definition. We have defined a pro-p Iwahori subgroup of G as the unique pro-p Sylow subgroup of an Iwahori subgroup, which in turn was defined as the preimage of $\mathbf{B}(\mathfrak{O}/\mathfrak{M})$ via the reduction map $\mathbf{G}(\mathfrak{O}) \longrightarrow \mathbf{G}(\mathfrak{O}/\mathfrak{M})$, for a choice of a Borel subgroup $\mathbf{B}$ of $\mathbf{G}$. A simpler equivalent definition is the following: a pro-p Iwahori subgroup of G is the preimage of $\mathbf{U}(\mathfrak{O}/\mathfrak{M})$ via the reduction map $\mathbf{G}(\mathfrak{O}) \longrightarrow \mathbf{G}(\mathfrak{O}/\mathfrak{M})$, where $\mathbf{U}$ is the unipotent radical of a Borel subgroup of $\mathbf{G}$. Moreover, every two choices of a pro-p Iwahori subgroup (or of a Iwahori subgroup) are isomorphic via conjugation by an element of G.

Let us make the definition explicit in the case $\mathbf{G} = \mathrm{GL}_n$: we may consider the Borel subgroup of upper triangular matrices, and see that the corresponding pro-p Iwahori subgroup is

$$I = \begin{pmatrix} 1+\mathfrak{M} & \mathfrak{O} & \dots & \mathfrak{O} \\ \mathfrak{M} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathfrak{O} \\ \mathfrak{M} & \dots & \mathfrak{M} & 1+\mathfrak{M} \end{pmatrix}.$$

As a side remark, the corresponding Iwahori subgroup has a similar description, where the diagonal entries lie in $\mathfrak{O}^\times$ instead of $1+\mathfrak{M}$. If we instead consider $\mathbf{G} = \mathrm{SL}_n$ (the case $\mathbf{G} = \mathrm{SL}_2$ will be the topic of part of this thesis), then the description is the same, but considering only matrices with determinant equal to 1.

Ollivier and Schneider have studied the algebra E^* in [OS19] (in the general setting) and in [OS21] (in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$). Let us briefly recall some of their main results:

- In [OS19, §3.2] the following isomorphisms of k-vector spaces are obtained:

$$E^* \cong H^*\left(I, k\left[G/I\right]\right) \cong \bigoplus_{w \in \widetilde{W}} H^*(I_w, k),$$

  where $H^*(\_,\_)$ denotes the cohomology of a pro-p group with respect to a discrete module, where $\widetilde{W}$ is a suitable index set (the so-called pro-p Iwahori–Weyl group), and where I_w is a suitable open subgroup of I.

- In [OS19, Proposition 5.3] a complete and explicit description of the multiplication in E^* is obtained in terms of cohomological operations on $H^*\left(I, k\left[G/I\right]\right)$.

- In [OS19, Proposition 6.1] an involutive anti-automorphism of the graded algebra E^* is constructed.

- In [OS19, §7.2] it is shown that, if $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and I is torsion-free, then E^* is supported in degrees $0, \dots, d$, where d is the dimension of G as an analytic manifold over $\mathbb{Q}_p$, and moreover that E^* satisfies a duality as an E^0-bimodule (i.e., $H_k(G, I)$-bimodule). It is easy to see that in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ the subgroup I is torsion-free, and so E^* is supported in degrees $0, 1, 2, 3$.

- Under the same assumptions as above, the structure of the top graded piece E^d as an E^0-bimodule is investigated in [OS19, §8] (with further assumptions needed for some results).

- In [OS21] the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ is investigated in further detail. In particular, the structure of E^* as an E^0-bimodule is completely determined.

- Furthermore, interesting representation-theoretic consequences are derived from such results. In particular, under the same assumptions as in the last point, it is shown in [OS21, Corollary 8.12] that an irreducible representation $V \in \mathrm{Rep}_k^\infty(G)$ is supersingular if and only if $H^*(I, V)$ is a supersingular left E^0-module (where a left E^0-module is defined to be supersingular if it is annihilated by a power of a certain ideal $\mathfrak{J}$ in a central subalgebra of E^0).

These results show that the Ext-algebra E^* is an interesting object in the context of the study of smooth representations of G, and, although rather complicated, also tractable using quite explicit methods.

The present thesis is devoted to investigate some further problems in the study of the Ext-algebra E^*, namely to try to answer the following questions:

(a) What is the (graded) centre of E^*? And more specifically:

(a.1) What is, explicitly, the centre of E^* in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$?

(a.2) What can be said about the centre of E^* in the general case? In particular, what are the 0^{th} and 1^{st} graded pieces of the centre?

(b) In the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$, since the structure of E^* as an E^0-bimodule is completely known, is it possible to describe the full multiplicative structure? And, in particular, does one have finite generation properties?

In the remaining part of this introduction, we discuss these problems in more detail.

(a) Let us begin with some motivation to study the centre of E^*. First of all, there is the general notion of Bernstein centre of an abelian (or just additive) category, i.e., the ring of endomorphisms of the identity functor of the category. For a category of left (or right) modules over a ring it can be identified with the centre of the ring. The centre of the categories of smooth representations we are considering was first studied by Bernstein in [BD84]. In particular, from the results quoted above in point (ii) and the previous remark about the category of modules, it follows that if J is an Iwahori subgroup, then the centre of the category $\mathrm{Rep}^{\infty,J}_{\mathbb{C}}(G)$ can be identified with the centre of the ring $H_{\mathbb{C}}(G, J)$. Furthermore, under the same assumptions Bernstein determined the centre of full category $\mathrm{Rep}^{\infty}_{\mathbb{C}}(G)$ by making use of a decomposition of this category as a product of subcategories ("Bernstein blocks"), of which one factor is precisely $\mathrm{Rep}^{\infty,J}_{\mathbb{C}}(G)$.

In contrast, in the characteristic p case the situation is less understood. Only very recently, in [AS21], Ardakov and Schneider have investigated and completely determined the centre of the category $\mathrm{Rep}^{\infty}_{k}(G)$. Their result shows that, in contrast to the case of $\mathrm{Rep}^{\infty,J}_{\mathbb{C}}(G)$, the Bernstein centre is quite small (for example, if $\mathbf{G}$ is semisimple, it can be identified with the group ring $k[Z(G)]$ of the finite group $Z(G)$). Hence, it should probably not be expected that the Bernstein centre plays the same important role as in the case $l = \mathbb{C}$.

However, in view of the equivalence of derived categories mentioned before, one should rather consider a notion of centre in this "derived" context. We shall not make this precise, but we remark that it is not even clear what should be the correct notion of centre of the derived category of $\mathcal{H}^{\bullet}_k(G, I)$-modules (see [Har16, after Question 4.3]). Since, as said before, the cohomology algebra E^* of $\mathcal{H}^{\bullet}_k(G, I)$ is more tractable, as a first step towards understanding such notions, one could try instead to study the (graded) centre of the Ext-algebra E^*.

As a further piece of motivation to study the centre of E^*, let us highlight the importance of the centre of E^0. This has been studied extensively in the literature, mainly by Vignéras. The main result, due to Schmidt and Vignéras, consists in explicitly determining a basis of $Z(E^0)$, proving that $Z(E^0)$ is a Noetherian ring, and that E^0 is finitely generated as a $Z(E^0)$-module (see Theorems 1.6.1 and 1.6.2 for precise statements and references). As a nice consequence of this result, one immediately sees that E^0 is a Noetherian ring. Furthermore, these results are a key ingredient used in the classification of simple supersingular E^0-modules by Ollivier (see [Oll14]). Therefore, one can ask whether the centre of E^* satisfies similar properties and plays a sort of analogous role (we point out, however, that this vague question is not likely to admit a positive answer: see Remark 2.1.2 for a more precise statement).

In the next two points, we will discuss the results about the centre of E^* proven in the present thesis.

(a.1) Chapter 2 of this thesis is devoted to the explicit description of the centre of E^* in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. In this case the graded algebra E^* is supported in degrees $0, 1, 2, 3$, and, even if computations can be rather involved, it is in principle possible to work with explicit formulas and compute explicit bases. We achieve the following result.

Theorem (see Theorem 2.1.1). *If $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$, then the centre of E^* admits the following description:*

- ⋆ *the 0^{th} graded piece $Z(E^*)^0$ is isomorphic to $k \times k$ as a k-algebra;*
- ⋆ *the 1^{st} graded piece $Z(E^*)^1$ is zero;*
- ⋆ *the 2^{nd} graded piece $Z(E^*)^2$ and the 3^{rd} graded piece $Z(E^*)^3$ are free modules of rank $\aleph_0$ over the ring $Z(E^*)^0 \cong k \times k$.*

Moreover, explicit k-bases of all the graded pieces of $Z(E^*)$ are computed (see Section 2.1). Note that this theorem completely determines the structure of $Z(E^*)$ as a graded-commutative k-algebra: indeed the 1^{st} graded piece is zero, and so the only products one needs to consider are those between an element of degree 0 and an element of degree 0, 2 or 3.

The above result is rather intriguing: the low graded pieces of $Z(E^*)$ are very small, resembling the result of Ardakov and Schneider mentioned above about the centre of $\mathrm{Rep}_k^\infty(G)$. However, the higher graded pieces are quite "big", perhaps suggesting non-trivial phenomena at the level of derived categories.

As just explained, the multiplicative structure of $Z(E^*)$ is rather uninteresting. However, for the top degree part we have $Z(E^*)^3 = Z_{E^0}(E^3)$ (where the notation $Z_{E^0}(E^3)$ means the set of elements of E^3 that are centralized by all the elements of E^0), and so $Z(E^*)^3$ also has a natural structure of module over the ring $Z(E^0)$. We determine this structure explicitly, under more general assumptions, as follows (recall that we briefly mentioned an ideal $\mathfrak{I}$ in a central subalgebra of E^0, which is used to define supersingular (left) E^0-modules).

Proposition (see Proposition 2.3.6). *Let $G = \mathrm{SL}_2(\mathfrak{F})$ and assume that I is torsion-free (in particular, $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$). Let d be the dimension of G as an analytic manifold over $\mathbb{Q}_p$ (so that E^* is supported in degrees $0, \ldots, d$). One has that the $Z(E^0)$-module $Z(E^*)^d = Z_{E^0}(E^d)$ can be decomposed as a direct sum*

$$Z_{E^0}(E^d) = M \oplus \mathcal{E},$$

where M is a finite direct sum of $Z(E^0)$-modules of k-dimension 1 and where $\mathcal{E}$ is the injective hull of $\big(Z(E^0)/\mathfrak{I}Z(E^0)\big)^\vee$ as a $Z(E^0)$-module (where $(\_)^\vee$ denotes the k-linear dual).

It is interesting to compare this with the following result from [OS21] (see Proposition 1.10.5): under the same assumptions of the above proposition (or rather, under more general assumptions) one has that E^d decomposes as a direct sum $E^d = M' \oplus \mathcal{E}'$, where M' is an E^0-bimodule of dimension 1 over k and where $\mathcal{E}'$ is an E^0-bimodule that is the injective hull of $(E^0/\mathfrak{J}E^0)^\vee$ both as a left and as a right E^0-module.

Returning to the case of $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$, another remark is that also for the 2^{nd} graded piece one has $Z(E^*)^2 = Z_{E^0}(E^2)$ (a property which, in contrast to degree 3, is not at all a priori clear). In Section 2.7, we also determine the structure of $Z(E^*)^2 = Z_{E^0}(E^2)$ as a $Z(E^0)$-module, and in particular we show that it is a quotient of $Z(E^*)^3 = Z_{E^0}(E^3)$ by a certain submodule having finite dimension over k.

(a.2) In Chapter 3 we generalize some results regarding the low graded pieces of $Z(E^*)$ to the case of more general groups G. Let us introduce some notation: we choose a split maximal torus $\mathbf{T}$ of $\mathbf{G}$, in a compatible way with respect to the choice of I (i.e., since we defined I by choosing a Borel subgroup, we require $\mathbf{T}$ to be contained in such Borel subgroup). Let us denote by T the group of $\mathfrak{F}$-rational points of $\mathbf{T}$, and by T^1 the unique maximal pro-p subgroup of T (concretely, choosing a splitting $\mathbf{T} \cong \mathbb{G}_{\mathrm{m}}^n$ for some $n \in \mathbb{Z}_{\geqslant 0}$, this means $T^1 \cong (1 + \mathfrak{M})^n$). Furthermore, let C be the group of $\mathfrak{F}$-rational points of the centre of $\mathbf{G}$.

We are now able to state the description of the 0^{th} graded piece of the centre, which we prove without any assumption of G (besides the general assumptions stated at the beginning of the introduction).

Theorem (see Theorem 3.1.10). *The 0^{th} graded piece $Z(E^*)^0$ of the centre of E^* is isomorphic as a k-algebra to the group algebra*

$$k\left[(C \cdot T^1)/T^1\right] \cong k\left[C/C^1\right],$$

where C^1 is the unique maximal pro-p subgroup of C.

Again, it is interesting to notice some similarity with the result of Ardakov and Schneider on the centre of $\mathrm{Rep}_k^\infty(G)$.

Furthermore, we study the 1^{st} graded piece of the centre of E^* and we manage to obtain a complete description under the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, as stated in the following theorem. In this statement, for a commutative k-algebra R and a k-vector space V, we consider the tensor product $R \otimes_k V$, endowed with its natural structure of (free) R-module obtained by acting on the first factor.

Theorem (see Theorem 3.2.26). *If $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, then the 1^{st} graded piece $Z(E^*)^1$ of the centre of E^* is isomorphic as a $Z(E^*)^0$-module to $Z(E^*)^0 \otimes_k H^1\big(T^1/T^1_{\check{\Phi}}, k\big)$, where*

$$T^1_{\check{\Phi}} \coloneqq \mathrm{Image}\left(\textstyle\prod_{\check{\alpha} \in \check{\Phi}} \check{\alpha} \colon \prod_{\check{\alpha} \in \check{\Phi}} (1 + \mathfrak{M}) \longrightarrow T^1\right),$$

and where $\check{\Phi}$ is the set of coroots associated with the pair $(\mathbf{G}, \mathbf{T})$.

This result can be slightly simplified under some further assumptions: indeed we prove the following corollary (we will actually prove it under moderately weaker assumptions).

Corollary (see Corollary 3.2.37). *If $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ and if p does not divide the connection index of the root system (i.e., the order of the finite group given by the weight lattice modulo the root lattice), then the 1^{st} graded piece $Z(E^*)^1$ of the centre of E^* is isomorphic as a $Z(E^*)^0$-module to $Z(E^*)^0 \otimes_k H^1\big((C^\circ)^1, k\big)$, where C° is the group of $\mathfrak{F}$-rational points of the connected centre of $\mathbf{G}$ and where $(C^\circ)^1$ is the unique maximal pro-p subgroup of C°.*

This is a slightly simpler description, because for example it is clear that, under the assumptions of the corollary, $Z(E^*)^1$ is zero if $\mathbf{G}$ is semisimple, since in that case C° is trivial (actually, it is not difficult to show that also the reverse implication holds). However, this property was not clear from the description of $Z(E^*)^1$ stated in the above theorem, and it is actually even false under the more general assumptions of the theorem. Indeed we prove the following characterization.

Corollary (see Corollary 3.2.39). *Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has that $Z(E^*)^1$ is zero if and only if $\mathbf{G}$ is semisimple with fundamental group of order not divisible by p.*

We do not deal with the problem of studying $Z(E^*)^1$ in the case that $\mathfrak{F}$ is more general. However, we point out where the proof fails (see Subsection 3.2.k).

(b) In Chapter 4 we investigate the multiplicative structure of E^* in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. As already mentioned, in [OS21] Ollivier and Schneider thoroughly discuss the structure of E^* as an E^0-bimodule. Moreover, they also discuss the full multiplicative structure of $Z_{Z(E^0)}(E^*)$, but not the full multiplicative structure of E^*.

We show that the Ext-algebra is generated by its 1^{st} graded piece, more precisely we prove the following proposition.

Theorem (see Theorem 4.8.1). *Assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. Let $T^*_{E^0}E^1$ be the tensor algebra of the E^0-bimodule E^1. One has that the natural map of graded k-algebras*

$$T^*_{E^0}E^1 \longrightarrow E^*$$

is surjective and the kernel is finitely generated as a bilateral ideal.

We also explicitly compute a set of generators for such kernel, thereby completely determining the multiplicative structure of E^* in terms of the k-algebra E^0 and of the E^0-bimodule E^1. Furthermore, one may ask whether the kernel of such map is generated by its 2^{nd} graded piece: the answer is negative, even if a more informal answer would be "almost", as made precise in the following statement.

Proposition (see again Theorem 4.8.1). *Assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. Let K^* be the kernel of the multiplication map $T^*_{E^0}E^1 \longrightarrow E^*$, and let K^*_2 be the the sub-bilateral ideal of K^* generated by the 2^{nd} graded piece K^2 of K^*. One has:*

- $\star$ *K^* is generated by K^2 and K^3 (as a bilateral ideal);*
- $\star$ *K^* is not generated by K^2, and more precisely K^3_2 is properly contained in K^3, but it has finite codimension in it.*

We conclude the chapter with a presentation of E^* as a (non-graded) k-algebra. In particular, we prove the following pleasant result.

Proposition (see Proposition 4.10.4). *Assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. One has that E^* is finitely presented as a k-algebra.*

We also compute explicitly a presentation (see again the quoted proposition).

Regarding the question whether the results in Chapter 4 generalize to other groups G, in Section 4.2 we show that the multiplication map $T^*_{E^0} E^1 \longrightarrow E^*$ is not surjective for $G = \mathrm{SL}_2(\mathbb{Q}_3)$.

To conclude this introduction, let us mention another fact that we prove for a general G (with some assumptions on the field $\mathfrak{F}$). We need some preliminaries: it is easy to see that T^1 is the unique pro-p Iwahori subgroup of T, and so we have the pro-p Iwahori–Hecke algebra $H_k(T, T^1)$. This algebra admits a particularly simple description: it is canonically isomorphic to the group algebra $k[T/T^1]$. We now consider the submonoid T^+ of T consisting of the elements which contracts the group $U \coloneqq \mathbf{U}(\mathfrak{F})$ (here, $\mathbf{U}$ is the unipotent radical of a Borel that we have used in the definition of I, and an element $t \in T$ is said to contract U if $tUt^{-1} \subseteq U$). Let $H_k(T, T^1)^+ \subseteq H_k(T, T^1)$ be the subalgebra corresponding to the monoid algebra $k[T^+/T^1]$ via the fixed isomorphism $H_k(T, T^1) \cong k[T/T^1]$. It is easy to see that $H_k(T, T^1)$ is a localization of $H_k(T, T^1)^+$ and it is well-known that $H_k(T, T^1)^+$ canonically embeds into $H_k(G, I) = E^0$ (see [Vig98, II.5. Proposition]). The following result generalizes these properties to the Ext-algebra.

Proposition (see Proposition 3.3.4 and Remark 3.3.7). *Assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ without non-trivial p-th roots of 1 (in particular $p \neq 2$). Let E^*_T be the pro-p Iwahori–Hecke* Ext*-algebra relative to the pair (T, T^1), and let us keep the notation E^* for the pro-p Iwahori–Hecke* Ext*-algebra relative to the pair (G, I). One has that there exists a (non-unique) sub-graded k-algebra $E^{+,*}_T \subseteq E^*_T$ with the following properties:*

- *E^*_T is a localization of $E^{+,*}_T$;*
- *$E^{+,0}_T$ is isomorphic to $H_k(T, T^1)^+$ via the natural isomorphism $E^0_T \cong H_k(T, T^1)$;*
- *$E^{+,*}_T$ embeds into E^* as a graded k-algebra.*

Acknowledgments

First of all, I would like to thank my advisor Peter Schneider for having suggested this research topic, for carefully guiding me during these years, for his encouragement, and more generally for all his help.

I am indebted to Claudius Heyer for many discussions that gave fundamental contributions to my research outputs, for being always very interested in my work and for his friendship.

I thank Rachel Ollivier for interesting ideas she shared with me.

I am grateful to all the people I had the pleasure to meet at the University of Münster. In particular, I would like to thank my office colleagues Jonas McCandless, Julian Poedtke and Dennis Wulle and my mentor Tim De Laat.

Special thanks go to my family, and in particular my parents Gabriella Vezzani and Marco Bodon for their continuous support. Finally, I would like to thank Francesca Bernini for all the beautiful and the less beautiful moments of our life together; I cannot thank her enough for what she had to endure during these years.

My research has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy EXC 2044 – 390685587, Mathematics Münster: Dynamics – Geometry – Structure.

Chapter 1

Background

In this chapter we introduce the main notions needed to define the pro-p Iwahori–Hecke Ext-algebra and to work with it. Furthermore, we give an overview of the main properties of the pro-p Iwahori–Hecke algebra and the pro-p Iwahori–Hecke Ext-algebra, both in the general case and for the group $\mathrm{SL}_2(\mathbb{Q}_p)$. Nothing in this chapter is original work.

1.1 General setting and notation

In this section we introduce the general setting and some pieces of notation that we will use throughout. The exposition partially follows [OS19, §2].

We will always work under the following assumptions and notation. Let us consider a locally compact non-archimedean field (with non-trivial absolute value), and let us denote the order of the residue field by $q = p^f$, for some prime number p. In other words, $\mathfrak{F}$ is either a finite extension of $\mathbb{Q}_p$ of inertia degree f or the field of formal Laurent series $\mathbb{F}_q((T))$. Furthermore, let us denote by $\mathfrak{O}$ the ring of integers of $\mathfrak{F}$, by $\mathfrak{M}$ the maximal ideal of $\mathfrak{O}$, by π a chosen uniformizer (fixed once and for all), and by $\mathrm{val}_{\mathfrak{F}}$ the normalized valuation of $\mathfrak{F}$.

We consider a connected split reductive group $\mathbf{G}$ over $\mathfrak{F}$; we denote its group of $\mathfrak{F}$-rational points by $G \coloneqq \mathbf{G}(\mathfrak{F})$, and we endow it with the topology induced by $\mathfrak{F}$, thus obtaining a locally profinite group. In general, we always adopt the convention that boldface letters denote algebraic groups over $\mathfrak{F}$ and the corresponding non-boldface letter denote the locally profinite group given by its $\mathfrak{F}$-rational points. We fix a $\mathfrak{F}$-split maximal torus $\mathbf{T}$. As just explained, T denotes the locally profinite group given by its $\mathfrak{F}$-rational points, and we further define T^0 to be the unique maximal compact subgroup of T, and T^1 to be the unique pro-p Sylow subgroup of T^0. Explicitly, this can be seen as follows: $\mathbf{T}$ is isomorphic over $\mathfrak{F}$ to some copies of the multiplicative group $\mathbb{G}_{\mathrm{m}}$, say $\mathbb{G}_{\mathrm{m}}^n$; then it is easy to see that inside the group $T \cong (\mathfrak{F}^\times)^n$ there exists a unique maximal compact subgroup $T^0 \cong (\mathfrak{O}^\times)^n$, and furthermore that the unique pro-p Sylow subgroup is $T^1 \cong (1 + \mathfrak{M})^n$.

If $\mathfrak{F}$ is an extension of $\mathbb{Q}_p$, we denote by d the dimension of G as an analytic manifold over $\mathbb{Q}_p$.

We denote by J a fixed Iwahori subgroup of G, chosen in a compatible way with respect to T, and we denote by I its unique pro-p Sylow subgroup, which is called pro-p Iwahori subgroup and which will be of central importance in the whole thesis. For further details about these definitions, see Section 1.3.

We consider the normalizer $\mathbf{N}$ of $\mathbf{T}$ in $\mathbf{G}$ (it is an algebraic subgroup of $\mathbf{G}$ defined over $\mathfrak{F}$), and we consider the associated Weyl group $W_0 \coloneqq N/T$. We further define

$W := N/T^0$ (sometimes called *Iwahori Weyl group* or *generalized affine Weyl group*) and $\widetilde{W} := N/T^1$ (sometimes called *pro-p Iwahori Weyl group*). The relationships between these objects and the Iwahori and pro-p Iwahori groups will be recalled in Section 1.3.

We fix a field k of characteristic p (i.e., the same characteristic as the residue field of $\mathfrak{F}$). This will be used as a "coefficient field", in the definition of the pro-p Iwahori–Hecke algebra and of the pro-p Iwahori–Hecke Ext-algebra.

We end this section with some notational conventions which will be used throughout:

- For a group G we denote by $[G, G]$ the subgroup generated by commutators. Also in the case that G is a topological group we denote by $[G, G]$ the (algebraic) commutator subgroup, while we use the notation $\overline{[G, G]}$ for the closed commutator subgroup.
- For a field l, we use the notation $\mathrm{Hom}_l(\_,\_)$ to denote homomorphisms of l-vector spaces.
- For a vector space V over a field l, we denote by $V^\vee$ its dual space $\mathrm{Hom}_l(V, l)$.
- For a subset X of a vector space V over a field l, the notation $\mathrm{span}_l\, X$ means the sub-vector space of V generated by X.
- For a field l and a set X, we denote by $l[X]$ the free l-vector space indexed by the elements of X and, for all $x \in X$ we denote by (x) or simply by x the corresponding element in $l[X]$.
- For a ring R (with 1, not necessarily commutative) we denote by $Z(R)$ the centre of R. For an R-bimodule M, we denote by $Z_R(M)$ the $Z(R)$-module given by the elements of M that are centralized by all the elements of R. We also use the notation $Z_{R'}(M')$ for subsets $R' \subseteq R$ and $M' \subseteq M$, always meaning the set of elements of M' that are centralized by all the elements of R'. For a graded ring R^*, we denote by $Z(R^*)$ the graded centre, and for elements $r, s \in R^*$ we denote by $[r, s]_{\mathrm{gr}}$ the graded commutator. If $r \in R^i$ and $s \in R^j$ with either i or j even, the graded commutator is simply the commutator, and we generally simply write $[r, s]$.

1.2 Some notions and facts from Bruhat–Tits theory

This section consists of a brief review of the results in Bruhat–Tits theory that we will need later on. The standard reference is the original treatise by Bruhat and Tits ([BT72] and [BT84]). Our exposition also follows [Hey19, §1] and [OS19, §2.1]. Recall that we are working only in the split case, and so we can avoid some of the technicalities of the theory.

We denote by $X^*(\mathbf{T})$ the group of characters of $\mathbf{T}$ and by $X_*(\mathbf{T})$ the group of cocharacters of $\mathbf{T}$. We consider the set of roots $\Phi \subseteq X^*(\mathbf{T})$ associated with the pair $(\mathbf{G}, \mathbf{T})$. We will use the following notation for the canonical pairing:

$$\langle \_, \_ \rangle : X_*(\mathbf{T}) \times X^*(\mathbf{T}) \longrightarrow \mathbb{Z}.$$

For all root $\alpha \in \Phi$, let us denote by $\mathbf{U}_\alpha$ the unipotent subgroup of $\mathbf{G}$ attached to it. We fix a choice of positive roots Φ^+, or, equivalently, of a basis Π of the root system. We further define $\mathbf{U}$ to be the unipotent subgroup generated by the $\mathbf{U}_\alpha$'s for $\alpha \in \Phi^+$ (this is the unipotent radical of the Borel subgroup $\mathbf{TU}$).

We fix a Chevalley system $(x_\alpha)_{\alpha\in\Phi}$, which, according to [BT84, 3.2.1 and 3.2.2], is defined as follows: for each $\alpha \in \Phi$ we choose an isomorphism $x_\alpha\colon \mathbb{G}_\mathrm{a} \longrightarrow \mathbf{U}_\alpha$ of algebraic groups over $\mathfrak{F}$ in such a way that the following conditions hold.

(Ch 1) For all $\alpha \in \Phi$ there exists a homomorphism $\varphi_\alpha\colon \mathrm{SL}_2 \longrightarrow \mathbf{G}$ of algebraic groups over $\mathfrak{F}$ such that, for all $\mathfrak{F}$-algebras R and all $u \in \mathbb{G}_\mathrm{a}(R)$ one has

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

Since SL_2 is generated by its unipotent subgroups, φ_α is necessarily unique.

(Ch 2) For all $\alpha, \beta \in \Phi$, denoting by r_α the reflection on the root lattice associated with α, there exists $\varepsilon_{\alpha,\beta} \in \{-1, 1\}$ such that for all $\mathfrak{F}$-algebras R and all $u \in \mathbb{G}_\mathrm{a}(R)$ one has

$$x_{r_\alpha(\beta)}(u) = \varphi_\alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot x_\beta(\varepsilon_{\alpha,\beta} u) \cdot \varphi_\alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

We list some consequences of the above definition (see [BT84, 3.2.1]).

- The homomorphism of algebraic groups

$$\begin{aligned} \check{\alpha}\colon \mathbb{G}_\mathrm{m} &\longrightarrow \mathbf{G} \\ x &\longmapsto \varphi_\alpha \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \end{aligned}$$

  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. We denote by $\check{\Phi} \subseteq X_*(\mathbf{T})$ the set of coroots.

- For all $u \in \mathfrak{F}^\times$ the element
$$\varphi_\alpha \begin{pmatrix} 0 & u \\ -u^{-1} & 0 \end{pmatrix}$$
  lies in N, and its image in W_0 corresponds to the reflection associated with α.

- For all $\mathfrak{F}$-algebras R, all $t \in \mathbf{T}(R)$ and all $u \in \mathbb{G}_\mathrm{a}(R)$ one has

$$t \cdot \varphi_\alpha \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \cdot t^{-1} = \varphi_\alpha \begin{pmatrix} 1 & \alpha(t)u \\ 0 & 1 \end{pmatrix} \tag{1}$$

  (see [Mil17, Equation (135)]).

Let $\mathbf{C}$ be the centre of $\mathbf{G}$ and let $\mathbf{C}^\circ$ be its identity component. The standard apartment associated with $\mathbf{T}$ in the semisimple building of $\mathbf{G}$ can be defined as

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

(we see it as an $\mathbb{R}$-vector space as well as an affine space over itself). Although sufficient for most of our purposes, this is a simplified definition with respect of that of Bruhat–Tits. The correct definition is the following: one fixes a discrete special valuation x_0 of the group root datum $(T, (U_\alpha)_{\alpha\in\Phi})$ compatible with $\mathrm{val}_{\mathfrak{F}}$ (for the definition of discrete special valuation see [BT72, (6.2.1), (6.2.13)] and for the definition of compatibility with $\mathrm{val}_{\mathfrak{F}}$ see [BT84, 5.1.22.]), and then one defines the apartment as the affine space $x_0 + \mathscr{A}$, where the operation "+" is defined as in [BT72, (6.2.5)]. Then $x_0 + \mathscr{A}$ consists of all the discrete valuations of $(T, (U_\alpha)_{\alpha\in\Phi})$ compatible with $\mathrm{val}_{\mathfrak{F}}$ (see [BT84, 5.1.23. Proposition]), and it is thus independent on the choice of x_0. However, we will need to fix an x_0 as above, for example in order to fix a specific Iwahori subgroup. So we make the following choice:

$$x_0 := \begin{pmatrix} \text{the discrete special valuation} \\ \text{associated with our fixed Chevalley system } (x_\alpha)_{\alpha\in\Phi} \end{pmatrix} \tag{2}$$

(see [BT72, Examples (6.2.3) b)]). Since we are implicitly identifying $x_0 + \mathscr{A}$ with $\mathscr{A}$, we view x_0 as the zero of $\mathscr{A}$.

We have an action of the finite Weyl group W_0 on $\mathscr{A}$ induced by the action of W_0 on $X_*(\mathbf{T})$, as well as an $\mathbb{R}$-bilinear map

$$\langle \_, \_ \rangle : \mathscr{A} \times \mathrm{span}_{\mathbb{R}}(\Phi) \longrightarrow \mathbb{R}$$

induced by the pairing $\langle \_, \_ \rangle : X_*(\mathbf{T}) \times X^*(\mathbf{T}) \longrightarrow \mathbb{Z}$ (note, however, that we cannot replace $\mathrm{span}_{\mathbb{R}}(\Phi)$ with $\mathbb{R} \otimes_{\mathbb{Z}} X^*(\mathbf{T})$ in general).

We define the set of affine roots $\Phi_{\mathrm{aff}} := \Phi \times \mathbb{Z}$, and we identify Φ with $\Phi \times \{0\}$, in such a way that $\Phi \subseteq \Phi_{\mathrm{aff}}$. To every affine root $(\alpha, \mathfrak{h}) \in \Phi_{\mathrm{aff}}$ we can attach a subgroup $\mathfrak{U}_{(\alpha,\mathfrak{h})}$ of U_α defined as follows:

$$\mathfrak{U}_{(\alpha,\mathfrak{h})} := \left\{ u \in U_\alpha \;\middle|\; x_\alpha^{-1}(u) \in \mathfrak{M}^{\mathfrak{h}} \right\};$$

in other words we have transported, via x_a, the filtration $(\mathfrak{M}^n)_{n\in\mathbb{Z}}$ of $\mathfrak{F}$, thus obtaining a filtration $(\mathfrak{U}_{(\alpha,n)})_{n\in\mathbb{Z}}$ of U_α.

Moreover, for each affine root $(\alpha, \mathfrak{h}) \in \Phi_{\mathrm{aff}}$ we define its associated hyperplane in the apartment as

$$H_{(\alpha,\mathfrak{h})} := \{ x \in \mathscr{A} \mid \langle x, \alpha \rangle + \mathfrak{h} = 0 \}.$$

We also introduce the following notation for the sets of hyperplanes:

$$\mathfrak{H} := \left\{ H_{(\alpha,\mathfrak{h})} \;\middle|\; (\alpha, \mathfrak{h}) \in \Phi_{\mathrm{aff}} \right\}.$$

The connected components of $\mathscr{A} \smallsetminus \bigcup_{H\in\mathfrak{h}} H$ are called *chambers*, and there exists a unique chamber $\mathfrak{C}$, called *fundamental chamber*, such that x_0 lies in its closure and such that all the positive roots assume positive values on each point of $\mathfrak{C}$ (equivalently, on at least one point of $\mathfrak{C}$). More generally, one calls *facet* an equivalence class in $\mathscr{A}$ with respect to the following equivalence relation: two points of $\mathscr{A}$ are equivalent if (and only if) for each hyperplane in $\mathfrak{h}$ either both points lie in the hyperplane or both points lie in the complement.

One has that the exact sequence of groups

$$1 \longrightarrow T/T^0 \longrightarrow W \longrightarrow W_0 \longrightarrow 1 \tag{3}$$

is split and that there exists a (necessarily unique) splitting such that for all $\alpha \in \Phi$ the reflection $s_\alpha \in W_0$ corresponding to α is sent to the class of $\varphi_\alpha\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in $W = N/T^0$: indeed let T_{-1} be the subgroup of T generated by $\check{\alpha}(-1)$ for $\alpha \in \Phi$; by [SFW67, Lemma 56] already the surjection $N/T_{-1} \longrightarrow W_0$ splits, and the above rule gives such a splitting (we can apply Steinberg's result, which is stated for semisimple split groups, because once we have a splitting of $N/T_{-1} \longrightarrow W_0$ for the derived group we also have such a splitting for the original group). We fix once and for all the splitting of (3) described above and write $W = W_0 \ltimes T/T^0$, seeing W_0 as a subgroup of W.

There is an isomorphism of abelian groups

$$\nu_{X_*} : T/T^0 \longrightarrow X_*(\mathbf{T}) \tag{4}$$

defined as follows: for all $\bar{t} \in T/T^0$ the cocharacter $\nu_{X_*}(\bar{t})$ is the unique cocharacter determined by the property $\langle \nu_{X_*}(\bar{t}), \chi \rangle = -\operatorname{val}_{\mathfrak{F}}(\chi(t))$ for all $\chi \in X^*(\mathbf{T})$. We will slightly abuse notation and write $\nu_{X_*}(x)$ not only for $x \in T/T^0$ but also for $x \in T/T^1$ and for $x \in T$.

We also consider the map

$$\nu_{\mathscr{A}} : T/T^0 \longrightarrow X_*(\mathbf{T})/X_*(\mathbf{C}^\circ) \subseteq \mathscr{A} \tag{5}$$

induced by ν_{X_*} and also in this case we will slightly abuse notation and write $\nu_{\mathscr{A}}(x)$ not only for $x \in T/T^0$ but also for $x \in T/T^1$ and for $x \in T$. If $\mathbf{G}$ is semisimple, then $\mathbf{C}^\circ$ is trivial, and ν_{X_*} and $\nu_{\mathscr{A}}$ are the same map. Moreover, going back to the general case, for all $\alpha \in \Phi$ we have

$$\langle \nu_{X_*}(x), \alpha \rangle = \langle \nu_{\mathscr{A}}(x), \alpha \rangle,$$

where on the left we are considering the pairing $\langle \_, \_ \rangle : X_*(\mathbf{T}) \times X^*(\mathbf{T}) \longrightarrow \mathbb{Z}$ and on the right the pairing $\langle \_, \_ \rangle : \mathscr{A} \times \operatorname{span}_{\mathbb{R}}(\Phi) \longrightarrow \mathbb{R}$. Since there is no ambiguity, we will simply use the notation

$$\langle \nu(x), \alpha \rangle. \tag{6}$$

We can now define an action of T/T^0 on the apartment by affine translations via ν:

$$\begin{aligned} T/T^0 \times \mathscr{A} &\longrightarrow \mathscr{A} \\ (t, x) &\longmapsto x + \nu_{\mathscr{A}}(t). \end{aligned}$$

The actions of W_0 and T/T^0 on the apartment combine into an action of W, in the sense that the following is a well defined action

$$\begin{aligned} W \times \mathscr{A} &\longrightarrow \mathscr{A} \\ \underset{\text{(where } t \in T/T^0 \text{ and } w_0 \in W_0)}{(w_0 t, x)} &\longmapsto w_0(x + \nu_{\mathscr{A}}(t)). \end{aligned}$$

Similarly, we also have the following well defined action of W on the affine roots:

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

Moreover, the actions of W on the apartment and on the affine roots are compatible, in the sense that for all $w \in W$ and all $(\alpha, \mathfrak{h}) \in \Phi_{\text{aff}}$ one has $wH_{(\alpha,\mathfrak{h})} = H_{w(\alpha,\mathfrak{h})}$ (and this explain the choice of the signs in the above action). Another important property is that for $w \in W$, for $n_w \in N$ representing w and for $(\alpha, \mathfrak{h}) \in \Phi_{\text{aff}}$ one has

$$n_w \mathcal{U}_{(\alpha,\mathfrak{h})} n_w^{-1} = \mathcal{U}_{w(\alpha,\mathfrak{h})}, \tag{7}$$

as shown in [BT72, Proposition (6.2.10) (iii)].

Let $(\alpha, \mathfrak{h}) \in \Phi_{\mathrm{aff}}$. We consider

$$n_{(\alpha,\mathfrak{h})} \coloneqq \varphi_\alpha \begin{pmatrix} 0 & \pi^{\mathfrak{h}} \\ -\pi^{-\mathfrak{h}} & 0 \end{pmatrix} \in N.$$

One can check that the class of $n_{(\alpha,\mathfrak{h})}$ in W acts on the apartment as the affine reflection through the hyperplane $H_{(\alpha,\mathfrak{h})}$. We define W_{aff} as the subgroup of W generated by the images of the elements $n_{(\alpha,\mathfrak{h})}$ for $(\alpha, \mathfrak{h}) \in \Phi_{\mathrm{aff}}$. Now, let us recall the notation Π for the basis of Φ corresponding to our choice of positive roots, and let us consider the partial order on Φ defined as follows: for $\alpha, \beta \in \Phi$ we say that $\alpha \leqslant \beta$ if $\beta - \alpha$ is a linear combination with non-negative coefficients of elements in Π. We define

$$\Pi_{\mathrm{aff}} \coloneqq \Pi \cup \{(\alpha, 1) \mid \alpha \text{ is minimal for } \leqslant\}.$$

For all $(\alpha, \mathfrak{h}) \in \Pi_{\mathrm{aff}}$ we define $s_{\alpha,\mathfrak{h}}$ to be the class of $n_{(\alpha,\mathfrak{h})}$ in W, and we consider

$$S_{\mathrm{aff}} \coloneqq \left\{ s_{(\alpha,\mathfrak{h})} \;\middle|\; (\alpha, \mathfrak{h}) \in \Pi_{\mathrm{aff}} \right\}.$$

It is easy to see that for each $s \in S_{\mathrm{aff}}$ there exists only one $(\alpha, \mathfrak{h}) \in \Pi_{\mathrm{aff}}$ such that $s = s_{(\alpha,\mathfrak{h})}$, and so we will use the notation $(\alpha_s, \mathfrak{h}_s)$ for such element of Π_{aff}. We will also use the notation

$$n_s \coloneqq n_{(\alpha_s,\mathfrak{h}_s)} = \varphi_{\alpha_s} \begin{pmatrix} 0 & \pi^{\mathfrak{h}_s} \\ -\pi^{-\mathfrak{h}_s} & 0 \end{pmatrix} \in N$$

(in particular, this is a fixed lifting of s to N). It is possible to prove that $(W_{\mathrm{aff}}, S_{\mathrm{aff}})$ is a Coxeter system (see [Bou81, Chapitre V, §3.2, Theoréme 1 (i)]), and that it extends the Coxter System given by W_0 together with the simple reflections associated with Π (also compare compatibility with the splitting of the surjection $W \longrightarrow W_0$ which we chose in (3)).

We define the set of *positive affine roots* Φ^+_{aff} as the set of affine roots taking non-negative values on $\mathfrak{C}$; in other words $\Phi^+_{\mathrm{aff}} = \Phi^+ \cup (\Phi \times \mathbb{Z}_{\geqslant 1})$. We further define the set of *negative affine roots* $\Phi^-_{\mathrm{aff}} \coloneqq \Phi_{\mathrm{aff}} \smallsetminus \Phi^+_{\mathrm{aff}}$. There is a "*length function*" on W which extends the length function of the Coxeter system $(W_{\mathrm{aff}}, S_{\mathrm{aff}})$ and can be defined as follows (see [Lus89, §1.4]):

$$\begin{aligned} \ell\colon W &\longrightarrow \mathbb{Z}_{\geqslant 0} \\ w &\longmapsto \#\left\{(\alpha, \mathfrak{h}) \in \Phi^+_{\mathrm{aff}} \;\middle|\; w(\alpha, \mathfrak{h}) \in \Phi^-_{\mathrm{aff}}\right\}. \end{aligned}$$

Note that the cardinality is indeed finite because for all $w \in W$ and all $\mathfrak{h} \in \mathbb{Z}$, the action of w sends $\Phi \times \{\mathfrak{h}\}$ to $\Phi \times \{\mathfrak{h} + n_w\}$ for a suitable $n_w \in \mathbb{Z}$ depending on w but not on $\mathfrak{h}$. One can prove the following useful expressions to compute the length (see [Vig16, Corollary 5.10]):

$$\ell(tw_0) = \sum_{\alpha \in \Phi^+ \cap w_0 \Phi^+} |\langle \nu(t), \alpha \rangle| + \sum_{\alpha \in \Phi^+ \cap w_0 \Phi^-} |\langle \nu(t), \alpha \rangle - 1| \quad \text{for } t \in T/T^0 \text{ and } w_0 \in W, \tag{8}$$

$$\ell(w_0 t) = \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^+} |\langle \nu(t), \alpha \rangle| + \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^-} |\langle \nu(t), \alpha \rangle + 1| \quad \text{for } t \in T/T^0 \text{ and } w_0 \in W. \tag{9}$$

In particular:

$$\ell(t) = \sum_{\alpha \in \Phi^+} |\langle \nu(t), \alpha \rangle| = \frac{1}{2} \sum_{\alpha \in \Phi} |\langle \nu(t), \alpha \rangle| \qquad \text{for } t \in T/T^0. \tag{10}$$

We define Ω to be the subgroup of W given by the elements of length 0. The group W decomposes as a semidirect product

$$W = \Omega \ltimes W_{\mathrm{aff}} \tag{11}$$

and the length function is constant on the double coset $\Omega w \Omega$ for all $w \in W$ (see [Lus89, §1.5]).

1.3 The pro-p Iwahori subgroup

In this section we will recall the definition of Iwahori subgroup from [BT84], and then we will instead focus on the pro-p Iwahori subgroup, which plays the most important role in this thesis.

We first consider the group scheme $\mathbf{G}_{\mathfrak{C}}$ associated with the chamber $\mathfrak{C}$ (see [BT84, 4.6.26]). Note that this depends on the choice of x_0 in (2), and so on the choice of the Chevalley system. We then consider the identity component $\mathbf{G}_{\mathfrak{C}}^{\circ}$ of $\mathbf{G}_{\mathfrak{C}}$ define the corresponding *Iwahori subgroup* J to be $J := \mathbf{G}_{\mathfrak{C}}^{\circ}(\mathfrak{O})$, seen as a profinite group with the topology induced by $\mathfrak{O}$ (for details on the definition see [BT84, §5.2]). Furthermore, J has a unique pro-p Sylow subgroup I, which we call the *pro-p Iwahori subgroup*.

The above are the choices of Iwahori and pro-p Iwahori subgroups that we will fix throughout the thesis. However, in [BT84, §5.2] Iwahori subgroups are defined by considering an arbitrary chamber in place of the fundamental chamber $\mathfrak{C}$. Every two Iwahori subgroups are conjugate (see [Vig16, after Definition 3.14]), and so every two pro-p Iwahori subgroups are. Parahoric subgroups are defined in the same way as Iwahori subgroups, but considering arbitrary facets instead of chambers.

Note that part of the literature (e.g., [Vig16]) makes use of another definition of Iwahori subgroup, due to Haines and Rapoport, and involving the Kottwitz homomorphism (see [HR08] for the equivalence of the two definitions).

We recall from [Vig16, after Definition 3.14] that, denoting by $\mathcal{K}$ a maximal parahoric subgroup of G and by $\mathcal{K}^1$ its unique maximal open normal pro-p subgroup, one has that $\mathcal{K}/\mathcal{K}^1$ is canonically the group of $\mathfrak{O}/\mathfrak{M}$-rational points of a reductive group $\overline{\mathbf{G}}$ over $\mathfrak{O}/\mathfrak{M}$. Moreover, we recall from [Vig16, Corollary 3.28] that the Iwahori subgroup J is the preimage in $\mathcal{K}$ of a the group of k-points of a Borel subgroup of $\overline{\mathbf{G}}$, and that the same holds replacing the Iwahori subgroup J with the pro-p Iwahori subgroup I and the Borel subgroup with its idempotent radical.

If $\mathbf{G}$ is (the base change of) a reductive group defined over $\mathfrak{O}$, then we can consider the maximal parahoric subgroup $\mathcal{K} := \mathbf{G}(\mathfrak{O})$, and then we see that this definition of Iwahori and pro-p Iwahori subgroups coincide with the definition used in the introduction, where we basically defined Iwahori (respectively, pro-p Iwahori) subgroups as the preimage of the subgroup of k-rational points of a Borel (respectively, unipotent radical of a Borel) in $\mathbf{G}_k$. Note also that the assumption that $\mathbf{G}$ is the base change of a reductive group defined over $\mathfrak{O}$ is basically automatically satisfied, in the sense that one can use the classification of (connected) split reductive groups by root data to produce a (connected) split reductive group defined over $\mathfrak{O}$ whose base change to $\mathfrak{F}$ is $\mathbf{G}$.

As outlined in Section 1.1, we define T^1 to be the (clearly unique) pro-p Sylow subgroup of the profinite group T^0. We are now going to state a fundamental set-theoretical (or topological) description of the pro-p Iwahori subgroup.

Lemma 1.3.1. *The multiplication map induces a homeomorphism*

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

where the products on the left hand side are ordered in some arbitrarily chosen way.

Proof. For the fact that the multiplication map induces a bijection as in the statement see [SS97, Proposition I.2.2] and [OS14, Lemma 4.8 and its proof]. The fact that it is also a homeomorphism is clear, since it is a continuous map between compact Hausdorff topological spaces. ■

We consider the group $\widetilde{W} := N/T^1$, for which we clearly have the exact sequences

$$1 \longrightarrow T/T^1 \longrightarrow \widetilde{W} \longrightarrow W_0 \longrightarrow 1,$$

$$1 \longrightarrow T/T^0 \longrightarrow \widetilde{W} \longrightarrow W \longrightarrow 1.$$

In contrast to what happens for W, in general it is not true that any of these short exact sequences is split (for example, if $\mathbf{G} = \mathrm{SL}_2$ and $p \neq 2$, one sees that any lift in $\widetilde{W}$ of the non-trivial element of W_0 has order 4). In any case, for all $s = s_{(\alpha_s,\mathfrak{h}_s)} \in S_{\mathrm{aff}}$ we fix the following lift of s to $\widetilde{W}$:

$$\widetilde{s} := \overline{n_s} \in \widetilde{W}, \qquad \text{where} \qquad n_s = \varphi_{\alpha_s}\begin{pmatrix} 0 & \pi^{\mathfrak{h}_s} \\ -\pi^{-\mathfrak{h}_s} & 0 \end{pmatrix} \in N. \tag{12}$$

The decomposition $W = \Omega \ltimes W_{\mathrm{aff}}$ stated in (11) yields

$$\widetilde{W} = \widetilde{\Omega} \cdot \widetilde{W_{\mathrm{aff}}},$$

where $\widetilde{\Omega}$ (respectively, $\widetilde{W_{\mathrm{aff}}}$) denotes the preimage of Ω (respectively, of W_{aff}) in $\widetilde{W}$.

There are well defined conjugation actions

$$\begin{aligned} N \times T/T^0 &\longrightarrow T/T^0 \\ (n,\bar{t}) &\longmapsto n\bar{t}n^{-1} := \overline{ntn^{-1}}, \end{aligned} \qquad \begin{aligned} N \times T/T^1 &\longrightarrow T/T^1 \\ (n,\bar{t}) &\longmapsto n\bar{t}n^{-1} := \overline{ntn^{-1}}, \end{aligned}$$

because conjugation by an element $n \in N$ must preserve the unique compact subgroup T^0 of T and the unique pro-p Sylow subgroup T^1 of T^0. Since T acts trivially on T/T^1 we obtain well defined conjugation actions

$$\begin{aligned} W_0 \times T/T^0 &\longrightarrow T/T^0 \\ (w,x) &\longmapsto wxw^{-1}, \end{aligned} \qquad \begin{aligned} W_0 \times T/T^1 &\longrightarrow T/T^1 \\ (w,x) &\longmapsto wxw^{-1}. \end{aligned}$$

The notation wxw^{-1} still makes sense if $w \in W$ or if $w \in \widetilde{W}$.

The relation between the group $\widetilde{W}$ and the pro-p Iwahori subgroup I is given by the following Bruhat decomposition (for the proof see [Vig16, Proposition 3.35]):

$$G = \dot{\bigcup_{w\in\widetilde{W}}} IwI, \tag{13}$$

where we do not distinguish between an element in N and its class in $\widetilde{W} = N/T^1$: this makes sense because the double coset IwI does not depend on the choice of a representative since $T^1 \subseteq I$.

We end this section with a variation of Lemma 1.3.1, consisting of the Iwahori decomposition of some subgroups of I, which will be very important for the study of the Ext-algebra. They are defined as follows: for all $w \in \widetilde{W}$ we set

$$I_w \coloneqq I \cap wIw^{-1},$$

where, as before, we do not distinguish between classes in $\widetilde{W} = N/T^1$ and representatives in N: this makes sense because $T^1 \subseteq I$ and so every $n \in N$ representing w defines the same group nIn^{-1}. Actually, it is also true that nIn^{-1} only depends on the class of n in W, because T^0 is contained in the Iwahori subgroup J (see, e.g., [Vig16, Corollary 3.20]), and I is normal in J (alternatively, the claim also follows from the next lemma).

Lemma 1.3.2. *Let $w \in \widetilde{W}$. One has the following description of the group I_w.*

- *The product map induces a homeomorphism*

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

  where the products on the left hand side are ordered in some arbitrarily chosen way and where

$$g_w(\alpha) \coloneqq -\inf \{\langle x, \alpha \rangle \ \mid \ x \in \mathfrak{C} \cup w\mathfrak{C}\}.$$

- *For each $\alpha \in \Phi$, the constant $g_w(\alpha)$ also admits the following description:*

$$g_w(\alpha) = \min \left\{ m \in \mathbb{Z} \ \middle| \ (\alpha, m) \in \Phi^+_{\mathrm{aff}} \cap w\Phi^+_{\mathrm{aff}} \right\}.$$

Proof. See [OS19, Lemma 2.3 and Remark 2.4]. The fact that the bijection induced by the multiplication map is also a homeomorphism is clear for topological reasons, as in Lemma 1.3.1. ∎

1.4 The pro-p Iwahori–Hecke algebra

1.4.a Definition and Iwahori–Matsumoto presentation

The pro-p Iwahori–Hecke algebra has been introduced and studied by Vignéras in [Vig05]. A throughout treatment, also extending to the case of non-split groups and to the case of an arbitrary coefficient ring can be found in [Vig16]. Here we will give the definition and recall some fundamental properties, but we will only work within the assumptions of the previous sections (i.e., $\mathbf{G}$ will be split) and the ring of coefficients will be the characteristic p field k fixed in Section 1.1 (i.e., k is a field of the same characteristic as the residue field of $\mathfrak{F}$). Our exposition follows [Vig16] and [OS19, §2.2].

Before defining the pro-p Iwahori–Hecke algebra, let us consider the representation of G over k given by $k[G/I]$: this is the free k-vector space generated by the right cosets of G modulo I, endowed with the left action of G given by $g \cdot (g'I) \coloneqq (gg'I)$ for all $g, g' \in G$. Since I is open in G and compact, we can identify this space with the k-vector space of compactly supported continuous maps from G to k which are constant on the left cosets of G modulo I, by identifying, for all $g \in G$ the coset gI

with its characteristic function $\mathbb{1}_{gI}$. The action of G is then by left translations, i.e., considering $f \in k[G/I]$ seen as a function $f\colon G \longrightarrow k$ and considering $g \in G$ we have $g \cdot f = f(g^{-1}\_)$.

The representation $k[G/I]$ defined above is (one of the possible concrete ways to construct) the compact induction $\text{c-ind}_I^G 1$ of the trivial representation from I to G.

We define the pro-p Iwahori–Hecke algebra $H = H_k(G, I)$ relative to the pair (G, I) with coefficients in k in the following way:

(i) $H := \mathrm{End}_{k[G]\text{-mod}}(k[G/I])^{\mathrm{op}}$. Here we are considering the endomorphism ring in the category of representations of G over k, or, equivalently, in the category of left k-modules, and we are considering the opposite ring: this last convention has of course no real content, but it has some slight advantages in various settings.

For the sake of completeness, we are now going to give some equivalent descriptions of this k-algebra.

(ii) It is easy to check that valuation at (I) gives an isomorphism of k-vector spaces $H \cong k[G/I]^I$ (where $(\_)^I$ denotes the subspace of I-invariant vectors). The product can be characterized as follows: let us consider

$$h, h' \in H = \mathrm{End}_{k[G]\text{-mod}}(k[G/I])^{\mathrm{op}},$$

and let us write $h((I)) = \sum_{\overline{g} \in G/I} a_g(gI)$ and $h'((I)) = \sum_{\overline{g'} \in G/I} {a'}_{g'}(g'I)$ for suitable coefficients $a_g, {a'}_{g'} \in k$ (almost all of them equal to 0). Then, we see that

$$(h \cdot h')((I)) = (h' \circ h)((I)) = \sum_{\substack{\overline{g} \in G/I, \\ \overline{g'} \in G/I}} a_g {a'}_{g'}(gg'I).$$

(iii) Now, to give an alternative description, let us consider the k-vector space $k[I \backslash G/I]$ (meaning the free k-vector space generated by the double cosets). As we did for $k[G/I]$, since I is open in G and compact, we can identify this space with the k-vector space of compactly supported continuous maps from G to k that are constant on the double cosets of G modulo I, by identifying, for all $g \in G$ the double coset IgI with its characteristic function $\mathbb{1}_{IgI}$. It is then easy to see that $k[G/I]^I \cong k[I \backslash G/I]$ as a k-vector space, since also $k[G/I]^I$ can be described as a space of functions in the above way. The product can then be characterized as a convolution: namely, considering $f, f' \in k[I \backslash G/I]$, seen as functions $f, f'\colon G \longrightarrow k$, we can define a convolution product

$$f * f' := \sum_{\overline{x} \in G/I} f(x) f'(x^{-1}\_).$$

We can then check that this convolution product coincides with the product on $k[G/I]^I$ we have already described: for this it suffices to check that given two elements $\sum_{\overline{g} \in G/I} a_g(gI) \in k[G/I]^I$ and $\sum_{\overline{g'} \in G/I} {a'}_{g'}(g'I) \in k[G/I]^I$ the following equality holds:

$$\Big(\sum_{\overline{g} \in G/I} a_g \mathbb{1}_{gI} \Big) * \Big(\sum_{\overline{g'} \in G/I} {a'}_{g'} \mathbb{1}_{g'I} \Big) = \sum_{\substack{\overline{g} \in G/I, \\ \overline{g'} \in G/I}} a_g {a'}_{g'} \mathbb{1}_{gg'I},$$

and this can be done explicitly.

Note that the definition of the Hecke algebra given here follows [OS19], while the definition in [Vig16] is slightly different: there H is defined as $\mathrm{End}_{k[G]\text{-mod}}(k[I\backslash G])$, where $k[I\backslash G]$ is endowed with the G-action defined by $g\cdot(Ig') := Ig'g^{-1}$ for all $g, g' \in G$ (i.e., the difference is that right cosets are used and that there is no opposite ring). Proceeding as before, considering $h, h' \in \mathrm{End}_{k[G]\text{-mod}}(k[I\backslash G])$, and writing $h((I)) = \sum_{\overline{g}\in I\backslash G} a_g(Ig)$ and $h'((I)) = \sum_{\overline{g'}\in I\backslash G} {a'}_{g'}(Ig')$ for suitable coefficients $a_g, {a'}_{g'} \in k$ one gets

$$(h\circ h')((I)) = \sum_{\substack{\overline{g}\in I\backslash G,\\ \overline{g'}\in I\backslash G}} a_g {a'}_{g'}(Igg').$$

Then, identifying $\mathrm{End}_{k[G]\text{-mod}}(k[I\backslash G])$ with $k[I\backslash G/I]$ via evaluation at (I) as above, one gets a convolution formula

$$f\star f' := \sum_{\overline{y}\in I\backslash G} f(\_y^{-1})f'(y),$$

for $f, f' \in k[I\backslash G/I]$, seen as functions $f, f' \colon G \longrightarrow k$. But it is easy to check that this coincides with the definition above, i.e.,

$$f\star f' = f * f'.$$

Hence, identifying both $\mathrm{End}_{k[G]\text{-mod}}(k[G/I])^{\mathrm{op}}$ and $\mathrm{End}_{k[G]\text{-mod}}(k[I\backslash G])$ with the space of double cosets $k[I\backslash G/I]$, we see that the two definitions coincide, and then all the formulas proved in [Vig16] are available and we should and must *not* rewrite them with the opposite product.

The most useful description of the pro-p Iwahori–Hecke algebra is through generators and relations with respect to the Iwahori–Matsumoto basis. Let us introduce this presentation: first of all we consider the already mentioned Bruhat decomposition relative to I (see (13))

$$G = \dot{\bigcup_{w\in\widetilde{W}}} IwI.$$

It is then clear that H admits a k-basis $(\tau_w)_{w\in\widetilde{W}}$ defined by $\tau_w := \mathbb{1}_{IwI}$, seeing H as $k[I\backslash G/I]$. This is called the *Iwahori–Matsumoto basis*. To describe the multiplication with respect to this basis, we first consider the following element of H for all $s \in S_{\mathrm{aff}}$:

$$\theta_s := -(\#\mu_{\breve{\alpha}_s})\cdot \sum_{t\in\breve{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])} \tau_{\widetilde{t}}, \tag{14}$$

where the notation is as follows: $[\_]\colon (\mathfrak{O}/\mathfrak{M})^\times \longrightarrow \mathfrak{F}$ denotes the Teichmüller lift, α_s denotes the root such that $s = s_{(\alpha_s,\mathfrak{h}_s)}$ with $(\alpha_s, \mathfrak{h}_s) \in \Phi_{\mathrm{aff}}$ (and $\breve{\alpha}_s$ denotes the corresponding coroot), and finally $\mu_{\breve{\alpha}_s}$ denotes the kernel of the composite group homomorphism $\breve{\alpha}_s([\_])\colon (\mathfrak{O}/\mathfrak{M})^\times \longrightarrow T$.

The following theorem describes the multiplication with respect to the Iwahori–Matsumoto basis.

Theorem 1.4.1 (Vignéras). *The Iwahori–Matsumoto basis $(\tau_w)_{w\in\widetilde{W}}$ satisfies the following relations.*

- Braid relations: *for all $w, w' \in \widetilde{W}$ such that $\ell(ww') = \ell(w) + \ell(w')$, one has $\tau_w \cdot \tau_{w'} = \tau_{ww'}$.*
- Quadratic relations: *for all $s \in S_{\mathrm{aff}}$ one has $\tau_{\widetilde{s}}^2 = -\theta_s\cdot\tau_{\widetilde{s}} = -\tau_{\widetilde{s}}\cdot\theta_s$.*

Regarding the quadratic relations, note that the above formula is valid also for a lift of s to $\widetilde{W}$ of the form $t\widetilde{s}$ or $\widetilde{s}t$ for some $t \in \check{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])$ in place of $\widetilde{s}$, but, in general, not for an arbitrary lift.

Proof of the theorem. This is proved in greater generality in [Vig16, Proposition 4.1 and Proposition 4.4]. See also [OS19, Equation (28)] for the problems with the quadratic relations as stated in [Vig05]. ∎

It is not difficult to see that the braid relations and the quadratic relations completely determine the multiplicative structure of H, and so we obtain yet another description of this k-algebra:

(iv) $H \cong \bigoplus_{w \in \widetilde{W}} k\tau_w$, with the unique k-algebra structure satisfying the braid relations and the quadratic relations.

1.4.b Bernstein presentation

To study problems such as an explicit description of the centre, it is useful to consider a different basis of H, called *Bernstein basis* (actually, there are more than one such bases). Introducing it requires some preliminaries, and we start with the definition of orientation: an *orientation* consist in choosing, for each hyperplane $H \in \mathfrak{H}$, one of the two half-spaces (called *positive*, with the other one called *negative*) defined by such hyperplane in such a way that:

- either for all finite subsets of Φ_{aff} the intersection of the corresponding negative half-spaces is non-empty,
- or for all finite subsets of Φ_{aff} the intersection of the corresponding positive half-spaces is non-empty.

Let $v \in W_{\text{aff}}$ be a reflection through an hyperplane; we denote by $H_v \in \mathfrak{H}$ such hyperplane. Note that if v is a reflection and $w \in W$, also wvw^{-1} is a reflection: indeed it is still an element of W_{aff} because W_{aff} is normal in W (see (11)) and it is easy to see that it fixes the hyperplane H_v pointwise. In particular, under such assumptions it makes sense to consider the hyperplane $H_{wvw^{-1}}$, which is equal to wH_v.

Let o be an orientation, let $w \in W$ (or $w \in \widetilde{W}$), let $s \in S_{\text{aff}}$ and recall the notation $\mathfrak{C}$ for the fundamental chamber. We define:

$$\epsilon_o(w,s) := \begin{cases} 1 & \text{if } w\mathfrak{C} \text{ is contained in the } o\text{-negative side of } H_{wsw^{-1}}, \\ -1 & \text{if } w\mathfrak{C} \text{ is contained in the } o\text{-positive side of } H_{wsw^{-1}}, \end{cases}$$

where the hyperplane $H_{wsw^{-1}}$ makes sense by what we said above. Under the same assumptions one then defines

$$\tau_{\widetilde{s}}^{(\epsilon_o(w,s))} := \begin{cases} \tau_{\widetilde{s}} & \text{if } \epsilon_o(w,s) = 1, \\ \tau_{\widetilde{s}} + \theta_s & \text{if } \epsilon_o(w,s) = -1. \end{cases}$$

Now let $w \in \widetilde{W}$ and let us consider a reduced decomposition $w = \widetilde{s}_1 \cdots \widetilde{s}_{\ell(w)}\omega$ for suitable elements $s_1, \ldots, s_{\ell(w)} \in S_{\text{aff}}$ and $\omega \in \widetilde{\Omega}$. We define

$$B_o(w) := \tau_{\widetilde{s}_1}^{(\epsilon_o(1,s_1))} \cdots \tau_{\widetilde{s}_i}^{(\epsilon_o(s_1 \cdots s_{i-1}, s_i))} \cdots \tau_{\widetilde{s}_{\ell(w)}}^{(\epsilon_o(s_1 \cdots s_{\ell(w)-1}, s_{\ell(w)}))} \cdot \tau_\omega. \tag{15}$$

This definition does not depend on the decomposition chosen (see [Vig16, Theorem 5.25]: the decomposition considered there is slightly more general). It is then easy to see that $(B_o(w))_{w\in\widetilde{W}}$ is a k-basis of H, called the *alcove walk basis* associated with the orientation o.

We will define in a moment the Bernstein basis as a special case of the above construction. Namely, we choose a basis Π' of the root system and we define the *spherical orientation* $o_{\Pi'}$ associated with Π' to be the orientation given by the following rule: we represent each hyperplane $H \in \mathfrak{H}$ as $H = H_{(\alpha,\mathfrak{h})}$ for suitable (uniquely determined) $\alpha \in \Phi$ positive with respect to Π' and $\mathfrak{h} \in \mathbb{Z}$; we then define the $o_{\Pi'}$-positive side of H to be given by $\{x \in V \mid \langle x, \alpha\rangle + \mathfrak{h} > 0\}$. It is easy to check that a spherical orientation is indeed an orientation, because a finite intersection of positive half-spaces contains a subset of the Π'-positive Weyl chamber with bounded complement (and so, in particular, it is non-empty).

The spherical orientation o_Π associated with our fixed basis Π is called *dominant*, whereas the spherical orientation $o_{-\Pi}$ associated with the basis $-\Pi$ is called the *antidominant*.

Finally, for all bases Π' of the root system, let us define the *Bernstein basis* $(B_{o_{\Pi'}}(w))_{w\in\widetilde{W}}$ associated with the spherical orientation $o_{\Pi'}$ to be the corresponding alcove walk basis.

1.4.c Idempotents

Following [OS19, 2.2.1], in this subsection we will introduce (under a small assumption on k) a decomposition of H induced by the idempotents of the group algebra $k\left[T^0/T^1\right]$.

Let us consider the group algebra $k\left[T^0/T^1\right]$. By the braid relations, there is an injective homomorphism of k-algebra

$$\begin{aligned} k\left[T^0/T^1\right] &\longrightarrow H \\ \underset{(\text{where } t\in T^0/T^1)}{(t)} &\longmapsto \tau_t. \end{aligned}$$

We denote the group of k-characters of $k\left[T^0/T^1\right]$ by $\widehat{T^0/T^1} \coloneqq \mathrm{Hom}_{\mathrm{gps.}}\left(T^0/T^1, k^\times\right)$. Choosing a splitting $\mathbf{T} \cong \mathbb{G}_{\mathrm{m}}^{\dim \mathbf{T}}$, one sees that $T^0/T^1 \cong (\mathbb{F}_q^\times)^{\dim \mathbf{T}}$. As usual with group algebras, for all $\lambda \in \widehat{T^0/T^1}$, one has an idempotent

$$\begin{aligned} e_\lambda &\coloneqq (\# T^0/T^1)^{-1} \sum_{t\in T^0/T^1} \lambda(t)^{-1}\tau_t \\ &= (-1)^{\dim \mathbf{T}} \sum_{t\in T^0/T^1} \lambda(t)^{-1}\tau_t, \end{aligned} \tag{16}$$

which we will see both as an element of $k\left[T^0/T^1\right]$ and of H.

From the braid relations it is easy to show that the following formulas hold:

$$\tau_w \cdot e_\lambda = e_{\lambda(w^{-1}\_w)} \cdot \tau_w \qquad \text{for all } w \in \widetilde{W} \text{ and all } \lambda \in \widehat{T^0/T^1}, \tag{17}$$

$$\tau_t \cdot e_\lambda = e_\lambda \cdot \tau_t = \lambda(t) e_\lambda \qquad \text{for all } t \in T^0/T^1 \text{ and all } \lambda \in \widehat{T^0/T^1}. \tag{18}$$

Note that the last formula justifies the presence of the exponent -1 in the definition of e_λ. Regarding the first formula, the notation $\lambda(w^{-1}\_w)$ means $\lambda(n^{-1}\_n)$ for some choice of a representative $n \in N$ of $w \in \widetilde{W} = N/T^1$ (and clearly the result is independent of the choice of a representative). Actually, similarly one also sees that there is a well defined action

$$\begin{aligned} W_0 \times \widehat{T^0/T^1} &\longrightarrow \widehat{T^0/T^1} \\ (w_0, \lambda) &\longmapsto \lambda(w_0^{-1} \_ w_0). \end{aligned}$$

If we assume that $\mathbb{F}_q \subseteq k$, then there are enough k-characters, meaning more precisely that one has a k-algebra decomposition

$$k\left[T^0/T^1\right] = \prod_{\lambda \in \widehat{T^0/T^1}} k e_\lambda \qquad \text{if } \mathbb{F}_q \subseteq k.$$

Looking at (17), we see that in general e_λ is not central in H, and so even if $\mathbb{F}_q \subseteq k$, we do not have a decomposition of H induced by the e_λ's. However, let us consider the set Γ of W_0-orbits of $\widehat{T^0/T^1}$ (relative to the W_0-action we have just defined); using again (17), it is immediate to see that, for all $\gamma \in \Gamma$, the element

$$e_\gamma \coloneqq \sum_{\lambda \in \Gamma} e_\lambda$$

is central in H. Moreover e_γ is an idempotent since each e_λ is, and, if we assume again that $\mathbb{F}_q \subseteq k$, then $\sum_{\gamma \in \Gamma} e_\gamma = 1$. Therefore, we can write H as a product of k-algebras

$$H = \prod_{\gamma \in \Gamma} e_\gamma H = \prod_{\gamma \in \Gamma} H e_\gamma \qquad \text{if } \mathbb{F}_q \subseteq k.$$

1.5 The pro-p Iwahori–Hecke algebra for SL_2

In this section we will treat the pro-p Iwahori–Hecke algebra in the case $\mathbf{G} = \mathrm{SL}_2$. We will partially follow the exposition of [OS18, §3.1 and §3.2.1] and [OS21, §2.3].

Assumptions. We work with $\mathbf{G} = \mathrm{SL}_2$. We fix the ($\mathfrak{F}$-split maximal) torus $\mathbf{T}$ of diagonal matrices, and we fix the following pro-p Iwahori subgroup I:

$$I = \begin{pmatrix} 1 + \mathfrak{M} & \mathfrak{O} \\ \mathfrak{M} & 1 + \mathfrak{M} \end{pmatrix} \cap \mathrm{SL}_2(\mathfrak{F}) \tag{19}$$

(we will explain below why this actually is a pro-p Iwahori subgroup and what are the corresponding choices of the positive root and the Chevalley system).

Of the two roots of $(\mathbf{G}, \mathbf{T})$ we fix the following as the positive root:

$$\begin{aligned} \alpha_0 \colon \qquad \mathbf{T} &\longrightarrow \mathbb{G}_{\mathrm{m}} \\ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} &\longmapsto t^2. \end{aligned}$$

With notation as in the definition of Chevalley system in Section 1.1, we see that the following maps define a Chevalley system:

$$\begin{aligned} x_{\alpha_0} \colon \mathbb{G}_{\mathrm{a}} &\longrightarrow \mathbf{G} = \mathrm{SL}_2 \\ u &\longmapsto \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \end{aligned} \qquad \begin{aligned} x_{-\alpha_0} \colon \mathbb{G}_{\mathrm{a}} &\longrightarrow \mathbf{G} = \mathrm{SL}_2 \\ u &\longmapsto \begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix}, \end{aligned}$$

and that the associated maps maps $\mathrm{SL}_2 \longrightarrow \mathbf{G} = \mathrm{SL}_2$ are

$$\begin{aligned} \varphi_{\alpha_0}\colon \quad \mathrm{SL}_2 &\longrightarrow \mathbf{G} = \mathrm{SL}_2 \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) &\longmapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \end{aligned} \qquad \begin{aligned} \varphi_{\alpha_0}\colon \quad \mathrm{SL}_2 &\longrightarrow \mathbf{G} = \mathrm{SL}_2 \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) &\longmapsto {}^{\mathrm{t}}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} d & -c \\ -b & a \end{smallmatrix}\right). \end{aligned}$$

Now, as in the situation of a general $\mathbf{G}$, let us consider the pro-p Iwahori subgroup associated with the fundamental chamber $\mathfrak{C}$ (whose definition depends on the choice of the positive root and of the Chevalley system). Then, using the Iwahori decomposition stated in general in Lemma 1.3.1, we see that this pro-p Iwahori subgroup is exactly the group I defined in (19), and that such Iwahori decomposition can be rewritten as follows:

$$\begin{aligned} \mathfrak{M} \times (1 + \mathfrak{M}) \times \mathfrak{O} &\longrightarrow I \\ (c, t, b) &\longmapsto \left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} t & tb \\ tc & tbc+t^{-1} \end{smallmatrix}\right). \end{aligned} \tag{20}$$

We define s_0 to be the class in $\widetilde{W}$ of the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in N$, and s_1 to be the class in $\widetilde{W}$ of the matrix $\left(\begin{smallmatrix} 0 & -\pi^{-1} \\ \pi & 0 \end{smallmatrix}\right) \in N$. We have that $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & -\pi^{-1} \\ \pi & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)$. The two elements s_0 and s_1 are lifts of the simple reflections $s_{(\alpha_0,0)} \in S_{\mathrm{aff}}$ and $s_{(-\alpha_0,1)} \in S_{\mathrm{aff}}$ respectively: indeed we can compute

$$\begin{aligned} n_{s_{(\alpha_0,0)}} &= \varphi_{\alpha_0} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \\ n_{s_{(-\alpha_0,1)}} &= \varphi_{-\alpha_0} \begin{pmatrix} 0 & \pi \\ -\pi^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \pi^{-1} \\ -\pi & 0 \end{pmatrix}. \end{aligned}$$

Defining

$$c_{-1} \coloneqq \overline{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}} \in \widetilde{W}, \tag{21}$$

we see that

$$s_0 = \widetilde{s}_{(\alpha_0,0)}, \qquad\qquad s_1 = c_{-1}\widetilde{s}_{(-\alpha_0,1)} = \widetilde{s}_{(-\alpha_0,1)}c_{-1}.$$

From the exact sequence

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

is easy to see that one has the following set theoretic description of W:

$$\begin{aligned} W &= \overline{\left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)}^{\mathbb{Z}} \,\dot{\cup}\, \overline{\left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)}^{\mathbb{Z}} \cdot \overline{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)} \\ &= \overline{(s_0 s_1)}^{\mathbb{Z}} \,\dot{\cup}\, \overline{(s_0 s_1)}^{\mathbb{Z}} \cdot \overline{s_0}. \end{aligned}$$

Looking at the exact sequence

$$1 \longrightarrow T^0/T^1 \longrightarrow \widetilde{W} \longrightarrow W \longrightarrow 1,$$

we then get the following set-theoretical description of $\widetilde{W}$:

$$\widetilde{W} = \left(T^0/T^1 \times (s_0 s_1)^{\mathbb{Z}}\right) \dot{\cup} \left(T^0/T^1 \times \left((s_0 s_1)^{\mathbb{Z}} \cdot s_0\right)\right). \tag{22}$$

We then see (also using that $s_i^{-1} = c_{-1}s_i$ for $i \in \{0,1\}$ and that c_{-1} is central) that the elements of $\widetilde{W}$ are those in the following list (where the parameters i and ω define an indexing, i.e., there are no repetitions):

$$\begin{array}{ll} \omega & \text{for } \omega \in T^0/T^1, \\ \omega(s_0s_1)^i & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}, \\ \omega(s_1s_0)^i & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}, \\ \omega s_0(s_1s_0)^i & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 0}, \\ \omega s_1(s_0s_1)^i & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 0}. \end{array} \tag{23}$$

We will use this explicit list of elements very often in the computations. Similarly one could (as we will sometimes do) consider the analogous list with ω on the right instead of on the left. Looking again at (22), using that $s_0s_1 \in T/T^1$ and using the formulas (8) or (9) one sees that the length of the above elements are respectively 0, i, i, $i+1$ and $i+1$.

Now we consider the pro-p Iwahori–Hecke algebra H for $\mathbf{G} = \mathrm{SL}_2$. Having determined $\widetilde{W}$ explicitly, we know that the Iwahori–Matsumoto basis looks as follows:

$$\begin{array}{ll} \tau_{\omega} & \text{for } \omega \in T^0/T^1, \\ \tau_{\omega(s_0s_1)^i} & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}, \\ \tau_{\omega(s_1s_0)^i} & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}, \\ \tau_{\omega s_0(s_1s_0)^i} & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 0}, \\ \tau_{\omega s_1(s_0s_1)^i} & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 0}. \end{array} \tag{24}$$

Since we know lengths explicitly, using the braid relations it is immediate to see that H is generated by τ_{s_0}, τ_{s_1} and τ_{ω} (for $\omega \in T^0/T^1$) as a k-algebra. Actually, since T^0/T^1 is cyclic, we can do better and say that H is generated by τ_{s_0}, τ_{s_1} and τ_{ω_0}, where ω_0 is a fixed generator of the cyclic group T^0/T^1.

Now, let us look at the quadratic relations. They simplify as follows:

$$\tau_{s_i}^2 = -e_1 \cdot \tau_{s_i} = -\tau_{s_i} \cdot e_1, \qquad \text{where } i \in \{0,1\} \text{ and } e_1 \coloneqq -\sum_{\omega \in T^0/T^1} \tau_{\omega}.$$

This follows immediately from Theorem 1.4.1 (and, for s_1, from the subsequent observation about the representatives for which the quadratic relations are still valid).

We will also consider an involutive automorphism defined as follows (this is done in greater generality in [OS21, §2.2.6]). Let $\varpi \coloneqq \left(\begin{smallmatrix} 0 & 1 \\ \pi & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathfrak{F})$. We can consider the automorphism

$$\begin{aligned} \mathrm{conj}_{\varpi} \colon G &\longrightarrow G \\ g &\longmapsto \varpi g \varpi^{-1}, \end{aligned}$$

which is clearly an involution. Moreover, we see that $\mathrm{conj}_{\varpi}(I) = I$ (equivalently, $\mathrm{conj}_{\varpi}(I) \subseteq I$), for example by working with the "Iwahori decomposition" stated in (20). It follows that conj_{ϖ} induces an involutive automorphism of the representation $k\,[G/I]$, and this in turn induces an automorphism

$$\Gamma_{\varpi} \colon H \longrightarrow H. \tag{25}$$

If we describe H as $k[I\backslash G/I]$, it is easy to see that $\Gamma_\varpi(\mathbb{1}_{IgI}) = \mathbb{1}_{I\varpi g\varpi^{-1}I}$ for all $g \in G$. Taking also into account that conj_ϖ induces an automorphism of $\widetilde{W}$, this shows that

$$\Gamma_\varpi(\tau_w) = \tau_{\varpi w \varpi^{-1}} \qquad \text{for all } w \in \widetilde{W},$$

and, more specifically,

$$\begin{aligned} \Gamma_\varpi(\tau_\omega) &= \tau_{\omega^{-1}} && \text{for all } \omega \in T^0/T^1, \\ \Gamma_\varpi(\tau_{s_0}) &= \tau_{s_1}, \\ \Gamma_\varpi(\tau_{s_1}) &= \tau_{s_0}. \end{aligned} \tag{26}$$

1.6 The centre of the pro-p Iwahori–Hecke algebra

The centre of the pro-p Iwahori–Hecke algebra has been studied by Vignéras in [Vig14], building on her previous work in [Vig05] and on Schmidt's Diplomarbeit [Sch09]. We will state the main results here, starting with the explicit description the centre as a k-vector space.

Theorem 1.6.1 (Schmidt, Vignéras). *Let o be a spherical orientation. Moreover, let us consider orbits of the conjugation action of W_0 on T/T^1. The following elements form a k-basis of the centre $Z(H)$ of the pro-p Iwahori Hecke algebra H:*

$$z_\mathcal{O} \coloneqq \sum_{x \in \mathcal{O}} B_o(x) \qquad \text{for all the } W_0\text{-orbits } \mathcal{O} \subseteq T/T^1.$$

Moreover, for all orbits $\mathcal{O}$ as above, the element $z_\mathcal{O}$ does not depend on the chosen spherical orientation.

Proof. See [Vig14, Theorem 1.3 and Lemma 2.1]. What is denoted by $\Lambda(1)$ in loc. cit. is T/T^1 in our context, since G is $\mathfrak{F}$-split. ■

The next theorem we are going to state gives a clear picture of the algebraic properties of the centre and the full algebra. We will not use this result for any proof, but it is nevertheless useful to state it both for its own importance and to draw comparisons with the Ext-algebra and its centre later on (see Remark 2.1.2, in which we will give counterexamples in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$).

Theorem 1.6.2 (Schmidt, Vignéras). *The centre $Z(H)$ of the pro-p Iwahori Hecke algebra H is a finitely generated (commutative) k-algebra, hence Noetherian. The pro-p Iwahori Hecke algebra H is a finitely generated as a module over its centre $Z(H)$.*

Proof. See [Vig14, Theorem 1.3]. ■

We have the following immediate but very important consequence: since H is finitely generated module over the Noetherian commutative k-algebra $Z(H)$, it is Noetherian as a $Z(H)$-module, hence in particular it is a Noetherian k-algebra.

1.7 The centre of the pro-p Iwahori–Hecke algebra for SL_2

Assumptions. We assume that $\mathbf{G} = \mathrm{SL}_2$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Later on, we will add the assumption that $\mathbb{F}_q \subseteq k$.

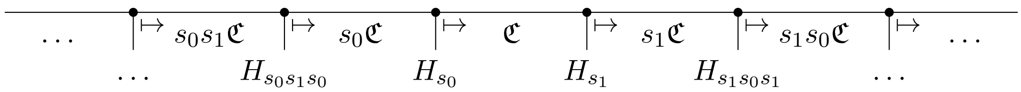
Under the above assumptions it is possible to achieve a very explicit description of the ring structure of the centre $Z(H)$. This is given in [OS18, §3.2.4], which we will follow.

Let us fix the dominant spherical orientation o_Π. Recall from (22) that we have a direct product decomposition $T/T^1 = T^0/T^1 \times (s_0 s_1)^{\mathbb{Z}}$, with $s_0 s_1$ represented by the matrix $\left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)$. It is also easy to see that the non-trivial element of W_0 act as the inverse on T/T^1. Using also that T^0/T^1 is the cyclic group of order $q-1$, one then explicitly determines the W_0-orbits in T/T^1, finding the following k-basis for $Z(H)$ according to Theorem 1.6.1:

$$\begin{aligned}
&B_{o_\Pi}(1), && \\
&B_{o_\Pi}(c_{-1}) && \text{if } p \neq 2, \\
&B_{o_\Pi}(\omega) + B_{o_\Pi}(\omega^{-1}) && \text{for } \{\omega, \omega^{-1}\} \subseteq T^0/T^1 \smallsetminus \{1, c_{-1}\}, \\
&B_{o_\Pi}(\omega(s_0 s_1)^i) + B_{o_\Pi}(\omega^{-1}(s_1 s_0)^i) && \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}.
\end{aligned}$$

Let us write this explicitly with respect to the Iwahori–Matsumoto basis. Making use of the formula $B_{o_\Pi}(tt') = B_{o_\Pi}(t) \cdot B_{o_\Pi}(t')$ for $t, t' \in T/T^1$ such that $\ell(tt') = \ell(t) + \ell(t')$ (see [Vig16, Corollary 5.28]), and also of the fact that $B_{o_\Pi}(\omega) = \tau_\omega$ for all $\omega \in T^0/T^1$ (since such ω's have length zero), we are reduced to compute the Bernstein elements $B_{o_\Pi}(s_0 s_1)$ and $B_{o_\Pi}(s_1 s_0)$.

The apartment can be drawn in the following way, where the small arrows represent the dominant spherical orientation:



One then sees that

$$\begin{aligned}
\epsilon_{o_\Pi}(1, s_0) &= 1, & \epsilon_{o_\Pi}(s_0, s_1) &= 1, \\
\epsilon_{o_\Pi}(1, s_1) &= -1, & \epsilon_{o_\Pi}(s_1, s_0) &= -1.
\end{aligned}$$

To apply the definition (15), there is the small problem that, while the element s_0 is equal to $\widetilde{s}_{(\alpha_0, 0)}$, the element s_1 is equal to $c_{-1}\widetilde{s}_{(-\alpha_0, 1)}$ rather than to $s_1' := \widetilde{s}_{(-\alpha_0, 1)}$. So working for the moment with s_1' instead of s_1, we find that

$$\begin{aligned}
B_{o_\Pi}(s_0 s_1') &= \tau_{s_0}^{(\epsilon_{o_\Pi}(1, s_0))} \cdot \tau_{s_1'}^{(\epsilon_{o_\Pi}(s_0, s_1'))} \\
&= \tau_{s_0} \cdot \tau_{s_1'}, \\
B_{o_\Pi}(s_1' s_0) &= \tau_{s_1'}^{(\epsilon_{o_\Pi}(1, s_1'))} \cdot \tau_{s_0}^{(\epsilon_{o_\Pi}(s_1', s_0))} \\
&= (\tau_{s_1'} + e_1) \cdot (\tau_{s_0} + e_1).
\end{aligned}$$

Multiplying both sides of each of the above equations by $\tau_{c_{-1}} = B_{o_\Pi}(c_{-1})$ (on the left, or, equivalently, on the right) we get that

$$\begin{aligned}
B_{o_\Pi}(s_0 s_1) &= \tau_{s_0} \cdot \tau_{s_1}, \\
B_{o_\Pi}(s_1 s_0) &= (\tau_{s_1} + e_1) \cdot (\tau_{s_0} + e_1).
\end{aligned}$$

Therefore, from our computations we deduce the following description of the canonical basis of $Z(H)$:

$$\begin{aligned}
&\tau_1, && \\
&\tau_{c_{-1}} && \text{if } p \neq 2, \\
&\tau_\omega + \tau_{\omega^{-1}} && \text{for } \{\omega, \omega^{-1}\} \subseteq T^0/T^1 \smallsetminus \{1, c_{-1}\}, \\
&\tau_\omega(\tau_{s_0}\tau_{s_1})^i + \tau_{\omega^{-1}}\big((\tau_{s_1}+e_1)(\tau_{s_0}+e_1)\big)^i && \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}.
\end{aligned} \tag{27}$$

Lemma 1.7.1 (Ollivier, Schneider). *Assume that $\mathbb{F}_q \subseteq k$. Let $\gamma \in \Gamma$, and let us write it as $\gamma = \{\lambda, \lambda^{-1}\}$.*

- *If $\lambda = \lambda^{-1}$ then the following is a k-basis of $e_\gamma Z(H)$:*

$$\begin{aligned}
&e_\lambda, && \\
&x_{\lambda,i} \coloneqq e_\lambda B_{o_\Pi}((s_0s_1)^i) + e_\lambda B_{o_\Pi}((s_1s_0)^i) && \text{for } i \in \mathbb{Z}_{\geqslant 1}.
\end{aligned}$$

- *If $\lambda \neq \lambda^{-1}$ then the following is a k-basis of $e_\gamma Z(H)$:*

$$\begin{aligned}
&e_\lambda + e_{\lambda^{-1}}, && \\
&x_{\lambda,i} \coloneqq e_\lambda B_{o_\Pi}((s_0s_1)^i) + e_{\lambda^{-1}} B_{o_\Pi}((s_1s_0)^i) && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
&x_{\lambda^{-1},i} \coloneqq e_{\lambda^{-1}} B_{o_\Pi}((s_0s_1)^i) + e_\lambda B_{o_\Pi}((s_1s_0)^i) && \text{for } i \in \mathbb{Z}_{\geqslant 1}.
\end{aligned}$$

Moreover, setting $x_\mu \coloneqq x_{\mu,1}$ for all $\mu \in \widehat{T^0/T^1}$, one has that $x_\mu^i = x_{\mu,i}$. Finally, denoting by X_μ an indeterminate for all $\mu \in \widehat{T^0/T^1}$, one has isomorphisms of k-algebras

$$\begin{aligned}
k[X_\lambda] &\xrightarrow{\cong} e_\gamma Z(E^0) && \\
1 &\longmapsto e_\gamma && \text{if } \gamma = \{\lambda\}, \\
X_\lambda &\longmapsto x_\lambda && \\
k[X_\lambda, X_{\lambda^{-1}}]/(X_\lambda \cdot X_{\lambda^{-1}}) &\xrightarrow{\cong} e_\gamma Z(E^0) && \\
1 &\longmapsto e_\gamma && \text{if } \gamma = \{\lambda, \lambda^{-1}\} \text{ with } \lambda \neq \lambda^{-1}. \\
X_\lambda &\longmapsto x_\lambda && \\
X_{\lambda^{-1}} &\longmapsto x_{\lambda^{-1}} &&
\end{aligned}$$

Proof. See [OS18, §3.2.4]. ∎

To conclude this overview of the centre of H for SL_2, we define the element

$$\zeta \coloneqq \tau_{s_0} \cdot \tau_{s_1} + (\tau_{s_1} + e_1) \cdot (\tau_{s_0} + e_1), \tag{28}$$

which, as we have seen, lies in the centre of H. It has the property that $k[\zeta]$ is isomorphic to the polynomial algebra $k[X]$. Although we will not use this, let us remark that the importance of ζ stems from the fact that $k[\zeta]$ is the k-algebra $\mathcal{Z}^\circ(H)$ introduced in [Oll14, §2.3.1], and the ideal $\zeta k[\zeta]$ is the ideal $\mathfrak{I}$ introduced in [Oll14, §5.2] (see [OS18, proof of Lemma 3.7]). Starting from these results, in [OS21, §2.3.5], the element ζ is used to define a notion of supersingularity.

1.8 Some results on the cohomology of pro-p groups

In this section we will make a brief digression on the cohomology of pro-p groups. We do this here because it will be needed the next section, and because we will use these results very often in the whole thesis.

For all pro-p groups K (or more generally profinite groups), and for all discrete (or smooth, according to different choices of terminology) K-modules A, we will denote by $H^*(K, A)$ the continuous cohomology of K with coefficients in A.

We start by recalling the definition of conjugation: let L be a locally profinite group, let $K \subseteq L$ be a closed compact subgroup, and let $x \in L$. Let us consider an abelian group A, which we endow with the trivial action of L and of its subgroups (one usually defines conjugation for more general L-modules, but we will only need this case). We denote by

$$x_* \colon H^*(K, A) \longrightarrow H^*(xKx^{-1}, A) \tag{29}$$

the conjugation map on cohomology, i.e., the map functorially induced by the conjugation map $\mathrm{conj}_{x^{-1}} \colon xKx^{-1} \longrightarrow K$. Now let $y \in K$: we recall from [NSW13, (1.6.3) Proposition] that the map $y_* \colon H^*(K, k) \longrightarrow H^*(K, k)$ is the identity (note that in loc. cit. the ambient group L is assumed to be profinite, but the proof, carried out by dimension shifting, does not use such assumption). Since $(xy)_* = (x)_* \circ (y)_*$, we conclude that x_* only depends of the class of x in the space of left cosets L/K.

For the rest of this section, we will treat cup products and cup products algebras. Whenever one has discrete G modules A, B and C with a $\mathbb{Z}$-bilinear K-equivariant map $A \times B \longrightarrow C$, there is a well defined cup product

$$\smile \colon H^i(K, A) \times H^j(K, B) \longrightarrow H^{i+j}(K, C) \tag{30}$$

for $i, j \in \mathbb{Z}_{\geqslant 0}$ (see [NSW13, Chapter I, §4]). In particular, we have the cup-product algebra $H^*(K, k)$ (endowing k with the trivial G-action).

In the literature, one usually finds statements about the cup-product algebra $H^*(K, \mathbb{F}_p)$; however, it is easy to extend such results to case of general k, because there is a natural isomorphism

$$H^*(K, k) \cong H^*(K, \mathbb{F}_p) \otimes_{\mathbb{F}_p} k. \tag{31}$$

This can be shown as follows: we can fix an $\mathbb{F}_p$-basis $(a_i)_i$ of k, and compute

$$H^*(K, k) = H^*\Big(K, \bigoplus_i \mathbb{F}_p a_i\Big) \cong \bigoplus_i H^*(K, \mathbb{F}_p a_i) \cong H^*(K, \mathbb{F}_p) \otimes_{\mathbb{F}_p} k,$$

where we have used that $H^*(K, \_)$ commutes with direct limits (see [Ser02, Chapter I, Proposition 8]) and hence with arbitrary direct sums, being an additive functor.

The first cohomology group of a pro-p group K is quite easy to study explicitly; to do this it is convenient to define the *Frattini quotient*:

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

The Frattini quotient is an abelian pro-p group in which p-powers are trivial, and so we may also regard it as a $\mathbb{F}_p$-vector space. We see that

$$H^1(K, k) \cong \mathrm{Hom}_{\text{top. gps.}}(K, k) \cong \mathrm{Hom}_{\text{top. gps.}}((K)_\Phi, k), \tag{32}$$

and that if $(K)_\Phi$ is finite-dimensional as a $\mathbb{F}_p$-vector space then

$$H^1(K, k) \cong \mathrm{Hom}_{\mathbb{F}_p}((K)_\Phi, k). \tag{33}$$

We will call a pro-p group K *uniform* if it is topologically finitely generated, torsion-free and powerful; by definition, the latter term means that the following condition is satisfied:

$$\begin{aligned} \overline{[K,K]} &\subseteq \overline{K^p} && \text{if } p \text{ is odd,} \\ \overline{[K,K]} &\subseteq \overline{K^4} && \text{if } p = 2. \end{aligned}$$

This definition of uniform pro-p groups is given as a characterization in [DDSMS03, Theorem 4.5].

The cohomology algebra of a uniform pro-p group admits a very simple description, according to the following non-trivial result of Lazard.

Theorem 1.8.1 (Lazard). *Let K be a uniform pro-p group. One has natural isomorphisms of k-algebras*

$$H^*(K,k) \cong \bigwedge\nolimits^* \left(H^1(K,k)\right) \cong \bigwedge\nolimits^* \left(\operatorname{Hom}_{\mathbb{F}_p}((K)_\Phi\,, k)\right),$$

where $\bigwedge^*(\_)$ denotes the exterior algebra. Moreover, $(K)_\Phi$ is a finite-dimensional $\mathbb{F}_p$-vector space, and so the above algebra has finite dimension as a k-vector space.

Proof. This is [Laz65, (2.5.7.1)]. Note, however, that the language used is not that of uniform pro-p groups but that of "équi-p-valué" groups. For a proof in the modern language see instead [SW00, Theorem 5.1.5]. In these references $k = \mathbb{F}_p$, but for general k we may use (31). ■

Lazard also proved a second result in the same spirit as the above theorem, with weaker assumptions and weaker conclusions. To state it, we recall the definition of analytic pro-p group and of Poincaré group. An *analytic pro-p group* is a pro-p group endowed with a structure of finite-dimensional analytic manifold over $\mathbb{Q}_p$, where the multiplication and the inverse are analytic maps. This is an intrinsic property of a pro-p group, in the sense that given an arbitrary pro-p group there exists at most one structure of analytic manifold making it into an analytic pro-p group (see [Laz65, Intrduction, §5 and Chapitre 3, (3.2.2)]).

Now, let us define Poincaré groups as in [Ser02, Chapter I, §4.5]. Let $n \in \mathbb{Z}_{\geqslant 1}$; a pro-$p$ group K is called a *Poincaré group* of dimension n if it satisfies the following properties:

- for all $i \in \mathbb{Z}_{\geqslant 0}$ the cohomology group $H^i(K,\mathbb{F}_p)$ is a finite-dimensional $\mathbb{F}_p$-vector space;
- the cohomology group $H^n(K,\mathbb{F}_p)$ is a one-dimensional $\mathbb{F}_p$-vector space;
- for all $i > n$ the cohomology group $H^i(K,\mathbb{F}_p)$ is zero;
- for all $i \in \{0,\dots,n\}$, the cup product

  $$\smile\colon H^i(K,\mathbb{F}_p) \times H^{n-i}(K,\mathbb{F}_p) \longrightarrow H^n(K,\mathbb{F}_p)$$

  is a non-degenerate bilinear map.

If K is a Poincaré group of dimension n, note that all the properties above still hold if we replace $\mathbb{F}_p$ by k, thanks to (31).

We can now state the above mentioned second result of Lazard.

Theorem 1.8.2 (Lazard). *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.*

Proof. See [SW00, Theorem 5.1.9 and the following lines]. ■

As mentioned before, disregarding the statement about the dimension, we see that this second theorem has both weaker assumptions and weaker conclusions than the first theorem: indeed a uniform pro-p group is also an analytic pro-p group (see [DDSMS03, Theorem 8.1]) and a pro-p group whose cohomology algebra is an exterior algebra clearly satisfies the definition of Poincaré group.

1.9 The Ext-algebra

In this section we will define the pro-p Iwahori–Hecke Ext-algebra, introduced by Ollivier and Schneider in [OS19], and we will state some of the main results proved there.

1.9.a Definition and description in terms of group cohomology

Let us denote by $\mathrm{Rep}_k^\infty(G)$ the category of smooth representations of G over k. This is an abelian category with enough injective objects (see [Vig96, I.5.9]), and so we can define Ext groups via injective resolutions.

We define

$$E^* := \mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(G)}\left(k\left[G/I\right], k\left[G/I\right]\right)^{\mathrm{op}},$$

as a graded k-algebra with respect to the (opposite of the) Yoneda product. From the definition it follows that $E^0 = H$.

At least as a k-vector space, the algebra E^* admits a concrete description in terms of profinite group cohomology. To show this, let us choose an injective resolution $k\left[G/I\right] \longrightarrow J^\bullet$ in $\mathrm{Rep}_k^\infty(G)$. The restriction functor from $\mathrm{Rep}_k^\infty(G)$ to $\mathrm{Rep}_k^\infty(I)$ preserves injective objects (see [Vig96, Chapitre I, 5.9 d)]), and so our resolution is also an injective resolution in $\mathrm{Rep}_k^\infty(I)$. By the Frobenius reciprocity for compact induction, the functors $\mathrm{Hom}_{\mathrm{Rep}_k^\infty(G)}\left(k\left[G/I\right], \_\right)$ and $(\_)^I$ are isomorphic, and so the two complexes $\mathrm{Hom}_{\mathrm{Rep}_k^\infty(G)}\left(k\left[G/I\right], J^\bullet\right)$ and $(J^\bullet)^I$ are isomorphic. The cohomology of the former complex is $\mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(G)}\left(k\left[G/I\right], k\left[G/I\right]\right)$, while the cohomology of the latter complex is $H^*\left(I, k\left[G/I\right]\right)$, and hence

$$E^* = H^*\left(I, k\left[G/I\right]\right).$$

From this identification, however, it is not clear at all how the product in E^* can be described in in $H^*\left(I, k\left[G/I\right]\right)$, but we will see later on a non-trivial theorem describing the multiplicative structure in terms of cohomological operations.

A fundamental tool to study the Ext-algebra is given by (a variation of) the Shapiro isomorphism. First of all, for all $w \in \widetilde{W}$ we define

$$\mathbf{X}(w) := k\left[IwI/I\right] \subseteq k\left[G/I\right]$$

(the definition makes sense because $T^1 \subseteq I$ and so every $n \in N$ representing w defines the same group InI). From the already mentioned Bruhat decomposition (see (13))

$$G = \dot{\bigcup_{w \in \widetilde{W}}} IwI,$$

we obtain the following k-vector space decomposition:

$$E^* = H^*\left(I, k\left[G/I\right]\right) = \bigoplus_{w \in \widetilde{W}} H^*\left(I, \mathbf{X}(w)\right).$$

This can be seen as an extension of the Iwahori–Matsumoto basis, in the sense that in degree zero this is exactly the decomposition $E^0 = H = \bigoplus_{w\in\widetilde{W}} k\tau_w$, since $H^0(I, \mathbf{X}(w)) = \mathbf{X}(w)^I = k\mathbb{1}_{IwI}$.

1.9.b Shapiro isomorphism

We are now going to further simplify the description of E^* in terms of group cohomology, by making use of the Shapiro isomorphism.

For all $w \in \widetilde{W}$ let us recall the subgroup $I_w := I \cap wIw^{-1}$ of I defined in Section 1.3. It is easy to see that the following are well defined bijections, one the inverse of the other:

$$\begin{aligned} IwI/I &\longrightarrow I/I_w \\ iwI &\longmapsto iI_w, \end{aligned} \qquad\qquad \begin{aligned} I/I_w &\longrightarrow IwI/I \\ iI_w &\longmapsto iwI. \end{aligned}$$

Now, the representation $k[I/I_w]$ of the group I is the smooth induction $\mathrm{Ind}_{I_w}^I(k)$ of the trivial representation from I_w to I, and one has the Shapiro isomorphism $H^*(I, \mathrm{Ind}_{I_w}^I(k)) \cong H^*(I_w, k)$ (see, e.g., [NSW13, (1.6.4) Proposition]). Combining these observations, we get the following isomorphism Sh_w, which we will call again Shapiro isomorphism:

$$\mathrm{Sh}_w\colon H^j(I, k[IwI/I]) \xrightarrow[\substack{\text{induced by} \\ k[IwI/I] \xrightarrow{\cong} k[I/I_w] \\ iwI \longmapsto iI_w}]{\cong} H^j(I, k[I/I_w]) \xrightarrow[\substack{\text{Shapiro isomorphism,} \\ \text{i.e., the map induced by} \\ \text{the inclusion } I_w \hookrightarrow I \text{ and by} \\ k[I/I_w] \longrightarrow k \\ iI_w \longmapsto \begin{cases} 1 & \text{if } iI_w = I_w \\ 0 & \text{otherwise} \end{cases}}]{\cong} H^j(I_w, k).$$

It is easy to see that Sh_w can also be described as the following composite map

$$\mathrm{Sh}_w\colon H^j(I, k[IwI/I]) \xrightarrow[\text{res}]{} H^j(I_w, k[IwI/I]) \xrightarrow[\substack{\text{induced by} \\ \mathrm{ev}_w\colon\ k[IwI/I] \longrightarrow k \\ f \longmapsto f(w)}]{} H^j(I_w, k). \tag{34}$$

We have thus obtained the following description of E^* (as a k-vector space):

$$E^* = \bigoplus_{w\in\widetilde{W}} H^*(I, \mathbf{X}(w)) \xrightarrow[\cong]{\bigoplus_{w\in\widetilde{W}} \mathrm{Sh}_w} \bigoplus_{w\in\widetilde{W}} H^*(I_w, k). \tag{35}$$

1.9.c Cup product

We are now going to describe a cup product on $H^*(I, k[G/I])$ (i.e., on E^*, seen as graded k-vector space). This is not the same as the (opposite of the) Yoneda product.

We consider the G-equivariant biliner map

$$k[G/I] \times k[G/I] \longrightarrow k[G/I]$$

defined by the pointwise product (here we see the elements of $k[G/I]$ as functions $G \longrightarrow k$), and then we can consider the associated cup product

$$\smile\colon H^i(I, k[G/I]) \times H^j(I, k[G/I]) \longrightarrow H^{i+j}(I, k[G/I]) \qquad \text{for } i, j \in \mathbb{Z}_{\geqslant 0}$$

as in (30). So we have a structure of graded-commutative k-algebra on $H^*(I, k[G/I])$ with respect to the cup product (see [NSW13, (1.4.4) Proposition]). Note that this is in general different from the (opposite of the) Yoneda product, as one easily sees in degree 0. It is easy to see that for all $w, v \in \widetilde{W}$ with $w \neq v$ (and all $i, j \in \mathbb{Z}_{\geqslant 0}$) one has $H^i(I, \mathbf{X}(w)) \smile H^j(I, \mathbf{X}(v)) = 0$ and $H^i(I, \mathbf{X}(w)) \smile H^j(I, \mathbf{X}(w)) \subseteq H^{i+j}(I, \mathbf{X}(w))$. Looking at the description of Sh_w we gave in (34), and using the fact that the cup product commutes with restriction, that the cup product is functorial and that $\mathrm{ev}_w(ff') = \mathrm{ev}_w(f)\,\mathrm{ev}_w(f')$, we see that the following diagram is commutative.

$$\begin{tikzcd}
H^i(I, \mathbf{X}(w)) \times H^j(I, \mathbf{X}(w)) \arrow[r, "\smile"] \arrow[d, "\mathrm{Sh}_w"', "\cong"] & H^{i+j}(I, \mathbf{X}(w)) \arrow[d, "\mathrm{Sh}_w"', "\cong"] \\
H^i(I_w, k) \times H^j(I_w, k) \arrow[r, "\smile"] & H^{i+j}(I_w, k).
\end{tikzcd}$$

1.9.d The product in the Ext-algebra

We are now going to state the already mentioned theorem on the explicit description of the (opposite of the) Yoneda product on E^* in terms of cohomological operations (restriction, corestriction, cup product and conjugation), together with further related results.

Theorem 1.9.1 (Ollivier, Schneider). *Let us fix a family of representatives $(\dot{w})_{w\in\widetilde{W}}$ for the elements of $\widetilde{W} = N/T^1$. Let $v, w \in \widetilde{W}$, let $i, j \in \mathbb{Z}_{\geqslant 0}$. Furthermore, let $\alpha \in H^i(I, \mathbf{X}(v))$ and let $\beta \in H^j(I, \mathbf{X}(w))$. One has*

$$\alpha \cdot \beta = \sum_{\substack{u \in \widetilde{W} \\ \text{s.t. } IuI \subseteq IvI \cdot IwI}} \gamma_u$$

with $\gamma_u \in H^{i+j}(I, \mathbf{X}(u))$ and

$$\mathrm{Sh}_u(\gamma_u) = \sum_{\overline{h} \in I_{v^{-1}} \backslash (v^{-1}Iu \cap IwI)/I_{u^{-1}}} \mathrm{cores}_{I_u}^{I_u \cap \dot{u}h^{-1}Ih\dot{u}^{-1}} \left(\widetilde{\Gamma}_{u,h}\right)$$

with

$$\widetilde{\Gamma}_{u,h} \coloneqq \mathrm{res}^{I\cap \dot{u}h^{-1}Ih\dot{u}^{-1}}_{I_u \cap \dot{u}h^{-1}Ih\dot{u}^{-1}} \left(a_* \,\mathrm{Sh}_v(\alpha)\right) \smile \mathrm{res}^{uIu^{-1}\cap \dot{u}h^{-1}Ih\dot{u}^{-1}}_{I_u \cap \dot{u}h^{-1}Ih\dot{u}^{-1}} \left((a\dot{v}c)_* \,\mathrm{Sh}_w(\beta)\right),$$

where $h = c\dot{w}d = \dot{v}^{-1}a^{-1}\dot{u}$ with $a, c, d \in I$.

Note that the two conjugations in the last displayed equation do make sense because, using the notation of the theorem, we have

$$\begin{aligned}
a \cdot (I \cap \dot{v}I\dot{v}^{-1}) \cdot a^{-1} &= I \cap a\dot{v}I\dot{v}^{-1}a^{-1} \\
&= I \cap \dot{u}h^{-1}Ih\dot{u}^{-1}, \\
(a\dot{v}c) \cdot (I \cap \dot{w}I\dot{w}^{-1}) \cdot (a\dot{v}c)^{-1} &= a\dot{v}I\dot{v}^{-1}a^{-1} \cap a\dot{v}c\dot{w}I\dot{w}^{-1}c^{-1}\dot{v}^{-1}a^{-1} \\
&= \dot{u}h^{-1}Ih\dot{u}^{-1} \cap \dot{u}d^{-1}Id\dot{u}^{-1} \\
&= \dot{u}h^{-1}Ih\dot{u}^{-1} \cap \dot{u}I\dot{u}^{-1}.
\end{aligned}$$

Proof of the theorem. See [OS19, Proposition 5.3]. ■

Given $v, w \in \widetilde{W}$, in view of the theorem it is useful to have at least some necessary conditions on $u \in \widetilde{W}$ for the property $IuI \subseteq IvI \cdot IwI$ to be satisfied.

Lemma 1.9.2. *Let $u, v, w \in \widetilde{W}$ be such that $IuI \subseteq IvI \cdot IwI$. One has the following properties:*

(i) $|\ell(v) - \ell(w)| \leqslant \ell(u) \leqslant \ell(v) + \ell(w)$*;*

(ii) if $\ell(vw) < \ell(v) + \ell(w)$*, then* $\ell(u) < \ell(v) + \ell(w)$*;*

(iii) if $\ell(vw) = \ell(v) + \ell(w)$*, then* $u = vw$*.*

Proof. Property (i) is proved in [OS19, Lemma 2.11]. Property (ii) follows from [OS19, Remark 2.10]. Property (iii) is proved in [OS19, Corollary 2.5] (also taking into account the Bruhat decomposition). ■

We are now going to state a corollary of the Theorem 1.9.1, which provides a much easier formula in the special case in which lengths add up. First note that from the lemma and the theorem it follows that for all $v, w \in \widetilde{W}$ such that $\ell(vw) = \ell(v) + \ell(w)$, for all $i, j \in \mathbb{Z}_{\geqslant 0}$, for all $\alpha \in H^i(I, \mathbf{X}(v))$ and $\beta \in H^j(I, \mathbf{X}(w))$, one has

$$\alpha \cdot \beta \in H^{i+j}(I, \mathbf{X}(vw)). \tag{36}$$

Corollary 1.9.3. *Let $v, w \in \widetilde{W}$ such that $\ell(vw) = \ell(v) + \ell(w)$, let $i, j \in \mathbb{Z}_{\geqslant 0}$, let $\alpha \in H^i(I, \mathbf{X}(v))$ and let $\beta \in H^j(I, \mathbf{X}(w))$. One has*

$$\alpha \cdot \beta = (\alpha \cdot \tau_w) \smile (\tau_v \cdot \beta).$$

Proof. See [OS19, Corollary 5.5]. ■

In the case that lengths do not add up, one still has some relations between the product in E^* and the cup product, at least if $\mathbf{G}$ is semisimple simply connected.

Proposition 1.9.4. *Assume that $\mathbf{G}$ is semisimple simply connected. Let $s \in S_{\mathrm{aff}}$ and $w \in \widetilde{W}$ such that $\ell(\widetilde{s}w) = \ell(w) - 1$, let $i, j \in \mathbb{Z}_{\geqslant 0}$, and let $\alpha \in H^i(I, \mathbf{X}(\widetilde{s}))$ and $\beta \in H^j(I, \mathbf{X}(w))$. One has*

$$\alpha \cdot \beta - (\alpha \cdot \tau_w) \smile (\tau_{\widetilde{s}} \cdot \beta) \in H^{i+j}(I, \mathbf{X}(\widetilde{s}w)).$$

Proof. See [OS21, Proposition 2.1]. ■

Now, we turn our attention on the action of E^0 on E^*: first of all we are going to state a corollary in the case in which lengths add up, which in particular gives a way to compute the products appearing on the right hand side of the equation in Corollary 1.9.3.

Corollary 1.9.5. *Let $v, w \in \widetilde{W}$ and let $\alpha \in H^i(I, \mathbf{X}(v))$.*

- *If $\ell(vw) = \ell(v) + \ell(w)$, then*

$$\alpha \cdot \tau_w \in H^i(I, \mathbf{X}(vw)) \qquad \text{and} \qquad \mathrm{Sh}_{vw}(\alpha \cdot \tau_w) = \mathrm{res}^{I_v}_{I_{vw}}\big(\mathrm{Sh}_v(\alpha)\big).$$

- *If $\ell(wv) = \ell(w) + \ell(v)$, then*

$$\tau_w \cdot \alpha \in H^i(I, \mathbf{X}(wv)) \qquad \text{and} \qquad \mathrm{Sh}_{wv}(\tau_w \cdot \alpha) = \mathrm{res}^{wI_v w^{-1}}_{I_{wv}}\big(w_* \mathrm{Sh}_v(\alpha)\big).$$

Proof. See [OS19, Corollary 5.5]. ■

Note that in the last formula conjugation by w is well defined (in the sense that it does not depend on the choice of a representative modulo T^1) by the discussion after (29).

Now, let us state a proposition which deals with the description (again, in terms of cohomological operations) of the action of the generators of E^0 on the left on E^*, in this way completely determining the structure of E^* as a graded left E^0-module. Of course Theorem 1.9.1 would already be sufficient for this purpose, but here the formulas will be more explicit. Recall the specific lift $\widetilde{s} = \overline{n_s} \in \widetilde{W}$ of an element $s \in S_{\mathrm{aff}}$ we defined in (12).

Proposition 1.9.6 (Ollivier, Schneider). *Let $w \in \widetilde{W}$, let $j \in \mathbb{Z}_{\geqslant 0}$ and let $\beta \in H^j(I, \mathbf{X}(w))$. One has the following formulas.*

(i) For all $\omega \in \widetilde{\Omega}$ one has

$$\begin{aligned} \tau_\omega \cdot \beta &\in H^j(I, \mathbf{X}(\omega w)), \\ \mathrm{Sh}_{\omega w}(\tau_\omega \cdot \beta) &= \omega_* \,\mathrm{Sh}_w(\beta). \end{aligned}$$

(ii) For all $s \in S_{\mathrm{aff}}$ such that $\ell(\widetilde{s}w) = \ell(w) + 1$ one has

$$\begin{aligned} \tau_{\widetilde{s}} \cdot \beta &\in H^j(I, \mathbf{X}(\widetilde{s}w)), \\ \mathrm{Sh}_{\widetilde{s}w}(\tau_{\widetilde{s}} \cdot \beta) &= \mathrm{res}^{\widetilde{s}I_w\widetilde{s}^{-1}}_{I_{\widetilde{s}w}} \left(\widetilde{s}_* \,\mathrm{Sh}_w(\beta)\right). \end{aligned}$$

(iii) For all $s \in S_{\mathrm{aff}}$ such that $\ell(\widetilde{s}w) = \ell(w) - 1$ one has

$$\begin{aligned} \tau_{\widetilde{s}} \cdot \beta &= \gamma_{\widetilde{s}w} + \sum_{t \in \check{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])} \gamma_{\overline{t}w} \\ &\in H^j(I, \mathbf{X}(\widetilde{s}w)) \oplus \bigoplus_{t \in \check{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])} H^j(I, \mathbf{X}(\overline{t}w)), \end{aligned}$$

where

$$\begin{aligned} \mathrm{Sh}_{\widetilde{s}w}(\gamma_{\widetilde{s}w}) &= \mathrm{cores}^{\widetilde{s}I_w\widetilde{s}^{-1}}_{I_{\widetilde{s}w}} \left(\widetilde{s}_* \,\mathrm{Sh}_w(\beta)\right), \\ \mathrm{Sh}_{\overline{t}w}(\gamma_{\overline{t}w}) &= \sum_{\substack{z \in (\mathfrak{O}/\mathfrak{M})^\times \\ \text{s.t. } \check{\alpha}_s([z]) = t}} \left(n_s t^{-1} x_{\alpha_s}(\pi^{\mathfrak{h}_s}[z]) n_s^{-1}\right)_* \mathrm{Sh}_w(\beta), \end{aligned}$$

where $(\alpha_s, \mathfrak{h}_s)$ is the affine root corresponding to s.

With the notation of the proposition, note that the following claims are implicit in the statement of the proposition: the fact that $I_{\widetilde{s}w} \subseteq \widetilde{s}I_w\widetilde{s}^{-1}$ if $\ell(\widetilde{s}w) = \ell(w)+1$, the fact that the opposite inclusion holds if instead $\ell(\widetilde{s}w) = \ell(w)-1$, and, using the notations of the third part, the fact that conjugation by $n_s t^{-1} x_{\alpha_s}(\pi^{\mathfrak{h}_s}[z]) n_s^{-1}$ sends I_w to $I_{\overline{t}w}$.

1.9.e Anti-involution

Following [OS19, §6], in this subsection we are going to define an involutive anti-automorphism (for brevity, *anti-involution*) on the Ext-algebra.

Let $w \in \widetilde{W}$ and $i \in \mathbb{Z}_{\geqslant 0}$. We start by defining an isomorphism $\mathcal{J}_w$ of k-vector spaces from $H^i(I, \mathbf{X}(w))$ to $H^i(I, \mathbf{X}(w^{-1}))$ as the unique map making the following diagram commutative:

$$\begin{tikzcd}
H^i(I, \mathbf{X}(w)) \arrow[r, "\mathcal{J}_w", "\cong"'] \arrow[d, "\mathrm{Sh}_w"', "\cong"] & H^i(I, \mathbf{X}(w^{-1})) \arrow[d, "\cong"', "\mathrm{Sh}_{w^{-1}}"] \\
H^i(I_w, k) \arrow[r, "\cong", "(w^{-1})_*"'] & H^i(I_{w^{-1}}, k).
\end{tikzcd} \tag{37}$$

Summing the $\mathcal{J}_w$'s over all $w \in \widetilde{W}$, we get an automorphism

$$\mathcal{J}\colon E^i = \bigoplus_{w\in\widetilde{W}} H^i(I, \mathbf{X}(w)) \longrightarrow \bigoplus_{w\in\widetilde{W}} H^i(I, \mathbf{X}(w^{-1})) = E^i,$$

of the k-vector space E^i; moreover it is easy to see that it is an involution.

Summing over all $i \in \mathbb{Z}_{\geqslant 0}$, we get an involutive automorphism

$$\mathcal{J}\colon E^* \longrightarrow E^*$$

of E^* as a graded k-vector space. The non-trivial result is how $\mathcal{J}$ behaves with respect to the product in E^*.

Theorem 1.9.7 (Ollivier, Schneider). *The map $\mathcal{J}\colon E^* \longrightarrow E^*$ is an involutive anti-automorphism, i.e., for all $i, j \in \mathbb{Z}_{\geqslant 0}$, all $\alpha \in E^i$ and all $\beta \in E^j$ one has*

$$\mathcal{J}(\alpha \cdot \beta) = (-1)^{ij} \mathcal{J}(\beta) \cdot \mathcal{J}(\alpha).$$

Proof. See [OS19, Proposition 6.1]. ■

It is easy to describe the action of $\mathcal{J}$ on E^0: indeed for all $v \in \widetilde{W}$ the element $\tau_v = \mathbb{1}_{IvI} \in H^0(I, \mathbb{Z}(v))$ corresponds to $1_k \in k = H^0(I_v, k)$ via the Shapiro isomorphism Sh_v (this can be seen for example using the alternative description (34) of the Shapiro isomorphism). Therefore, we see from the diagram (37) that for all $w \in \widetilde{W}$ we have

$$\mathcal{J}(\tau_w) = \tau_{w^{-1}}. \tag{38}$$

1.9.f Duality

In this section we will see a duality theorem for the Ext-algebra E^* under the extra assumption that the pro-p Iwahori subgroup I is torsion-free.

Assumptions. Let us assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free. The former assumption is implied by the latter whenever $T \subsetneq G$, since the groups $\mathcal{U}_{(\alpha,\mathfrak{h})}$'s are annihilated by p.

Under our assumption, clearly also the subgroup I_w for $w \in \widetilde{W}$ are torsion-free. Being open subgroups of G, they are analytic groups over $\mathbb{Q}_p$ of the same dimension, equal to the dimension d of G as an analytic manifold over $\mathbb{Q}_p$. We can apply Lazard theorem on Poincaré groups (Theorem 1.8.2), obtaining that I as well as all its subgroups I_w for $w \in \widetilde{W}$ are Poincaré groups of dimension d. Recalling from (35) the identification of graded k-vector spaces $E^* \cong \bigoplus_{w\in\widetilde{W}} H^*(I_w, k)$ and the link between cohomology with coefficients in $\mathbb{F}_p$ and cohomology with coefficients in k (see (31)), we see that E^* is supported in degrees 0 to d:

$$E^* = \bigoplus_{i=0}^{d} E^i.$$

For all k-vector spaces V, let us denote by $V^\vee$ the k-linear dual

$$V^\vee \coloneqq \mathrm{Hom}_k(V, k).$$

Let us define the *finite dual* of E^i as:

$$(E^i)^{\vee,\mathrm{finite}} \coloneqq \bigoplus_{w\in\widetilde{W}} \left(H^i(I, \mathbf{X}(w))\right)^\vee \subseteq \Big(\bigoplus_{w\in\widetilde{W}} H^i(I, \mathbf{X}(w))\Big)^\vee = (E^i)^\vee.$$

The k-vector space $(E^i)^\vee$ is naturally an E^0-bimodule, the bimodule structure being given by

$$\begin{aligned} E^0 \times (E^i)^\vee &\longrightarrow (E^i)^\vee \\ (h, \varphi) &\longmapsto \varphi(\_ \cdot h) \end{aligned}$$

and

$$\begin{aligned} (E^i)^\vee \times E^0 &\longrightarrow (E^i)^\vee \\ (\varphi, h) &\longmapsto \varphi(h \cdot \_). \end{aligned}$$

We will consider instead a "twisted" E^0-bimodule structure on $(E^i)^\vee$ defined through the anti-involution; it is defined in the following way (we use the notation ${}^{\mathcal{J}}\big((E^i)^\vee\big)^{\mathcal{J}}$ for the k-vector space $(E^i)^\vee$ endowed with this "twisted" E^0-bimodule structure):

$$\begin{aligned} E^0 \times {}^{\mathcal{J}}\big((E^i)^\vee\big)^{\mathcal{J}} &\longrightarrow {}^{\mathcal{J}}\big((E^i)^\vee\big)^{\mathcal{J}} \\ (h, \varphi) &\longmapsto \varphi(\mathcal{J}(h) \cdot \_) \end{aligned}$$

and

$$\begin{aligned} {}^{\mathcal{J}}\big((E^i)^\vee\big)^{\mathcal{J}} \times E^0 &\longrightarrow {}^{\mathcal{J}}\big((E^i)^\vee\big)^{\mathcal{J}} \\ (\varphi, h) &\longmapsto \varphi(\_ \cdot \mathcal{J}(h)). \end{aligned}$$

We also need some more pieces of notation in order to state the duality theorem: let us consider the G-equivariant map

$$\begin{aligned} \mathcal{S}\colon\ k\,[G/I] &\longrightarrow k \\ f &\longmapsto \sum_{\overline{g}\in G/I} f(g) \end{aligned} \tag{39}$$

and its induced map

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

Moreover, since we are dealing with a Poincaré group of dimension d, the cohomology group $H^d(I, \mathbb{F}_p)$ is a one-dimensional $\mathbb{F}_p$-vector space, and so $H^d(I, k)$ is a one-dimensional k-vector space (by (31)). We may therefore fix an isomorphism of k-vector spaces

$$\eta\colon H^d(I, k) \longrightarrow k.$$

Theorem 1.9.8 (Ollivier, Schneider). *Always under the assumption that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free, and defining $\mathcal{S}$ and η as above, the following is an injective homomorphism of E^0-bimodules:*

$$\Delta^i\colon E^i \longrightarrow {}^{\mathfrak{J}}\Big((E^{d-i})^\vee\Big)^{\mathfrak{J}}$$
$$\alpha \longmapsto \left(\begin{array}{ccc} E^{d-i} & \longrightarrow & k \\ \beta & \longmapsto & \left(\eta\circ\mathcal{S}^d\right)(\alpha\smile\beta)\end{array}\right).$$

Moreover, its image is ${}^{\mathfrak{J}}\Big((E^{d-i})^{\vee,\mathrm{finite}}\Big)^{\mathfrak{J}}$, which in particular is a sub-E^0-bimodule of ${}^{\mathfrak{J}}\Big((E^{d-i})^\vee\Big)^{\mathfrak{J}}$.

Proof. See [OS19, Proposition 7.18]. ■

1.9.g The top graded piece

In the last section we have seen in particular that, under the assumption that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free, the Ext-algebra is supported in degrees 0 to d (where d is the dimension of G as an analytic manifold over $\mathbb{Q}_p$) and that the top graded piece E^d is "dual" to E^0 (in a sense made precise by Theorem 1.9.8). Since we know the algebra $E^0 = H$ quite explicitly, it is possible to describe E^d quite explicitly as well, as we will recall from [OS19, §8] in this section.

Assumptions. Let us assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free. Recall that the former assumption is implied by the latter whenever $T \subsetneq G$.

We fix an isomorphism of k-vector spaces $\eta\colon H^d(I,k) \longrightarrow k$ in order to apply the duality theorem (Theorem 1.9.8), and then we fix the k-basis $(\phi_w)_{w\in\widetilde{W}}$ of $(E^d)^{\vee,\mathrm{finite}}$ dual to the Iwahori–Matsumoto basis $(\tau_w)_{w\in\widetilde{W}}$: this means that (for all $w\in\widetilde{W}$) ϕ_w is the unique element of E^d such that

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

Now, given $\alpha\in E^d$, which can be written as $\alpha = \sum_{w\in\widetilde{W}}\alpha_w$ for suitable elements $\alpha_w \in H^d(I,\mathbf{X}(w))$, we see that $\alpha\smile\tau_v = \alpha_v$ for all $v\in\widetilde{W}$ (indeed, it is easy to see that the cup product of two cohomology classes coming from different $\widetilde{W}$-components is zero, as stated in [OS19, Equation 43]; moreover the elements of the Iwahori–Matsumoto basis act as the identity on their $\widetilde{W}$-component). It follows that ϕ_w can be characterized as the unique element of $H^d(I,\mathbf{X}(w))$ such that

$$\left(\eta\circ\mathcal{S}^d\right)(\phi_w) = 1. \tag{40}$$

We are now going to state the explicit formulas describing the structure of E^d as an E^0-bimdodule. Before, we recall that for all $s\in S_{\mathrm{aff}}$ we defined

$$\theta_s := -(\#\mu_{\check{\alpha}_s})\cdot\sum_{t\in\check{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])}\tau_{\widetilde{t}}\in E^0,$$

and that we chose a specific lift $\widetilde{s}\in\widetilde{W}$ of s in (12).

Proposition 1.9.9 (Ollivier, Schneider). *Always under the assumption that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free, the following formulas hold for all $w \in \widetilde{W}$, for all $\omega \in \widetilde{\Omega}$ and for all $s \in S_{\mathrm{aff}}$:*

$$
\begin{aligned}
&\tau_\omega \cdot \phi_w = \phi_{\omega w}, && (41)\\
&\phi_w \cdot \tau_\omega = \phi_{w\omega}, && (42)\\
&\tau_{\widetilde{s}} \cdot \phi_w = \begin{cases} \phi_{\widetilde{s}w} + (\#\mu_{\breve{\alpha}_s}) \cdot \sum_{t \in \breve{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])} \phi_{\bar{t}w} & \text{if } \ell(\widetilde{s}w) = \ell(w) - 1,\\ 0 & \text{if } \ell(\widetilde{s}w) = \ell(w) + 1, \end{cases} && (43)\\
&\qquad\quad = \begin{cases} \phi_{\widetilde{s}w} - \theta_s \cdot \phi_w & \text{if } \ell(\widetilde{s}w) = \ell(w) - 1,\\ 0 & \text{if } \ell(\widetilde{s}w) = \ell(w) + 1, \end{cases}\\
&\phi_w \cdot \tau_{\widetilde{s}} = \begin{cases} \phi_{w\widetilde{s}} + (\#\mu_{\breve{\alpha}_s}) \cdot \sum_{t \in \breve{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])} \phi_{w\bar{t}} & \text{if } \ell(w\widetilde{s}) = \ell(w) - 1,\\ 0 & \text{if } \ell(w\widetilde{s}) = \ell(w) + 1, \end{cases} && (44)\\
&\qquad\quad = \begin{cases} \phi_{w\widetilde{s}} - \phi_w \cdot \theta_s & \text{if } \ell(w\widetilde{s}) = \ell(w) - 1,\\ 0 & \text{if } \ell(w\widetilde{s}) = \ell(w) + 1. \end{cases}
\end{aligned}
$$

Proof. See [OS19, Proposition 8.2]. ∎

As for the quadratic relations stated in Theorem 1.4.1, note that the above formulas are valid also for a lift of s to $\widetilde{W}$ of the form $t\widetilde{s}$ or $\widetilde{s}t$ for some $t \in \breve{\alpha}_s([(\mathfrak{O}/\mathfrak{M})^\times])$ in place of $\widetilde{s}$, but, in general, not for an arbitrary lift.

Also the behaviour of the anti-involution $\mathcal{J}$ is particularly simple on E^d; indeed one has the following formula, which is proved in [OS19, Equation (89)]:

$$\mathcal{J}(\phi_w) = \phi_{w^{-1}} \qquad \text{for all } w \in \widetilde{W}. \tag{45}$$

We end this section with a decomposition of E^d as an E^0-bimodule under some special assumptions.

Proposition 1.9.10 (Ollivier, Schneider). *Assume that Ω is finite and that $\#\Omega$ is invertible in k (and, as in the whole subsection, that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free). One has that E^d decomposes into a direct sum E^0-bimodules*

$$E^d = k\phi \oplus \ker(\mathcal{S}^d),$$

where $\phi := \sum_{\omega \in \widetilde{\Omega}} \phi_\omega$. Moreover, E^0 acts on $k\phi$ on the right and on the left through the following character:

$$
\begin{aligned}
\chi_{\mathrm{triv}} \colon E^0 &\longrightarrow k\\
\tau_w &\longmapsto \begin{cases} 1 & \text{if } \ell(w) = 0,\\ 0 & \text{if } \ell(w) \geqslant 1. \end{cases}
\end{aligned}
$$

Proof. See [OS19, Proposition 8.6]. ∎

1.9.h Filtrations

Let $i \in \mathbb{Z}_{\geqslant 0}$. As in [OS21, §2.2.4] we define the following two filtrations of k-vector spaces, the first one decreasing and the second one increasing:

$$(F^n E^i)_{n\in\mathbb{Z}_{\geqslant 0}} \qquad \text{defined by} \qquad F^n E^i := \bigoplus_{\substack{w\in\widetilde{W} \\ \text{s.t. } \ell(w)\geqslant n}} H^i(I, \mathbf{X}(w)),$$

$$(F_n E^i)_{n\in\mathbb{Z}_{\geqslant 0}} \qquad \text{defined by} \qquad F_n E^i := \bigoplus_{\substack{w\in\widetilde{W} \\ \text{s.t. } \ell(w)\leqslant n}} H^i(I, \mathbf{X}(w)).$$

The following properties hold.

- For all $n \in \mathbb{Z}_{\geqslant 0}$ the subspace $F^n E^0$ is a bilateral ideal of E^0 (immediate from the braid and quadratic relations, see Theorem 1.4.1).
- For all $n, m, i, j \in \mathbb{Z}_{\geqslant 0}$ one has $F_n E^i \cdot F_m E^j \subseteq F_{n+m} E^{i+j}$ (see [OS21, §2.2.4]).
- Assuming that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ and that I is torsion-free, for all $n \in \mathbb{Z}_{\geqslant 0}$ the subspace $F_n E^d$ is a sub-E^0-bimodule of E^d, or, equivalently, it is a bilateral ideal of E^* (immediate from the formulas for the action of E^0 on E^d, see Proposition 1.9.9).

1.10 The Ext-algebra for SL_2

In the special case of $\mathbf{G} = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ it is possible to carry out explicit computations on the Ext-algebra. Under these assumptions, I is torsion-free, since G does not contain non-trivial p-torsion elements (because the characteristic polynomial of such a matrix would be divisible by the p^{th} cyclotomic polynomial). Since the dimension of G as an analytic manifold over $\mathbb{Q}_p$ is 3 we deduce from Subsection 1.9.f that

$$E^* = E^0 \oplus E^1 \oplus E^2 \oplus E^3. \tag{46}$$

Explicit formulas as well as results on the structure E^* as an E^0-bimodule have been obtained in this case by Ollivier and Schneider in [OS21]. In this section, we will state the main formulas as well as some other structural results.

Some of the result are true under more general assumptions, and so we will specify the appropriate assumptions in each subsection.

1.10.a Preliminaries

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). We does not enforce any restriction on $\mathfrak{F}$.

- We fix the following group isomorphism:

$$\begin{aligned} \omega_{(-)}\colon\ (\mathfrak{O}/\mathfrak{M})^\times &\longrightarrow T^0/T^1 \\ u &\longmapsto \omega_u := \overline{\begin{pmatrix} [u]^{-1} & 0 \\ 0 & [u] \end{pmatrix}}, \end{aligned} \tag{47}$$

where $[u]$ denotes the Teichmüller lift of u.

- Assume that $q = p$. Then $\mathfrak{O}/\mathfrak{M} = \mathbb{F}_p$, in the sense that there exists a unique field isomorphism between the two, and $\mathbb{F}_p \subseteq k$, in the sense that there exists a unique field homomorphism. Therefore, it make sense to consider the unique group homomorphism
$$\underline{\mathrm{id}}\colon T^0/T^1 \longrightarrow k \tag{48}$$
such that $\underline{\mathrm{id}} \circ \omega_{(\_)}$ is equal to the identity map $\mathbb{F}_p \longrightarrow k$. More concretely,
$$\begin{aligned} \underline{\mathrm{id}}\colon \qquad T^0/T^1 &\longrightarrow k \\ \underset{\text{(where } t \in \mathbb{Z}_p^\times)}{\overline{\left(\begin{smallmatrix} t^{-1} & 0 \\ 0 & t \end{smallmatrix}\right)}} &\longmapsto \bar{t}. \end{aligned}$$

- Recall that in (25) we considered the automorphism $\Gamma_\varpi\colon H \longrightarrow H$ induced by conjugation by $\varpi := \left(\begin{smallmatrix} 0 & 1 \\ \pi & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathfrak{F})$. In [OS21, §2.2.6] it is shown that Γ_ϖ can be naturally extended to an automorphism
$$\Gamma_\varpi\colon E^* \longrightarrow E^*,$$
such that for all $w \in \widetilde{W}$ one has that $\Gamma_\varpi\big(H^*(I, \mathbf{X}(w))\big) \subseteq H^*(I, \mathbf{X}(\varpi w \varpi^{-1}))$ and that the following diagram commutes (this of course completely determines Γ_ϖ):
$$\begin{tikzcd} H^j(I, \mathbf{X}(w)) \arrow[r, "\mathrm{Sh}_w"] \arrow[d, "\Gamma_\varpi"'] & H^j(I_w, k) \arrow[d, "\varpi_*"', "\substack{\text{induced by} \\ \mathrm{conj}_{\varpi^{-1}}\colon I_{\varpi w \varpi^{-1}} \longrightarrow I_w \\ (=\mathrm{conj}_\varpi)}"] \\ H^j(I, \mathbf{X}(\varpi w \varpi^{-1})) \arrow[r, "\mathrm{Sh}_{\varpi w \varpi^{-1}}"'] & H^j(I_{\varpi w \varpi^{-1}}, k). \end{tikzcd}$$
The map Γ_ϖ is an automorphism of E^* as a graded k-algebra, it also preserves the cup product and commutes with the anti-involution $\mathcal{J}$ (see again [OS21, §2.2.6]):
$$\Gamma_\varpi \circ \mathcal{J} = \mathcal{J} \circ \Gamma_\varpi. \tag{49}$$

- Recall the element $\zeta \in Z(H) = Z(E^0)$, defined in (28) as
$$\zeta := \tau_{s_0} \cdot \tau_{s_1} + (\tau_{s_1} + e_1) \cdot (\tau_{s_0} + e_1).$$
We will see that it is not central in $Z(E^*)$. The following two homomorphisms of E^0-bimodules are crucially used in [OS21] to study the structure of E^* as a graded E^0-bimodule:
$$\begin{aligned} f\colon\ E^* &\longrightarrow E^* \\ x &\longmapsto \zeta \cdot x \cdot \zeta, \end{aligned} \tag{50}$$
$$\begin{aligned} g\colon\ E^* &\longrightarrow E^* \\ x &\longmapsto \zeta \cdot x - x \cdot \zeta. \end{aligned} \tag{51}$$
For all $i \in \mathbb{Z}_{\geqslant 0}$, we will denote by $f_i\colon E^i \longrightarrow E^i$ and $g_i\colon E^i \longrightarrow E^i$ the restrictions of f and g respectively.

1.10.b The 1st graded piece E^1: elements as triples

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5), with $\mathfrak{F}$ arbitrary and $p \neq 2$. Later on, we will assume furthermore that $\mathfrak{F} = \mathbb{Q}_p$.

Let us start with the explicit description of E^1 as a k-vector space: recalling that $E^1 \cong \bigoplus_{w \in \widetilde{W}} H^1(I_w, k)$, we see that such a description can be achieved through an explicit description of the cohomology group $H^1(I_w, k)$ for all $w \in \widetilde{W}$. Recall from (32) that to this end one should compute the Frattini quotient $(I_w)_\Phi$ of I_w. This can be done as follows.

Lemma 1.10.1. *Let $w \in \widetilde{W}$. One has the following description of the Frattini quotient of I_w.*

- *If $\ell(s_0 w) = \ell(w) + 1$ then one has the group isomorphism*

$$\begin{array}{ccc} \mathfrak{O}/\mathfrak{M} \times \dfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})} \times \mathfrak{O}/\mathfrak{M} & \longrightarrow & (I_w)_\Phi \\ (\overline{c}, \overline{t}, \overline{b}) & \longmapsto & \overline{\left(\begin{smallmatrix} 1 & 0 \\ \pi^{\ell(w)+1}c & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)}. \end{array}$$

- *If $\ell(s_1 w) = \ell(w) + 1$ then one has the group isomorphism*

$$\begin{array}{ccc} \mathfrak{O}/\mathfrak{M} \times \dfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})} \times \mathfrak{O}/\mathfrak{M} & \longrightarrow & (I_w)_\Phi \\ (\overline{c}, \overline{t}, \overline{b}) & \longmapsto & \overline{\left(\begin{smallmatrix} 1 & 0 \\ \pi c & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & \pi^{\ell(w)}b \\ 0 & 1 \end{smallmatrix}\right)}. \end{array}$$

Proof. The computation of the abelianization of I_w is in [OS18, Proposition 3.62.ii, Equation (26) and the preceiding lines], and the description of the Frattini quotient follows. ■

From the above lemma, we see in particular that the Frattini quotient is finite, and so we might apply the formula $H^1(I_w, k) \cong \mathrm{Hom}_{\mathbb{F}_p}((I_w)_\Phi, k)$ (see (33)). We consider the fixed isomorphism of k-vector spaces obtained by dualizing (i.e., by applying the functor $\mathrm{Hom}_{\mathbb{F}_p}(\_, k)$ to) the isomorphisms of $\mathbb{F}_p$-vector spaces in the lemma:

$$\mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \times \mathrm{Hom}_{\mathbb{F}_p}\left(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}, k\right) \times \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \longrightarrow H^1(I_w, k),$$

and considering the postcomposition with the inverse of the Shapiro isomorphism $H^1(I_w, k) \cong H^1(I, \mathbf{X}(w))$, we obtain an isomorphism

$$(-,-,-)_w \colon \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \times \mathrm{Hom}_{\mathbb{F}_p}\left(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}, k\right) \times \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \longrightarrow H^1(I, \mathbf{X}(w)).$$

Let $w \in \widetilde{W}$. In many statements, we will say "let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$", meaning that we consider arbitrary elements $c^-, c^+ \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$ and an arbitrary element $c^0 \in \mathrm{Hom}_{\mathbb{F}_p}\left(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}, k\right)$, and that we consider the corresponding element $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$.

Assumptions. For the rest of this subsection, let us assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5), always with the condition $p \neq 2$.

We have:

$$\operatorname{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \cong k, \tag{52}$$

$$\operatorname{Hom}_{\mathbb{F}_p}\left(\tfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}, k\right) \cong \begin{cases} 0 & \text{if } \ell(w)=0, \\ k & \text{if } \ell(w) \geqslant 1; \end{cases} \tag{53}$$

indeed the first isomorphism is obvious, and to prove the second one can use the isomorphism given by the logarithm and the exponential $1+\mathfrak{M} \cong \mathfrak{M}$, through which one sees that $(1+\mathfrak{M})^p = 1+\mathfrak{M}^2$, which in turn proves that the claimed isomorphism holds. In particular, we have

$$\dim_k H^1(I, \mathbf{X}(w)) = \begin{cases} 2 & \text{if } \ell(w)=0, \\ 3 & \text{if } \ell(w) \geqslant 1. \end{cases} \tag{54}$$

It will be sometimes useful to fix a basis for each $H^1(I, \mathbf{X}(w))$ (for $w \in \widetilde{W}$) in a uniform way. To this end, let us consider the following isomorphism, induced by the logarithm:

$$\begin{aligned} \iota\colon\ (1+\mathfrak{M})/(1+\mathfrak{M}^2) &\longrightarrow \mathfrak{O}/\mathfrak{M} = \mathbb{F}_p \\ \overline{1+px} &\longmapsto \overline{x}. \end{aligned} \tag{55}$$

We fix an element $\mathbf{c} \in \operatorname{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \smallsetminus \{0\}$, and for all $w \in \widetilde{W}$ we define

$$\begin{aligned} \beta_w^- &\coloneqq (\mathbf{c}, 0, 0)_w, \\ \beta_w^+ &\coloneqq (0, 0, \mathbf{c})_w, \\ \beta_w^0 &\coloneqq (0, \mathbf{c}\iota, 0)_w \qquad \text{if } \ell(w) \geqslant 1. \end{aligned} \tag{56}$$

This is clearly a k-basis of $H^1(I, \mathbf{X}(w))$. In some situations further assumptions on $\mathbf{c}$ will be introduced (see Subsection 4.5.a).

1.10.c The 1^{st} graded piece E^1: explicit formulas

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5), with $\mathfrak{F}$ arbitrary and $p \neq 2$. We will introduce other assumptions for some of the formulas. In any case, all the formulas will be valid at least for $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$ and $\pi = p$.

We are now going to list many formulas involving this description of the elements of E^1 as triples proved in [OS21]. Namely, we are going to state how the involutions $\mathfrak{J}$ and Γ_ϖ behave, and we are going to describe the multiplication on the left, and, partially, on the right, by elements of E^0, at least in the case $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$. Note that the description of the left action of E^0, together with the description of $\mathfrak{J}$, already determines the right action of E^0.

- Action of the anti-involution $\mathfrak{J}$ on E^1 (see [OS21, Lemma 4.7]):

  Let $w \in \widetilde{W}$ and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. Furthermore, let $u_w \in (\mathfrak{O}/\mathfrak{M})^\times$ 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). One has:

$$\mathfrak{J}\big((c^-, c^0, c^+)_w\big) = \begin{cases} \big(c^-(u_w^2 \cdot \_), c^0, c^+(u_w^{-2} \cdot \_)\big)_{w^{-1}} & \text{if } \ell(w) \text{ is even}, \\ \big(-c^+(u_w^{-2} \cdot \_), -c^0, -c^-(u_w^2 \cdot \_)\big)_{w^{-1}} & \text{if } \ell(w) \text{ is odd}. \end{cases} \tag{57}$$

- Action of the involutive automorphism Γ_ϖ on E^1 (see [OS21, Lemma 4.4]):

  Let $w \in \widetilde{W}$ and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$\Gamma_\varpi\big((c^-, c^0, c^+)_w\big) = (c^+, -c^0, c^-)_{\varpi w \varpi^{-1}}. \tag{58}$$

- Left and right action of τ_ω on E^1 for $\omega \in T^0/T^1$ (see [OS21, Equations (64) and (66)]):

  Let $u \in (\mathfrak{O}/\mathfrak{M})^\times$, let $w \in \widetilde{W}$ and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$\tau_{\omega_u} \cdot (c^-, c^0, c^+)_w = \big(c^-(u^{-2} \cdot \_), c^0, c^+(u^2 \cdot \_)\big)_{\omega_u w}, \tag{59}$$
$$(c^-, c^0, c^+)_w \cdot \tau_{\omega_u} = (c^-, c^0, c^+)_{w\omega_u}. \tag{60}$$

  Note that, if $q = p$, then in the first formula we can write $c^-(u^{-2} \cdot \_) = u^{-2}c^-$ and $c^+(u^2 \cdot \_) = u^2 c^+$.

- Action of the idempotents on E^1:

  Assume that $q = p$, let $\lambda \in \widehat{T^0/T^1}$, let $w \in \widetilde{W}$ and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$\begin{aligned} (c^-, 0, 0)_w \cdot e_\lambda &= e_{\lambda^{(-1)^{\ell(w)}}\, \underline{\mathrm{id}}^{-2}} \cdot (c^-, 0, 0)_w, \\ (0, c^0, 0)_w \cdot e_\lambda &= e_{\lambda^{(-1)^{\ell(w)}}} \cdot (0, c^0, 0)_w \qquad \text{(if } \ell(w) \geqslant 1\text{)}, \\ (0, 0, c^+)_w \cdot e_\lambda &= e_{\lambda^{(-1)^{\ell(w)}}\, \underline{\mathrm{id}}^{2}} \cdot (0, 0, c^+)_w. \end{aligned} \tag{61}$$

  These formulas can be easily computed from formulas (59) and (60), and they are also proven in [OS21, Equation (69)] (for $\lambda = \underline{\mathrm{id}}^m$ for some $m \in \mathbb{Z}$, i.e., for every λ).

- Left action of τ_{s_0} and τ_{s_1} when lengths add up:

  For all $n \in \mathbb{Z}_{\geqslant 0}$, let us define

$$\Psi_n \colon \operatorname{Hom}_{\mathbb{F}_p}\Big(\tfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{n+1})}, k\Big) \longrightarrow \operatorname{Hom}_{\mathbb{F}_p}\Big(\tfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{n+2})}, k\Big)$$

  as the map induced from the natural map $\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{n+2})} \longrightarrow \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{n+1})}$. Furthermore, let $w \in \widetilde{W}$ and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$\begin{aligned} \tau_{s_0} \cdot (c^-, c^0, c^+)_w &= (0, -\Psi_{\ell(w)}(c^0), -c^-)_{s_0 w} \quad \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \tau_{s_1} \cdot (c^-, c^0, c^+)_w &= (-c^+, -\Psi_{\ell(w)}(c^0), 0)_{s_1 w} \quad \text{if } \ell(s_1 w) = \ell(w) + 1. \end{aligned} \tag{62}$$

  This is proved in [OS21, Proposition 4.9] in the case $\mathfrak{F} = \mathbb{Q}_p$ for $p \neq 2, 3$. We add a proof for the general case ($\mathfrak{F}$ arbitrary and $p \neq 2$) further below. Note that if $\mathfrak{F} = \mathbb{Q}_p$ for $p \neq 2$ the formulas simplify as follows:

$$\begin{aligned} \tau_{s_0} \cdot (c^-, c^0, c^+)_w &= (0, -c^0, -c^-)_{s_0 w} \quad \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \tau_{s_1} \cdot (c^-, c^0, c^+)_w &= (-c^+, -c^0, 0)_{s_1 w} \quad \text{if } \ell(s_1 w) = \ell(w) + 1; \end{aligned} \tag{63}$$

  indeed if $\ell(w) = 0$ then $c^0 = 0$ and the new formula trivially holds, whereas if $\ell(w) \geqslant 1$ then $\Psi_{\ell(w)}$ is the identity by (53).

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

  For all $n, m \in \mathbb{Z}_{\geqslant 0}$ with $m \geqslant n$, let us define

$$\Psi_{n,m} \colon \operatorname{Hom}_{\mathbb{F}_p}\left(\tfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{n+1})}, k\right) \longrightarrow \operatorname{Hom}_{\mathbb{F}_p}\left(\tfrac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{m+1})}, k\right)$$

  as the map induced from the natural map $\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{m+1})} \longrightarrow \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{n+1})}$. Furthermore, let $w, v \in \widetilde{W}$ such that $\ell(wv) = \ell(w) + \ell(v)$ and such that $\ell(v) \geqslant 1$, and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$\begin{aligned} (c^-, c^0, c^+)_w \cdot \tau_v &= \big(c^-, \Psi_{\ell(w),\ell(wv)}(c^0), 0\big)_{wv} \quad \text{if } \ell(s_1 wv) = \ell(wv) + 1, \\ (c^-, c^0, c^+)_w \cdot \tau_v &= \big(0, \Psi_{\ell(w),\ell(wv)}(c^0), c^+\big)_{wv} \quad \text{if } \ell(s_0 wv) = \ell(wv) + 1. \end{aligned} \tag{64}$$

  This is proved in [OS21, Lemma 4.12] in the case $\mathfrak{F} = \mathbb{Q}_p$ for $p \neq 2, 3$. We add a proof for the general case ($\mathfrak{F}$ arbitrary and $p \neq 2$) further below. As we did for the formulas for the left action, note that if $\mathfrak{F} = \mathbb{Q}_p$ for $p \neq 2$ these formulas simplify as follows:

$$\begin{aligned} (c^-, c^0, c^+)_w \cdot \tau_v &= \big(c^-, c^0, 0\big)_{wv} \quad \text{if } \ell(s_1 wv) = \ell(wv) + 1, \\ (c^-, c^0, c^+)_w \cdot \tau_v &= \big(0, c^0, c^+\big)_{wv} \quad \text{if } \ell(s_0 wv) = \ell(wv) + 1. \end{aligned} \tag{65}$$

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

  Assume that $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$ and $\pi = p$. We recall from (55) the definition of the following isomorphism:

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

  Let $w \in \widetilde{W}$ and let $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$\begin{aligned} \tau_{s_0} \cdot (c^-, c^0, c^+)_w &= e_1(-c^-, -c^0, -c^+)_w + e_{\underline{\mathrm{id}}}(0, -2c^-\iota, 0)_w + (0, 0, -c^-)_{s_0 w} \\ &\qquad \text{if } \ell(s_0 w) = \ell(w) - 1 \text{ and } \ell(w) \geqslant 2, \\ \tau_{s_0} \cdot (c^-, c^0, c^+)_w &= e_1(-c^-, -c^0, -c^+)_w + e_{\underline{\mathrm{id}}}(0, -2c^-\iota, c^0\iota^{-1})_w \\ &\qquad + e_{\underline{\mathrm{id}}^2}(0, 0, c^-)_w + (0, 0, -c^-)_{s_0 w} \\ &\qquad \text{if } \ell(s_0 w) = \ell(w) - 1 \text{ and } \ell(w) = 1 \text{ (i.e., if } w \in (T^0/T^1) \cdot s_0), \\ \tau_{s_1} \cdot (c^-, c^0, c^+)_w &= e_1(-c^-, -c^0, -c^+)_w + e_{\underline{\mathrm{id}}^{-1}}(0, 2c^+\iota, 0)_w + (-c^+, 0, 0)_{s_1 w} \\ &\qquad \text{if } \ell(s_1 w) = \ell(w) - 1 \text{ and } \ell(w) \geqslant 2, \\ \tau_{s_1} \cdot (c^-, c^0, c^+)_w &= e_1(-c^-, -c^0, -c^+)_w + e_{\underline{\mathrm{id}}^{-1}}(-c^0\iota^{-1}, 2c^+\iota, 0)_w \\ &\qquad + e_{\underline{\mathrm{id}}^{-2}}(c^+, 0, 0)_w + (-c^+, 0, 0)_{s_1 w} \\ &\qquad \text{if } \ell(s_1 w) = \ell(w) - 1 \text{ and } \ell(w) = 1 \text{ (i.e., if } w \in (T^0/T^1) \cdot s_1). \end{aligned} \tag{66}$$

  This is proved in [OS21, Proposition 4.9].

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

  Assume that $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$ and $\pi = p$, and let ι be the isomorphism defined in (55).

  - ⋆ Let $(c^-, c^0, c^+)_{s_0} \in H^1(I, \mathbf{X}(s_0))$, and let $v \in \widetilde{W}$ such that $\ell(s_0 v) = \ell(v) - 1$. One has:

$$(0, c^0, 0)_{s_0} \cdot \tau_w = -e_1(0, c^0, 0)_w - e_{\underline{\mathrm{id}}^{-1}}(c^0\iota^{-1}, 0, 0)_w. \tag{67}$$

⋆ Let $(c^-, c^0, c^+)_{s_1} \in H^1(I, \mathbf{X}(s_1))$, and let $v \in \widetilde{W}$ such that $\ell(s_1 v) = \ell(v) - 1$. One has:

$$(0, c^0, 0)_{s_1} \cdot \tau_w = -e_1(0, c^0, 0)_w + e_{\underline{\mathrm{id}}}(0, 0, c^0 \iota^{-1})_w. \tag{68}$$

This is proved in [OS21, Lemma 4.12].

We conclude this subsection with the proof of the two formulas (62) and (64) that are are proved in [OS21] only under more restrictive assumptions.

Proof of (62) *and* (64). First of all let us derive formulas (62) from formulas (64) using the anti-involution $\mathcal{J}$. Let us only treat the case of s_0; the other case can be proved similarly or derived from this one using the involutive automorphism Γ_ϖ. Without loss of generality, we may assume that $w = (s_1 s_0)^i$ for some $i \in \mathbb{Z}_{\geqslant 0}$ or that $w = s_1(s_0 s_1)^i$ for some $i \in \mathbb{Z}_{\geqslant 0}$: indeed if our formula is true in these special cases, then, using the formula (60), we immediately obtain the formula in the general case. We now compute

$$\begin{aligned}
\tau_{s_0} \cdot (c^-, c^0, c^+)_{(s_1 s_0)^i} &= \mathcal{J}\big(\mathcal{J}\big((c^-, c^0, c^+)_{(s_1 s_0)^i}\big) \cdot \mathcal{J}(\tau_{s_0})\big) \\
&= \mathcal{J}\big((c^-, c^0, c^+)_{(s_0 s_1)^i} \cdot \tau_{s_0 c_{-1}}\big) \\
&\qquad \text{by (57)} \\
&= \mathcal{J}\big((c^-, \Psi_{\ell((s_0 s_1)^i), \ell((s_0 s_1)^i)+1}(c^0), 0)_{(s_0 s_1)^i s_0 c_{-1}}\big) \\
&\qquad \text{by (62) and (60)} \\
&= (0, -\Psi_{\ell((s_1 s_0)^i)}(c^0), -c^-)_{(s_0 s_1)^i s_0} \\
&\qquad \text{by (57)}, \\
\tau_{s_0} \cdot (c^-, c^0, c^+)_{s_1 (s_0 s_1)^i} &= \mathcal{J}\big(\mathcal{J}\big((c^-, c^0, c^+)_{s_1 (s_0 s_1)^i}\big) \cdot \mathcal{J}(\tau_{s_0})\big) \\
&= \mathcal{J}\big((-c^+, -c^0, -c^-)_{s_1 (s_0 s_1)^i c_{-1}} \cdot \tau_{s_0 c_{-1}}\big) \\
&\qquad \text{by (57)} \\
&= \mathcal{J}\big((0, -\Psi_{\ell(s_1 (s_0 s_1)^i), \ell(s_1 (s_0 s_1)^i)+1}(c^0), -c^-)_{s_1 (s_0 s_1)^i s_0}\big) \\
&\qquad \text{by (62) and (60)} \\
&= \big((0, -\Psi_{\ell(s_1 (s_0 s_1)^i)}(c^0), -c^-)_{(s_0 s_1)^{i+1}} \\
&\qquad \text{by (57)}.
\end{aligned}$$

This proves the cases of (62) we had to show.

We now turn to the proof of (64). To compute the product, we use the formula of Corollary 1.9.5:

$$\begin{gathered}
(c^-, c^0, c^+)_w \cdot \tau_v \in H^1(I, \mathbf{X}(wv)), \\
\mathrm{Sh}_{wv}((c^-, c^0, c^+)_w \cdot \tau_v) = \mathrm{res}^{I_w}_{I_{wv}}\big(\mathrm{Sh}_w((c^-, c^0, c^+)_w)\big).
\end{gathered} \tag{69}$$

Therefore, the computation of the product amounts to the computation of a restriction (i.e., the map induced on cohomology by the inclusion $I_{wv} \hookrightarrow I_w$). We look at the Frattini quotients (described in Lemma 1.10.1) and compute the map $(I_{wv})_\Phi \longrightarrow (I_w)_\Phi$ induced by the inclusion:

$$\begin{tikzcd}
(I_{wv})_\Phi \arrow[rr, "\text{ind. by. } I_{wv} \hookrightarrow I_w"] & & (I_w)_\Phi \\
\frac{\mathfrak{O}}{\mathfrak{M}} \times \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p (1+\mathfrak{M}^{\ell(wv)+1})} \times \frac{\mathfrak{O}}{\mathfrak{M}} \arrow[u, "\cong", "\overline{\begin{pmatrix} 1 & 0 \\ \pi^{\ell(wv)+1} c & 1 \end{pmatrix} \cdot \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}} \mapsfrom (\overline{c}, \overline{t}, \overline{b})"'] \arrow[rr, "(\overline{c}, \overline{t}, \overline{b}) \mapsto (0, \overline{t}, \overline{b})"] & & \frac{\mathfrak{O}}{\mathfrak{M}} \times \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p (1+\mathfrak{M}^{\ell(w)+1})} \times \frac{\mathfrak{O}}{\mathfrak{M}}. \arrow[u, "\overline{\begin{pmatrix} 1 & 0 \\ \pi^{\ell(w)+1} c & 1 \end{pmatrix} \cdot \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}} \mapsfrom (\overline{c}, \overline{t}, \overline{b})", "\cong"']
\end{tikzcd}$$

Therefore on cohomology the picture is the following (in the diagram, to save space we use the notation $(\_)' \coloneqq \mathrm{Hom}_{\mathbb{F}_p}(\_, k)$):

$$\begin{tikzcd}
H^1(I_{wv}, k) \arrow[d, "\cong"'] & & H^1(I_w, k) \arrow[ll, "\mathrm{res}^{I_w}_{I_{wv}}"'] \arrow[d, "\cong"] \\
\left(\frac{\mathfrak{O}}{\mathfrak{M}}\right)' \times \left(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(wv)+1})}\right)' \times \left(\frac{\mathfrak{O}}{\mathfrak{M}}\right)' & & \left(\frac{\mathfrak{O}}{\mathfrak{M}}\right)' \times \left(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}\right)' \times \left(\frac{\mathfrak{O}}{\mathfrak{M}}\right)'. \arrow[ll, "{(0,\Psi_{\ell(w),\ell(wv)}(c^0),c^+) \leftarrow\!\shortmid (c^-,c^0,c^+)}"']
\end{tikzcd}$$

Looking again at (69), we conclude that

$$(c^-, c^0, c^+)_w \cdot \tau_v = (0, \Psi_{\ell(w),\ell(wv)}(c^0), c^+)_{wv},$$

as we wanted. ■

1.10.d The 1^{st} graded piece E^1: the E^0-bimodule structure

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5), and we choose $\pi = p$.

Recall from (50) and (51) the definitions of the maps f_1 and g_1. In [OS21] a complete description of E^1 as an E^0-bimodule is achieved, using the kernels of the maps f_1 and g_1. In the following proposition we partially recall this result; for the complete statements see the results in [OS21] quoted in the proof.

Proposition 1.10.2. *One has the following facts:*

- *The intersection* $\ker(f_1) \cap \ker(g_1)$ *is zero, and hence we have an exact sequence of* E^0*-bimodules*

$$0 \longrightarrow \ker(f_1) \oplus \ker(g_1) \longrightarrow E^1 \longrightarrow \frac{E^1}{\ker(f_1)\oplus\ker(g_1)} \longrightarrow 0.$$

- *The* E^0*-bimodule* $\frac{E^1}{\ker(f_1)\oplus\ker(g_1)}$ *has dimension* 4 *as a* k*-vector space, and a* k*-basis is given by*

$$e_{\underline{\mathrm{id}}} \cdot \beta_1^+ \cdot e_{\underline{\mathrm{id}}^{-1}}, \qquad e_{\underline{\mathrm{id}}} \cdot \beta_{s_1}^+ \cdot e_{\underline{\mathrm{id}}},$$
$$e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \cdot e_{\underline{\mathrm{id}}}, \qquad e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_{s_0}^- \cdot e_{\underline{\mathrm{id}}^{-1}}.$$

- *The* E^0*-bimodule* $\ker(f_1)$ *is an* $(E^0)_\zeta$*-bimodule (where* $(E^0)_\zeta$ *denotes the localization of* E^0 *at the powers of* ζ*: the Ore conditions are satisfied and such localization is a classical ring of fractions: see [OS21, Remark 8.7]), and it is generated as an* $(E^0)_\zeta$*-bimodule by the following two elements:*

$$\beta_1^+ - 2e_{\underline{\mathrm{id}}}\beta_{s_0}^0 - e_{\underline{\mathrm{id}}}\beta_{s_1 s_0}^+, \qquad \beta_1^- + 2e_{\underline{\mathrm{id}}^{-1}}\beta_{s_1}^0 - e_{\underline{\mathrm{id}}^{-1}}\beta_{s_0 s_1}^-.$$

- *The* E^0*-bimodule* $\ker(g_1)$ *is isomorphic to* F^1E^0*, and an explicit isomorphism is given by*

$$\begin{aligned} F^1E^0 &\longrightarrow \ker(g_1) \\ \tau_w &\longmapsto \beta_w^{0,\star}, \end{aligned} \tag{70}$$

where

$$\beta_w^{0,\star} := \begin{cases} \beta_w^0 & \text{if } \ell(s_0 w) = \ell(w)+1 \text{ and } \ell(w) \geqslant 2, \\ -\beta_w^0 & \text{if } \ell(s_1 w) = \ell(w)+1 \text{ and } \ell(w) \geqslant 2, \\ \beta_w^0 - e_{\underline{\mathrm{id}}}\beta_\omega^+ & \text{if } w = s_1\omega \text{ for some } \omega \in T^0/T^1, \\ -\beta_w^0 - e_{\underline{\mathrm{id}}^{-1}}\beta_\omega^- & \text{if } w = s_0\omega \text{ for some } \omega \in T^0/T^1. \end{cases} \tag{71}$$

Proof. For the first two statements see [OS21, Proposition 7.9 and its proof]. For the third statement see [OS21, Proposition 4.28 and Proposition 7.7]. For the fourth statement see [OS21, Proposition 7.3]. ■

We also give the following less sophisticated result on the finite generation of E^1, which will be fundamental for our computations.

Lemma 1.10.3. *One has the following facts.*

(i) Let $c^-, c^+ \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$ and let $c^0 \in \mathrm{Hom}_{\mathbb{F}_p}\left(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}, k\right)$. The following formulas hold:

$$(c^-,0,0)_1 \cdot \tau_w = (c^-,0,0)_w \tag{72}$$
$$\text{for } w \in \widetilde{W} \text{ with } \ell(s_1 w) = \ell(w)+1,$$
$$(0,0,c^+)_1 \cdot \tau_w = (0,0,c^+)_w \tag{73}$$
$$\text{for } w \in \widetilde{W} \text{ with } \ell(s_0 w) = \ell(w)+1,$$
$$\tau_{(s_1s_0)^i} \cdot (c^-,0,0)_1 = (c^-,0,0)_{(s_1s_0)^i} \tag{74}$$
$$\text{for all } i \in \mathbb{Z}_{\geqslant 0},$$
$$\tau_{s_0(s_1s_0)^i} \cdot (c^-,0,0)_1 = (0,0,-c^-)_{s_0(s_1s_0)^i} \tag{75}$$
$$\text{for all } i \in \mathbb{Z}_{\geqslant 0},$$
$$\tau_{(s_0s_1)^i} \cdot (0,0,c^+)_1 = (0,0,c^+)_{(s_0s_1)^i} \tag{76}$$
$$\text{for all } i \in \mathbb{Z}_{\geqslant 0},$$
$$\tau_{s_1(s_0s_1)^i} \cdot (0,0,c^+)_1 = (-c^+,0,0)_{s_1(s_0s_1)^i} \tag{77}$$
$$\text{for all } i \in \mathbb{Z}_{\geqslant 0},$$
$$(0,c^0,0)_{s_i} \cdot \tau_w = (0,c^0,0)_{s_i w} \tag{78}$$
$$\text{for } i \in \{0,1\} \text{ and } w \in \widetilde{W} \text{ with } \ell(s_i w) = \ell(w)+1,$$
$$\tau_w \cdot (0,c^0,0)_{s_i} = (-1)^{\ell(w)}(0,c^0,0)_{ws_i} \tag{79}$$
$$\text{for } i \in \{0,1\} \text{ and } w \in \widetilde{W} \text{ with } \ell(ws_i) = \ell(w)+1.$$

(ii) One has that the following elements generate E^1 as an E^0-bimodule:

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

(where the notation has been introduced in (56)*).*

Proof. Let us prove the two statements.

(i) Formulas (72), (73) and (78) are immediate consequence of the formulas describing the right action of E^0 when lengths add up (namely, formulas (65)). Formulas (74), (75), (76) and (77) can be shown using the formulas describing the left action of E^0 when lengths add up (namely, formulas (63)). The same is true for formula (79), also recalling the left action of τ_ω for $\omega \in T^0/T^1$ of formula (59).

(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 $\ell(v) \geqslant 1$) lie in the sub-E^0 bimodule generated by the four elements in the statement. For β_v^0 this is clear form formula (78) (or from formula (79)). For β_v^- and β_v^+, using (60) (or (59)), 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 $i \in \mathbb{Z}_{\geqslant 0}$. Then we can apply the formulas in part (i) to conclude. ■

1.10.e The 2^{nd} graded piece E^2

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5), and we choose $\pi = p$.

As already said, under our assumptions I is torsion-free, and, since G has dimension 3 as an analytic manifold over $\mathbb{Q}_p$, Theorem 1.9.8 yields a duality between E^1 and E^2. By construction, this duality comes from a duality between $H^1(I, \mathbf{X}(w))$ and $H^2(I, \mathbf{X}(w))$ for all $w \in \widetilde{W}$. Recall that we described $H^1(I, \mathbf{X}(w))$ via our fixed isomorphism

$$(-,-,-)_w \colon \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \times \mathrm{Hom}_{\mathbb{F}_p}\Big(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}, k\Big) \times \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \longrightarrow H^1(I, \mathbf{X}(w)).$$

For a finite-dimensional $\mathbb{F}_p$-vector space V one has a natural identification

$$\mathrm{Hom}_k\big(\mathrm{Hom}_{\mathbb{F}_p}(V, k), k\big) \cong V \otimes_{\mathbb{F}_p} k.$$

Using this identification and the above isomorphism, we obtain an isomorphism

$$(-,-,-)_w \colon (\mathfrak{O}/\mathfrak{M} \otimes_{\mathbb{F}_p} k) \times \Big(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})} \otimes_{\mathbb{F}_p} k\Big) \times (\mathfrak{O}/\mathfrak{M} \otimes_{\mathbb{F}_p} k) \longrightarrow H^2(I, \mathbf{X}(w)).$$

Recall from the analogous statement for $H^1(I, \mathbf{X}(w))$ that the dimension of the k-vector space $H^2(I, \mathbf{X}(w))$ is 3 if $\ell(w) \geqslant 1$, and it is 2 if $\ell(w) = 0$ (in this case $\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})}$ is the trivial group).

As for E^1, it is sometimes useful to fix a basis for each $H^1(I, \mathbf{X}(w))$ (for $w \in \widetilde{W}$) in a uniform way. To this end, let us fix an element $\boldsymbol{\alpha} \in \big(\mathfrak{O}/\mathfrak{M}\big) \smallsetminus \{0\}$, and, recalling the definition of the map

$$\begin{aligned} \iota \colon\ (1+\mathfrak{M})/(1+\mathfrak{M}^2) &\longrightarrow \mathfrak{O}/\mathfrak{M} = \mathbb{F}_p \\ \overline{1+px} &\longmapsto \overline{x}, \end{aligned}$$

we define, for all $w \in \widetilde{W}$,

$$\begin{aligned} \alpha_w^- &:= (\boldsymbol{\alpha}, 0, 0)_w, \\ \alpha_w^+ &:= (0, 0, \boldsymbol{\alpha})_w, \\ \alpha_w^0 &:= (0, \iota^{-1}(\boldsymbol{\alpha}), 0)_w \qquad \text{if } \ell(w) \geqslant 1. \end{aligned} \tag{80}$$

This is clearly a k-basis of $H^2(I, \mathbf{X}(w))$. In some situations further assumptions on $\boldsymbol{\alpha}$ will be introduced (see Subsection 4.5.a).

We recall some explicit formulas from [OS21].

- Action of the anti-involution $\mathcal{J}$ on E^2 (see [OS21, Equations (86) and (87)]):

  Let $w \in \widetilde{W}$ and let $(\alpha^-, \alpha^0, \alpha^+)_w \in H^2(I, \mathbf{X}(w))$. Furthermore, let $u_w \in (\mathfrak{O}/\mathfrak{M})^\times$ be such that $\omega_{u_w}^{-1} w$ lies in the subgroup of $\widetilde{W}$ generated by s_0 and s_1 (as already stated, 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). One has:

$$\mathcal{J}\big((\alpha^-,\alpha^0,\alpha^+)_w\big) = \begin{cases} \big(u_w^{-2}\alpha^-, \alpha^0, u_w^2\alpha^+\big)_{w^{-1}} & \text{if } \ell(w) \text{ is even,} \\ \big(-u_w^2\alpha^+, -\alpha^0, -u_w^{-2}\alpha^-\big)_{w^{-1}} & \text{if } \ell(w) \text{ is odd.} \end{cases} \tag{81}$$

- Action of the involutive automorphism Γ_ϖ on E^2 (see [OS21, Lemma 5.2]):
  Let $w \in \widetilde{W}$ and let $(\alpha^-,\alpha^0,\alpha^+)_w \in H^2(I,\mathbf{X}(w))$. One has:

$$\Gamma_\varpi\big((\alpha^-,\alpha^0,\alpha^+)_w\big) = (\alpha^+,-\alpha^0,\alpha^-)_{\varpi w\varpi^{-1}}. \tag{82}$$

- Left and right action of τ_ω on E^1 for $\omega \in T^0/T^1$:
  Let $u \in (\mathfrak{O}/\mathfrak{M})^\times$, let $w \in \widetilde{W}$ and let $(\alpha^-,\alpha^0,\alpha^+)_w \in H^2(I,\mathbf{X}(w))$. One has:

$$\tau_{\omega_u}\cdot(\alpha^-,\alpha^0,\alpha^+)_w = (u^2\alpha^-,\alpha^0,u^{-2}\alpha^+)_{\omega_u w}, \tag{83}$$
$$(\alpha^-,\alpha^0,\alpha^+)_w\cdot\tau_{\omega_u} = (\alpha^-,\alpha^0,\alpha^+)_{w\omega_u}. \tag{84}$$

  For the proof of the first formula see [OS21, 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.

- Action of the idempotents on E^2:
  Let $\lambda \in \widehat{T^0/T^1}$, let $w \in \widetilde{W}$ and let $(\alpha^-,\alpha^0,\alpha^+)_w \in H^2(I,\mathbf{X}(w))$. One has:

$$\begin{aligned} \alpha_w^-\cdot e_\lambda &= e_{\lambda^{(-1)^{\ell(w)}}\cdot\underline{\mathrm{id}}^2}\cdot\alpha_w^-, \\ \alpha_w^0\cdot e_\lambda &= e_{\lambda^{(-1)^{\ell(w)}}}\cdot\alpha_w^0 & \text{(if } \ell(w)\geqslant 1), \\ \alpha_w^+\cdot e_\lambda &= e_{\lambda^{(-1)^{\ell(w)}}\cdot\underline{\mathrm{id}}^{-2}}\cdot\alpha_w^+. \end{aligned} \tag{85}$$

- Left action of τ_{s_0} and τ_{s_1} when lengths add up (see [OS21, Proposition 5.5]):
  Let $w \in \widetilde{W}$ and let $(\alpha^-,\alpha^0,\alpha^+)_w \in H^2(I,\mathbf{X}(w))$. One has:

$$\begin{aligned} \tau_{s_0}\cdot(\alpha^-,\alpha^0,\alpha^+)_w &= (-\alpha^+,0,0)_{s_0w} \\ &\qquad \text{if } \ell(s_0w)=\ell(w)+1, \\ \tau_{s_1}\cdot(\alpha^-,\alpha^0,\alpha^+)_w &= (0,0,-\alpha^-)_{s_1w} \\ &\qquad \text{if } \ell(s_1w)=\ell(w)+1. \end{aligned} \tag{86}$$

- Left action of τ_{s_0} and τ_{s_1} when lengths do not add up (see [OS21, Proposition 5.5]):

Let $w \in \widetilde{W}$ and let $(\alpha^-, \alpha^0, \alpha^+)_w \in H^2(I, \mathbf{X}(w))$. One has:

$$\begin{aligned}
\tau_{s_0} \cdot (\alpha^-, \alpha^0, \alpha^+)_w &= e_1(-\alpha^-, -\alpha^0, -\alpha^+)_w + e_{\underline{\mathrm{id}}}(2\iota(\alpha^0), 0, 0)_w \\
&\quad + (-\alpha^+, -\alpha^0, 0)_{s_0 w} \\
&\quad \text{if } \ell(s_0 w) = \ell(w) - 1 \text{ and } \ell(w) \geqslant 2, \\
\tau_{s_0} \cdot (\alpha^-, \alpha^0, \alpha^+)_w &= e_1(-\alpha^-, -\alpha^0, -\alpha^+)_w + e_{\underline{\mathrm{id}}}(2\iota(\alpha^0), -\iota^{-1}(\alpha^+), 0)_w \\
&\quad + e_{\underline{\mathrm{id}}^2}(\alpha^+, 0, 0)_w + (-\alpha^+, 0, 0)_{s_0 w} \\
&\quad \text{if } \ell(s_0 w) = \ell(w) - 1 \text{ and } \ell(w) = 1 \text{ (i.e., if } w \in (T^0/T^1) \cdot s_0), \\
\tau_{s_1} \cdot (\alpha^-, \alpha^0, \alpha^+)_w &= e_1(-\alpha^-, -\alpha^0, -\alpha^+)_w + e_{\underline{\mathrm{id}}^{-1}}(0, 0, -2\iota(\alpha^0))_w \\
&\quad + (0, -\alpha^0, -\alpha^-)_{s_1 w} \\
&\quad \text{if } \ell(s_1 w) = \ell(w) - 1 \text{ and } \ell(w) \geqslant 2, \\
\tau_{s_1} \cdot (\alpha^-, \alpha^0, \alpha^+)_w &= e_1(-\alpha^-, -\alpha^0, -\alpha^+)_w + e_{\underline{\mathrm{id}}^{-1}}(0, \iota^{-1}(\alpha^-), -2\iota(\alpha^0))_w \\
&\quad + e_{\underline{\mathrm{id}}^{-2}}(0, 0, \alpha^-)_w + (0, 0, -\alpha^-)_{s_1 w} \\
&\quad \text{if } \ell(s_1 w) = \ell(w) - 1 \text{ and } \ell(w) = 1 \text{ (i.e., if } w \in (T^0/T^1) \cdot s_1).
\end{aligned} \tag{87}$$

We will now (partially) state the description of E^2 as an E^0-bimodule proved in [OS21]. As for E^1, for the complete statements see the results in [OS21] quoted in the proof. As in Proposition 1.10.2, we consider the localization $(E^0)_\zeta$ of E^0 at the powers of ζ.

Proposition 1.10.4. *The following statements hold.*

- *One has the following decomposition (of E^0-bimodules):*

$$E^2 = \ker(f_2) \oplus \ker(g_2).$$

- *The E^0-bimodule* $\ker(f_1)$ *is an $(E^0)_\zeta$-bimodule, and it is generated as an $(E^0)_\zeta$-bimodule by the following two elements:*

$$\alpha_1^- - e_{\underline{\mathrm{id}}}\alpha_{s_0}^0, \qquad\qquad \alpha_1^+ + e_{\underline{\mathrm{id}}^{-1}}\alpha_{s_1}^0.$$

- *Let us define $(F^1E^0)^{\vee,\mathrm{finite}}$ as the sub-k-vector space of $(F^1E^0)^\vee$ spanned by the "dual basis" $(\tau_w^\vee|_{F^1E^0})_{w\in\widetilde{W}^{\ell\geqslant 1}}$ of the basis $(\tau_w)_{w\in\widetilde{W}^{\ell\geqslant 1}}$ of F^1E^0. Equivalently,*

$$(F^1E^0)^{\vee,\mathrm{finite}} = \bigcup_{n\in\mathbb{Z}_{\geqslant 1}} \left(F^1E^0/F^nE^0\right)^\vee,$$

from which it is clear that $(F^1E^0)^{\vee,\mathrm{finite}}$ is a sub-E^0-bimodule of $(F^1E^0)^\vee$. One has that there exists a unique isomorphism of E^0-bimodules of the following form:

$$\begin{aligned}
{}^{\mathcal{J}}\!\left((F^1E^0)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}} &\longrightarrow \ker(g_2) \\
\underset{(w\in\widetilde{W} \text{ with } \ell(w)\geqslant 1)}{\tau_w^\vee|_{F^1E^0}} &\longmapsto \alpha_w^{0,\star},
\end{aligned}$$

where $\alpha_w^{0,\star}$ has the property that

$$\begin{aligned}
\alpha_w^{0,\star} - \alpha_w^0 &\in e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}}\ker(f_2) \quad \text{if } \ell(s_0 w) = \ell(w) + 1, \\
\alpha_w^{0,\star} + \alpha_w^0 &\in e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}}\ker(f_2) \quad \text{if } \ell(s_1 w) = \ell(w) + 1.
\end{aligned} \tag{88}$$

Proof. For the first statement see [OS21, Proposition 7.12]. For the second statement see [OS21, §7.3.2] and in particular [OS21, Propsition 7.18]. For the third statement see [OS21, Equations (123) and (124)]; uniqueness is clear because the difference of two isomorphisms satisfying the claimed property would take values in $\ker(f_2) \cap \ker(g_2) = \{0\}$. ■

1.10.f The top graded piece E^d

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5) and that I is torsion-free.

Note that the torsion-free assumption implies in particular that field is a finite extension of $\mathbb{Q}_p$, because if instead $\mathfrak{F}$ is a field of Laurent series then $\left(\begin{smallmatrix} 1 & \mathfrak{O} \\ 0 & 1 \end{smallmatrix}\right)$ is annihilated by p. It also implies that $p \neq 2, 3$, because for example $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & -1 \\ 3 & 1-3 \end{smallmatrix}\right)$ are torsion elements in the pro-p Iwahori subgroup for $p = 2$ and $p = 3$ respectively. Recall also from (46) that the torsion-free assumption is satisfied if $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$.

Finally, recall that under our assumptions I is a Poincaré group of dimension d, where d is the dimension of G as an analytic manifold over $\mathbb{Q}_p$.

Let us see how the explicit formulas for the left and right action of E^0 on E^d look like. For all $\omega \in T^0/T^1$, for all $j \in \{0, 1\}$ and for all $w \in \widetilde{W}$, we have:

$$
\begin{aligned}
&\tau_\omega \cdot \phi_w = \phi_{\omega w}, \\
&\phi_w \cdot \tau_\omega = \phi_{w\omega}, \\
&\tau_{s_j} \cdot \phi_w = \begin{cases} \phi_{s_j w} - e_1 \cdot \phi_w & \text{if } \ell(s_j w) = \ell(w) - 1, \\ 0 & \text{if } \ell(s_j w) = \ell(w) + 1, \end{cases} \\
&\phi_w \cdot \tau_{s_j} = \begin{cases} \phi_{w s_j} - \phi_w \cdot e_1 & \text{if } \ell(w s_j) = \ell(w) - 1, \\ 0 & \text{if } \ell(w s_j) = \ell(w) + 1. \end{cases}
\end{aligned} \tag{89}
$$

This is immediate from the general formulas for the left and right actions of E^0 on E^d stated in Proposition 1.9.9 (and, for s_1, from the subsequent observation about the representatives for which the formulas are still valid).

We remark that for all $w \in \widetilde{W}$ we have

$$
e_1 \cdot \phi_w = \phi_w \cdot e_1. \tag{90}
$$

This is easy to see using the fact that for all $\omega \in T^0/T^1$ one has either $\omega w = w\omega$ or $\omega w = w\omega^{-1}$, depending on the length of w.

The following proposition describes the E^0-bimodule structure of E^d. The map $\mathcal{S}$ and its induced map on cohomology were defined in (39).

Proposition 1.10.5. *One has a decomposition of E^0-bimodules*

$$
E^d = k e_1 \phi_1 \oplus \ker(\mathcal{S}^d).
$$

Moreover, E^0 acts on $k e_1$ on the right and on the left through the character

$$
\begin{aligned}
\chi_{\mathrm{triv}} \colon E^0 &\longrightarrow k \\
\tau_w &\longmapsto \begin{cases} 1 & \text{if } \ell(w) = 0, \\ 0 & \text{if } \ell(w) \geqslant 1, \end{cases}
\end{aligned} \tag{91}
$$

and $\ker(\mathcal{S}^d)$ is the injective hull of $\left(E^0/\zeta E^0\right)^\vee$ as a left as well as a right E^0-module.

Proof. The first two claims follows from the more general statement of Proposition 1.9.10, and the third claim is proved in [OS21, Proposition 3.3]. ∎

Chapter 2

The centre of the Ext-algebra for $\mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$

2.1 Summary of the results

In this chapter we will determine completely the centre of E^* for the group $\mathrm{SL}_2(\mathbb{Q}_p)$ for $p \neq 2, 3$. Recall from (46) that under these assumptions we have

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

We will prove the following theorem, which achieves the claimed description of the centre.

Theorem 2.1.1. *If $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the usual choices made in Section 1.5), then the centre of E^* can be described in the following way.*

- *The 0^{th} graded piece $Z(E^*)^0$ is isomorphic to $k \times k$ as a k-algebra. As a k-vector space, it is spanned by τ_1 and $\tau_{c_{-1}}$ where c_{-1} is the element of $\widetilde{W}$ represented by the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.*
- *The 1^{st} graded piece $Z(E^*)^1$ is zero.*
- *The 2^{nd} graded piece $Z(E^*)^2$ is free as a module over the ring $Z(E^*)^0 \cong k \times k$ of rank $\aleph_0$. Moreover, choosing $\pi = p$, an explicit k-basis is the following:*

$$e_1 \cdot \alpha^0_{s_0}, \qquad e_{\chi_0} \cdot \alpha^0_{s_0}, \qquad e_1 \cdot \alpha^0_{s_1}, \qquad e_{\chi_0} \cdot \alpha^0_{s_1},$$

$$e_\lambda \alpha^0_{(s_1 s_0)^i} - e_{\lambda^{-1}} \alpha^0_{(s_0 s_1)^i}$$
$$\text{for } \lambda \in \widehat{T^0/T^1} \smallsetminus \{1, \underline{\mathrm{id}}\} \text{ and } i \in \mathbb{Z}_{\geqslant 1},$$

$$e_{\underline{\mathrm{id}}} \alpha^0_{(s_1 s_0)^i} - e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0 s_1)^i}$$
$$+ 2 \sum_{j=0}^{i-1} \Big(e_{\underline{\mathrm{id}}^{-1}} \cdot (\alpha^+_{s_0 (s_1 s_0)^i} - \alpha^+_{s_1 (s_0 s_1)^i}) + e_{\underline{\mathrm{id}}} \cdot (\alpha^-_{s_1 (s_0 s_1)^i} - \alpha^-_{s_0 (s_1 s_0)^i}) \Big)$$
$$\text{for } i \in \mathbb{Z}_{\geqslant 1},$$

$$e_1 \alpha^0_{(s_1 s_0)^i} + e_1 \alpha^0_{(s_0 s_1)^i} - e_1 \cdot \alpha^0_{(s_1 s_0)^i s_1} - e_1 \cdot \alpha^0_{(s_0 s_1)^i s_0}$$
$$\text{for } i \in \mathbb{Z}_{\geqslant 1},$$

where the e_λ's are the idempotent of E^0 defined in (16), and where the elements α^0_w (for $w \in \widetilde{W}$) were defined in (80).

- *The 3^{rd} graded piece $Z(E^*)^3$ is free as a module over the ring $Z(E^*)^0 \cong k \times k$ of rank $\aleph_0$. Moreover, an explicit k-basis is the following:*

$$\begin{aligned}
&e_\lambda \phi_1 \qquad \text{for } \lambda \in \widehat{T^0/T^1}. \\
&e_1\phi_{s_0}, \qquad e_1\phi_{s_1}, \qquad e_{\chi_0}\phi_{s_0}, \qquad e_{\chi_0}\phi_{s_1}, \\
&U_{\lambda,i} := e_\lambda \phi_{(s_1s_0)^i} + e_{\lambda^{-1}}\phi_{(s_0s_1)^i} \\
&\qquad \text{for } \lambda \in \widehat{T^0/T^1} \smallsetminus \{1\} \text{ and } i \in \mathbb{Z}_{\geqslant 1}, \\
&U_{1,i} := e_1\phi_{(s_1s_0)^i} + e_1\phi_{(s_0s_1)^i} - e_1\phi_{s_1(s_0s_1)^i} - e_1\phi_{s_0(s_1s_0)^i} \\
&\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1},
\end{aligned}$$

  where the e_λ's are as above and where $(\phi_w)_{w\in\widetilde{W}}$ is the basis of E^3 defined in Subsection 1.9.g.

Proof. The 0^{th} graded piece will be determined in Proposition 2.4.1. The 1^{st} graded piece will be determined in Proposition 2.5.2.

The basis of $Z(E^*)^2$ will be computed in Proposition 2.6.12 (with some different sign conventions) and the basis of $Z(E^*)^3$ will be computed in Lemma 2.3.1.

Finally, the freeness results will be proved in Remark 2.8.1. ∎

Furthermore, in this chapter we will prove the following additional facts:

- If $G = \mathrm{SL}_2(\mathfrak{F})$ and I is torsion-free, we determine a basis of $Z(E^*)^d$ (Proposition 2.2.1). If furthermore $\mathbb{F}_q \subseteq k$, then one can use the same basis of $Z(E^*)^d$ defined in the above theorem (Lemma 2.3.1).

- If $G = \mathrm{SL}_2(\mathfrak{F})$, if I is torsion-free and if $\mathbb{F}_q \subseteq k$, we determine the structure of $Z(E^*)^d = Z_{E^0}(E^d)$ as a $Z(E^0)$-module (Proposition 2.3.6). In particular we show that there is a decomposition of $Z(E^0)$-modules

$$Z(E^*)^d = ke_1\phi_1 \oplus N \oplus \mathcal{E},$$

  where N is a finite direct sum of submodules of dimension 1 over k and where $\mathcal{E}$ is the injective hull of $\big(Z(E^0)/\zeta Z(E^0)\big)^\vee$ (the element ζ was defined in (28)).

  This result yields a strong analogy with the description of E^d as an E^0-bimodule recalled from [OS19] and [OS21] in Proposition 1.10.5.

- If $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ we show that $Z(E^*)^2 = Z_{E^0}(E^2)$ (see Proposition 2.6.12). Hence $Z(E^*)^2$ has a structure of as $Z(E^0)$-module, and we determine it in Subsection 2.7.

We conclude this overview by highlighting the stark contrast between the algebraic properties of $Z(E^*)$ and of $Z(E^0)$ (compare with Theorem 1.6.2 and the following lines).

Remark 2.1.2. Assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$. One has the following (negative) results:

- $Z(E^*)$ is not Noetherian as a k-algebra;

- E^* is not finitely generated as a $Z(E^*)$-module;

- E^* is not left nor right Noetherian as a k-algebra.

Proof. Let us prove the three claims.

- If, by contradiction, $Z(E^*)$ were Noetherian as a k-algebra, then the ideal $Z(E^*)^3$ would be finitely generated. And this is not the case since $Z(E^*)^0$ has finite dimension as a k-vector space, while $Z(E^*)^3$ has infinite dimension as a k-vector space.

- If, by contradiction, E^* were finitely generated as a $Z(E^*)$-module, then E^0 would be finitely generated as a $Z(E^*)^0$-module. And, again, this is not the case since $Z(E^*)^0$ has finite dimension as a k-vector space, while E^0 has infinite dimension as a k-vector space.

- The k-algebra E^* is not left nor right Noetherian because we have the ascending exhaustive filtration of bilateral sub-ideals of E^3

$$E^3 = \bigcup_{n \in \mathbb{Z}_{\geqslant 0}} F_n E^3,$$

which shows that E^3 is not finitely generated, even as a bilateral ideal. ■

2.2 The top graded piece of the centre

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5) and that I is torsion-free.

Recall from Subsection 1.10.f that the above assumption implies that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ with $p \neq 2, 3$ and also that I is a Poincaré group of dimension d, where d is the dimension of G as an analytic manifold over $\mathbb{Q}_p$. Finally, recall that the torsion-free assumption is satisfied if $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$.

As in Subsection 1.9.g, let us consider the k-basis $(\phi_w)_{w \in \widetilde{W}}$ of E^d obtained by dualizing the k-basis $(\tau_w)_{w \in \widetilde{W}}$ of E^0. Also recall the definition of c_{-1} from (21).

Proposition 2.2.1. *$Z(E^*)^d$ is the sub-k-vector space of E^d having the following basis:*

$$\phi_\omega \qquad \text{for } \omega \in T^0/T^1,$$

$$\sum_{\substack{\vartheta \in T^0/T^1 \\ \text{square}}} \phi_{\vartheta s_0}, \qquad \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{not a square}}} \phi_{\vartheta s_0}, \qquad \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{square}}} \phi_{\vartheta s_1}, \qquad \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{not a square}}} \phi_{\vartheta s_1},$$

$$\phi_{\omega (s_0 s_1)^i} + \phi_{\omega^{-1} (s_1 s_0)^i} + \sum_{\vartheta \in T^0/T^1} \left(\phi_{\vartheta (s_0 s_1)^i s_0} + \phi_{\vartheta (s_1 s_0)^i s_1} \right)$$
$$\text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}.$$

Remark 2.2.2. Before seeing the proof of the proposition, let us remark that some possible alternative choices of a basis:

- It is easy to see that we can replace the four elements

$$\sum_{\substack{\vartheta \in T^0/T^1 \\ \text{square}}} \phi_{\vartheta s_0}, \qquad \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{not a square}}} \phi_{\vartheta s_0}, \qquad \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{square}}} \phi_{\vartheta s_1}, \qquad \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{not a square}}} \phi_{\vartheta s_1}$$

with the following four elements:

$$e_1 \cdot \phi_{s_0}, \qquad e_{\chi_0} \cdot \phi_{s_0}, \qquad e_1 \cdot \phi_{s_1}, \qquad e_{\chi_0} \cdot \phi_{s_1},$$

where χ_0 is the quadratic character (Legendre symbol).

- The elements of the form

$$\phi_{\omega(s_0s_1)^i} + \phi_{\omega^{-1}(s_1s_0)^i} + \sum_{\vartheta \in T^0/T^1} \left(\phi_{\vartheta(s_0s_1)^is_0} + \phi_{\vartheta(s_1s_0)^is_1}\right)$$

(for $\omega \in T^0/T^1$ and $i \in \mathbb{Z}_{\geqslant 1}$) can be rewritten as

$$\phi_{\omega(s_0s_1)^i} + \phi_{\omega^{-1}(s_1s_0)^i} - e_1 \cdot \phi_{(s_0s_1)^is_0} - e_1 \cdot \phi_{(s_1s_0)^is_1}.$$

Up to replacing ω by ωc_{-1}, they can also be rewritten as

$$(\tau_{s_0} + \tau_{s_1}) \cdot \left(\phi_{\omega(s_0s_1)^is_0} + \phi_{\omega^{-1}(s_1s_0)^is_1}\right) \qquad \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}$$

or as

$$\left(\phi_{\omega(s_0s_1)^is_0} + \phi_{\omega^{-1}(s_1s_0)^is_1}\right) \cdot (\tau_{s_0} + \tau_{s_1}) \qquad \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}.$$

Proof of the proposition. Recall from (89) that for all $\omega \in T^0/T^1$, $j \in \{0, 1\}$, $w \in \widetilde{W}$, we have the following formulas describing left and right action of E^0 on E^d:

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

Let us consider the following decomposition of E^d as a k-vector space:

$$E = \bigoplus_{i \in \mathbb{Z}_{\geqslant 0}} E_i^d, \qquad \text{where } E_i^d := \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) = i}} k\phi_w.$$

For $v \in \widetilde{W}$, let us consider the k-linear maps

$$\begin{aligned} C_v \colon E^d &\longrightarrow E^d \\ \phi &\longmapsto \tau_v \cdot \phi - \phi \cdot \tau_v. \end{aligned}$$

To ease notation let us define $E_{-1}^d := \{0\}$. By the explicit formulas above it is easy to see that

$$C_\omega(E_i^d) \subseteq E_i^d \qquad \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 0}, \tag{92}$$

and that

$$\begin{aligned} C_{s_0}(E_i^d) &\subseteq E_{i-1}^d \oplus E_i^d & &\text{for } i \in \mathbb{Z}_{\geqslant 0}, \\ C_{s_1}(E_i^d) &\subseteq E_{i-1}^d \oplus E_i^d & &\text{for } i \in \mathbb{Z}_{\geqslant 0}. \end{aligned}$$

Moreover, we claim that

$$\begin{aligned} C_{s_0}\left(E_{2i}^d \oplus E_{2i+1}^d\right) &\subseteq E_{2i-1}^d \oplus E_{2i}^d & &\text{for } i \in \mathbb{Z}_{\geqslant 0}, \\ C_{s_1}\left(E_{2i}^d \oplus E_{2i+1}^d\right) &\subseteq E_{2i-1}^d \oplus E_{2i}^d & &\text{for } i \in \mathbb{Z}_{\geqslant 0}. \end{aligned} \tag{93}$$

Let us prove the first inclusion (the other being completely analogous): by the formulas above the only thing which remains to check is that $C_{s_0}(E^d_{2i+1}) \subseteq E^d_{2i}$. This is true since

$$\begin{aligned}
C_{s_0}\left(\phi_{\omega s_0(s_1s_0)^i}\right) &= \phi_{c_{-1}\omega^{-1}(s_1s_0)^i} - e_1\phi_{\omega s_0(s_1s_0)^i} - \phi_{c_{-1}\omega(s_0s_1)^i} + \phi_{\omega s_0(s_1s_0)^i}e_1 \\
&= \phi_{c_{-1}\omega^{-1}(s_1s_0)^i} - \phi_{c_{-1}\omega(s_0s_1)^i} \in E^d_{2i}, \\
C_{s_0}\left(\phi_{\omega s_1(s_0s_1)^i}\right) &= 0 - 0 = 0,
\end{aligned}$$

where we have used that e_1 centralizes E^d.

Let us consider $\sigma \in E^d$ and let us decompose it as

$$\sigma = \sum_{i \in \mathbb{Z}_{\geqslant 0}} \sigma_i,$$

for suitable $\sigma_i \in E^d_i$ (almost all of them equal to 0). Using (92) and (93), we see that σ is centralized by the whole E^0 if and only if $\sigma_{2i} + \sigma_{2i+1}$ is centralized by the whole E^0 for all $i \in \mathbb{Z}_{\geqslant 0}$.

Hence, in order to compute $Z_{E^0}(E^d)$, it suffices to compute $Z_{E^0}\left(E^d_{2i} \oplus E^d_{2i+1}\right)$ for all $i \in \mathbb{Z}_{\geqslant 0}$. Hence, with notation as above, let us assume that $\sigma = \sigma_{2i} + \sigma_{2i+1}$ for some $i \in \mathbb{Z}_{\geqslant 0}$, and let us determine the conditions under which σ is centralized by the whole E^0. To this end, let us distinguish the two cases $i \geqslant 1$ and $i = 0$.

- Assume that $\sigma = \sigma_{2i} + \sigma_{2i+1}$ with $i \in \mathbb{Z}_{\geqslant 1}$. Let us write it as

  $$\begin{aligned}
  \sigma = &\sum_{\omega \in T^0/T^1} a_\omega \phi_{\omega(s_0s_1)^i} + \sum_{\omega \in T^0/T^1} b_\omega \phi_{\omega(s_1s_0)^i} \\
  &+ \sum_{\omega \in T^0/T^1} a'_\omega \phi_{\omega(s_0s_1)^i s_0} + \sum_{\omega \in T^0/T^1} b'_\omega \phi_{\omega(s_1s_0)^i s_1},
  \end{aligned}$$

  for suitable $a_\omega, b_\omega, a'_\omega, b'_\omega \in k$.

  Using the already mentioned formulas for the left and right action of E^0 on E^d and the fact that e_1 centralises E^d, we compute the following:

  $$\begin{aligned}
  \tau_{s_0} \cdot \sigma = &\sum_{\omega \in T^0/T^1} a_\omega \phi_{c_{-1}\omega^{-1}(s_1s_0)^{i-1}s_1} - \sum_{\omega \in T^0/T^1} a_\omega e_1 \phi_{\omega(s_0s_1)^i} \\
  &+ \sum_{\omega \in T^0/T^1} a'_\omega \phi_{c_{-1}\omega^{-1}(s_1s_0)^i} - \sum_{\omega \in T^0/T^1} a'_\omega e_1 \phi_{\omega(s_0s_1)^i s_0}, \\
  \sigma \cdot \tau_{s_0} = &\sum_{\omega \in T^0/T^1} b_\omega \phi_{c_{-1}\omega(s_1s_0)^{i-1}s_1} - \sum_{\omega \in T^0/T^1} b_\omega e_1 \phi_{\omega(s_1s_0)^i} \\
  &+ \sum_{\omega \in T^0/T^1} a'_\omega \phi_{c_{-1}\omega(s_0s_1)^i} - \sum_{\omega \in T^0/T^1} a'_\omega e_1 \phi_{\omega(s_0s_1)^i s_0}.
  \end{aligned}$$

  Let us compute the parts where e_1 appears: let $w \in \widetilde{W}$, and for all $\omega \in T^0/T^1$ let $d_\omega \in k$. One has

  $$\begin{aligned}
  \sum_{\omega \in T^0/T^1} d_\omega e_1 \phi_{\omega w} &= - \sum_{\omega \in T^0/T^1} \Big(d_\omega \sum_{\omega' \in T^0/T^1} \phi_{\omega'\omega w} \Big) \\
  &= - \sum_{\omega \in T^0/T^1} \Big(d_\omega \sum_{\omega' \in T^0/T^1} \phi_{\omega' w} \Big) \\
  &= - \sum_{\omega' \in T^0/T^1} \Big(\Big(\sum_{\omega \in T^0/T^1} d_\omega \Big) \phi_{\omega' w} \Big).
  \end{aligned}$$

This concludes the previous computation, and we can deduce that

$$\tau_{s_0}\cdot\sigma=\sigma\cdot\tau_{s_0}\quad\Longleftrightarrow\quad\begin{cases} b_\omega=a_{\omega^{-1}} & \text{for all } \omega\in T^0/T^1\\ a'_\omega=\sum_{\vartheta\in T^0/T^1}a_\vartheta & \text{for all } \omega\in T^0/T^1\\ a'_\omega=\sum_{\vartheta\in T^0/T^1}b_\vartheta & \text{for all } \omega\in T^0/T^1\end{cases}$$

$$\Longleftrightarrow\quad\begin{cases} b_\omega=a_{\omega^{-1}} & \text{for all } \omega\in T^0/T^1\\ a'_\omega=\sum_{\vartheta\in T^0/T^1}a_\vartheta & \text{for all } \omega\in T^0/T^1.\end{cases}$$

Doing the same computations with s_1 instead of s_0 (or arguing with the involutive automorphism Γ_ϖ), one gets

$$\tau_{s_1}\cdot\sigma=\sigma\cdot\tau_{s_1}\quad\Longleftrightarrow\quad\begin{cases} b_\omega=a_{\omega^{-1}} & \text{for all } \omega\in T^0/T^1\\ b'_\omega=\sum_{\vartheta\in T^0/T^1}a_\vartheta & \text{for all } \omega\in T^0/T^1.\end{cases}$$

Hence

$$\begin{pmatrix}\sigma\text{ commutes with}\\ \text{both }\tau_{s_0}\text{ and }\tau_{s_1}\end{pmatrix}\quad\Longleftrightarrow\quad\begin{cases} b_\omega=a_{\omega^{-1}} & \text{for all } \omega\in T^0/T^1\\ a'_\omega=\sum_{\vartheta\in T^0/T^1}a_\vartheta & \text{for all } \omega\in T^0/T^1\\ b'_\omega=\sum_{\vartheta\in T^0/T^1}a_\vartheta & \text{for all } \omega\in T^0/T^1.\end{cases}$$

We have thus proved that, given $\sigma\in E^d_{2i}\oplus E^d_{2i+1}$ with $i\in\mathbb{Z}_{\geqslant 1}$, one has that σ commutes with both τ_{s_0} and τ_{s_1} if and only if it is of the form

$$\begin{aligned}\sigma=&\sum_{\omega\in T^0/T^1}c_\omega\left(\phi_{\omega(s_0s_1)^i}+\phi_{\omega^{-1}(s_1s_0)^i}\right)\\ &+\Big(\sum_{\omega\in T^0/T^1}c_\omega\Big)\cdot\sum_{\omega\in T^0/T^1}\left(\phi_{\omega(s_0s_1)^is_0}+\phi_{\omega(s_1s_0)^is_1}\right)\end{aligned}\tag{94}$$

for some $c_\omega\in k$ (where $\omega\in T^0/T^1$). But if σ is of this form, then it commutes also with τ_ω for all $\omega\in T^0/T^1$, because for all $\vartheta\in T^0/T^1$ and $w\in\widetilde{W}$ one has $\vartheta w=w\vartheta$ if $\ell(w)$ is even and $\vartheta w=w\vartheta^{-1}$ if $\ell(w)$ is odd.

Hence, this proves that, given $\sigma\in E^d_{2i}\oplus E^d_{2i+1}$ with $i\in\mathbb{Z}_{\geqslant 1}$,, one has that σ is centralized by the whole E^0 if and only if it is of the form (94).

- Now, let us assume instead that $\sigma=\sigma_0+\sigma_1$ with $\sigma_0\in E^d_0$ and $\sigma_1\in E^d_1$, and let us determine the conditions under which σ is centralized by the whole E^0.
  - ⋆ It is immediate from the explicit formulas that all of E^d_0 is centralized by the whole E^0.
  - ⋆ It remains to describe which of the $\sigma=\sigma_1\in E^d_1$ centralize all of E^0. Hence, let us assume that σ is of the form

$$\sigma=\sum_{\omega\in T^0/T^1}a_\omega\phi_{\omega s_0}+\sum_{\omega\in T^0/T^1}b_\omega\phi_{\omega s_1},$$

for some $a_\omega,b_\omega\in k$. Let us compute

$$\begin{aligned}\tau_{s_0}\cdot\sigma&=\sum_{\omega\in T^0/T^1}a_\omega\phi_{c_{-1}\omega^{-1}}-e_1\sum_{\omega\in T^0/T^1}a_\omega\phi_{\omega s_0},\\ \sigma\cdot\tau_{s_0}&=\sum_{\omega\in T^0/T^1}a_\omega\phi_{c_{-1}\omega}-e_1\sum_{\omega\in T^0/T^1}a_\omega\phi_{\omega s_0}.\end{aligned}$$

Hence we deduce that

$$\tau_{s_0} \cdot \sigma = \sigma \cdot \tau_{s_0} \iff \left(a_\omega = a_{\omega^{-1}} \text{ for all } \omega \in T^0/T^1\right). \tag{95}$$

In the same way we deduce that

$$\tau_{s_1} \cdot \sigma = \sigma \cdot \tau_{s_1} \iff \left(b_\omega = b_{\omega^{-1}} \text{ for all } \omega \in T^0/T^1\right). \tag{96}$$

Now, given $\omega \in T^0/T^1$, let us compute

$$\begin{aligned}
\tau_\omega \cdot \sigma &= \sum_{\omega' \in T^0/T^1} a_{\omega'} \phi_{\omega\omega' s_0} + \sum_{\omega' \in T^0/T^1} b_{\omega'} \phi_{\omega\omega' s_1}, \\
\sigma \cdot \tau_\omega &= \sum_{\omega' \in T^0/T^1} a_{\omega'} \phi_{\omega^{-1}\omega' s_0} + \sum_{\omega' \in T^0/T^1} b_{\omega'} \phi_{\omega^{-1}\omega' s_1} \\
&= \sum_{\omega'' \in T^0/T^1} a_{\omega^2\omega''} \phi_{\omega\omega'' s_0} + \sum_{\omega'' \in T^0/T^1} b_{\omega^2\omega''} \phi_{\omega\omega'' s_1}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\left(\tau_\omega \cdot \sigma = \sigma \cdot \tau_\omega \text{ for all } \omega \in T^0/T^1\right) \\
&\iff \begin{cases} a_{\omega'} = a_{\omega^2\omega'} & \text{for all } \omega, \omega' \in T^0/T^1 \\ b_{\omega'} = b_{\omega^2\omega'} & \text{for all } \omega, \omega' \in T^0/T^1 \end{cases} \\
&\iff \begin{cases} a_\vartheta = a_{\vartheta'} & \text{for all } \vartheta, \vartheta' \in T^0/T^1 \text{ such that } \vartheta^{-1}\vartheta' \text{ is a square} \\ b_\vartheta = b_{\vartheta'} & \text{for all } \vartheta, \vartheta' \in T^0/T^1 \text{ such that } \vartheta^{-1}\vartheta' \text{ is a square.} \end{cases}
\end{aligned}$$

Since by assumption $q \neq 2$, we have $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$, and so we have proved that, given $\sigma \in E_1^d$, one has that σ commutes with τ_ω for all $\omega \in T^0/T^1$ if and only if σ is of the form

$$\sigma = a \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{square}}} \phi_{\vartheta s_0} + a' \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{not a square}}} \phi_{\vartheta s_0} + b \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{square}}} \phi_{\vartheta s_1} + b' \sum_{\substack{\vartheta \in T^0/T^1 \\ \text{not a square}}} \phi_{\vartheta s_1}, \tag{97}$$

for some $a, a', b, b' \in k$. Moreover, from the characterization above of the properties of commuting with τ_{s_0} and τ_{s_1} ((95) and (96)), we see that if σ is of the form (97), then it automatically commutes with both τ_{s_0} and τ_{s_1}.
Therefore we conclude that, given $\sigma \in E_1^d$, one has that σ centralizes all of E^0 if and only if it is of the form (97). ■

2.3 Structure of top graded piece of the centre as a $Z(E^0)$-module

Since $Z(E^*)^d = Z_{E^0}(E^d)$, there is a natural structure of $Z(E^0)$-module on $Z(E^*)^d$. In this section we are going to describe such structure.

2.3.a Assumptions and preliminaries

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5), that I is torsion-free and that $\mathbb{F}_q \subseteq k$.

Recall under these assumptions $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ with $p \neq 2, 3$ and that I is a Poincaré group of dimension d, where d is the dimension of G as an analytic manifold over $\mathbb{Q}_p$. The assumption $\mathbb{F}_q \subseteq k$ will be used in a moment for the existence of enough k-characters of the group T^0/T^1.

Recall the notation

$$\begin{aligned} \widehat{T^0/T^1} &:= \operatorname{Hom}\left(T^0/T^1, k^\times\right), \\ \Gamma &:= \left\{ \{\lambda, \lambda^{-1}\} \;\middle|\; \lambda \in \widehat{T^0/T^1} \right\}. \end{aligned}$$

Moreover, as in Remark 2.2.2, let us consider the quadratic character

$$\begin{aligned} \chi_0 \colon\ T^0/T^1 &\longrightarrow k^\times \\ \omega &\longmapsto \begin{cases} 1 & \text{if } \omega \text{ is a square,} \\ -1 & \text{if } \omega \text{ is not a square.} \end{cases} \end{aligned}$$

Since $p \neq 2$ we have

$$\Gamma = \{\{1\}\} \,\dot\cup\, \{\{\chi_0\}\} \,\dot\cup\, \{\gamma \in \Gamma \mid \#\gamma = 2\}.$$

Recall from Lemma 1.7.1 that since $\mathbb{F}_q \subseteq k$ we have a direct product decomposition

$$Z(E^0) = \prod_{\gamma \in \Gamma} e_\gamma Z(E^0) = \prod_{\gamma \in \Gamma} Z(E^0) e_\gamma.$$

Moreover, for all $\mu \in \widehat{T^0/T^1}$, let us define

$$\begin{aligned} x_\mu &:= e_\mu B_{o_\Pi}(s_0 s_1) + e_{\mu^{-1}} B_{o_\Pi}(s_1 s_0) \\ &= \begin{cases} e_\mu \tau_{s_0 s_1} + e_{\mu^{-1}} \tau_{s_1 s_0} & \text{if } \mu \neq 1, \\ e_1 \zeta = e_1 \tau_{s_0 s_1} + e_1 \tau_{s_1 s_0} + e_1 \tau_{s_0} + e_1 \tau_{s_1} + e_1 & \text{if } \mu \neq 1. \end{cases} \end{aligned}$$

From the above mentioned lemma, we know that the components $e_\gamma Z(E^0)$ can be described in the following way:

$$\begin{aligned} k[X_\lambda] &\xrightarrow{\cong} e_\gamma Z(E^0) \\ 1 &\longmapsto e_\gamma \qquad\qquad \text{if } \gamma = \{1\} \text{ or } \gamma = \{\chi_0\}, \\ X_\lambda &\longmapsto x_\lambda \\ \frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}})} &\xrightarrow{\cong} e_\gamma Z(E^0) \\ 1 &\longmapsto e_\gamma \qquad\qquad \text{if } \gamma = \{\lambda, \lambda^{-1}\} \text{ with } \lambda \neq \lambda^{-1}. \\ X_\lambda &\longmapsto x_\lambda \\ X_{\lambda^{-1}} &\longmapsto x_{\lambda^{-1}} \end{aligned} \tag{98}$$

The decomposition $Z(E^0) = \prod_{\gamma \in \Gamma} e_\gamma Z(E^0)$ induces a decomposition

$$Z(E^*)^d = \prod_{\gamma \in \Gamma} e_\gamma Z(E^*)^d.$$

The following lemma, which easily follows from the results in Section 2.2, describes a k-basis of $Z(E^*)^d$ that decomposes into bases of each of the components $e_\gamma Z(E^*)^d$.

Lemma 2.3.1. *The following is a k-basis of $Z(E^*)^d$:*

$$e_\lambda \phi_1 \qquad \text{for } \lambda \in \widehat{T^0/T^1},$$

$$e_1\phi_{s_0}, \qquad e_1\phi_{s_1}, \qquad e_{\chi_0}\phi_{s_0}, \qquad e_{\chi_0}\phi_{s_1},$$

$$U_{\lambda,i} \coloneqq e_\lambda \phi_{(s_1s_0)^i} + e_{\lambda^{-1}}\phi_{(s_0s_1)^i}$$
$$\text{for } \lambda \in \widehat{T^0/T^1} \smallsetminus \{1\} \text{ and } i \in \mathbb{Z}_{\geqslant 1},$$

$$U_{1,i} \coloneqq e_1\phi_{(s_1s_0)^i} + e_1\phi_{(s_0s_1)^i} - e_1\phi_{s_1(s_0s_1)^i} - e_1\phi_{s_0(s_1s_0)^i}$$
$$\text{for } i \in \mathbb{Z}_{\geqslant 1}.$$

Moreover, defining $U_{\lambda,i}$ also for $i = 0$ (and for all $\lambda \in \widehat{T^0/T^1}$) in the same fashion as above, one still has that $U_{\lambda,i} \in Z(E^*)^d$.

Proof. This easily follows from Proposition 2.2.1 and Remark 2.2.2. The rest being clear, let us check, for all $i \in \mathbb{Z}_{\geqslant 1}$, the correspondence between the elements of the form

$$\phi_{\omega(s_0s_1)^i} + \phi_{\omega^{-1}(s_1s_0)^i} - e_1 \cdot \phi_{(s_0s_1)^is_0} - e_1 \cdot \phi_{(s_1s_0)^is_1} \qquad \text{for } \omega \in T^0/T^1$$

and the elements of the form

$$U_{\lambda,i} = \begin{cases} e_\lambda\phi_{(s_1s_0)^i} + e_{\lambda^{-1}}\phi_{(s_0s_1)^i} & \text{for } \lambda \in \widehat{T^0/T^1}, \\ e_1\phi_{(s_1s_0)^i} + e_1\phi_{(s_0s_1)^i} - e_1\phi_{s_1(s_0s_1)^i} - e_1\phi_{s_0(s_1s_0)^i} & \text{for } \lambda = 1. \end{cases}$$

For all $\lambda \in \widehat{T^0/T^1} \smallsetminus \{1\}$, one has

$$\sum_{\omega \in T^0/T^1} \lambda(\omega) \cdot \big(\phi_{\omega(s_0s_1)^i} + \phi_{\omega^{-1}(s_1s_0)^i} - e_1 \cdot \phi_{(s_0s_1)^is_0} - e_1 \cdot \phi_{(s_1s_0)^is_1}\big)$$
$$= -e_{\lambda^{-1}}\phi_{(s_0s_1)^i} - e_\lambda\phi_{(s_1s_0)^i},$$

where the terms $e_1 \cdot \phi_{(s_0s_1)^is_0}$ and $e_1 \cdot \phi_{(s_1s_0)^is_1}$ disappear because $\sum_{\omega \in T^0/T^1} \lambda(\omega) = 0$. On the other side, doing the same computation with $\lambda = 1$, we get:

$$\sum_{\omega \in T^0/T^1} \big(\phi_{\omega(s_0s_1)^i} + \phi_{\omega^{-1}(s_1s_0)^i} - e_1 \cdot \phi_{(s_0s_1)^is_0} - e_1 \cdot \phi_{(s_1s_0)^is_1}\big)$$
$$= -e_1\phi_{(s_0s_1)^i} - e_1\phi_{(s_1s_0)^i} + e_1 \cdot \phi_{(s_0s_1)^is_0} + e_1 \cdot \phi_{(s_1s_0)^is_1},$$

using also that $\sum_{\omega \in T^0/T^1} 1_k = -1_k$.

Vice-versa, using the orthogonality relation

$$\sum_{\lambda \in \widehat{T^0/T^1}} \lambda(\omega^{-1})\lambda(\vartheta) = \begin{cases} -1_k & \text{if } \omega = \vartheta \\ 0 & \text{if } \omega \neq \vartheta \end{cases} \qquad \text{for all } \omega, \vartheta \in T^0/T^1,$$

we see that for all $\omega \in T^0/T^1$, one has

$$\sum_{\lambda \in \widehat{T^0/T^1}} \lambda(\omega^{-1})e_\lambda = -\sum_{\lambda \in \widehat{T^0/T^1}} \sum_{\vartheta \in T^0/T^1} \lambda(\omega^{-1})\lambda(\vartheta)\tau_{\vartheta^{-1}}$$
$$= \tau_{\omega^{-1}},$$

and so

$$\sum_{\lambda \in \widehat{T^0/T^1}} \lambda(\omega)U_{\lambda,i} = \sum_{\lambda \in \widehat{T^0/T^1}} \lambda(\omega)\big(e_\lambda\phi_{(s_1s_0)^i} + e_{\lambda^{-1}}\phi_{(s_0s_1)^i}\big)$$
$$- e_1\phi_{s_1(s_0s_1)^i} - e_1\phi_{s_0(s_1s_0)^i}$$
$$= -\phi_{\omega^{-1}(s_1s_0)^i} - \phi_{\omega(s_0s_1)^i} - e_1\phi_{s_1(s_0s_1)^i} - e_1\phi_{s_0(s_1s_0)^i}. \qquad \blacksquare$$

Returning to the decomposition

$$Z(E^*)^d = \bigoplus_{\gamma \in \Gamma} e_\gamma Z(E^*)^d,$$

we get the following description of the component $e_\gamma Z(E^*)^d$ for $\gamma \in \Gamma$:

- If $\gamma = \{\lambda\}$ (in which case $\lambda = 1$ or $\lambda = \chi_0$), then the following is a k-basis of $e_\gamma Z(E^*)^d$:

$$e_\lambda \phi_1, \qquad e_\lambda \phi_{s_0}, \qquad e_\lambda \phi_{s_1}, \qquad U_{\lambda,i} \quad (\text{for } i \in \mathbb{Z}_{\geqslant 1}). \tag{99}$$

- If $\gamma = \{\lambda, \lambda^{-1}\}$ with $\lambda \neq \lambda^{-1}$, then the following is a k-basis of $e_\gamma Z(E^*)^d$:

$$e_\lambda \phi_1, \qquad e_{\lambda^{-1}} \phi_1, \qquad U_{\lambda,i} \quad (\text{for } i \in \mathbb{Z}_{\geqslant 1}), \qquad U_{\lambda^{-1},i} \quad (\text{for } i \in \mathbb{Z}_{\geqslant 1}). \tag{100}$$

2.3.b The components $e_\gamma Z(E^*)^d$

We are now going to describe the components $e_\gamma Z(E^*)^d$ for $\gamma \in \Gamma$, and more precisely we will determine their $e_\gamma Z(E^0)$-module structure. We will do this in three lemmas, which will deal respectively with the components $e_1 Z(E^*)^d$, $e_{\chi_0} Z(E^*)^d$ and $e_\gamma Z(E^*)^d$ for γ such that $\#\gamma = 2$.

Lemma 2.3.2. *Identifying $e_1 Z(E^0)$ with the polynomial ring $k[X_1]$ as in* (98)*, one has the following isomorphism of $k[X_1]$-modules:*

$$\begin{aligned}
\frac{k[X_1]}{(X_1 - 1)} \oplus \frac{k[X_1]}{(X_1)} \oplus \frac{k[X_1, X_1^{-1}]}{k[X_1]} &\xrightarrow{\quad\cong\quad} e_1 Z(E^*)^d \\
(\overline{1}, 0, 0) &\longmapsto e_1 \phi_1, \\
(0, \overline{1}, 0) &\longmapsto e_1 \phi_{s_0} - e_1 \phi_{s_1}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(0, 0, \overline{X_1^{-i}}\right)} &\longmapsto U_{1,i-1}.
\end{aligned}$$

Moreover, the direct summand $\frac{k[X_1, X_1^{-1}]}{k[X_1]}$ is the injective hull of $k = \frac{k[X_1]}{(X_1)}$ as a $k[X_1]$-module.

Proof. The fact that $\frac{k[X_1, X_1^{-1}]}{k[X_1]}$ is the injective hull of $k = \frac{k[X_1]}{(X_1)}$ as a $k[X_1]$-module is shown in [Lam12, Proposition 3.91.(1)].

We have seen in (99) that the following is a k-basis of $e_1 Z(E^*)^d$:

$$e_1 \phi_1, \qquad e_1 \phi_{s_0}, \qquad e_1 \phi_{s_1}, \qquad U_{1,i} \quad (\text{for } i \in \mathbb{Z}_{\geqslant 1}). \tag{101}$$

Recall also that we introduced the notation $U_{1,0}$, although this is not an element of such basis. For such element, we have

$$U_{1,0} = 2 e_1 \phi_1 - e_1 \phi_{s_0} - e_1 \phi_{s_1}.$$

With these facts, we see that the map in the lemma is an isomorphism of k-vector spaces, and it remains to check that it preserves the action of X_1.

We claim that one has the following formulas for the action of $e_1 Z(E^0)$ on the above k-basis of $e_1 Z(E^*)^d$:

$$\begin{aligned}
x_1 \cdot e_1\phi_1 &= e_1\phi_1, \\
x_1 \cdot e_1\phi_{s_0} &= e_1\phi_1, \\
x_1 \cdot e_1\phi_{s_1} &= e_1\phi_1, \\
x_1 \cdot U_{1,i} &= U_{1,i-1} && \text{for all } i \in \mathbb{Z}_{\geqslant 1}.
\end{aligned}$$

Once the formulas are proved, we are done, because it is then easy to check that the action of X_1 is preserved by the isomorphism in the statement of the lemma. The proof of the formulas is a quick computation; we spell out some details, starting with the first two. We make repeated use of the formulas for the left action of E^0 on E^d stated in (89):

$$\begin{aligned}
x_1 \cdot e_1\phi_1 &= e_1\left(\tau_{s_1}\tau_{s_0} + \tau_{s_0}\tau_{s_1} + \tau_{s_0} + \tau_{s_1} + 1\right)\phi_1 \\
&= e_1\phi_1, \\
x_1 \cdot e_1\phi_{s_0} &= e_1\left(\tau_{s_0}\tau_{s_1} + (\tau_{s_1} + e_1)(\tau_{s_0} + e_1)\right)\phi_{s_0} \\
&= 0 + e_1(\tau_{s_1} + e_1)\phi_{c_{-1}} \\
&= e_1\phi_{c_{-1}} \\
&= e_1\phi_1.
\end{aligned}$$

The third formula we have to prove is identical to the second one, and regarding the last one, we have

$$x_1 \cdot U_{1,i} = x_1 \cdot e_1\phi_{(s_1s_0)^i} + x_1 \cdot e_1\phi_{(s_0s_1)^i} - x_1 \cdot e_1\phi_{s_1(s_0s_1)^i} - x_1 \cdot e_1\phi_{s_0(s_1s_0)^i},$$

and to finish the computation it suffices to compute that $x_1 \cdot \phi_{s_1s_0w} = \phi_w$ for all $w \in \widetilde{W}$ such that $\ell(s_0w) = \ell(w) + 1$, and similarly for $x_1 \cdot \phi_{s_0s_1w}$ if w is such that $\ell(s_1w) = \ell(w) + 1$. ■

Lemma 2.3.3. *Identifying $e_{\chi_0}Z(E^0)$ with the polynomial ring $k[X_{\chi_0}]$ as in* (98)*, one has the following isomorphism of $k[X_{\chi_0}]$-modules:*

$$\begin{aligned}
\frac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \frac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \frac{k[X_{\chi_0}, X_{\chi_0}^{-1}]}{k[X_{\chi_0}]} &\xrightarrow{\ \cong\ } e_{\chi_0}Z(E^*)^d \\
(\overline{1}, 0, 0) &\longmapsto e_{\chi_0}\phi_{s_0}, \\
(0, \overline{1}, 0) &\longmapsto e_{\chi_0}\phi_{s_1}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(0, 0, \overline{X_{\chi_0}^{-i}}\right)} &\longmapsto U_{\chi_0, i-1}.
\end{aligned}$$

Proof. Recall from (99) that we have fixed the following k-basis of $e_{\chi_0}Z(E^0)$:

$$e_{\chi_0}\phi_1, \qquad e_{\chi_0}\phi_{s_0}, \qquad e_{\chi_0}\phi_{s_1}, \qquad U_{\chi_0,i} \quad (\text{for } i \in \mathbb{Z}_{\geqslant 1}), \tag{102}$$

and that we have

$$U_{\chi_0,0} = 2e_{\chi_0}\phi_1.$$

Similarly to the proof of the previous lemma, using the formulas for the left action of E^0 on E^d stated in (89) one checks the following formulas for the action of $e_{\chi_0}Z(E^0)$ on the above k-basis of $e_{\chi_0}Z(E^*)^d$:

$$\begin{aligned} x_{\chi_0} \cdot e_{\chi_0}\phi_1 &= 0, \\ x_{\chi_0} \cdot e_{\chi_0}\phi_{s_0} &= 0, \\ x_{\chi_0} \cdot e_{\chi_0}\phi_{s_1} &= 0, \\ x_{\chi_0} \cdot U_{\chi_0,i} &= U_{\chi_0,i-1} && \text{for all } i \in \mathbb{Z}_{\geqslant 1}. \end{aligned}$$

From these formulas, it is clear that one has the isomorphism in the statement of the lemma.

The statement about the injective hull has already been recalled from [Lam12, Proposition 3.91.(1)] in the proof of the last lemma. ■

To describe the component $e_\gamma Z(E^*)^d$ for $\gamma \in \Gamma$ such that $\#\gamma = 2$, we need to set up some notation. Let X and Y be indeterminates, and let us consider the k-vector space

$$\begin{aligned} \mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k) &:= \left\{ \Theta \in \mathrm{Hom}_k(k[X,Y],k) \;\middle|\; \begin{array}{l} \Theta\left((X\cdot Y) + (X,Y)^n\right) = 0 \\ \text{for some } n \in \mathbb{Z}_{\geqslant 0} \end{array} \right\} \\ &= \left\{ \Theta \in \mathrm{Hom}_k(k[X,Y],k) \;\middle|\; \begin{array}{l} \Theta\left((X\cdot Y, X^n, Y^n)\right) = 0 \\ \text{for some } n \in \mathbb{Z}_{\geqslant 0} \end{array} \right\} \\ &= \varinjlim_{n \in \mathbb{Z}_{\geqslant 0}} \mathrm{Hom}_k\left(\tfrac{k[X,Y]}{(X\cdot Y, X^n, Y^n)}, k \right), \end{aligned}$$

where $\mathrm{Hom}_k(\_,\_)$ means homomorphisms of k-vector spaces. The k-vector space $\mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k)$ has a natural structure of $\frac{k[X,Y]}{(X\cdot Y)}$-module, and it is proved in [Lam12, Theorem 3.90.(1)] that $\mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k)$ is the injective hull of the $\frac{k[X,Y]}{(X\cdot Y)}$-module $\frac{k[X,Y]}{(X,Y)}$ (which we will simply denote by k), where we view k as a submodule of $\mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k)$ by identifying $1 \in k$ with the element $(1)^\vee \in \mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k)$ that has value 1 at 1 and that is 0 on (X,Y).

It is easy to see that the following is a k-basis of $\mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k)$:

$$\begin{aligned} (1)^\vee \colon \; k[X,Y] &\longrightarrow k \\ 1 &\longmapsto 1 \\ \text{other monomials} &\longmapsto 0, \\[1ex] (X^i)^\vee \colon \; k[X,Y] &\longrightarrow k \\ X^i &\longmapsto 1 \qquad \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ \text{other monomials} &\longmapsto 0 \\[1ex] (Y^i)^\vee \colon \; k[X,Y] &\longrightarrow k \\ Y^i &\longmapsto 1 \qquad \text{for } i \in \mathbb{Z}_{\geqslant 1}. \\ \text{other monomials} &\longmapsto 0 \end{aligned} \tag{103}$$

It is also easy to check formulas, which describe the action of $k[X,Y]$ on $\mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k)$:

$$\begin{aligned} X\cdot(1)^\vee &= 0, \\ Y\cdot(1)^\vee &= 0, \\ X\cdot(X^i)^\vee &= (X^{i-1})^\vee \quad \text{for } i\in\mathbb{Z}_{\geqslant 1}, \\ Y\cdot(X^i)^\vee &= 0 \qquad\qquad\ \ \text{for } i\in\mathbb{Z}_{\geqslant 1}, \\ X\cdot(Y^i)^\vee &= 0 \qquad\qquad\ \ \text{for } i\in\mathbb{Z}_{\geqslant 1}, \\ Y\cdot(Y^i)^\vee &= (Y^{i-1})^\vee \quad \text{for } i\in\mathbb{Z}_{\geqslant 1}. \end{aligned} \tag{104}$$

Lemma 2.3.4. *Let $\gamma\in\Gamma$ with $\#\gamma = 2$ and let us write it as $\{\lambda,\lambda^{-1}\}$. Furthermore, let us identify $e_\gamma Z(E^0)$ with the ring $\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda\cdot X_{\lambda^{-1}})}$ as in (98). Let us see k as a $\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda\cdot X_{\lambda^{-1}})}$-module by identifying it with $\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda,X_{\lambda^{-1}})}$, and let $\mathcal{E}_{\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda\cdot X_{\lambda^{-1}})}}(k)$ be defined as above.*

One has the following isomorphism of $k[X_\lambda,X_{\lambda^{-1}}]/(X_\lambda\cdot X_{\lambda^{-1}})$-modules:

$$\begin{aligned} k\oplus\mathcal{E}_{\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda\cdot X_{\lambda^{-1}})}}(k) &\xrightarrow{\ \cong\ } e_\gamma Z(E^*)^d \\ (1,0) &\longmapsto e_\lambda\phi_1 - e_{\lambda^{-1}}\phi_1, \\ \underset{(\text{for } i\in\mathbb{Z}_{\geqslant 1})}{\big(0,(X_\lambda^i)^\vee\big)} &\longmapsto U_{\lambda,i}, \\ \underset{(\text{for } i\in\mathbb{Z}_{\geqslant 1})}{\big(0,(X_{\lambda^{-1}}^i)^\vee\big)} &\longmapsto U_{\lambda^{-1},i}, \\ \big(0,(1)^\vee\big) &\longmapsto U_{\lambda,0} = U_{\lambda^{-1},0}. \end{aligned}$$

Furthermore, $\mathcal{E}_{\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda\cdot X_{\lambda^{-1}})}}(k)$ is the injective hull of k as a $\frac{k[X_\lambda,X_{\lambda^{-1}}]}{(X_\lambda\cdot X_{\lambda^{-1}})}$-module.

Proof. The statement about the injective hull has already been recalled from [Lam12, Theorem 3.90.(1)]. Let us check that we have an isomorphism as claimed. The fact that we do have a well defined isomorphism of k-vector spaces is clear: indeed we know a specific k-basis on the left hand side from (103), we know a specific basis on the right hand side from (100), namely

$$e_\lambda\phi_1, \qquad e_{\lambda^{-1}}\phi_1, \qquad U_{\lambda,i}\quad(\text{for } i\in\mathbb{Z}_{\geqslant 1}), \qquad U_{\lambda^{-1},i}\quad(\text{for } i\in\mathbb{Z}_{\geqslant 1}),$$

and it is immediate to see that

$$U_{\lambda,0} = U_{\lambda^{-1},0} = e_\lambda\phi_1 + e_{\lambda^{-1}}\phi_1.$$

So, we have an isomorphism of k-vector spaces and it remains to check that it preserves the actions of X_λ and $X_{\lambda^{-1}}$. Similarly to the proof of the Lemmas 2.3.2 and 2.3.3, using the formulas for the left action of E^0 on E^d stated in (89) one checks the following formulas for the action of $e_\gamma Z(E^0)$ on $e_\gamma Z(E^*)^d$:

$$\begin{aligned} x_\lambda\cdot e_\lambda\phi_1 &= 0, & x_{\lambda^{-1}}\cdot e_\lambda\phi_1 &= 0, & & \\ x_\lambda\cdot e_{\lambda^{-1}}\phi_1 &= 0, & x_{\lambda^{-1}}\cdot e_{\lambda^{-1}}\phi_1 &= 0, & & \\ x_\lambda\cdot U_{\lambda,i} &= U_{\lambda,i-1}, & x_{\lambda^{-1}}\cdot U_{\lambda,i} &= 0 & &\text{for all } i\in\mathbb{Z}_{\geqslant 1}, \\ x_\lambda\cdot U_{\lambda^{-1},i} &= 0, & x_{\lambda^{-1}}\cdot U_{\lambda^{-1},i} &= U_{\lambda^{-1},i-1} & &\text{for all } i\in\mathbb{Z}_{\geqslant 1}. \end{aligned}$$

Comparing these formulas with formulas (104), it is easy to see our isomorphism does preserve the actions of X_λ and $X_{\lambda^{-1}}$. ∎

2.3.c Final description of the structure of $Z(E^*)^d$ as a $Z(E^0)$-module

In the previous subsection we have described the $e_\gamma Z(E^0)$-module structure of $e_\gamma Z(E^*)^d$ for $\gamma \in \Gamma$. In this subsection we will deduce from this the $Z(E^0)$-module structure of $Z(E^*)^d$. We start with a completely general and elementary lemma about injective hulls.

Lemma 2.3.5. *Let $R_1, \ldots, R_n$ be commutative rings with unit. Let M_i be an R_i module for all $i \in \{1, \ldots, n\}$. One has*

$$\mathcal{E}_{\prod_{i=1}^n R_i}\left(\bigoplus_{i=1}^n M_i\right) \cong \bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i),$$

where the notation $\mathcal{E}_{(\_)}(\_)$ denotes "the" injective hull.

Proof. For all $i \in \{1, \ldots, n\}$ let us set

$$e_i \coloneqq (0, \ldots, 0, \underset{i}{\underset{\sqcup}{1}}, 0, \ldots, 0) \in \prod_{i=1}^n R_i.$$

One of the characterizations/definitions of being an injective hull is being injective and an essential extension. Therefore, we have to prove that $\bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i)$ is an injective $\prod_{i=1}^n R_i$-module and that it is an essential extension of $\bigoplus_{i=1}^n M_i$. As regards the first claim, let us consider a diagram of the form

$$\begin{tikzcd} N \arrow[r, hook, "\delta"] \arrow[d, "\varphi"'] & L \arrow[dl, dashed, "\exists ? \widetilde{\varphi}"] \\ \bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i). & \end{tikzcd}$$

Since the e_i's are orthogonal idempotents whose sum is 1, it is easy to see that we have the following decompositions:

$$\begin{tikzcd} \bigoplus_{i=1}^n e_i N \arrow[r, hook, "\delta = \bigoplus_{i=1}^n \delta\big|_{e_i N}"] \arrow[d, "\varphi = \bigoplus_{i=1}^n \varphi\big|_{e_i N}"'] & \bigoplus_{i=1}^n e_i L \arrow[dl, dashed, "\exists ? \widetilde{\varphi}"] \\ \bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i). & \end{tikzcd}$$

Now, since $\mathcal{E}_{R_i}(M_i)$ is an injective R_i-module for all i, we can construct $\widetilde{\varphi}$ componentwise.

It remains to prove that $\bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i)$ is an essential extension of $\bigoplus_{i=1}^n M_i$. Let $N \subseteq \bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i)$ be a nonzero submodule. Since $N = \bigoplus_{i=1}^n e_i N$, there must exist i_0 such that $e_{i_0} N \neq 0$. Since $e_{i_0} \cdot \left(\bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i)\right) = \mathcal{E}_{R_{i_0}}(M_{i_0})$, we have that $e_{i_0} N$ is a nonzero R_{i_0}-submodule of $\mathcal{E}_{R_{i_0}}(M_{i_0})$, hence it intersects M_{i_0} non-trivially. Therefore

$$N \cap \left(\bigoplus_{i=1}^n M_i\right) \supseteq e_{i_0} N \cap M_{i_0} \neq 0,$$

and this concludes the proof that $\bigoplus_{i=1}^n \mathcal{E}_{R_i}(M_i)$ is an essential extension of $\bigoplus_{i=1}^n M_i$. ∎

Let $\gamma \in \Gamma$, and let k_{e_γ} be the k-vector space k endowed with the unique structure of $Z(E^0)$-module such that e_γ acts by 1, $e_{\gamma'}$ acts by 0 for all $\gamma' \in \Gamma \smallsetminus \{\gamma\}$, and x_λ acts by 0 for all $\lambda \in \gamma$ (equivalently, for all $\lambda \in \widehat{T^0/T^1}$); as usual, the notation x_λ is as in Lemma 1.7.1. Concretely, this module can be obtained for example as $e_\gamma Z(E^0)/(x_\lambda, x_\lambda^{-1})$, where $\{\lambda, \lambda^{-1}\} = \gamma$. To ease notation, in the case $\gamma = \{\lambda\}$ we simply write k_{e_λ} instead of $k_{e_{\{\lambda\}}}$.

Moreover, let $k_{e_1,\chi_{\mathrm{triv}}}$ be the k-vector space k endowed with the unique structure of $Z(E^0)$-module such that e_1 acts by 1, $e_{\gamma'}$ acts by 0 for all $\gamma' \in \Gamma \smallsetminus \{1\}$, and x_1 acts by 1 (equivalently, ζ acts by 1). Concretely, this module can be obtained for example as $e_1 Z(E^0)/(e_1 Z(E^0) \cap F^1 E^0)$. Equivalently, the action of $Z(E^0)$ on $k_{e_1,\chi_{\mathrm{triv}}}$ is through $\chi_{\mathrm{triv}} \colon E^0 \longrightarrow k$ (see (91)).

Proposition 2.3.6. *There is a decomposition of $Z(E^0)$-modules*

$$Z(E^*)^d = ke_1\phi_1 \oplus N \oplus \mathcal{E},$$

where, with notation as above,

(i) $ke_1\phi_1$ is isomorphic to $k_{e_1,\chi_{\mathrm{triv}}}$;

(ii) N is a finite direct sum of submodules of dimension 1 over k, and more precisely,

$$N \cong k_{e_1} \oplus k_{e_{\chi_0}} \oplus k_{e_{\chi_0}} \oplus \bigoplus_{\substack{\gamma \in \Gamma \\ \text{with } \#\gamma = 2}} k_{e_\gamma};$$

(iii) $\mathcal{E}$ is the injective hull of all the following $Z(E^0)$-modules:

- $\star$ $\bigoplus_{\gamma \in \Gamma} k_{e_\gamma}$,
- $\star$ $\big(Z(E^0)/\zeta Z(E^0)\big)^\vee$,
- $\star$ $Z(E^0)/\zeta Z(E^0)$,

and moreover the last two $Z(E^0)$-modules are isomorphic.

Finally, this decomposition is compatible with the decomposition

$$E^d = ke_1\phi_1 \oplus \ker(\mathcal{S}^d)$$

of Proposition 1.10.5, in the sense that $N \oplus \mathcal{E}$ is contained in $\ker(\mathcal{S}^d)$.

Proof. Referring to Lemmas 2.3.2, 2.3.3 and 2.3.4, we define N to be the sub-$Z(E^0)$-module generated by the elements

$$\begin{aligned} & e_1\phi_{s_0} - e_1\phi_{s_1}, \\ & e_{\chi_0}\phi_{s_0}, \\ & e_{\chi_0}\phi_{s_1}, \\ & e_\lambda\phi_1 - e_{\lambda^{-1}}\phi_1 && \text{for } \lambda \in \widehat{T^0/T^1} \smallsetminus \{1, \chi_0\} \end{aligned}$$

(generated as a submodule or as a k-vector space). Furthermore, let us define $\mathcal{E}$ as the sub-$Z(E^0)$-module generated by the elements

$$U_{\lambda,i} \qquad \text{for } \lambda \in \widehat{T^0/T^1} \text{ and } i \in \mathbb{Z}_{\geqslant 0}$$

(again, generated as a submodule or as a k-vector space).

Parts (i) and (ii) of the statement are clear from the three lemmas. It remains to show (iii) and compatibility with the decomposition $E^d = ke_1\phi_1 \oplus \ker(\mathcal{S}^d)$.

Regarding the compatibility with the decomposition $E^d = ke_1\phi_1 \oplus \ker(\mathcal{S}^d)$, we have to show that $N \oplus \mathcal{E} \subseteq \ker(\mathcal{S}_d)$. Let us consider the e_γ-component of both sides for $\gamma \in \Gamma \smallsetminus \{1\}$: we certainly have $e_\gamma \cdot (N \oplus \mathcal{E}) \subseteq e_\gamma \ker(\mathcal{S}_d)$, because from the decomposition $E^d = ke_1\phi_1 \oplus \ker(\mathcal{S}^d)$ we see that $e_\gamma \ker(\mathcal{S}_d)$ is the full $e_\gamma E^d$. It remains to show that $e_1 \cdot (N \oplus \mathcal{E}) \subseteq \ker(\mathcal{S}_d)$, i.e., that $e_1\phi_{s_0} - e_1\phi_{s_1} \in \ker(\mathcal{S}_d)$ and that $U_{1,i} \in \ker(\mathcal{S}_d)$ for all $i \in \mathbb{Z}_{\geqslant 0}$. All these elements are of the form

$$\sum_{w \in X} \phi_w - \sum_{w \in Y} \phi_w$$

for suitable finite subsets $X, Y \subseteq \widetilde{W}$ having the same cardinality. Then the result follows because $(\eta \circ \mathcal{S}^d)(\phi_w) = 1$ for all $w \in \widetilde{W}$ (see (40)).

The fact that $\mathcal{E}$ is the injective hull of $\bigoplus_{\gamma \in \Gamma} k_{e_\gamma}$ as a $Z(E^0)$-module is clear from the three lemmas together with Lemma 2.3.5. It remains to prove that it is also the injective hull of $\big(Z(E^0)/\zeta Z(E^0)\big)^\vee$ and/or of $Z(E^0)/\zeta Z(E^0)$ and that these two $Z(E^0)$-modules are isomorphic. We are going to do this component-wise, and we start by studying the components of $Z(E^0)/\zeta Z(E^0)$.

The decomposition $Z(E^0) = \prod_{\gamma \in \Gamma} e_\gamma Z(E^0)$ induces a decomposition

$$Z(E^0)/\zeta Z(E^0) = \prod_{\gamma \in \Gamma} e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0).$$

Let $\gamma \in \Gamma$: we distinguish two cases on the basis of the cardinality of γ.

- Assume that $\gamma = \{\lambda\}$ (for $\lambda = 1$ or $\lambda = \chi_0$).

  Recall that in this case $e_\gamma Z(E^0)$ is isomorphic to the polynomial ring $k[X_\lambda]$, an explicit isomorphism being given by sending X_λ to $x_\lambda = e_\lambda \zeta = e_\gamma \zeta$. Therefore, via this identification, we find that

  $$e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0) \cong k[X_\lambda]/(X_\lambda) = k.$$

  In particular, we see that the k-dual of $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ is isomorphic to $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ itself as a $e_\gamma Z(E^0)$-module.

- Assume that $\gamma = \{\lambda, \lambda^{-1}\}$ with $\lambda \neq \lambda^{-1}$.

  Recall that in this case $e_\gamma Z(E^0)$ is isomorphic to the ring $\frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}})}$, an explicit isomorphism being given by sending X_λ to x_λ and $X_{\lambda^{-1}}$ to $x_{\lambda^{-1}}$. Since $e_\gamma \zeta = x_\lambda + x_{\lambda^{-1}}$, we deduce that, under this identification we have

  $$e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0) \cong \frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}}, X_\lambda + X_{\lambda^{-1}})}.$$

  This quotient has dimension 2 as a k-vector space, and we fix the following generators:

  $$\begin{aligned} u &:= \overline{1}, \\ v &:= \overline{X_\lambda} = -\overline{X_{\lambda^{-1}}}. \end{aligned}$$

  We have the formulas

  $$\begin{aligned} X_\lambda \cdot u &= v, \quad X_{\lambda^{-1}} \cdot u = -v, \\ X_\lambda \cdot v &= 0, \quad X_{\lambda^{-1}} \cdot v = 0, \end{aligned} \tag{105}$$

and of course $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ can be characterized as the unique $k[X_\lambda, X_{\lambda^{-1}}]$-module of dimension 2 over k with generators u and v satisfying the above formulas.

The k-dual of $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ is isomorphic to $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ itself as a $e_\gamma Z(E^0)$-module. To check this, we have to show that $\frac{k[X,Y]}{(X \cdot Y, X+Y)}$ is isomorphic to its k-dual as a $k[X,Y]$-module, or, equivalently, as a $\frac{k[X,Y]}{(X \cdot Y, X+Y)}$-module (here we are using indeterminates X and Y instead of X_λ and $X_{\lambda^{-1}}$ in order to simplify notation). Now,

$$\frac{k[X,Y]}{(X \cdot Y, X+Y)} \cong k[X]/(X^2),$$

and $k[X]/(X^2)$ is isomorphic to its k-dual as a $k[X]/(X^2)$-module (this can be seen directly but is also a known fact about Frobenius algebras). Therefore, $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ is isomorphic to its k-dual as a $e_\gamma Z(E^0)$-module.

So far, we have described explicitly the components $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ for $\gamma \in \Gamma$ and we have also shown that $Z(E^0)/\zeta Z(E^0)$ is isomorphic to its k-dual as a $Z(E^0)$-module (indeed it is easy to see that this can be checked component-wise, and we have shown this).

It remains to prove that $e_\gamma N$ is the injective hull of $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ as a $e_\gamma Z(E^0)$-module for all $\gamma \in \Gamma$, and then we are done by Lemma 2.3.5. Again, we distinguish two cases depending on the cardinality of γ.

- Assume that $\gamma = \{\lambda\}$ (for $\lambda = 1$ or $\lambda = \chi_0$).

  We know that the factor $\frac{k[X_\lambda, X_\lambda^{-1}]}{k[X_\lambda]}$ appearing in the decomposition of $e_\gamma Z(E^*)^d$ of Lemma 2.3.2 (for $\lambda = 1$) and of Lemma 2.3.3 (for $\lambda = \chi_0$) is the injective hull of

  $$k = k[X_\lambda]/(X_\lambda) \cong e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0).$$

- Assume that $\gamma = \{\lambda, \lambda^{-1}\}$ with $\lambda \neq \lambda^{-1}$.

  We know that the factor $\mathcal{E}_{\frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}})}}(k)$ in the decomposition of $e_\gamma Z(E^*)^d$ of Lemma 2.3.2 is the injective hull of k as a $\frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}})}$-module. We have instead to show that $\mathcal{E}_{\frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}})}}(k)$ is the injective hull of another module.

  Again, let us rename the indeterminates X and Y to improve readability. We showed that $\mathcal{E}_{\frac{k[X,Y]}{(X \cdot Y)}}(k)$ admits the following k-basis (see (103))

  $$\begin{aligned} &(1)^\vee, && \\ &(X^i)^\vee && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ &(Y^i)^\vee && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \end{aligned}$$

  basis which satisfies the following formulas (see (104)):

  $$\begin{aligned} X \cdot (1)^\vee &= 0, && \\ Y \cdot (1)^\vee &= 0, && \\ X \cdot (X^i)^\vee &= (X^{i-1})^\vee && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ Y \cdot (X^i)^\vee &= 0 && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ X \cdot (Y^i)^\vee &= 0 && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ Y \cdot (Y^i)^\vee &= (Y^{i-1})^\vee && \text{for } i \in \mathbb{Z}_{\geqslant 1}. \end{aligned}$$

Let us define

$$u' \coloneqq (X)^\vee - (Y)^\vee,$$
$$v' \coloneqq (1)^\vee,$$
$$M \coloneqq \operatorname{span}_k\{v', u'\} \subseteq \mathcal{E}_{\frac{k[X_\lambda, X_{\lambda-1}]}{(X_\lambda \cdot X_{\lambda-1})}}(k).$$

It is easy to see that M is a sub-$k[X,Y]$-module and that we have the inclusions of $k[X,Y]$-modules

$$k \cong k \cdot (1)^\vee \hookrightarrow M \hookrightarrow \mathcal{E}_{\frac{k[X,Y]}{(X \cdot Y)}}(k),$$

whose composite is the inclusion of k in $\mathcal{E}_{\frac{k[X,Y]}{(X \cdot Y)}}(k)$. We know that the module on the right is the injective hull of the module on the left, and so it is also the injective hull of the module in the middle.

But it is easy to see that

$$X \cdot u' = v', \qquad Y \cdot u' = -v',$$
$$X \cdot v' = 0, \qquad Y \cdot v' = 0,$$

and these formulas are the same as (105), with obvious change of notation. Therefore we can conclude that M is isomorphic to $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ as a module over $e_\gamma Z(E^0) \cong k[X_\lambda, X_{\lambda-1}]$, because we said that $e_\gamma Z(E^0)/e_\gamma \zeta Z(E^0)$ can be characterized as the unique $k[X_\lambda, X_{\lambda-1}]$-module of dimension 2 over k with generators u and v satisfying (105). ■

2.4 The 0^{th} graded piece of the centre

Assumptions. We assume that $G = \mathrm{SL}_2(\mathfrak{F})$ with $p \neq 2$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5).

Under the above assumptions, we are going to describe the 0^{th} graded piece of the centre of E^*. The hypothesis $p \neq 2$ makes available the description of the Frattini quotient stated in Lemma 1.10.1 (and such hypothesis will also be used many times in the computations). However, when we will treat the case of a general group G in Section 3.1, we will see that also in the case $p = 2$ the description would be similar (the centre is trivial in that case).

Recall the definition

$$c_{-1} \coloneqq \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} T^1 \in \widetilde{W}.$$

Proposition 2.4.1. *One has*

$$Z(E^*)^0 = k\tau_1 + k\tau_{c_{-1}}.$$

Therefore, as a k-algebra, $Z(E^*)^0$ can be described as

$$\begin{aligned} k[X]/(X^2-1) &\xrightarrow{\cong} Z(E^*)^0 \\ \overline{X} &\longmapsto \tau_{c_{-1}} \end{aligned}$$

or as

$$\begin{aligned} k \times k &\xrightarrow{\cong} Z(E^*)^0 \\ (1,0) &\longmapsto \frac{1}{2}\left(\tau_1 + \tau_{c_{-1}}\right) \\ (0,1) &\longmapsto \frac{1}{2}\left(\tau_1 - \tau_{c_{-1}}\right). \end{aligned}$$

Proof. Let us check the two inclusions in the claimed equality $Z(E^*)^0 = k\tau_1 + k\tau_{c_{-1}}$.

"$\supseteq$") Let us prove the inclusion $Z(E^*)^0 \supseteq k\tau_1 + k\tau_{c_{-1}}$.

It suffices to show that, for all $i \in \mathbb{Z}_{\geqslant 1}$, all $w \in \widetilde{W}$ and all $\beta \in H^i(I, \mathbf{X}(w))$, one has $\beta \cdot \tau_{c_{-1}} = \tau_{c_{-1}} \cdot \beta$.

Since lengths add up, we can apply the formulas of Corollary 1.9.5, obtaining

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

But $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ lies in the centre of G, and so $wc_{-1} = c_{-1}w$ and every conjugation by c_{-1} appearing in the above formulas is trivial. Hence,

$$\begin{aligned} &\beta \cdot \tau_{c_{-1}} \in H^i(I, \mathbf{X}(wc_{-1})) &&\text{and} &&\mathrm{Sh}_{wc_{-1}}(\beta \cdot \tau_{c_{-1}}) = \mathrm{Sh}_w(\beta), \\ &\tau_{c_{-1}} \cdot \beta \in H^i(I, \mathbf{X}(wc_{-1})) &&\text{and} &&\mathrm{Sh}_{wc_{-1}}(\tau_{c_{-1}} \cdot \beta) = \mathrm{Sh}_w(\beta). \end{aligned}$$

In other words, $\beta \cdot \tau_{c_{-1}} = \tau_{c_{-1}} \cdot \beta$, as we wanted to show.

"$\subseteq$") Let us prove the inclusion $Z(E^*)^0 \subseteq k\tau_1 + k\tau_{c_{-1}}$.

Let us define $\Xi \coloneqq \big\{\{\omega, \omega^{-1}\} \;\big|\; \omega \in \big(T^0/T^1\big) \smallsetminus \{1, c_{-1}\}\big\}$ and let us fix a choice function

$$\begin{aligned} \Xi &\longrightarrow \big(T^0/T^1\big) \smallsetminus \{1, c_{-1}\} \\ \xi &\longmapsto \omega_\xi \in \xi. \end{aligned}$$

Recall from (27) that following is a k-basis of $Z(E^0)$:

$$\begin{aligned} &\tau_1, \\ &\tau_{c_{-1}}, \\ &\tau_{\omega_\xi} + \tau_{\omega_\xi^{-1}}, && \text{for } \xi \in \Xi, \\ &\zeta_{i,\omega} \coloneqq \tau_\omega(\tau_{s_0}\tau_{s_1})^i + \tau_{\omega^{-1}}\big((\tau_{s_1} + e_1)(\tau_{s_0} + e_1)\big)^i && \text{for } i \in \mathbb{Z}_{\geqslant 1} \text{ and } \omega \in T^0/T^1. \end{aligned}$$

Now let $x \in Z(E^*)^0 \subseteq Z(E^0)$ and let us write it with respect to the above basis as

$$x = a\tau_1 + b\tau_{c_{-1}} + \sum_{\xi \in \Xi} c_\xi \cdot \left(\tau_{\omega_\xi} + \tau_{\omega_\xi^{-1}}\right) + \sum_{\substack{i \in \{1, \dots, n\}, \\ \omega \in T^0/T^1}} d_{i,\omega}\zeta_{i,\omega},$$

for suitable $n \in \mathbb{Z}_{\geqslant 1}$ and $a, b, c_\xi, d_{i,\omega} \in k$. We have to show that $c_\xi = 0$ for all $\xi \in \Xi$ and that $d_{i,\omega} = 0$ for all $i \in \{1, \dots, n\}$ and all $\omega \in T^0/T^1$. Since we already know that $\tau_1, \tau_{c_{-1}} \in Z(E^*)$, we can assume without loss of generality that $a = 0$ and $b = 0$.

Let us consider an element $c^- \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$, which we will later choose according to our needs, and let us define

$$\gamma_{c^-} := (c^-, 0, 0)_1.$$

For $L \in \mathbb{Z}_{\geqslant 0}$ and $y \in E^*$ we say that x is supported in length less or equal than L if $y \in \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \leqslant L}} H^*(I, \mathbf{X}(w))$. We recall from Theorem 1.9.1 and from Lemma 1.9.2 (i) that the product of two elements of E^* supported in lengths less or equal respectively than L_1 and L_2 is supported in length less or equal than $L_1 + L_2$, and so we deduce that

$$\begin{aligned} \gamma_{c^-} \cdot x &= \gamma_{c^-} \cdot \Big(a\tau_1 + b\tau_{c_{-1}} + \sum_{\xi \in \Xi} c_\xi \cdot \Big(\tau_{\omega_\xi} + \tau_{\omega_\xi^{-1}} \Big) + \sum_{\substack{i \in \{1, \ldots, n\}, \\ \omega \in T^0/T^1}} d_{i,\omega} \zeta_{i,\omega} \Big) \\ &= \underbrace{\ldots}_{\substack{\text{supported in} \\ \text{length} < 2n}} + \sum_{\omega \in T^0/T^1} d_{n,\omega} \gamma_{c^-} \cdot \big(\tau_{\omega (s_0 s_1)^n} + \tau_{\omega^{-1} (s_1 s_0)^n} \big) \end{aligned}$$

and similarly

$$x \cdot \gamma_{c^-} = \underbrace{\ldots}_{\substack{\text{supported in} \\ \text{length} < 2n}} + \sum_{\omega \in T^0/T^1} d_{n,\omega} \cdot \big(\tau_{\omega (s_0 s_1)^n} + \tau_{\omega^{-1} (s_1 s_0)^n} \big) \cdot \gamma_{c^-}.$$

Applying the formulas (64) for the right action of E^0 on E^1, we see that for all $i \in \mathbb{Z}_{\geqslant 1}$ and all $\omega \in T^0/T^1$ we have

$$\begin{aligned} \gamma_{c^-} \cdot \tau_{\omega (s_0 s_1)^n} &= (c^-, 0, 0)_{\omega (s_0 s_1)^n}, \\ \gamma_{c^-} \cdot \tau_{\omega^{-1} (s_1 s_0)^n} &= 0. \end{aligned}$$

On the other side, using the formulas (62) for the left action of τ_{s_0} and τ_{s_1} on E^1, we find that

$$\begin{aligned} \tau_{(s_0 s_1)^n} \cdot \gamma_{c^-} &= 0, \\ \tau_{(s_1 s_0)^n} \cdot \gamma_{c^-} &= (c^-, 0, 0)_{(s_1 s_0)^n}, \end{aligned}$$

and further applying the formula (59) describing the left action of τ_ω on E^1, we obtain

$$\begin{aligned} \tau_{\omega (s_0 s_1)^n} \cdot \gamma_{c^-} &= 0, \\ \tau_{\omega^{-1} (s_1 s_0)^n} \cdot \gamma_{c^-} &= \big(c^-(\underline{\mathrm{id}}(\omega)^2 \cdot \_), 0, 0 \big)_{\omega^{-1} (s_1 s_0)^n} \end{aligned}$$

(recall that $\underline{\mathrm{id}}$ was defined in (48)).

We deduce that

$$\begin{aligned} 0 &= [\gamma_{c^-}, x] \\ &= \underbrace{\ldots}_{\substack{\text{supported in} \\ \text{length} < 2n}} + \sum_{\omega \in T^0/T^1} d_{n,\omega} \cdot \Big((c^-, 0, 0)_{\omega (s_0 s_1)^n} \\ &\qquad - \big(c^-(\underline{\mathrm{id}}(\omega)^2 \cdot \_), 0, 0 \big)_{\omega^{-1} (s_1 s_0)^n} \Big), \end{aligned}$$

and so, choosing $c^- \neq 0$, we obtain $d_{n,\omega} = 0$ for all $\omega \in T^0/T^1$.

We are thus reduced to proving that an element of the form

$$x = \sum_{\xi \in \Xi} c_\xi \cdot \left(\tau_{\omega_\xi} + \tau_{\omega_\xi^{-1}} \right) \in Z(E^*)^0$$

is zero. Since multiplication by γ_{c^-} on the left and on the right preserves the decomposition $\bigoplus_{\omega \in T^0/T^1} H^*(I, \mathbf{X}(\omega))$, to prove our claim it suffices to show that for all $\omega \in T^0/T^1 \smallsetminus \{1, c_{-1}\}$ we can choose c^- (possibly depending on ω) such that $[\gamma_{c^-}, \tau_\omega] \neq 0$. Using formulas (59) and (60), we see that

$$[\gamma_{c^-}, \tau_\omega] = \left(c^-, 0, 0\right)_\omega - \left(c^-(\underline{\mathrm{id}}(\omega)^2 \cdot \_), 0, 0\right)_\omega.$$

From this, we see that $[\gamma_{c^-}, \tau_\omega] \neq 0$ if we choose c^- in such a way that $c^-(\underline{\mathrm{id}}(\omega)^2) \neq c^-(1)$. There exists such a choice because $\underline{\mathrm{id}}(\omega)^2 \neq 1$. ∎

2.5 The 1st graded piece of the centre

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$.

In this section we will show that, under the above assumptions, the 1st graded piece of the centre is zero. As a first step, in the next lemma we compute explicitly $Z_{E^0}(E^1)$.

Lemma 2.5.1. *The $Z(E^0)$-bimodule $Z_{E^0}(E^1)$ is isomorphic to $Z(E^0) \cap F^1E^0$, and an explicit k-basis is given by*

$$\gamma_{i,\omega} := \beta^0_{\omega(s_0s_1)^i} - \beta^0_{\omega^{-1}(s_1s_0)^i} + e_1\beta^0_{s_0(s_1s_0)^{i-1}} - e_1\beta^0_{s_1(s_0s_1)^{i-1}}$$
$$\text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1},$$

Proof. Clearly $Z_{E^0}(E^1) \subseteq \ker(g_1)$, and hence $Z_{E^0}(E^1) = Z_{E^0}(\ker(g_1))$. Using the isomorphism of E^0-bimodules $\ker(g_1) \cong F^1E^0$ stated in (70), we deduce that

$$Z_{E^0}(E^1) \cong Z_{E^0}(F^1E^0) = Z(E^0) \cap F^1E^0.$$

To compute a basis, we start from the basis

$$\begin{array}{ll} \tau_1, & \\ \tau_{c_{-1}} & \text{if } p \neq 2, \\ \tau_\omega + \tau_{\omega^{-1}} & \text{for } \{\omega, \omega^{-1}\} \subseteq T^0/T^1 \smallsetminus \{1, c_{-1}\}, \\ \tau_\omega \cdot (\tau_{s_0} \cdot \tau_{s_1})^i + \tau_{\omega^{-1}} \cdot \left((\tau_{s_1} + e_1) \cdot (\tau_{s_0} + e_1)\right)^i & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}. \end{array}$$

of $Z(E^0)$ computed in (27). It is easy to show by induction that for all $\omega \in T^0/T^1$ and all $i \in \mathbb{Z}_{\geqslant 1}$ one has

$$\begin{aligned} &\tau_\omega \cdot (\tau_{s_0} \cdot \tau_{s_1})^i + \tau_{\omega^{-1}} \cdot \left((\tau_{s_1} + e_1) \cdot (\tau_{s_0} + e_1)\right)^i \\ &\quad = \tau_{\omega(s_0s_1)^i} + \tau_{\omega^{-1}(s_1s_0)^i} + e_1\tau_{s_0(s_1s_0)^{i-1}} + e_1\tau_{s_1(s_0s_1)^{i-1}} \\ &\qquad + \sum_{j=1}^{i-1} \left(e_1\tau_{(s_0s_1)^j} + e_1\tau_{(s_1s_0)^j} + e_1\tau_{s_0(s_1s_0)^{j-1}} + e_1\tau_{s_1(s_0s_1)^{j-1}} \right) \\ &\qquad + e_1. \end{aligned}$$

It follows that the following is another k-basis of $Z(E^0)$:

$$\begin{array}{ll} \tau_1, & \\ \tau_{c_{-1}} & \text{if } p \neq 2, \\ \tau_\omega + \tau_{\omega^{-1}} & \text{for } \{\omega, \omega^{-1}\} \subseteq T^0/T^1 \smallsetminus \{1, c_{-1}\}, \\ \begin{array}{l} \tau_{\omega(s_0s_1)^i} + \tau_{\omega^{-1}(s_1s_0)^i} \\ \qquad + e_1\tau_{s_0(s_1s_0)^{i-1}} + e_1\tau_{s_1(s_0s_1)^{i-1}} \end{array} & \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}. \end{array}$$

Each one of the above elements lies either in F_0E^0 or in F^1E^0, and so we see that the following is a basis of $Z(E^0) \cap F^1E^0$:

$$\begin{gathered} \tau_{\omega(s_0s_1)^i} + \tau_{\omega^{-1}(s_1s_0)^i} + e_1\tau_{s_0(s_1s_0)^{i-1}} + e_1\tau_{s_1(s_0s_1)^{i-1}} \\ \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}. \end{gathered}$$

Now, using the explicit description of the isomorphism $\ker(g_1) \cong F^1E^0$ in (70) and (71), we see that the following is a k-basis of $Z_{E^0}(E^1)$:

$$\begin{gathered} -\beta^0_{\omega(s_0s_1)^i} + \beta^0_{\omega^{-1}(s_1s_0)^i} - e_1\beta^0_{s_0(s_1s_0)^{i-1}} + e_1\beta^0_{s_1(s_0s_1)^{i-1}} \\ \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}, \end{gathered}$$

and up to changing signs this is the basis in the statement of the lemma. ■

We are now ready to show that $Z(E^*)^1 = 0$.

Proposition 2.5.2. *One has that $Z(E^*)^1 = 0$, and, more precisely,*

$$Z_{E^0 \cup H^1(I, \mathbf{X}(1))}(E^1) = 0.$$

Proof. From the formulas for the multiplication in E^* when lengths add up (Equation (36)), it follows that multiplication on the left or on the right by an element of $H^1(I, \mathbf{X}(1))$ preserves the components of the decomposition

$$E^* = \bigoplus_{w \in \widetilde{W}} H^*(I, \mathbf{X}(w)).$$

In particular we have the following: for all $w \in \widetilde{W}$ and for all $\gamma \in E^1$, one has

$$\mathrm{pr}_w\left(\left[\beta_1^-, \gamma\right]_{\mathrm{gr}}\right) = \left[\beta_1^-, \mathrm{pr}_w(\gamma)\right]_{\mathrm{gr}},$$

where $\mathrm{pr}_w \colon E^* \longrightarrow H^*(I, \mathbf{X}(w))$ denotes the projection with respect to the above decomposition and where $[\_,\_]_{\mathrm{gr}}$ denotes the graded commutator. Let us apply this in our situation: let us consider an element of $Z_{E^0}(E^1)$ written in the form

$$\sum_{\substack{i \in \mathbb{Z}_{\geqslant 1}, \\ \omega \in T^0/T^1}} c_{\omega,i}\gamma_{\omega,i},$$

where the elements $\gamma_{\omega,i}$ form the basis of $Z_{E^0}(E^1)$ computed in Lemma 2.5.1 and where the $c_{\omega,i}$'s are suitable coefficients in k (equal to zero for almost every i). Now, for $i_0 \in \mathbb{Z}_{\geqslant 0}$ and $\omega_0 \in T^0/T^1$, let us compute:

$$\begin{aligned} \mathrm{pr}_{\omega_0(s_0s_1)^{i_0+1}}\left(\left[\beta_1^-, \sum_{\substack{i \in \mathbb{Z}_{\geqslant 1}, \\ \omega \in T^0/T^1}} c_{\omega,i}\gamma_{\omega,i}\right]_{\mathrm{gr}}\right) &= \left[\beta_1^-, \mathrm{pr}_{\omega_0(s_0s_1)^{i_0+1}}\left(\sum_{\substack{i \in \mathbb{Z}_{\geqslant 1}, \\ \omega \in T^0/T^1}} c_{\omega,i}\gamma_{\omega,i}\right)\right]_{\mathrm{gr}} \\ &= \sum_{\substack{i \in \mathbb{Z}_{\geqslant 1}, \\ \omega \in T^0/T^1}} c_{\omega,i}\left[\beta_1^-, \mathrm{pr}_{\omega_0(s_0s_1)^{i_0+1}}(\gamma_{\omega,i})\right]_{\mathrm{gr}} \\ &= c_{\omega_0,i_0}\left[\beta_1^-, \beta^0_{\omega_0(s_0s_1)^{i_0+1}}\right]_{\mathrm{gr}}. \end{aligned}$$

Now, if we prove that, for all $i \in \mathbb{Z}_{\geqslant 0}$ and all $\omega \in T^0/T^1$, one has

$$\text{(Claim)} \qquad \left[\beta_1^-, \beta^0_{\omega(s_0s_1)^{i+1}}\right]_{\mathrm{gr}} \neq 0,$$

then all the coefficients $c_{\omega,i}$'s are zero, and we are done.

Recall from Lemma 1.10.3 that the following formulas hold:

$$\tau_{\omega(s_0s_1)^{i+1}} \cdot \beta_1^- = 0, \tag{106}$$

$$\beta_1^- \cdot \tau_{\omega(s_0s_1)^{i+1}} = \beta^-_{\omega(s_0s_1)^{i+1}}. \tag{107}$$

Let us compute $\left[\beta_1^-, \beta^0_{\omega(s_0s_1)^{i+1}}\right]_{\mathrm{gr}}$ using the relation between (the opposite of) the Yoneda product and the cup product (see Corollary 1.9.3) and the formulas (106) and (107). One has:

$$\begin{aligned}
\left[\beta_1^-, \beta^0_{\omega(s_0s_1)^{i+1}}\right]_{\mathrm{gr}} &= \beta_1^- \cdot \beta^0_{\omega(s_0s_1)^{i+1}} + \beta^0_{\omega(s_0s_1)^{i+1}} \cdot \beta_1^- \\
&= \left(\beta_1^- \cdot \tau_{\omega(s_0s_1)^{i+1}}\right) \smile \left(\tau_1 \cdot \beta^0_{\omega(s_0s_1)^{i+1}}\right) \\
&\qquad + \left(\beta^0_{\omega(s_0s_1)^{i+1}} \cdot \tau_1\right) \smile \left(\tau_{\omega(s_0s_1)^{i+1}} \cdot \beta_1^-\right) \\
&= \beta^-_{\omega(s_0s_1)^{i+1}} \smile \beta^0_{\omega(s_0s_1)^{i+1}} + \beta^0_{\omega(s_0s_1)^{i+1}} \smile 0 \\
&= \beta^-_{\omega(s_0s_1)^{i+1}} \smile \beta^0_{\omega(s_0s_1)^{i+1}}.
\end{aligned}$$

Therefore our claim has translated into proving that the above cup product is nonzero. But it is true for all $w \in \widetilde{W} \smallsetminus \left(T^0/T^1\right)$ that $\beta_w^- \smile \beta_w^0 \neq 0$: indeed, since the Shapiro isomorphism commutes with cup products, this is equivalent to showing that $\mathrm{Sh}_w(\beta_w^-) \smile \mathrm{Sh}_w(\beta_w^0) \neq 0$; and this is true, because $\mathrm{Sh}_w(\beta_w^-)$ and $\mathrm{Sh}_w(\beta_w^0)$ are two linearly independent elements of $H^1(I_w, k)$ and because the cup product algebra $H^*(I_w, k)$ can be identified with the exterior algebra $\bigwedge^* \left(H^1(I_w, k)\right)$ (indeed, I_w is a uniform pro-p group, as explained in [OS21, §4.2.3] and then Lazard's Theorem 1.8.1 applies). ■

2.6 The 2^{nd} graded piece of the centre

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. The first lemma will be stated under more general assumptions.

In this section we will compute explicitly the 2^{nd} graded piece of the centre, under the above assumptions. The proof will be divided into three subsections:

- In Subsection 2.6.a we will compute $Z_{E^0}(E^2)$. More precisely, we will determine a basis of $Z_{E^0}(E^2)$ in terms of the family of elements $(\alpha_w^{0,\star})_{w \in \widetilde{W}}$ defined (in an implicit way) in Proposition 1.10.4. The strategy consists in using the quoted proposition in order to relate $Z_{E^0}(E^2)$ with $Z_{E^0}(E^3)$.
- In Subsection 2.6.b we will rewrite the basis of $Z_{E^0}(E^2)$ in terms of the "standard" basis

$$\alpha_w^-, \qquad \alpha_w^0 \quad (\text{if } \ell(w) \geqslant 1), \qquad \alpha_w^+ \qquad \text{for } w \in \widetilde{W},$$

  which we have defined in (80). The purpose is twofold: this new rewrite has the advantage of being more explicit, and moreover it will be used to prove the final statement in the last subsection.

- In Subsection 2.6.c we will prove that the inclusion $Z(E^*)^2 \subseteq Z_{E^0}(E^2)$ is actually an equality, in particular achieving a complete description of $Z(E^*)^2$.

2.6.a Computation of $Z_{E^0}(E^2)$

Lemma 2.6.1. *Assume more generally that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the usual fixed choices as in Section 1.5) and that I is torsion-free. The natural homomorphism of $Z(E^0)$-modules*

$$Z_{E^0}(E^d) \longrightarrow Z_{E^0}\left(E^d/F_0E^d\right)$$

is surjective and it induces a bijection when restricted to the sub-k-vector space $Z_{E^0}(E^d) \cap F^1E^d$.

Proof. The fact that the restriction to $Z_{E^0}(E^d) \cap F^1E^d$ is injective follows from the fact that the map $F^1E^0 \longrightarrow E^d/F_0E^d$ is injective. It remains to show that for every element of $Z_{E^0}\left(E^d/F_0E^d\right)$, its (unique) representative $\sigma \in F^1E^d$ is centralized by E^0. We decompose σ as

$$\sigma = \sum_{i \in \mathbb{Z}_{\geqslant 0}} \sigma_i, \qquad \text{with } \sigma_i \in E^d_i := \bigoplus_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w)=i}} k\phi_w$$

(hence $\sigma_0 = 0$). As in the proof of Proposition 2.2.1, for all $v \in \widetilde{W}$, let us consider the map

$$\begin{aligned} C_v\colon\ E^d &\longrightarrow E^d \\ \phi &\longmapsto \tau_v \cdot \phi - \phi \cdot \tau_v, \end{aligned}$$

and, to ease notation, let us define $E^d_{-1} := \{0\}$. In the proof of loc. cit. (see (93)) we showed that

$$\begin{aligned} C_{s_0}\left(E^d_{2i} \oplus E^d_{2i+1}\right) &\subseteq E^d_{2i-1} \oplus E^d_{2i} &&\text{for } i \in \mathbb{Z}_{\geqslant 0}, \\ C_{s_1}\left(E^d_{2i} \oplus E^d_{2i+1}\right) &\subseteq E^d_{2i-1} \oplus E^d_{2i} &&\text{for } i \in \mathbb{Z}_{\geqslant 0}. \end{aligned}$$

Let $j \in \{0,1\}$. By assumption, σ is mapped to $Z_{E^0}\left(E^d/F_0E^d\right)$, and so

$$F_0E^d \ni C_{s_j}(\sigma) = \sum_{i \in \mathbb{Z}_{\geqslant 0}} C_{s_j}(\sigma_{2i} + \sigma_{2i+1}).$$

From the above inclusions, we get that $C_{s_j}(\sigma_{2i} + \sigma_{2i+1}) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$. It is also easy to see that $C_\omega(\sigma_{2i} + \sigma_{2i+1}) = 0$ for such i's, and so we conclude that $\sigma_{2i} + \sigma_{2i+1}$ is centralized by E^0 for all $i \in \mathbb{Z}_{\geqslant 1}$.

Therefore, it remains to show that σ_1 is centralized by E^0. But in the last part of the proof of Proposition 2.2.1, we saw that if an element of $E^d_0 \oplus E^d_1$ is centralized by τ_ω for all $\omega \in T^0/T^1$, then it is automatically centralized by the whole E^0. So in our case it suffices to check that σ_1 is centralized by τ_ω for all $\omega \in T^0/T^1$, which is easy. ∎

Remark 2.6.2. One has an isomorphism of E^0-bimodules

$$\begin{aligned} {}^{\mathcal{J}}\!\left((F^1E^0)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}} &\longrightarrow E^3/F_0E^3 \\ \underset{(w \in \widetilde{W} \text{ with } \ell(w) \geqslant 1)}{\tau_w^\vee\big|_{F^1E^0}} &\longmapsto \overline{\phi_w}, \end{aligned}$$

which by composition with the isomorphism in Proposition 1.10.4 gives an isomorphism

$$\begin{array}{ccc} E^3/F_0E^3 & \longrightarrow & \ker(g_2) \\ \underset{(w \in \widetilde{W} \text{ with } \ell(w) \geqslant 1)}{\overline{\phi_w}} & \longmapsto & \alpha_w^{0,\star}. \end{array}$$

Proof. Similarly to Proposition 1.10.4 we use the identifications

$$(E^0)^{\vee,\mathrm{finite}} \cong \bigcup_{n\in\mathbb{Z}_{\geqslant 1}} \left(E^0/F^nE^0\right)^{\vee}, \qquad (F^1E^0)^{\vee,\mathrm{finite}} \cong \bigcup_{n\in\mathbb{Z}_{\geqslant 1}} \left(F^1E^0/F^nE^0\right)^{\vee}.$$

We see that the kernel of the restriction map $(E^0)^{\vee,\mathrm{finite}} \longrightarrow (F^1E^0)^{\vee,\mathrm{finite}}$ coincides with $\left(E^0/F^1E^0\right)^{\vee}$. Via the isomorphism

$$\begin{array}{ccc} {}^{\jmath}\left((E^0)^{\vee,\mathrm{finite}}\right)^{\jmath} & \longrightarrow & E^3 \\ \underset{(w \in \widetilde{W})}{\tau_w^{\vee}\big|_{F^1E^0}} & \longmapsto & \phi_w, \end{array}$$

the submodule ${}^{\jmath}\left(\left(E^0/F^1E^0\right)^{\vee}\right)^{\jmath}$ corresponds to F_0E^3. Hence, considering the corresponding quotients on both sides we get the isomorphism claimed in the remark. ■

Corollary 2.6.3. *One has that $Z_{E^0}(E^2)$ is isomorphic to $Z_{E^0}(E^3)/F_0E^3$ as a $Z(E^0)$-module, and the following is a k-basis of $Z_{E^0}(E^2)$:*

$$\begin{array}{llll} e_1 \cdot \alpha_{s_0}^{0,\star}, & e_{\chi_0} \cdot \alpha_{s_0}^{0,\star}, & e_1 \cdot \alpha_{s_1}^{0,\star}, & e_{\chi_0} \cdot \alpha_{s_1}^{0,\star}, \\ \multicolumn{4}{l}{\alpha_{\omega(s_0s_1)^i}^{0,\star} + \alpha_{\omega^{-1}(s_1s_0)^i}^{0,\star} - e_1 \cdot \alpha_{(s_0s_1)^is_0}^{0,\star} - e_1 \cdot \alpha_{(s_1s_0)^is_1}^{0,\star}} \\ \multicolumn{4}{l}{\qquad \text{for } \omega \in T^0/T^1 \text{ and } i \in \mathbb{Z}_{\geqslant 1}.} \end{array}$$

Proof. The last remark yields that $Z_{E^0}(E^2)$ is isomorphic to $Z_{E^0}\left(E^3/F_0E^3\right)$. Furthermore, Lemma 2.6.1 yields that $Z_{E^0}\left(E^3/F_0E^3\right)$ coincides with the image of the map

$$Z_{E^0}(E^3) \longrightarrow Z_{E^0}\left(E^3/F_0E^3\right).$$

This image is $Z_{E^0}(E^3)/F_0E^3$ because $F_0E^3 \subseteq Z_{E^0}(E^3)$ (see, e.g., Proposition 2.2.1). The claim about the explicit basis then follows from the computation of the basis of $Z_{E^0}(E^3)$ in Proposition 2.2.1 (actually, in Remark 2.2.2), by making use of the isomorphism

$$\begin{array}{ccc} E^3/F_0E^3 & \longrightarrow & \ker(g_2) \\ \underset{(w \in \widetilde{W} \text{ with } \ell(w) \geqslant 1)}{\overline{\phi_w}} & \longmapsto & \alpha_w^{0,\star}. \end{array}$$

■

Remark 2.6.4. Equivalently, it is easy to see that also the following is a k-basis of $\ker(g_2)$ (this can be obtained as in the proof of the last corollary by using the alternative k-basis of $Z_{E^0}(E^d)$ computed in Lemma 2.3.1, or, alternatively, manipulating the basis of $\ker(g_2)$ computed in the last corollary):

$$\begin{array}{llll} e_1 \cdot \alpha^{0,\star}_{s_0}, & e_{\chi_0} \cdot \alpha^{0,\star}_{s_0}, & e_1 \cdot \alpha^{0,\star}_{s_1}, & e_{\chi_0} \cdot \alpha^{0,\star}_{s_1}, \\ \multicolumn{4}{l}{e_\lambda \alpha^{0,\star}_{(s_1 s_0)^i} + e_{\lambda^{-1}} \alpha^{0,\star}_{(s_0 s_1)^i}} \\ \multicolumn{4}{l}{\qquad\qquad \text{for } \lambda \in \widehat{T^0/T^1} \smallsetminus \{1\} \text{ and } i \in \mathbb{Z}_{\geqslant 1},} \\ \multicolumn{4}{l}{e_1 \alpha^{0,\star}_{(s_1 s_0)^i} + e_1 \alpha^{0,\star}_{(s_0 s_1)^i} - e_1 \cdot \alpha^{0,\star}_{(s_1 s_0)^i s_1} - e_1 \cdot \alpha^{0,\star}_{(s_0 s_1)^i s_0}} \\ \multicolumn{4}{l}{\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1}.} \end{array}$$

2.6.b Rewrite of the basis of $Z_{E^0}(E^2)$

Let $w \in \widetilde{W}$ such that $\ell(w) \geqslant 1$. Recall that we have the following partial description of $\alpha^{0,\star}_w$ (already recalled in (88)):

$$\begin{aligned} \alpha^{0,\star}_w - \alpha^0_w &\in e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}} \ker(f_2) && \text{if } \ell(s_0 w) = \ell(w) + 1, \\ \alpha^{0,\star}_w + \alpha^0_w &\in e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}} \ker(f_2) && \text{if } \ell(s_1 w) = \ell(w) + 1. \end{aligned}$$

In view of Corollary 2.6.3 we would like to compute also the $e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}}$-component of $\alpha^{0,\star}_w$ in the cases $w = (s_0 s_1)^i$ or $w = (s_1 s_0)^i$ for some $i \in \mathbb{Z}_{\geqslant 1}$. This is basically already carried out in the proof of [OS21, Lemma 7.11]. However, the formulas are computationally involved and only partially written down explicitly, and so we will derive them step by step from loc. cit. in the following two lemmas and one corollary.

Lemma 2.6.5. *One has:*

$$e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0 s_1)^i} = -e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0 s_1)^i} + 2 \sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}} \alpha^+_{s_0 (s_1 s_0)^i} - 2 \sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}} \alpha^+_{s_1 (s_0 s_1)^i},$$

or, equivalently,

$$\begin{aligned} e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0 s_1)^i} e_{\underline{\mathrm{id}}^{-1}} = {} & -e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0 s_1)^i} e_{\underline{\mathrm{id}}^{-1}} \\ & + 2 \sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}} \alpha^+_{s_0 (s_1 s_0)^i} e_{\underline{\mathrm{id}}^{-1}} - 2 \sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}} \alpha^+_{s_1 (s_0 s_1)^i} e_{\underline{\mathrm{id}}^{-1}}. \end{aligned}$$

Note that the equivalence of the two statements follows from the fact that $e_{\underline{\mathrm{id}}^{-1}}$ commutes with α^+_w for all $w \in \widetilde{W}$ of odd length (see (85)), it commutes with α^0_w for all $w \in \widetilde{W}$ of even length (see again (85)), and it commutes with $\alpha^{0,\star}_w$ for all $w \in \widetilde{W}$ of even length (see the description of $\ker(g_2)$ as an E^0-bimodule in Proposition 1.10.4).

Proof. From what we said above about the α^0_w's, it follows that

$$e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0 s_1)^i} e_{\underline{\mathrm{id}}^{-1}} = \gamma - e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0 s_1)^i} e_{\underline{\mathrm{id}}^{-1}} \qquad \text{for some } \gamma \in \ker(f_2).$$

Let us look at the direct sum decomposition $E^2 = \ker(f_2) \oplus \ker(g_2)$, which we recalled in Proposition 1.10.4 quoting [OS21, Proposition 7.12]. In loc. cit. it is proved that, via the isomorphism $E^2 \cong {}^{\mathcal{J}}\big((E^1)^{\vee,\mathrm{finite}}\big)^{\mathcal{J}}$, this decomposition corresponds to a decomposition

$${}^{\mathcal{J}}\Big((E^1)^{\vee,\mathrm{finite}}\Big)^{\mathcal{J}} = K_{f_1} \oplus K_{g_1},$$

where

$$K_{f_1} \coloneqq \left\{ \xi \in {}^{\mathcal{J}}\!\left((E^1)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}} \;\middle|\; \xi\big|_{\ker(g_1)} = 0 \right\},$$
$$K_{g_1} \coloneqq \left\{ \xi \in {}^{\mathcal{J}}\!\left((E^1)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}} \;\middle|\; \xi\big|_{\ker(f_1)} = 0 \right\}.$$

So, starting with the element $\xi = e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0s_1)^i} e_{\underline{\mathrm{id}}^{-1}} = \gamma - e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0s_1)^i} e_{\underline{\mathrm{id}}^{-1}}$ and applying to it the isomorphism $E^2 \cong {}^{\mathcal{J}}\!\left((E^1)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}}$, we view it as an element $\xi = \theta + \eta \in {}^{\mathcal{J}}\!\left((E^1)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}}$ for $\theta \in K_{f_1}$ corresponding to γ and for $\eta \in K_{g_1}$ corresponding to $-e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0s_1)^i} e_{\underline{\mathrm{id}}^{-1}}$. We write this correspondence using a pairing notation:

$$\begin{aligned}
\xi &= \left\langle e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0s_1)^i} e_{\underline{\mathrm{id}}^{-1}}, _ \right\rangle, \\
\theta &= \langle \gamma, _ \rangle, \\
\eta &= \left\langle -e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0s_1)^i} e_{\underline{\mathrm{id}}^{-1}}, _ \right\rangle.
\end{aligned}$$

The element η (which is what we are interested in) is explicitly computed in [OS21, Proof of Lemma 7.11]. Namely, in loc. cit. the linear form $\eta\colon E^1 \longrightarrow k$ is defined in the following way (there, ξ is an arbitrary element in the subspace $e_{\underline{\mathrm{id}}}(E^1)^{\vee,\mathrm{finite}} e_{\underline{\mathrm{id}}} = e_{\underline{\mathrm{id}}^{-1}}\, {}^{\mathcal{J}}\!\left((E^1)^{\vee,\mathrm{finite}}\right)^{\mathcal{J}} e_{\underline{\mathrm{id}}^{-1}}$):

$$\begin{aligned}
\eta\big|_{e_{\underline{\mathrm{id}}} \ker(f_1) e_{\underline{\mathrm{id}}}} &= 0, \\
\eta\big|_{e_{\underline{\mathrm{id}}} \ker(g_1) e_{\underline{\mathrm{id}}}} &= \xi\big|_{e_{\underline{\mathrm{id}}} \ker(g_1) e_{\underline{\mathrm{id}}}}, \\
\eta\big|_{e_{\underline{\mathrm{id}}} \beta^+_{s_1} e_{\underline{\mathrm{id}}}} &= 2 \sum_{j=1}^{+\infty} \xi\left(e_{\underline{\mathrm{id}}} \beta^0_{s_0s_1} e_{\underline{\mathrm{id}}}\right)
\end{aligned}$$

(here, we use the decomposition $e_{\underline{\mathrm{id}}} E^1 e_{\underline{\mathrm{id}}} = e_{\underline{\mathrm{id}}} \ker(f_1) e_{\underline{\mathrm{id}}} \oplus e_{\underline{\mathrm{id}}} \ker(g_1) e_{\underline{\mathrm{id}}} \oplus k e_{\underline{\mathrm{id}}} \beta^+_{s_1} e_{\underline{\mathrm{id}}}$, which follows from Proposition 1.10.2, and using this decomposition we define η as a linear form $\eta\colon e_{\underline{\mathrm{id}}} E^1 e_{\underline{\mathrm{id}}} \longrightarrow k$, and extend it by 0 on the components $e_\lambda E^1 e_\mu$ for $\lambda, \mu \in \widehat{T^0/T^1}$ with $(\lambda, \mu) \neq (\underline{\mathrm{id}}, \underline{\mathrm{id}})$; moreover, note that the infinite sum does make sense because ξ lies in the finite dual of E^1). In [OS21, Proof of Lemma 7.11], it is shown that $e_{\underline{\mathrm{id}}} E^1 e_{\underline{\mathrm{id}}}$ is the k-vector space generated by the following elements:

$$\begin{aligned}
&e_{\underline{\mathrm{id}}} \beta^0_w e_{\underline{\mathrm{id}}} && \text{for } w \in \widetilde{W} \text{ with positive even length,} \\
&e_{\underline{\mathrm{id}}} \beta^+_w e_{\underline{\mathrm{id}}} && \text{for } w \in \widetilde{W} \text{ with odd length.}
\end{aligned}$$

By deleting what is redundant, we get the following k-basis (the fact that these elements are nonzero follows from (61)):

$$\begin{aligned}
&e_{\underline{\mathrm{id}}} \beta^0_{(s_0s_1)^j} e_{\underline{\mathrm{id}}} && \text{for } j \in \mathbb{Z}_{\geqslant 1}, \\
&e_{\underline{\mathrm{id}}} \beta^0_{(s_1s_0)^j} e_{\underline{\mathrm{id}}} && \text{for } j \in \mathbb{Z}_{\geqslant 1}, \\
&e_{\underline{\mathrm{id}}} \beta^+_{s_0(s_1s_0)^j} e_{\underline{\mathrm{id}}} && \text{for } j \in \mathbb{Z}_{\geqslant 0}, \\
&e_{\underline{\mathrm{id}}} \beta^+_{s_1(s_0s_1)^j} e_{\underline{\mathrm{id}}} && \text{for } j \in \mathbb{Z}_{\geqslant 0}.
\end{aligned} \tag{108}$$

Let $w \in \widetilde{W}$ with positive even length. From the definition of $\beta^{0,\star}_w$ (see (71)), we get that

$$e_{\underline{\mathrm{id}}} \beta^0_w e_{\underline{\mathrm{id}}} = \pm e_{\underline{\mathrm{id}}} \beta^{0,\star}_w e_{\underline{\mathrm{id}}} \in \ker(g_1).$$

Hence, for $j \in \mathbb{Z}_{\geqslant 1}$ we have

$$\begin{aligned}
\eta\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) &= \xi\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) \\
&= \Big\langle e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}}, e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}}\Big\rangle \\
&= \Big\langle \alpha^0_{(s_0s_1)^i}, \beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}}\Big\rangle \\
&= -\Big\langle \alpha^0_{(s_0s_1)^i}, \sum_{\omega\in T^0/T^1}\underline{\mathrm{id}}(\omega^{-1})\beta^0_{(s_0s_1)^j\omega}\Big\rangle \\
&= \begin{cases} -1 & \text{if } j = i, \\ 0 & \text{if } j \neq i, \end{cases}
\end{aligned}$$

and similarly we see that

$$\eta\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_1s_0)^j}e_{\underline{\mathrm{id}}}\big) = 0.$$

In [OS21, Proof of Lemma 7.11], the following values of η are computed:

$$\begin{aligned}
\eta\big(e_{\underline{\mathrm{id}}}\beta^+_{s_0(s_1s_0)^j}e_{\underline{\mathrm{id}}}\big) &= -2\sum_{l=j+1}^{+\infty}\xi\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^l}e_{\underline{\mathrm{id}}}\big), \\
\eta\big(e_{\underline{\mathrm{id}}}\beta^+_{s_1(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) &= 2\sum_{l=j+1}^{+\infty}\xi\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^l}e_{\underline{\mathrm{id}}}\big).
\end{aligned}$$

Hence, we deduce that

$$\begin{aligned}
\eta\big(e_{\underline{\mathrm{id}}}\beta^+_{s_0(s_1s_0)^j}e_{\underline{\mathrm{id}}}\big) &= \begin{cases} 2 & \text{if } j \leqslant i-1, \\ 0 & \text{if } j \geqslant i, \end{cases} \\
\eta\big(e_{\underline{\mathrm{id}}}\beta^+_{s_1(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) &= \begin{cases} -2 & \text{if } j \leqslant i-1, \\ 0 & \text{if } j \geqslant i. \end{cases}
\end{aligned}$$

We claim that η is equal to

$$\begin{aligned}
\eta' \coloneqq{}& \big\langle e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}}, _\big\rangle \\
&- 2\sum_{j=0}^{i-1}\big\langle e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_0(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}}, _\big\rangle + 2\sum_{j=0}^{i-1}\big\langle e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_1(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}}, _\big\rangle,
\end{aligned}$$

element which can be rewritten as

$$\begin{aligned}
\eta' ={}& \big\langle \alpha^0_{(s_0s_1)^i}, e_{\underline{\mathrm{id}}}\cdot_\cdot e_{\underline{\mathrm{id}}}\big\rangle \\
&- 2\sum_{j=0}^{i-1}\big\langle \alpha^+_{s_0(s_1s_0)^i}, e_{\underline{\mathrm{id}}}\cdot_\cdot e_{\underline{\mathrm{id}}}\big\rangle + 2\sum_{j=0}^{i-1}\big\langle \alpha^+_{s_1(s_0s_1)^i}, e_{\underline{\mathrm{id}}}\cdot_\cdot e_{\underline{\mathrm{id}}}\big\rangle.
\end{aligned}$$

It is easy to see that η' is zero on $e_\lambda E^1 e_\mu$ for $\lambda, \mu \in \widehat{T^0/T^1}$ with $(\lambda, \mu) \neq (\underline{\mathrm{id}}, \underline{\mathrm{id}})$, and we compute

$$\begin{aligned}
\eta'\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) &= \big\langle \alpha^0_{(s_0s_1)^i}, e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big\rangle \\
&= \begin{cases} -1 & \text{if } j = i, \\ 0 & \text{if } j \neq i. \end{cases}
\end{aligned}$$

Furthermore, we compute

$$\begin{aligned}
\eta'\big(e_{\underline{\mathrm{id}}}\beta^{+}_{s_0(s_1s_0)^j}e_{\underline{\mathrm{id}}}\big) &= -2\sum_{j=0}^{i-1}\big\langle \alpha^{+}_{s_0(s_1s_0)^i}, e_{\underline{\mathrm{id}}}\beta^{+}_{s_0(s_1s_0)^j}e_{\underline{\mathrm{id}}}\big\rangle \\
&= \begin{cases} 2 & \text{if } j \leqslant i-1, \\ 0 & \text{if } j \geqslant i. \end{cases} \\
\eta'\big(e_{\underline{\mathrm{id}}}\beta^{+}_{s_1(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) &= 2\sum_{j=0}^{i-1}\big\langle \alpha^{+}_{s_1(s_0s_1)^i}, e_{\underline{\mathrm{id}}}\beta^{+}_{s_1(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big\rangle \\
&= \begin{cases} -2 & \text{if } j \leqslant i-1, \\ 0 & \text{if } j \geqslant i. \end{cases}
\end{aligned}$$

Recalling the description of the basis (108) of $e_{\underline{\mathrm{id}}}E^1e_{\underline{\mathrm{id}}}$, we see that these values completely determine η' and that η' coincides with η on the whole E^1.

Recalling that $\eta = \left\langle -e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}}, \_\right\rangle$, we conclude that

$$\begin{aligned}
e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}} &= -e_{\underline{\mathrm{id}}^{-1}}\alpha^{0}_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}} \\
&\qquad + 2\sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}}\alpha^{+}_{s_0(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}} - 2\sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}}\alpha^{+}_{s_1(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}},
\end{aligned}$$

and this is the formula we had to show. ∎

Lemma 2.6.6. *One has:*

$$e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_1s_0)^i} = e_{\underline{\mathrm{id}}^{-1}}\alpha^{0}_{(s_1s_0)^i},$$

or, equivalently,

$$e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}} = e_{\underline{\mathrm{id}}^{-1}}\alpha^{0}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}}.$$

The equivalence of the two statements can be seen in the same way as in the last lemma.

Proof. The proof is completely analogous to (but quicker than) the proof of the last lemma. Using (88) we write

$$e_{\underline{\mathrm{id}}^{-1}}\alpha^{0}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}} = \gamma + e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}} \qquad \text{for some } \gamma \in \ker(f_2),$$

and with the same notation as in the proof of the last lemma we view this as an element

$$\xi = \theta + \eta \in {}^{\mathcal{J}}\Big((E^1)^{\vee,\mathrm{finite}}\Big)^{\mathcal{J}},$$

for $\theta \in K_{f_1}$ corresponding to γ and for $\eta \in K_{g_1}$ corresponding to $e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}}$.

The explicit definition of η from ξ and the formulas are the same as in the last lemma, because in [OS21, Proof of Lemma 7.11] such formulas are proved for an arbitrary element

$$\xi \in e_{\underline{\mathrm{id}}}(E^1)^{\vee,\mathrm{finite}}e_{\underline{\mathrm{id}}} = e_{\underline{\mathrm{id}}^{-1}}\,{}^{\mathcal{J}}\Big((E^1)^{\vee,\mathrm{finite}}\Big)^{\mathcal{J}}\,e_{\underline{\mathrm{id}}^{-1}};$$

in particular we have

$$\begin{aligned}
\eta\big|_{e_{\underline{\mathrm{id}}}\ker(f_1)e_{\underline{\mathrm{id}}}} &= 0,\\
\eta\big|_{e_{\underline{\mathrm{id}}}\ker(g_1)e_{\underline{\mathrm{id}}}} &= \xi\big|_{e_{\underline{\mathrm{id}}}\ker(g_1)e_{\underline{\mathrm{id}}}},\\
\eta\big|_{e_{\underline{\mathrm{id}}}\beta^+_{s_1}e_{\underline{\mathrm{id}}}} &= 2\sum_{j=1}^{+\infty}\xi\big(e_{\underline{\mathrm{id}}}\beta^0_{s_0s_1}e_{\underline{\mathrm{id}}}\big),
\end{aligned}$$

and we have the formulas

$$\begin{aligned}
\eta\big(e_{\underline{\mathrm{id}}}\beta^+_{s_0(s_1s_0)^j}e_{\underline{\mathrm{id}}}\big) &= -2\sum_{l=j+1}^{+\infty}\xi\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^l}e_{\underline{\mathrm{id}}}\big) = 0,\\
\eta\big(e_{\underline{\mathrm{id}}}\beta^+_{s_1(s_0s_1)^j}e_{\underline{\mathrm{id}}}\big) &= 2\sum_{l=j+1}^{+\infty}\xi\big(e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^l}e_{\underline{\mathrm{id}}}\big) = 0.
\end{aligned}$$

Recall from the proof of the last lemma that $e_{\underline{\mathrm{id}}}E^1e_{\underline{\mathrm{id}}}$ is the k-vector space having the following k-basis:

$$\begin{aligned}
&e_{\underline{\mathrm{id}}}\beta^0_{(s_0s_1)^j}e_{\underline{\mathrm{id}}} &&\text{for } j\in\mathbb{Z}_{\geqslant 1},\\
&e_{\underline{\mathrm{id}}}\beta^0_{(s_1s_0)^j}e_{\underline{\mathrm{id}}} &&\text{for } j\in\mathbb{Z}_{\geqslant 1},\\
&e_{\underline{\mathrm{id}}}\beta^+_{s_0(s_1s_0)^j}e_{\underline{\mathrm{id}}} &&\text{for } j\in\mathbb{Z}_{\geqslant 0},\\
&e_{\underline{\mathrm{id}}}\beta^+_{s_1(s_0s_1)^j}e_{\underline{\mathrm{id}}} &&\text{for } j\in\mathbb{Z}_{\geqslant 0}.
\end{aligned}$$

But the elements in the first two lines lie in $\ker(g_1)$ (see (71)), and so at these elements the linear forms η and ξ have the same value. On the elements of the last two lines we have just said that η is zero (as is ξ). Therefore we deduce that $\eta=\xi$, and so by definition of η and ξ we get

$$e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}} = e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}}.$$

■

Corollary 2.6.7. *Let $i\in\mathbb{Z}_{\geqslant 1}$. The following formulas hold:*

$$\begin{aligned}
\alpha^{0,\star}_{(s_0s_1)^i} &= -\alpha^0_{(s_0s_1)^i} + 2\sum_{j=0}^{i-1}e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_0(s_1s_0)^i} - 2\sum_{j=0}^{i-1}e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_1(s_0s_1)^i}\\
\alpha^{0,\star}_{(s_1s_0)^i} &= \alpha^0_{(s_1s_0)^i} + 2\sum_{j=0}^{i-1}e_{\underline{\mathrm{id}}}\alpha^-_{s_1(s_0s_1)^i} - 2\sum_{j=0}^{i-1}e_{\underline{\mathrm{id}}}\alpha^-_{s_0(s_1s_0)^i},
\end{aligned}$$

Proof. Recall from (88) that

$$\begin{aligned}
x &\coloneqq \alpha^{0,\star}_{(s_0s_1)^i} + \alpha^0_{(s_0s_1)^i} \in e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}}\ker(f_2),\\
y &\coloneqq \alpha^{0,\star}_{(s_1s_0)^i} - \alpha^0_{(s_1s_0)^i} \in e_{\{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}\}}\ker(f_2).
\end{aligned}$$

We have to compute x and y. Since both $\alpha^{0,\star}_w$ and α^0_w commute with both $e_{\underline{\mathrm{id}}}$ and $e_{\underline{\mathrm{id}}^{-1}}$ for all $w\in\widetilde{W}$ of even length (for $\alpha^{0,\star}_w$ this is (85), and for $\alpha^{0,\star}_w$ one can use the description of $\ker(g_2)$ as an E^0-bimodule given in Proposition 1.10.4), we deduce that

$$\begin{aligned}
x &= e_{\underline{\mathrm{id}}}x + e_{\underline{\mathrm{id}}^{-1}}x\\
&= e_{\underline{\mathrm{id}}}xe_{\underline{\mathrm{id}}} + e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}.
\end{aligned}$$

and the same for y. Now, let us write

$$\begin{aligned}
e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}} &= e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}} - e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}},\\
e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}} &= -e_{\underline{\mathrm{id}}^{-1}}ye_{\underline{\mathrm{id}}^{-1}} + e_{\underline{\mathrm{id}}^{-1}}\alpha^{0,\star}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}},\\
e_{\underline{\mathrm{id}}}\alpha^0_{(s_0s_1)^i}e_{\underline{\mathrm{id}}} &= e_{\underline{\mathrm{id}}}xe_{\underline{\mathrm{id}}} - e_{\underline{\mathrm{id}}}\alpha^{0,\star}_{(s_0s_1)^i}e_{\underline{\mathrm{id}}},\\
e_{\underline{\mathrm{id}}}\alpha^0_{(s_1s_0)^i}e_{\underline{\mathrm{id}}} &= -e_{\underline{\mathrm{id}}}ye_{\underline{\mathrm{id}}} + e_{\underline{\mathrm{id}}}\alpha^{0,\star}_{(s_1s_0)^i}e_{\underline{\mathrm{id}}}.
\end{aligned}$$

Here, the two terms on the right hand side of each of the four equalities lie respectively in $\ker(f_2)$ and in $\ker(g_2)$. Since $\Gamma_\varpi(\zeta) = \zeta$, we deduce that the decomposition $E^2 = \ker(f_2) \oplus \ker(g_2)$ is Γ_ϖ-invariant. Using the formulas for the action of Γ_ϖ on E^2 (see (82)), we compute

$$\begin{aligned}
\Gamma_\varpi\big(e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_0s_1)^i}e_{\underline{\mathrm{id}}^{-1}}\big) &= -e_{\underline{\mathrm{id}}}\alpha^0_{(s_1s_0)^i}e_{\underline{\mathrm{id}}},\\
\Gamma_\varpi\big(e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_1s_0)^i}e_{\underline{\mathrm{id}}^{-1}}\big) &= -e_{\underline{\mathrm{id}}}\alpha^0_{(s_0s_1)^i}e_{\underline{\mathrm{id}}}.
\end{aligned}$$

And so by the said Γ_ϖ-invariance it follows that

$$\begin{aligned}
-e_{\underline{\mathrm{id}}}ye_{\underline{\mathrm{id}}} &= -\Gamma_\varpi\big(e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}\big),\\
e_{\underline{\mathrm{id}}}xe_{\underline{\mathrm{id}}} &= -\Gamma_\varpi\big(-e_{\underline{\mathrm{id}}^{-1}}ye_{\underline{\mathrm{id}}^{-1}}\big),
\end{aligned}$$

i.e., changing signs,

$$\begin{aligned}
e_{\underline{\mathrm{id}}}ye_{\underline{\mathrm{id}}} &= \Gamma_\varpi\big(e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}\big),\\
e_{\underline{\mathrm{id}}}xe_{\underline{\mathrm{id}}} &= \Gamma_\varpi\big(e_{\underline{\mathrm{id}}^{-1}}ye_{\underline{\mathrm{id}}^{-1}}\big).
\end{aligned}$$

The value of $e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}$ has been computed in Lemma 2.6.5, while the value of $e_{\underline{\mathrm{id}}^{-1}}ye_{\underline{\mathrm{id}}^{-1}}$ has been computed in Lemma 2.6.6 (and is zero). Hence, also recalling once again the formulas (82) for the action of Γ_ϖ on E^2, we get:

$$\begin{aligned}
x &= e_{\underline{\mathrm{id}}}xe_{\underline{\mathrm{id}}} + e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}\\
&= e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}\\
&= 2\sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_0(s_1s_0)^i} - 2\sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_1(s_0s_1)^i},
\end{aligned}$$

and

$$\begin{aligned}
y &= e_{\underline{\mathrm{id}}}ye_{\underline{\mathrm{id}}} + e_{\underline{\mathrm{id}}^{-1}}ye_{\underline{\mathrm{id}}^{-1}}\\
&= \Gamma_\varpi\big(e_{\underline{\mathrm{id}}^{-1}}xe_{\underline{\mathrm{id}}^{-1}}\big)\\
&= 2\sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}}\alpha^-_{s_1(s_0s_1)^i} - 2\sum_{j=0}^{i-1} e_{\underline{\mathrm{id}}}\alpha^-_{s_0(s_1s_0)^i}.
\end{aligned}$$

■

Corollary 2.6.8. *The k-basis of $Z_{E^0}(E^2)$ computed in Remark 2.6.4 can be explic-*

itly described as follows:

$$
\begin{aligned}
&e_1 \cdot \alpha^{0,\star}_{s_0} = -e_1 \cdot \alpha^0_{s_0}, \qquad\qquad e_{\chi_0} \cdot \alpha^{0,\star}_{s_0} = -e_{\chi_0} \cdot \alpha^0_{s_0},\\
&e_1 \cdot \alpha^{0,\star}_{s_1} = e_1 \cdot \alpha^0_{s_1}, \qquad\qquad e_{\chi_0} \cdot \alpha^{0,\star}_{s_1} = e_{\chi_0} \cdot \alpha^0_{s_1},\\
&e_\lambda \alpha^{0,\star}_{(s_1s_0)^i} + e_{\lambda^{-1}} \alpha^{0,\star}_{(s_0s_1)^i} = e_\lambda \alpha^0_{(s_1s_0)^i} - e_{\lambda^{-1}} \alpha^0_{(s_0s_1)^i}\\
&\qquad\qquad \text{for } \lambda \in \widehat{T^0/T^1} \smallsetminus \{1, \underline{\mathrm{id}}\} \text{ and } i \in \mathbb{Z}_{\geqslant 1},\\
&e_{\underline{\mathrm{id}}} \alpha^{0,\star}_{(s_1s_0)^i} + e_{\underline{\mathrm{id}}^{-1}} \alpha^{0,\star}_{(s_0s_1)^i} = e_{\underline{\mathrm{id}}} \alpha^0_{(s_1s_0)^i} - e_{\underline{\mathrm{id}}^{-1}} \alpha^0_{(s_0s_1)^i}\\
&\quad + 2\sum_{j=0}^{i-1} \Big(e_{\underline{\mathrm{id}}^{-1}} \alpha^+_{s_0(s_1s_0)^i} - e_{\underline{\mathrm{id}}^{-1}} \alpha^+_{s_1(s_0s_1)^i} + e_{\underline{\mathrm{id}}} \alpha^-_{s_1(s_0s_1)^i} - e_{\underline{\mathrm{id}}} \alpha^-_{s_0(s_1s_0)^i} \Big)\\
&\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1},\\
&e_1 \alpha^{0,\star}_{(s_1s_0)^i} + e_1 \alpha^{0,\star}_{(s_0s_1)^i} - e_1 \cdot \alpha^{0,\star}_{(s_1s_0)^i s_1} - e_1 \cdot \alpha^{0,\star}_{(s_0s_1)^i s_0}\\
&\quad = e_1 \alpha^0_{(s_1s_0)^i} + e_1 \alpha^0_{(s_0s_1)^i} - e_1 \cdot \alpha^0_{(s_1s_0)^i s_1} - e_1 \cdot \alpha^0_{(s_0s_1)^i s_0}\\
&\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1}.
\end{aligned}
$$

Proof. For all the components except the $e_{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}}$-component this is immediate from formula (88), while for the $e_{\underline{\mathrm{id}},\underline{\mathrm{id}}^{-1}}$-component we use the last corollary. ■

2.6.c Computation of $Z(E^*)^2$

Recall that in this subsection we want to prove that the inclusion $Z(E^*)^2 \subseteq Z_{E^0}(E^2)$ is actually an equality. This means proving that every element of E^1 centralizes $Z_{E^0}(E^2)$. As we know from Lemma 1.10.3 that E^1 is generated by β_1^-, β_1^+, $\beta^0_{s_0}$ and $\beta^0_{s_1}$ as an E^0-bimodule, it suffices to check that these four elements centralize $Z_{E^0}(E^2)$. Equivalently (looking at the definitions of $\beta^{0,\star}_{s_0}$ and $\beta^{0,\star}_{s_1}$), we see that β_1^-, β_1^+, $\beta^{0,\star}_{s_0}$ and $\beta^{0,\star}_{s_1}$ generate E^1 as an E^0-bimodule, and so we might instead check that these last four elements centralize $Z_{E^0}(E^2)$. This is a better choice because of the following lemma, whose proof can be derived from results in [OS21] without carrying out explicit computations.

Lemma 2.6.9. *Each element of* $\ker(g_1)$ *(in particular,* $\beta^{0,\star}_{s_0}$ *and* $\beta^{0,\star}_{s_1}$*) commutes with each element of* $Z_{E^0}(E^2)$*.*

Proof. In [OS21, Proposition 9.6] the multiplication between elements of $\ker(g_1)$ and elements of $\ker(g_2)$ is determined via the following commutative diagrams:

$$
\begin{tikzcd}
\ker(g_1) \times \ker(g_2) \arrow[r, "\text{multipl.}"] \arrow[d, "(\cong)\times(\cong)", "{\substack{(\beta_w^{0,\star},\alpha_v^{0,\star}) \\ \mapsto \\ (\tau_w, \tau_v^\vee|_{F^1E^0})}}"'] & E^3 \arrow[d, "{\substack{\phi_w \\ \mapsto \\ \tau_w^\vee}}", "\cong"'] \\
F^1E^0 \times {}^{\eth}\big((F^1E^0)^{\vee,\mathrm{finite}}\big)^{\eth} \arrow[r, "{(\tau,\alpha)\mapsto -\alpha(\eth(\tau)\cdot\_)}"'] & {}^{\eth}\big((E^0)^{\vee,\mathrm{finite}}\big)^{\eth},
\end{tikzcd}
\tag{109}
$$

and

$$
\begin{tikzcd}
\ker(g_2) \times \ker(g_1) \arrow[r, "\text{multipl.}"] \arrow[d, "(\cong)\times(\cong)", "{\substack{(\alpha_v^{0,\star},\beta_w^{0,\star}) \\ \mapsto \\ (\tau_v^\vee|_{F^1E^0}, \tau_w)}}"'] & E^3 \arrow[d, "{\substack{\phi_w \\ \mapsto \\ \tau_w^\vee}}", "\cong"'] \\
{}^{\eth}\big((F^1E^0)^{\vee,\mathrm{finite}}\big)^{\eth} \times F^1E^0 \arrow[r, "{(\alpha,\tau)\mapsto -\alpha(\_\cdot\eth(\tau))}"'] & {}^{\eth}\big((E^0)^{\vee,\mathrm{finite}}\big)^{\eth}.
\end{tikzcd}
\tag{110}
$$

Using the isomorphism ${}^{\partial}\big((F^1E^0)^{\vee,\mathrm{finite}}\big)^{\partial} \cong E^3/F_0E^3$ of Remark 2.6.2, we claim that we obtain the following commutative diagrams:

$$\begin{tikzcd}
\ker(g_1)\times\ker(g_2) \arrow[dd, "{(\cong)\times(\cong)}", "{(\beta_w^{0,\star},\alpha_v^{0,\star}) \mapsto (\tau_w,\overline{\phi_v})}"'] \arrow[dr, "\text{multipl.}"] & \\
& E^3, \\
F^1E^0\times E^3/F_0E^3 \arrow[ur, "{(\tau,\overline{\phi})\mapsto -\tau\cdot\phi}"'] &
\end{tikzcd} \tag{111}$$

and

$$\begin{tikzcd}
\ker(g_2)\times\ker(g_1) \arrow[dd, "{(\cong)\times(\cong)}", "{(\alpha_v^{0,\star},\beta_w^{0,\star}) \mapsto (\overline{\phi_v},\tau_w)}"'] \arrow[dr, "\text{multipl.}"] & \\
& E^3. \\
E^3/F_0E^3\times F^1E^0 \arrow[ur, "{(\overline{\phi},\tau)\mapsto -\phi\cdot\tau}"'] &
\end{tikzcd} \tag{112}$$

We check this for the first case, the second one being completely analogous. Let us work with the diagram (109): we first rewrite the map on the bottom as

$$\begin{aligned}
F^1E^0 \times {}^{\partial}\Big((F^1E^0)^{\vee,\mathrm{finite}}\Big)^{\partial} &\longrightarrow E^3 \\
(\tau, \tau_v^{\vee}\big|_{F^1E^0}) &\longmapsto -\tau_v^{\vee}\big|_{F^1E^0}(\partial(\tau)\cdot _) = -\tau_v^{\vee}(\partial(\tau)\cdot_) = -\tau\cdot\tau_v^{\vee}.
\end{aligned}$$

Hence the map obtained by composing the map on the bottom with the inverse of the map on the right (always of the diagram (109)) is

$$\begin{aligned}
F^1E^0 \times {}^{\partial}\Big((F^1E^0)^{\vee,\mathrm{finite}}\Big)^{\partial} &\longrightarrow {}^{\partial}\Big((E^0)^{\vee,\mathrm{finite}}\Big)^{\partial} \\
(\tau, \tau_v^{\vee}\big|_{F^1E^0}) &\longmapsto -\tau\cdot\phi_v.
\end{aligned}$$

Replacing ${}^{\partial}\big((F^1E^0)^{\vee,\mathrm{finite}}\big)^{\partial}$ with E^3/F_0E^3, we get a map

$$\begin{aligned}
F^1E^0\times E^3/F_0E^3 &\longrightarrow E^3 \\
(\tau,\overline{\phi_v}) &\longmapsto -\tau\cdot\phi_v.
\end{aligned}$$

Now, this is basically the map on the lower diagonal arrow of the diagram (111), except that here we are taking a specific representative for each element of E^3/F_0E^3, whereas in the map in the diagram we claimed that we could take arbitrary representatives. But this is allowed because looking at the explicit formulas for the action of E^0 on E^3 we see that multiplication by an element of F^1E^0 sends F_0E^3 to zero. This shows that the map on the lower diagonal arrow of the diagram (111) is well defined and that such diagram commutes.

Now, looking back at the statement of the lemma we want to prove, we see that using the diagrams (111) and (112) such statement can be rephrased as follows: for all $\tau\in F^1E^0$ and all $\overline{\phi}\in Z_{E^0}(E^3/F_0E^3)$ one has $-\tau\cdot\phi = -\phi\cdot\tau$. We recall that in Lemma 2.6.1 we have shown that each element of $Z_{E^0}(E^3/F_0E^3)$ admits a lift in $Z_{E^0}(E^3)$, and so the claim follows. ∎

In view of what we said before the lemma, it remains to prove that β_1^- and β_1^+ centralize $Z_{E^0}(E^2)$. After a preliminary remark about cup products, in the next lemma we will compute products between β_1^- (respectively, β_1^+) and elements of E^2.

Remark 2.6.10. Let $w \in \widetilde{W}$. Let us consider $(c^-, c^0, c^+)_w \in H^1(I, \mathbf{X}(w))$ and $(\alpha^-, \alpha^0, \alpha^+)_w \in H^1(I, \mathbf{X}(w))$. One has:

$$(\alpha^-, \alpha^0, \alpha^+)_w \smile (c^-, c^0, c^+)_w = \big\langle (\alpha^-, \alpha^0, \alpha^+), (c^-, c^0, c^+) \big\rangle \, \phi_w, \tag{113}$$

where $\langle \_, \_ \rangle$ denotes the natural component-wise pairing (recall that we are considering $\alpha^-, \alpha^+ \in \mathfrak{O}/\mathfrak{M} \otimes_{\mathbb{F}_p} k$ and $c^-, c^+ \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$, and that, if $\ell(w) \geqslant 1$, we are considering $\alpha^0 \in \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p} \otimes_{\mathbb{F}_p} k$ and $c^0 \in \mathrm{Hom}_{\mathbb{F}_p}\big(\frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p}, k\big)$).

Proof. Let us recall from (40) that ϕ_w is the unique element of $H^3(I, \mathbf{X}(w))$ such that

$$\Big(\eta \circ \mathcal{S}^d\Big)(\phi_w) = 1.$$

Therefore any other $\varphi \in H^d(I, \mathbf{X}(w))$ is such that

$$\varphi = \big(\eta \circ \mathcal{S}^d\big)(\varphi) \cdot \phi_w$$

(to show this it suffices to write φ as a scalar multiple of ϕ_w and applying the map $\eta \circ \mathcal{S}^d$ to determine the value of such scalar). In particular, since we know that $(\alpha^-, \alpha^0, \alpha^+)_w \smile (c^-, c^0, c^+)_w \in H^3(I, \mathbf{X}(w))$, we deduce that

$$(\alpha^-, \alpha^0, \alpha^+)_w \smile (c^-, c^0, c^+)_w = \big(\eta \circ \mathcal{S}^d\big)\big((\alpha^-, \alpha^0, \alpha^+)_w \smile (c^-, c^0, c^+)_w\big) \cdot \phi_w.$$

The explicit identification of $H^2(I, \mathbf{X}(w))$ with $H^1(I, \mathbf{X}(w))^\vee$ is, by construction, through the isomorphism

$$\begin{aligned} H^2(I, \mathbf{X}(w)) &\longrightarrow H^1(I, \mathbf{X}(w))^\vee \\ \alpha &\longmapsto \big(\eta \circ \mathcal{S}^d\big)(\alpha \smile \_), \end{aligned}$$

but then the value of $\big(\eta \circ \mathcal{S}^d\big)\big((\alpha^-, \alpha^0, \alpha^+)_w \smile (c^-, c^0, c^+)_w\big)$ is exactly the value of the natural pairing $\big\langle (\alpha^-, \alpha^0, \alpha^+), (c^-, c^0, c^+) \big\rangle$. ■

Lemma 2.6.11. *Let $w \in \widetilde{W}$. Let us consider $(c^-, 0, c^+)_1 \in H^1(I, \mathbf{X}(1))$ and let us consider $(\alpha^-, \alpha^0, \alpha^+)_w \in H^2(I, \mathbf{X}(w))$. One has:*

$$\begin{aligned} &(c^-, 0, c^+)_1 \cdot (\alpha^-, \alpha^0, \alpha^+)_w \\ &\qquad = \begin{cases} (\langle c^-, \alpha^- \rangle + \langle c^+, \alpha^+ \rangle)\, \phi_w & \text{if } w \in T^0/T^1, \\ \langle c^-, \alpha^- \rangle \phi_w & \text{if } w \notin T^0/T^1 \text{ and } \ell(s_1 w) = \ell(w) + 1, \\ \langle c^+, \alpha^+ \rangle \phi_w & \text{if } w \notin T^0/T^1 \text{ and } \ell(s_0 w) = \ell(w) + 1. \end{cases} \end{aligned} \tag{114}$$

Proof. Using the relation between (the opposite of) Yoneda product and cup product (Corollary 1.9.3) and since the cup product between an element of E^1 and an element of E^2 is commutative, we find that

$$\begin{aligned} (c^-, 0, c^+)_1 \cdot (\alpha^-, \alpha^0, \alpha^+)_w &= \big((c^-, 0, c^+)_1 \cdot \tau_w\big) \smile \big(\tau_1 \cdot (\alpha^-, \alpha^0, \alpha^+)_w\big) \\ &= (\alpha^-, \alpha^0, \alpha^+)_w \smile \big((c^-, 0, c^+)_1 \cdot \tau_w\big). \end{aligned}$$

Thanks to the formulas (65) for the right action of E^0 on E^1 the term on the right can be computed as

$$(c^-,0,c^+)_1\cdot\tau_w=\begin{cases}(c^-,0,c^+)_w & \text{if } w\in T^0/T^1,\\ (c^-,0,0)_w & \text{if } w\notin T^0/T^1 \text{ and } \ell(s_1w)=\ell(w)+1,\\ (0,0,c^+)_w & \text{if } w\notin T^0/T^1 \text{ and } \ell(s_0w)=\ell(w)+1.\end{cases}$$

Now we can compute the cup product above using the explicit formula (113), finding that

$$\begin{aligned}(c^-,0,c^+)_1\cdot(\alpha^-,\alpha^0,\alpha^+)_w &= (\alpha^-,\alpha^0,\alpha^+)_w\smile\big((c^-,0,c^+)_1\cdot\tau_w\big)\\ &=\begin{cases}(\langle c^-,\alpha^-\rangle+\langle c^+,\alpha^+\rangle)\,\phi_w & \text{if } w\in T^0/T^1,\\ \langle c^-,\alpha^-\rangle\phi_w & \text{if } w\notin T^0/T^1 \text{ and } \ell(s_1w)=\ell(w)+1,\\ \langle c^+,\alpha^+\rangle\phi_w & \text{if } w\notin T^0/T^1 \text{ and } \ell(s_0w)=\ell(w)+1.\end{cases}\end{aligned}$$

■

Proposition 2.6.12. *One has that the inclusion $Z(E^*)^2\subseteq Z_{E^0}(E^2)$ is actually an equality, and furthermore $Z_{E^0}(E^2)$ is isomorphic to $Z_{E^0}(E^3)/F_0E^3$ as a $Z(E^0)$-bimodule, and an explicit k-basis is given in Corollary 2.6.8.*

Proof. It remains to check the first statement, the second one having been proved in Corollary 2.6.3 and the third one in Corollary 2.6.8. We have already explained at the beginning of this subsection that it suffices to check that the four elements β_1^-, β_1^+, $\beta_{s_0}^{0,\star}$ and $\beta_{s_1}^{0,\star}$ centralize $Z_{E^0}(E^2)$, and the last two elements have already been dealt with in Lemma 2.6.9. Hence, it only remains to check that the elements of the k-basis computed in Corollary 2.6.8 commute with β_1^- and β_1^+. To compute these products we use Lemma 2.6.11: for all $w\in\widetilde{W}\smallsetminus\big(T^0/T^1\big)$, one has

$$\begin{aligned}&\beta_1^-\cdot\alpha_w^0=0,\\ &\beta_1^+\cdot\alpha_w^0=0,\\ &\alpha_w^0\cdot\beta_1^-=\mathcal{J}\left(\beta_1^-\cdot(-1)^{\ell(w)}\alpha_{w^{-1}}^0\right)=0,\\ &\alpha_w^0\cdot\beta_1^+=\mathcal{J}\left(\beta_1^+\cdot(-1)^{\ell(w)}\alpha_{w^{-1}}^0\right)=0.\end{aligned}$$

It follows immediately that the commutators $[\beta_1^-,\alpha]$ and $[\beta_1^+,\alpha]$ are both equal to zero for α equal to one of the following elements of our k-basis of $Z_{E^0}(E^2)$:

$$\begin{aligned}&-e_1\alpha_{s_0}^0, \qquad -e_{\chi_0}\alpha_{s_0}^0, \qquad e_1\alpha_{s_1}^0, \qquad e_{\chi_0}\alpha_{s_1}^0,\\ &e_\lambda\alpha^0_{(s_1s_0)^i}-e_{\lambda^{-1}}\alpha^0_{(s_0s_1)^i}\\ &\qquad\text{for } i\in\mathbb{Z}_{\geqslant 1} \text{ and for } \lambda\in\widehat{T^0/T^1}\smallsetminus\{1,\underline{\mathrm{id}}\},\\ &e_1\alpha^0_{(s_1s_0)^i}-e_1\alpha^0_{(s_0s_1)^i}-e_1\alpha^0_{s_1(s_0s_1)^i}+e_1\alpha^0_{s_0(s_1s_0)^i}\\ &\qquad\text{for } i\in\mathbb{Z}_{\geqslant 1}.\end{aligned}$$

It remains to compute the commutators $[\beta_1^-,\alpha]$ and $[\beta_1^+,\alpha]$ where

$$\begin{aligned}\alpha := {}& e_{\underline{\mathrm{id}}}\alpha^0_{(s_1s_0)^i}-e_{\underline{\mathrm{id}}^{-1}}\alpha^0_{(s_0s_1)^i}\\ &+2\sum_{j=0}^{i-1}\left(e_{\underline{\mathrm{id}}}\alpha^-_{s_1(s_0s_1)^j}-e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_1(s_0s_1)^j}-e_{\underline{\mathrm{id}}}\alpha^-_{s_0(s_1s_0)^j}+e_{\underline{\mathrm{id}}^{-1}}\alpha^+_{s_0(s_1s_0)^j}\right)\end{aligned}$$

for $i \in \mathbb{Z}_{\geqslant 1}$. Since the first two terms do not contribute to the computation of the commutator, it suffices to prove that the commutators $\left[\beta_1^-, e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right]$ and $\left[\beta_1^+, e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right]$ are both zero for w of the form $s_1(s_0s_1)^j$ or $s_0(s_1s_0)^j$ (for $j \in \mathbb{Z}_{\geqslant 0}$). Using the formulas (57), (81) and (45) for the involutive anti-automorphism $\mathcal{J}$ and the formulas of Lemma 2.6.11 for the left action of β_1^- and β_1^+ on E^2 we compute

$$\begin{aligned}
\alpha_w^- \cdot \beta_1^- &= \mathcal{J}\left(\mathcal{J}(\beta_1^-)\cdot\mathcal{J}(\alpha_w^-)\right) = \mathcal{J}\left(\beta_1^-\cdot(-\alpha_{w^{-1}}^+)\right) = 0,\\
\alpha_w^+ \cdot \beta_1^- &= \mathcal{J}\left(\mathcal{J}(\beta_1^-)\cdot\mathcal{J}(\alpha_w^+)\right) = \mathcal{J}\left(\beta_1^-\cdot(-\alpha_{w^{-1}}^-)\right) = \mathcal{J}(-\phi_{w^{-1}}) = -\phi_w,\\
\alpha_w^- \cdot \beta_1^+ &= \mathcal{J}\left(\mathcal{J}(\beta_1^+)\cdot\mathcal{J}(\alpha_w^-)\right) = \mathcal{J}\left(\beta_1^+\cdot(-\alpha_{w^{-1}}^+)\right) = \mathcal{J}(-\phi_{w^{-1}}) = -\phi_w,\\
\alpha_w^+ \cdot \beta_1^+ &= \mathcal{J}\left(\mathcal{J}(\beta_1^+)\cdot\mathcal{J}(\alpha_w^+)\right) = \mathcal{J}\left(\beta_1^+\cdot(-\alpha_{w^{-1}}^-)\right) = 0.
\end{aligned}$$

We are now able to compute both $\left[\beta_1^-, e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right]$ and $\left[\beta_1^+, e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right]$, also making use of the formulas (61) for the left and right action of the idempotents on E^1. Let us start with the former commutator: one has

$$\begin{aligned}
&\beta_1^- \cdot \left(e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right) = e_{\underline{\mathrm{id}}^{-1}}\beta_1^-\cdot\alpha_w^- - e_{\underline{\mathrm{id}}^{-3}}\beta_1^-\cdot\alpha_w^+ = e_{\underline{\mathrm{id}}^{-1}}\phi_w,\\
&\left(e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right)\cdot\beta_1^- = -e_{\underline{\mathrm{id}}^{-1}}\cdot(-\phi_w) = e_{\underline{\mathrm{id}}^{-1}}\phi_w,
\end{aligned}$$

and hence the former commutator is zero. Similarly, for the latter commutator one has

$$\begin{aligned}
&\beta_1^+ \cdot \left(e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right) = e_{\underline{\mathrm{id}}^{3}}\beta_1^+\cdot\alpha_w^- - e_{\underline{\mathrm{id}}}\beta_1^+\cdot\alpha_w^+ = -e_{\underline{\mathrm{id}}}\phi_w,\\
&\left(e_{\underline{\mathrm{id}}}\alpha_w^- - e_{\underline{\mathrm{id}}^{-1}}\alpha_w^+\right)\cdot\beta_1^+ = -e_{\underline{\mathrm{id}}}\phi_w,
\end{aligned}$$

and hence the latter commutator is zero as well. ■

2.7 Structure of the 2^{nd} graded piece of the centre as a $Z(E^0)$-module

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$.

Since we know from Proposition 2.6.12 that $Z(E^*)^2 = Z_{E^0}(E^2)$, it follows that $Z(E^*)^2$ has a natural structure of $Z(E^0)$-module. Moreover, from the same proposition we know that $Z_{E^0}(E^2)$ is isomorphic to $Z_{E^0}(E^3)/F_0E^3$ as a $Z(E^0)$-bimodule. Since we know the structure of $Z_{E^0}(E^3)$ as a $Z(E^0)$-module explicitly, it will then be easy to describe the structure of such quotient.

Recall the decomposition $Z(E^0) = \prod_{\gamma\in\Gamma} e_\gamma Z(E^0)$ and the description of the components $e_\gamma Z(E^0)$ stated in Section 1.7, which we already used for the description of $Z(E^*)^3$ in Section 2.3. As in Section 2.3, we distinguish the components relative to the idempotents e_1, e_{χ_0} (where χ_0 is the quadratic character) and e_γ for $\gamma \in \Gamma$ of cardinality 2.

- Recall from Lemma 2.3.2 that, identifying $e_1 Z(E^0)$ with the polynomial ring $k[X_1]$

as in Lemma 1.7.1, one has the following isomorphism of $k[X_1]$-modules:

$$\begin{aligned}
\frac{k[X_1]}{(X_1-1)} \oplus \frac{k[X_1]}{(X_1)} \oplus \frac{k[X_1, X_1^{-1}]}{k[X_1]} &\xrightarrow{\quad\cong\quad} e_1 Z(E^*)^3 \\
(\overline{1}, 0, 0) &\longmapsto e_1\phi_1, \\
(0, \overline{1}, 0) &\longmapsto e_1\phi_{s_0} - e_1\phi_{s_1}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(0, 0, \overline{X_1^{-i}}\right)} &\longmapsto U_{1,i-1},
\end{aligned}$$

where $U_{1,i-1} \coloneqq e_1\phi_{(s_1s_0)^{i-1}} + e_1\phi_{(s_0s_1)^{i-1}} - e_1\phi_{s_1(s_0s_1)^{i-1}} - e_1\phi_{s_0(s_1s_0)^{i-1}}$. Now, from the isomorphism $Z_{E^0}(E^3)/F_0E^3 \xrightarrow{\cong} Z_{E^0}(E^2)$ we obtain an isomorphism

$$e_1Z_{E^0}(E^3)/e_1F_0E^3 \xrightarrow{\cong} e_1Z_{E^0}(E^2),$$

of which we know an explicit description (compare Remark 2.6.2). It is then easy to compute that we have an isomorphism

$$\begin{aligned}
\frac{k[X_1]}{(X_1)} \oplus \frac{k[X_1, X_1^{-1}]}{k[X_1]} &\xrightarrow{\quad\cong\quad} e_1 Z(E^*)^2 \\
(0, \overline{1}, 0) &\longmapsto e_1\alpha_{s_0}^{0,\star} - e_1\alpha_{s_1}^{0,\star}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(0, 0, \overline{X_1^{-i}}\right)} &\longmapsto V_{1,i-1},
\end{aligned}$$

where

$$V_{1,i-1} \coloneqq \begin{cases} e_1\alpha^{0,\star}_{(s_1s_0)^{i-1}} + e_1\alpha^{0,\star}_{(s_0s_1)^{i-1}} - e_1\alpha^{0,\star}_{s_1(s_0s_1)^{i-1}} - e_1\alpha^{0,\star}_{s_0(s_1s_0)^{i-1}} & \text{if } i \geqslant 2, \\ -e_1\alpha^{0,\star}_{s_1} - e_1\alpha^{0,\star}_{s_0} & \text{if } i = 1. \end{cases}$$

- Recall from Lemma 2.3.3 that, identifying $e_{\chi_0}Z(E^0)$ with the polynomial ring $k[X_{\chi_0}]$ as in Lemma 1.7.1, one has the following isomorphism of $k[X_{\chi_0}]$-modules:

$$\begin{aligned}
\frac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \frac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \frac{k[X_{\chi_0}, X_{\chi_0}^{-1}]}{k[X_{\chi_0}]} &\xrightarrow{\quad\cong\quad} e_{\chi_0} Z(E^*)^3 \\
(\overline{1}, 0, 0) &\longmapsto e_{\chi_0}\phi_{s_0}, \\
(0, \overline{1}, 0) &\longmapsto e_{\chi_0}\phi_{s_1}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(0, 0, \overline{X_{\chi_0}^{-i}}\right)} &\longmapsto U_{\chi_0,i-1},
\end{aligned}$$

where $U_{\chi_0,i-1} \coloneqq e_{\chi_0}\phi_{(s_1s_0)^{i-1}} + e_{\chi_0}\phi_{(s_0s_1)^{i-1}}$. Proceeding as for the $e_1Z(E^0)$-

component, we find the following isomorphism:

$$\begin{array}{rcl}
\dfrac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \dfrac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \dfrac{k[X_{\chi_0}, X_{\chi_0}^{-1}]}{k[X_{\chi_0}] \cdot X_{\chi_0}^{-1}} & \xrightarrow{\ \cong\ } & e_{\chi_0} Z(E^*)^2 \\
(\overline{1}, 0, 0) & \longmapsto & e_{\chi_0} \alpha_{s_0}^{0,\star}, \\
(0, \overline{1}, 0) & \longmapsto & e_{\chi_0} \alpha_{s_1}^{0,\star}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 2})}{\left(0, 0, \overline{X_{\chi_0}^{-i}}\right)} & \longmapsto & V_{\chi_0, i-1},
\end{array}$$

where $V_{\chi_0,i-1} \coloneqq e_{\chi_0} \alpha^{0,\star}_{(s_1 s_0)^{i-1}} + e_{\chi_0} \alpha^{0,\star}_{(s_0 s_1)^{i-1}}$.

With a shifting of the indices, we also get

$$\frac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \frac{k[X_{\chi_0}]}{(X_{\chi_0})} \oplus \frac{k[X_{\chi_0}, X_{\chi_0}^{-1}]}{k[X_{\chi_0}]} \cong e_{\chi_0} Z(E^*)^2.$$

- Now let us treat the e_γ-component for $\gamma = \{\lambda, \lambda^{-1}\} \in \Gamma$ of cardinality 2. As in Lemma 1.7.1 we identify $e_\gamma Z(E^0)$ with the ring $\frac{k[X_\lambda, X_{\lambda^{-1}}]}{(X_\lambda \cdot X_{\lambda^{-1}})}$, where X_λ and $X_{\lambda^{-1}}$ are indeterminates. For the moment let us use the letters X and Y for such indeterminates to simplify notation; recall that in order to describe $e_\gamma Z(E^*)^3$ we considered the injective hull of $k = \frac{k[X,Y]}{(X,Y)}$ as a $\frac{k[X,Y]}{(X \cdot Y)}$-module, which we denoted by
$$\mathcal{E}_{\frac{k[X,Y]}{(X\cdot Y)}}(k).$$
We showed that it admits the following k-basis (see (103))
$$\begin{array}{ll}
(1)^\vee, & \\
(X^i)^\vee & \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
(Y^i)^\vee & \text{for } i \in \mathbb{Z}_{\geqslant 1},
\end{array}$$
basis which satisfies the following formulas (see (104)):
$$\begin{array}{rll}
X \cdot (1)^\vee = 0, & & \\
Y \cdot (1)^\vee = 0, & & \\
X \cdot (X^i)^\vee = (X^{i-1})^\vee & \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
Y \cdot (X^i)^\vee = 0 & \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
X \cdot (Y^i)^\vee = 0 & \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
Y \cdot (Y^i)^\vee = (Y^{i-1})^\vee & \text{for } i \in \mathbb{Z}_{\geqslant 1}.
\end{array} \tag{115}$$
Now, let us recall the description of $e_\gamma Z(E^*)^3$ from Lemma 2.3.4: we have the

following isomorphism of $\frac{k[X_\lambda, X_{\lambda-1}]}{(X_\lambda \cdot X_{\lambda-1})}$-modules:

$$\begin{aligned}
k \oplus \mathcal{E}_{\frac{k[X_\lambda, X_{\lambda-1}]}{(X_\lambda \cdot X_{\lambda-1})}}(k) &\xrightarrow{\quad\cong\quad} e_\gamma Z(E^*)^3 \\
(1,0) &\longmapsto e_\lambda \phi_1 - e_{\lambda^{-1}} \phi_1, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\big(0, (X_\lambda^i)^\vee\big)} &\longmapsto U_{\lambda,i}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\big(0, (X_{\lambda-1}^i)^\vee\big)} &\longmapsto U_{\lambda^{-1},i}, \\
\big(0, (1)^\vee\big) &\longmapsto U_{\lambda,0} = U_{\lambda^{-1},0},
\end{aligned}$$

where for $\mu \in \{\lambda, \lambda^{-1}\}$ and $i \in \mathbb{Z}_{\geqslant 0}$ we had

$$U_{\mu,i} := e_\mu \phi_{(s_1 s_0)^i} + e_{\mu^{-1}} \phi_{(s_0 s_1)^i}.$$

Therefore, with the same argument as for the previous components, we get an isomorphism

$$\begin{aligned}
\Big(\mathcal{E}_{\frac{k[X_\lambda, X_{\lambda-1}]}{(X_\lambda \cdot X_{\lambda-1})}}(k)\Big)/\big(k \cdot (1)^\vee\big) &\xrightarrow{\ \cong\ } e_\gamma Z(E^*)^2 \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\overline{(X_\lambda^i)^\vee}} &\longmapsto V_{\lambda,i}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\overline{(X_{\lambda-1}^i)^\vee}} &\longmapsto V_{\lambda^{-1},i},
\end{aligned}$$

where for $\mu \in \{\lambda, \lambda^{-1}\}$ and $i \in \mathbb{Z}_{\geqslant 1}$ we define

$$V_{\mu,i} := e_\mu \alpha^{0,\star}_{(s_1 s_0)^i} + e_{\mu^{-1}} \alpha^{0,\star}_{(s_0 s_1)^i}.$$

By the formulas (115), we see that the quotient $\Big(\mathcal{E}_{\frac{k[X,Y]}{(X \cdot Y)}}(k)\Big)/\big(k \cdot (1)^\vee\big)$ can be described in a much simpler way, namely as

$$\begin{aligned}
\frac{k[X, X^{-1}]}{k[X]} \oplus \frac{k[Y, Y^{-1}]}{k[Y]} &\xrightarrow{\ \cong\ } \Big(\mathcal{E}_{\frac{k[X,Y]}{(X \cdot Y)}}(k)\Big)/\big(k \cdot (1)^\vee\big) \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\big(\overline{(X^{-i})^\vee}, 0\big)} &\longmapsto \overline{(X^i)^\vee}, \\
\underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\big(0, \overline{(Y^{-i})^\vee}\big)} &\longmapsto \overline{(Y^i)^\vee},
\end{aligned}$$

where we see the first direct summand as a $k[X, Y]$-module by declaring that X acts in the obvious way and that Y acts by zero, and symmetrically for the second direct summand. Hence, we obtain an isomorphism

$$\begin{array}{ccc} \dfrac{k[X_\lambda, X_\lambda^{-1}]}{k[X_\lambda]} \oplus \dfrac{k[X_{\lambda^{-1}}, X_{\lambda^{-1}}^{-1}]}{k[X_{\lambda^{-1}}]} & \xrightarrow{\cong} & e_\gamma Z(E^*)^2 \\ \underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(\overline{(X_\lambda^{-i})^\vee}, 0\right)} & \longmapsto & V_{\lambda,i}, \\ \underset{(\text{for } i \in \mathbb{Z}_{\geqslant 1})}{\left(0, \overline{(X_{\lambda^{-1}}^{-i})^\vee}\right)} & \longmapsto & V_{\lambda^{-1},i}. \end{array}$$

For the next two remarks, let us assume again that $\gamma = \{\lambda, \lambda^{-1}\} \in \Gamma$ is of cardinality 2, and let us denote by M_λ and $M_{\lambda^{-1}}$ the two direct summands of $e_\gamma Z(E^*)^2$ corresponding respectively to $\frac{k[X_\lambda, X_\lambda^{-1}]}{k[X_\lambda]}$ and to $\frac{k[X_{\lambda^{-1}}, X_{\lambda^{-1}}^{-1}]}{k[X_{\lambda^{-1}}]}$ via the above isomorphism.

Remark 2.7.1. With notation as above, neither M_λ, nor $M_{\lambda^{-1}}$, nor the whole $e_\gamma Z(E^*)^2$ are injective $e_\gamma Z(E^0)$-modules.

Proof. Since a direct summand of an injective module is injective as well, it suffices to show that the $k[X,Y]/(X \cdot Y)$-module $k[X, X^{-1}]/k[X]$ is not injective. It is easy to see that the following homomorphism of k-vector spaces is also an homomorphism of $k[X,Y]/(X \cdot Y)$-modules:

$$\begin{array}{ccc} \dfrac{(X,Y)k[X,Y]}{(X \cdot Y)} & \longrightarrow & \dfrac{k[X,X^{-1}]}{k[X]} \\ \underset{(\text{for all } i \in \mathbb{Z}_{\geqslant 1})}{\overline{X^i}} & \longmapsto & 0, \\ \overline{Y} & \longmapsto & \overline{X^{-1}}, \\ \underset{(\text{for all } i \geqslant 2)}{\overline{Y^i}} & \longmapsto & 0. \end{array}$$

Assume by contradiction that there exists a homomorphism of $k[X,Y]/(X \cdot Y)$-modules

$$\varphi \colon \frac{k[X,Y]}{(X \cdot Y)} \longrightarrow \frac{k[X,X^{-1}]}{k[X]}$$

extending the one above. Then one has

$$0 = Y \cdot \varphi(\overline{1}) = \varphi(\overline{Y}) = \overline{X^{-1}} \neq 0,$$

and this contradiction concludes the proof. ∎

Remark 2.7.2. With notation as above, M_λ is an injective module over the ring

$$R_\lambda \coloneqq \frac{e_\gamma Z(E^0)}{\mathrm{Ann}_{e_\gamma Z(E^0)}(M_\lambda)}$$

(and the analogous result holds for M_λ^{-1}). More precisely, M_λ is the injective hull of k as a module over the ring R_λ (where $\overline{x_\lambda}$ acts by zero on k).

Proof. Using our fixed isomorphism $k[X_\lambda, X_{\lambda^{-1}}]/(X_\lambda \cdot X_{\lambda^{-1}}) \cong e_\gamma Z(E^0)$, and denoting by X and Y the indeterminates X_λ and $X_{\lambda^{-1}}$ respectively in order to simplify notation, one has:

$$R_\lambda = \frac{e_\gamma Z(E^0)}{\mathrm{Ann}_{e_\gamma Z(E^0)}(M_\lambda)} \cong \frac{\dfrac{k[X,Y]}{(X \cdot Y)}}{\mathrm{Ann}_{\frac{k[X,Y]}{(X\cdot Y)}}\left(\dfrac{k[X,X^{-1}]}{k[X]}\right)} = \frac{\dfrac{k[X,Y]}{(X \cdot Y)}}{\dfrac{(Y)}{(X \cdot Y)}} \cong k[X],$$

and $\frac{k[X,X^{-1}]}{k[X]}$ is the injective hull of k as a module over $k[X]$ (where X acts by zero on k), as explained in [Lam12, Proposition 3.91.(1)]. ■

2.8 Multiplicative structure of $Z(E^*)$

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). To use results proved in the previous sections we may assume without loss of generality that $\pi = p$ (there is no loss of generality because our statements will be independent of such choice, while in the previous sections computations and explicit formula for bases could depend on it). In Remark 2.8.2 we will work under more general assumptions.

Since $Z(E^*)^1 = 0$, the multiplicative structure of $Z(E^*)$ is very simple: describing the multiplication amounts to describing the multiplication on $Z(E^*)^0$ and to describing $Z(E^*)^2$ and $Z(E^*)^3$ as $Z(E^*)^0$-modules. Recall from Proposition 2.4.1 that $Z(E^*)^0$ can be described as

$$\begin{aligned} k \times k &\xrightarrow{\ \cong\ } Z(E^*)^0 \\ (1,0) &\longmapsto \frac{1}{2}\left(\tau_1 + \tau_{c_{-1}}\right), \\ (0,1) &\longmapsto \frac{1}{2}\left(\tau_1 - \tau_{c_{-1}}\right). \end{aligned}$$

It remains to describe $Z(E^*)^2$ and $Z(E^*)^3$ as $Z(E^*)^0$-modules.

Remark 2.8.1. Both $Z(E^*)^2$ and $Z(E^*)^3$ are free $Z(E^*)^0$-modules of rank $\aleph_0$.

Proof. Let $i = 2$ or $i = 3$. For all $\{\lambda, \lambda^{-1}\} \in \Gamma$, one has that $\tau_{c_{-1}}$ acts on the component $e_{\{\lambda,\lambda^{-1}\}} Z(E^*)^i$ by multiplication by $\lambda(c_{-1}) \in \{1, -1\}$. Let us identify $Z(E^*)^0$ with $k \times k$ via the above isomorphism: then $k \times 0$ is the unique $Z(E^*)^0$-module of dimension 1 over k such that $\tau_{c_{-1}}$ acts by 1, while $0 \times k$ is the unique $Z(E^*)^0$-module of dimension 1 over k such that $\tau_{c_{-1}}$ acts by -1.

Now, let us choose a k-basis of $e_{\{\lambda,\lambda^{-1}\}} Z(E^*)^i$: by the explicit description of this submodule we know that such basis has cardinality $\aleph_0$ (see Lemma 2.3.1 and Proposition 2.6.12). Combining this with the above remarks about the action of $\tau_{c_{-1}}$, we see that $e_{\{\lambda,\lambda^{-1}\}} Z(E^*)^i$ is either isomorphic to $\bigoplus_{n \in \mathbb{Z}_{\geqslant 0}} (k \times 0)$ or to $\bigoplus_{n \in \mathbb{Z}_{\geqslant 0}} (0 \times k)$ as a module over the ring $k \times k \cong Z(E^*)^0$. Therefore

$$Z(E^*)^i \cong \Big(\bigoplus_{j \in J_1} (k \times 0)\Big) \oplus \Big(\bigoplus_{j \in J_2} (0 \times k)\Big),$$

for suitable sets J_1 and J_2 that are either empty or of cardinality $\aleph_0$. Since there exists at least one $\lambda \in \widehat{T^0/T^1}$ such that $\lambda(c_{-1}) = 1$ (e.g., $\lambda = 1$) and at least one

$\lambda \in \widehat{T^0/T^1}$ such that $\lambda(c_{-1}) = -1$ (e.g., $\lambda = \underline{\mathrm{id}}$), we conclude that both J_1 and J_2 have cardinality $\aleph_0$, and so $Z(E^*)^i$ is free as a module of rank $\aleph_0$ over the ring $k \times k \cong Z(E^*)^0$. ■

Remark 2.8.2. Under the more general assumptions that $G = \mathrm{SL}_2(\mathfrak{F})$ (with the usual fixed choices as in Section 1.5), that I is torsion-free and that $\mathbb{F}_q \subseteq k$, the same proof shows that $Z(E^*)^d$ is a free $Z(E^*)^0$-module of rank $\aleph_0$ (recall that d denotes the dimension of G as an analytic manifold over $\mathbb{Q}_p$).

Chapter 3

The Ext-algebra for more general groups: low graded pieces of the centre and other remarks

This chapter is mainly devoted to understanding the 0^{th} and 1^{st} graded pieces of the centre for general groups G. We achieve the following results.

- In Section 3.1 we completely determine the 0^{th} graded piece of the centre without further assumptions.
- In Section 3.2 we completely determine the 1^{st} graded piece of the centre under the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$.

Furthermore, the final Section 3.3 is devoted to extending to the Ext-algebras the following result about pro-p Iwahori–Hecke algebras: denoting by T^+ is the sub-monoid of T consisting of the elements t such that $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant 0$ for all $\alpha \in \Pi$, one has an injective homomorphism of k-algebras

$$\begin{aligned} k[T^+/T^1] &\longrightarrow H \\ (t) &\longmapsto \tau_t. \end{aligned}$$

3.1 The 0^{th} graded piece of the centre

Assumptions. We put ourselves in the general assumptions of Section 1.1, without any restriction on $\mathbf{G}$ and $\mathfrak{F}$.

In this section we will describe the 0^{th} graded piece of the centre of the Ext-algebra E^*. The first subsection contains the main statement, while the second subsection deals with the proofs.

3.1.a Statement

Recall from Section 1.2 that we denote by $\mathbf{C}$ the centre of $\mathbf{G}$ (meaning the whole centre, not just its identity component). As usual, we denote by C its group of $\mathfrak{F}$-rational points. Recall from [Mil17, Proposition 17.71 (b)] that $\mathbf{C}$ is contained in $\mathbf{T}$, and hence C is contained in T. As a side remark, note that C is the centre of

G: indeed if an element $g \in G$ centralizes the whole G, then $G \subseteq C_{\mathbf{G}}(g)(\mathfrak{F})$, where $C_{\mathbf{G}}(g)$ is the schematic centralizer of g in $\mathbf{G}$. But $C_{\mathbf{G}}(g)$ is a closed subscheme of $\mathbf{G}$ (see [Mil17, Proposition 1.79]), and G is schematically dense in $\mathbf{G}$ (see [Mil17, Theorem 17.93]), and hence we conclude that $\mathbf{G} = C_{\mathbf{G}}(g)$, i.e., that $g \in \mathbf{C}(\mathfrak{F}) = C$.

We will now state the theorem describing the 0^{th} graded piece of the centre of the Ext-algebra. We will prove it in the next subsection, splitting the argument into various lemmas.

Theorem (see Theorem 3.1.10). *Let us define*

$$\widetilde{C} := (C \cdot T^1)/T^1.$$

One has the following facts:

- *One has the following isomorphism of k-algebras describing the 0^{th} graded piece of the centre of E^*:*

$$\begin{array}{ccc} k[\widetilde{C}] & \longrightarrow & Z(E^*)^0 \\ \underset{(\text{with } c \in \widetilde{C})}{(c)} & \longmapsto & \tau_c. \end{array}$$

- *The obvious inclusion $Z(E^*)^0 \subseteq Z_{E^0 \cup H^1(I,\mathbf{X}(1))}(E^0)$ is actually an equality.*

- *$\widetilde{C}$ is a subgroup of $\widetilde{\Omega} \cap T/T^1$ and it can also be described as*

$$\widetilde{C} = \{t \in T \ \mid \ \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\}/T^1.$$

  Moreover, in the obvious isomorphism $C/(C \cap T^1) \cong (C \cdot T^1)/T^1 = \widetilde{C}$, the group $C \cap T^1$ can be described as the (unique) pro-p Sylow subgroup of the unique maximal compact subgroup of C.

We complement this theorem with a few remarks: namely, we discuss the fact that the inclusion $\widetilde{C} \subseteq Z(\widetilde{W})$ is not an equality in general, we discuss $Z(E^*)^0$ for the groups SL_n and GL_n, and we determine when $Z(E^*)^0$ is "trivial" (i.e., just equal to k).

Remark (see Remark 3.1.11). The inclusion $\widetilde{C} \subseteq Z(\widetilde{W})$ might be strict in general, but it is an equality if the order of the fundamental group of the derived group of $\mathbf{G}$ is not divisible by 2.

Example 3.1.1. We briefly discuss the examples $\mathbf{G} = \mathrm{SL}_n$ and $\mathbf{G} = \mathrm{GL}_n$.

- Let $\mathbf{G} = \mathrm{SL}_n$, for $n \in \mathbb{Z}_{\geqslant 2}$. One has $C \cong \boldsymbol{\mu}_n(\mathfrak{F})$. By the theorem we know that we have an isomorphism $Z(E^*)^0 \cong k\left[C/(C \cap T^1)\right]$, and that $(C \cap T^1)$ is the p-Sylow subgroup of C. It follows that

$$Z(E^*)^0 \cong k\left[\boldsymbol{\mu}_n(\mathbb{F}_q)\right] \cong k[X]/(X^{\gcd(n,q-1)} - 1).$$

  In particular, if $\mathbb{F}_q \subseteq k$, then $Z(E^*)^0 \cong \prod_{i=1}^{\gcd(n,q-1)} k$.

- Let $\mathbf{G} = \mathrm{GL}_n$, for $n \in \mathbb{Z}_{\geqslant 1}$. One has $C \cong \mathfrak{F}^\times \cong \mathbb{Z} \times \mathbb{F}_q^\times \times (1 + \mathfrak{M})$. Again we use the isomorphism $Z(E^*)^0 \cong k\left[C/(C \cap T^1)\right]$, together with the description of $C \cap T^1$ as the pro-p Sylow subgroup of the unique maximal compact subgroup of $\mathfrak{O}$, and we get

$$Z(E^*)^0 \cong k\left[\mathbb{Z} \times \mathbb{F}_q^\times\right] \cong k[X, X^{-1}, Y]/(Y^{q-1} - 1).$$

  In particular, if $\mathbb{F}_q \subseteq k$, then $Z(E^*)^0 \cong \prod_{i=1}^{q-1} k[X, X^{-1}]$.

Remark 3.1.2. The inclusion $k \subseteq Z(E^*)^0$ is an equality if and only if $\mathbf{G}$ has finite centre $\mathbf{C}$ of order coprime with $q-1$ (compare also the example of SL_n above).

Proof. As in the above examples, it is useful to work with the description

$$Z(E^*)^0 \cong k\left[C/(C \cap T^1)\right].$$

Since $\mathbf{C}$ is contained in a split torus, it must have the following form (see [Mil17, Proposition 12.3 and Theorem 12.9]):

$$\mathbf{C} \cong \mathbb{G}_{\mathrm{m}}^r \times \boldsymbol{\mu}_{n_1} \times \cdots \times \boldsymbol{\mu}_{n_m}$$

for some $r, m \in \mathbb{Z}_{\geqslant 0}$ and some $n_1, \dots, n_m \in \mathbb{Z}_{\geqslant 1}$. Making use of the fact that $\mathfrak{F}^\times = \pi^{\mathbb{Z}} \times \boldsymbol{\mu}_{q-1}(\mathfrak{F}) \times (1 + \mathfrak{M})$ with $\boldsymbol{\mu}_{q-1}(\mathfrak{F}) \cong \mathbb{F}_q^\times$ and of the fact that $C \cap T^1$ can is the pro-p Sylow subgroup of the unique maximal compact subgroup of C, it is easy to see that

$$C/(C \cap T^1) \cong \mathbb{Z}^r \times ((\mathbb{F}_q)^\times)^r \times \boldsymbol{\mu}_{n_1}(\mathbb{F}_q) \times \cdots \times \boldsymbol{\mu}_{n_m}(\mathbb{F}_q),$$

and so $C/(C \cap T^1)$ is trivial if and only if $r = 0$ and $n_1, \dots, n_m$ are coprime with $q-1$. ■

3.1.b Proofs

Recall from Theorem 1.6.1 that the centre of E^0 has the following k-basis:

$$z_{\mathcal{O}} := \sum_{x \in \mathcal{O}} B_o(x) \qquad \text{for all the } W_0\text{-orbits } \mathcal{O} \subseteq T/T^1, \tag{116}$$

where o is a fixed spherical orientation and where $(B_o(w))_{w \in \widetilde{W}}$ denotes the associated Bernstein basis.

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

$$B_o(w) - \tau_w \in \bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) < \ell(w)}} k\tau_v.$$

This is easy to see: indeed, following [Vig16, Proof of Corollary 5.26] let us write $w = \widetilde{s}_1 \cdots \widetilde{s}_{\ell(w)}\omega$ for suitable $s_1, \dots, s_{\ell(w)} \in S_{\mathrm{aff}}$ and $\omega \in \widetilde{\Omega}$; from the definition of the Bernstein basis, or more generally of the alcove walk basis, one sees that $B_o(w) - \tau_w$ is a k-linear combination of elements of the form $\tau_{w'}$, where $w' = \widetilde{s}'_1 \cdots \widetilde{s}'_r\omega'$ for suitable $s'_1, \dots s'_r \in \{s_1, \dots s_{\ell(w)}\}$ with $r < \ell(w)$ and $\omega' \in \widetilde{\Omega}$, and the claim follows.

Therefore the following formula holds:

$$z_{\mathcal{O}} = \sum_{x \in \mathcal{O}} \tau_x + r_{\mathcal{O}} \qquad \text{for some} \qquad r_{\mathcal{O}} \in \bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) < \ell(\mathcal{O})}} k\tau_v, \tag{117}$$

where $\ell(\mathcal{O})$ is defined as $\ell(x)$ for $x \in \mathcal{O}$ (this is independent of the choice of x because of the formula $\ell(x) = \frac{1}{2}\sum_{\alpha \in \Phi} |(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(x)|$ recalled in (10)).

We are now going to see a couple of preliminary statements before the stating the most important lemma for the proof of Theorem 3.1.10.

Remark 3.1.3. Let $x \in T/T^1$. Recall from Lemma 1.3.2 the Iwahori decomposition of the group I_x: the product map induces a homeomorphism

$$\prod_{\alpha \in \Phi^-} \mathfrak{U}_{(\alpha, g_x(\alpha))} \times T^1 \times \prod_{\alpha \in \Phi^+} \mathfrak{U}_{(\alpha, g_x(\alpha))} \longrightarrow I_x,$$

where the products on the left hand side are ordered in some arbitrarily chosen way and where $g_x(\alpha) = \min \left\{ m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \cap x\Phi^+_{\text{aff}} \right\}$. Since $x \in T/T^1$, we claim that the definition of $g_x(\alpha)$ simplifies as follows:

$$g_x(\alpha) = \begin{cases} \max\{1, (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(x) + 1\} & \text{if } \alpha \in \Phi^-, \\ \max\{0, (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(x)\} & \text{if } \alpha \in \Phi^+. \end{cases}$$

Proof. One has:

$$\begin{aligned} g_{\bar{t}}(\alpha) &= \min \left\{ m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \cap \bar{t}\Phi^+_{\text{aff}} \right\} \\ &= \min \left\{ m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \text{ and } \bar{t}^{-1} \cdot (\alpha, m) \in \Phi^+_{\text{aff}} \right\} \\ &= \min \left\{ m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \text{ and } (\alpha, m - (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t)) \in \Phi^+_{\text{aff}} \right\} \\ &= \begin{cases} \min \left\{ m \in \mathbb{Z} \mid m \geqslant 1 \text{ and } m - (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant 1 \right\} & \text{if } \alpha \in \Phi^- \\ \min \left\{ m \in \mathbb{Z} \mid m \geqslant 0 \text{ and } m - (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant 0 \right\} & \text{if } \alpha \in \Phi^+ \end{cases} \\ &= \begin{cases} \max\{1, (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) + 1\} & \text{if } \alpha \in \Phi^- \\ \max\{0, (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t)\} & \text{if } \alpha \in \Phi^+. \end{cases} \end{aligned}$$

■

Lemma 3.1.4. *Let $s \in S_{\text{aff}}$ and let $(\alpha_s, \mathfrak{h}_s)$ be the corresponding affine root. One has that I_s is normal in I and that there are the following isomorphisms*

$$I/I_s \xrightarrow[\bar{u} \leftarrow \bar{u}]{\cong} \mathfrak{U}_{(\alpha_s, \mathfrak{h}_s)}/\mathfrak{U}_{(\alpha_s, \mathfrak{h}_s + 1)} \xrightarrow[\varphi_{\alpha_s}\left(\begin{smallmatrix} 1 & a\pi^{\mathfrak{h}_s} \\ 0 & 1 \end{smallmatrix}\right) \leftarrow \bar{a}]{\cong} \mathfrak{O}/\mathfrak{M}.$$

Proof. See [OS19, Corollary 2.5.iii and Equation (12)]. ■

Remark 3.1.5. Let us remark that $T^1 \subseteq \{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\}$, so that it makes sense to define the quotient $\{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\} / T^1$, which we will consider in the next lemma. Indeed, a root α sends the unique maximal compact subgroup T^0 of T to the unique maximal compact subgroup $\mathfrak{O}^\times$ of $\mathfrak{F}^\times$, and α sends the unique pro-p Sylow subgroup T^1 of T^0 to the unique pro-p Sylow $1 + \mathfrak{M}$ of $\mathfrak{O}^\times$.

The next lemma is the main part of the proof of Theorem 3.1.10. Indeed, although the lemma itself does not describe the 0th graded piece of the centre, it gives a quite strong necessary condition for an element to lie in $Z(E^*)^0$.

Lemma 3.1.6. *Let*

$$\widetilde{C}' := \{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\} / T^1.$$

One has that every element of E^0 that commutes with the whole E^0 and the whole $H^1(I, \mathbf{X}(1))$ lies in the k-vector space spanned by the elements of the following set:

$$\left\{ z_{\mathcal{O}} \;\middle|\; \mathcal{O} \subseteq T/T^1 \text{ orbit for } W_0 \text{ made of elements of } \widetilde{C}' \right\},$$

where the $z_{\mathcal{O}}$'s are defined in (116).

In the statement of the lemma, we have used the notation $\widetilde{C}'$ in order to distinguish it from $\widetilde{C} \coloneqq (C\cdot T^1)/T^1$, although a posteriori these two groups will be equal, as claimed in Theorem 3.1.10. We also remark that with this alternative description of $\widetilde{C}'$ it also follows that the orbits in the statement of the lemma have cardinality equal to 1.

Proof of the lemma. Let $z \in E^0$ be an element which commutes with the whole E^0 and the whole $H^1(I, \mathbf{X}(1))$. Using the description of the centre of E^0 as in (116), we can write z as

$$z = \sum_{\substack{\mathcal{O}\subseteq T/T^1 \\ W_0\text{-orbit}}} a_{\mathcal{O}} z_{\mathcal{O}},$$

for suitable coefficients $a_{\mathcal{O}} \in k$ (almost all of them equal to zero). Clearly we might assume that $z \neq 0$ and set

$$L \coloneqq \max\left\{\ell(\mathcal{O}) \;\middle|\; \mathcal{O} \subseteq T/T^1 \text{ orbit such that } z_{\mathcal{O}} \text{ is in the support of } z\right\}.$$

We have seen in (117) that for all $\mathcal{O}$ one has

$$z_{\mathcal{O}} = \sum_{x\in\mathcal{O}} \tau_x + r_{\mathcal{O}} \qquad \text{for a suitable} \qquad r_{\mathcal{O}} \in \bigoplus_{\substack{v\in\widetilde{W} \\ \text{s.t. } \ell(v)<\ell(\mathcal{O})}} k\tau_v,$$

and therefore

$$z = \sum_{\substack{\mathcal{O}\text{ orbit} \\ \text{s.t. } \ell(\mathcal{O})=L}} \sum_{x\in\mathcal{O}} a_{\mathcal{O}}\tau_x + r, \tag{118}$$

for a suitable r supported in length strictly less than L. Let $\gamma \in H^1(I, \mathbf{X}(1))$, for the moment without further assumptions. Let us compute separately $\gamma\cdot z$ and $z\cdot\gamma$ and then let us try to deduce some constraints on the coefficients $a_{\mathcal{O}}$'s from the fact that $\gamma \cdot z$ and $z\cdot\gamma$ are equal. Since for all $w \in \widetilde{W}$ one has that both $\gamma\cdot\tau_w$ and $\tau_w\cdot\gamma$ lie in $H^1(I, \mathbf{X}(w))$ (see Corollary 1.9.5), we deduce that

$$\begin{aligned}
\gamma\cdot z &= \sum_{\substack{\mathcal{O}\text{ orbit} \\ \text{s.t. } \ell(\mathcal{O})=L}} \sum_{x\in\mathcal{O}} a_{\mathcal{O}} \underbrace{\gamma\cdot\tau_x}_{\in H^1(I,\mathbf{X}(x))} + \underbrace{\gamma\cdot r}_{\substack{\text{supported in} \\ \text{length}<L}}, \\
z\cdot\gamma &= \sum_{\substack{\mathcal{O}\text{ orbit} \\ \text{s.t. } \ell(\mathcal{O})=L}} \sum_{x\in\mathcal{O}} a_{\mathcal{O}} \underbrace{\tau_x\cdot\gamma}_{\in H^1(I,\mathbf{X}(x))} + \underbrace{r\cdot\gamma}_{\substack{\text{supported in} \\ \text{length}<L}}.
\end{aligned}$$

Let $\mathcal{O}$ be an orbit of length L and let $x \in \mathcal{O}$. Furthermore, let us consider the projection map $\mathrm{pr}_{H^1(I,\mathbf{X}(x))}\colon E^1 \longrightarrow H^1(I, \mathbf{X}(x))$, meaning the projection with respect to the direct sum decomposition $E^1 = \bigoplus_{w\in\widetilde{W}} H^1(I, \mathbf{X}(w))$. One has:

$$\begin{aligned}
\mathrm{pr}_{H^1(I,\mathbf{X}(x))}(\gamma\cdot z) &= a_{\mathcal{O}}\gamma\cdot\tau_x, \\
\mathrm{pr}_{H^1(I,\mathbf{X}(x))}(z\cdot\gamma) &= a_{\mathcal{O}}\tau_x\cdot\gamma.
\end{aligned}$$

Since we are assuming that γ and z commute, we have found that (for all orbits $\mathcal{O}$ of length L) one has:

$$a_{\mathcal{O}} = 0 \qquad \text{or} \qquad \gamma\cdot\tau_x = \tau_x\cdot\gamma \text{ for all } \gamma \in H^1(I,\mathbf{X}(1)) \text{ and all } x \in \mathcal{O}. \tag{119}$$

Now, let us compute explicitly $\gamma \cdot \tau_x$ and $\tau_x \cdot \gamma$, in order to prove that they are different "for many choices of x and γ". Corollary 1.9.5 yields the following explicit description of $\gamma \cdot \tau_x$ and $\tau_x \cdot \gamma$:

$$\begin{aligned} \mathrm{Sh}_x(\gamma \cdot \tau_x) &= \mathrm{res}^{I}_{I_x} \big(\mathrm{Sh}_1(\gamma)\big), \\ \mathrm{Sh}_x(\tau_x \cdot \gamma) &= \mathrm{res}^{xIx^{-1}}_{I_x} \big(x_* \,\mathrm{Sh}_1(\gamma)\big). \end{aligned} \tag{120}$$

Let $\alpha \in \Pi$ and let $s_{(\alpha,0)}$ be the element of S_{aff} corresponding to the affine root $(\alpha, 0)$. Since $\alpha \in \Pi$, one has that $s_{(\alpha,0)} \in S_{\mathrm{aff}}$, and we can apply Lemma 3.1.4, which states that $I_{s_{(\alpha,0)}}$ is normal in I and that we have an isomorphism $I/I_{s_{(\alpha,0)}} \cong \mathfrak{O}/\mathfrak{M}$. Let $f \colon \mathfrak{O}/\mathfrak{M} \longrightarrow k$ be an homomorphism of $\mathbb{F}_p$-vector spaces, and let us define following composite map:

$$\xi_{\alpha,f}\colon \quad I \xrightarrow{\text{quot.}} I/I_{s_{(\alpha,0)}} \xrightarrow[\overline{u} \leftarrow\!\shortmid \overline{u}]{\cong} \mathfrak{U}_{(\alpha,0)}/\mathfrak{U}_{(\alpha,1)} \xrightarrow[\varphi_\alpha\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \leftarrow\!\shortmid \overline{a}]{\cong} \mathfrak{O}/\mathfrak{M} \xrightarrow{f} k.$$

The map $\xi_{\alpha,f}$ is a homomorphism of topological groups from I to k, i.e., an element of $H^1(I, k)$. Let us define $\gamma_{\alpha,f} := \mathrm{Sh}_1^{-1}(\xi_{\alpha,f}) \in H^1(I, \mathbf{X}(1))$ (here the Shapiro isomorphism is basically the identity, but we write it explicitly to emphasize that we consider $\gamma_{\alpha,f} \in H^1(I, \mathbf{X}(1)) \subseteq E^1$). Putting this into the formulas (120), we get

$$\begin{aligned} \mathrm{Sh}_x(\gamma_{\alpha,f} \cdot \tau_x) &= \mathrm{res}^{I}_{I_x} \big(\xi_{\alpha,f}\big), \\ \mathrm{Sh}_x(\tau_x \cdot \gamma_{\alpha,f}) &= \mathrm{res}^{xIx^{-1}}_{I_x} \big(x_* \xi_{\alpha,f}\big). \end{aligned} \tag{121}$$

Let $t_x \in T$ be a representative of x. By the explicit description of I_x given in Remark 3.1.3, we know that $\mathfrak{U}_{(\alpha, g_x(\alpha))} \subseteq I_x$, where $g_x(\alpha) = \max\{0, (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x)\}$. Therefore, it makes sense to compute the image of $\mathrm{Sh}_x(\gamma_{\alpha,f} \cdot \tau_x)$ and the image of $\mathrm{Sh}_x(\tau_x \cdot \gamma_{\alpha,f})$ on the subgroup $\mathfrak{U}_{(\alpha, g_x(\alpha))} \subseteq I_x$. This yields:

$$\begin{aligned} \mathrm{Sh}_x(\gamma_{\alpha,f} \cdot \tau_x)(\mathfrak{U}_{(\alpha,g_x(\alpha))}) &= \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,g_x(\alpha))}), \\ \mathrm{Sh}_x(\tau_x \cdot \gamma_{\alpha,f})(\mathfrak{U}_{(\alpha,g_x(\alpha))}) &= \big(x_* \xi_{\alpha,f}\big)(\mathfrak{U}_{(\alpha,g_x(\alpha))}) \\ &= \xi_{\alpha,f}(t_x^{-1} \mathfrak{U}_{(\alpha,g_x(\alpha))} t_x) \\ &= \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,g_x(\alpha) - (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x))}), \end{aligned}$$

where in the last step we have used (7).

Let us examine the following cases.

- Assume that $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x) > 0$, and choose $f \neq 0$ (clearly it exists). One has

$$\begin{aligned} \mathrm{Sh}_x(\gamma_{\alpha,f} \cdot \tau_x)(\mathfrak{U}_{(\alpha,g_x(\alpha))}) &= \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,g_x(\alpha))}) \\ &= \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x))}) \\ &\subseteq \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,1)}) \\ &= \{0\}, \\ \mathrm{Sh}_x(\tau_x \cdot \gamma_{\alpha,f})(\mathfrak{U}_{(\alpha,g_x(\alpha))}) &= \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x) - (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x))}) \\ &= \xi_{\alpha,f}(\mathfrak{U}_{(\alpha,0)}) \\ &= f\,(\mathfrak{O}/\mathfrak{M}) \\ &\neq \{0\}. \end{aligned}$$

  Hence $\gamma_{\alpha,f} \cdot \tau_x \neq \tau_x \cdot \gamma_{\alpha,f}$.

- In a similar fashion, assume that $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x) < 0$, and choose again $f \neq 0$. One has

$$\begin{aligned}
\mathrm{Sh}_x(\gamma_{\alpha,f} \cdot \tau_x)(\mathcal{U}_{(\alpha,g_x(\alpha))}) &= \xi_{\alpha,f}(\mathcal{U}_{(\alpha,g_x(\alpha))}) \\
&= \xi_{\alpha,f}(\mathcal{U}_{(\alpha,0)}) \\
&= f\,(\mathfrak{O}/\mathfrak{M}) \\
&\neq \{0\}, \\
\mathrm{Sh}_x(\tau_x \cdot \gamma_{\alpha,f})(\mathcal{U}_{(\alpha,g_x(\alpha))}) &= \xi_{\alpha,f}(\mathcal{U}_{(\alpha,0-(\mathrm{val}_{\mathfrak{F}} \circ\alpha)(t_x))}) \\
&\subseteq \xi_{\alpha,f}(\mathcal{U}_{(\alpha,1)}) \\
&= \{0\}.
\end{aligned}$$

  Hence $\gamma_{\alpha,f} \cdot \tau_x \neq \tau_x \cdot \gamma_{\alpha,f}$.

- Assume that $(\mathrm{val}_{\mathfrak{F}} \circ\alpha)(t_x) = 0$ (i.e., that $\alpha(t_x) \in \mathfrak{O}^\times$) and furthermore that $\alpha(t_x) \notin 1 + \mathfrak{M}$. For the moment, let us not make any assumptions on f. Since $g_x(\alpha) = 0$, one has that $\mathcal{U}_{(\alpha,0)} \subseteq I_x$ and so it makes sense to compute the following:

$$\begin{aligned}
\mathrm{Sh}_x(\gamma_{\alpha,f} \cdot \tau_x)\left(\varphi_\alpha\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) &= \xi_{\alpha,f}\left(\varphi_\alpha\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) \\
&= f\left(\overline{1}\right), \\
\mathrm{Sh}_x(\tau_x \cdot \gamma_{\alpha,f})\left(\varphi_\alpha\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) &= (x_*\xi_{\alpha,f})\left(\varphi_\alpha\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) \\
&= \xi_{\alpha,f}\left(t_x^{-1} \cdot \varphi_\alpha\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \cdot t_x\right) \\
&= \xi_{\alpha,f}\left(\varphi_\alpha\begin{pmatrix}1 & \alpha(t_x)^{-1}\\ 0 & 1\end{pmatrix}\right) \\
&= f\left(\overline{\alpha(t_x)^{-1}}\right),
\end{aligned}$$

  where we have used the equality $t_x^{-1} \cdot \varphi_\alpha\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \cdot t_x = \varphi_\alpha\left(\begin{smallmatrix}1 & \alpha(t_x)^{-1}\\ 0 & 1\end{smallmatrix}\right)$ (see (1)). Since we have assumed that $\alpha(t_x) \notin 1 + \mathfrak{M}$, obviously $\overline{\alpha(t_x)^{-1}} \neq \overline{1}$, and we can find $f \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$ such that $f\left(\overline{\alpha(t_x)}\right) \neq f\left(\overline{1}\right)$. It is therefore clear that for such choice of f one has $\gamma_{\alpha,f} \cdot \tau_x \neq \tau_x \cdot \gamma_{\alpha,f}$.

Now we are able to give huge constraints on the orbits appearing in the support of z.

- First of all, we claim that the maximal length L is actually zero: indeed, by contradiction, if it were strictly bigger than zero then, choosing $\mathcal{O}$ of length L such that $a_{\mathcal{O}} \neq 0$ and choosing $x \in \mathcal{O}$, there would exist $\alpha \in \Pi$ such that $(\mathrm{val}_{\mathfrak{F}} \circ\alpha)(t_x) \neq 0$ (indeed there would exists an $\alpha \in \Phi^+$ with this property by the length formula (10), and then there would exists also an $\alpha \in \Pi$ with the same property). But for such α we have proved above that, choosing $f \neq 0$, one has $\gamma_{\alpha,f} \cdot \tau_x \neq \tau_x \cdot \gamma_{\alpha,f}$ and this forces $a_{\mathcal{O}}$ to be zero (see (119)), yielding a contradiction.

- Now, since we have proved that $L = 0$, the description of z we gave in (118) becomes much simpler:

$$z = \sum_{\substack{\mathcal{O} \text{ orbit} \\ \text{s.t. } \ell(\mathcal{O}) = 0}} a_{\mathcal{O}} \sum_{x \in \mathcal{O}} \tau_x.$$

To finish the proof, it remains to show that for all orbit $\mathcal{O}$ of length zero such that $a_{\mathcal{O}} \neq 0$, all $x \in \mathcal{O}$ and all $\alpha \in \Phi$ (equivalently, all $\alpha \in \Pi$) one has $\alpha(t_x) \in 1 + \mathfrak{M}$. Assume by contradiction that this is false and let us consider $\mathcal{O}$, x and α which do not satisfy this condition (we can assume $\alpha \in \Pi$). Then since the length of x is zero one has $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_x) = 0$ by the length formula (10) and, since moreover $\alpha(t_x) \notin 1 + \mathfrak{M}$, we have shown that for a suitable choice of f one has $\gamma_{\alpha,f} \cdot \tau_x \neq \tau_x \cdot \gamma_{\alpha,f}$. But this forces $a_{\mathcal{O}}$ to be zero (see (119)), yielding a contradiction and completing the proof. ∎

Remark 3.1.7. For later use we record the following fact: let

$$\widetilde{C}' \coloneqq \{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\} / T^1$$

as in the last lemma (we will prove in Theorem 3.1.10 that $\widetilde{C}' = (C \cdot T^1)/T^1$). Let us consider $x \in \left(T/T^1\right) \smallsetminus \widetilde{C}'$. In the proof of the last lemma we constructed an element $\gamma \in H^1(I, \mathbf{X}(1)) = H^1(I, k)$ such that

$$[\gamma, \tau_x] \neq 0.$$

Moreover $[\gamma, \tau_x]$ has the property that $\mathrm{Sh}_x([\gamma, \tau_x])$ is zero on T^1, as it is easy to see from the formulas of Corollary 1.9.5 since conjugation by x^{-1} acts trivially on T^1 (actually, for the specific γ we have constructed it is also easy to see that both $\mathrm{Sh}_x(\gamma \cdot \tau_x)$ and $\mathrm{Sh}_x(\tau_x \cdot \gamma)$ are zero on T^1).

Lemma 3.1.8. *Let $\omega \in \widetilde{\Omega}$, let $i \in \mathbb{Z}_{\geqslant 0}$, let $v \in \widetilde{W}$, and let $\beta \in H^i(I, \mathbf{X}(v))$. One has the following formulas:*

$$\begin{aligned} &\beta \cdot \tau_\omega \in H^i(I, \mathbf{X}(v\omega)) && \text{and} && \mathrm{Sh}_{v\omega}(\beta \cdot \tau_\omega) = \mathrm{Sh}_v(\beta), \\ &\tau_\omega \cdot \beta \in H^i(I, \mathbf{X}(\omega v)) && \text{and} && \mathrm{Sh}_{\omega v}(\tau_\omega \cdot \beta) = \omega_* \,\mathrm{Sh}_v(\beta). \end{aligned}$$

In particular, for all $c \in \widetilde{C}$, one has that τ_c centralizes E^*.

Note that the final part of the statement follows from the first one because $\widetilde{C} \subseteq \widetilde{\Omega}$, for example by the length formula (10).

Proof. Since the length function is constant on each double coset modulo $\widetilde{\Omega}$ (see after (11)), we can apply Corollary 1.9.5, finding that

$$\begin{aligned} &\beta \cdot \tau_\omega \in H^i(I, \mathbf{X}(v\omega)) && \text{and} && \mathrm{Sh}_{v\omega}(\beta \cdot \tau_\omega) = \mathrm{res}^{I_v}_{I_{v\omega}}\left(\mathrm{Sh}_v(\beta)\right), \\ &\tau_\omega \cdot \beta \in H^i(I, \mathbf{X}(\omega v)) && \text{and} && \mathrm{Sh}_{\omega v}(\tau_\omega \cdot \beta) = \mathrm{res}^{\omega I_v \omega^{-1}}_{I_{\omega v}}\left(n_* \,\mathrm{Sh}_v(\beta)\right). \end{aligned}$$

Since ω has length zero, conjugation by ω normalizes I (see [OS19, after Equation (5)]), and hence one has

$$\begin{aligned} I_{v\omega} &= I \cap v\omega I \omega^{-1} v^{-1} = I \cap v I v^{-1} = I_v, \\ \omega I_v \omega^{-1} &= \omega I \omega^{-1} \cap \omega v I v^{-1} \omega^{-1} = I \cap \omega v I v^{-1} \omega^{-1} = I_{\omega v}, \end{aligned}$$

and the claimed formulas follow. ∎

Lemma 3.1.9. *Let $t \in T$ such that $\alpha(t) \in 1 + \mathfrak{M}$ for all $\alpha \in \Phi$ (in this lemma Φ could be replaced by any other subset of $X^*(\mathbf{T})$). Then there exists $t' \in T$ with the following properties:*

- $\overline{t} = \overline{t'}$ *in T/T^1,*

- $\alpha(t') = 1$ *for all* $\alpha \in \Phi$.

Proof. Since $\mathbf{T}$ is $\mathfrak{F}$-split, it is isomorphic to $\mathbb{G}_{\mathrm{m}}^n$ over $\mathfrak{F}$ (where $n = \dim(\mathbf{T})$). Since this isomorphism preserves the formation of T, T^0 and T^1, there is no loss of generality in assuming that $\mathbf{T} = \mathbb{G}_{\mathrm{m}}^n$. Recall that one has the isomorphism of topological groups

$$\begin{aligned} \mathbb{Z} \times \boldsymbol{\mu}_{q-1}(\mathfrak{F}) \times (1 + \mathfrak{M}) &\longrightarrow \mathfrak{F}^\times \\ (m, x, u) &\longmapsto \pi^m \cdot x \cdot u. \end{aligned}$$

Since $T = (\mathfrak{F}^\times)^n$, we can write t as

$$t = (\pi^{m_i} \cdot x_i \cdot u_i)_{i \in \{1,\dots,n\}},$$

for suitable $m_i \in \mathbb{Z}$, $x_i \in \boldsymbol{\mu}_{q-1}(\mathfrak{F})$ and $u_i \in 1 + \mathfrak{M}$. Let us define

$$t' := (\pi^{m_i} \cdot x_i)_{i \in \{1,\dots,n\}}.$$

Clearly, since $T/T^1 = (\mathfrak{F}^\times/(1 + \mathfrak{M}))^n$, the requirement that $\bar{t} = \overline{t'}$ in T/T^1 is satisfied. Now, let $\alpha \in \Phi \subseteq X^*(\mathbf{T})$ and let us write it (in multiplicative notation) as $\alpha = \prod_{i=1}^n \mathrm{pr}_i^{c_i}$, where $(\mathrm{pr}_i)_{i \in \{1,\dots,n\}}$ is the standard basis of $X^*(\mathbf{T})$ made of projection maps. One has

$$\begin{aligned} 1 + \mathfrak{M} \ni \alpha(t) &= \pi^{\sum_{i=1}^n c_i m_i} \cdot \prod_{i=1}^n x_i^{c_i} \cdot \prod_{i=1}^n u_i^{c_i}, \\ \alpha(t') &= \pi^{\sum_{i=1}^n c_i m_i} \cdot \prod_{i=1}^n x_i^{c_i}. \end{aligned}$$

By the first line and the isomorphism describing $\mathfrak{F}^\times$, we see that $\pi^{\sum_i m_i c_i} \cdot \prod_i x_i^{c_i} = 1$. Hence $\alpha(t') = 1$, proving the last statement we had to check. ■

Theorem 3.1.10. *Let us define*

$$\widetilde{C} := (C \cdot T^1)/T^1.$$

One has the following facts:

- *One has the following isomorphism of* k*-algebras describing the* 0^{th} *graded piece of the centre of* E^**:*

$$\begin{aligned} k[\widetilde{C}] &\longrightarrow Z(E^*)^0 \\ \underset{(\text{with } c \in \widetilde{C})}{(c)} &\longmapsto \tau_c. \end{aligned}$$

- *The obvious inclusion* $Z(E^*)^0 \subseteq Z_{E^0 \cup H^1(I, \mathbf{X}(1))}(E^0)$ *is actually an equality.*

- $\widetilde{C}$ *is a subgroup of* $\widetilde{\Omega} \cap T/T^1$ *and it can also be described as*

$$\widetilde{C} = \{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\}/T^1.$$

  Moreover, in the obvious isomorphism $C/(C \cap T^1) \cong (C \cdot T^1)/T^1 = \widetilde{C}$*, the group* $C \cap T^1$ *can be described as the (unique) pro-*p *Sylow subgroup of the unique maximal compact subgroup of* C*.*

Proof. Let us prove the various facts not following the order of the statements.

- The fact that
$$(C \cdot T^1)/T^1 = \{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\}/T^1, \tag{122}$$
can be seen as follows: we recall from [Mil17, Proof of Proposition 21.8] that one has an equality of algebraic groups
$$\mathbf{C} = \bigcap_{\alpha \in \Phi} \ker(\alpha \colon \mathbf{T} \longrightarrow \mathbb{G}_{\mathrm{m}}).$$
Looking at the claimed equality (122), we see that the inclusion from left to right is then immediate, and the inclusion from right to left follows from Lemma 3.1.9, because for every element of the quotient $\{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\}/T^1$ we can find a representative that lies in the group of $\mathfrak{F}$-rational points of the intersection $\bigcap_{\alpha\in\Phi} \ker(\alpha \colon \mathbf{T} \longrightarrow \mathbb{G}_{\mathrm{m}})$, i.e., of $\mathbf{C}$.

- The fact that $\widetilde{C}$ is a subgroup of $\widetilde{\Omega}$ (and hence of $\widetilde{\Omega} \cap T/T^1$) follows from the fact that if $t \in T$ is such that $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) = 0$ (in particular, if $\alpha(t) \in 1 + \mathfrak{M}$) for all $\alpha \in \Phi$, then $\ell(\bar{t}) = 0$ (see (10)).

- The fact that the map $\widetilde{C} \ni c \mapsto \tau_c$ does take values in $Z(E^*)^0$ has been seen in Lemma 3.1.8.

- The fact that the map $k[\widetilde{C}] \longrightarrow Z(E^*)^0$ of the statement is a homomorphism of k-algebras follows from the fact that $\widetilde{C} \subseteq \widetilde{\Omega}$.

- The fact that the map $k[\widetilde{C}] \longrightarrow Z(E^*)^0$ of the statement is injective is clear.

- The fact that the map $k[\widetilde{C}] \longrightarrow Z(E^*)^0$ of the statement is surjective can be seen as follows: we have seen in Lemma 3.1.6 that every element of $Z_{E^0 \cup H^1(I,\mathbf{X}(1))}(E^0)$ lies in the k-vector space spanned by the following set:
$$\left\{ z_{\mathcal{O}} \;\middle|\; \mathcal{O} \subseteq T/T^1 \text{ orbit for } W_0 \text{ made of elements of } \widetilde{C} \right\},$$
If $\bar{t} \in \widetilde{C}$, we might assume that $t \in C$, and hence it is clear that the W_0-orbit $\mathcal{O}_{\bar{t}}$ of $\bar{t}$ consists only of $\bar{t}$, and hence $z_{\mathcal{O}_{\bar{t}}} = \tau_{\bar{t}}$. Therefore every element of $Z_{E^0 \cup H^1(I,\mathbf{X}(1))}(E^0)$ lies in the k-vector space spanned by the set
$$\left\{ \tau_c \;\middle|\; c \in \widetilde{C} \right\}.$$

- The fact that the obvious inclusion $Z(E^*)^0 \subseteq Z_{E^0 \cup H^1(I,\mathbf{X}(1))}(E^0)$ is actually an equality follows from the fact that in the last step above we have worked only with $Z_{E^0 \cup H^1(I,\mathbf{X}(1))}(E^0)$ and not with the full $Z(E^*)^0$.

- The fact that $C \cap T^1$ is equal to the unique pro-p Sylow of the unique maximal compact subgroup of C can be seen as follows: first of all $\mathbf{C}$, being a closed subgroup of a split torus, is isomorphic over $\mathfrak{F}$ to a product of a split torus and a finite algebraic group (see [Mil17, Proposition 12.3 and Theorem 12.9]), and hence C actually has a unique maximal compact subgroup. Now let C^1 be the unique pro-p Sylow of the unique maximal compact subgroup of C: the inclusion $C \cap T^1 \subseteq C^1$ is clear because $C \cap T^1 \subseteq C$ and because $C \cap T^1$ is a pro-p group, being a closed subgroup of T^1. Similarly, since $C \subseteq T$ we have $C^1 \subseteq T^1$, proving the last inclusion we had to show. ■

Remark 3.1.11. The inclusion $\widetilde{C} \subseteq Z(\widetilde{W})$ might be strict in general, but it is an equality if the order of the fundamental group of the derived group of $\mathbf{G}$ is not divisible by 2.

Proof. For the moment let us not make any assumption on $\mathbf{G}$. Let $w \in \widetilde{W}$. First of all we recall from [Vig14, Lemma 2.1] that if $w \notin T/T^1$ then the conjugacy class of w is infinite. In particular, this shows that $Z(\widetilde{W}) \subseteq T/T^1$. Now let $t \in T$ and let $\alpha \in \Pi$. We recall the conjugation formula

$$t \cdot \varphi_\alpha \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot t^{-1} = \varphi_\alpha \begin{pmatrix} 1 & \alpha(t) \\ 0 & 1 \end{pmatrix},$$

from (1) and the notation $n_{s_{(\alpha,0)}}$ we introduced for the fixed lift in N of $s_{(\alpha,0)} \in S_{\mathrm{aff}}$ (explicitly, the definition is $n_{s_{(\alpha,0)}} \coloneqq \varphi_\alpha\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$). Using also the definition of Chevalley basis and the equality $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we compute

$$\begin{aligned} t \cdot n_{s_{(\alpha,0)}} \cdot t^{-1} &= t \cdot \varphi_\alpha\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot \varphi_\alpha\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \cdot \varphi_\alpha\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot t^{-1} \\ &= t \cdot \varphi_\alpha\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot t^{-1} \cdot t \cdot \varphi_{-\alpha}\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \cdot t^{-1} \cdot t \cdot \varphi_\alpha\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot t^{-1} \\ &= \varphi_\alpha\begin{pmatrix} 1 & \alpha(t) \\ 0 & 1 \end{pmatrix} \cdot \varphi_{-\alpha}\begin{pmatrix} 1 & \alpha(t)^{-1} \\ 0 & 1 \end{pmatrix} \cdot \varphi_\alpha\begin{pmatrix} 1 & \alpha(t) \\ 0 & 1 \end{pmatrix} \\ &= \varphi_\alpha\left(\begin{pmatrix} 1 & \alpha(t) \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -\alpha(t)^{-1} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \alpha(t) \\ 0 & 1 \end{pmatrix}\right) \\ &= \breve{\alpha}(\alpha(t)) \cdot n_{s_{(\alpha,0)}}. \end{aligned}$$

We remark that if 2 does not divide the order of the fundamental group of the derived group $\mathbf{G}'$ of $\mathbf{G}$ then $\breve{\alpha} \colon \mathbb{G}_{\mathrm{m}} \longrightarrow \mathbf{T}$ is a monomorphism. This is basically shown in [Jan03, Part II, Chapter 1, Equation (7)]: indeed let us identify the roots systems of $(\mathbf{G}, \mathbf{T})$ and of $(\mathbf{G}', \mathbf{T}')$, where $\mathbf{T}' \coloneqq \mathbf{G}' \cap \mathbf{T}$ is the corresponding split maximal torus of $\mathbf{T}'$. In loc. cit. it is shown that $\breve{\alpha} \colon \mathbb{G}_{\mathrm{m}} \longrightarrow \mathbf{T}'$ is either a monomorphism or has kernel equal to $\boldsymbol{\mu}_2$, and that this last case is equivalent to the condition that $\breve{\alpha} \in 2X_*(\mathbf{T}')$, say $\breve{\alpha} = 2\lambda$ for some $\lambda \in X_*(\mathbf{T}')$. Recalling that the fundamental group is isomorphic to the quotient $X_*(\mathbf{T}')/(\mathrm{span}_{\mathbb{Z}} \breve{\Phi})$ (see [Con20, §9.3]), and using the assumption that 2 does not divide the order of the fundamental group, we see that $\frac{1}{2}\breve{\alpha} = \lambda \in \mathrm{span}_{\mathbb{Z}} \breve{\Phi}$, which is not possible since $\breve{\alpha} \in \breve{\Pi}$ and $\breve{\Pi}$ is a basis of $\mathrm{span}_{\mathbb{R}} \breve{\Phi}$.

Now, assume that the class $\bar{t}$ of t in T/T^1 is central in $\widetilde{W}$, and, again, that 2 does not divide the order of the fundamental group of $\mathbf{G}'$. Then the computation above yields that $\breve{\alpha}(\alpha(t)) \in T^1$. A monomorphism of algebraic groups such as $\breve{\alpha} \colon \mathbb{G}_{\mathrm{m}} \longrightarrow \mathbf{T}'$ is automatically a closed embedding for the Zariski topology (see [Mil17, Proposition 1.41]), and this also shows that the map $\breve{\alpha} \colon \mathfrak{F}^\times \longrightarrow T$ is closed for the $\mathfrak{F}$-topology, and hence it is an isomorphism of topological groups onto its image. As we said that $\breve{\alpha}(\alpha(t)) \in T^1$, it follows that $\alpha(t)$ must lie in the pro-p Sylow of the unique maximal compact subgroup of $\mathfrak{F}^\times$, i.e., it must lie in $1 + \mathfrak{M}$. Now the desired conclusion that $\bar{t} \in \widetilde{C}$ follows from the equality $\widetilde{C} = \{t \in T \mid \alpha(t) \in 1 + \mathfrak{M} \text{ for all } \alpha \in \Phi\}/T^1$ of Theorem 3.1.10 (where Φ can be clearly replaced by Π).

It remains to make an example in which the inclusion $\widetilde{C} \subseteq Z(\widetilde{W})$ is strict, and this is suggested by the above computation of $t \cdot n_{s_{(\alpha,0)}} \cdot t^{-1}$. Indeed, we assume $p \neq 2$, we choose $\mathfrak{F}$ such that there exists a square root r_0 of -1, we consider $G \coloneqq \mathrm{PGL}_2(\mathfrak{F})$ and we define

$$\mathfrak{r}_0 \coloneqq \overline{\begin{pmatrix} r_0 & 0 \\ 0 & r_0^{-1} \end{pmatrix}} \in \mathrm{PGL}_2(\mathfrak{F}).$$

We want to prove that the class $\overline{\mathfrak{r}_0}$ of $\mathfrak{r}_0$ modulo T^1 lies in $Z(\widetilde{W})$ but not in $\widetilde{C}$. Regarding the second fact, since $C = \{1\}$, it suffices to show that $\mathfrak{r}_0 \notin T^1$, and this is clear because $\mathfrak{r}_0$ has order 2, while T^1 is a pro-p group. Regarding the statement that $\overline{\mathfrak{r}_0}$ lies in $Z(\widetilde{W})$, we see that, since the conjugation action of $\widetilde{W}$ on T/T^1 factors through W_0, it suffices to check that conjugating $\overline{\mathfrak{r}_0}$ by the class of the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ we get $\overline{\mathfrak{r}_0}$ again, and this is clear because conjugating $\mathfrak{r}_0$ by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ we obtain $\mathfrak{r}_0^{-1}$, which is equal to $\mathfrak{r}_0$. ■

3.2 The 1^{st} graded piece of the centre

In this section we will describe the 1^{st} graded piece of the centre of the Ext-algebra E^* in the case that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. Since the main results are scattered into various subsections, in the first subsection we will describe the main statements and we will give a rough overview of the strategy of proof.

Assumptions. We put ourselves in the general assumptions of Section 1.1, i.e., we assume that $\mathfrak{F}$ is a locally compact nonarchimedean field, that $\mathbf{G}$ is a connected reductive split group over $\mathfrak{F}$ and that k is a field of the same characteristic of the residue field of $\mathfrak{F}$. We will assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ only where explicitly stated.

3.2.a Summary of the results

The following are the main results about the 1^{st} graded piece of the centre that we will prove:

(i) In Theorem 3.2.26 we describe the degree 1 part of the centre if $\mathfrak{F}$ is an unramified extensions of $\mathbb{Q}_p$: namely, we exhibit an isomorphism of $Z(E^*)^0$-modules
$$Z(E^*)^1 \cong Z(E^*)^0 \otimes_k H^1\big(T^1/T^1_{\check{\Phi}}, k\big),$$
where
$$T^1_{\check{\Phi}} := \operatorname{Image}\big(\textstyle\prod_{\alpha\in\Pi} \check{\alpha} \colon \prod_{\alpha\in\Pi}(1+\mathfrak{M}) \longrightarrow T^1\big),$$
and where by $Z(E^*)^0 \otimes_k H^1\big(T^1/T^1_{\check{\Phi}}, k\big)$ we simply mean the free $Z(E^*)^0$-module obtained by base change from the k-vector space $H^1\big(T^1/T^1_{\check{\Phi}}, k\big)$.

The proof is divided into two parts: in the first one we show that
$$Z(E^*)^1 \cong Z(E^*)^0 \otimes_k \left(Z(E^*)^1 \cap H^1(I, \mathbf{X}(1))\right), \tag{123}$$
while in the second one we show that
$$Z(E^*)^1 \cap H^1(I, \mathbf{X}(1)) \cong H^1\big(T^1/T^1_{\check{\Phi}}, k\big). \tag{124}$$

(ii) In Corollary 3.2.37 we refine the above description under the additional assumption that p divides neither the order of $\mathbf{C}^\circ \cap \mathbf{T}'$ nor the order of the fundamental group of $\mathbf{G}'$. In this case we show that
$$Z(E^*)^1 \cong Z(E^*)^0 \otimes_k H^1\big((C^\circ)^1, k\big),$$
where C° is the group of $\mathfrak{F}$-rational points of the connected centre of $\mathbf{G}$ and where $(C^\circ)^1$ is the unique pro-p Sylow subgroup of the unique maximal compact subgroup of C°.

Furthermore, we show that the additional assumptions on p are optimal in a suitable sense (Remark 3.2.38) and that they are satisfied whenever p does not divide the connection index of the root system, i.e., the order of the finite group given by the weight lattice modulo the root lattice (see again Corollary 3.2.37).

(iii) In Corollary 3.2.39 we give a characterization of the condition $Z(E^*)^1 = 0$ (again under the assumption that $\mathfrak{F}$ is an unramified extensions of $\mathbb{Q}_p$), thus generalizing the result that $Z(E^*)^1 = 0$ if $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (Proposition 2.5.2). Namely, we prove that $Z(E^*)^1$ is zero if and only if $\mathbf{G}$ is semisimple with fundamental group of order not divisible by p.

We now give an overview of the organization of this section.

- Subsection 3.2.b consists in adapting some of the proofs in [Vig14] (where the centre $Z(H) = Z(E^0)$ is studied) to the study of $Z_{E^0}(E^1)$. This object is more complicated than $Z(H)$ and we do not pursue a description of it. Rather, we prove a result (Lemma 3.2.6) which gives a very rough description of how its elements look like.
- Subsection 3.2.c consists in two lemmas and a proposition. The first result (Lemma 3.2.7) is again about $Z_{E^0}(E^1)$, and complements the description given in the preceding subsection. The second result (Lemma 3.2.10), instead, is about $Z_{E^1}(E^1)$, and more precisely about $Z_{H^1(I,\mathbf{X}(1))}(E^1)$: it is here that we make the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. Finally, in Proposition 3.2.11, we prove (123), i.e., the first part of our theorem.
- Subsections 3.2.d, 3.2.e and 3.2.f consist in preliminary work to prove the second part of the theorem. The results shown are about G, and the Ext-algebra is not involved.
- In Subsection 3.2.g we use the above preliminaries to conclude the proof of the theorem by showing (124).
- Subsection 3.2.h deals with the examples $\mathbf{G} = \mathrm{GL}_n$ and $\mathbf{G} = \mathrm{PGL}_n$. In these special cases the determinant function can be used to describe $Z(E^*)^1$ (for PGL_n we mean the "determinant" function $\mathrm{PGL}_n(\mathfrak{F}) \longrightarrow \mathfrak{F}^\times/(\mathfrak{F}^\times)^n$).
- In Subsection 3.2.i we consider the graded algebra

$$E^*(CI, I) := \mathrm{Ext}^*_{\mathrm{Rep}^\infty_k(G)}(\text{c-ind}_I^{CI}, \text{c-ind}_I^{CI})^{\mathrm{op}}.$$

  We show that it naturally embeds into E^* and that, via this embedding, there is some relation with the centre of E^*: namely one has that $Z(E^*)^0 = E^0(CI, I)$ and that $Z(E^*)^1 \subseteq E^1(CI, I)$ if $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. However, we also show that in general $Z(E^*) \nsubseteq E^*(CI, I)$.
- In Subsection 3.2.j we prove the two above mentioned Corollaries 3.2.37 and 3.2.39.
- In Subsection 3.2.k we show where our proof fails if $\mathfrak{F}$ is not necessary an unramified extension of $\mathbb{Q}_p$.

3.2.b A first lemma about $Z_{E^0}(E^1)$

The purpose of this subsection is to prove the following lemma, which gives a very partial but useful description of $Z_{E^0}(E^1)$. The strategy of the proof consists in using (a slight modification of) a lemma by Vignéras (Lemma 3.2.1) and then in doing an analysis of the conditions on $x \in T/T^1$ under which the subgroup $\mathcal{U}_{(\alpha, g_w(\alpha))} \subseteq I_w$ (for $\alpha \in \Phi$ and $w \in \widetilde{W}$) is contained in I_{wx}, along with with a similar analysis for I_{xw} (Lemma 3.2.5).

Lemma (see Lemma 3.2.6). *Let $\beta \in E^1$ be an element which is centralized by the τ_x's for $x \in T/T^1$. Let us write*

$$\beta = \sum_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \leqslant L}} \beta_w,$$

for suitable $L \in \mathbb{Z}_{\geqslant 0}$ and $\beta_w \in H^1(I, \mathbf{X}(w))$ (almost all of them equal to zero). One has that $\beta_w = 0$ for all $w \in \widetilde{W} \smallsetminus \big(T/T^1\big)$ of length L.

The next lemma and remark are basically stated and proved in [Vig14, Lemma 2.11 and Equation (8)], where they are used to prove a statement analogous to (but more precise than) Lemma 3.2.6 for the pro-p Iwahori–Hecke algebra E^0 instead of E^1.

The only difference between the following and the lemma in [Vig14] is that we need a slightly finer control on the signs of $\langle \nu(x), \alpha \rangle$ (recall this notation from (6)). For the proof, we will follow the same strategy as in the cited paper.

Lemma 3.2.1. *Let $w \in W \smallsetminus \big(T/T^0\big)$ and let us write it as $w = w_0 x_0$ with $w_0 \in W_0 \smallsetminus \{1\}$ and $x_0 \in T/T^0$. Let M be a positive integer. One has that there exists $x \in T/T^0$ such that:*

- *(A) $\ell(wx) = \ell(w) + \ell(x)$;*
- *(B) $\ell(wxw^{-1}x^{-1}) > M$;*
- *(C) For all $\alpha \in \Phi$ such that $\langle \nu(x_0), \alpha \rangle \neq 0$ one has that the signs of $\langle \nu(x), \alpha \rangle$ and $\langle \nu(x_0), \alpha \rangle$ are the same;*
- *(D1) For all $\alpha \in \Phi$ such that $\langle \nu(x_0), \alpha \rangle = 0$ one has that $\langle \nu(x), \alpha \rangle > 0$ if $\alpha \in \Phi^+$ and $\langle \nu(x), \alpha \rangle < 0$ if $\alpha \in \Phi^-$.*

Similarly, there exists $x \in T/T^0$ which satisfies the properties (A), (B), (C) and the following:

- *(D2) For all $\alpha \in \Phi$ such that $\langle \nu(x_0), \alpha \rangle = 0$ one has that $\langle \nu(x), \alpha \rangle < 0$ if $\alpha \in w_0^{-1}\Phi^+$ and $\langle \nu(x), \alpha \rangle > 0$ if $\alpha \in w_0^{-1}\Phi^-$.*

Proof. First of all we claim the existence of $x \in T/T^0$ satisfying the properties (A), (C), (D1) (respectively (D2)), and the following property, less strong than (B):

(B$_0$) $\ell(wxw^{-1}x^{-1}) > 0$.

Since the map $\nu_{\mathscr{A}} : T/T^0 \longrightarrow X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)$ is surjective, and since the intersection of $X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)$ with a Weyl chamber in $\mathscr{A} = (X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)) \otimes_{\mathbb{Z}} \mathbb{R}$ is non-empty, we can choose $y \in T/T^0$ satisfying one of the following two properties:

1. $\langle \nu(y), \alpha \rangle > 0$ for all $\alpha \in \Phi^+$ and $\langle \nu(y), \alpha \rangle < 0$ for all $\alpha \in \Phi^-$;
2. $\langle \nu(y), \alpha \rangle < 0$ for all $\alpha \in w_0^{-1}\Phi^+$ and $\langle \nu(y), \alpha \rangle > 0$ for all $\alpha \in w_0^{-1}\Phi^-$.

- Let us set $x \coloneqq x_0^n y$ for $n \in \mathbb{Z}_{\geqslant 1}$. We claim that if n is big enough then the property (C) is satisfied, as well as (D1) in case (1) and (D2) in case (2).

  From the equality

$$\begin{aligned} \langle \nu(x), \alpha \rangle &= \langle \nu(x_0^n y), \alpha \rangle \\ &= n\langle \nu(x_0), \alpha \rangle + \langle \nu(y), \alpha \rangle, \end{aligned}$$

it is clear that if $\langle \nu(x_0), \alpha \rangle \neq 0$ and if n is big enough then the signs of $\langle \nu(x), \alpha \rangle$ and of $\langle \nu(x_0), \alpha \rangle$ are the same.

On the other side, if $\langle \nu(x_0), \alpha \rangle = 0$ then the signs of $\langle \nu(x), \alpha \rangle$ and of $\langle \nu(y), \alpha \rangle$ are the same, so we get (D1) in case (1) and (D2) in case (2).

- We claim that if $x \in T/T^0$ satisfies properties (C) and (D1) (respectively (D2)), then it satisfies property (A).

  Looking at the explicit length formula (9), we see that

$$\begin{aligned}
\ell(wx) &= \ell(w_0 x_0 x) \\
&= \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^+} |\langle \nu(x_0 x), \alpha \rangle| + \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^-} |\langle \nu(x_0 x), \alpha \rangle + 1| \\
&\leqslant \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^+} \big(|\langle \nu(x_0), \alpha \rangle| + |\langle \nu(x), \alpha \rangle| \big) \\
&\quad + \sum_{\alpha \in \Phi^+ \cap w_0^{-1} \Phi^-} \big(|\langle \nu(x_0), \alpha \rangle + 1| + |\langle \nu(x), \alpha \rangle| \big) \\
&= \ell(w) + \ell(x),
\end{aligned}$$

  and 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 $\langle \nu(x_0), \alpha \rangle$ 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 $\langle \nu(x), \alpha \rangle$ and of $\langle \nu(x_0), \alpha \rangle + 1$ are compatible, meaning that their product is bigger or equal than zero.

  For all $\alpha \in \Phi$ such that $\langle \nu(x_0), \alpha \rangle \neq 0$, property (C) says that $\langle \nu(x), \alpha \rangle$ and $\langle \nu(x_0), \alpha \rangle$ have the same sign, and so (i) and (ii) are satisfied if $\langle \nu(x_0), \alpha \rangle \neq 0$.

  On the other side, condition (i) is automatically true if $\langle \nu(x_0), \alpha \rangle = 0$, while condition (ii) holds if $\langle \nu(x_0), \alpha \rangle = 0$ thanks to either (D1) or (D2).

- Now we claim that if $x \in T/T^0$ satisfies properties (C) and (D1) (respectively (D2)), then it satisfies also property (B_0).

  First of all, let us note that

$$\ell(wxw^{-1}x^{-1}) = \ell(w_0 x_0 x x_0^{-1} w_0^{-1} x^{-1}) = \ell(w_0 x w_0^{-1} x^{-1}).$$

  Let us write down the length formula for $w_0 x w_0^{-1} x^{-1}$ (see (10)):

$$\ell(w_0 x w_0^{-1} x^{-1}) = \sum_{\alpha \in \Phi^+} \big| \langle \nu(w_0 x w_0^{-1}), \alpha \rangle - \langle \nu(x), \alpha \rangle \big| .$$

  Note that $\nu_{\mathscr{A}}(x)$ lies in an open Weyl chamber because every root is nonzero on x by properties (C) and (D1) (respectively (C) and (D2)). The Weyl group W_0 acts simply transitively on the Weyl chambers ([Bou81, Chap. V, §3, n° 5, Théorème 2]), hence $\nu_{\mathscr{A}}(x)$ and $\nu_{\mathscr{A}}(w_0 x w_0^{-1})$ lie in different open Weyl chambers, meaning that there exists a root α_0 (which we might assume to be positive) such that the signs of $\langle \nu(x), \alpha_0 \rangle$ and of $\langle \nu(w_0 x w_0^{-1}), \alpha_0 \rangle$ are different. This means that $\langle \nu(w_0 x w_0^{-1}), \alpha_0 \rangle - \langle \nu(x), \alpha_0 \rangle \neq 0$ and hence $\ell(w_0 x w_0^{-1} x^{-1}) > 0$.

Now it remains to show the existence of $x \in T/T^0$ satisfying properties (A), (B), (C) and (D1) (respectively (D2)). We claim that this can be accomplished by replacing x by x^m where m is a big enough positive integer. Indeed, properties (C) and (D1) (respectively (D2)) are clearly true for x^m if they are true for x, but also property (A) continues to be true because we have seen that it follows from properties (C) and (D1) (respectively (D2)). Finally, as regards property (B), we have

$$\begin{aligned} \ell(wx^m w^{-1} x^{-m}) &= \ell((wxw^{-1}x^{-1})^m) \\ &= m\ell(wxw^{-1}x^{-1}) \\ &\geqslant m, \end{aligned}$$

where the second equality follows from the length formula. So property (B) holds if m is big enough. ■

Remark 3.2.2. Under the assumptions of the last lemma and using the same notation, let us choose the constant M to be $2\ell(w)$. One has:

$$2\ell(w) < \ell(wxw^{-1}x^{-1}) = \ell(x^{-1}wxw^{-1}) \leqslant \ell(x^{-1}wx) + \ell(w),$$

where we have used that wxw^{-1} and x^{-1} commute since they both of them lie in T/T^0. So we have obtained:

(B*) $\ell(x^{-1}wx) > \ell(w)$. ■

Now, let us see the "symmetric version" of Lemma 3.2.1 and Remark 3.2.2 when considering the decomposition $W = \big(T/T^0\big) \rtimes W_0$ instead of the decomposition $W = W_0 \ltimes \big(T/T^0\big)$.

Remark 3.2.3. Similarly to Lemma 3.2.1, let $w \in W \smallsetminus \big(T/T^0\big)$ and let us write it as $w = x_0' w_0$ with $w_0 \in W_0 \smallsetminus \{1\}$ and $x_0' \in T/T^0$. One has that there exists $x' \in T/T^0$ such that:

(A') $\ell(x'w) = \ell(x') + \ell(w)$;

(B*') $\ell(x'w(x')^{-1}) > \ell(w)$;

(C') For all $\alpha \in \Phi$ such that $\langle \nu(x_0'), \alpha \rangle \neq 0$ one has that the signs of $\langle \nu(x'), \alpha \rangle$ and $\langle \nu(x_0'), \alpha \rangle$ are the same.

Similarly, we could give conditions analogous to (D1) and (D2), but we will not need them.

Proof. Let us apply Lemma 3.2.1 and Remark 3.2.2 to $w^{-1} = w_0^{-1} \cdot (x_0')^{-1}$, thus finding x satisfying the following properties:

(A) $\ell(w^{-1}x) = \ell(w^{-1}) + \ell(x)$;

(B*) $\ell(x^{-1}w^{-1}x) > \ell(w^{-1}) = \ell(w)$;

(C) For all $\alpha \in \Phi$ such that $\langle \nu((x_0')^{-1}), \alpha \rangle \neq 0$ (i.e., such that $\langle \nu(x_0'), \alpha \rangle \neq 0$) one has that the signs of $\langle \nu(x), \alpha \rangle$ and $\langle \nu((x_0')^{-1}), \alpha \rangle$ are the same.

Let us define $x' := x^{-1}$. It is easy to see that the conditions (A'), (B*') and (C') are satisfied. ■

The next lemma is a weaker version of [Vig14, Proposition 2.10 and Lemma 2.12] for E^i in place of the pro-p Iwahori–Hecke algebra E^0.

Lemma 3.2.4. *Let $\beta \in E^i$ and let us write it as*

$$\beta = \sum_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) \leqslant L}} \beta_v,$$

for suitable $L \in \mathbb{Z}_{\geqslant 0}$ and $\beta_v \in H^i(I, \mathbf{X}(v))$ (almost all of them equal to zero). Let us consider $w \in \widetilde{W}$ of length L.

- *If $x \in T/T^1$ satisfies the following properties:*

  (A) $\ell(wx) = \ell(w) + \ell(x)$,

  (B)* $\ell(x^{-1}wx) > \ell(w)$,

  then the following formulas hold:

$$\begin{aligned} \mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\beta \cdot \tau_x) &= \beta_w \cdot \tau_x, \\ \mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\tau_x \cdot \beta) &= 0. \end{aligned}$$

  In particular, if β is centralized by τ_x then $\beta_w \cdot \tau_x = 0$.

- *If $x' \in T/T^1$ satisfies the following properties:*

  (A') $\ell(x'w) = \ell(x') + \ell(w)$,

  (B')* $\ell(x'w(x')^{-1}) > \ell(w)$,

  then the following formulas hold:

$$\begin{aligned} \mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\beta \cdot \tau_{x'}) &= 0, \\ \mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\tau_{x'} \cdot \beta) &= \tau_{x'} \cdot \beta_w. \end{aligned}$$

  In particular, if β is centralized by $\tau_{x'}$ then $\tau_{x'} \cdot \beta_w = 0$.

Proof. Let us prove the four formulas.

- Let us start with multiplication by τ_x on the right:

$$\beta \cdot \tau_x = \sum_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) \leqslant L}} \beta_v \cdot \tau_x.$$

  Let $v \in \widetilde{W}$ with $\ell(v) \leqslant L$. Recall that

$$\beta_v \cdot \tau_x \in \bigoplus_{\substack{u \in \widetilde{W} \\ \text{s.t. } IuI \subseteq IvI \cdot IxI}} H^i(I, \mathbf{X}(u))$$

  (see Theorem 1.9.1).

  - ⋆ If v is such that $\ell(vx) < \ell(v) + \ell(x)$ and if u is as above, then by Lemma 1.9.2 (ii) one has
$$\ell(u) < \ell(v) + \ell(x) \leqslant L + \ell(x),$$
    while wx has length $L + \ell(x)$, and so $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\beta_v \cdot \tau_x) = 0$.
  - ⋆ If v is such that $\ell(vx) = \ell(v) + \ell(x)$ then $\beta_v \cdot \tau_x \in H^i(I, \mathbf{X}(vx))$ and so $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\beta_v \cdot \tau_x)$ is zero if $v \neq w$ and is $\beta_w \cdot \tau_x$ if $v = w$.

This proves that $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\beta \cdot \tau_x) = \beta_w \cdot \tau_x$.

- Now let us consider $\tau_x \cdot \beta$ and let us prove that $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\tau_x \cdot \beta) = 0$. One has:

$$\tau_x \cdot \beta = \sum_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) \leqslant L}} \tau_x \cdot \beta_v.$$

Let $v \in \widetilde{W}$ with $\ell(v) \leqslant L$. As before, we have

$$\tau_x \cdot \beta_v \in \bigoplus_{\substack{u \in \widetilde{W} \\ \text{s.t. } IuI \subseteq IxI \cdot IvI}} H^i(I, \mathbf{X}(u)).$$

  - ⋆ If v is such that $\ell(xv) < \ell(x) + \ell(v)$ then, as before, $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\beta_v \cdot \tau_x) = 0$.
  - ⋆ If v is such that $\ell(xv) = \ell(x) + \ell(v)$, then $\tau_x \cdot \beta_v \in H^i(I, \mathbf{X}(xv))$ and so $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\tau_x \cdot \beta_v)$ is zero if $xv \neq wx$ and is $\tau_x \cdot \beta_v$ if $xv = wx$. But this last case is not possible, because we would have $v = x^{-1}wx$, and so by assumption $\ell(v) = \ell(x^{-1}wx) > \ell(w) = L$, which is a contradiction.

This proves that $\mathrm{pr}_{H^i(I,\mathbf{X}(wx))}(\tau_x \cdot \beta) = 0$.

- Now let us consider $\beta \cdot \tau_{x'}$ and let us prove that $\mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\beta \cdot \tau_{x'}) = 0$.

Using (A') and (B*') is easy to see that $\ell(w^{-1}(x')^{-1}) = \ell(w^{-1}) + \ell((x')^{-1})$ and that $\ell(((x')^{-1})^{-1}w^{-1}(x')^{-1}) > \ell(w^{-1})$. This means that $(x')^{-1}$ satisfies (A) and (B*) if we put w^{-1} in place of w. Let us compute $\mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\beta \cdot \tau_{x'})$ using the involutive anti-automorphism $\mathfrak{J}$. First of all let us note that

$$\mathfrak{J}(\beta) = \sum_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v) \leqslant L}} \mathfrak{J}(\beta_v)$$

with $\mathfrak{J}(\beta_v) \in H^i(I, \mathbf{X}(v^{-1}))$ (and $\ell(v^{-1}) = \ell(v)$). Now, let us proceed with the computation:

$$\begin{aligned}
\mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\beta \cdot \tau_{x'}) &= \mathfrak{J}\left(\mathfrak{J}\left(\mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\beta \cdot \tau_{x'})\right)\right) \\
&= \mathfrak{J}\left(\mathrm{pr}_{H^i(I,\mathbf{X}(w^{-1}(x')^{-1}))}\left(\mathfrak{J}(\beta \cdot \tau_{x'})\right)\right) \\
&= \mathfrak{J}\left(\mathrm{pr}_{H^i(I,\mathbf{X}(w^{-1}(x')^{-1}))}\left(\tau_{(x')^{-1}} \cdot \mathfrak{J}(\beta)\right)\right) \\
&= 0,
\end{aligned}$$

by the first formula we have proved in this lemma.

- Now let us consider $\tau_{x'} \cdot \beta$ and let us prove that $\mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\tau_{x'} \cdot \beta) = \tau_{x'} \cdot \beta_w$.

Doing the same computations as above, we find that

$$\begin{aligned}
\mathrm{pr}_{H^i(I,\mathbf{X}(x'w))}(\tau_{x'} \cdot \beta) &= \mathfrak{J}\left(\mathrm{pr}_{H^i(I,\mathbf{X}(w^{-1}(x')^{-1}))}\left(\mathfrak{J}(\beta) \cdot \tau_{(x')^{-1}}\right)\right) \\
&= \mathfrak{J}\left(\mathfrak{J}(\beta_w) \cdot \tau_{(x')^{-1}}\right) \\
&= \tau_{x'} \cdot \beta_w,
\end{aligned}$$

where in the second equality we have used the second formula we have proved in this lemma. ■

We recall from 1.3.2 the Iwahori decomposition of I_w for $w \in \widetilde{W}$:

$$\prod_{\alpha\in\Phi^-} \mathcal{U}_{(\alpha,g_w(\alpha))} \times T^1 \times \prod_{\alpha\in\Phi^+} \mathcal{U}_{(\alpha,g_w(\alpha))} \xrightarrow[\text{multiplication}]{\text{bijection given by}} I_w$$

where for all $\alpha \in \Phi$ we have

$$g_w(\alpha) = \min\left\{m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \cap w\Phi^+_{\text{aff}}\right\}.$$

In the next lemma we wish to relate the indices $g_w(\alpha)$, $g_{wx}(\alpha)$, and $g_{x'w}(\alpha)$ for suitable choices of $x \in T/T^1$ or of $x' \in T/T^1$. We recall, as one immediately see from the above expression, that $g_w(\alpha)$ only depends on the class of w in W, and so for simplicity in the next lemma we will work with W instead of $\widetilde{W}$ and with T/T^0 instead of T/T^1 (as we did in all the lemmas so far).

Lemma 3.2.5. *Let $w \in W \smallsetminus \left(T/T^0\right)$ and let $\alpha \in \Phi$. One has that at least one of the following statements is true.*

(i) There exists $x \in T/T^0$ satisfying the following properties:

(A) $\ell(wx) = \ell(w) + \ell(x)$;

(B)* $\ell(x^{-1}wx) > \ell(w)$;

(E) $g_{wx}(\alpha) = g_w(\alpha)$.

(i') There exists $x' \in T/T^0$ satisfying the following properties:

(A') $\ell(x'w) = \ell(x') + \ell(w)$;

(B')* $\ell(x'w(x')^{-1}) > \ell(w)$;

(E') $g_{x'w}(\alpha) = g_w(\alpha) - \langle \nu(x'), \alpha\rangle$.

Proof. Referring to Lemma 3.2.1 and Remark 3.2.2, let us choose $x \in T/T^0$ satisfying the properties (A), (B*), (C) and either (D1) or (D2). Similarly, referring to Remark 3.2.3, let us choose $x' \in T/T^0$ satisfying the properties (A'), (B*'), (C').

Let $\alpha \in \Phi$: we want to compute $g_w(\alpha)$, $g_{wx}(\alpha)$, $g_{x'w}(\alpha)$. Let us write

$$w = w_0x_0 = x_0'w_0,$$

for suitable $w_0 \in W_0 \smallsetminus \{1\}$ and suitable $x_0, x_0' \in T/T^0$ (clearly $x_0' = w_0x_0w_0^{-1}$). Furthermore, 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 Lemma 1.3.2, for all $t, t' \in T/T^0$ we compute:

$$\begin{aligned}
g_{w_0t}(\alpha) &= \min\left\{m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \cap w_0t\Phi^+_{\text{aff}}\right\}\\
&= \min\left\{m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \text{ and } t^{-1}w_0^{-1}(\alpha, m) \in \Phi^+_{\text{aff}}\right\}\\
&= \min\left\{m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \text{ and } \left(w_0^{-1}\alpha, m - \left\langle \nu(t^{-1}), w_0^{-1}\alpha\right\rangle\right) \in \Phi^+_{\text{aff}}\right\}\\
&= \min\left\{m \in \mathbb{Z} \;\middle|\; (\alpha, m) \in \Phi^+_{\text{aff}} \text{ and } \left(w_0^{-1}\alpha, m + \left\langle \nu(t), w_0^{-1}\alpha\right\rangle\right) \in \Phi^+_{\text{aff}}\right\}\\
&= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(t), w_0^{-1}\alpha\right\rangle\right\};\\
g_{t'w_0}(\alpha) &= g_{w_0w_0^{-1}t'w_0}(\alpha)\\
&= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(w_0^{-1}t'w_0), w_0^{-1}\alpha\right\rangle\right\}\\
&= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(t'), \alpha\right\rangle\right\}.
\end{aligned}$$

Replacing t and t' by the elements we are interested in, we get:

$$\begin{aligned} g_w(\alpha) &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0), w_0^{-1}\alpha \right\rangle\right\} \\ &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0'), \alpha \right\rangle\right\}; \\ g_{wx}(\alpha) &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0), w_0^{-1}\alpha \right\rangle - \left\langle \nu(x), w_0^{-1}\alpha \right\rangle\right\}; \\ g_{x'w}(\alpha) &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0'), \alpha \right\rangle - \left\langle \nu(x'), \alpha \right\rangle\right\}. \end{aligned}$$

Let us distinguish three cases.

- If $\left\langle \nu(x_0), w_0^{-1}\alpha \right\rangle > 0$, then property (C) says that $\left\langle \nu(x_0), w_0^{-1}\alpha \right\rangle > 0$ as well, and so we get

$$\begin{aligned} g_{wx}(\alpha) &= \max\{\varepsilon_\alpha, \text{something} \leqslant 0\} \\ &= g_w(\alpha). \end{aligned}$$

- If $\left\langle \nu(x_0), w_0^{-1}\alpha \right\rangle < 0$, then we have that $\langle \nu(x_0'), \alpha \rangle < 0$ (because these two quantities are the same since $x_0' = w_0 x_0 w_0^{-1}$). This implies that $\langle \nu(x'), \alpha \rangle < 0$ by property (C'), and so

$$\begin{aligned} g_{x'w}(\alpha) &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0'), \alpha \right\rangle - \left\langle \nu(x'), \alpha \right\rangle\right\} \\ &= \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0'), \alpha \right\rangle - \left\langle \nu(x'), \alpha \right\rangle \\ &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0'), \alpha \right\rangle\right\} - \left\langle \nu(x'), \alpha \right\rangle \\ &= g_w(\alpha) - \left\langle \nu(x'), \alpha \right\rangle. \end{aligned}$$

- If $\left\langle \nu(x_0), w_0^{-1}\alpha \right\rangle = 0$ (equivalently $\langle \nu(x_0'), \alpha \rangle = 0$), then we distinguish the following three cases.

  ⋆ Let us assume that $w_0^{-1}\alpha \in \Phi^+$.
  We choose x satisfying property (D1) and in this way we have $\left\langle \nu(x), w_0^{-1}\alpha \right\rangle > 0$. Therefore, one has

$$\begin{aligned} g_{wx}(\alpha) &= \max\left\{\varepsilon_\alpha, 0 - \left\langle \nu(x), w_0^{-1}\alpha \right\rangle\right\} \\ &= \varepsilon_\alpha \\ &= \max\{\varepsilon_\alpha, 0\} \\ &= g_w(\alpha). \end{aligned}$$

  ⋆ Let us assume that $w_0^{-1}\alpha \in w_0^{-1}\Phi^-$ (i.e., $\alpha \in \Phi^-$).
  We choose x satisfying property (D2) and in this way we have $\left\langle \nu(x), w_0^{-1}\alpha \right\rangle > 0$. Therefore, one has

$$\begin{aligned} g_{wx}(\alpha) &= \max\left\{1, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x), w_0^{-1}\alpha \right\rangle\right\} \\ &= 1 \\ &= \max\left\{1, \varepsilon_{w_0^{-1}\alpha}\right\} \\ &= g_w(\alpha). \end{aligned}$$

⋆ It remains to treat the case $\alpha \in \Phi^+ \cap w_0\Phi^-$.

Even if we could have done this, we have not stated the existence of x' satisfying properties analogous to (D1) or (D2). Nevertheless, already property (A') (additivity of lengths) suffices to gain control on the sign of $\langle \nu(x'), \alpha\rangle$. Let us recall from (8) the following length formula for $t'w_0$, where $t' \in T/T^0$:

$$\ell(t'w_0) = \sum_{\beta\in\Phi^+\cap w_0\Phi^+} \left|\langle \nu(t'), \beta\rangle\right| + \sum_{\beta\in\Phi^+\cap w_0\Phi^-} \left|\langle \nu(t'), \beta\rangle - 1\right|.$$

Since $\ell(x'x_0'w_0) = \ell(x') + \ell(x_0w_0)$, It is easy to see that, for all $\beta \in \Phi^+ \cap w_0\Phi^-$ (in particular for $\beta = \alpha$), we must have that the signs of $\langle \nu(x'), \beta\rangle$ and of $\langle \nu(x_0'), \beta\rangle - 1$ are compatible (meaning that their product is bigger or equal than zero). Since $\langle \nu(x_0'), \alpha\rangle = 0$ by assumption, it follows that $\langle \nu(x'), \alpha\rangle \leqslant 0$, and so we can conclude the following:

$$\begin{aligned} g_{x'w}(\alpha) &= \max\left\{\varepsilon_\alpha, \varepsilon_{w_0^{-1}\alpha} - \left\langle \nu(x_0'), \alpha\right\rangle - \left\langle \nu(x'), \alpha\right\rangle\right\} \\ &= \max\left\{0, 1 - 0 - \left\langle \nu(x'), \alpha\right\rangle\right\} \\ &= 1 - \left\langle \nu(x'), \alpha\right\rangle \\ &= \max\left\{0, 1 - 0\right\} - \left\langle \nu(x'), \alpha\right\rangle \\ &= g_w(\alpha) - \left\langle \nu(x'), \alpha\right\rangle. \end{aligned}$$

■

We are now ready to prove the lemma we stated at the beginning of the subsection.

Lemma 3.2.6. *Let $\beta \in E^1$ be an element which is centralized by the τ_x's for $x \in T/T^1$. Let us write*

$$\beta = \sum_{\substack{w\in\widetilde{W} \\ \text{s.t. } \ell(w) \leqslant L}} \beta_w,$$

for suitable $L \in \mathbb{Z}_{\geqslant 0}$ and $\beta_w \in H^1(I, \mathbf{X}(w))$ (almost all of them equal to zero). One has that $\beta_w = 0$ for all $w \in \widetilde{W} \smallsetminus \left(T/T^1\right)$ of length L.

Proof. Let $w \in \widetilde{W} \smallsetminus \left(T/T^1\right)$ of length L. Let us prove that $\beta_w = 0$ by proving that $\mathrm{Sh}_w(\beta_w)$ is zero on all the subgroups appearing in the Iwahori decomposition of I_w. First of all, let $\alpha \in \Phi$ and let us prove that $\mathrm{Sh}_w(\beta_w)$ is zero on $\mathfrak{U}_{(\alpha, g_w(\alpha))}$.

Lemma 3.2.5 says that at least one of the following two properties is true (there we worked with the groups W and T/T^0 and here we are working with the groups $\widetilde{W}$ and T/T^1, but clearly this does not matter).

(i) There exists $x \in T/T^1$ satisfying the following properties:

- (A) $\ell(wx) = \ell(w) + \ell(x)$;
- (B*) $\ell(x^{-1}wx) > \ell(w)$;
- (E) $g_{wx}(\alpha) = g_w(\alpha)$.

(i') There exists $x' \in T/T^1$ satisfying the following properties:

- (A') $\ell(x'w) = \ell(x') + \ell(w)$;
- (B*') $\ell(x'w(x')^{-1}) > \ell(w)$;
- (E') $g_{x'w}(\alpha) = g_w(\alpha) - \langle \nu(x'), \alpha\rangle$.

In particular x and x' (when they exist) satisfy the assumptions of Lemma 3.2.4, and so such lemma tells us the following:

- in case (i) one has that $\beta_w \cdot \tau_x = 0$;
- in case (i') one has that $\tau_{x'} \cdot \beta_w = 0$.

Let us see what happens in the two cases.

- Let us assume that we are in case (i).

  Since lengths add up, one has that $\beta_w \cdot \tau_x \in H^1(I, \mathbf{X}(wx))$ and that we can compute it as follows (see Corollary 1.9.5):

  $$0 = \mathrm{Sh}_{wx}(\beta_w \cdot \tau_x) = \mathrm{res}^{I_w}_{I_{wx}} \big(\mathrm{Sh}_w(\beta_w) \big).$$

  And therefore, considering the group $\mathcal{U}_{(\alpha, g_{wx}(\alpha))} = \mathcal{U}_{(\alpha, g_w(\alpha))}$, one has:

  $$\begin{aligned} 0 &= \big(\mathrm{Sh}_{wx}(\beta_w \cdot \tau_x) \big)(\mathcal{U}_{(\alpha, g_{wx}(\alpha))}) \\ &= \big(\mathrm{Sh}_{wx}(\beta_w \cdot \tau_x) \big)(\mathcal{U}_{(\alpha, g_w(\alpha))}) \\ &= \big(\mathrm{Sh}_w(\beta_w) \big)(\mathcal{U}_{(\alpha, g_w(\alpha))}). \end{aligned}$$

- Let us assume that we are in case (i').

  Since lengths add up, one has that $\tau_{x'} \cdot \beta_w \in H^1(I, \mathbf{X}(x'w))$ and that we can compute it as follows (see Corollary 1.9.5):

  $$0 = \mathrm{Sh}_{x'w}(\tau_{x'} \cdot \beta_w) = \mathrm{res}^{x' I_w (x')^{-1}}_{I_{x'w}} \big((x')_* \, \mathrm{Sh}_w(\beta_w) \big).$$

  And therefore, considering the group $\mathcal{U}_{(\alpha, g_{wx}(\alpha))} = \mathcal{U}_{(\alpha, g_w(\alpha) - \langle \nu(x'), \alpha \rangle)}$, one has:

  $$\begin{aligned} 0 &= \big(\mathrm{Sh}_{x'w}(\tau_{x'} \cdot \beta_w) \big)(\mathcal{U}_{(\alpha, g_{wx}(\alpha))}) \\ &= \big(\mathrm{Sh}_{x'w}(\tau_{x'} \cdot \beta_w) \big)(\mathcal{U}_{(\alpha, g_w(\alpha) - \langle \nu(x'), \alpha \rangle)}) \\ &= \big((x')_* \, \mathrm{Sh}_w(\beta_w) \big)(\mathcal{U}_{(\alpha, g_w(\alpha) - \langle \nu(x'), \alpha \rangle)}) \\ &= \mathrm{Sh}_w(\beta_w) \left((x')^{-1} \mathcal{U}_{(\alpha, g_w(\alpha) - \langle \nu(x'), \alpha \rangle)} x' \right) \\ &= \mathrm{Sh}_w(\beta_w) \left(\mathcal{U}_{(x')^{-1}(\alpha, g_w(\alpha) - \langle \nu(x'), \alpha \rangle)} \right) \\ &= \mathrm{Sh}_w(\beta_w) \left(\mathcal{U}_{(\alpha, g_w(\alpha) - \langle \nu(x'), \alpha \rangle - \langle \nu((x')^{-1}), \alpha \rangle)} \right) \\ &= \mathrm{Sh}_w(\beta_w) \left(\mathcal{U}_{(\alpha, g_w(\alpha))} \right), \end{aligned}$$

where we used the conjugation formula (1). This concludes the proof that $\mathrm{Sh}_w(\beta_w)$ is zero on $\mathcal{U}_{(\alpha, g_w(\alpha))}$.

It remains to prove that $\mathrm{Sh}_w(\beta_w)$ is zero on T^1, but this is easier. Let us choose $x \in T/T^1$ satisfying just properties (A) and (B*) (there exists such an x for example by Lemma 3.2.1 and Remark 3.2.2). As before, we have:

$$\begin{aligned} 0 &= \big(\mathrm{Sh}_{wx}(\beta_w \cdot \tau_x) \big)(T^1) \\ &= \big(\mathrm{Sh}_w(\beta_w) \big)(T^1). \end{aligned}$$

This shows that $\mathrm{Sh}_w(\beta_w)$ is zero also on T^1 and so we conclude that β_w is zero by the Iwahori decomposition. ■

3.2.c The 1st graded piece of the centre for unramified extensions of $\mathbb{Q}_p$: partial description

In this subsection we will partially describe the degree 1 part of the centre of E^* for unramified extensions of $\mathbb{Q}_p$ (Proposition 3.2.11). The description will be completed later, in Subsection 3.2.g, after an analysis of the commutator subgroup $[G, G]$ of the group of $\mathfrak{F}$-rational points G of $\mathbf{G}$.

The proof will be based on Lemma 3.2.6 and on two more lemmas.

Lemma 3.2.7. *Let $\beta \in E^1$ be an element which is centralized by the τ_x's for $x \in T/T^1$. Let us write*

$$\beta = \sum_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \leqslant L}} \beta_w,$$

for suitable $L \in \mathbb{Z}_{\geqslant 0}$ and $\beta_w \in H^1(I, \mathbf{X}(w))$ (almost all of them equal to zero). Let $x \in T/T^1$ of length L and let us consider

$$\mathrm{Sh}_x(\beta_x) \in H^1(I_x, k).$$

One has that $\mathrm{Sh}_x(\beta_x)$ is zero on the "unipotent factors" of the Iwahori decomposition of I_x (i.e., on the factors $\mathcal{U}_{(\alpha, g_x(\alpha))}$'s for $\alpha \in \Phi$).

Before seeing the proof, let us remark that, using the notation of the lemma, we already know from Lemma 3.2.6 that β_w is zero for $w \in \widetilde{W} \smallsetminus \left(T/T^1\right)$ of length L. So it makes sense to focus on β_x for $x \in T/T^1$ (of length L), as we do in the statement of the above lemma.

Proof of the lemma. Let us split the proof into some steps.

- As a first step, we choose a certain element $y \in T/T^1$, which we will use later on to perform multiplications by τ_y on the left and on the right.

  Let us recall from (5) the surjective map $\nu_{\mathscr{A}} \colon T/T^0 \longrightarrow X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)$, which we rather view as a map with source T/T^1, and let us choose $\mathfrak{c}$ to be an open Weyl chamber in $\mathscr{A} = (X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)) \otimes_{\mathbb{Z}} \mathbb{R}$ such that $\nu_{\mathscr{A}}(x) \in \bar{\mathfrak{c}}$. For the moment let us choose y in the following way: since $\nu_{\mathscr{A}}$ is surjective, and since the intersection of $X_*(\mathbf{T})/X_*(\mathbf{C}^\circ)$ with a Weyl chamber is non-empty, we can choose $y \in T/T^1$ such that $\nu_{\mathscr{A}}(y) \in \mathfrak{c}$. It follows that y satisfies the following two properties:

  (i) $\ell(xy) = \ell(x) + \ell(y)$ (because this property is equivalent, by the length formula, to the property that for all $\alpha \in \Phi$, the signs of $\langle \nu(x), \alpha \rangle$ and of $\langle \nu(y), \alpha \rangle$ are compatible, in the sense that their product is bigger or equal then zero);

  (ii) for all $\alpha \in \Phi$ the quantity $\langle \nu(y), \alpha \rangle$ is nonzero (by definition of (open) Weyl chamber).

  Up to replacing y with a suitable power, we can assume that $|\langle \nu(y), \alpha \rangle|$ is big enough. In particular we can choose y such that

  (ii') for all $\alpha \in \Phi$ one has $|\langle \nu(y), \alpha \rangle| \geqslant M$,

  where M is a constant such that $\mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha)+M)}\right) = 0$ for all $\alpha \in \Phi$ (there exists such a constant because $\left(\mathcal{U}_{(\alpha, g_x(\alpha)+m)}\right)_{m \in \mathbb{Z}_{\geqslant 0}}$ is a fundamental system of neighbourhoods of the identity in the group $\mathcal{U}_{(\alpha, g_x(\alpha))}$ and clearly this choice can also be made independent of α since the set of roots is finite).

- As a second step, let us remark that, thanks to property (i), we have

  (Claim) $$\mathrm{pr}_{H^1(I,\mathbf{X}(xy))}[\tau_y,\beta] = [\tau_y,\beta_x].$$

  (and so $[\tau_y,\beta_x]=0$, since β commutes with τ_y by assumption). To prove the claim, let us prove that $\mathrm{pr}_{H^1(I,\mathbf{X}(xy))}(\beta\cdot\tau_y) = \beta_x\cdot\tau_y$, the proof of the corresponding statement regarding multiplication on the left by τ_y being completely symmetric since $xy=yx$. Of course, we have that

  $$\beta\cdot\tau_y = \sum_{\substack{w\in\widetilde{W} \\ \text{s.t. } \ell(w)\leqslant L}} \beta_w\cdot\tau_y.$$

  Let $w\in\widetilde{W}$ with $\ell(w)\leqslant L$. Recall that

  $$\beta_w\cdot\tau_y \in \bigoplus_{\substack{u\in\widetilde{W} \\ \text{s.t. } IuI\subseteq IwI\cdot IyI}} H^i(I,\mathbf{X}(u))$$

  (see Theorem 1.9.1). We have the following two possibilities.

  $\star$ If w is such that $\ell(wy)<\ell(w)+\ell(y)$ and if u is as above, then by Lemma 1.9.2 (ii) one has
  $$\ell(u)<\ell(w)+\ell(y)\leqslant L+\ell(y),$$
  while xy has length $L+\ell(y)$, and so $\mathrm{pr}_{H^i(I,\mathbf{X}(xy))}(\beta_w\cdot\tau_y)=0$.

  $\star$ If w is such that $\ell(wy)=\ell(w)+\ell(y)$ then $\beta_w\cdot\tau_y\in H^i(I,\mathbf{X}(wy))$ and so $\mathrm{pr}_{H^i(I,\mathbf{X}(xy))}(\beta_w\cdot\tau_y)$ is zero if $w\neq x$ and is $\beta_x\cdot\tau_y$ if $w=x$ (moreover, for $w=x$ the condition $\ell(wy)=\ell(w)+\ell(y)$ is indeed satisfied by property (i)).

  This proves that $\mathrm{pr}_{H^i(I,\mathbf{X}(xy))}(\beta\cdot\tau_y)=\beta_x\cdot\tau_y$.

- As a third step, we use the fact that $[\tau_y,\beta_x]=0$, together with properties (i) and (ii'), to show that for all $\alpha\in\Phi$ one has that $\mathrm{Sh}_x(\beta_x)$ is zero on $\mathcal{U}_{(\alpha,g_x(\alpha))}$, thus completing the proof.

  Since lengths add up, products can be easily computed (Corollary 1.9.5), and precisely we get the following explicit descriptions of $\beta_x\cdot\tau_y$ and of $\tau_y\cdot\beta_x$ (both lying in $H^1(I,\mathbf{X}(xy))$):

  $$\begin{aligned}\mathrm{Sh}_{xy}(\beta_x\cdot\tau_y) &= \mathrm{res}^{I_x}_{I_{xy}}\big(\mathrm{Sh}_x(\beta_x)\big),\\ \mathrm{Sh}_{xy}(\tau_y\cdot\beta_x) &= \mathrm{res}^{yI_xy^{-1}}_{I_{xy}}\big(y_*\,\mathrm{Sh}_x(\beta_x)\big).\end{aligned}$$

  Since $\beta_x\cdot\tau_y=\tau_y\cdot\beta_x$, we can of course equate the values of the right hand sides of the two above equations on the whole I_{xy}, and in particular we can do this on the subset $\mathcal{U}_{(\alpha,g_{xy}(\alpha))}\subseteq I_{xy}$, finding that:

  $$\begin{aligned}\mathrm{Sh}_x(\beta_x)\big(\mathcal{U}_{(\alpha,g_{xy}(\alpha))}\big) &= \mathrm{Sh}_x(\beta_x)\big(y^{-1}\mathcal{U}_{(\alpha,g_{xy}(\alpha))}y\big)\\ &= \mathrm{Sh}_x(\beta_x)\big(\mathcal{U}_{(\alpha,g_{xy}(\alpha)+\langle\nu(y),\alpha\rangle)}\big)\,.\end{aligned} \tag{125}$$

  Now (thanks to property (ii)) we can distinguish the two cases $\langle\nu(y),\alpha\rangle>0$ and $\langle\nu(y),\alpha\rangle<0$. Before, we recall from Lemma 1.3.2 the following formula for the computation of $g_z(\alpha)$ for $z\in T/T^1$:

  $$\begin{aligned}g_z(\alpha) &= \min\big\{m\in\mathbb{Z}\;\big|\;(\alpha,m)\in\Phi^+_{\text{aff}}\cap z\Phi^+_{\text{aff}}\big\}\\ &= \min\big\{m\in\mathbb{Z}\;\big|\;(\alpha,m)\in\Phi^+_{\text{aff}}\text{ and } z^{-1}(\alpha,m)\in\Phi^+_{\text{aff}}\big\}\\ &= \min\big\{m\in\mathbb{Z}\;\big|\;(\alpha,m)\in\Phi^+_{\text{aff}}\text{ and } (\alpha,m+\langle\nu(z),\alpha\rangle)\in\Phi^+_{\text{aff}}\big\}\\ &= \max\{\varepsilon_\alpha,\varepsilon_\alpha-\langle\nu(z),\alpha\rangle\},\end{aligned}$$

where

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

* $\star$ If $\langle \nu(y), \alpha \rangle > 0$, then by condition (i) we have $\langle \nu(x), \alpha \rangle \geqslant 0$ and $\langle \nu(xy), \alpha \rangle > 0$, and so the above formula for $g_z(\alpha)$ tells us that

$$\begin{aligned} g_{xy}(\alpha) &= \varepsilon_\alpha \\ &= g_x(\alpha). \end{aligned}$$

  So in the formula (125) we can replace $g_{xy}(\alpha)$ with $g_x(\alpha)$, obtaining

$$\mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha))}\right) = \mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha) + \langle \nu(y), \alpha \rangle)}\right).$$

* $\star$ If $\langle \nu(y), \alpha \rangle < 0$, then by condition (i) we have $\langle \nu(x), \alpha \rangle \leqslant 0$ and $\langle \nu(xy), \alpha \rangle < 0$, and so the above formula for $g_z(\alpha)$ tells us that

$$\begin{aligned} g_{xy}(\alpha) &= \varepsilon_\alpha - \langle \nu(x), \alpha \rangle - \langle \nu(y), \alpha \rangle \\ &= g_x(\alpha) - \langle \nu(y), \alpha \rangle. \end{aligned}$$

  So in formula (125) we can replace $g_{xy}(\alpha)$ with $g_x(\alpha) - \langle \nu(y), \alpha \rangle$, obtaining

$$\mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha) - \langle \nu(y), \alpha \rangle)}\right) = \mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha)}\right).$$

In both cases we have thus obtained

$$\begin{aligned} \mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha))}\right) &= \mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha) + |\langle \nu(y), \alpha \rangle|)}\right) \\ &\subseteq \mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha) + M)}\right) \qquad \text{by (ii')}. \end{aligned}$$

But by definition of M we have $\mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha)+M)}\right) = 0$, and therefore we get

$$\mathrm{Sh}_x(\beta_x)\left(\mathcal{U}_{(\alpha, g_x(\alpha))}\right) = 0,$$

thus concluding the proof. ∎

Remark 3.2.8. In the above proof, in the case that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, we could have avoided topological considerations for the choice of M and we could have set M equal to the ramification index.

The following remark is not needed in any subsequent proof, but it is perhaps interesting to compare it with Lemma 3.2.7.

Remark 3.2.9. Assume that $q \neq 2, 3$. Let $\beta \in E^1$ be an element which is centralized by the τ_ω's for $\omega \in T^0/T^1$. Let us write

$$\beta = \sum_{w \in \widetilde{W}} \beta_w,$$

for suitable $\beta_w \in H^1(I, \mathbf{X}(w))$ (almost all of them equal to zero). Let $x \in T/T^1$ and let us consider

$$\mathrm{Sh}_x(\beta_x) \in H^1(I_x, k).$$

One has that $\mathrm{Sh}_x(\beta_x)$ is zero on the "unipotent factors" of the Iwahori decomposition of I_x.

Before seeing the proof, let us compare this remark with Lemma 3.2.7: the assumption $q \neq 2, 3$ has been added, whereas the assumption that β is centralized by the τ_x's for $x \in T/T^1$ has been relaxed replacing T/T^1 with T^0/T^1. Finally, the assumption that x has "maximal length" with respect to the support of β has been dropped.

We will see that the proof is shorter. However, the statement of the remark cannot hold in general if $q = 2$ or $q = 3$ because in these cases it is possible that all the τ_ω's for $\omega \in T^0/T^1$ are central (as it happens for $\mathrm{SL}_2(\mathbb{Q}_2)$ and $\mathrm{SL}_2(\mathbb{Q}_3)$, see Theorem 3.1.10). So we still need Lemma 3.2.7.

Proof of the remark. Let $\alpha \in \Phi$. We have to prove that $\mathrm{Sh}_x(\beta_x)$ is zero on $\mathcal{U}_{(\alpha, g_x(\alpha))}$. Since $q \neq 2, 3$, the group $(\mathfrak{O}/\mathfrak{M})^\times$ is cyclic of order at least 3. Therefore we can choose $c_0 \in \mathfrak{O}^\times$ such that $c_0^2 \not\equiv 1$ modulo $\mathfrak{M}$.

Since the length of $\breve{\alpha}(c_0)$ and every element of $\widetilde{W}$ add up, we see that

$$\mathrm{pr}_{H^1(I, \mathbf{X}(\breve{\alpha}(c_0)x))}(\tau_{\breve{\alpha}(c_0)} \cdot \beta) = \tau_{\breve{\alpha}(c_0)} \cdot \beta_x,$$
$$\mathrm{pr}_{H^1(I, \mathbf{X}(x\breve{\alpha}(c_0)))}(\beta \cdot \tau_{\breve{\alpha}(c_0)}) = \beta_x \cdot \tau_{\breve{\alpha}(c_0)},$$

but $\breve{\alpha}(c_0)x = x\breve{\alpha}(c_0)$, and since β commutes with $\tau_{\breve{\alpha}(c_0)}$ by assumption, we deduce that

$$\tau_{\breve{\alpha}(c_0)} \cdot \beta_x = \beta_x \cdot \tau_{\breve{\alpha}(c_0)}.$$

Applying the Shapiro isomorphism $\mathrm{Sh}_{\breve{\alpha}(c_0)x} = \mathrm{Sh}_{x\breve{\alpha}(c_0)}$ to both sides, we get the following (by the formulas of Corollary 1.9.5):

$$\mathrm{res}^{\breve{\alpha}(c_0) I_x \breve{\alpha}(c_0)^{-1}}_{I_{\breve{\alpha}(c_0)x}} \big((\breve{\alpha}(c_0))_* \,\mathrm{Sh}_x(\beta_x) \big) = \mathrm{res}^{I_x}_{I_{x\breve{\alpha}(c_0)}} \big(\mathrm{Sh}_x(\beta_x) \big).$$

Since $\breve{\alpha}(c_0) \in T^0/T^1$, all the subgroups of I appearing in the restrictions are equal to I_x (recall from Section 1.3 that T^0 normalizes I).

Therefore, the formula above simplifies to

$$(\breve{\alpha}(c_0))_* \,\mathrm{Sh}_x(\beta_x) = \mathrm{Sh}_x(\beta_x).$$

Hence, for all $g \in I_x$ one has that

$$\mathrm{Sh}_x(\beta_x)\big(\breve{\alpha}(c_0)^{-1} \cdot g \cdot \breve{\alpha}(c_0) \cdot g^{-1}\big) = 0.$$

Since $\mathcal{U}_{(\alpha, g_x(\alpha))} \subseteq I_x$, it does make sense to compute the last identity for

$$g \coloneqq \varphi_\alpha \begin{pmatrix} 1 & a\pi^{g_x(\alpha)} \\ 0 & 1 \end{pmatrix},$$

for $a \in \mathfrak{O}$. Doing this we get:

$$\begin{aligned} 0 &= \mathrm{Sh}_x(\beta_x) \left(\breve{\alpha}(c_0)^{-1} \cdot \varphi_\alpha \begin{pmatrix} 1 & a\pi^{g_x(\alpha)} \\ 0 & 1 \end{pmatrix} \cdot \breve{\alpha}(c_0) \cdot \left(\varphi_\alpha \begin{pmatrix} 1 & a\pi^{g_x(\alpha)} \\ 0 & 1 \end{pmatrix} \right)^{-1} \right) \\ &= \mathrm{Sh}_x(\beta_x) \left(\varphi_\alpha \left(\begin{pmatrix} c_0^{-1} & 0 \\ 0 & c_0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a\pi^{g_x(\alpha)} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_0 & 0 \\ 0 & c_0^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & -a\pi^{g_x(\alpha)} \\ 0 & 1 \end{pmatrix} \right) \right) \\ &= \mathrm{Sh}_x(\beta_x) \left(\varphi_\alpha \begin{pmatrix} 1 & (c_0^{-2} - 1)a\pi^{g_x(\alpha)} \\ 0 & 1 \end{pmatrix} \right). \end{aligned}$$

By definition of c_0, one has that $c_0^{-2} - 1 \in \mathfrak{O} \smallsetminus \mathfrak{M}$. This means that we have shown that $\mathrm{Sh}_x(\beta_x)$ is zero at all the elements of the form $\varphi_\alpha\left(\begin{smallmatrix} 1 & b\pi^{g_x(\alpha)} \\ 0 & 1 \end{smallmatrix}\right)$ with $b \in \mathfrak{O}$, or, equivalently, that it is zero on the whole $\mathcal{U}_{(\alpha, g_x(\alpha))}$. ■

As in Theorem 3.1.10, we will use the notation $\widetilde{C} \coloneqq (C \cdot T^1)/T^1$, where C is the group of $\mathfrak{F}$-rational points of the centre $\mathbf{C}$ of $\mathbf{G}$. In view of Lemma 3.2.7, it is interesting to study commutators involving an element $\gamma \in H^1(I, \mathbf{X}(x))$ for $x \in T/T^1$ such that $\mathrm{Sh}_x(\gamma)$ is 0 on the "unipotent factors" of the Iwahori decomposition of I_x. We will do this in the next lemma, under some further assumptions.

Lemma 3.2.10. *Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. Let us consider $x \in \big(T/T^1\big) \smallsetminus \widetilde{C}$ and let $\gamma \in H^1(I, \mathbf{X}(x))$ be such that $\mathrm{Sh}_x(\gamma)$ is 0 on the "unipotent factors" of the Iwahori decomposition of I_x (i.e., on the factors $\mathfrak{U}_{(\alpha, g_x(\alpha))}$'s for $\alpha \in \Phi$) but nonzero on T^1. One has that there exists $\xi \in H^1(I, \mathbf{X}(1)) \cong H^1(I, k)$ such that*

$$[\xi, \gamma]_{\mathrm{gr}} \neq 0.$$

Proof. Since $x \in \big(T/T^1\big) \smallsetminus \widetilde{C}$, we know from Remark 3.1.7 that there exists an element $\xi \in H^1(I, \mathbf{X}(1)) = H^1(I, k)$ with the following properties:

- $[\xi, \tau_x]$ is nonzero;
- $\mathrm{Sh}_x([\xi, \tau_x])$ is zero on T^1.

We claim that

$$[\xi, \gamma]_{\mathrm{gr}} \neq 0. \tag{Claim}$$

Since $\xi \in H^1(I, \mathbf{X}(1))$, we can apply the formula relating the (opposite of the) Yoneda product and the cup product (Corollary 1.9.3), obtaining

$$\begin{aligned}
[\xi, \gamma]_{\mathrm{gr}} &= \xi \cdot \gamma + \gamma \cdot \xi \\
&= \big((\xi \cdot \tau_x) \smile \gamma\big) + \big(\gamma \smile (\tau_x \cdot \xi)\big) \\
&= \big((\xi \cdot \tau_x) \smile \gamma\big) - \big((\tau_x \cdot \xi) \smile \gamma\big) \\
&= [\xi, \tau_x] \smile \gamma,
\end{aligned}$$

And so we have to prove that $[\xi, \tau_x] \smile \gamma$ is nonzero, or equivalently that

$$\mathrm{Sh}_x([\xi, \tau_x]) \smile \mathrm{Sh}_x(\gamma) \neq 0. \tag{Claim}$$

By the defining properties of ξ, we can choose $\alpha \in \Phi$ (actually from the construction we could assume $\alpha \in \Pi$ but we will not need this) such that $\mathrm{Sh}_x([\xi, \tau_x])$ is nonzero on $\mathfrak{U}_{(\alpha, g_x(\alpha))}$: so let us choose $u_0 \in \mathfrak{U}_{(\alpha, g_x(\alpha))}$ such that $\mathrm{Sh}_x([\xi, \tau_x])$ is nonzero at u_0 and let us write $u_0 = \varphi_\alpha\left(\begin{smallmatrix} 1 & a_0 \\ 0 & 1 \end{smallmatrix}\right)$ for a suitable $a_0 \in \mathfrak{O}$ (more precisely $a_0 \in \mathfrak{M}^{g_x(\alpha)}$). Moreover, by assumption we can choose $t_0 \in T^1$ such that $\mathrm{Sh}_x(\gamma)(t_0) \neq 0$.

The cohomology class $\mathrm{Sh}_x([\xi, \tau_x]) \smile \mathrm{Sh}_x(\gamma)$ can be represented by an inhomogenous 2-cocycle in the following way:

$$\mathrm{Sh}_x([\xi, \tau_x]) \smile \mathrm{Sh}_x(\gamma) = \overline{\theta}, \quad \text{where} \quad \begin{aligned} \theta\colon I_x \times I_x &\longrightarrow k \\ (g, h) &\longmapsto \mathrm{Sh}_x([\xi, \tau_x])(g) \cdot \mathrm{Sh}_x(\gamma)(h). \end{aligned}$$

Assume by contradiction that the cup product is zero; this means that there exists a continuous map $\psi\colon I_x \longrightarrow k$ such that θ is the differential of ψ. Explicitly, this means that for all $g, h \in I_x$ one has

$$\mathrm{Sh}_x([\xi, \tau_x])(g) \cdot \mathrm{Sh}_x(\gamma)(h) = \psi(g) + \psi(h) - \psi(gh).$$

Plugging in $g \coloneqq u_0$ and $h \coloneqq t_0$, we get:

$$\psi(u_0 t_0) = \psi(u_0) + \psi(t_0) + c_0, \qquad \text{for some nonzero } c_0 \in k. \tag{126}$$

On the other side, we also get

$$\psi(gh) = \psi(g) + \psi(h), \qquad \text{if either } g \in T^1 \text{ or } h \in \mathfrak{U}_{(\alpha, g_x(\alpha))}. \tag{127}$$

Let

$$u_1 \coloneqq t_0^{-1} u_0 t_0 = \varphi_\alpha \begin{pmatrix} 1 & \alpha(t_0^{-1}) a_0 \\ 0 & 1 \end{pmatrix},$$

where we used the conjugation formula (1). Using the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, we have $\alpha(t_0^{-1}) \in 1 + \mathfrak{M} = 1 + p\mathfrak{O}$, and so we can write u_1 as $u_0 u_2^p$ for some $u_2 \in \mathfrak{U}_{(\alpha, g_x(\alpha))}$. Therefore we have

$$u_0 t_0 = t_0 u_1 = t_0 u_0 u_2^p.$$

Putting together what we have found, we finally reach the following contradiction:

$$\begin{aligned}
\psi(u_0) + \psi(t_0) + c_0 &= \psi(u_0 t_0) && \text{(by (126))} \\
&= \psi(t_0 u_0 u_2^p) && \text{(by the last equation)} \\
&= \psi(t_0) + \psi(u_0 u_2^p) && \text{(by (127))} \\
&= \psi(t_0) + \psi(u_0), && \begin{pmatrix} \text{since } \psi|_{\mathfrak{U}_{(\alpha, g_x(\alpha))}} \text{ is a group} \\ \text{homomorphism by (127)} \end{pmatrix}
\end{aligned}$$

which is against the fact that $c_0 \neq 0$. ∎

Before stating the first proposition describing $Z(E^*)^1$ for unramified extensions $\mathfrak{F}$ of $\mathbb{Q}_p$, we recall from Theorem 3.1.10 that $Z(E^*)^0$ can be described via the following isomorphism, where, as already recalled, $\widetilde{C} \coloneqq (C \cdot T^1)/T^1$:

$$\begin{aligned}
k[\widetilde{C}] &\longrightarrow Z(E^*)^0 \\
\underset{(\text{with } c \in \widetilde{C})}{(c)} &\longmapsto \tau_c.
\end{aligned}$$

Proposition 3.2.11. *Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has that $Z(E^*)^1$ can be described in the following way: there is a k-vector space decomposition*

$$Z(E^*)^1 = \bigoplus_{c \in \widetilde{C}} Z(E^*)^1_c, \qquad \text{where} \qquad Z(E^*)^1_c \coloneqq Z(E^*)^1 \cap H^1(I, \mathbf{X}(c)).$$

Moreover, one has an isomorphism of $Z(E^*)^0$-modules

$$\begin{aligned}
Z(E^*)^0 \otimes_k Z(E^*)^1_1 &\xrightarrow{\cong} Z(E^*)^1 \\
z \otimes \xi &\longmapsto z \cdot \xi
\end{aligned}$$

(here, $Z(E^*)^0 \otimes_k Z(E^*)^1_1$ denotes the free $Z(E^*)^0$-module obtained by base change from the k-vector space $Z(E^*)^1_1$). This isomorphism can also be described as

$$\begin{aligned}
k[\widetilde{C}] \otimes_k Z(E^*)^1_1 &\xrightarrow{\cong} Z(E^*)^1 \\
\underset{(\text{with } c \in \widetilde{C})}{(c) \otimes \xi} &\longmapsto \tau_c \cdot \xi \in Z(E^*)^1_c.
\end{aligned}$$

To complete the study of $Z(E^*)^1$ (if $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$) it remains to describe explicitly $Z(E^*)^1_c$ for all $c \in \widetilde{C}$, or, equivalently, to describe explicitly $Z(E^*)^1_1$ (this is equivalent because $Z(E^*)^1_1$ is isomorphic as a k-vector space to $Z(E^*)^1_c$, via multiplication by τ_c).

Proof of the proposition. Let $\beta \in Z(E^*)^1$, and let us write it as

$$\beta = \sum_{\substack{w \in \widetilde{W} \\ \text{s.t. } \ell(w) \leqslant L}} \beta_w,$$

for suitable $L \in \mathbb{Z}_{\geqslant 0}$ and $\beta_w \in H^1(I, \mathbf{X}(w))$. From the lemmas we have proved, we obtain the following constraints on the components β_w's.

- Lemma 3.2.6 tells us that for $w \in \widetilde{W} \smallsetminus (T/T^1)$ of length L one has $\beta_w = 0$.
- Lemma 3.2.7 tells us that for $x \in (T/T^1)$ of length L one has that $\mathrm{Sh}_x(\beta_x)$ is zero on the "unipotent factors" of the Iwahori decomposition of I_x.
- Now let $x \in (T/T^1) \smallsetminus \widetilde{C}$ of length L. We have just said that $\mathrm{Sh}_x(\beta_x)$ is zero on the "unipotent factors" of the Iwahori decomposition of I_x. If, by contradiction, $\mathrm{Sh}_x(\beta_x)$ were nonzero on T^1, then by Lemma 3.2.10 there would exist $\xi \in H^1(I, \mathbf{X}(1)) = H^1(I, k)$ such that $[\xi, \gamma]_{\mathrm{gr}} \neq 0$. But since multiplication by ξ on the left and on the right preserves the decomposition $E^1 = \bigoplus_{w \in \widetilde{W}} H^1(I, \mathbf{X}(w))$ this is against the assumption that $\beta \in Z(E^*)^1$. Therefore we have reached a contradiction, and this means that $\mathrm{Sh}_x(\beta_x)$ is zero also on T^1.

In conclusion, we have proved that if $w \in \widetilde{W}$ is of length L then β_w is nonzero at most if $w \in \widetilde{C}$. Since the elements of $\widetilde{C}$ have length zero (e.g., by the length formula (10)), we deduce that

$$\beta = \sum_{c \in \widetilde{C}} \beta_c.$$

For the same reason, we see that for all $j \in \mathbb{Z}_{\geqslant 0}$, for all $v \in \widetilde{W}$ and for all $\gamma \in H^j(I, \mathbf{X}(v))$, multiplication on the left or on the right by γ transforms the decomposition $\bigoplus_{c \in \widetilde{C}} H^1(I, \mathbf{X}(c))$ into the decomposition $\bigoplus_{c \in \widetilde{C}} H^1(I, \mathbf{X}(cv))$. Therefore, for all $c \in \widetilde{C}$ one has that $\beta_c \in Z(E^*)^1$. This proves that we have a decomposition

$$Z(E^*)^1 = \bigoplus_{c \in \widetilde{C}} Z(E^*)^1_c, \qquad \text{where} \qquad Z(E^*)^1_c \coloneqq Z(E^*)^1 \cap H^1(I, \mathbf{X}(c)).$$

Now, let us look the map

$$\begin{array}{ccc} Z(E^*)^0 \otimes_k Z(E^*)^1_1 & \xrightarrow{\cong} & Z(E^*)^1 \\ \underset{(\text{with } c \in \widetilde{C})}{\tau_c \otimes \xi} & \longmapsto & \tau_c \cdot \xi, \end{array}$$

which is clearly a well defined homomorphism of $Z(E^*)^0$-modules. It is also easy to show that it is bijective, because on the left side we have a k-vector space decomposition $\bigoplus_{c \in \widetilde{C}} \tau_c \otimes Z(E^*)^1_1$, and the above map preserves the decompositions

$$\bigoplus_{c \in \widetilde{C}} \tau_c \otimes Z(E^*)^1_1 \longrightarrow \bigoplus_{c \in \widetilde{C}} Z(E^*)^1_c,$$

So bijectivity follows from the fact that for all $c \in \widetilde{C}$ one has a bijection

$$\begin{aligned} Z(E^*)^1_1 &\longleftrightarrow Z(E^*)^1_c \\ \xi &\longmapsto \tau_c \cdot \xi, \\ \tau_{c^{-1}} \cdot \xi' &\longleftarrow\!\shortmid \xi', \end{aligned}$$

thus ending the proof. ■

3.2.d Results about split tori

The two lemmas in this section are immediate consequences of the contravariant equivalence of abelian categories between the category of diagonalizable algebraic groups and the category of finitely generated abelian groups (see [Mil17, Theorem 12.9]). The second lemma will only be used in Subsection 3.2.j, and not to prove Theorem 3.2.26.

Lemma 3.2.12. *Let $\mathbf{S}_1$ and $\mathbf{S}_2$ be $\mathfrak{F}$-split tori, let $r_1 \coloneqq \dim \mathbf{S}_1$, let $r_2 \coloneqq \dim \mathbf{S}_2$, and let $f\colon \mathbf{S}_1 \longrightarrow \mathbf{S}_2$ be a morphism of algebraic tori. If $r_1 \leqslant r_2$, then there exist splittings of $\mathbf{S}_1$ and $\mathbf{S}_2$ and there exist integers $n_1, \dots, n_{r_1} \in \mathbb{Z}_{\geqslant 0}$ such that the following diagram commutes:*

$$\begin{tikzcd} \mathbf{S}_1 \arrow[rrr, "f"] \arrow[d, leftrightarrow, "\cong"'] & & & \mathbf{S}_2 \arrow[d, leftrightarrow, "\cong"] \\ \mathbb{G}_{\mathrm{m}}^{r_1} \arrow[rrr, "{(t_1,\dots,t_{r_1}) \mapsto \left(t_1^{n_1},\dots,t_{r_1}^{n_{r_1}},1,\dots,1\right)}"'] & & & \mathbb{G}_{\mathrm{m}}^{r_2}. \end{tikzcd}$$

Similarly, if $r_1 \geqslant r_2$, then there exist splittings of $\mathbf{S}_1$ and $\mathbf{S}_2$ and there exist integers $n_1, \dots, n_{r_2} \in \mathbb{Z}_{\geqslant 0}$ such that the following diagram commutes:

$$\begin{tikzcd} \mathbf{S}_1 \arrow[rrr, "f"] \arrow[d, leftrightarrow, "\cong"'] & & & \mathbf{S}_2 \arrow[d, leftrightarrow, "\cong"] \\ \mathbb{G}_{\mathrm{m}}^{r_1} \arrow[rrr, "{(t_1,\dots,t_{r_1}) \mapsto \left(t_1^{n_1},\dots,t_{r_2}^{n_{r_2}}\right)}"'] & & & \mathbb{G}_{\mathrm{m}}^{r_2}. \end{tikzcd}$$

Proof. This follows from the contravariant equivalence of abelian categories between the category of diagonalizable algebraic groups and the category of finitely generated abelian groups (see [Mil17, Theorem 12.9]) and from the existence of the Smith normal form for maps of finitely generated free abelian groups. ■

Before stating the next lemma, we recall that a finite linear algebraic group $\mathbf{F}$ over a field l is an affine group scheme over l such that $l[\mathbf{F}]$ has finite dimension as an l-vector space. Such dimension is called the **order** of $\mathbf{F}$, and it coincides with the order of $\mathbf{F}(\bar{l})$ if l has characteristic 0. If we assume that $\mathbf{F}$ is a finite diagonalizable group (over l), then $\mathbf{F} \cong \boldsymbol{\mu}_{n_1} \times \cdots \times \boldsymbol{\mu}_{n_m}$ for suitable $n_1, \dots, n_m \in \mathbb{Z}_{\geqslant 1}$ (see [Mil17, Proposition 12.3 and Theorem 12.9]), and then the order of $\mathbf{F}$ is $n_1 \cdots n_m$.

Lemma 3.2.13. *Let $\mathbf{S}_1$ and $\mathbf{S}_2$ be $\mathfrak{F}$-split tori, and let $f\colon \mathbf{S}_1 \longrightarrow \mathbf{S}_2$ be a morphism of algebraic tori, surjective and with finite kernel, say of order n. Let S_1^1 (respectively,*

S_2^1) *be the unique pro-p Sylow subgroup of the unique maximal compact subgroup of* S_1 *(respectively, of* S_2*). Let us consider the induced homomorphism of pro-p groups*

$$f^1\colon S_1^1 \longrightarrow S_2^1.$$

One has:

- f^1 *is injective if and only if either p does not divide n or* $\mathfrak{F}$ *does not contain non-trivial p-th roots of unity;*
- f^1 *is surjective if and only if p does not divide n.*

Proof. It is easy to see, for example using Lemma 3.2.12, that $\mathbf{S}_1$ and $\mathbf{S}_2$ have the same dimension, say r. Therefore, by Lemma 3.2.12 there exist splittings of $\mathbf{S}_1$ and of $\mathbf{S}_2$ and $n_1, \dots n_r \in \mathbb{Z}_{>0}$ (nonzero because otherwise f would not be surjective) such that the following diagram commutes:

$$\begin{tikzcd}
\mathbf{S}_1 \arrow[rr, "f"] \arrow[d, leftrightarrow, "\cong"'] & & \mathbf{S}_2 \arrow[d, leftrightarrow, "\cong"] \\
\mathbb{G}_{\mathrm{m}}^r \arrow[rr, "(t_1,\dots,t_r)\mapsto(t_1^{n_1},\dots,t_r^{n_r})"'] & & \mathbb{G}_{\mathrm{m}}^r.
\end{tikzcd}$$

So $\ker f \cong \boldsymbol{\mu}_{n_1} \times \cdots \times \boldsymbol{\mu}_{n_r}$ and $n = n_1 \cdots n_r$. Looking at the induced homomorphism of pro-p groups $f^1\colon S_1^1 \longrightarrow S_2^1$, we have

$$\begin{aligned}
\ker f^1 &= \big(\boldsymbol{\mu}_{n_1}(\mathfrak{F}) \cap (1+\mathfrak{M})\big) \times \cdots \times \big(\boldsymbol{\mu}_{n_r}(\mathfrak{F}) \cap (1+\mathfrak{M})\big), \\
\operatorname{coker} f^1 &= (1+\mathfrak{M})/(1+\mathfrak{M})^{n_1} \times \cdots \times (1+\mathfrak{M})/(1+\mathfrak{M})^{n_r}.
\end{aligned}$$

For all $m > 0$, one has that $\boldsymbol{\mu}_m(\mathfrak{F}) \cap (1+\mathfrak{M})$ is non-trivial if and only if p divides m and $\mathfrak{F}$ (and hence $1+\mathfrak{M}$) contains non-trivial p-th roots, and so the claim about injectivity follows. As regards surjectivity, we note that $(1+\mathfrak{M})^m = 1+\mathfrak{M}$ if p does not divide m (for example because exponentiation by m is an invertible map with inverse exponentiation by $m^{-1} \in \mathbb{Z}_p^\times$) whereas if p divides m then

$$(1+\mathfrak{M})^m \subseteq (1+\mathfrak{M})^p \subseteq 1 + p\mathfrak{M} + \mathfrak{M}^p \subseteq 1 + \mathfrak{M}^2 \subsetneq 1 + \mathfrak{M},$$

and therefore it follows that f^1 is surjective if and only if p does not divide n. ■

3.2.e A result about the fundamental group

Assuming that $\mathbf{G}$ is semisimple, its fundamental group can be defined in the following way (see, e.g., [Hum98, §31.1]):

$$\begin{aligned}
\Lambda_{\mathrm{w}}/X^*(\mathbf{T}) \quad \text{where } \Lambda_{\mathrm{w}} &:= \{\chi \in X^*(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{R} \mid \langle \check{\alpha}, \chi \rangle \in \mathbb{Z} \text{ for all } \alpha \in \Phi\} \\
&= \{\chi \in X^*(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{R} \mid \langle \check{\alpha}, \chi \rangle \in \mathbb{Z} \text{ for all } \alpha \in \Pi\};
\end{aligned} \tag{128}$$

here the equality stems from the fact that the simple coroots form a basis of the coroot lattice. With this definition, the fundamental group is abstractly isomorphic to the following group (see [Con20, §9.3]):

$$X_*(\mathbf{T})/\operatorname{span}_{\mathbb{Z}} \check{\Phi},$$

which can also be expressed as

$$X_*(\mathbf{T})/\operatorname{span}_{\mathbb{Z}} \check{\Pi}.$$

The following lemma should be well-known, but the author was not able to find a reference; our proof is inspired by [Mil17, Proof of Proposition 21.8].

Lemma 3.2.14. *Assume that* $\mathbf{G}$ *is semisimple. One has that the morphism of algebraic tori*

$$\prod_{\alpha\in\Pi} \breve{\alpha}\colon \prod_{\alpha\in\Pi} \mathbb{G}_{\mathrm{m}} \longrightarrow \mathbf{T}$$

is surjective and has finite kernel whose order is equal to the order of the fundamental group of $\mathbf{G}$.

Remark 3.2.15. It follows from the lemma that if $\mathbf{G}$ is semisimple simply connected then the map

$$\prod_{\alpha\in\Pi} \breve{\alpha}\colon \prod_{\alpha\in\Pi} \mathbb{G}_{\mathrm{m}} \longrightarrow \mathbf{T}$$

is an isomorphism. Indeed a morphism of split tori that has trivial kernel and cokernel is an isomorphism, by the contravariant equivalence of categories between split tori and finitely generated abelian groups.

Proof of the lemma. Let us consider the exact sequence

$$1 \longrightarrow \ker \breve{\boldsymbol{\alpha}} \longrightarrow \textstyle\prod_{\alpha\in\Pi} \mathbb{G}_{\mathrm{m}} \xrightarrow{\breve{\boldsymbol{\alpha}} := \prod_{\alpha\in\Pi} \breve{\alpha}} \mathbf{T} \longrightarrow \operatorname{coker} \breve{\boldsymbol{\alpha}} \longrightarrow 1,$$

and let us apply the contravariant functor X^*, which defines a contravariant equivalence of abelian categories between the category of diagonalizable algebraic groups and the category of finitely generated abelian groups (see [Mil17, Theorem 12.9]), thus getting an exact sequence

$$0 \longrightarrow X^*(\operatorname{coker} \breve{\boldsymbol{\alpha}}) \longrightarrow X^*(\mathbf{T}) \xrightarrow{\chi\mapsto(\langle\breve{\alpha},\chi\rangle)_{\alpha\in\Pi}} \textstyle\bigoplus_{\alpha\in\Pi} \mathbb{Z} \longrightarrow X^*(\ker \breve{\boldsymbol{\alpha}}) \longrightarrow 0.$$

Since $\langle -,- \rangle$ is a perfect pairing, the map in the middle is injective, and therefore $X^*(\operatorname{coker} \breve{\boldsymbol{\alpha}})$ is trivial. This means that $\operatorname{coker} \breve{\boldsymbol{\alpha}}$ is trivial by the contravariant equivalence of abelian categories. As regards the kernel of $\breve{\boldsymbol{\alpha}}$, we have

$$X^*(\ker \breve{\boldsymbol{\alpha}}) \cong \frac{\bigoplus_{\alpha\in\Pi} \mathbb{Z}}{\{(\langle\breve{\alpha},\chi\rangle)_{\alpha\in\Pi} \ \mid\ \chi \in X^*(\mathbf{T})\}}.$$

The map

$$\begin{aligned} \Lambda_{\mathrm{w}} &\longrightarrow \bigoplus_{\alpha\in\Pi} \mathbb{Z} \\ \chi &\longmapsto (\langle\breve{\alpha},\chi\rangle)_{\alpha\in\Pi} \end{aligned}$$

is an isomorphism by definition of the weight lattice Λ_{w} and by the fact that $(\breve{\alpha})_{\alpha\in\Pi}$ is an $\mathbb{R}$-basis of $X^*(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{R}$. It follows that we get isomorphisms

$$X^*(\ker \breve{\boldsymbol{\alpha}}) \cong \frac{\bigoplus_{\alpha\in\Pi} \mathbb{Z}}{\{(\langle\breve{\alpha},\chi\rangle)_{\alpha\in\Pi} \ \mid\ \chi \in X^*(\mathbf{T})\}} \cong \Lambda_{\mathrm{w}}/X^*(\mathbf{T}).$$

In other words, $X^*(\ker \breve{\boldsymbol{\alpha}})$ is isomorphic to the fundamental group of $\mathbf{G}$. Let us write

$$X^*(\ker \breve{\boldsymbol{\alpha}}) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_m\mathbb{Z},$$

for suitable $m \in \mathbb{Z}_{\geqslant 0}$ and $n_1, \dots, n_m \in \mathbb{Z}_{\geqslant 1}$. The functor $M \mapsto \operatorname{Spec}(k[M])$ is a quasi-inverse of the functor $X^*(\_)$, and applying it to the group $\mathbb{Z}/n\mathbb{Z}$ (for $n \in \mathbb{Z}_{\geqslant 1}$) we get $\boldsymbol{\mu}_n$: see [Mil17, Proposition 12.3 and Theorem 12.9] for both of these facts. This means that

$$\ker \breve{\boldsymbol{\alpha}} \cong \boldsymbol{\mu}_{n_1} \times \cdots \times \boldsymbol{\mu}_{n_m},$$

and so we see that $\ker \breve{\boldsymbol{\alpha}}$ is a finite algebraic group of order equal to the order of $X^*(\ker \breve{\boldsymbol{\alpha}})$ and hence to the order of the fundamental group of $\mathbf{G}$. ∎

3.2.f Results about the commutator subgroup of the group of rational points

We are now going to collect some facts about the commutator subgroup $[G, G]$ of the group of $\mathfrak{F}$-rational points G of $\mathbf{G}$. Here we will always mean the commutator subgroup in the abstract group-theoretical sense, but we will prove that it is automatically closed in the $\mathfrak{F}$-topology.

The main result in this subsection is that the abelianization $G/[G, G]$ is isomorphic to a quotient of T, quotient that we will describe explicitly (Lemma 3.2.19). This is probably well known, but the author was not able to find the precise statement the literature. Similar problems are studied in [BT73], and it would be possible to reduce our statements to various results in loc. cit. (see in particular [BT73, (1) in the proof of Proposition 3.19, Corollaire 6.5, Remarque 6.6, Proposition 6.14]). However, since one would still need to do some work to extend results from the semisimple case to general case and since it is possible to write down a more self-contained and relatively short proof, we carry out such proof, without relying on the results in [BT73].

From now on we will use the following notation.

- We define $\mathbf{G}' := [\mathbf{G}, \mathbf{G}]$ (the derived subgroup of $\mathbf{G}$) and we define $\mathbf{T}' := \mathbf{T} \cap \mathbf{G}'$: this is a $\mathfrak{F}$-split maximal torus of $\mathbf{G}'$ (and so in particular $\mathbf{G}'$ is $\mathfrak{F}$-split); indeed $\mathbf{T}'$ is a maximal $\mathfrak{F}$-torus of $\mathbf{G}'$ by [CGP15, Lemma 1.2.5 part (iii)], and, by the same argument with $\overline{\mathfrak{F}}$ in place of $\mathfrak{F}$, it is a maximal $\overline{\mathfrak{F}}$-torus. Moreover, the fact that $\mathbf{T}'$ is $\mathfrak{F}$-split follows from the fact that a $\mathfrak{F}$-subtorus of a $\mathfrak{F}$-split torus is split (see [Bor91, Chapter III, §8.14, Corollary]).

- We consider the fundamental central covering $\widetilde{\mathbf{G}} \longrightarrow \mathbf{G}'$ of the derived group $\mathbf{G}'$. The existence of the fundamental central covering of a split semisimple group, such as $(\mathbf{G}', \mathbf{T}')$, can be proved via the "Existence theorem" as in [Mil17, Corollary 23.56], constructing it from an isogeny of root data in the sense of [Mil17, Definition 23.1]: in particular $\widetilde{\mathbf{G}}$ comes equipped with a $\mathfrak{F}$-split maximal torus $\widetilde{\mathbf{T}}$ and and the central isogeny $\widetilde{\mathbf{G}} \longrightarrow \mathbf{G}'$ sends $\widetilde{\mathbf{T}}$ to $\mathbf{T}'$.

- We thus have the following homomorphisms, whose composite will be denoted by $f_\sim$:

$$f_\sim\colon \quad (\widetilde{\mathbf{G}}, \widetilde{\mathbf{T}}) \xrightarrow{\quad f_{\sim,1} \quad} (\mathbf{G}', \mathbf{T}') \xrightarrow{\qquad\quad} (\mathbf{G}, \mathbf{T}),$$

and the three root systems involved can be identified (since the three adjoint groups coincide).

The following lemma is proved in [uu13]. For convenience of the reader, we hereby add the argument.

Lemma 3.2.16. *One has* $[G, G] \subseteq f_\sim(\widetilde{G})$*.*

Proof (from [uu13]). By the universal property of the quotient of an algebraic subgroup over a subgroup, the commutator map $c\colon \mathbf{G}\times\mathbf{G} \longrightarrow \mathbf{G}$ factors (as a morphism of schemes over $\mathfrak{F}$) through the quotient

$$\begin{tikzcd}
\mathbf{G}\times\mathbf{G} \arrow[rr, "c"] \arrow[dr] & & \mathbf{G}. \\
& \dfrac{\mathbf{G}\times\mathbf{G}}{Z(\mathbf{G})\times Z(\mathbf{G})} = (\mathbf{G}/Z(\mathbf{G}))\times(\mathbf{G}/Z(\mathbf{G})) \arrow[ur, dashed, "\exists"'] &
\end{tikzcd}$$

Denoting by $\widetilde{c}$ the commutator map on $\widetilde{\mathbf{G}}$, we can of course repeat the same argument, finding a commutative diagram

$$\begin{tikzcd}
\widetilde{\mathbf{G}}\times\widetilde{\mathbf{G}} \arrow[rr, "\widetilde{c}"] \arrow[dr] & & \widetilde{\mathbf{G}}. \\
& \dfrac{\widetilde{\mathbf{G}}\times\widetilde{\mathbf{G}}}{Z(\widetilde{\mathbf{G}})\times Z(\widetilde{\mathbf{G}})} = \left(\widetilde{\mathbf{G}}/Z(\widetilde{\mathbf{G}})\right)\times\left(\widetilde{\mathbf{G}}/Z(\widetilde{\mathbf{G}})\right) \arrow[ur, dashed, "\exists"'] &
\end{tikzcd}$$

As we have already remarked, the adjoint groups $\widetilde{\mathbf{G}}/Z(\widetilde{\mathbf{G}})$ and $\mathbf{G}/Z(\mathbf{G})$ can be identified via $f_\sim$, and so we get the following commutative diagram (the fact that the square on the right commutes can be proved by remarking that all the other squares and triangles commute and that the oblique arrow at the top left is surjective):

$$\begin{tikzcd}
\widetilde{\mathbf{G}}\times\widetilde{\mathbf{G}} \arrow[rr, "\widetilde{c}"] \arrow[dr] \arrow[dd, "f_\sim\times f_\sim"'] & & \widetilde{\mathbf{G}} \arrow[dd, "f_\sim"] \\
& \left(\widetilde{\mathbf{G}}/Z(\widetilde{\mathbf{G}})\right)\times\left(\widetilde{\mathbf{G}}/Z(\widetilde{\mathbf{G}})\right) \arrow[ur, dashed] \arrow[dd, "\cong"] & \\
\mathbf{G}\times\mathbf{G} \arrow[rr, "c"] \arrow[dr] & & \mathbf{G}. \\
& (\mathbf{G}/Z(\mathbf{G}))\times(\mathbf{G}/Z(\mathbf{G})) \arrow[ur, dashed] &
\end{tikzcd}$$

Considering the composite of suitable maps in the above commutative diagram, we get a morphism of $\mathfrak{F}$-schemes $\varphi\colon \mathbf{G}\times\mathbf{G}\longrightarrow\widetilde{\mathbf{G}}$ such that the following diagram commute:

$$\begin{tikzcd}
\mathbf{G}\times\mathbf{G} \arrow[rr, "c"] \arrow[dr, "\varphi"'] & & \mathbf{G}. \\
& \widetilde{\mathbf{G}} \arrow[ur, "f_\sim"'] &
\end{tikzcd}$$

Therefore, passing to $\mathfrak{F}$-rational points, we see that $[G,G]\subseteq f_\sim(\widetilde{G})$, as we wanted to show. ■

Remark 3.2.17. Even if we will only need the inclusion of the previous lemma, it is actually true that $[G,G]=f_\sim(\widetilde{G})$. This is shown in [uu13] using (proven cases of) the Kneser–Tits conjecture. However, this fact will also follow from the next results we will prove: see Remark 3.2.20.

Remark 3.2.18. For all roots $\alpha\in\Phi$ let us denote by $\breve{\alpha}_{\widetilde{\mathbf{G}}}$ the morphism "$\breve{\alpha}$" relative to the pair $(\widetilde{\mathbf{G}},\widetilde{\mathbf{T}})$, whereas we will still denote by $\breve{\alpha}$ the one relative to the pair $(\mathbf{G},\mathbf{T})$, which is the same as the one relative to the pair $(\mathbf{G}',\mathbf{T}')$. Recall that since $\widetilde{\mathbf{G}}$ is semisimple simply connected, the map

$$\prod_{\alpha\in\Pi}\breve{\alpha}_{\widetilde{\mathbf{G}}}\colon \prod_{\alpha\in\Pi}\mathbb{G}_{\mathrm{m}}\longrightarrow\widetilde{\mathbf{T}}$$

is an isomorphism (Remark 3.2.15). Finally, since $f_{\sim,1}$ is a central isogeny between $(\widetilde{\mathbf{G}},\widetilde{\mathbf{T}})$ and $(\mathbf{G}',\mathbf{T}')$, it follows that $f_{\sim,1}\circ\breve{\alpha}_{\widetilde{\mathbf{G}}}=\breve{\alpha}$ (see [Mil17, Proposition 23.5]).

We conclude that we have the following commutative diagram:

$$\begin{tikzcd}
\prod_{\alpha\in\Pi}\mathbb{G}_{\mathrm{m}} \arrow[rr, "\prod_{\alpha\in\Pi}\breve{\alpha}_{\widetilde{\mathbf{G}}}", "\cong"'] \arrow[dr, "\prod_{\alpha\in\Pi}\breve{\alpha}"'] & & \widetilde{\mathbf{T}} \arrow[dl, "f_{\sim,1}"] \\
& \mathbf{T}'. &
\end{tikzcd}$$

In particular, the following equality holds:

$$\begin{aligned} T_{\breve{\Phi}} &:= \mathrm{Image}\left(\prod_{\alpha\in\Pi}\breve{\alpha}\colon \mathfrak{F}^{\times} \longrightarrow T'\right) \\ &= \mathrm{Image}\left(f_{\sim,1}\colon \widetilde{T} \longrightarrow T'\right). \end{aligned} \tag{129}$$

Lemma 3.2.19. *Let $T_{\breve{\Phi}}$ be as above. One has an isomorphism of topological groups*

$$\begin{aligned} T/T_{\breve{\Phi}} &\xrightarrow{\cong} G/[G,G] \\ \bar{t} &\longmapsto \bar{t}, \end{aligned}$$

and moreover $[G,G]$ is closed in G (for the $\mathfrak{F}$-topology) and $T_{\breve{\Phi}} \subseteq T' \subseteq T$ are closed inclusions (for the $\mathfrak{F}$-topology).

Proof. Let us divide the proof into the following parts: the map is well-defined, injective, surjective, a homeomorphism (and therefore an isomorphism of topological groups), and we have the claimed closed inclusions.

- Let us prove that the map in the statement is well-defined.

  We have to prove that for all $\alpha\in\Pi$ and for all $a\in\mathfrak{F}^{\times}$ one has $\breve{\alpha}(a)\in[G,G]$. It is well-known that $\mathrm{SL}_n(l)$ is generated by transvection matrices for all $n\geqslant 2$ and all fields l; moreover if the field l has at least 4 elements, it is easy to show that transvection matrices are in the commutator subgroup: we thus conclude that $[\mathrm{SL}_n(l),\mathrm{SL}_n(l)]=\mathrm{SL}_n(l)$ if l is a field with at least 4 elements. In particular, we obtain that $\breve{\alpha}(a)\in\varphi_\alpha\big([\mathrm{SL}_2(\mathfrak{F}),\mathrm{SL}_2(\mathfrak{F})]\big)\subseteq[G,G]$, as we wanted.

- Let us prove that the map in the statement is injective.

  Let $t\in T\cap[G,G]$, and let us show that $t\in T_{\breve{\Phi}}$. Since $[G,G]\subseteq f_{\sim}(\widetilde{G})$ (Lemma 3.2.16), we can write $t=f_{\sim}(\widetilde{g})$ for some $\widetilde{g}\in\widetilde{G}$. If we prove that $\widetilde{g}\in\widetilde{T}$ then we are done by the second definition of $T_{\breve{\Phi}}$, and to prove this claim it is sufficient to show that

  (Claim) $$\widetilde{g}\in\widetilde{\mathbf{T}}(\overline{\mathfrak{F}}).$$

  One has that $t\in T\cap[G,G]\subseteq\mathbf{T}(\overline{\mathfrak{F}})\cap\mathbf{G}'(\overline{\mathfrak{F}})=\mathbf{T}'(\overline{\mathfrak{F}})$, and the restriction $f_{\sim,1}\colon\widetilde{\mathbf{T}}(\overline{\mathfrak{F}})\longrightarrow\mathbf{T}'(\overline{\mathfrak{F}})$ is surjective: indeed, a surjective morphism of algebraic group varieties is such that the image of a maximal torus is a maximal torus (see [Bor91, Proposition 11.14 part (1)] or [Mil17, Proposition 17.20]). Therefore, we get that $t=f_{\sim}(\widetilde{t})$ for some $\widetilde{t}\in\widetilde{\mathbf{T}}(\overline{\mathfrak{F}})$. In particular $\widetilde{g}\cdot\widetilde{t}^{-1}\in\ker(f_{\sim,1})(\overline{\mathfrak{F}})$; but $\ker(f_{\sim,1})$ is contained in the centre of $\widetilde{\mathbf{G}}$, and in a reductive group the centre is contained in every maximal torus (see [Hum98, Section 26.2, Corollary A.(b)]). Therefore $\widetilde{g}\cdot\widetilde{t}^{-1}\in\widetilde{\mathbf{T}}(\overline{\mathfrak{F}})$ and so $\widetilde{g}\in\widetilde{\mathbf{T}}(\overline{\mathfrak{F}})$, as we wanted to prove.

- Let us prove that the map in the statement is surjective.

  Let us use the Bruhat decomposition:

$$G = \dot{\bigcup_{w \in W_0}} U \cdot n_w \cdot T \cdot U,$$

  where $n_w \in N$ is a representative of $w \in W_0$ and where $\mathbf{U}$ is the unipotent subgroup generated by the $\mathbf{U}_\alpha$'s for $\alpha \in \Phi^+$ (and, as an algebraic variety, it is isomorphic via the multiplication map to the direct product of the $\mathbf{U}_\alpha$'s: see [Mil17, Theorem 21.68 (a)]; in particular, U is generated by the U_α's).

  As we shown before, for all $\alpha \in \Phi$, an element in the image of $\varphi_\alpha\colon \mathrm{SL}_2(\mathfrak{F}) \longrightarrow G$ lies in the commutator subgroup $[G, G]$. Applying this to the elements $n_{s_{(\alpha,0)}}$ for all $\alpha \in \Pi$, we get that for all $w \in W_0$ one has $n_w \in [G, G]$ for a suitably chosen representative $n_w \in N$ of w. In a similar way one shows that $U_\alpha \subseteq [G, G]$ for all $\alpha \in \Phi^+$ and so $U \subseteq [G, G]$ (in this case the argument is simpler because we can consider the commutator $[\left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)] = \left(\begin{smallmatrix} 1 & (u^2-1)\cdot a \\ 0 & 1 \end{smallmatrix}\right)$ for all $a \in \mathfrak{F}$ and for a fixed $u \in \mathfrak{F}^\times$ having non-trivial square). In conclusion, by the Bruhat decomposition, we get that every element of G can be represented by an element of T in the quotient $G/[G, G]$, thus proving that the map in the statement is surjective.

- Let us prove that the map in the statement is a homeomorphism for the $\mathfrak{F}$-topology.

  Continuity is clear since the map in question is induced by the inclusion of T in G. It remains to show that the map

$$\begin{aligned} T &\longrightarrow G/[G, G] \\ t &\longmapsto \bar{t} \end{aligned}$$

  is open. We consider the map

$$\mathbf{U}^- \times \mathbf{T} \times \mathbf{U} \longrightarrow \mathbf{G} \tag{130}$$

  defined by multiplication, where $\mathbf{U}$ is the subgroup generated by the $\mathbf{U}_\alpha$'s for $\alpha \in \Phi^+$ and where $\mathbf{U}^-$ is the subgroup generated by the $\mathbf{U}_\alpha$'s for $\alpha \in \Phi^-$. We recall that the above map is an open immersion of schemes over $\mathfrak{F}$. An open immersion of $\mathfrak{F}$-schemes of finite type induces, taking $\mathfrak{F}$-rational points, an open immersion for the $\mathfrak{F}$-topology (see, e.g., [Con12, Proposition 3.1]). Therefore the map

$$U^- \times T \times U \longrightarrow G$$

  induced by multiplication is open for the $\mathfrak{F}$-topology. In particular, for every open subset V of T, one has that $U^- \cdot V \cdot U$ is open in G. But then the image of $U^- \cdot V \cdot U$ in $G/[G, G]$ is open in $G/[G, G]$ because the quotient map is always open for topological groups. But this last open image is just the image of V in $G/[G, G]$, since we have already remarked that $U \subseteq [G, G]$, and clearly the same holds for U^-. We have thus shown that the image in $G/[G, G]$ of every open subset V of T is open.

- Let us prove that the inclusions $T_{\check{\Phi}} \subseteq T' \subseteq T$ and $[G, G] \subseteq G$ are all closed.

  The fact that T' is closed in T is clear because $\mathbf{T}'$ is a closed subscheme of $\mathbf{T}$. The fact that $T_{\check{\Phi}}$ is closed in T' can be proved via the following more general statement:

if $\mathbf{S}_1$ and $\mathbf{S}_2$ are $\mathfrak{F}$-split tori, and if $\varphi\colon \mathbf{S}_1 \longrightarrow \mathbf{S}_2$ is a morphism of algebraic tori, then the induced map $\varphi\colon S_1 \longrightarrow S_2$ has closed image (for the $\mathfrak{F}$-topology). To show this, thanks to Lemma 3.2.12, it is enough to show that $(\mathfrak{F}^\times)^n$ is closed in $\mathfrak{F}^\times$ for all $n \in \mathbb{Z}$. This is immediate using the decomposition

$$(\mathfrak{F}^\times)^n = \pi^{n\mathbb{Z}} \times (\mathfrak{O}^\times)^n \subseteq \pi^{\mathbb{Z}} \times \mathfrak{O}^\times = \mathfrak{F}^\times,$$

since the factor $\pi^{\mathbb{Z}}$ is discrete, and the factor $\mathfrak{O}^\times$ is compact Hausdorff.

It remains to check that the inclusion $[G,G] \subseteq G$ is closed, but this now follows from the fact that the quotient $G/[G,G] \cong T/T_{\check{\Phi}}$ is Hausdorff since $T_{\check{\Phi}}$ is closed in T. ■

Remark 3.2.20. As claimed in Remark 3.2.17, the inclusion $[G,G] \subseteq f_\sim(\widetilde{G})$ of Lemma 3.2.16 is actually an equality. Indeed, this is equivalent to saying that $[\widetilde{G},\widetilde{G}] = \widetilde{G}$. If we apply the last lemma to $\widetilde{G}$ in place of G, we see that this is equivalent to the condition $\widetilde{T}_{\check{\Phi}} = \widetilde{T}$, and this is clear from the definition of $\widetilde{T}_{\check{\Phi}}$ (129), because $f_\sim$ is the identity in this setting.

3.2.g The 1st graded piece of the centre for unramified extensions of $\mathbb{Q}_p$: full description in the general case

In this subsection we are going to complete the description of the 1st graded piece of the centre of E^* under the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. Recall from Proposition 3.2.11 that it remains to describe $Z(E^*)^1 \cap H^1(I, \mathbf{X}(1))$.

Let us define

$$T^1_{\check{\Phi}} \coloneqq \mathrm{Image}\left(\textstyle\prod_{\alpha\in\Pi} \check{\alpha}\colon\ \prod_{\alpha\in\Pi}(1+\mathfrak{M}) \longrightarrow (T')^1\right). \tag{131}$$

It is easy to check using Lemma 3.2.12 that $T^1_{\check{\Phi}}$ is the (unique) pro-p Sylow subgroup of the unique maximal compact subgroup of $T_{\check{\Phi}}$ (which we defined in (129)).

Lemma 3.2.21. *Assume either that $p \neq 2$ or that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has that $T^1_{\check{\Phi}}$ is trivial in the Frattini quotient of I.*

Proof. We are going to give two different proofs in the two (very overlapping) cases $p \neq 2$ and $\mathfrak{F}$ unramified extension of $\mathbb{Q}_p$, both of them basically taken from [OS18, §3.8]. Let $I^{(\mathrm{SL}_2)}$ be the standard pro-p Iwahori subgroup of $\mathrm{SL}_2(\mathfrak{F})$ (as in Section 1.5).

- If $p \neq 2$, then it is easy to compute the commutator subgroup $[I^{(\mathrm{SL}_2)}, I^{(\mathrm{SL}_2)}]$ explicitly (see [OS18, Proposition 3.62 i)]) and in particular to show that

$$\left\{\begin{pmatrix} x & 0 \\ 0 & x^{-1}\end{pmatrix} \;\middle|\; x \in 1+\mathfrak{M}\right\} \subseteq \left[I^{(\mathrm{SL}_2)}, I^{(\mathrm{SL}_2)}\right].$$

  Using the maps φ_α's for $\alpha \in \Pi$, we see that the image of the map $\prod_{\alpha\in\Pi} \check{\alpha}\big|_{1+\mathfrak{M}}$ (i.e., $T^1_{\check{\Phi}}$) is contained in the commutator subgroup $[I,I]$, and in particular it is trivial in the Frattini quotient of I.

- If $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, then we follow the proof of [OS18, Proposition 3.64 i)], which is stated only for $\mathfrak{F} = \mathbb{Q}_p$ but basically works for all unramified extensions. For all $a \in \mathfrak{O}$ let us set:

$$u_+(a) \coloneqq \begin{pmatrix} 1 & a \\ 0 & 1\end{pmatrix}, \qquad\qquad u_-(a) \coloneqq \begin{pmatrix} 1 & 0 \\ a & 1\end{pmatrix}.$$

One can check the following equality for all $a \in \mathfrak{O}$:

$$\begin{pmatrix} 1+ap & 0 \\ 0 & (1+ap)^{-1} \end{pmatrix} = [u_+(1), u_-(pa)] \cdot \Big(u_-(pa) u_+(\tfrac{a}{1+pa})^p u_-(pa)^{-1} \Big) \cdot u_-(-pa^2)^p.$$

The first factor of this decomposition is a commutator of elements of $I^{(\mathrm{SL}_2)}$; the second factor is conjugate in $I^{(\mathrm{SL}_2)}$ to a p-th power, and the third factor is a p-th power in $I^{(\mathrm{SL}_2)}$. Applying φ_α (for $\alpha \in \Pi$), we get that $\breve{\alpha}(1+ap)$ is trivial in the Frattini quotient of I. Now we use the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, yielding that every element of $1+\mathfrak{M}$ is representable as $1+ap$ for some $a \in \mathfrak{O}$, and so we have proved that the image of the map $\prod_{\alpha\in\Pi} \breve{\alpha}\big|_{1+\mathfrak{M}}$ (i.e., $T^1_{\breve{\Phi}}$) is trivial in the Frattini quotient of I. ■

Lemma 3.2.22. *The pro-p group $T^1/T^1_{\breve{\Phi}}$ is a direct factor (as a topological group) of the locally profinite group $T/T_{\breve{\Phi}} \cong G/[G,G]$ (where the isomorphism holds by Lemma 3.2.19).*

Proof. By Lemma 3.2.12, there exists a commutative diagram of the following form, where the vertical maps come from isomorphism of $\mathfrak{F}$-split tori, where $r := \dim \mathbf{T}$ and $r' := \#\Pi = \dim \mathbf{T}'$, and where $n_1, \dots n_{r'}$ are suitable integers:

$$\begin{tikzcd}
\prod_{\alpha\in\Pi} \mathfrak{F}^\times \arrow[rr, "\prod_{\alpha\in\Pi}\breve{\alpha}"] \arrow[d, leftrightarrow, "\cong"'] & & T \arrow[d, leftrightarrow, "\cong"] \\
(\mathfrak{F}^\times)^{r'} \arrow[rr, "{(t_1,\dots,t_{r'}) \mapsto \left(t_1^{n_1},\dots,t_{r'}^{n_{r'}},1,\dots,1\right)}"'] & & (\mathfrak{F}^\times)^r.
\end{tikzcd}$$

Therefore, via the isomorphism on the right side of the diagram, we have:

$$\begin{aligned}
T/T_{\breve{\Phi}} &\cong (\mathfrak{F}^\times/(\mathfrak{F}^\times)^{n_1}) \times \cdots \times (\mathfrak{F}^\times/(\mathfrak{F}^\times)^{n_{r'}}) \times \mathfrak{F}^\times \times \cdots \times \mathfrak{F}^\times, \\
T^1/T^1_{\breve{\Phi}} &\cong \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^{n_1}} \times \cdots \times \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^{n_{r'}}} \times (1+\mathfrak{M}) \times \cdots \times (1+\mathfrak{M}).
\end{aligned}$$

Using the factorization $\mathfrak{F}^\times = \pi^{\mathbb{Z}} \times \boldsymbol{\mu}_{q-1}(\mathfrak{F}) \times (1+\mathfrak{M})$, we see that $T^1/T^1_{\breve{\Phi}}$ is a direct factor (as a topological group) of $T/T_{\breve{\Phi}}$. ■

Remark 3.2.23. Although we will not use this, it is interesting to compare this result with the following: in [Koz18, Lemma 5.1] it is proved that if $p \neq 2, 3$ then $T^1/T^1_{\breve{\Phi}}$ is a direct factor of $I/\overline{[I,I]}$.

Lemma 3.2.24. *Let $\psi\colon G \longrightarrow k$ be a homomorphism of topological groups. Let us define $\psi_I \in H^1(I,k)$ as the restriction of ψ to I and, for all $c \in \widetilde{C}$, let us define $\psi_c := \mathrm{Sh}_c^{-1}(\psi_I) \in H^1(I, \mathbf{X}(c))$. One has that ψ_c is in the centre of E^*.*

Proof. To show our claim that $\psi_c \in Z(E^*)$, let us first prove that ψ_c is centralized by the whole E^0, i.e., that it commutes with τ_w for all $w \in \widetilde{W}$: recall that c has length zero (see Theorem 3.1.10), so the formulas for the products are "the simple ones", and applying them we find that

$$\begin{aligned}
\psi_c \cdot \tau_w &\in H^1(I, \mathbf{X}(cw)), \\
\tau_w \cdot \psi_c &\in H^1(I, \mathbf{X}(wc)) = H^1(I, \mathbf{X}(cw)), \\
\mathrm{Sh}_{cw}(\psi_c \cdot \tau_w) &= \mathrm{res}^{I_c}_{I_{cw}} \psi_I = \psi\big|_{I_w}, \\
\mathrm{Sh}_{cw}(\tau_w \cdot \psi_c) &= \mathrm{res}^{wI_cw^{-1}}_{I_{wc}} w_*\psi_I = \psi\big(w^{-1} \cdot (_) \cdot w\big)\big|_{I_w} = \psi\big|_{I_w}.
\end{aligned} \tag{132}$$

We conclude that $\psi_c \cdot \tau_w = \tau_w \cdot \psi_c$.

Now we have to show that $\psi_c \in Z(E^*)$, i.e., that it commutes (in the "graded-commutative" sense) with every element of the form $\gamma \in H^i(I, \mathbf{X}(w))$ for $i \in \mathbb{Z}_{\geqslant 0}$ and $w \in \widetilde{W}$. We have already said that c has length zero, and so we can apply the formula relating the (opposite of the) Yoneda product and the cup product (Corollary 1.9.3), finding that

$$\begin{aligned}
\psi_c \cdot \gamma &= (\psi_c \cdot \tau_w) \smile (\tau_c \cdot \gamma) \\
&= (\tau_w \cdot \psi_c) \smile (\tau_c \cdot \gamma) && \text{(since } \psi_c \text{ and } \tau_w \text{ commute)} \\
&= (\tau_w \cdot \psi_c) \smile (\gamma \cdot \tau_c) && \text{(because } \tau_c \in Z(E^*)\text{, see Theorem 3.1.10)} \\
&= (-1)^i (\gamma \cdot \tau_c) \smile (\tau_w \cdot \psi_c) \\
&= (-1)^i \gamma \cdot \psi_c,
\end{aligned}$$

i.e., ψ_c and γ commute (in the "graded-commutative" sense). ■

Proposition 3.2.25. *Assume either that $p \neq 2$ or that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, and let $c \in \widetilde{C}$. Using the notation*

$$Z(E^*)^1_c \coloneqq Z(E^*)^1 \cap H^1(I, \mathbf{X}(c))$$

and considering the image via the Shapiro isomorphism

$$\mathrm{Sh}_c\left(Z(E^*)^1_c\right) \subseteq H^1(I_c, k) = H^1(I, k),$$

one has that the restriction map $\mathrm{res}^I_{T^1} \colon H^1(I, k) \longrightarrow H^1(T^1, k)$ induces an isomorphism

$$\mathrm{Sh}_c\left(Z(E^*)^1_c\right) \cong H^1\big(T^1/T^1_{\check{\Phi}}, k\big),$$

where $T^1_{\check{\Phi}}$ was defined in (131).

Proof. Let us show that the map

$$\begin{aligned}
\mathrm{Sh}_c\left(Z(E^*)^1_c\right) &\longrightarrow H^1\big(T^1/T^1_{\check{\Phi}}, k\big) \\
\xi &\longmapsto \left(\begin{aligned} T^1/T^1_{\check{\Phi}} &\longrightarrow k \\ \bar{t} &\longmapsto \xi(t) \end{aligned} \right)
\end{aligned}$$

is well-defined, injective and surjective.

- The above map is well-defined (and would be well-defined on the whole $H^1(I, k)$), because we have shown in Lemma 3.2.21 that $T^1_{\check{\Phi}}$ is trivial in the Frattini quotient of I.

- The above map is injective because an element in $\mathrm{Sh}_c\left(Z(E^*)^1_c\right)$ (which is a homomorphism of topological groups from I to k) is zero on the the "unipotent factors" of the Iwahori decomposition of I (see Lemma 3.2.7).

- It remains to show that the above map is surjective. Lemma 3.2.22 tells us that $T^1/T^1_{\check{\Phi}}$ is a direct factor of $G/[G, G]$: in other words, we can fix a splitting

$$\begin{tikzcd} T^1/T^1_{\check{\Phi}} \arrow[r, "\bar{t} \mapsto \bar{t}"] & G/[G, G], \arrow[l, bend left, dashed, "\sigma"] \end{tikzcd}$$

Given $\xi \in H^1\left(T^1/T^1_{\check{\Phi}}, k\right)$, we can define ξ_I as the composite

$$\xi_I\colon \quad I \xrightarrow{\ \subseteq\ } G \xrightarrow{\text{quot.}} G/[G,G] \xrightarrow{\ \sigma\ } T^1/T^1_{\check{\Phi}} \xrightarrow{\ \xi\ } k.$$

It is clear that ξ_I is an element of $H^1(I,k)$ whose image in $H^1\big(T^1/T^1_{\check{\Phi}}, k\big)$ is equal to ξ. It remains to check that $\xi_I \in \mathrm{Sh}_c\left(Z(E^*)^1_c\right)$, i.e., that $\mathrm{Sh}_c^{-1}(\xi_I)$ is in the centre of E^*. Since ξ_I is the restriction of a homomorphism of topological groups $G \longrightarrow k$, this last claim follows from Lemma 3.2.24. ■

Theorem 3.2.26. *Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has that $Z(E^*)^1$ can be described in the following way: there is a k-vector space decomposition*

$$Z(E^*)^1 = \bigoplus_{c\in\widetilde{C}} Z(E^*)^1_c, \qquad \text{where} \qquad Z(E^*)^1_c \coloneqq Z(E^*)^1 \cap H^1(I, \mathbf{X}(c)).$$

Moreover, one has an isomorphism of $Z(E^*)^0$-modules

$$\begin{aligned} Z(E^*)^0 \otimes_k Z(E^*)^1_1 &\xrightarrow{\ \cong\ } Z(E^*)^1 \\ z \otimes \xi &\longmapsto z\cdot \xi \end{aligned}$$

(here, $Z(E^*)^0 \otimes_k Z(E^*)^1_1$ denotes the free $Z(E^*)^0$-module obtained by base change from the k-vector space $Z(E^*)^1_1$). This isomorphism can also be described as

$$\begin{aligned} k[\widetilde{C}] \otimes_k Z(E^*)^1_1 &\xrightarrow{\ \cong\ } Z(E^*)^1 \\ \underset{(\text{with } c\in\widetilde{C})}{(c)\otimes\xi} &\longmapsto \tau_c\cdot\xi \in Z(E^*)^1_c. \end{aligned}$$

Finally, for all $c \in \widetilde{C}$, the restriction map $\mathrm{res}^I_{T^1}\colon H^1(I,k) \longrightarrow H^1(T^1,k)$ induces an isomorphism of k-vector spaces

$$\mathrm{Sh}_c\left(Z(E^*)^1_c\right) \cong H^1\big(T^1/T^1_{\check{\Phi}}, k\big),$$

where $T^1_{\check{\Phi}}$ was defined in (131).

Proof. The above statement combines the statements of Proposition 3.2.11 and of Proposition 3.2.25. ■

Remark 3.2.27. Under the assumptions of the theorem we have that the obvious inclusion

$$Z(E^*)^1 \subseteq Z_{E^0\cup H^1(I,\mathbf{X}(1))}(E^1)$$

is actually an equality. This is because to determine $Z(E^*)^1$ we have only used graded commutators with elements in E^0 and $H^1(I,\mathbf{X}(1))$ (see in particular Lemmas 3.2.6, 3.2.7 and 3.2.10).

Remark 3.2.28. With reference to the theorem, let us drop the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, but let us add the assumption that $p \neq 2$, in such a way that Proposition 3.2.25 is still applicable. Since the elements of $\widetilde{C}$ have length zero (e.g., by the length formula), it is easy to see that

$$Z(E^*)^1 \cap \Big(\bigoplus_{c\in\widetilde{C}} H^1(I,\mathbf{X}(c))\Big) = \bigoplus_{c\in\widetilde{C}} \big(Z(E^*)^1 \cap H^1(I,\mathbf{X}(c))\big) = \bigoplus_{c\in\widetilde{C}} Z(E^*)^1_c.$$

Applying Proposition 3.2.25, it is not difficult to see that one has the following isomorphism of $Z(E^*)^0$-modules (generalizing the above Theorem 3.2.26):

$$Z(E^*)^1 \cap \Big(\bigoplus_{c\in\widetilde{C}} H^1(I,\mathbf{X}(c))\Big) \cong Z(E^*)^0 \otimes_k Z(E^*)^1_1 \cong Z(E^*)^0 \otimes_k H^1\big(T^1/T^1_{\check{\Phi}}, k\big).$$

3.2.h Examples

In this subsection we will discuss the examples $\mathbf{G} = \mathrm{GL}_n$ and $\mathbf{G} = \mathrm{PGL}_n$.

Example 3.2.29. Assume that $\mathbf{G} = \mathrm{GL}_n$ let us choose $\mathbf{T}$ to be the diagonal torus. For the moment, let us not make any assumptions on $\mathfrak{F}$. Let $c \in \widetilde{C}$ and let

$$f\colon 1 + \mathfrak{M} \longrightarrow k$$

be a homomorphism of topological groups. Let $\xi_{c,f} \in H^1(I, \mathbf{X}(c)) \cong H^1(I, k)$ be the cohomology class such that $\mathrm{Sh}_c(\xi_{c,f})$ is the following homomorphism of topological groups:

$$\mathrm{Sh}_c(\xi_{c,f})\colon \quad I_c = I \xrightarrow{\quad\det\quad} 1 + \mathfrak{M} \xrightarrow{\quad f \quad} k.$$

Since $\mathrm{Sh}_c(\xi_{c,f})$ is the restriction to $I_c = I$ of a homomorphism of topological groups from G to k, Lemma 3.2.24 shows that $\xi_{c,f}$ lies in the centre of E^*.

So, even without assumptions on $\mathfrak{F}$, we have produced elements in $Z(E^*)^1$. Now, let us relate this to the description of $Z(E^*)^1$ of Theorem 3.2.26.

Let us still not make any assumption on $\mathfrak{F}$. Note that the determinant

$$\det\colon T^1 \longrightarrow 1 + \mathfrak{M}$$

is surjective and has kernel

$$T^1 \cap \mathrm{SL}_n(\mathfrak{F}) = T^1 \cap T' = (T')^1 = T^1_{\check{\Phi}};$$

here the second equality uses that $T^1 \cap T'$ is pro-p and contained in T', and the third equality uses that $T_{\check{\Phi}} = T'$ by Remark 3.2.15 (since $\mathbf{G}' = \mathrm{SL}_n$ is simply connected). Therefore the determinant induces an isomorphism

$$T^1/T^1_{\check{\Phi}} \longrightarrow 1 + \mathfrak{M}.$$

It follows that

$$H^1(1 + \mathfrak{M}, k) \cong H^1\left(T^1/T^1_{\check{\Phi}}, k\right)$$

via the determinant.

Now let us assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, in such a way that the description of $Z(E^*)$ of Theorem 3.2.26 holds. Then if we combine the above isomorphism with the isomorphism

$$H^1\left(I_c, k\right) \cong H^1\left(T^1/T^1_{\check{\Phi}}, k\right)$$

defined by the restriction map (see again Theorem 3.2.26), we obtain an isomorphism

$$H^1\left(I_c, k\right) \cong H^1(1 + \mathfrak{M}, k).$$

It is easy to check that the following is a right inverse of such isomorphism, hence an inverse:

$$\begin{aligned} H^1(1 + \mathfrak{M}, k) &\longrightarrow H^1\left(I_c, k\right) \\ f &\longmapsto f \circ \det = \mathrm{Sh}(\xi_{c,f}). \end{aligned}$$

This shows that, if $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, then the above procedure yields all the elements of $Z(E^*)^1$. Moreover, using again Theorem 3.2.26,

$$Z(E^*)^1 \cong Z(E^*)^0 \otimes_k H^1(1 + \mathfrak{M}, k)$$

as a $Z(E^*)^0$-module.

Without assumptions on $\mathfrak{F}$, instead, we still have a morphism of $Z(E^*)^0$-modules

$$\begin{aligned} Z(E^*)^0 \otimes_k H^1(1+\mathfrak{M}, k) &\longrightarrow Z(E^*)^1 \\ \underset{(\text{with } c \in \widetilde{C})}{\tau_c \otimes \xi} &\longmapsto \tau_c \otimes \xi_{1,f} = \xi_{c,f}, \end{aligned}$$

where the equality follows from formulas (132). This homomorphism is injective because it preserves the decompositions

$$\bigoplus_{c \in \widetilde{C}} \tau_c \otimes H^1(1+\mathfrak{M}, k) \longrightarrow \bigoplus_{c \in \widetilde{C}} Z(E^*)^1 \cap H^1(I, \mathbf{X}(c)),$$

and because the map $f \mapsto \xi_{1,f}$ is injective (for all nonzero $f \in H^1(1+\mathfrak{M}, k)$ we find an element $t \in T^1 \subseteq I$ such that $f(\det(x)) \neq 0$). However, as we are not under the assumptions of Theorem 3.2.26, we do not know whether it is surjective or not.

Lastly, we compute the rank of the free $Z(E^*)^0$-module $Z(E^*)^0 \otimes_k H^1(1+\mathfrak{M}, k)$ (which is the same as the dimension of the k-vector space $H^1(1+\mathfrak{M}, k)$), as follows.

- If $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, then the quotient $(1+\mathfrak{M})/(1+\mathfrak{M})^p$ is finite-dimensional as a $\mathbb{F}_p$-vector space; more precisely (see [FV02, Chapter I, (6.5), Corollary, part (3)]) $1+\mathfrak{M}$ is a finitely generated $\mathbb{Z}_p$-module (via exponentiation) having free part of rank $[\mathfrak{F} : \mathbb{Q}_p]$ and torsion part consisting of the p^r-th roots of unity of $\mathfrak{F}^\times$ (for $r \in \mathbb{Z}_{\geqslant 0}$), and so

  $$\begin{aligned} &\dim_{\mathbb{F}_p}\left((1+\mathfrak{M})/(1+\mathfrak{M})^p\right) \\ &\qquad = \begin{cases} [\mathfrak{F} : \mathbb{Q}_p] & \text{if } \mathfrak{F} \text{ contains no non-trivial } p\text{-th roots of } 1, \\ [\mathfrak{F} : \mathbb{Q}_p] + 1 & \text{if } \mathfrak{F} \text{ contains non-trivial } p\text{-th roots of } 1. \end{cases} \end{aligned}$$

  Hence,

  $$\begin{aligned} &\operatorname{rank}_{Z(E^*)^0} Z(E^*)^0 \otimes_k H^1(1+\mathfrak{M}, k) \\ &\qquad = \dim_k H^1(1+\mathfrak{M}, k) \\ &\qquad = \dim_{\mathbb{F}_p} (1+\mathfrak{M})/(1+\mathfrak{M})^p \\ &\qquad = \begin{cases} [\mathfrak{F} : \mathbb{Q}_p] & \text{if } \mathfrak{F} \text{ contains no non-trivial } p\text{-th roots of } 1, \\ [\mathfrak{F} : \mathbb{Q}_p] + 1 & \text{if } \mathfrak{F} \text{ contains non-trivial } p\text{-th roots of } 1. \end{cases} \end{aligned}$$

- If instead $\mathfrak{F} = \mathbb{F}_q((X))$, then one has a bijection

  $$\begin{aligned} \eta \colon \prod_{\substack{i \in \mathbb{Z}_{\geqslant 1} \\ \text{with } p \nmid i}} \prod_{j \in \mathcal{J}} \mathbb{Z}_p &\longrightarrow 1+\mathfrak{M} \\ (a_{i,j})_{i,j} &\longmapsto \prod_{\substack{i \in \mathbb{Z}_{\geqslant 1} \\ \text{with } p \nmid i}} \prod_{j \in \mathcal{J}} (1+jX^i)^{a_{i,j}}, \end{aligned}$$

  where $\mathcal{J}$ is a fixed basis of $\mathbb{F}_q$ as a $\mathbb{F}_p$-vector space (see [FV02, Chapter I, (6.2), Proposition]). The map η is actually an isomorphism of topological groups: indeed it is clearly a group homomorphism between compact Hausdorff topological groups, and hence it suffices to check continuity. Since the source is first countable, it suffices to check sequential continuity. Let $(a_m)_{m\in\mathbb{Z}_{\geqslant 0}}$ be a sequence on the source, where $a_m = (a_{m,i,j})_{i,j}$ with $a_{m,i,j} \in \mathbb{Z}_p$, and assume that it has limit $a = (a_{i,j})_{i,j}$ (this is a limit in the product topology, i.e., a pointwise limit). For all $l \in \mathbb{Z}_{\geqslant 1}$, the sequence $(b_{l,m})_{m\in\mathbb{Z}_{\geqslant 0}}$ in $1 + \mathfrak{M}$ defined by

$$b_{l,m} \coloneqq \prod_{\substack{i\in\{1,\dots,l\}\\ \text{with } p\nmid i}} \prod_{j\in\mathcal{J}} (1 + jX^i)^{a_{m,i,j}}$$

converges to

$$\prod_{\substack{i\in\{1,\dots,l\}\\ \text{with } p\nmid i}} \prod_{j\in\mathcal{J}} (1 + jX^i)^{a_{i,j}}.$$

Denoting by $\overline{x}$ the class modulo $1+\mathfrak{M}^l$ of an element $x \in 1+\mathfrak{M}$, this shows that the sequence $\left(\overline{\eta(a_m)}\right)_{m\in\mathbb{Z}_{\geqslant 0}}$ converges to $\overline{\eta(a)}$. But $1+\mathfrak{M} = \varprojlim_r (1+\mathfrak{M})/(1+\mathfrak{M}^r)$, and the inverse limit topology is induced by the product topology, and so convergence on each of the factors $(1 + \mathfrak{M})/(1 + \mathfrak{M}^r)$ implies convergence on $1 + \mathfrak{M}$.

We deduce that

$$\begin{aligned}
H^1(1 + \mathfrak{M}, k) &\cong H^1\left(\mathbb{Z}_p^{\mathbb{Z}_{\geqslant 0}}, k\right) \\
&\cong H^1\left(\mathbb{Z}_p^{\mathbb{Z}_{\geqslant 0}}/p\mathbb{Z}_p^{\mathbb{Z}_{\geqslant 0}}, k\right) \\
&\cong H^1\left(\mathbb{F}_p^{\mathbb{Z}_{\geqslant 0}}, k\right) \\
&\cong H^1\Big(\varprojlim_{n\in\mathbb{Z}_{\geqslant 0}} \mathbb{F}_p^n, k\Big) \\
&\cong \varinjlim_{n\in\mathbb{Z}_{\geqslant 0}} H^1\left(\mathbb{F}_p^n, k\right) \\
&\cong \varinjlim_{n\in\mathbb{Z}_{\geqslant 0}} k^n \\
&= \bigoplus_{n\in\mathbb{Z}_{\geqslant 0}} k,
\end{aligned}$$

where we have used the behaviour of profinite group cohomology with respect to inverse and direct limits (see [Ser02, Chapter I, Proposition 8]). We conclude that

$$\begin{aligned}
\operatorname{rank}_{Z(E^*)^0}\left(Z(E^*)^0 \otimes_k H^1(1 + \mathfrak{M}, k)\right) &= \dim_k H^1(1 + \mathfrak{M}, k) \\
&= \aleph_0.
\end{aligned}$$

■

Example 3.2.30. Let $\mathbf{G} = \mathrm{PGL}_n$ (we will later assume that p divides n to get something non-trivial) and let us choose $\mathbf{T}$ to be the diagonal torus. For the moment, let us not make any assumptions on $\mathfrak{F}$. One has a well-defined “determinant” function

$$\begin{aligned}
\overline{\det}\colon \qquad \mathrm{PGL}_n(\mathfrak{F}) &\longrightarrow \mathfrak{F}^\times/(\mathfrak{F}^\times)^n \\
\underset{(\text{with } g \in \mathrm{GL}_n(\mathfrak{F}))}{\overline{g}} &\longmapsto \overline{\det(g)}.
\end{aligned}$$

Let us consider a homomorphism of topological groups

$$f\colon (1 + \mathfrak{M})/(1 + \mathfrak{M})^n \longrightarrow k.$$

Identifying $H^1(I, \mathbf{X}(1))$ with $H^1(I, k)$, we define $\xi_f \in H^1(I, \mathbf{X}(1))$ to be the following homomorphism of topological groups:

$$\xi_f \colon \quad I \xrightarrow{\quad \overline{\det} \quad} (1+\mathfrak{M})/(1+\mathfrak{M})^n \xrightarrow{\quad f \quad} k.$$

Since ξ_f is the restriction to I of a homomorphism of topological groups from G to k, Lemma 3.2.24 shows that ξ_f lies in the centre of E^*. We have thus constructed a map of k-vector spaces

$$\begin{aligned} H^1\big((1+\mathfrak{M})/(1+\mathfrak{M})^n, k\big) &\longrightarrow Z(E^*)^1 \\ f &\longmapsto \xi_f, \end{aligned}$$

which is injective since for all nonzero $f \in H^1\big((1+\mathfrak{M})/(1+\mathfrak{M})^n, k\big)$ we find an element $t \in T^1 \subseteq I$ such that $f(\overline{\det}(x)) \neq 0$. Regarding whether we have found something non-trivial or not, we note the following:

$$\begin{aligned} H^1\big((1+\mathfrak{M})/(1+\mathfrak{M})^n, k\big) &\cong H^1\big((1+\mathfrak{M})/(1+\mathfrak{M})^p(1+\mathfrak{M})^n, k\big) \\ &\cong \begin{cases} 0 & \text{if } p \nmid n, \\ H^1\big((1+\mathfrak{M})/(1+\mathfrak{M})^p, k\big) & \text{if } p \nmid n; \end{cases} \\ &\cong \begin{cases} 0 & \text{if } p \nmid n, \\ H^1\big(1+\mathfrak{M}, k\big) & \text{if } p \nmid n, \end{cases} \end{aligned}$$

where we used that if p does not divide n then exponentiation by n is an automorphism of $1+\mathfrak{M}$ (having inverse the exponentiation by $n^{-1} \in \mathbb{Z}_p^\times$). We have thus found that

- If p does not divide n then the above procedure does not yield non-trivial elements in $Z(E^*)^1$.
- If p divides n then the above procedure does yield non-trivial elements in $Z(E^*)^1$ (it is easy to see that $H^1\big(1+\mathfrak{M}, k\big)$ is non-trivial, and in any case we have even computed it explicitly in the example of GL_n).

Let us prove that

$$T^1_{\check{\Phi}} = \ker\big(\overline{\det}\big|_{T^1}\big).$$

Let us consider the simply connected covering

$$(\mathrm{SL}_n, \mathbf{T}_{\mathrm{SL}_n}) \longrightarrow (\mathrm{PGL}_n, \mathbf{T}),$$

where $\mathbf{T}_{\mathrm{SL}_n}$ is the diagonal torus of SL_n. Recall that $T_{\check{\Phi}}$ is the image of T_{SL_n} via the above covering. It is then clear that every element of $T_{\check{\Phi}}$ is in the kernel of $\overline{\det}$. In particular, we have the inclusion $T^1_{\check{\Phi}} \subseteq \ker\big(\overline{\det}\big|_{T^1}\big)$. For the other inclusion, let $x \in \ker\big(\overline{\det}\big|_{T^1}\big)$. Denoting by $\mathbf{T}_{\mathrm{GL}_n}$ the diagonal torus of GL_n, we can choose a lift $t \in T_{\mathrm{GL}_n}$ of x. There exists $u \in \mathfrak{F}^\times$ such that

$$\det(t) = u^n = \det \widehat{u}, \qquad\qquad \text{where } \widehat{u} := \begin{pmatrix} u & & \\ & \ddots & \\ & & u \end{pmatrix}.$$

Using the decomposition $\mathfrak{F}^\times = \pi^{\mathbb{Z}} \times \boldsymbol{\mu}_{q-1}(\mathfrak{F}) \times (1+\mathfrak{M})$, we see that without loss of generality we may assume that $u \in 1+\mathfrak{M}$, and so $\widehat{u} \in T^1_{\mathrm{GL}_n}$. Now, $t\widehat{u}^{-1}$ is an element of $T^1_{\mathrm{GL}_n}$ with determinant 1, and so it is an element of $T^1_{\mathrm{SL}_n}$. Since SL_n is simply connected, we know by Remark 3.2.15 that $t\widehat{u}^{-1}$ lies in the image of

$$\prod_{\alpha\in\Pi}\check{\alpha}\colon \prod_{\alpha\in\Pi}(1+\mathfrak{M}) \longrightarrow T_{\mathrm{SL}_n}.$$

Therefore the element $x=\bar{t}=\overline{t\widehat{u}}$ lies in $T^1_{\check{\Phi}}$. This concludes the proof that

$$T^1_{\check{\Phi}} = \ker\left(\overline{\det}\big|_{T^1}\right).$$

If $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, one can prove, using this equality and reproducing the same argument as in the example of GL_n, that the above procedure yields all the elements of $Z(E^*)^1$ and hence that

$$Z(E^*)^1 \cong \begin{cases} 0 & \text{if } p\nmid n,\\ H^1(1+\mathfrak{M},k) & \text{if } p\mid n.\end{cases}$$

■

3.2.i A remark about a graded-commutative algebra inside E^*

Let $K_1 \supseteq K_2 \supseteq K_3$ be open inclusions of locally profinite groups. Later on we will further assume that K_3 is compact. As compact induction is transitive, we have a homomorphism of k-algebras

$$\begin{aligned} \mathrm{End}_{k[K_2]\text{-mod}}(\text{c-ind}_{K_3}^{K_2} 1) \longrightarrow\ & \mathrm{End}_{k[K_1]\text{-mod}}(\text{c-ind}_{K_3}^{K_1} 1) \\ & = \mathrm{End}_{k[K_1]\text{-mod}}(\text{c-ind}_{K_2}^{K_1}\text{c-ind}_{K_3}^{K_2} 1) \\ h \longmapsto\ & \text{c-ind}_{K_2}^{K_1} h. \end{aligned} \tag{133}$$

Recall the concrete description of the above rings of endomorphisms as in Subsection 1.4.a (where the product can be described as a convolution):

$$\begin{aligned} \mathrm{End}_{k[K_i]\text{-mod}}(\text{c-ind}_{K_3}^{K_i} 1) &\xrightarrow{\cong} k\left[K_3\backslash K_i/K_3\right] \\ h &\longmapsto h(1) \end{aligned} \qquad \text{for } i=1,2,$$

where we read $h(1)$ as a K_3-bi-invariant function $K_i \longrightarrow k$. The explicit identification

$$\text{c-ind}_{K_2}^{K_1}\text{c-ind}_{K_3}^{K_2} 1 = \text{c-ind}_{K_3}^{K_1} 1$$

is given by

$$\begin{aligned} \text{c-ind}_{K_2}^{K_1}\text{c-ind}_{K_3}^{K_2} 1 &\longrightarrow \text{c-ind}_{K_3}^{K_1} 1 \\ f &\longmapsto \left(\begin{aligned} K_1 &\longrightarrow k \\ x &\longmapsto f(x)(1) \end{aligned}\right). \end{aligned}$$

We then see that the homomorphism (133) admits the following concrete description:

$$\begin{aligned} k\left[K_3\backslash K_2/K_3\right] &\longrightarrow k\left[K_3\backslash K_1/K_3\right] \\ K_3xK_3 &\longmapsto K_3xK_3. \end{aligned} \tag{134}$$

In the next lemma, we extend this to the level of Ext groups. For $i=1,2$ we consider

$$\mathrm{Ext}^*\left(\text{c-ind}_{K_i}^{K_1} 1, \text{c-ind}_{K_i}^{K_1} 1\right) = \mathrm{Ext}^*\left(k[K_i/K_3], k[K_i/K_3]\right).$$

Lemma 3.2.31. *Let $K_1 \supseteq K_2 \supseteq K_3$ be open inclusions of locally profinite groups, with K_3 is compact. One has that the map*

$$H^*(K_3, \text{c-ind}_{K_3}^{K_2} 1) \longrightarrow H^*(K_3, \text{c-ind}_{K_3}^{K_1} 1)$$

induced by the canonical map of K_2-representations $\text{c-ind}_{K_3}^{K_2} 1 \longrightarrow \text{c-ind}_{K_3}^{K_1} 1$, i.e., by the canonical inclusion $k[K_2/K_3] \longrightarrow k[K_1/K_3]$ is an injective homomorphism of graded k-algebras, with respect to the (opposite of the) Yoneda product.

Proof. We identify

$$\mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, \text{c-ind}_{K_3}^{K_i} 1\big) = \mathrm{Hom}_{D(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, (\text{c-ind}_{K_3}^{K_i} 1)[*]\big), \tag{135}$$

(see [Har66, Chapter I, Corollary 6.5]) where the notation is as follows: $D(K_i)$ is the derived category of $\mathrm{Rep}_k^\infty(K_i)$, the $\text{c-ind}_{K_3}^{K_i} 1$ appearing on the right hand side means the complex concentrated in degree 0 associated with $\text{c-ind}_{K_3}^{K_i} 1$, and the notation $(\text{c-ind}_{K_3}^{K_i} 1)[*]$ means translation by $*$. With this description, the Yoneda product is the composition of morphisms in $D(K_i)$.

Since compact induction from an open subgroup is exact (left exactness is easy and right exactness follows from the fact it is a left adjoint), the functor $\text{c-ind}_{K_2}^{K_1}$ induces a map on the level of derived categories

$$\begin{array}{ccc}
\mathrm{Hom}_{D(K_2)}\big(\text{c-ind}_{K_3}^{K_2} 1, (\text{c-ind}_{K_3}^{K_2} 1)[*]\big) & \longrightarrow & \mathrm{Hom}_{D(K_1)}\big(\text{c-ind}_{K_3}^{K_1} 1, (\text{c-ind}_{K_3}^{K_1} 1)[*]\big) \\
\hline
\left(\begin{tikzcd} & V \arrow[dl, "f"', "\text{q.is.}"] \arrow[dr, "g"] & \\ \text{c-ind}_{K_3}^{K_2} 1 & & (\text{c-ind}_{K_3}^{K_2} 1)[*] \end{tikzcd}\right) & \longmapsto & \left(\begin{tikzcd} & V \arrow[dl, "\text{c-ind}_{K_2}^{K_1} f"', "\text{q.is.}"] \arrow[dr, "\text{c-ind}_{K_2}^{K_1} g"] & \\ \text{c-ind}_{K_3}^{K_1} 1 & & (\text{c-ind}_{K_3}^{K_1} 1)[*] \end{tikzcd}\right).
\end{array} \tag{136}$$

It is then clear that this map preserves the Yoneda product. Let us see this on the level of injective resolutions; denoting by $K(K_i)$ the homotopy category of the category of unbounded complexes in $\mathrm{Rep}_k^\infty(K_i)$, denoting by Ext^* the Ext functor defined in terms of injective resolutions and choosing an injective resolution $J_i^\bullet$ of $\text{c-ind}_{K_3}^{K_i} 1$, the identification (135) can be made explicit as follows:

$$\begin{aligned}
\mathrm{Hom}_{D(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, (\text{c-ind}_{K_3}^{K_i} 1)[*]\big) &= \mathrm{Hom}_{D(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, J_i^\bullet[*]\big) \\
&= \mathrm{Hom}_{K(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, J_i^\bullet[*]\big) \\
&= \mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, \text{c-ind}_{K_3}^{K_i} 1\big).
\end{aligned} \tag{137}$$

Here, the first identification is induced by the natural map $\text{c-ind}_{K_3}^{K_i} 1 \longrightarrow J_i^\bullet[*]$, which is a quasi-isomorphism; the second identification stems from the fact that every morphism in $D(K_i)$ having as target a complex of injective objects comes from an actual morphism of complexes (see [Har66, Chapter I, proof of Theorem 6.4]); the third identification is obtained by sending a morphism of complexes $\text{c-ind}_{K_3}^{K_i} 1 \longrightarrow J_i^\bullet[*]$ to the class of its 0-component.

Now, let us express the map (136) as a map

$$\mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_2)}\big(\text{c-ind}_{K_3}^{K_2} 1, \text{c-ind}_{K_3}^{K_2} 1\big) \longrightarrow \mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_3)}\big(\text{c-ind}_{K_3}^{K_1} 1, \text{c-ind}_{K_3}^{K_1} 1\big),$$

where the Ext-groups are defined in terms of the chosen injective resolutions. Since $J_1^\bullet$ is an injective resolution of $\text{c-ind}_{K_3}^{K_1} 1$, there exists a unique morphism Ψ in $K(K_1)$

making the following diagram commute (note that the first row is exact because $\text{c-ind}_{K_2}^{K_1}$ is an exact functor):

$$\begin{tikzcd}
\text{c-ind}_{K_3}^{K_1} 1 \arrow[r] \arrow[d, equal] & \text{c-ind}_{K_2}^{K_1} J_2^\bullet \arrow[d, "\Psi"] \\
\text{c-ind}_{K_3}^{K_1} 1 \arrow[r] & J_1^\bullet.
\end{tikzcd}$$

It is then easy to describe explicitly the (obviously unique) dashed maps making the following diagram commute:

$$\begin{tikzcd}
\mathrm{Hom}_{D(K_2)}\big(\text{c-ind}_{K_3}^{K_2} 1, (\text{c-ind}_{K_3}^{K_2} 1)[*]\big) \arrow[r, "(136)"] \arrow[d, "\cong", "(137)"'] & \mathrm{Hom}_{D(K_1)}\big(\text{c-ind}_{K_3}^{K_1} 1, (\text{c-ind}_{K_3}^{K_1} 1)[*]\big) \arrow[d, "\cong", "(137)"'] \\
\mathrm{Hom}_{D(K_2)}\big(\text{c-ind}_{K_3}^{K_2} 1, J_2^\bullet[*]\big) \arrow[r, dashed] \arrow[dr, dashed] & \mathrm{Hom}_{D(K_1)}\big(\text{c-ind}_{K_3}^{K_1} 1, (\text{c-ind}_{K_2}^{K_1} J_2^\bullet)[*]\big) \arrow[d, "\cong", "\text{ind. by } \Psi"'] \\
 & \mathrm{Hom}_{D(K_1)}\big(\text{c-ind}_{K_3}^{K_1} 1, J_1^\bullet[*]\big).
\end{tikzcd}$$

Looking again at (137) we then get that, defining the Ext-groups in terms of our chosen injective resolutions, the map (136) is the same as the map

$$\begin{aligned}
\mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_2)}\big(\text{c-ind}_{K_3}^{K_2} 1, \text{c-ind}_{K_3}^{K_2} 1\big) &\longrightarrow \mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_3)}\big(\text{c-ind}_{K_3}^{K_1} 1, \text{c-ind}_{K_3}^{K_1} 1\big) \\
\overline{\Big(\text{c-ind}_{K_3}^{K_2} 1 \xrightarrow{f} J_2^n\Big)} &\longmapsto \overline{\Big(\text{c-ind}_{K_3}^{K_1} 1 \xrightarrow{\text{c-ind}_{K_2}^{K_1} f} \text{c-ind}_{K_2}^{K_1} J_2^n \xrightarrow{\Psi} J_1^n\Big)}.
\end{aligned} \tag{138}$$

Now,since we are assuming that K_3 is compact, exactly as in Subsection 1.9.a we have an identification

$$\mathrm{Ext}^*_{\mathrm{Rep}_k^\infty(K_i)}(\text{c-ind}_{K_3}^{K_i} 1) \cong H^*(K_3, \text{c-ind}_{K_3}^{K_i} 1),$$

which can be obtained as follows: recall that we have chosen an injective resolution $\text{c-ind}_{K_3}^{K_i} 1 \longrightarrow J_i^\bullet$ in $\mathrm{Rep}_k^\infty(K_i)$: this is also an injective resolution in $\mathrm{Rep}_k^\infty(K_3)$ (because the restriction functor from $\mathrm{Rep}_k^\infty(K_i)$ to $\mathrm{Rep}_k^\infty(K_3)$ preserves injective objects, see [Vig96, Chapitre I, 5.9 d)]). Then, the left hand side (respectively, the right hand side) of the above identification is the cohomology of the complex obtained by applying the functor $\mathrm{Hom}_{\mathrm{Rep}_k^\infty(K_i)}\big(\text{c-ind}_{K_3}^{K_i} 1, \_\big)$ (respectively, the functor $(\_)^I$, which is isomorphic to the previous one) to the complex $J_i^\bullet$.

For $n \in \mathbb{Z}_{\geqslant 0}$ and for f as in (138), we have the following commutative diagram

$$\begin{tikzcd}
\text{c-ind}_{K_3}^{K_1} 1 \arrow[r, "\text{c-ind}_{K_2}^{K_1} f"] & \text{c-ind}_{K_2}^{K_1} J_2^n \arrow[r, "\Psi"] & J_1^n, \\
\text{c-ind}_{K_3}^{K_2} 1 \arrow[r, "f"] \arrow[u, hook] & J_2^n \arrow[u, hook] \arrow[ur, "\widetilde{\Psi}"'] & \\
1 \arrow[u, hook] & &
\end{tikzcd}$$

where $\widetilde{\Psi}$ is the obvious composite morphism. Looking at the commutative diagram

$$\begin{tikzcd}
\text{c-ind}_{K_3}^{K_2} 1 \arrow[r] \arrow[d, hook] & J_2^\bullet \arrow[d, hook] \arrow[dd, bend left=60, "\widetilde{\Psi}"] \\
\text{c-ind}_{K_3}^{K_1} 1 \arrow[r] \arrow[d, equal] & \text{c-ind}_{K_2}^{K_1} J_2^\bullet \arrow[d, "\Psi"] \\
\text{c-ind}_{K_3}^{K_1} 1 \arrow[r] & J_1^\bullet,
\end{tikzcd}$$

we see that the map (138) (i.e, the map (136)) is the same as the map

$$H^*(K_3, \text{c-ind}_{K_3}^{K_2} 1) \longrightarrow H^*(K_3, \text{c-ind}_{K_3}^{K_1} 1) \tag{139}$$

induced by the canonical map of K_2-representations $\text{c-ind}_{K_3}^{K_2} 1 \longrightarrow \text{c-ind}_{K_3}^{K_1} 1$, i.e., by the canonical inclusion $k[K_2/K_3] \longrightarrow k[K_1/K_3]$. The latter map is a split injecitve homomorphism of K_2-representations, because the map

$$\begin{aligned}
k[K_1/K_3] &\longrightarrow k[K_2/K_3] \\
(xK_3) &\longmapsto \begin{cases} (xK_3) & \text{if } x \in K_2 \\ 0 & \text{if } x \notin K_2 \end{cases}
\end{aligned}$$

is a well-defined homomorphism of K_2-representations that provides a left inverse. Since profinite group cohomology commutes with direct sums, we conclude that the map (139) (equivalently, the map (138) or, again equivalently, the map (136)) is injective. ■

Returning to our setting, let us consider

$$K_1 := G, \qquad K_2 := CI, \qquad K_3 := I.$$

From the above abstract situation (and considering now the opposite product, in accordance with our conventions) we get an injective homomorphism of graded k-algebras

$$\begin{tikzcd}
\operatorname{Ext}^*_{\operatorname{Rep}_k^\infty(G)}(\text{c-ind}_I^{CI}, \text{c-ind}_I^{CI})^{\mathrm{op}} \arrow[r] \arrow[d, equal] & \operatorname{Ext}^*_{\operatorname{Rep}_k^\infty(G)}(\text{c-ind}_I^{G}, \text{c-ind}_I^{G})^{\mathrm{op}}. \arrow[d, equal] \\
E^*(CI, I) & E^*(G, I) \arrow[d, equal] \\
 & E^*
\end{tikzcd}$$

This homomorphism, when seen as a map

$$H^*(I, k[CI/I]) \longrightarrow H^*(I, k[G/I]), \tag{140}$$

is just the map induced by the inclusion $k[CI/I] \longrightarrow k[G/I]$. Since $C \cap I = C \cap T^1$ and since C is central, we have

$$CI/I = \dot{\bigcup_{c \in C/(C \cap T^1)}} cI/I = \dot{\bigcup_{c \in C/(C \cap T^1)}} IcI/I.$$

On the other side, we have

$$G/I = \dot{\bigcup_{w \in \widetilde{W}}} IwI/I = \Big(\dot{\bigcup_{c \in C/(C \cap T^1)}} IcI/I \Big) \mathbin{\dot\cup} \Big(\dot{\bigcup_{w \in \widetilde{W} \smallsetminus (C/(C \cap T^1))}} IwI/I \Big).$$

Using the decompositions of I-representations

$$\begin{aligned} k[CI/I] &= \bigoplus_{c \in C/(C \cap T^1)} \mathbf{X}(c), \\ k[G/I] &= \Big(\bigoplus_{c \in C/(C \cap T^1)} \mathbf{X}(c) \Big) \oplus \Big(\bigoplus_{w \in \widetilde{W} \smallsetminus (C/(C \cap T^1))} \mathbf{X}(w) \Big), \end{aligned}$$

we see that the map (140) has image $\bigoplus_{c \in C/(C \cap T^1)} H^*(I, \mathbf{X}(c)) \subseteq E^*$. Therefore we have an identification (which we will treat as an equality)

$$E^*(CI, I) = \bigoplus_{c \in C/(C \cap T^1)} H^*(I, \mathbf{X}(c)) \subseteq E^*.$$

There seems to be some relations between the subalgebra $E^*(CI, I)$ and the centre of E^*, although only regarding low graded pieces. The following remark summarizes some facts in this direction.

Remark 3.2.32. The following facts hold.

(i) $E^*(CI, I) \cong k[\widetilde{C}] \otimes_k H^*(I, k)$ as a graded k-algebra, where $k[\widetilde{C}]$ is the group algebra of the group $\widetilde{C} = (C \cdot T^1)/T^1$ and where $H^*(I, k)$ is the usual cohomology algebra with respect to the tensor product. In particular, $E^*(CI, I)$ is graded-commutative.

(ii) $Z(E^*)^0 = E^0(CI, I)$;

(iii) If $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, then $Z(E^*)^1 \subseteq E^1(CI, I)$, with equality not holding in general.

(iv) In general, it is not true that $Z(E^*) \subseteq E^*(CI, I)$.

Proof. We prove the four claims stated above.

(i) We claim that the map

$$\begin{aligned} k[\widetilde{C}] \otimes_k H^*(I, k) &\longrightarrow E^*(CI, I) \\ \underset{(\text{with } c \in \widetilde{C})}{(c) \otimes \gamma} &\longmapsto \tau_c \cdot \mathrm{Sh}_1^{-1}(\gamma) \end{aligned} \tag{141}$$

is a well-defined isomorphism of k-algebras (here Sh_1^{-1} is basically the identity map on the cohomology space $H^*(I, k) = H^*(I, \mathbf{X}(1))$; nevertheless, we write it explicitly in order to stress the fact that we are considering the inclusion $\mathrm{Sh}_1^{-1}(\gamma) \in H^*(I, \mathbf{X}(1)) \subseteq E^*$). First of all recall from Theorem 3.1.10 that we have an isomorphism of k-algebras

$$\begin{aligned} k[\widetilde{C}] &\longrightarrow Z(E^*)^0 \\ \underset{(\text{with } c \in \widetilde{C})}{(c)} &\longmapsto \tau_c, \end{aligned}$$

and recall from Corollary 1.9.3 that the inclusion

$$H^*(I,k) \cong H^*(I,\mathbf{X}(1)) \longrightarrow E^*$$

is a homomorphism of k-algebras. It follows that we have a well-defined homomorphism of k-vector spaces

$$\begin{aligned} k[\widetilde{C}] \otimes_k H^*(I,k) &\longrightarrow E^* \\ \underset{(\text{with } c\in\widetilde{C})}{(c)\otimes\gamma} &\longmapsto \tau_c \cdot \mathrm{Sh}_1^{-1}(\gamma), \end{aligned}$$

and that this is actually a k-algebra homomorphism, because the image of the map $k[\widetilde{C}] \longrightarrow E^*$ is central in E^*. It is also clear that the image of the map displayed above is contained in the subalgebra $E^*(CI,I)$, and so we have shown that (141) is a well-defined homomorphism of k-algebras. To show that it is bijective, recalling that $\widetilde{C} = (C\cdot T^1)/T^1 = C/(C\cap T^1)$, it suffices to consider the decompositions

$$\begin{aligned} k[\widetilde{C}] \otimes_k H^*(I,k) &= \bigoplus_{c\in\widetilde{C}} (c)\otimes H^*(I,k), \\ E^*(CI,I) &= \bigoplus_{c\in\widetilde{C}} H^*(I,\mathbf{X}(c)) \\ &= \bigoplus_{c\in\widetilde{C}} \tau_c \cdot H^*(I,\mathbf{X}(1)), \end{aligned}$$

where the last equality is clear from the explicit description of the product in E^* (see, e.g., Theorem 1.9.1) and from the fact that every $c\in\widetilde{C}$ has length 0. From the above decompositions, bijectivity of the map (141) follows.

(ii) The equality $Z(E^*)^0 = E^0(CI,I)$ is now clear because both terms coincide with the image of the isomorphism (141) in degree 0.

(iii) If $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$, then the inclusion $Z(E^*)^1 \subseteq E^1(CI,I)$ holds because in Proposition 3.2.11 we showed that

$$\begin{aligned} Z(E^*)^1 &\subseteq \bigoplus_{c\in\widetilde{C}} H^1(I,\mathbf{X}(c)) \\ &= \bigoplus_{c\in\widetilde{C}} \tau_c \cdot H^1(I,\mathbf{X}(1)). \end{aligned}$$

In general this is not an equality: indeed $E^1(CI,I) \supseteq H^1(I,k)$, and $H^1(I,k)$ is always non-zero (if $\mathbf{G} \neq \{1\}$), while $Z(E^*)^1$ might be zero (the first fact is general: for a non-trivial pro-p group K the cohomology group $H^1(K,k)$ is always non-trivial, see, e.g., the argument in the proof of Corollary 3.2.39; for the second fact see, e.g., Corollary 3.2.39, or the explicit result for $\mathrm{SL}_2(\mathbb{Q}_p)$ with $p\neq 2,3$ proved in Proposition 2.5.2).

(iv) The fact that in general we do not have $Z(E^*) \subseteq E^*(CI,I)$ is clear from the description of $Z(E^*)^d$ for $G = \mathrm{SL}_2(\mathfrak{F})$ with the assumption that I is torsion-free (see Proposition 2.2.1). ■

3.2.j The 1^{st} graded piece of the centre for unramified extensions of $\mathbb{Q}_p$: special cases

In this subsection we will derive two corollaries (Corollary 3.2.37 and Corollary 3.2.39) from Theorem 3.2.26. Before, we need some notation and some lemmas.

Let us define $\mathbf{C}^\circ$ as the identity component of the centre $\mathbf{C}$ of $\mathbf{G}$. We have already recalled (e.g., in Section 3.1.a) that $\mathbf{C}$ is defined over $\mathfrak{F}$ and that $\mathbf{C} \subseteq \mathbf{T}$. We also remark that $\mathbf{C}^\circ$ is a $\mathfrak{F}$-split torus, because it is a (closed) connected subgroup defined over $\mathfrak{F}$ of a $\mathfrak{F}$-split torus (see [Bor91, Chapter III, §8.5, Corollary and §8.14, Corollary]).

For all $w \in W$, we define I'_w to be the subgroup of I_w generated by $(T')^1$ and the "unipotent factors" in the Iwahori decomposition of I_w. This can be also characterized as the group $(I^{(\mathbf{G}')})_w$ obtained by replacing I with the pro-p Iwahori subgroup $I^{(\mathbf{G}')}$ of $\mathbf{G}'$ corresponding to I. We add the proof of this fact together with a more precise explanation of what we mean by $I^{(\mathbf{G}')}$ and by $(I^{(\mathbf{G}')})_w$ (which only makes sense assuming $w \in W_{\mathrm{aff}}$).

Proof of the claim. Since that for all $\omega \in \Omega$ one has $I_{w\omega} = I_w$, we may assume that $w \in W_{\mathrm{aff}}$. One can canonically identify the root systems of $(\mathbf{G}, \mathbf{T})$ and $(\mathbf{G}', \mathbf{T}')$. We make the same choice of positive roots and we choose compatible Chevalley systems on $(\mathbf{G}, \mathbf{T})$ and $(\mathbf{G}', \mathbf{T}')$. The corresponding apartments are then canonically identified, as well as the corresponding groups "W_{aff}" generated by affine reflections in the apartment. Let us look at the Iwahori decomposition of I_w:

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

The groups $\mathbf{U}_\alpha$'s associated with $(\mathbf{G}, \mathbf{T})$ and with $(\mathbf{G}', \mathbf{T}')$ are canonically identified, as well as and their filtrations. Also the respective functions $g_{(\_)}(\_)$'s coincide. Considering the the pro-p Iwahori subgroup $I^{(\mathbf{G}')}$ of $(\mathbf{G}', \mathbf{T}')$ (associated with the same choice of positive roots / with the same fundamental chamber we are considering for I), we therefore conclude that the Iwahori decomposition of the subgroup $(I^{(\mathbf{G}')})_w$ consists exactly of the same factors as the Iwahori decomposition of I except that one has $(T')^1$ in place of T^1. ∎

Lemma 3.2.33. *The following are equivalent:*

(1) p does not divide the order of $\mathbf{C}^\circ \cap \mathbf{T}'$;

(2) $T^1 = (C^\circ)^1 \cdot (T')^1$;

(3) $T^1 = (C^\circ)^1 \times (T')^1$;

(4) $I_w = (C^\circ)^1 \times I'_w$ for all $w \in \widetilde{W}$.

Proof. Let us prove the equivalences (1) $\iff$ (2) $\iff$ (3), and then the implications (3) $\implies$ (4) and (4) $\implies$ (2).

(1) $\iff$ (2) $\iff$ (3) : We have the following exact sequence, where the first algebraic group is finite (see [Bor91, Chapter V, §21.1]):

$$1 \longrightarrow \mathbf{C}^\circ \cap \mathbf{T}' \longrightarrow \mathbf{C}^\circ \times \mathbf{T}' \longrightarrow \mathbf{T} \longrightarrow 1.$$

We can therefore apply Lemma 3.2.13, which tells us that the induced map $(C^\circ)^1 \times (T')^1 \longrightarrow T^1$ is surjective if and only if p does not divide the order of $\mathbf{C}^\circ \cap \mathbf{T}'$, and in this case it is also injective, yielding the required equivalences.

(3) $\Longrightarrow$ (4) : Combining (3) with the Iwahori factorization of I_w, we find that multiplication defines a bijection

$$\prod_{\alpha\in\Phi^-} \mathfrak{U}_{(\alpha,g_w(\alpha))} \times (C^\circ)^1 \times (T')^1 \times \prod_{\alpha\in\Phi^+} \mathfrak{U}_{(\alpha,g_w(\alpha))} \longrightarrow I_w.$$

The map $(C^\circ)^1 \times I'_w \longrightarrow I_w$ defined by multiplication is a group homomorphism because $(C^\circ)^1$ is central, and it is bijective by the above Iwahori factorization.

(4) $\Longrightarrow$ (2) : Let us consider $t \in T^1$ and let us show that $t \in (C^\circ)^1 \cdot (T')^1$. By (4) we can write $t = ci$, for some $c \in (C^\circ)^1$ and some $i \in I'$. Considering the Iwahori factorization of i with respect to I' (recall that I' is a pro-p Iwahori subgroup for (G', T')), and comparing it with the Iwahori factorization of $i = tc^{-1} \in T^1$ with respect to I, we see that i cannot have "unipotent components"; in other words we see that $i \in (T')^1$, thus finishing the proof that $t \in (C^\circ)^1 \cdot (T')^1$. ■

Lemma 3.2.34. *Let us consider the map*

$$\prod_{\alpha\in\Pi} \breve{\alpha}\big|_{1+\mathfrak{M}} \colon \prod_{\alpha\in\Pi} (1+\mathfrak{M}) \longrightarrow (T')^1.$$

One has:

- $\prod_{\alpha\in\Pi} \breve{\alpha}\big|_{1+\mathfrak{M}}$ *is injective if and only if either p does not divide the order of the fundamental group of $\mathbf{G}'$ or $\mathfrak{F}$ does not contain non-trivial p-th roots of unity;*
- $\prod_{\alpha\in\Pi} \breve{\alpha}\big|_{1+\mathfrak{M}}$ *is surjective onto $(T')^1$ (i.e., $(T')^1 = T^1_{\breve{\Phi}}$) if and only if p does not divide the order of the fundamental group of $\mathbf{G}'$.*

Proof. Lemma 3.2.14 tells us that the morphism of algebraic tori

$$\prod_{\alpha\in\Pi} \breve{\alpha} \colon \prod_{\alpha\in\Pi} \mathbb{G}_{\mathrm{m}} \longrightarrow \mathbf{T}'$$

is surjective (onto $\mathbf{T}'$) with kernel having order equal to the order of the fundamental group of $\mathbf{G}'$. The result about injectivity and surjectivity of the map $\prod_{\alpha\in\Pi} \breve{\alpha}\big|_{1+\mathfrak{M}}$ then follows from Lemma 3.2.13. ■

Lemma 3.2.35. *The following are equivalent:*

1. *p divides neither the order of $\mathbf{C}^\circ \cap \mathbf{T}'$ nor the order of the fundamental group of $\mathbf{G}'$;*
2. *$T^1 = (C^\circ)^1 \times T^1_{\breve{\Phi}}$;*
3. *$T^1/T^1_{\breve{\Phi}} = (C^\circ)^1$ (meaning that the natural map from the right side to the left side is an isomorphism);*
4. *$T^1 = (C^\circ)^1 \cdot T^1_{\breve{\Phi}}$.*

Proof. The implications (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) being obvious, it suffices to prove the implications (1) $\Longrightarrow$ (2) and (4) $\Longrightarrow$ (1).

(1) $\Longrightarrow$ (2) : The condition that p does not divide the order of $\mathbf{C}^\circ \cap \mathbf{T}'$ implies that $T^1 = (C^\circ)^1 \times (T')^1$ (Lemma 3.2.33), while the condition that p does not divide the order of the fundamental group of $\mathbf{G}'$ implies that $T' = T^1_{\breve{\Phi}}$ (Lemma 3.2.34).

(4) $\Longrightarrow$ (1) : Since $T^1 = (C^\circ)^1 \cdot T^1_{\check{\Phi}}$, a fortiori one has $T^1 = (C^\circ)^1 \cdot (T')^1$. Lemma 3.2.33 tells us that this last condition is equivalent to the condition that p does not divide the order of $\mathbf{C}^\circ \cap \mathbf{T}'$, thus proving part of the statement (1), and also that the product is actually a direct product, namely $T^1 = (C^\circ)^1 \times (T')^1$. In particular, we have

$$(C^\circ)^1 \cdot T^1_{\check{\Phi}} = T^1 = (C^\circ)^1 \times (T')^1,$$

and therefore the inclusion $T^1_{\check{\Phi}} \subseteq (T')^1$ must be an equality. Lemma 3.2.34 tells us that this last condition is equivalent to the condition that p does not divide the order of the fundamental group of $\mathbf{G}'$, thus proving the remaining part of the statement (1). ■

The following lemma is surely well-known.

Lemma 3.2.36. *One has that p divides the connection index (i.e., the order of the finite group given by the weight lattice modulo the root lattice) if and only if p divides either the order of $Z(\mathbf{G}')$ or the order of the fundamental group of $\mathbf{G}'$.*

Proof. Let us consider the split semisimple group $\mathbf{G}'$ with maximal (split) torus $\mathbf{T}'$ and root system $\Phi(\mathbf{G}', \mathbf{T}') = \Phi(\mathbf{G}, \mathbf{T})$. Recall from (128) the notation Λ_{w} for the weight lattice. Let us consider the exact sequence

$$0 \longrightarrow X^*(\mathbf{T}')/\operatorname{span}_{\mathbb{Z}} \Phi \longrightarrow \Lambda_{\mathrm{w}}/\operatorname{span}_{\mathbb{Z}} \Phi \longrightarrow \Lambda_{\mathrm{w}}/X^*(\mathbf{T}') \longrightarrow 0, \quad (142)$$

where the term on the middle is the group whose order is called connection index, while the term on the right is the fundamental group of $\mathbf{G}'$. We see that p divides the connection index if and only if it divides either the order of the fundamental group of $\mathbf{G}'$ or the order of the group $X^*(\mathbf{T}')/\operatorname{span}_{\mathbb{Z}} \Phi$.

It remains to relate the term on the left with $Z(\mathbf{G}')$, but in [Mil17, Proposition 21.8] it is shown that there is a group isomorphism

$$X^*(Z(\mathbf{G}')) \cong X^*(\mathbf{T}')/\operatorname{span}_{\mathbb{Z}} \Phi.$$

Now we are done because the order of the algebraic group $Z(\mathbf{G}')$ is the same as the order of the abstract group $X^*(Z(\mathbf{G}'))$: indeed a finite diagonalizable group, such as $Z(\mathbf{G}')$, is isomorphic to copies of $\boldsymbol{\mu}_n$ (see [Mil17, Proposition 12.3 and Theorem 12.9]), say

$$Z(\mathbf{G}') \cong \boldsymbol{\mu}_{n_1} \times \cdots \times \boldsymbol{\mu}_{n_m}.$$

Thus, we obtain that the order of $Z(\mathbf{G}')$ is $n_1 \cdots n_m$ and that the group $X^*(Z(\mathbf{G}'))$ has also order $n_1 \cdots n_m$, because

$$X^*(Z(\mathbf{G}')) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_1\mathbb{Z}.$$ ■

Corollary 3.2.37. *Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has the following facts.*

(a) Assume that p divides neither the order of $\mathbf{C}^\circ \cap \mathbf{T}'$ (equivalently, the order of $(\mathbf{C}^\circ \cap \mathbf{T}')(\overline{\mathfrak{F}})$) nor the order of the fundamental group of $\mathbf{G}'$. Then, there is a decomposition $I = (C^\circ)^1 \times I'$ and two maps

$$H^1(I, k) \underset{\mathrm{pr}^*_{(C^\circ)^1}}{\overset{\mathrm{res}^I_{(C^\circ)^1}}{\rightleftarrows}} H^1\left((C^\circ)^1, k\right)$$

define an isomorphism $\mathrm{Sh}_c\left(Z(E^*)^1_c\right) \cong H^1\left((C^\circ)^1, k\right)$ *for all* $c \in \widetilde{C}$.

In particular, combining this with the description of $Z(E^*)^1$ *of Theorem 3.2.26, we get that the composite map*

$$Z(E^*)^0 \otimes_k H^1\big((C^\circ)^1, k\big) \xrightarrow{\mathrm{id}_{Z(E^*)^0} \otimes_k \mathrm{pr}^*_{(C^\circ)^1}} Z(E^*)^0 \otimes_k H^1(I, k) \xrightarrow{\text{mult.}} E^1$$

defines an isomorphism of $Z(E^*)^0$*-modules* $Z(E^*)^0 \otimes_k H^1\big((C^\circ)^1, k\big) \cong Z(E^*)^1$.

(b) *The two conditions in (a) hold if* p *does not divide the connection index of the root system (i.e., the order of the finite group given by the weight lattice modulo the root lattice).*

Proof. Let us prove the two parts of the corollary.

(a) Since p does not divide the order of $\mathbf{C}^\circ \cap \mathbf{T}'$, from Lemma 3.2.33 we get that $I = (C^\circ)^1 \times I'$. Moreover, using both assumptions on p, from Lemma 3.2.35 we get that $T^1/T^1_{\check{\Phi}} = (C^\circ)^1$. Let $c \in \widetilde{C}$, and recall from Proposition 3.2.25 that we have an isomorphism

$$\begin{aligned} \mathrm{Sh}_c\left(Z(E^*)^1_c\right) &\longrightarrow H^1\big(T^1/T^1_{\check{\Phi}}, k\big) \\ \xi &\longmapsto \left(\begin{array}{ccc} T^1/T^1_{\check{\Phi}} & \longrightarrow & k \\ \bar{t} & \longmapsto & \xi(t) \end{array}\right), \end{aligned} \tag{143}$$

and hence an isomorphism

$$\mathrm{Sh}_c\left(Z(E^*)^1_c\right) \xrightarrow{\mathrm{res}^I_{(C^\circ)^1}} H^1\left((C^\circ)^1, k\right). \tag{144}$$

It remains to check that the projection map from $I = (C^\circ)^1 \times I'$ to $(C^\circ)^1$ defines an inverse

$$H^1\left((C^\circ)^1, k\right) \xrightarrow{\mathrm{pr}^*_{(C^\circ)^1}} \mathrm{Sh}_c\left(Z(E^*)^1_c\right)$$

for the above isomorphism (144). In the proof of Proposition 3.2.25 we have explicitly described the inverse map

$$H^1\big(T^1/T^1_{\check{\Phi}}, k\big) \longrightarrow \mathrm{Sh}_c\left(Z(E^*)^1_c\right)$$

of the isomorphism (143) in the following way: it sends each $\xi \in H^1\big(T^1/T^1_{\check{\Phi}}, k\big)$ to the following element of $\mathrm{Sh}_c\left(Z(E^*)^1_c\right)$:

$$\xi_I\colon \quad I \xrightarrow{\subseteq} G \xrightarrow{\text{quot.}} G/[G,G] \xrightarrow{\sigma} T^1/T^1_{\check{\Phi}} \xrightarrow{\xi} k,$$

where σ is a chosen splitting (recall from Lemma 3.2.22 that $T^1/T^1_{\check{\Phi}}$ is a direct factor of $T/T_{\check{\Phi}} \cong G/[G,G]$). Hence, identifying $T^1/T^1_{\check{\Phi}}$ with $(C^\circ)^1$, we have that the inverse map

$$H^1\left((C^\circ)^1, k\right) \longrightarrow \mathrm{Sh}_c\left(Z(E^*)^1_c\right)$$

of the isomorphism (144) can be constructed by sending each $\vartheta \in H^1\left((C^\circ)^1, k\right)$ to the following element of $\mathrm{Sh}_c\left(Z(E^*)_c^1\right)$:

$$\vartheta_I \colon I \xrightarrow{\subseteq} G \xrightarrow{\text{quot.}} G/[G,G] \xrightarrow{\sigma} T^1/T^1_{\check{\Phi}} \xrightarrow[\bar{t} \leftarrow t]{\cong} (C^\circ)^1 \xrightarrow{\vartheta} k.$$

Therefore, it remains to check that $\vartheta_I = \mathrm{pr}^*_{(C^\circ)^1}(\vartheta)$: both maps coincide with ϑ on $(C^\circ)^1$, and so the only thing left to show is that the map ϑ_I is zero on I'. To this end, let us consider the Iwahori decomposition of I': it is easy to see that $U_\alpha \subseteq [G,G]$ for all $\alpha \in \Phi$ (this is done in detail in the proof of Lemma 3.2.19), and so we get that ϑ_I is zero on the "unipotent factors" of the Iwahori decomposition of I'. It now remains to check that ϑ_I is zero on $(T')^1$, but this is clear since $(T')^1 = T^1_{\check{\Phi}}$ under our assumptions, by Lemma 3.2.34.

(b) Assuming that p does not divide the connection index, Lemma 3.2.36 gives us that p divides neither the order of $Z(\mathbf{G}')$ nor the order of the fundamental group of $\mathbf{G}'$. But $\mathbf{C}^\circ \cap \mathbf{T}' \subseteq Z(\mathbf{G}')$, and so we also get that p does not divide the order of $\mathbf{C}^\circ \cap \mathbf{T}'$. ∎

Remark 3.2.38. Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. Let us show that the assumptions in part (a) of the corollary are optimal, in the sense that the restriction map

$$\mathrm{res}^I_{(C^\circ)^1} \colon H^1(I,k) \longrightarrow H^1\left((C^\circ)^1, k\right)$$

induces an isomorphism $\mathrm{Sh}_1\left(Z(E^*)_1^1\right) \cong H^1\left((C^\circ)^1, k\right)$ if and only if p divides neither the order of $\mathbf{C}^\circ \cap \mathbf{T}'$ nor the order of the fundamental group of $\mathbf{G}'$.

Proof. One implication is part of the statement of the corollary, and hence it remains to show that if the above restriction map induces an isomorphism, then the condition on p holds. Recall from Theorem 3.2.26 that the restriction map

$$\mathrm{res}^I_{T^1} \colon H^1(I,k) \longrightarrow H^1\left(T^1, k\right)$$

induces an isomorphism

$$\overline{\mathrm{res}^I_{T^1}} \colon \mathrm{Sh}_1\left(Z(E^*)_1^1\right) \longrightarrow H^1\left(T^1/(T_{\check{\Phi}})^1, k\right).$$

It is then easy to check that the following is a commutative diagram

$$\begin{tikzcd}
\mathrm{Sh}_1\left(Z(E^*)_1^1\right) \arrow[rr, "\mathrm{res}^I_{(C^\circ)^1}", "\cong"'] \arrow[dr, "\cong", "\overline{\mathrm{res}^I_{T^1}}"'] & & H^1\left((C^\circ)^1, k\right), \\
& H^1\left(T^1/(T_{\check{\Phi}})^1, k\right) \arrow[ur, "\mathrm{nat}"'] &
\end{tikzcd}$$

where nat is the map induced by the natural map $(C^\circ)^1 \longrightarrow T^1/(T_{\check{\Phi}})^1$. It follows that nat is an isomorphism. Now, a homomorphism of pro-p groups is surjective if and only if the map obtained by applying the functor $H^1(\_, k)$ is injective (this is shown in [NSW13, (1.6.14) Proposition] for $k = \mathbb{F}_p$, and the general case follows since $H^1(\_, k) \cong H^1(\_, \mathbb{F}_p) \otimes_{\mathbb{F}_p} k$, as recalled in (31)). We conclude that the natural map $(C^\circ)^1 \longrightarrow T^1/(T_{\check{\Phi}})^1$ is surjective, and by Lemma 3.2.35 (points (1) and (4)) this is equivalent to the claimed conditions on p. ∎

Corollary 3.2.39. *Assume that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$. One has that $Z(E^*)^1$ is zero if and only if $\mathbf{G}$ is semisimple with fundamental group of order not divisible by p.*

Proof. We know from Theorem 3.2.26 that $Z(E^*)^1$ is isomorphic to

$$Z(E^*)^0 \otimes_k H^1\big(T^1/T^1_{\check{\Phi}}, k\big).$$

It follows that $Z(E^*)^1$ is zero if and only if $H^1\big(T^1/T^1_{\check{\Phi}}, k\big)$ is 0, or, equivalently, if and only if $T^1/T^1_{\check{\Phi}}$ is trivial (because for a non-trivial pro-p group P one has that $H^1(P, \mathbb{F}_p)$ is nonzero: if P is abelian, as in our case, this can be easily shown by choosing a proper open normal subgroup, getting an abelian p-group as a quotient, and in general one can proceed in the same way and use the fact that a p-group is solvable).

- Assume that $\mathbf{G}$ is semisimple with fundamental group of order not divisible by p. In this situation Lemma 3.2.35 tells us that $T^1/T^1_{\check{\Phi}} = (C^\circ)^1 = 1$.
- Now assume that $T^1/T^1_{\check{\Phi}}$ is trivial and let us prove that $\mathbf{G}$ is semisimple with fundamental group of order not divisible by p. Since $T^1 = T^1_{\check{\Phi}}$, a fortiori one has $T^1 = (C^\circ)^1 \cdot T^1_{\check{\Phi}}$, but then Lemma 3.2.35 gives us that $T^1/T^1_{\check{\Phi}} = (C^\circ)^1$, and so $(C^\circ)^1$ is trivial. This means that $\mathbf{C}^\circ$ is trivial, but this condition is equivalent to the condition that the reductive group $\mathbf{G}$ is semisimple (see [Mil17, Proposition 19.10]). Moreover, since we have already remarked that the equivalent conditions in Lemma 3.2.35 hold under our assumption that $T^1/T^1_{\check{\Phi}}$ is trivial, we also have that p does not divide the order of the fundamental group of $\mathbf{G}' = \mathbf{G}$. ■

3.2.k A remark about the ramified case

A part for the case $p = 2$, in our argument for the proof of Theorem 3.2.26 we have only used the assumption that $\mathfrak{F}$ is an unramified extension of $\mathbb{Q}_p$ for the proof of Lemma 3.2.10. In the following example, we point out that such lemma becomes false for more general fields.

Example 3.2.40. Assume that $\mathbf{G} = \mathrm{SL}_2$ (with the usual choices as in Section 1.5) and that $\mathfrak{F}$ satisfies the following properties: $p \in \mathfrak{M}^2$, $q = p$ and $p \neq 2$. In other words we are assuming either that $\mathfrak{F}$ is a proper totally ramified extension of $\mathbb{Q}_p$ with $p \neq 2$ or that it is the field of Laurent series $\mathbb{F}_p((X))$ with $p \neq 2$. Let $w \in \widetilde{W}$ with $\ell(w) \geqslant 1$. We show that there is an element $\gamma_0 \in H^1(I_w, k)$ that is 0 on the "unipotent factors" of the Iwahori decomposition of I_w and such that the element $\mathrm{Sh}_w^{-1}(\gamma_0) \in E^1$ commutes (in the "graded-commutative" sense) with all the elements of $H^1(I, \mathbf{X}(1))$.

Proof. Recall from Lemma 1.10.1 that since $p \neq 2$ we have an isomorphism

$$\begin{aligned} \mathfrak{O}/\mathfrak{M} \times \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})} \times \mathfrak{O}/\mathfrak{M} &\longrightarrow (I_w)_\Phi \\ (\overline{c}, \overline{t}, \overline{b}) &\longmapsto \overline{\begin{pmatrix} 1 & 0 \\ \pi^{n_w^-} c & 1 \end{pmatrix} \cdot \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \pi^{n_w^+} b \\ 0 & 1 \end{pmatrix}} \end{aligned}$$

for suitable $n_w^-, n_w^+ \in \mathbb{Z}_{\geqslant 0}$ such that $n_w^- + n_w^+ = \ell(w) + 1$. It is easy to see that the inverse of this isomorphism is explicitly given by

$$\begin{aligned} (I_w)_\Phi &\longrightarrow \mathfrak{O}/\mathfrak{M} \times \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})} \times \mathfrak{O}/\mathfrak{M} \\ \overline{\begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix}} &\longmapsto \Big(\overline{c \cdot (1+\pi a)^{-1}}, \overline{1+\pi a}, \overline{b \cdot (1+\pi a)^{-1}}\Big) = \big(\overline{c}, \overline{1+\pi a}, \overline{b}\big) . \end{aligned} \tag{145}$$

Let us consider the following group homomorphism:

$$\begin{aligned} 1+\mathfrak{M} &\longrightarrow \mathfrak{M}/\mathfrak{M}^2 \\ 1+x &\longmapsto \overline{x}. \end{aligned}$$

It is immediate to see that $(1+\mathfrak{M})^p$ is sent to 0, and, since $\ell(w) \geqslant 1$, the same is true for $1+\mathfrak{M}^{\ell(w)+1}$. Hence we get a well defined group homomorphism

$$\begin{aligned} \frac{1+\mathfrak{M}}{(1+\mathfrak{M})^p(1+\mathfrak{M}^{\ell(w)+1})} &\longrightarrow \mathfrak{M}/\mathfrak{M}^2 \\ \overline{1+x} &\longmapsto \overline{x}. \end{aligned}$$

Putting together (145), this isomorphism and the fact that $\mathfrak{O}/\mathfrak{M} = \mathbb{F}_p \subseteq k$, we get that the following is a well defined homomorphism of topological groups (i.e., an element of $H^1(I_w, k)$):

$$\begin{aligned} \gamma_0\colon \qquad I_w &\longrightarrow k \\ \begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix} &\longmapsto \overline{a} \in \mathfrak{O}/\mathfrak{M}. \end{aligned}$$

Since $n_w^- + n_w^+ = \ell(w)+1 \geqslant 2$, looking at the equality $\det\left(\begin{smallmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{smallmatrix}\right) = 1$, it is immediate to see that

$$\gamma_0 \begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix} = \overline{a} = -\overline{d}. \tag{146}$$

Let $\xi \in H^1(I, \mathbf{X}(1))$. Let $(\gamma_0)_w \coloneqq \mathrm{Sh}_w^{-1}(\gamma_0) \in H^1(I, \mathbf{X}(w))$. As in the proof of Lemma 3.2.10 we do the following computation:

$$\begin{aligned} [\xi, (\gamma_0)_w]_{\mathrm{gr}} &= \xi \cdot (\gamma_0)_w + (\gamma_0)_w \cdot \xi \\ &= \big((\xi \cdot \tau_w) \smile (\gamma_0)_w\big) + \big((\gamma_0)_w \smile (\tau_w \cdot \xi)\big) \\ &= \big((\xi \cdot \tau_w) \smile (\gamma_0)_w\big) - \big((\tau_w \cdot \xi) \smile (\gamma_0)_w\big) \\ &= [\xi, \tau_w] \smile (\gamma_0)_w, \end{aligned}$$

Therefore, to prove that $(\gamma_0)_w$ commutes with ξ we can, equivalently, prove that $[\xi, \tau_w] \smile (\gamma_0)_w = 0$, or, since the Shapiro isomorphism commutes with the cup product, prove that

$$\text{(Claim)} \qquad \mathrm{Sh}_w([\xi, \tau_w]) \smile \gamma_0 = 0.$$

Recall from Subsection 1.10.b that $H^1(I, \mathbf{X}(1))$ is given by the elements

$$(c^-, 0, c^+)_1 \qquad \text{for } c^-, c^+ \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \cong k.$$

From the formulas (62), it is easy to see that the commutator $[\xi, \tau_w]$ lies in the subspace of $H^1(I, \mathbf{X}(w))$ given by

$$(c^-, 0, c^+)_w \qquad \text{for } c^-, c^+ \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \cong k.$$

Using the inverse of the isomorphism describing the Frattini quotient we wrote in (145), we see that $\mathrm{Sh}_w([\xi, \tau_w])$ lies in the sub-k-vector space of $H^1(I_w, k)$ generated by the following two elements:

$$\begin{aligned} \gamma_-\colon \qquad & I_w \longrightarrow k \\ & \begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix} \longmapsto \overline{c} \in \mathfrak{O}/\mathfrak{M} = \mathbb{F}_p, \\ \gamma_+\colon \qquad & I_w \longrightarrow k \\ & \begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix} \longmapsto \overline{b} \in \mathfrak{O}/\mathfrak{M} = \mathbb{F}_p. \end{aligned}$$

So looking at the claim above, we see that in order to show our statement it suffices to prove that

$$\text{(Claim)} \qquad \gamma_- \smile \gamma_0 = 0 \qquad \text{and} \qquad \gamma_+ \smile \gamma_0 = 0.$$

As we are assuming that $p \in \mathfrak{M}^2$, it follows that $\mathfrak{O}/\mathfrak{M}^2$ is an $\mathbb{F}_p$-vector space. We can thus fix the following map (homomorphism of topological groups):

$$\Sigma\colon \mathfrak{O} \xrightarrow{\text{quot.}} \mathfrak{O}/\mathfrak{M}^2 \xrightarrow[\mathfrak{M}/\mathfrak{M}^2 \longrightarrow \mathfrak{O}/\mathfrak{M}^2]{\substack{\text{a chosen section of the} \\ \text{inclusion of } \mathbb{F}_p\text{-vector spaces}}} \mathfrak{M}/\mathfrak{M}^2 \xrightarrow{\pi^{-1}\cdot(\_)} \mathfrak{O}/\mathfrak{M} \hookrightarrow k.$$

By definition, it has the property that $\Sigma(\pi x) = \overline{x}$ for all $x \in \mathfrak{O}$. We define the following continuous maps (we will see that they are *not* group homomorphisms, since they will have non-zero differentials):

$$\begin{aligned} \psi_-\colon \qquad & I \longrightarrow k \\ & \begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix} \longmapsto \Sigma(c), \\ \psi_+\colon \qquad & I \longrightarrow k \\ & \begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix} \longmapsto \Sigma(b). \end{aligned}$$

We compute the differential of ψ_- (i.e., $d\psi_-(g, g') \coloneqq \psi_-(g) + \psi_-(g') - \psi_-(gg')$ for all $g, g' \in I_w$):

$$\begin{aligned} & d\psi_- \left(\begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix}, \begin{pmatrix} 1+\pi a' & \pi^{n_w^+} b' \\ \pi^{n_w^-} c' & 1+\pi d' \end{pmatrix} \right) \\ & \quad = \Sigma(c) + \Sigma(c') - d\psi_- \begin{pmatrix} * & * \\ \pi^{n_w^-} c \cdot (1+\pi a') + (1+\pi d) \cdot \pi^{n_w^-} c' & * \end{pmatrix} \\ & \quad = \Sigma(c) + \Sigma(c') - \Sigma\big(c + c' + \pi \cdot (ca' + dc')\big) \\ & \quad = \overline{ca' + dc'}. \end{aligned}$$

Similarly one computes that

$$d\psi_+ \left(\begin{pmatrix} 1+\pi a & \pi^{n_w^+} b \\ \pi^{n_w^-} c & 1+\pi d \end{pmatrix}, \begin{pmatrix} 1+\pi a' & \pi^{n_w^+} b' \\ \pi^{n_w^-} c' & 1+\pi d' \end{pmatrix} \right) = \overline{ab' + bd'}.$$

Recalling (146) and the definitions of γ_- and of γ_+, we deduce the following equalities for all $g, g' \in I_w$:

$$d\psi_-(g, g') = \gamma_-(g)\gamma_0(g') - \gamma_0(g)\gamma_-(g'),$$
$$d\psi_+(g, g') = \gamma_0(g)\gamma_+(g') - \gamma_+(g)\gamma_0(g').$$

This yields

$$\gamma_- \smile \gamma_0 - \gamma_0 \smile \gamma_- = 0,$$
$$\gamma_0 \smile \gamma_+ - \gamma_+ \smile \gamma_0 = 0.$$

Using anti-commutativity of the cup product and that $p \neq 2$, we deduce that both $\gamma_- \smile \gamma_0$ and $\gamma_0 \smile \gamma_+$ are zero, thus concluding the proof of our claim. ■

3.3 "Toric" subalgebras

In this section we want to extend the following known result on the pro-p Iwahori–Hecke algebra to the Ext-algebra (with some assumptions on the field $\mathfrak{F}$).

Assumptions. We put ourselves in the general assumptions of Section 1.1, without any restriction on $\mathbf{G}$ and $\mathfrak{F}$. Whenever we will use more restrictive assumptions, these will be explicitly stated.

Let us denote by H_T the pro-p Iwahori–Hecke algebra associated with the group T (with respect to its unique pro-p Iwahori subgroup T^1), while we reserve the notation H for the pro-p Iwahori–Hecke algebra associated with G. Using the braid relations it is easy to see that one has a k-algebra isomorphism

$$\begin{aligned} k[T/T^1] &\longrightarrow H_T \\ \underset{(\text{for } t \in T/T^1)}{(t)} &\longmapsto \tau_t. \end{aligned}$$

Now, we consider the submonoids of T:

$$\begin{aligned} T^- &:= \left\{ t \in T \;\middle|\; (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant 0 \text{ for all } \alpha \in \Phi^- \right\} \\ &\qquad\qquad (\text{submodnoid of } \textbf{antidominant elements}), \\ T^+ &:= \left\{ t \in T \;\middle|\; (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant 0 \text{ for all } \alpha \in \Phi^+ \right\} \\ &\qquad\qquad (\text{submodnoid of } \textbf{dominant elements}). \end{aligned}$$

Let $H_{T^\pm} \subseteq H_T$ be the subalgebra corresponding to the monoid algebra $k[T^\pm/T^1]$ via the fixed isomorphism $H_T \cong k[T/T^1]$. It is easy to see that H_T is a localization of $H_{T^\pm}$ and it is well-known that one has an injective k-algebra homomorphism

$$\begin{aligned} H_{T^\pm} &\longrightarrow H \\ \underset{(\text{for } t \in T^\pm/T^1)}{\tau_t} &\longmapsto \tau_t. \end{aligned}$$

(this is easy to see using the braid relations and additivity of the length on a closed Weyl chamber, see also [Vig98, II.5. Proposition]).

In Proposition 3.3.4 and in Remark 3.3.7 we extend these results (in a suitable sense) to Ext-algebra setting, under the assumption that $\mathfrak{F}$ does not contain non-trivial roots of 1.

We start by introducing some notation and proving some preliminary lemmas towards this result.

Let $j \in \mathbb{Z}_{\geqslant 0}$. We define

$$T_j^- := \left\{ t \in T \;\middle|\; (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant j \text{ for all } \alpha \in \Phi^- \right\},$$
$$T_j^+ := \left\{ t \in T \;\middle|\; (\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t) \geqslant j \text{ for all } \alpha \in \Phi^+ \right\}.$$

From the definitions, we have

$$T^- = T_0^-,$$
$$T^+ = T_0^+.$$

It is easy to see that T_j^- and T_j^+ are sub-semigroups of T (actually even more: we have a well defined multiplication action of the monoid $T^\pm$ on $T_j^\pm$).

Let us choose a split torus $\mathscr{T}$ over $\mathfrak{O}$ such that its base change $\mathscr{T}_{\mathfrak{F}}$ is isomorphic to $\mathbf{T}$. Such a torus can be obtained for example by choosing a splitting of $\mathbf{T}$, or using the more canonical construction of [BT84, 1.2.11], or by considering the identity component of the Néron model of $\mathbf{T}$ (the last one is the approach used in [OS19, §7.2.2]). In any case, $\mathscr{T}$ does not depend on the chosen construction, in the sense that if $\mathscr{T}$ and $\mathscr{T}'$ are two split tori over $\mathfrak{O}$ such that both base changes $\mathscr{T}_{\mathfrak{F}}$ and $\mathscr{T}'_{\mathfrak{F}}$ are isomorphic to $\mathbf{T}$, then there is a unique isomorphism f of group schemes over $\mathfrak{O}$ making the following diagram commute:

$$\begin{tikzcd} & \mathscr{T} \arrow[dd, "f"] \\ \mathbf{T} \arrow[ur] \arrow[dr] & \\ & \mathscr{T}', \end{tikzcd}$$

where the arrows on the left are the structural maps of the base change. The claim can be proved as follows: it is clear that there is a unique isomorphism $f_{\mathfrak{F}}$ of group schemes over $\mathfrak{F}$ making the following diagram commute:

$$\begin{tikzcd} & \mathscr{T}_{\mathfrak{F}} \arrow[dd, "f_{\mathfrak{F}}"] \\ \mathbf{T} \arrow[ur] \arrow[dr] & \\ & \mathscr{T}'_{\mathfrak{F}}, \end{tikzcd}$$

but then we see that there exists a unique isomorphism $f \colon \mathscr{T} \longrightarrow \mathscr{T}'$ whose base change to $\mathfrak{F}$ is $f_{\mathfrak{F}}$: this is immediate by choosing splittings of $\mathscr{T}$ and of $\mathscr{T}'$, and by remarking that a homomorphism over $\mathfrak{O}$ or over $\mathfrak{F}$ is given by a matrix with integer coefficients.

For all $j \in \mathbb{Z}_{\geqslant 0}$, we define

$$T^{j+1} = \ker\left(\mathscr{T}(\mathfrak{O}) \xrightarrow{\text{reduction}} \mathscr{T}\left(\mathfrak{O}/\mathfrak{M}^{j+1}\right)\right) \subseteq \mathscr{T}(\mathfrak{F}) = T.$$

Lemma 3.3.1. *Let $j \in \mathbb{Z}_{\geqslant 0}$. One has that, for all $t \in T_j^- \cup T_j^+$, the map*

$$I_t \xrightarrow[\text{decomp.}]{\text{Iwahori}} \prod_{\alpha \in \Phi^-} \mathfrak{U}_{(\alpha, g_t(\alpha))} \times T^1 \times \prod_{\alpha \in \Phi^+} \mathfrak{U}_{(\alpha, g_t(\alpha))} \xrightarrow{\text{proj.}} T^1 \xrightarrow{\text{quot.}} T^1/T^{j+1}$$

is a group homomorphism (and so a homomorphism of topological groups).

Proof. Let us divide the proof into two parts: in the first part we will prove the claim for $t \in T_j^-$, while in the second part we will use this result to prove the claim for $t \in T_j^+$.

- Let us prove the claim for $t \in T_j^-$. As in [OS19, §7.2.2], let us denote by $\mathbf{G}_{x_0}$ the Bruhat group scheme associated with the fixed hyperspecial vertex x_0 corresponding to the 0 point of the apartment, let us define $K_{x_0} := \mathbf{G}_{x_0}^\circ(\mathfrak{O})$, i.e., the parahoric subgroup associated with x_0, and, for all $m \in \mathbb{Z}_{\geqslant 1}$, let us further define

$$K_{x_0,m} := \ker\left(\mathbf{G}_{x_0}^\circ(\mathfrak{O}) \xrightarrow{\text{reduction}} \mathbf{G}_{x_0}^\circ\left(\mathfrak{O}/\mathfrak{M}^m\right)\right).$$

We have the following explicit description of $K_{x_0,m}$ (see [OS19, Proposition 7.9]): the map defined by multiplication induces a bijection

$$\prod_{\alpha\in\Phi^-} \mathcal{U}_{(\alpha,m)} \times T^m \times \prod_{\alpha\in\Phi^+} \mathcal{U}_{(\alpha,m)} \longrightarrow K_{x_0,m}. \tag{147}$$

Since $K_{x_0,m}$ is normal in K_{x_0} by definition, it follows that $I_t \cap K_{x_0,m}$ is normal in I_t (we are implicitly using that I_t is contained in K_{x_0}). For all $\alpha \in \Phi^-$, the factor in the Iwahori decomposition of I_t associated with α is $\mathcal{U}_{(\alpha,g_t(\alpha))}$, where $g_t(\alpha) = \max\{1, (\mathrm{val}_{\mathfrak{F}} \circ\alpha)(t) + 1\} \geqslant j+1$ (see Lemma 1.3.2). For a subgroup H of I_t, let us denote by $\overline{H}$ the image of H in the quotient group $I_t/\left(I_t \cap K_{x_0,j+1}\right)$. Choosing $m := j+1$, from the last inequality we get that every element of the quotient $I_t/\left(I_t \cap K_{x_0,j+1}\right)$ can be represented as a product of an element in $\overline{T^1}$ and an element in $\overline{U_t^+}$, where $U_t^+ := \mathrm{Image}\left(\prod_{\alpha\in\Phi^+} \mathcal{U}_{(\alpha,g_t(\alpha))}\right) \subseteq I_t$. We see that U_t^+ is a subgroup of I_t: indeed with notation as in (130), we have an injective map induced by multiplication

$$U^- \times T \times U \longrightarrow G,$$

but then we see that the inclusion $U_t^+ \subseteq I_t \cap U$ is actually an equality, because, given an element $u \in I_t \cap U$, we consider its Iwahori decomposition and we see that it cannot have non-tirivial factors lying in U^- or in T. Therefore, we have shown that $U_t^+ = I_t \cap U$, and in particular U_t^+ is a subgroup of I_t. Since furthermore T^1 normalizes U_t^+ (by (1)), it follows that $\overline{U_t^+}$ is normal in $I_t/\left(I_t \cap K_{x_0,j+1}\right)$. We have a natural group homomorphism

$$\begin{array}{ccccc} T^1/T^{j+1} & \longrightarrow & \dfrac{I_t/\left(I_t \cap K_{x_0,j+1}\right)}{\overline{U_t^+}} & \cong & \dfrac{I_t}{\left(I_t \cap K_{x_0,j+1}\right)\cdot U_t^+} \\ \overline{t} & \longmapsto & \overline{\overline{t}}, & & \end{array}$$

which is surjective by the description of the elements of $I_t/\left(I_t \cap K_{x_0,j+1}\right)$ we have just given, but which is also injective: indeed let us consider an element in $x \in T^1$ which is sent to the identity, i.e., such that $x \in \left(I_t \cap K_{x_0,j+1}\right)\cdot U_t^+ \subseteq K_{x_0,j+1}\cdot U_t^+$; we can write such element as $x = u^- y u^+ (u^+)'$ for some u^- in the image of $\prod_{\alpha\in\Phi^-} \mathcal{U}_{(\alpha,j+1)}$, some $y \in T^{j+1}$, some u^+ in the image of $\prod_{\alpha\in\Phi^+} \mathcal{U}_{(\alpha,j+1)}$ and some $(u^+)' \in U_t^+$. But then using the Iwahori decomposition (of I) it follows that $x = y \in T^{j+1}$, thus concluding the proof of the injectivity of the above map.

Now we are done, because the composite map

$$I_t \xrightarrow[g\mapsto\overline{g}]{} \frac{I_t}{\left(I_t \cap K_{x_0,j+1}\right)\cdot U_t^+} \xrightarrow[\overline{x}\leftarrow\overline{x}]{\cong} T^1/T^{j+1}$$

is exactly the map in the statement of the lemma (because we already know that the first map is trivial on the "unipotent factors" of the Iwahori decomposition of I_t), and it is obviously a group homomorphism.

- Let us prove the claim for $t \in T_j^+$. Using the formula to compute the index $g_{t'}(\alpha)$ for $t' \in \{t, t^{-1}\}$ and $\alpha \in \Phi$ (Remark 3.1.3), and using the explicit formula to compute the conjugation action of an element of T^1 on the "unipotent factors" (formula (1)), it is easy to see that the rectangles in the following diagram are commutative:

$$\begin{tikzcd} I_t \arrow[r, "\substack{\text{Iwahori}\\ \text{decomp.}}"] \arrow[d, "\cong"', "\mathrm{conj}_{t^{-1}}"] & \prod_{\alpha\in\Phi^-} \mathfrak{U}_{(\alpha,1)} \times T^1 \times \prod_{\alpha\in\Phi^+} \mathfrak{U}_{(\alpha,(\mathrm{val}_{\mathfrak{F}}\circ\alpha)(t))} \arrow[r, "\text{proj.}"] \arrow[d, "\cong"', "\mathrm{conj}_{t^{-1}}"] & T^1 \arrow[r, "\text{quot.}"] \arrow[d, equal] & T^1/T^{j+1} \arrow[d, equal] \\ I_{t^{-1}} \arrow[r, "\substack{\text{Iwahori}\\ \text{decomp.}}"] & \prod_{\alpha\in\Phi^-} \mathfrak{U}_{(\alpha,1+(\mathrm{val}_{\mathfrak{F}}\circ\alpha)(t^{-1}))} \times T^1 \times \prod_{\alpha\in\Phi^+} \mathfrak{U}_{(\alpha,0)} \arrow[r, "\text{proj.}"] & T^1 \arrow[r, "\text{quot.}"] & T^1/T^{j+1}. \end{tikzcd}$$

  Since $t \in T_j^+$, it follows that $t^{-1} \in T_j^-$, and so we already know that the composite of the bottom maps is a group homomorphism. Hence the composite of the maps at the top is a group homomorphism, as we wanted to show. ∎

Corollary 3.3.2. *Assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, let j be a positive integer such that $1 + \mathfrak{M}^{j+1} \subseteq (1 + \mathfrak{M})^p$, and let $t \in T_j^- \cup T_j^+$. One has that the map*

$$\mathcal{T}_t\colon\ I_t \xrightarrow{\substack{\text{Iwahori}\\ \text{decomp.}}} \prod_{\alpha\in\Phi^-} \mathfrak{U}_{(\alpha,g_t(\alpha))} \times T^1 \times \prod_{\alpha\in\Phi^+} \mathfrak{U}_{(\alpha,g_t(\alpha))} \xrightarrow{\text{proj.}} T^1 \xrightarrow{\text{quot.}} T^1/(T^1)^p$$

is a group homomorphism (and hence a homomorphism of topological groups).

Proof. If we show that $T^{j+1} \subseteq (T^1)^p$, then we get the desired result by composing the group homomorphism of Lemma 3.3.1 with the natural map $T^1/T^{j+1} \longrightarrow T^1/(T^1)^p$. We fix an $\mathfrak{O}$-isomorphism between $\mathscr{T}$ and $\mathbb{G}_{\mathrm{m}}^n$ (for some $n \in \mathbb{Z}_{\geqslant 0}$). By definition we have that

$$T^{j+1} = \ker\left(\mathscr{T}(\mathfrak{O}) \xrightarrow{\text{reduction}} \mathscr{T}\big(\mathfrak{O}/\mathfrak{M}^{j+1}\big)\right).$$

Using our $\mathfrak{O}$-isomorphism, we see that the condition $1 + \mathfrak{M}^{j+1} \subseteq (1 + \mathfrak{M})^p$ tells us that $T^{j+1} \subseteq (T^1)^p$. ∎

Lemma 3.3.3. *Assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ without non-trivial p-th roots (in particular $p \neq 2$), let j be a positive integer such that $1+\mathfrak{M}^{j+1} \subseteq (1+\mathfrak{M})^p$, and let $t \in T_j^- \cup T_j^+$. One has that the map*

$$\begin{aligned} \mathcal{T}_t^\vee\colon\ H^1(T^1, k) \cong \mathrm{Hom}_{\mathbb{F}_p}\big(T^1/(T^1)^p, k\big) &\longrightarrow \mathrm{Hom}_{\text{top. gps.}}(I_t, k) \cong H^1(I_t, k) \\ \beta &\longmapsto \beta \circ \mathcal{T}_t \end{aligned}$$

(which is well defined by Corollary 3.3.2) can be extended in a unique way to a homomorphism of k-algebras (with respect to the cup product)

$$\mathcal{T}_t^\vee\colon H^*(T^1, k) \longrightarrow H^*(I_t, k).$$

Proof. Since $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, it follows that $1+\mathfrak{M}$ is topologically finitely generated (see for example [FV02, Chapter I, (6.5), Corollary, part (1)]). Since $\mathfrak{F}$ has no non-trivial p-th roots, it follows that $1+\mathfrak{M}$ is torsion-free. Hence, $1+\mathfrak{M}$ is a uniform pro-p group (see the definition given in Section 1.8). Lazard Theorem on uniform pro-p groups (Theorem 1.8.1) then yields that the cohomology algebra of T^1 (with respect to the cup product) can be identified with the exterior algebra generated by the first cohomology group:

$$H^*(T^1,k) \cong \bigwedge\nolimits_k^* \left(\mathrm{Hom}_{\mathbb{F}_p}\left(T^1/(T^1)^p,k\right)\right).$$

On the other hand, even if the pro-p group I_t is not necessarily uniform, we still we still have a natural homomorphism of k-algebras from the tensor algebra to the cohomology algebra (since $p \neq 2$):

$$\bigwedge\nolimits_k^* \left(H^1(I_t,k)\right) \longrightarrow H^*(I_t,k).$$

We can consider the homomorphism of k-algebras $\bigwedge_k^*(\mathcal{T}_t^\vee)$ functorially induced by $\mathcal{T}_t^\vee$ on the tensor algebras, getting a composite homomorphism

$$H^*(T^1,k) \xrightarrow{\cong} \bigwedge\nolimits_k^* \left(\mathrm{Hom}_{\mathbb{F}_p}\left(T^1/(T^1)^p,k\right)\right) \xrightarrow{\bigwedge_k^*(\mathcal{T}_t^\vee)} \bigwedge\nolimits_k^* \left(H^1(I_t,k)\right) \longrightarrow H^*(I_t,k).$$

This is the required homomorphism of k-algebras extending the original map $\mathcal{T}_t^\vee$. Its explicit description is

$$\begin{array}{ccc} H^*(T^1,k) & \longrightarrow & H^*(I_t,k) \\ \underset{\left(\text{for } \beta_i \in H^1(T^1,k) \text{ for all } i\in\{1,\dots,n\}\right)}{\beta_1 \smile \cdots \smile \beta_n} & \longmapsto & \left(\beta_1 \circ \mathrm{pr}_{T^1}^{I_t}\right) \smile \cdots \smile \left(\beta_n \circ \mathrm{pr}_{T^1}^{I_t}\right). \end{array}$$

Uniqueness is clear because any homomorphism of k-algebras extending $\mathcal{T}_t^\vee$ must act in this way on a cup product. ■

Let us denote by E_T^* the pro-p Iwahori–Hecke algebra associated with the group T (with respect to the unique pro-p Iwahori subgroup T^1). We have a "Bruhat" decomposition

$$E_T^* = \bigoplus_{i\in\mathbb{Z}_{\geqslant 0}} \bigoplus_{t\in T/T^1} H^i(T^1,\mathbf{X}_T(t)), \tag{148}$$

where $\mathbf{X}_T(t) \coloneqq \mathrm{ind}_{T^1}^{T^1tT^1}(k) \cong k$. For the 0^{th} graded piece we have the identification $E_T^0 \cong k[T/T^1]$ (length function is constantly 0) and we will simply write t in place of τ_t (this is useful in order to distinguish it from $\tau_t \in E^0$). Using again that the length function is constantly 0, the multiplicative structure can be easily described in the following way: let $t,t' \in T/T^1$, let $\beta \in H^i(T^1,k)$, let $\beta' \in H^{i'}(T^1,k)$ and let us denote

$$\begin{aligned} (\beta)_t &\coloneqq \mathrm{Sh}_t^{-1}(\beta) \in H^i(T^1,\mathbf{X}_T(t)) \subseteq E_T^*, \\ (\beta')_{t'} &\coloneqq \mathrm{Sh}_t^{-1}(\beta') \in H^{i'}(T^1,\mathbf{X}_T(t')) \subseteq E_T^*. \end{aligned}$$

Then the formula relating the (opposite of the) Yoneda product with the cup product (Corollary 1.9.3), combined with the explicit description of the action of the multiplication by elements of degree 0 (Corollary 1.9.5), gives us the following:

$$\begin{aligned} (\beta)_t \cdot t' &= t' \cdot (\beta)_t = (\beta)_{tt'}, \\ (\beta)_t \cdot (\beta')_{t'} &= \left((\beta)_t \cdot t'\right) \smile \left(t \cdot (\beta')_{t'}\right) \\ &= (\beta)_{tt'} \smile (\beta')_{tt'} \\ &= (\beta \smile \beta')_{tt'}, \end{aligned} \tag{149}$$

and so this describes multiplication in E_T^*. In particular, E_T^* is a graded-commutative k-algebra.

Proposition 3.3.4. *Assume that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ without non-trivial p-th roots (in particular $p \neq 2$), and let j be a positive integer such that the inclusion $1+\mathfrak{M}^{j+1} \subseteq (1+\mathfrak{M})^p$ holds. Let E_T^* and $\mathbf{X}_T(\_)$ be defined as above, and let us further consider the following subspace of E_T^*:*

$$\begin{aligned} E^*_{T^\pm,j} &\coloneqq \left(\bigoplus_{t\in T^\pm/T^1} H^0(T^1,\mathbf{X}_T(t)) \right) \oplus \left(\bigoplus_{i\in\mathbb{Z}_{\geqslant 1}} \bigoplus_{t\in T_j^\pm/T^1} H^i(T^1,\mathbf{X}_T(t)) \right) \\ &\cong k\left[T^\pm/T^1\right] \oplus \left(\bigoplus_{i\in\mathbb{Z}_{\geqslant 1}} \bigoplus_{t\in T_j^\pm/T^1} H^i(T^1,k) \right). \end{aligned} \tag{150}$$

One has that $E^*_{T^\pm,j}$ is as sub-k-algebra of E_T^* and that there is an injective homomorphism of graded k-algebras

$$\mathfrak{T}_{T^\pm,j} \colon E^*_{T^\pm,j} \longrightarrow E^*$$

defined in the following way:

- *in degree 0 one uses the canonical identification $H^0(T^1,\mathbf{X}_T(t)) \cong k \cong H^0(I,\mathbf{X}(t))$ for all $t \in T^\pm/T^1$.*
- *for $i \in \mathbb{Z}_{\geqslant 1}$ and for $t \in T_j^\pm/T^1$ one uses the map*

$$H^i(T^1,\mathbf{X}_T(t)) \cong H^i(T^1,k) \xrightarrow{\mathcal{T}_t^\vee} H^i(I_t,k) \cong H^i(I,\mathbf{X}(t))$$

  defined in Lemma 3.3.3.

Proof. It is obvious that $\mathfrak{T}_{T^\pm,j}$ s a well-defined homomorphism of k-vector spaces. It remains to check that $E^*_{T^\pm,j}$ is a sub-k-algebra of E_T^*, that $\mathfrak{T}_{T^\pm,j}$ is injective and that it preserves the product.

- It is easy to see that $E^*_{T^\pm,j}$ is a sub-k-algebra of E_T^*: indeed this follows from the fact that $T^\pm$ is a submonoid of T, from the fact that one has a well-defined multiplication action of $T^\pm$ on $T_j^\pm$, and from the explicit description of the multiplication in E_T^* given in Formula (150).
- Let us prove injectivity. By construction $\mathfrak{T}_{T^\pm,j}$ preserves the degree and the decomposition with respect to the "Iwahori Weyl groups" T/T^1 on the left side and $\widetilde{W}$ on the right side. Moreover, in degree 0 injectivity is clear. It therefore suffices to show that, for all $t \in T_j^\pm$, the map

$$\begin{array}{cccc} \mathcal{T}_t^\vee\colon & H^*(T^1,k) & \longrightarrow & H^*(I_t,k) \\ & \begin{array}{c}\beta_1 \smile \cdots \smile \beta_n \\ \left(\begin{array}{c}\text{for } \beta_i \in H^1(T^1,k) \\ \text{for all } i \in \{1,\dots,n\}\end{array}\right)\end{array} & \longmapsto & \left(\beta_1 \circ \mathrm{pr}^{I_t}_{T^1}\right) \smile \cdots \smile \left(\beta_n \circ \mathrm{pr}^{I_t}_{T^1}\right). \end{array}$$

  is injective. But it is easy to see that $\mathrm{res}^{I_t}_{T^1} \circ \mathcal{T}_t^\vee = \mathrm{id}_{H^*(T^1,k)}$, and so injectivity follows.

- Let us prove that $\mathfrak{T}_{T^\pm,j}$ preserves the product between two elements of degree 0. We are claiming that the map

$$\begin{aligned} k\left[T^\pm/T^1\right] &\longrightarrow E^0 \\ t &\longmapsto \tau_t \end{aligned}$$

preserves the product: this is true because, by using the length formula (10), one sees that the lengths of two elements of $T^\pm/T^1$ always add up.

- Let us prove that $\mathfrak{T}_{T^\pm,j}$ respects the products between elements of degree 0 and elements of degree 1. In other words, let $t \in T^\pm/T^1$, let $t' \in T_j^\pm/T^1$, let $\beta \in H^1(T^1,k)$, and let $(\beta)_{t'}$ denote the image of β in $H^1(I,\mathbf{X}_T(t'))$. We have to prove that

(Claim)
$$\begin{aligned} \mathfrak{T}_{T^\pm,j}(t\cdot(\beta)_{t'}) &= \tau_t \cdot \mathfrak{T}_{T^\pm,j}((\beta)_{t'}), \\ \mathfrak{T}_{T^\pm,j}((\beta)_{t'}\cdot t) &= \mathfrak{T}_{T^\pm,j}((\beta)_{t'})\cdot \tau_t. \end{aligned}$$

It is easy to see that

$$\begin{aligned} \mathfrak{T}_{T^\pm,j}(t\cdot(\beta)_{t'}) &= \mathfrak{T}_{T^\pm,j}((\beta)_{tt'}) \\ &= \left(\beta\circ \mathrm{pr}_{T^1}^{I_{tt'}}\right)_{tt'}. \end{aligned}$$

Of course, since t and $(\beta)_{t'}$ commute, we get the same result for the multiplication on the right. So, what we have to prove are the following two equalities:

(Claim)
$$\tau_t\cdot\left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)_{t'} = \left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)_{t'}\cdot\tau_t = \left(\beta\circ \mathrm{pr}_{T^1}^{I_{tt'}}\right)_{tt'}.$$

As before, the lengths of t and t' add up and so we can apply the following formulas to compute the product (see Corollary 1.9.5): for all $\gamma\in H^1(I_{t'},k)$ we have

$$\begin{aligned} (\gamma)_{t'}\cdot\tau_t &= \left(\mathrm{res}^{I_{t'}}_{I_{t't}}\gamma\right)_{t't}, \\ \tau_t\cdot(\gamma)_{t'} &= \left(\mathrm{res}^{tI_{t'}t^{-1}}_{I_{tt'}} t^*\gamma\right)_{tt'}. \end{aligned}$$

Therefore, setting $\gamma \coloneqq \beta\circ\mathrm{pr}_{T^1}^{I_{t'}}$, we get the following (with obvious notation for inclusions and conjugations):

$$\begin{aligned} \left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)_{t'}\cdot\tau_t &= \left(\mathrm{res}^{I_{t'}}_{I_{t't}}\left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)\right)_{t't} \\ &= \left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\circ \mathrm{incl}^{I_{t'}}_{I_{t't}}\right)_{t't} \\ &= \left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\circ \mathrm{incl}^{I_{t'}}_{I_{tt'}}\right)_{tt'}, \\ \tau_t\cdot\left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)_{t'} &= \left(\mathrm{res}^{tI_{t'}t^{-1}}_{I_{tt'}} t^*\left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)\right)_{tt'} \\ &= \left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\circ \mathrm{conj}_{t^{-1}}\circ \mathrm{incl}^{tI_{t'}t^{-1}}_{I_{tt'}}\right)_{tt'}. \end{aligned}$$

It is easy to see that the maps $\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\circ \mathrm{incl}^{I_{t'}}_{I_{tt'}}$ and $\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\circ \mathrm{conj}_{t^{-1}}\circ \mathrm{incl}^{tI_{t'}t^{-1}}_{I_{tt'}}$ are both trivial on the "unipotent factors" of the Iwahori decomposition of $I_{tt'}$ and that they both coincide with β on T^1. Therefore both maps are equal to $\beta\circ\mathrm{pr}_{T^1}^{I_{tt'}}$, thus proving our claim that

$$\tau_t\cdot\left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)_{t'} = \left(\beta\circ \mathrm{pr}_{T^1}^{I_{t'}}\right)_{t'}\cdot\tau_t = \left(\beta\circ \mathrm{pr}_{T^1}^{I_{tt'}}\right)_{tt'},$$

and with it that $\mathfrak{T}_{T^\pm,j}$ respects the products between elements of degree 0 and elements of degree 1.

- Let us prove that $\mathfrak{T}_{T^\pm,j}$ respects the products between elements of degree 0 and elements of degree i for $i \in \mathbb{Z}_{\geqslant 1}$, by reducing to the case $i=1$. Let $v, w \in \widetilde{W}$ such that the lengths add up. Furthermore let $\gamma_{w,1}, \dots \gamma_{w,i} \in H^1(I, \mathbf{X}(w))$. We claim that

$$\tau_v \cdot (\gamma_{w,1} \smile \cdots \smile \gamma_{w,i}) = (\tau_v \cdot \gamma_{w,1}) \smile \cdots \smile (\tau_v \cdot \gamma_{w,i}), \tag{151}$$
$$(\gamma_{w,1} \smile \cdots \smile \gamma_{w,i}) \cdot \tau_v = (\gamma_{w,1} \cdot \tau_v) \smile \cdots \smile (\gamma_{w,i} \cdot \tau_v). \tag{152}$$

This formula can be proved as follows: both sides of the first equation (respectively, the second equation) are elements of $H^i(I, \mathbf{X}(vw))$, and so it remains to check that applying the Shapiro isomorphism to both sides we get an equality, and this can be proved by using the formulas of Corollary 1.9.5 (which compute the (opposite of the) Yoneda product in terms of restrictions and conjugations) and by remarking that the Shapiro isomorphism, restrictions and conjugations commute with the cup product.

Now let $t \in T^\pm/T^1$, let $t' \in T^\pm_j/T^1$, let $\beta \in H^i(T^1, k)$, and as usual let $(\beta)_{t'}$ denote the image of β in $H^i(I, \mathbf{X}_T(t'))$. Again, we have to show that

(Claim)
$$\mathfrak{T}_{T^\pm,j}(t \cdot (\beta)_{t'}) = \tau_t \cdot \mathfrak{T}_{T^\pm,j}((\beta)_{t'}),$$
$$\mathfrak{T}_{T^\pm,j}((\beta)_{t'} \cdot t) = \mathfrak{T}_{T^\pm,j}((\beta)_{t'}) \cdot \tau_t.$$

Now, β can be represented by a sum of cup products of elements having degree 1, and so, by linearity, we can assume without loss of generality that $\beta = \beta_1 \smile \cdots \smile \beta_i$. Therefore, we find that

$$\begin{aligned}
\mathfrak{T}_{T^\pm,j}\big(t \cdot (\beta)_{t'}\big) &= \mathfrak{T}_{T^\pm,j}\big(t \cdot (\beta_1 \smile \cdots \smile \beta_i)_{t'}\big) \\
&= \mathfrak{T}_{T^\pm,j}\big((\beta_1 \smile \cdots \smile \beta_i)_{tt'}\big) \\
&= \mathfrak{T}_{T^\pm,j}\big((\beta_1)_{tt'} \smile \cdots \smile (\beta_i)_{tt'}\big) \\
&= \mathfrak{T}_{T^\pm,j}\big((\beta_1)_{tt'}\big) \smile \cdots \smile \mathfrak{T}_{T^\pm,j}\big((\beta_i)_{tt'}\big) && \text{(by def. of } \mathfrak{T}_{T^\pm,j}) \\
&= \big(\tau_t \cdot \mathfrak{T}_{T^\pm,j}((\beta_1)_{t'})\big) \smile \cdots \smile \big(\tau_t \cdot \mathfrak{T}_{T^\pm,j}((\beta_i)_{t'})\big) && \text{(already proved)} \\
&= \tau_t \cdot \big(\mathfrak{T}_{T^\pm,j}((\beta_1)_{t'}) \smile \cdots \smile \mathfrak{T}_{T^\pm,j}((\beta_i)_{t'})\big) && \text{(by (151))} \\
&= \tau_t \cdot \mathfrak{T}_{T^\pm,j}\big((\beta_1)_{t'} \smile \cdots \smile (\beta_i)_{t'}\big) && \text{(by def. of } \mathfrak{T}_{T^\pm,j}) \\
&= \tau_t \cdot \mathfrak{T}_{T^\pm,j}(\beta).
\end{aligned}$$

The proof of the other formula we had to check is completely analogous.

- Now we can prove that $\mathfrak{T}_{T^\pm,j}$ respects all products. We have already checked products involving elements of degree 0, so it suffices to check the following: for all $t, t' \in T^\pm_j$, for all $i, i' \in \mathbb{Z}_{\geqslant 1}$, for all $\beta \in H^i(I, \mathbf{X}_T(t))$, for all $\beta' \in H^{i'}(I, \mathbf{X}_T(t'))$ one has:

(Claim)
$$\mathfrak{T}_{T^\pm,j}(\beta \cdot \beta') = \mathfrak{T}_{T^\pm,j}(\beta) \cdot \mathfrak{T}_{T^\pm,j}(\beta').$$

On the left hand side we can of course use the formula relating the (opposite of the) Yoneda product and the cup product (Corollary 1.9.3), but also on the right hand side, since $\mathfrak{T}_{T^\pm,j}(\beta) \in H^i(I, \mathbf{X}_T(t))$, $\mathfrak{T}_{T^\pm,j}(\beta') \in H^{i'}(I, \mathbf{X}_T(t'))$ and $\ell(tt') = \ell(t) + \ell(t')$ as usual. So our claim becomes

(Claim)
$$\mathfrak{T}_{T^\pm,j}\left((\beta \cdot t') \smile (t \cdot \beta')\right) = \big(\mathfrak{T}_{T^\pm,j}(\beta) \cdot \tau_{t'}\big) \smile \big(\tau_t \cdot \mathfrak{T}_{T^\pm,j}(\beta')\big).$$

We already know that $\mathfrak{T}_{T^\pm,j}$ preserves the product when one of the two factors has degree 0. Therefore, it suffices to check that the map

$$\mathfrak{T}_{T^\pm,j} \colon H^*(T^1, \mathbf{X}_T(tt')) \longrightarrow H^*(I, \mathbf{X}(tt'))$$

preserves the cup product. This can be easily seen by applying the Shapiro isomorphism on both sides (as it preserves the cup product) and using the explicit description of the map $\mathcal{T}_{tt'}^{\vee}\colon H^*(T^1,k) \longrightarrow H^*(I_{tt'},k)$. ∎

We complement the proposition with some remarks.

Remark 3.3.5. If $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2$, or more generally if $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$ with ramification index strictly smaller than $p-1$, then, using the logarithm and the exponential, one sees that $(1+\mathfrak{M})^p = 1+\mathfrak{M}^2$ and that there are no non-trivial p-th roots. Thus, in such cases, we can apply the previous proposition with $j=1$.

The following remarks highlights that, in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2,3$, the proposition yields an optimal result.

Remark 3.3.6. Let us assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2,3$ (with the usual choices as in Section 1.5). Also taking the last remark into account, the proposition yields an injective homomorphism of graded k-algebras

$$E^*_{T^\pm,1} \longrightarrow E^*,$$

where

$$\begin{aligned}
E^0_{T^\pm,1} &= \bigoplus_{t \in T^\pm/T^1} H^0(T^1, \mathbf{X}_T(t)) \cong k\left[T^\pm/T^1\right], \\
E^1_{T^\pm,1} &= \bigoplus_{t \in T_1^\pm/T^1} H^1(T^1, \mathbf{X}_T(t)), \\
E^i_{T^\pm,1} &= 0 && \text{for all } i \in \mathbb{Z}_{\geqslant 2}.
\end{aligned}$$

We remark that the above homomorphism cannot be extended to a (not necessarily injective) graded k-algebra homomorphism $E^*_{T^\pm,0} \longrightarrow E^*$.

Proof. It is easy to check that, for all $t \in T_1^\pm/T^1$, the injective homomorphism $E^*_{T^\pm,1} \longrightarrow E^*$ sends $H^1(T^1, \mathbf{X}_T(t))$ to $k \cdot \beta_t^0$ (with notation as in (56)). Since furthermore $H^1(T^1,\mathbf{X}_T(t)) = t \cdot H^1(T^1, \mathbf{X}_T(1))$, assuming by contradiction that the homomorphism $E^*_{T^\pm,1} \longrightarrow E^*$ can be extended to a homomorphism of graded k-algebras $E^*_{T^\pm,0} \longrightarrow E^*$, we see that there exists $x \in E^1$ such that

$$\tau_t \cdot x = \beta_t^0.$$

To simplify the computations, let us choose $\lambda \in \widehat{T^0/T^1}$ with $\lambda \neq 1, \underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}$ (there exists such λ since $p \geqslant 5$) and we consider the equation

$$e_\lambda \tau_t \cdot x = e_\lambda \beta_t^0. \tag{153}$$

Looking at the explicit formulas (63) and (66) we see that for all $w \in \widetilde{W}$ (of length $\geqslant 1$ in the last line) we have:

$$\begin{aligned}
e_\lambda \tau_t \cdot \beta_w^- &\in \mathrm{span}_k \left\{ \beta_v^-, \beta_v^+ \;\middle|\; v \in \widetilde{W} \right\}, \\
e_\lambda \tau_t \cdot \beta_w^+ &\in \mathrm{span}_k \left\{ \beta_v^-, \beta_v^+ \;\middle|\; v \in \widetilde{W} \right\}, \\
e_\lambda \tau_t \cdot \beta_w^0 &\in \begin{cases} e_\lambda \beta_{tw}^0 & \text{if } \ell(tw) = \ell(t) + \ell(w), \\ 0 & \text{if } \ell(tw) < \ell(t) + \ell(w). \end{cases}
\end{aligned}$$

Therefore,

$$e_\lambda \tau_t \cdot x \in \mathrm{span}_k \left\{ \beta_v^-, \beta_v^+ \;\middle|\; v \in \widetilde{W} \right\} \oplus \mathrm{span}_k \left\{ \beta_v^0 \;\middle|\; v \in \widetilde{W} \text{ with } \ell(v) \geqslant \ell(t)+1 \right\},$$

contradicting (153). ∎

Remark 3.3.7. Let us work under our general assumptions without the restrictions on $\mathfrak{F}$ assumed in the proposition. We remark that $E^*_{T^\pm}$ is a localization of $E^*_{T^\pm,j}$ (note that $E^*_{T^\pm,j}$ is still defined and still a subalgebra of $E^*_{T^\pm}$).

Proof. The case of $E^*_{T^-}$ being completely analogous, let us work with $E^*_{T^+}$. We can choose $t_0^+ \in T^+/T^1$ such that $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_0^+) \geqslant 1$ for all $\alpha \in \Phi^+$. We claim that the inclusion

$$E^*_{T^+,j} \longrightarrow E^*_{T^+}$$

induces an isomorphism

$$\big(E^*_{T^+,j}\big)_{t_0^+} \longrightarrow E^*_{T^+},$$

where on the left hand side the notation $(\_)_{t_0^+}$ means localization at the powers of t_0^+: first of all let us note that the localization does make sense, because in a graded-commutative ring the left and right Ore conditions are always satisfied. Since t_0^+ is invertible in the bigger ring $E^*_{T^+}$, by the universal property of the localization, the inclusion map $E^*_{T^+,j} \longrightarrow E^*_{T^+}$ defines a map

$$\begin{aligned} \big(E^*_{T^+,j}\big)_{t_0^+} &\longrightarrow E^*_{T^+} \\ \frac{x}{(t_0^+)^n} &\longmapsto (t_0^+)^{-n} \cdot x = x \cdot (t_0^+)^{-n}. \end{aligned}$$

This map is injective, again since t_0^+ is invertible in $E^*_{T^+}$. It remains to show that it is also surjective, i.e., with reference to the "Bruhat decomposition" (148), that for all $i \in \mathbb{Z}_{\geqslant 0}$, for all $t \in T/T^1$ and for all $\beta \in H^i(I, \mathbf{X}_T(t))$ one has that β lies in the image of our map. But recall from (149) that for $n \in \mathbb{Z}$ we have

$$(t_0^+)^n \cdot \beta \in H^i\big(I, \mathbf{X}_T((t_0^+)^n t)\big).$$

As $(\mathrm{val}_{\mathfrak{F}} \circ \alpha)(t_0^+) \geqslant 1$ for all $\alpha \in \Phi^+$, it follows that $(t_0^+)^n t \in T_j^+$ for n big enough, thus finishing the proof of surjectivity of our map. ∎

Chapter 4

The Ext-algebra and the tensor algebra of E^1 for $\mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$

In this chapter we will work with the algebra E^* in the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$, and we will prove finite generation properties.

The starting point is that under the above assumptions the algebra E^* is generated by E^1, meaning more precisely that the multiplication map

$$\mathcal{M}\colon T^*_{E^0} E^1 \longrightarrow E^*$$

(where $T^*_{E^0} E^1$ is the tensor algebra generated by the E^0-bimodule E^1) is surjective (Lemma 4.1.1).

It then becomes interesting to compute the kernel of the above multiplication map, to ask if it is finitely generated as a bilateral ideal and to ask whether it is generated by its 2nd graded piece. The main result of this chapter (Theorem 4.8.1 and Remark 4.8.2) answers these questions: we show that $\ker(\mathcal{M})$ is indeed finitely generated as a bilateral ideal and we compute explicitly a finite system of generators: such system consists of elements supported only in degrees 2 and 3. In fact, we show that $\ker(\mathcal{M})$ is *not* generated by its 2nd graded piece.

Another important result in this chapter is an explicit presentation of E^* as a k-algebra: we obtain it in Proposition 4.10.4, showing that E^* is finitely presented as a k-algebra.

We also give a counterexample in the case $G = \mathrm{SL}_2(\mathbb{Q}_3)$: more precisely we show that for this group the multiplication map $\mathcal{M}$ is not surjective (see Section 4.2).

4.1 E^* is generated by E^1

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5) and furthermore we choose $\pi = p$.

In this section we will prove that the Ext-algebra E^* is generated by its first graded piece as a graded algebra. We start by setting up the following notation.

- Let us consider the tensor algebra $T^*_{E^0} E^1$ generated by the E^0-bimodule E^1, i.e., the graded k-algebra given by

$$\begin{aligned} T^0_{E^0}E^1 &\coloneqq E^0, \\ T^i_{E^0}E^1 &\coloneqq \underbrace{E^1 \otimes_{E^0} \cdots \otimes_{E^0} E^1}_{i \text{ times}} \qquad\qquad \text{for all } i \in \mathbb{Z}_{\geqslant 1}. \end{aligned}$$

We have the multiplication map (which is a homomorphism of graded k-algebras)

$$\begin{aligned} \mathcal{M}\colon \qquad T^*_{E^0}E^1 &\longrightarrow E^* \\ E^0 \ni x &\longmapsto x, \\ \beta_1 \otimes \cdots \otimes \beta_i &\longmapsto \beta_1 \cdots \beta_i. \end{aligned}$$

- Let us denote by $E^*_{\langle 1\rangle}$ the image of the above tensor algebra via the multiplication map. In other terms,

$$\begin{aligned} E^0_{\langle 1\rangle} &\coloneqq E^0, \\ E^i_{\langle 1\rangle} &\coloneqq \left\{\begin{matrix} \text{sums of } i\text{-fold products} \\ \text{of elements of } E^1 \end{matrix}\right\} \subseteq E^i \qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1}. \end{aligned}$$

  We want to prove that $E^* = E^*_{\langle 1\rangle}$. We will thus have to check that $E^3 \subseteq E^3_{\langle 1\rangle}$ and that $E^2 \subseteq E^2_{\langle 1\rangle}$.

- We now compute a certain formula for a threefold product that we will use repeatedly: let $\beta_1, \delta_1 \in H^1(I, \mathbf{X}(1))$, let $w \in \widetilde{W}$, and let $\gamma_w \in H^1(I, \mathbf{X}(w))$. Using the relation between (the opposite of the) Yoneda product and the cup product (Corollary 1.9.3), we obtain the following formula for the product $\beta_1 \cdot \gamma_w \cdot \delta_1$:

$$\begin{aligned} \beta_1 \cdot \gamma_w \cdot \delta_1 &= \big((\beta_1 \cdot \tau_w) \smile \gamma_w\big) \cdot \delta_1 \\ &= \big((\beta_1 \cdot \tau_w) \smile \gamma_w\big) \smile (\tau_w \cdot \delta_1) \\ &= (\beta_1 \cdot \tau_w) \smile \gamma_w \smile (\tau_w \cdot \delta_1). \end{aligned} \tag{154}$$

- We will use the notations $(c^-, c^0, c^+)_w$ and $(\alpha^-, \alpha^0, \alpha^+)_w$ to describe respectively elements of E^1 and of E^2 (see respectively Subsection 1.10.b and Subsection 1.10.e).

- We will also frquently use the formulas in Lemma 1.10.3.

Lemma 4.1.1. *One has $E^3 = E^3_{\langle 1\rangle}$, i.e., the multiplication map $\mathcal{M}_3\colon T^3_{E^0}E^1 \longrightarrow E^3$ is surjective.*

Proof. We split the proof into three parts.

- We first prove that $H^3(I, \mathbf{X}(s_0(s_1s_0)^i)) \subseteq E^3_{\langle 1\rangle}$ for all $i \in \mathbb{Z}_{\geqslant 0}$.

  Let us choose nonzero elements $c, e \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$ and a nonzero element $d \in \mathrm{Hom}_{\mathbb{F}_p}((1+\mathfrak{M})/(1+\mathfrak{M})^p, k)$. We have:

$$\begin{aligned} &(c,0,0)_1 \cdot (0,d,0)_{s_0(s_1s_0)^i} \cdot (e,0,0)_1 \\ &\quad = \big((c,0,0)_1 \cdot \tau_{s_0(s_1s_0)^i}\big) \smile (0,d,0)_{s_0(s_1s_0)^i} \smile \big(\tau_{s_0(s_1s_0)^i} \cdot (e,0,0)_1\big) \\ &\qquad\quad \text{by (154)} \\ &\quad = (c,0,0)_{s_0(s_1s_0)^i} \smile (0,d,0)_{s_0(s_1s_0)^i} \smile (0,0,-e)_{s_0(s_1s_0)^i} \\ &\qquad\quad \text{by (72) and (75).} \end{aligned} \tag{155}$$

Since we know that $H^*(I, \mathbf{X}(s_0(s_1s_0)^i))$ is an exterior algebra with respect to the cup product, we have that the above cup product generates $H^3(I, \mathbf{X}(s_0(s_1s_0)^i))$, and therefore we obtain the inclusion $H^3(I, \mathbf{X}(s_0(s_1s_0)^i)) \subseteq E^3_{\langle 1\rangle}$.

- We now prove that $H^3(I, \mathbf{X}(s_1(s_0s_1)^i)) \subseteq E^3_{\langle 1\rangle}$ for all $i \in \mathbb{Z}_{\geqslant 0}$.

  With notation as before, we have:

$$\begin{aligned}
&(0,0,c)_1 \cdot (0,d,0)_{s_1(s_0s_1)^i} \cdot (0,0,e)_1 \\
&\qquad = \big((0,0,c)_1 \cdot \tau_{s_1(s_0s_1)^i}\big) \smile (0,d,0)_{s_1(s_0s_1)^i} \smile \big(\tau_{s_1(s_0s_1)^i} \cdot (0,0,e)_1\big) \\
&\qquad\qquad \text{by (154)} \\
&\qquad = (0,0,c)_{s_1(s_0s_1)^i} \smile (0,d,0)_{s_1(s_0s_1)^i} \smile (-e,0,0)_{s_1(s_0s_1)^i} \\
&\qquad\qquad \text{by (72) and (77).}
\end{aligned} \tag{156}$$

- We finally use the previous two steps to prove that $H^3(I, \mathbf{X}(w)) \subseteq E^3_{\langle 1\rangle}$ for all $w \in \widetilde{W}$.

  We have already proved that $H^3(I, \mathbf{X}(w)) \subseteq E^3_{\langle 1\rangle}$ for $w \in \widetilde{W}$ of the form $s_0(s_1s_0)^i$ or $s_1(s_0s_1)^i$ (for some $i \in \mathbb{Z}_{\geqslant 0}$). The result for w of the form $\omega s_0(s_1s_0)^i$ or $\omega s_1(s_0s_1)^i$ (for some $\omega \in T^0/T^1$ and some $i \in \mathbb{Z}_{\geqslant 0}$) follows immediately, because multiplication on the left by τ_ω defines an isomorphism between $H^3(I, \mathbf{X}(v))$ and $H^3(I, \mathbf{X}(\omega v))$ for all $v \in \widetilde{W}$. Now it remains to show the result for w of even length: do this end, let us consider the k-basis $(\phi_v)_{v \in \widetilde{W}}$ of E^3 dual to the Iwahori–Matsumoto basis of E^0, let us consider $i \in \mathbb{Z}_{\geqslant 0}$ and $\omega \in T^0/T^1$. Applying the formula for the left action of E^0 on E^3 (see (89)), we find that

$$\tau_{s_0} \cdot \phi_{s_0^{-1}(s_1s_0)^i\omega} = \phi_{(s_1s_0)^i\omega} + e_1 \cdot \phi_{s_0^{-1}(s_1s_0)^i\omega}.$$

  Both the term on the left side and the second term on the right side lie in $E^3_{\langle 1\rangle}$, and hence also $\phi_{(s_1s_0)^i\omega}$ lies in $E^3_{\langle 1\rangle}$. This, together with the completely analogous proof for w of the form $(s_0s_1)^i\omega$, concludes the proof for w of even length. ■

Remark 4.1.2. For $i \in \mathbb{Z}_{\geqslant 1}$ it is possible to write elements of $H^3(I, \mathbf{X}((s_0s_1)^i))$ and $H^3(I, \mathbf{X}((s_1s_0)^i))$ as threefold products as we did for the case of even length. Although this is not needed for the above proof, we will need such computations later on:

$$\begin{aligned}
&(c,0,0)_1 \cdot (0,d,0)_{(s_0s_1)^i} \cdot (0,0,e)_1 \\
&\qquad = \big((c,0,0)_1 \cdot \tau_{(s_0s_1)^i}\big) \smile (0,d,0)_{(s_0s_1)^i} \smile \big(\tau_{(s_0s_1)^i} \cdot (0,0,e)_1\big) \\
&\qquad\qquad \text{by (154)} \\
&\qquad = (c,0,0)_{(s_0s_1)^i} \smile (0,d,0)_{(s_0s_1)^i} \smile (0,0,e)_{(s_0s_1)^i} \\
&\qquad\qquad \text{by (72) and (76),} \\
&(0,0,c)_1 \cdot (0,d,0)_{(s_1s_0)^i} \cdot (e,0,0)_1 \\
&\qquad = \big((0,0,c)_1 \cdot \tau_{(s_1s_0)^i}\big) \smile (0,d,0)_{(s_1s_0)^i} \smile \big(\tau_{(s_1s_0)^i} \cdot (e,0,0)_1\big) \\
&\qquad\qquad \text{by (154)} \\
&\qquad = (0,0,c)_{(s_1s_0)^i} \smile (0,d,0)_{(s_1s_0)^i} \smile (e,0,0)_{(s_1s_0)^i} \\
&\qquad\qquad \text{by (73) and (74).}
\end{aligned} \tag{157}$$

Lemma 4.1.3. *One has $E^2 = E^2_{\langle 1\rangle}$, i.e., the multiplication map $\mathcal{M}_2 \colon T^2_{E^0}E^1 \longrightarrow E^2$ is surjective.*

Proof. We split the proof into three parts.

- We first prove that $H^2(I, \mathbf{X}((s_1s_0)^i)) \subseteq E^2_{\langle 1\rangle}$ for $i \in \mathbb{Z}_{\geqslant 1}$.

  Let $\beta_{(s_1s_0)^i}, \gamma_{(s_1s_0)^i} \in H^1(I, \mathbf{X}((s_1s_0)^i))$, let $c^-, c^+ \in \operatorname{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k)$ and let $c^0 \in \operatorname{Hom}_{\mathbb{F}_p}((1+\mathfrak{M})/(1+\mathfrak{M})^p, k)$. We compute:

$$\begin{aligned} \beta_{(s_1s_0)^i} \cdot (c^-,0,0)_1 &= \beta_{(s_1s_0)^i} \smile (\tau_{(s_1s_0)^i} \cdot (c^-,0,0)_1) \\ &= \beta_{(s_1s_0)^i} \smile (c^-,0,0)_{(s_1s_0)^i} && \text{by (74)}, \\ (0,0,c^+)_1 \cdot \gamma_{(s_1s_0)^i} &= ((0,0,c^+)_1 \cdot \tau_{(s_1s_0)^i}) \smile \gamma_{(s_1s_0)^i} \\ &= (0,0,c^+)_{(s_1s_0)^i} \smile \gamma_{(s_1s_0)^i} && \text{by (73)}. \end{aligned} \tag{158}$$

  By making suitable choices of $\beta_{(s_1s_0)^i}$ and of $\gamma_{(s_1s_0)^i}$, we thus get that the following elements lie in $E^2_{\langle 1\rangle}$:

$$\begin{gathered} (0,c^0,0)_{(s_1s_0)^i} \smile (c^-,0,0)_{(s_1s_0)^i}, \\ (0,0,c^+)_{(s_1s_0)^i} \smile (c^-,0,0)_{(s_1s_0)^i}, \\ (0,0,c^+)_{(s_1s_0)^i} \smile (0,c^0,0)_{(s_1s_0)^i}. \end{gathered}$$

  As $i \geqslant 1$, we know that $H^*(I, \mathbf{X}((s_1s_0)^i))$ is an exterior algebra with respect to the cup product: therefore, choosing nonzero elements c^-, c^0 and c^+, we get that the above three cup products generate $H^2(I, \mathbf{X}((s_1s_0)^i))$, and we thus get that $H^2(I, \mathbf{X}((s_1s_0)^i)) \subseteq E^2_{\langle 1\rangle}$.

- We now prove that $H^2(I, \mathbf{X}(w) \subseteq E^2_{\langle 1\rangle}$ for $w \in \widetilde{W}$ of the form $w = (s_0s_1)^i$ for $i \in \mathbb{Z}_{\geqslant 1}$ or of the form $w = s_0(s_1s_0)^i$ for $i \in \mathbb{Z}_{\geqslant 0}$ or of the form $s_1(s_0s_1)^i$ for $i \in \mathbb{Z}_{\geqslant 0}$.

  The proof is completely analogous to the above. The relevant equalities are the following:

  - ⋆ If $w = (s_0s_1)^i$ for $i \in \mathbb{Z}_{\geqslant 1}$:

$$\begin{aligned} \beta_{(s_0s_1)^i} \cdot (0,0,c^+)_1 &= \beta_{(s_0s_1)^i} \smile (0,0,c^+)_{(s_0s_1)^i} && \text{by (76)}, \\ (c^-,0,0)_1 \cdot \gamma_{(s_0s_1)^i} &= (c^-,0,0)_{(s_0s_1)^i} \smile \gamma_{(s_0s_1)^i} && \text{by (72)}. \end{aligned} \tag{159}$$

  - ⋆ If $w = s_0(s_1s_0)^i$ for $i \in \mathbb{Z}_{\geqslant 0}$:

$$\begin{aligned} \beta_{s_0(s_1s_0)^i} \cdot (c^-,0,0)_1 &= \beta_{s_0(s_1s_0)^i} \smile (0,0,-c^-)_{s_0(s_1s_0)^i} && \text{by (75)}, \\ (c^-,0,0)_1 \cdot \gamma_{s_0(s_1s_0)^i} &= (c^-,0,0)_{s_0(s_1s_0)^i} \smile \gamma_{s_0(s_1s_0)^i} && \text{by (72)}. \end{aligned} \tag{160}$$

  - ⋆ If $w = s_1(s_0s_1)^i$ for $i \in \mathbb{Z}_{\geqslant 0}$:

$$\begin{aligned} \beta_{s_1(s_0s_1)^i} \cdot (0,0,c^+)_1 &= \beta_{s_1(s_0s_1)^i} \smile (-c^+,0,0)_{s_1(s_0s_1)^i} && \text{by (77)}, \\ (0,0,c^+)_1 \cdot \gamma_{s_1(s_0s_1)^i} &= (0,0,c^+)_{s_1(s_0s_1)^i} \smile \gamma_{s_1(s_0s_1)^i} && \text{by (73)}. \end{aligned} \tag{161}$$

- We finally use the previous two steps to prove that $H^2(I, \mathbf{X}(w)) \subseteq E^2_{\langle 1\rangle}$ for all $w \in \widetilde{W}$.

  Multiplication on the left by τ_ω defines an isomorphism between $H^2(I, \mathbf{X}(v))$ and $H^2(I, \mathbf{X}(\omega v))$ for all $v \in \widetilde{W}$. Therefore, from the four special cases that we have already treated, it follows that $H^2(I, \mathbf{X}(w)) \subseteq E^2_{\langle 1\rangle}$ for all $w \in \widetilde{W}$ of strictly positive length. It therefore remains to treat the case of length 0. Let $\omega \in T^0/T^1$ and let $\alpha^-, \alpha^+ \in \mathfrak{O}/\mathfrak{M} \otimes_{\mathbb{F}_p} k$; the formulas for the left action of E^0 on E^2 tell us the following:

$$\begin{aligned}
\tau_{s_0} \cdot (0,0,\alpha^+)_{s_0^{-1}\omega} + (\alpha^+,0,0)_\omega &\in \bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v)=1}} H^2(I, \mathbf{X}(v)), \\
\tau_{s_1} \cdot (\alpha^-,0,0)_{s_1^{-1}\omega} + (0,0,\alpha^-)_\omega &\in \bigoplus_{\substack{v \in \widetilde{W} \\ \text{s.t. } \ell(v)=1}} H^2(I, \mathbf{X}(v)).
\end{aligned} \tag{162}$$

These equations, together with the fact that we have already proved the result for w of strictly positive length, prove that $H^2(I, \mathbf{X}(\omega)) \subseteq E^2_{\langle 1 \rangle}$. ∎

Corollary 4.1.4. *One has $E^* = E^*_{\langle 1 \rangle}$, i.e., the multiplication map*

$$\mathcal{M} \colon T^*_{E^0} E^1 \longrightarrow E^*$$

is surjective.

Proof. This follows from the last two lemmas. ∎

4.2 Counterexample: E^* is not generated by E^1 in the case $G = \mathrm{SL}_2(\mathbb{Q}_3)$

In this section we will work with $\mathbf{G} = \mathrm{SL}_2(\mathbb{Q}_3)$ and we will show that, contrary to what happens for $\mathrm{SL}_2(\mathbb{Q}_p)$ for $p \neq 2, 3$, the Ext-algebra E^* is not generated by its 1^{st} graded piece as a graded algebra.

We start with a very general lemma, surely well-known. The proof of the first part was suggested to the author by Claudius Heyer.

Lemma 4.2.1. *Let K be a pro-p group. One has the following facts.*

(i) If K is p-adic analytic, then $H^n(K,k)$ is a finite-dimensional k-vector space for all $n \in \mathbb{Z}_{\geqslant 0}$;

(ii) If K has torsion, then $H^n(K,k)$ is nonzero for all $n \in \mathbb{Z}_{\geqslant 0}$.

Proof. Let us prove the two statements.

(i) Without loss of generality, using (31), we may assume that $k = \mathbb{F}_p$. We first recall that since K is a p-adic analytic pro-p group, it has an open normal subgroup K' that is a uniform pro-p group (see [DDSMS03, 8.34 Corollary]). In particular, each cohomology group $H^i(K', \mathbb{F}_p)$ is a finite-dimensional $\mathbb{F}_p$-vector space (see Theorem 1.8.1).

Let us look at the Hochschild–Serre spectral sequence (see [NSW13, (2.4.1) Theorem]):
$$H^i\left(K/K', H^j(K', \mathbb{F}_p)\right) \Longrightarrow H^{i+j}(K, \mathbb{F}_p).$$
Since for all i and j both K/K' and $H^j(K', \mathbb{F}_p)$ have finite cardinality, also $H^i\left(K/K', H^j(K', \mathbb{F}_p)\right)$ has finite cardinality as well. So we have a convergent first quadrant spectral sequence whose entries (of the second page and hence of all pages) are finite-dimensional $\mathbb{F}_p$-vector spaces. Hence also $H^{i+j}(K, \mathbb{F}_p)$ is a finite-dimensional $\mathbb{F}_p$-vector space for all i and j.

(ii) The result being trivial for $n = 0$, we can work with $n \geqslant 1$. Let L be a pro-p group. One has that the following conditions are equivalent:

- $\star$ L has cohomological dimension (i.e., p-th cohomological dimension) smaller or equal than $n-1$,
- $\star$ $H^n(L, \mathbb{F}_p)$ is nonzero,
- $\star$ $H^n(L', \mathbb{F}_p)$ is nonzero for all closed subgroups L' of L.

(see [Ser02, Chapter I, Proposition 21 and Proposition 21']). In our case we can choose a (necessarily closed) cyclic p-group K' inside K. It satisfies $H^n(K', \mathbb{F}_p) = \mathbb{F}_p$ (this is computed for example in [NSW13, (1.7.1) Proposition]), and so $H^n(K, \mathbb{F}_p)$ must be nonzero by the above equivalence, and hence also $H^n(K, k)$ (using (31)). ∎

Example 4.2.2. Let $G = \mathrm{SL}_2(\mathbb{Q}_3)$ (with the usual choices as in Section 1.5). Then the Ext-algebra E^* is not generated by E^1.

Proof. We divide the proofs into some steps.

- We remark that if $\ell(w) \geqslant 1$, then I_w is torsion-free.

  Let us see which matrices in I have order 3. Since $\mathbb{Q}_3$ does not contain non-trivial 3-roots, if a matrix in $\mathrm{SL}_2(\mathbb{Q}_3)$ has order $p = 3$, then the characteristic polynomial is divisible by (i.e., is equal to) the 3-rd cyclotomic polynomial. So we are looking for matrices of the following form:

$$\begin{pmatrix} 1+3a & b \\ 3c & 1+3d \end{pmatrix},$$

  with

$$\begin{aligned} 1 &= \det \begin{pmatrix} 1+3a & b \\ 3c & 1+3d \end{pmatrix} = 1 + 3a + 3d + 3^2ad - 3bc, \\ -1 &= \mathrm{tr} \begin{pmatrix} 1+3a & b \\ 3c & 1+3d \end{pmatrix} = 2 + 3a + 3d. \end{aligned}$$

  Replacing $1+3a+3d$ in the first equation by its value given by the second equation, we get in particular that

$$3 = 3^2ad - 3bc.$$

  From this equation we see that $bc \notin \mathfrak{M}$ and so, recalling from Lemma 1.10.1 that I_w is either equal to $\left(\begin{smallmatrix} 1+\mathfrak{M} & \mathfrak{O} \\ \mathfrak{M}^{\ell(w)+1} & 1+\mathfrak{M} \end{smallmatrix}\right)$ or to $\left(\begin{smallmatrix} 1+\mathfrak{M} & \mathfrak{M}^{\ell(w)} \\ \mathfrak{M} & 1+\mathfrak{M} \end{smallmatrix}\right)$ (where matrices are understood to have determinant equal to 1), we see that I_w cannot contain elements of order 3, and hence that it cannot contain torsion elements.

- Now, let again $w \in \widetilde{W}$ with $\ell(w) \geqslant 1$. Since I_w is an open subgroup of the 3-dimensional analytic pro-p group G, it is a 3-dimensional analytic pro-p group as well. As we have furthermore proved that I_w is torsion-free, Theorem 1.8.2 yields that I_w is a Poincaré group of dimension 3. In particular, $H^m(I_w, k) = 0$ for all $m \in \mathbb{Z}_{\geqslant 4}$. Therefore, taking into account that the only elements of length zero are 1 and c_{-1} (which was defined in (21)), we get

$$E^m = H^m(I, \mathbf{X}(1)) \oplus H^m(I, \mathbf{X}(c_{-1})) \qquad \text{for all } m \in \mathbb{Z}_{\geqslant 4}.$$

- Now, let us assume by contradiction that E^* is generated by E^1.

  For the moment let $x \in E^n$ with $n \in \mathbb{Z}_{\geqslant 1}$. We can write it as $x = \sum_j \beta_{j1} \cdots \beta_{jn}$ for suitable elements $\beta_{ji} \in E^1$. Let us assume that $n = n_1 n_2$ with $n_1 \in \mathbb{Z}_{\geqslant 1}$ and $n_2 \in \mathbb{Z}_{\geqslant 1}$. We see that x can be written as a sum of products of elements in E^{n_1}. Let us further assume that $x \in H^n(I, \mathbf{X}(1))$ and that $n_1 \geqslant 4$; then using the decomposition $E^{n_1} = H^{n_1}(I, \mathbf{X}(1)) \oplus H^{n_1}(I, \mathbf{X}(c_{-1}))$ we see that x can be written as $x = \sum_{j'} \gamma_{j'1} \cdots \gamma_{j'n_2}$ for suitable elements $\gamma_{j'i'}$ each of them either lying in $H^{n_1}(I, \mathbf{X}(1))$ or lying in $H^{n_1}(I, \mathbf{X}(c_{-1}))$. But putting together the fact that $H^m(I, \mathbf{X}(c_{-1})) = \tau_{c_{-1}} \cdot H^m(I, \mathbf{X}(1))$ for all $m \in \mathbb{Z}_{\geqslant 0}$, the fact that $\tau_{c_{-1}}$ is central and the assumption that $x \in H^n(I, \mathbf{X}(1))$, we see that without loss of generality we may assume that each of the $\gamma_{j'i'}$ lies in $H^{n_1}(I, \mathbf{X}(1))$. This shows that the image of the natural map

  $$T_k^\bullet\big(H^{n_1}(I, \mathbf{X}(1))\big) \longrightarrow E^*$$

  contains $H^{n_1 n_2}(I, \mathbf{X}(1))$ for all $n_1 \in \mathbb{Z}_{\geqslant 4}$ and $n_2 \in \mathbb{Z}_{\geqslant 1}$.

  Since the image of the above map is contained in $H^*(I, \mathbf{X}(1)) \cong H^*(I, k)$, and since the product is the cup product (see Corollary 1.9.3), it follows that, changing notation, we can rephrase this by saying that the image of the natural homomorphism of k-algebras

  $$T_k^\bullet\big(H^{n_1}(I, k)\big) \longrightarrow H^*(I, k)$$

  contains $H^{n_1 n_2}(I, k)$ for all $n_1 \in \mathbb{Z}_{\geqslant 4}$ and $n_2 \in \mathbb{Z}_{\geqslant 1}$. Now, we fix $n_1 := 5$ (any other odd integer bigger then 4 would work). Then for all $\gamma \in H^5(I, \mathbf{X}(1))$ we have that $\gamma \smile \gamma = 0$. But then the above homomorphism of k-algebras factors through a homomorphism of k-algebras

  $$\textstyle\bigwedge_k^\bullet \big(H^5(I, k)\big) \longrightarrow H^*(I, k),$$

  which, of course, has again the property that its image contains $H^{5n_2}(I, k)$ for all $n_2 \in \mathbb{Z}_{\geqslant 1}$. But $H^5(I, k)$ is a finite-dimensional k-vector space (Lemma 4.2.1 part (i)) and so $\bigwedge_k^\bullet \big(H^5(I, k)\big)$ is a finite-dimensional k-vector space as well, whereas $\bigoplus_{n_2 \in \mathbb{Z}_{\geqslant 1}} H^{5n_2}(I, k)$ is an infinite-dimensional k-vector space: indeed I has torsion (for example, one can consider the matrix $\left(\begin{smallmatrix} 1 & -1 \\ 3 & 1-3 \end{smallmatrix}\right)$), and so each summand is nonzero (Lemma 4.2.1 part (ii)). This contradicts the claim about the image of the above map. ■

4.3 The tensor algebra

Assumptions. In this section we put ourselves in the general assumptions of Section 1.1, without any restriction on $\mathbf{G}$ and $\mathfrak{F}$. We will assume that $\mathbf{G} = \mathrm{SL}_2$ only when talking about the automorphism Γ_ϖ.

We work with the tensor algebra

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

generated by the E^0-bimodule E^1. We have the multiplication map (which is a homomorphism of graded k-algebras)

$$\begin{aligned} \mathcal{M}\colon \qquad T_{E^0}^* E^1 &\longrightarrow E^* \\ E^0 \ni x &\longmapsto x, \\ \beta_1 \otimes \cdots \otimes \beta_i &\longmapsto \beta_1 \cdots \beta_i. \end{aligned}$$

In this section, we are going to give definitions of an involutive anti-automorphism $\mathfrak{J}$ on $T^*_{E^0}E^1$ (compatible with the involutive anti-automorphism $\mathfrak{J}$ on E^*) and, if $\mathbf{G} = \mathrm{SL}_2$, of an involutive automorphism Γ_ϖ on $T^*_{E^0}E^1$ (compatible with the involutive automorphism Γ_ϖ on E^*). We begin with the second one.

If $\mathbf{G} = \mathrm{SL}_2$ (with the usual choices as in Section 1.5), it is easy to see that we have an involutive automorphism induced by $\Gamma_\varpi \colon E^* \longrightarrow E^*$, which we will denote again by Γ_ϖ, defined as follows:

$$\begin{aligned} \Gamma_\varpi\colon \qquad T^*_{E^0}E^1 &\longrightarrow T^*_{E^0}E^1 \\ E^0 \ni x &\longmapsto \Gamma_\varpi(x), \\ \beta_1 \otimes \cdots \otimes \beta_i &\longmapsto \Gamma_\varpi(\beta_1) \otimes \cdots \otimes \Gamma_\varpi(\beta_i). \end{aligned}$$

It is immediate to check that this definition is compatible with the multiplication map, in the sense that the following diagram is commutative:

$$\begin{tikzcd} T^*_{E^0}E^1 \arrow[r, "\mathcal{M}"] \arrow[d, "\Gamma_\varpi"'] & E^* \arrow[d, "\Gamma_\varpi"] \\ T^*_{E^0}E^1 \arrow[r, "\mathcal{M}"'] & E^*. \end{tikzcd} \tag{163}$$

Let us go back to the case of a general $\mathbf{G}$: we have the following involutive anti-automorphism induced by $\mathfrak{J}\colon E^* \longrightarrow E^*$, which we will denote again by $\mathfrak{J}$:

$$\begin{aligned} \mathfrak{J}\colon \qquad T^*_{E^0}E^1 &\longrightarrow T^*_{E^0}E^1 \\ E^0 \ni x &\longmapsto \mathfrak{J}(x), \\ \beta_1 \otimes \cdots \otimes \beta_i &\longmapsto (-1)^{\lfloor i/2 \rfloor}\mathfrak{J}(\beta_i) \otimes \cdots \otimes \mathfrak{J}(\beta_1). \end{aligned}$$

Proof that $\mathfrak{J}$ is an involutive anti-automorphism on $T^*_{E^0}E^1$. The map $\mathfrak{J}$ is an involutive automorphism of graded k-vector spaces, and we have to show that it is anti-commutative, i.e., that it satisfies the following equation, for $i, j \in \mathbb{Z}_{\geqslant 0}$, for $\beta \in T^i_{E^0}E^1$ and for $\gamma \in T^j_{E^0}E^1$:

$$\text{(Claim)} \qquad \mathfrak{J}(\beta \cdot \gamma) = (-1)^{ij}\mathfrak{J}(\gamma) \cdot \mathfrak{J}(\beta).$$

We first check what happens if either i or j are equal to 0. The equation is satisfied if both i and j are equal to 0, because then we are simply working with the anti-involution on E^0. On the other side, in the case where only one among i and j is equal to 0, the claim basically follows from the analogous property for the anti-involution defined on E^0 and E^1.

Now we shall treat the case $i, j \geqslant 1$. For this, without loss of generality we may assume that $\beta = \beta_1 \otimes \cdots \otimes \beta_i$ for some $\beta_1, \ldots, \beta_i \in E^1$ and similarly $\gamma = \gamma_1 \otimes \cdots \otimes \gamma_j$. We can now compute

$$\begin{aligned} \mathfrak{J}(\beta \cdot \gamma) &= \mathfrak{J}(\beta_1 \otimes \cdots \otimes \beta_i \otimes \gamma_1 \otimes \cdots \otimes \gamma_j) \\ &= (-1)^{\lfloor (i+j)/2 \rfloor}\mathfrak{J}(\gamma_j) \otimes \cdots \otimes \mathfrak{J}(\gamma_1) \otimes \mathfrak{J}(\beta_i) \otimes \cdots \otimes \mathfrak{J}(\beta_1) \\ &= (-1)^{\lfloor (i+j)/2 \rfloor - \lfloor i/2 \rfloor - \lfloor j/2 \rfloor}\mathfrak{J}(\gamma) \otimes \mathfrak{J}(\beta). \end{aligned}$$

To check our claim it remains to prove that the above coefficient is equal to $(-1)^{ij}$. We do this by distinguishing some cases:

- if both i and j are even:

$$(-1)^{\lfloor (i+j)/2 \rfloor - \lfloor i/2 \rfloor - \lfloor j/2 \rfloor} = (-1)^{(i+j)/2 - i/2 - j/2} = 1 = (-1)^{ij};$$

- if i is even and j is odd:

$$(-1)^{\lfloor (i+j)/2 \rfloor - \lfloor i/2 \rfloor - \lfloor j/2 \rfloor} = (-1)^{(i+j-1)/2 - i/2 - (j-1)/2} = 1 = (-1)^{ij};$$

- if i is odd and j is even, then the result follows from the above, exchanging i and j;

- if both i and j are odd:

$$(-1)^{\lfloor (i+j)/2 \rfloor - \lfloor i/2 \rfloor - \lfloor j/2 \rfloor} = (-1)^{(i+j)/2 - (i-1)/2 - (j-1)/2} = -1 = (-1)^{ij}.$$

This concludes the proof that the equality $\mathcal{J}(\beta \cdot \gamma) = (-1)^{ij} \mathcal{J}(\gamma) \cdot \mathcal{J}(\beta)$ holds. ■

Furthermore, $\mathcal{J}$ is compatible with the multiplication map, in the sense that the following diagram is commutative:

$$\begin{tikzcd} T^*_{E^0} E^1 \arrow[r, "\mathcal{M}"] \arrow[d, "\mathcal{J}"'] & E^* \arrow[d, "\mathcal{J}"] \\ T^*_{E^0} E^1 \arrow[r, "\mathcal{M}"'] & E^*. \end{tikzcd} \tag{164}$$

Proof of the fact that the above diagram is commutative. In degree 0 and 1 there is nothing to check, and so by induction we might assume that the claim is true in degree $i \geqslant 1$ and check that it is true in degree $i+1$. We may work with simple tensors, i.e., let us consider $\beta_1, \ldots, \beta_{i+1} \in E^1$ and let us compute

$$\begin{aligned} \mathcal{M}\big(\mathcal{J}(\beta_1 \otimes \cdots \otimes \beta_{i+1})\big) &= \mathcal{M}\big((-1)^{\lfloor (i+1)/2 \rfloor} \mathcal{J}(\beta_{i+1}) \otimes \cdots \otimes \mathcal{J}(\beta_1)\big) \\ &= (-1)^{\lfloor (i+1)/2 \rfloor} \mathcal{J}(\beta_{i+1}) \cdots \mathcal{J}(\beta_1) \\ &= (-1)^{\lfloor (i+1)/2 \rfloor} (-1)^{-\lfloor i/2 \rfloor} \mathcal{J}(\beta_{i+1}) \cdot \mathcal{M}\big(\mathcal{J}(\beta_1 \otimes \cdots \otimes \beta_i)\big) \\ &= (-1)^{\lfloor (i+1)/2 \rfloor} (-1)^{-\lfloor i/2 \rfloor} \mathcal{J}(\beta_{i+1}) \cdot \mathcal{J}\big(\mathcal{M}(\beta_1 \otimes \cdots \otimes \beta_i)\big) \\ &= (-1)^{\lfloor (i+1)/2 \rfloor} (-1)^{-\lfloor i/2 \rfloor} (-1)^i \mathcal{J}\big(\mathcal{M}(\beta_1 \otimes \cdots \otimes \beta_i) \cdot \beta_{i+1}\big) \\ &= (-1)^{\lfloor (i+1)/2 \rfloor} (-1)^{-\lfloor i/2 \rfloor} (-1)^i \mathcal{J}\big(\mathcal{M}(\beta_1 \otimes \cdots \otimes \beta_{i+1})\big). \end{aligned}$$

Distinguishing on the parity of i, one easily see that the coefficient in the last line is always 1. ■

4.4 An "algorithm" for the computation of kernels

In this section we will explain the strategy to compute the kernel of the multiplication map

$$\mathcal{M} \colon T^*_{E^0} E^1 \longrightarrow E^*.$$

We work 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 $\mathcal{F} \colon M \longrightarrow N$ be a surjective homomorphism of A-bimodules (in our case $\mathcal{F} = \mathcal{M}$). To compute the kernel of $\mathcal{F}$ 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 $\mathcal{F}$ as a map of k-vector spaces:

$$\begin{tikzcd} M \arrow[r, two heads, "\mathcal{F}"] & N \arrow[l, dashed, bend left, "\mathcal{R}"] \end{tikzcd}$$

(equivalently, for each $l \in \mathbf{L}$ we fix an element $\mathcal{R}(n_l)$ in the non-empty set $\mathcal{F}^{-1}(n_l)$). Clearly, for all $i \in \mathbf{I}$ and all $l \in \mathbf{L}$, one has

$$\begin{aligned} \mathcal{R}(a_i n_l) - a_i\mathcal{R}(n_l) &\in \ker\mathcal{F}, \\ \mathcal{R}(n_l a_i) - \mathcal{R}(n_l)a_i &\in \ker\mathcal{F}. \end{aligned}$$

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 $l \in \mathbf{L}$. We have that $M' \subseteq \ker\mathcal{F}$ and that the following maps are well defined:

$$\begin{tikzcd} M/M' \arrow[r, two heads, "\overline{\mathcal{F}}", "\overline{m}\mapsto\mathcal{F}(m)"'] & N. \arrow[l, dashed, bend left, "\overline{\mathcal{R}}", "\overline{\mathcal{R}(n)}\leftarrow\!\shortmid n"'] \end{tikzcd}$$

Of course $\overline{\mathcal{R}}$ is a splitting of $\overline{\mathcal{F}}$, but this time it is a splitting as a map of A-bimodules, thanks to the definition of M'. It follows that

$$(\ker\mathcal{F})/M' = \ker\overline{\mathcal{F}} = \left\langle \overline{m_j - (\mathcal{R}\circ\phi)(m_j)} \;\middle|\; j \in \mathbf{J} \right\rangle,$$

where the pointed braces denote the generated sub-A-bimodule. We conclude that $\ker\mathcal{F}$ is the sub-A-bimodule of M generated by the following elements:

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

4.5 The kernel in degree 2

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. With respect to Section 1.10 and Chapter 2, the families of elements $(\beta_w^-)_w$, $(\beta_w^0)_w$, $(\beta_w^+)_w$, $(\alpha_w^-)_w$, $(\alpha_w^0)_w$, $(\alpha_w^+)_w$, and $(\phi_w)_w$ will be chosen in a more restrictive way (see Subsection 4.5.a for the details).

In this section we will compute the kernel of the degree 2 multiplication map

$$\mathcal{M}_2 \colon T^2_{E^0}(E^1) \longrightarrow E^2.$$

The idea is to roughly follow the "algorithm" outlined in the previous section.

4.5.a Preliminaries

Following [OS21, §4.2.3], we want to fix k-bases for E^1 and E^2 "in a compatible way". To this end, recall that in (56) we considered an element $\mathbf{c} \in \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{O}/\mathfrak{M}, k) \smallsetminus \{0\}$, and for all $w \in \widetilde{W}$ we defined the following k-basis of $H^1(I, \mathbf{X}(w))$:

$$\begin{aligned} \beta_w^- &\coloneqq (\mathbf{c}, 0, 0)_w, \\ \beta_w^+ &\coloneqq (0, 0, \mathbf{c})_w, \\ \beta_w^0 &\coloneqq (0, \mathbf{c}\iota, 0)_w \qquad \text{if } \ell(w) \geqslant 1, \end{aligned}$$

where ι was the isomorphism induced by the logarithm defined in (55). On the other side, in (80) we considered an element $\boldsymbol{\alpha} \in \left(\mathfrak{O}/\mathfrak{M}\right) \smallsetminus \{0\}$, and for all $w \in \widetilde{W}$ we defined the following k-basis of $H^2(I, \mathbf{X}(w))$:

$$\begin{aligned} \alpha_w^- &\coloneqq (\boldsymbol{\alpha}, 0, 0)_w, \\ \alpha_w^+ &\coloneqq (0, 0, \boldsymbol{\alpha})_w, \\ \alpha_w^0 &\coloneqq (0, \iota^{-1}(\boldsymbol{\alpha}), 0)_w \qquad \text{if } \ell(w) \geqslant 1. \end{aligned}$$

We now choose $\mathbf{c}$ and $\boldsymbol{\alpha}$ satisfying the following constraint:

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

Recall that we chose an isomorphism $\eta \colon H^3(I, k) \longrightarrow k$ to define the duality (Theorem 1.9.8). In [OS21, Lemma 4.5], it is shown that there exists a (necessarily unique) choice of η such that the following property holds:

$$\beta_w^- \smile \beta_w^0 \smile \beta_w^+ = \phi_w \qquad \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geqslant 1. \tag{165}$$

We will always work with these fixed choices of $\mathbf{c}$, $\boldsymbol{\alpha}$ and η.

It is possible to show that the following relations hold (see [OS21, Lemma 5.3]):

$$\alpha_w^0 = \beta_w^+ \smile \beta_w^- \qquad \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geqslant 1, \tag{166}$$

$$\alpha_w^- = \beta_w^0 \smile \beta_w^+ \qquad \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geqslant 1, \tag{167}$$

$$\alpha_w^+ = \beta_w^- \smile \beta_w^0 \qquad \text{for all } w \in \widetilde{W} \text{ such that } \ell(w) \geqslant 1. \tag{168}$$

4.5.b Generators of $T^2_{E_0} E^1$ as an E^0-bimodule

In this subsection we will compute a (quite simple) set of generators of $T^2_{E_0} E^1$ as an E^0-bimodule. Recall that this is useful in order to implement the "algorithm" of Section 4.4.

We recall that the following are generators of E^1 as an E^0-bimodule (see Lemma 1.10.3):

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

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):

$$\beta_1^- \otimes \beta_w^\sigma, \quad \beta_1^+ \otimes \beta_w^\sigma, \quad \beta_{s_0}^0 \otimes \beta_w^\sigma, \quad \beta_{s_1}^0 \otimes \beta_w^\sigma \qquad \begin{array}{l} \text{for } w \in \widetilde{W} \text{ and } \sigma \in \{-, 0, +\} \\ \text{(with } \ell(w) \geqslant 1 \text{ in the case } \sigma = 0). \end{array} \tag{169}$$

Lemma 4.5.1. *The following elements generate $E^1 \otimes_{E^0} E^1$ as an E^0-bimodule:*

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

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

Proof. We start from the generators in (169).

We recall from (65) that

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

Combining these two facts (and the behaviour of multiplication by τ_ω for $\omega \in T^0/T^1$, see (60)), we get that the following elements generate $E^1 \otimes_{E^0} E^1$ as an E^0-bimodule:

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

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 1.10.3, we can rewrite the last four lines as:

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

From (65), 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 $\gamma \in \{\beta^0_{s_0}, \beta^0_{s_1}\}$.

Let us start with the following case:

$$\begin{aligned}(\beta^0_{s_0} \cdot \tau_{(s_1 s_0)^i}) \otimes \beta^-_1 &= \beta^0_{s_0(s_1 s_0)^i} \otimes \beta^-_1\\ &= \tau_{(s_0 s_1)^i} \beta^0_{s_0} \otimes \beta^-_1,\end{aligned}$$

where we used the formulas (63) and (65). We see that the element $\beta^0_{s_0} \otimes \beta^-_1$ is a generator already appearing in the first lines, and so the generator $(\beta^0_{s_0} \cdot \tau_{(s_1 s_0)^i}) \otimes \beta^-_1$ is superfluous. The other three cases where lengths add up are similar.

Now it remains to consider the following elements, where we apply the formulas (67) and (68) and then proceed with the computations as usual:

$$\begin{aligned}(\beta^0_{s_1} \cdot \tau_{(s_1 s_0)^i}) \otimes \beta^-_1 &= \left(-e_1 \cdot \beta^0_{(s_1 s_0)^i} + e_{\underline{\mathrm{id}}} \cdot \beta^+_{(s_1 s_0)^i}\right) \otimes \beta^-_1\\ &= e_1 \cdot \tau_{(s_1 s_0)^{i-1} s_1} \cdot \beta^0_{s_0} \otimes \beta^-_1 + e_{\underline{\mathrm{id}}} \cdot \beta^+_1 \otimes \beta^-_{(s_1 s_0)^i},\\ (\beta^0_{s_1} \cdot \tau_{s_1(s_0 s_1)^i}) \otimes \beta^+_1 &= \left(-e_1 \cdot \beta^0_{s_1(s_0 s_1)^i} + e_{\underline{\mathrm{id}}} \cdot \beta^+_{s_1(s_0 s_1)^i}\right) \otimes \beta^+_1\\ &= -e_1 \cdot \tau_{(s_1 s_0)^i} \cdot \beta^0_{s_1} \otimes \beta^+_1 - e_{\underline{\mathrm{id}}} \cdot \beta^+_1 \otimes \beta^-_{s_1(s_0 s_1)^i},\\ (\beta^0_{s_0} \cdot \tau_{(s_0 s_1)^i}) \otimes \beta^+_1 &= \left(-e_1 \cdot \beta^0_{(s_0 s_1)^i} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_{(s_0 s_1)^i}\right) \otimes \beta^+_1\\ &= e_1 \cdot \tau_{(s_0 s_1)^{i-1} s_0} \cdot \beta^0_{s_1} \otimes \beta^+_1 - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^+_{(s_0 s_1)^i},\\ (\beta^0_{s_0} \cdot \tau_{s_0(s_1 s_0)^i}) \otimes \beta^-_1 &= \left(-e_1 \cdot \beta^0_{s_0(s_1 s_0)^i} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_{s_0(s_1 s_0)^i}\right) \otimes \beta^-_1\\ &= -e_1 \cdot \tau_{(s_0 s_1)^i} \cdot \beta^0_{s_0} \otimes \beta^-_1 + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^+_{s_0(s_1 s_0)^i}.\end{aligned}$$

This shows that these last four families of generators are superfluous, thus concluding the proof. ■

Remark 4.5.2. As already used in the last computation in the proof of the lemma, the last four families of generators can also be rewritten in the following form:

$$\begin{aligned}\beta^+_1 \otimes \beta^-_{(s_1 s_0)^i} &= \beta^+_{(s_1 s_0)^i} \otimes \beta^-_1 && \text{for } i \in \mathbb{Z}_{\geqslant 1},\\ \beta^+_1 \otimes \beta^-_{s_1(s_0 s_1)^i} &= -\beta^+_{s_1(s_0 s_1)^i} \otimes \beta^+_1 && \text{for } i \in \mathbb{Z}_{\geqslant 0},\\ \beta^-_1 \otimes \beta^+_{(s_0 s_1)^i} &= \beta^-_{(s_0 s_1)^i} \otimes \beta^+_1 && \text{for } i \in \mathbb{Z}_{\geqslant 1},\\ \beta^-_1 \otimes \beta^+_{s_0(s_1 s_0)^i} &= -\beta^-_{s_0(s_1 s_0)^i} \otimes \beta^-_1 && \text{for } i \in \mathbb{Z}_{\geqslant 0}.\end{aligned}$$

This will be used multiple times in later computations.

4.5.c A section of the multiplication map in degree 2

In Lemma 4.1.3 we have proved that the multiplication map $\mathcal{M}_2 \colon T^2_{E^0} E^1 \longrightarrow E^2$ is surjective. The proof was very explicit, and so looking at the details of such computations it is immediate to construct a section of $\mathcal{M}_2$, as a map of k-vector spaces.

We spell out a couple of details: in (158) we have seen that

$$\beta^0_{(s_1 s_0)^i} \cdot \beta^-_1 = \beta^0_{(s_1 s_0)^i} \smile \beta^-_{(s_1 s_0)^i}.$$

Using (168), we see that

$$\beta^0_{(s_1 s_0)^i} \cdot \beta^-_1 = -\alpha^+_{(s_1 s_0)^i}.$$

In the same way, using all the computations in Lemma 4.1.3 (namely, using (158), (159), (160), (161)) one finds an explicit element in the preimage via $\mathcal{M}_2$ of each of the elements α_w^-, α_w^0, α_w^+ for w of the following forms: $w = (s_1s_0)^i$ with $i \in \mathbb{Z}_{\geqslant 1}$, or $w = (s_0s_1)^i$ with $i \in \mathbb{Z}_{\geqslant 1}$, or $w = s_0(s_1s_0)^i$ with $i \in \mathbb{Z}_{\geqslant 0}$, or $w = s_1(s_0s_1)^i$ with $i \in \mathbb{Z}_{\geqslant 0}$. Finally, using (162), one also finds an explicit element in the preimage via $\mathcal{M}_2$ of each of the elements α_1^- and α_1^+.

All in all, it is easy to see that the following is a section of $\mathcal{M}_2$, as a map of k-vector spaces.

$$
\begin{aligned}
\mathcal{R}_2\colon\ E^2 &\longrightarrow T^2_{E^0}E^1 = E^1 \otimes_{E^0} E^1 \\
\tau_\omega \cdot \alpha^-_{(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^+ \otimes \beta^0_{(s_1s_0)^i} && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^0_{(s_1s_0)^i} &\longmapsto \tau_\omega \cdot \beta_1^+ \otimes \beta^-_{(s_1s_0)^i} = \tau_\omega \cdot \beta^+_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^+_{(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta^0_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^-_{(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta^0_{(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^0_{(s_0s_1)^i} &\longmapsto -\tau_\omega \cdot \beta_1^- \otimes \beta^+_{(s_0s_1)^i} = -\tau_\omega \cdot \beta^-_{(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^+_{(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^- \otimes \beta^0_{(s_0s_1)^i} && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^-_{s_0(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^0_{s_0(s_1s_0)^i} &\mapsto -\tau_\omega \cdot \beta_1^- \otimes \beta^+_{s_0(s_1s_0)^i} = \tau_\omega \cdot \beta^-_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^+_{s_0(s_1s_0)^i} &\longmapsto \tau_\omega \cdot \beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^-_{s_1(s_0s_1)^i} &\longmapsto -\tau_\omega \cdot \beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^0_{s_1(s_0s_1)^i} &\mapsto \tau_\omega \cdot \beta_1^+ \otimes \beta^-_{s_1(s_0s_1)^i} = -\tau_\omega \cdot \beta^+_{s_1(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha^+_{s_1(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha_1^- &\longmapsto \tau_\omega \cdot \Big(\mathcal{R}_2\big(\alpha_1^- + \tau_{s_0} \cdot \alpha^+_{s_0^{-1}}\big) - \tau_{s_0} \cdot \mathcal{R}_2\big(\alpha^+_{s_0^{-1}}\big)\Big) && \text{for } \omega \in T^0/T^1, \\
\tau_\omega \cdot \alpha_1^+ &\longmapsto \tau_\omega \cdot \Big(\mathcal{R}_2\big(\alpha_1^+ + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}}\big) - \tau_{s_1} \cdot \mathcal{R}_2\big(\alpha^-_{s_1^{-1}}\big)\Big) && \text{for } \omega \in T^0/T^1.
\end{aligned}
\tag{170}
$$

The claimed equalities have already been observed in Remark 4.5.2.

For later use, we compute the explicit expression of $\mathcal{R}_2(\alpha_1^-)$, making use of the formulas (87) for the left action of E^0 on E^2:

$$
\begin{aligned}
\mathcal{R}_2(\alpha_1^-) &= \mathcal{R}_2\big(\alpha_1^- + \tau_{s_0} \cdot \alpha^+_{s_0^{-1}}\big) - \tau_{s_0} \cdot \mathcal{R}_2\big(\alpha^+_{s_0^{-1}}\big) \\
&= \mathcal{R}_2\Big(-e_1 \cdot \alpha^+_{s_0^{-1}} - e_{\underline{\mathrm{id}}} \cdot \alpha^0_{s_0^{-1}} + e_{\underline{\mathrm{id}}^2} \cdot \alpha^-_{s_0^{-1}}\Big) - \tau_{s_0} \cdot \mathcal{R}_2\big(\alpha^+_{s_0^{-1}}\big) \\
&= \mathcal{R}_2\Big(-e_1 \cdot \alpha^+_{s_0} + e_{\underline{\mathrm{id}}} \cdot \alpha^0_{s_0} + e_{\underline{\mathrm{id}}^2} \cdot \alpha^-_{s_0}\Big) - \tau_{s_0 c_{-1}} \cdot \mathcal{R}_2\big(\alpha^+_{s_0}\big) \\
&= -e_1 \cdot \beta_1^- \otimes \beta^0_{s_0} - e_{\underline{\mathrm{id}}} \cdot \beta_1^- \otimes \beta^+_{s_0} - e_{\underline{\mathrm{id}}^2} \cdot \beta^0_{s_0} \otimes \beta_1^- - \tau_{s_0 c_{-1}} \cdot \beta_1^- \otimes \beta^0_{s_0} \\
&= -e_1 \cdot \beta_1^- \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^-_{s_0} \otimes \beta_1^- - e_{\underline{\mathrm{id}}^2} \cdot \beta^0_{s_0} \otimes \beta_1^- - \tau_{s_0^{-1}} \cdot \beta_1^- \otimes \beta^0_{s_0}.
\end{aligned}
\tag{171}
$$

Lemma 4.5.3. *The map $\mathcal{R}_2$ commutes with the automorphism Γ_ϖ. More precisely,* *the following diagram is commutative:*

$$\begin{tikzcd}
E^2 \arrow[r, "\mathcal{R}_2"] \arrow[d, "\Gamma_\varpi"] & E^1 \otimes_{E^0} E^1 \arrow[d, "\Gamma_\varpi"] \\
E^2 \arrow[r, "\mathcal{R}_2"] & E^1 \otimes_{E^0} E^1 .
\end{tikzcd}$$

Proof. In the following we will make repeated use of the explicit formulas (26), (58) and (82) for the action of Γ_ϖ on E^0, E^1 and E^2 respectively. We consider some of the lines in the definition of $\mathcal{R}_2$ (170) and we apply Γ_ϖ on both sides, getting the following (where $\omega \in T^0/T^1$ and where $i \in \mathbb{Z}_{\geqslant 1}$ for the first three lines and $i \in \mathbb{Z}_{\geqslant 0}$ for the following three lines):

$$\begin{gathered}
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^-_{(s_1s_0)^i}\right) = \tau_{\omega^{-1}} \cdot \alpha^+_{(s_0s_1)^i} \longmapsto ? \longrightarrow \Gamma_\varpi\left(-\tau_\omega \cdot \beta^+_1 \otimes \beta^0_{(s_1s_0)^i}\right) = \tau_{\omega^{-1}} \cdot \beta^-_1 \otimes \beta^0_{(s_0s_1)^i}, \\
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^0_{(s_1s_0)^i}\right) = -\tau_{\omega^{-1}} \cdot \alpha^0_{(s_0s_1)^i} \longmapsto ? \longrightarrow \Gamma_\varpi\left(\tau_\omega \cdot \beta^+_1 \otimes \beta^-_{(s_1s_0)^i}\right) = \tau_{\omega^{-1}} \cdot \beta^-_1 \otimes \beta^+_{(s_0s_1)^i}, \\
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^+_{(s_1s_0)^i}\right) = \tau_{\omega^{-1}} \cdot \alpha^-_{(s_0s_1)^i} \longmapsto ? \longrightarrow \Gamma_\varpi\left(-\tau_\omega \cdot \beta^0_{(s_1s_0)^i} \otimes \beta^-_1\right) = \tau_{\omega^{-1}} \cdot \beta^0_{(s_0s_1)^i} \otimes \beta^+_1, \\
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^-_{s_1(s_0s_1)^i}\right) = \tau_{\omega^{-1}} \cdot \alpha^+_{s_0(s_1s_0)^i} \longmapsto ? \longrightarrow \Gamma_\varpi\left(-\tau_\omega \cdot \beta^+_1 \otimes \beta^0_{s_1(s_0s_1)^i}\right) = \tau_{\omega^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0(s_1s_0)^i}, \\
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^0_{s_1(s_0s_1)^i}\right) = -\tau_{\omega^{-1}} \cdot \alpha^0_{s_0(s_1s_0)^i} \longmapsto ? \longrightarrow \Gamma_\varpi\left(\tau_\omega \cdot \beta^+_1 \otimes \beta^-_{s_1(s_0s_1)^i}\right) = \tau_{\omega^{-1}} \cdot \beta^-_1 \otimes \beta^+_{s_0(s_1s_0)^i}, \\
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^+_{s_1(s_0s_1)^i}\right) = \tau_{\omega^{-1}} \cdot \alpha^-_{s_0(s_1s_0)^i} \longmapsto ? \longrightarrow \Gamma_\varpi\left(\tau_\omega \cdot \beta^0_{s_1(s_0s_1)^i} \otimes \beta^+_1\right) = -\tau_{\omega^{-1}} \cdot \beta^0_{s_0(s_1s_0)^i} \otimes \beta^-_1, \\
\Gamma_\varpi\left(\tau_\omega \cdot \alpha^+_1\right) = \tau_{\omega^{-1}} \cdot \alpha^-_1 \longmapsto ? \longrightarrow \Gamma_\varpi\left(\tau_\omega \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)\right).
\end{gathered}$$

By looking at the definition of $\mathcal{R}_2$ (170), we see that the left hand sides of the first six lines are actually mapped to the respective right hand sides. Now it remains to compute the right hand side of the last line:

$$\begin{aligned}
\Gamma_\varpi & \left(\tau_\omega \cdot \left(\mathcal{R}_2(\alpha^+_1 + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}}) - \tau_{s_1} \cdot \mathcal{R}_2(\alpha^-_{s_1^{-1}})\right)\right) \\
&= \tau_{\omega^{-1}} \cdot \left(\Gamma_\varpi\left(\mathcal{R}_2(\alpha^+_1 + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}})\right) - \tau_{s_0} \cdot \Gamma_\varpi\left(\mathcal{R}_2(\alpha^-_{s_1^{-1}})\right)\right) \\
&= \tau_{\omega^{-1}} \cdot \left(\mathcal{R}_2\left(\Gamma_\varpi(\alpha^+_1 + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}})\right) - \tau_{s_0} \cdot \mathcal{R}_2\left(\Gamma_\varpi(\alpha^-_{s_1^{-1}})\right)\right) \\
&\qquad \qquad \big(\text{since } \Gamma_\varpi \circ \mathcal{R}_2 \text{ and } \mathcal{R}_2 \circ \Gamma_\varpi \text{ coincide on } \textstyle\bigoplus_{\vartheta \in T^0/T^1} H^2(I, \mathbf{X}(\vartheta s_1))\big) \\
&= \tau_{\omega^{-1}} \cdot \left(\mathcal{R}_2(\alpha^-_1 + \tau_{s_0} \cdot \alpha^+_{s_0^{-1}}) - \tau_{s_0} \cdot \mathcal{R}_2(\alpha^+_{s_0^{-1}})\right) \\
&= \mathcal{R}_2\left(\tau_{\omega^{-1}} \cdot \alpha^-_1\right),
\end{aligned}$$

and hence also for the last one of the seven lines above it is true that the left hand side gets mapped to the right hand side by $\mathcal{R}_2$. So these seven lines show 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 $\mathcal{R}_2$ (170).

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 on $\Gamma_\varpi(x)$. Indeed, applying Γ_ϖ to both sides of the equality $(\mathcal{R}_2 \circ \Gamma_\varpi)(x) = (\Gamma_\varpi \circ \mathcal{R}_2)(x)$, we get

$$\begin{aligned}
(\Gamma_\varpi \circ \mathcal{R}_2 \circ \Gamma_\varpi)(x) &= (\Gamma_\varpi \circ \Gamma_\varpi \circ \mathcal{R}_2)(x) \\
&= \mathcal{R}_2(x) \\
&= (\mathcal{R}_2 \circ \Gamma_\varpi \circ \Gamma_\varpi)(x),
\end{aligned}$$

thus proving the claim. In this way the proof of the lemma is complete, because it is easy to check that the remaining "half" of the elements in our k-basis of E^2 can be obtained by applying Γ_ϖ to elements of the first "half". ■

Remark 4.5.4. We have already computed the explicit expression of $\mathcal{R}_2(\alpha_1^-)$. One could compute $\mathcal{R}_2(\alpha_1^+)$ in a similar way, but since now we know that $\mathcal{R}_2$ is Γ_ϖ-invariant we can get such explicit expression in a quicker way:

$$\begin{aligned}\mathcal{R}_2(\alpha_1^+) &= \Gamma_\varpi(\mathcal{R}_2(\alpha_1^+)) \\ &= \Gamma_\varpi\left(-e_1\cdot\beta_1^-\otimes\beta_{s_0}^0 + e_{\underline{\mathrm{id}}}\cdot\beta_{s_0}^-\otimes\beta_1^- - e_{\underline{\mathrm{id}}^2}\cdot\beta_{s_0}^0\otimes\beta_1^- - \tau_{s_0^{-1}}\cdot\beta_1^-\otimes\beta_{s_0}^0\right) \\ &= e_1\cdot\beta_1^+\otimes\beta_{s_1}^0 + e_{\underline{\mathrm{id}}^{-1}}\cdot\beta_{s_1}^+\otimes\beta_1^+ + e_{\underline{\mathrm{id}}^{-2}}\cdot\beta_{s_1}^0\otimes\beta_1^+ + \tau_{s_1^{-1}}\cdot\beta_1^+\otimes\beta_{s_1}^0.\end{aligned} \tag{172}$$

Lemma 4.5.5. *The map defined exactly as $\mathcal{R}_2$ but by putting multiplication by τ_ω (for $\omega\in T^0/T^1$) on the right everywhere instead of on the left everywhere is actually the same map as $\mathcal{R}_2$. In other words, the map $\mathcal{R}_2$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules.*

Proof. Let $\omega\in T^0/T^1$ and let $w\in\widetilde{W}$; from the formulas describing the structure of E^1 and E^2 as $k\left[T^0/T^1\right]$-bimodules (see (59) and (60)), we get that, up to a certain coefficient, the element $\tau_\omega\cdot\beta_w^-$ coincide either with $\beta_w^-\cdot\tau_\omega$ or with $\beta_w^-\cdot\tau_{\omega^{-1}}$ depending on the length of w. And the same holds for β_w^+, α_w^- or α_w^+ in place of β_w^-, and (if the length of w is nonzero) also for β_w^0 and α_w^0. Now, let us use the notation ω_u for $u\in\mathbb{F}_p^\times$ as in (59) and (60) and let us apply such formulas to some of the lines in the definition of $\mathcal{R}_2$ (170): namely, let us consider the following lines:

$$\begin{array}{lll}
\tau_{\omega_u}\cdot\alpha^-_{(s_1s_0)^i} \longmapsto -\tau_{\omega_u}\cdot\beta_1^+\otimes\beta^0_{(s_1s_0)^i} & & \text{for } i\in\mathbb{Z}_{\geqslant 1} \text{ and } \omega\in T^0/T^1,\\
\tau_{\omega_u}\cdot\alpha^0_{(s_1s_0)^i} \longmapsto \tau_{\omega_u}\cdot\beta_1^+\otimes\beta^-_{(s_1s_0)^i} & & \text{for } i\in\mathbb{Z}_{\geqslant 1} \text{ and } \omega\in T^0/T^1,\\
\tau_{\omega_u}\cdot\alpha^+_{(s_1s_0)^i} \longmapsto -\tau_{\omega_u}\cdot\beta^0_{(s_1s_0)^i}\otimes\beta_1^- & & \text{for } i\in\mathbb{Z}_{\geqslant 1} \text{ and } \omega\in T^0/T^1,\\
\tau_{\omega_u}\cdot\alpha^-_{s_0(s_1s_0)^i} \longmapsto -\tau_{\omega_u}\cdot\beta^0_{s_0(s_1s_0)^i}\otimes\beta_1^- & & \text{for } i\in\mathbb{Z}_{\geqslant 0} \text{ and } \omega\in T^0/T^1,\\
\tau_{\omega_u}\cdot\alpha^0_{s_0(s_1s_0)^i} \longmapsto -\tau_{\omega_u}\cdot\beta_1^-\otimes\beta^+_{s_0(s_1s_0)^i} & & \text{for } i\in\mathbb{Z}_{\geqslant 0} \text{ and } \omega\in T^0/T^1,\\
\tau_{\omega_u}\cdot\alpha^+_{s_0(s_1s_0)^i} \longmapsto \tau_{\omega_u}\cdot\beta_1^-\otimes\beta^0_{s_0(s_1s_0)^i} & & \text{for } i\in\mathbb{Z}_{\geqslant 0} \text{ and } \omega\in T^0/T^1,\\
\tau_{\omega_u}\cdot\alpha_1^- \longmapsto \tau_{\omega_u}\cdot\left(\mathcal{R}_2(\alpha_1^- + \tau_{s_0}\cdot\alpha^+_{s_0^{-1}}) - \tau_{s_0}\cdot\mathcal{R}_2(\alpha^+_{s_0^{-1}})\right) & & \text{for } \omega\in T^0/T^1.
\end{array}$$

We now apply the formulas outlined above relating multiplication by τ_{ω_u} on the left and on the right, obtaining the following:

$$\begin{array}{l}
u^2\alpha^-_{(s_1s_0)^i}\cdot\tau_{\omega_u} \longmapsto -u^2\beta_1^+\otimes\beta^0_{(s_1s_0)^i}\cdot\tau_{\omega_u},\\
\alpha^0_{(s_1s_0)^i}\cdot\tau_{\omega_u} \longmapsto u^2\beta_1^+\otimes u^{-2}\beta^-_{(s_1s_0)^i}\cdot\tau_{\omega_u},\\
u^{-2}\alpha^+_{(s_1s_0)^i}\cdot\tau_{\omega_u} \longmapsto -\beta^0_{(s_1s_0)^i}\otimes u^{-2}\beta_1^-\cdot\tau_{\omega_u},\\
u^2\alpha^-_{s_0(s_1s_0)^i}\cdot\tau_{\omega_{u^{-1}}} \longmapsto -\beta^0_{s_0(s_1s_0)^i}\otimes(u^{-1})^{-2}\beta_1^-\cdot\tau_{\omega_{u^{-1}}},\\
\alpha^0_{s_0(s_1s_0)^i}\cdot\tau_{\omega_{u^{-1}}} \longmapsto -u^{-2}\beta_1^-\otimes u^2\beta^+_{s_0(s_1s_0)^i}\cdot\tau_{\omega_{u^{-1}}},\\
u^{-2}\alpha^+_{s_0(s_1s_0)^i}\cdot\tau_{\omega_{u^{-1}}} \longmapsto u^{-2}\beta_1^-\otimes\beta^0_{s_0(s_1s_0)^i}\cdot\tau_{\omega_{u^{-1}}},\\
u^2\alpha_1^-\cdot\tau_{\omega_u} \longmapsto \mathcal{R}_2(u^2\alpha_1^-\cdot\tau_{\omega_u} + \tau_{s_0}\cdot(u^{-1})^{-2}\alpha^+_{s_0^{-1}}\cdot\tau_{\omega_u}) - \tau_{s_0}\cdot\mathcal{R}_2((u^{-1})^{-2}\alpha^+_{s_0^{-1}}\cdot\tau_{\omega_u}).
\end{array}$$

From the first six lines, it is clear that $\mathcal{R}_2$ is a homomorphism of right $k\left[T^0/T^1\right]$-modules when restricted to the submodule

$$\bigoplus_{i\in\mathbb{Z}_{\geqslant 1}}\bigoplus_{\vartheta\in T^0/T^1} H^2\left(I,\mathbf{X}(\vartheta(s_1s_0)^i)\right)\oplus\bigoplus_{i\in\mathbb{Z}_{\geqslant 0}}\bigoplus_{\vartheta\in T^0/T^1} H^2\left(I,\mathbf{X}(\vartheta s_0(s_1s_0)^i)\right).$$

We can now conclude the computation in the last line using the fact that $\mathcal{R}_2$ is a homomorphism of right $k\left[T^0/T^1\right]$-modules when restricted to the subspace $\bigoplus_{\vartheta\in T^0/T^1} H^2(I,\mathbf{X}(\vartheta s_0))$, getting the following result:

$$u^2\mathcal{R}_2\big(\alpha_1^- + \tau_{s_0}\cdot\alpha^+_{s_0^{-1}}\big)\cdot\tau_{\omega_u} - u^2\tau_{s_0}\cdot\mathcal{R}_2\big(\alpha^+_{s_0^{-1}}\big)\cdot\tau_{\omega_u}.$$

So far, we have thus shown that $\mathcal{R}_2(x\cdot\tau_\vartheta) = \mathcal{R}_2(x)\cdot\tau_\vartheta$ for all $\vartheta\in T^0/T^1$ and at least for some of the elements x in our fixed k-basis of E^2. All the remaining elements of our basis are of the form $\Gamma_\varpi(x)$ for x such that the last equality hold, but then, using the last lemma we get

$$\begin{aligned}
\mathcal{R}_2\left(\Gamma_\varpi(x)\cdot\tau_\vartheta\right) &= \mathcal{R}_2\left(\Gamma_\varpi(x\cdot\tau_{\vartheta^{-1}})\right)\\
&= \Gamma_\varpi\left(\mathcal{R}_2(x\cdot\tau_{\vartheta^{-1}})\right)\\
&= \Gamma_\varpi\left(\mathcal{R}_2(x)\cdot\tau_{\vartheta^{-1}}\right)\\
&= \Gamma_\varpi\left(\mathcal{R}_2(x)\right)\cdot\tau_\vartheta\\
&= \mathcal{R}_2\left(\Gamma_\varpi(x)\right)\cdot\tau_\vartheta.
\end{aligned}$$

This shows that the equation $\mathcal{R}_2(y\cdot\tau_\vartheta) = \mathcal{R}_2(y)\cdot\tau_\vartheta$ is satisfied for all $\vartheta\in T^0/T^1$ and for y running through the remaining elements of our k-basis. ■

Remark 4.5.6. With the last lemma at our disposal, we can simplify the definition of $\mathcal{R}_2$ (170) in the following way:

$$\begin{array}{rlll}
\mathcal{R}_2\colon & E^2 & \longrightarrow T^2_{E^0}E^1 = E^1\otimes_{E^0}E^1 & \\
& \alpha^-_{s_1v} & \longmapsto -\beta_1^+\otimes\beta^0_{s_1v} & \text{for } v\in\widetilde{W} \text{ s.t. } \ell(s_1v)=\ell(v)+1,\\
& \alpha^0_{s_1v} & \longmapsto \beta_1^+\otimes\beta^-_{s_1v} & \text{for } v\in\widetilde{W} \text{ s.t. } \ell(s_1v)=\ell(v)+1,\\
& \alpha^+_{s_1v} & \longmapsto \beta^0_{s_1}\otimes\beta^+_{v} & \text{for } v\in\widetilde{W} \text{ s.t. } \ell(s_1v)=\ell(v)+1,\\
& \alpha^-_{s_0w} & \longmapsto -\beta^0_{s_0}\otimes\beta^-_{w} & \text{for } w\in\widetilde{W} \text{ s.t. } \ell(s_0w)=\ell(w)+1,\\
& \alpha^0_{s_0w} & \longmapsto -\beta^-_{1}\otimes\beta^+_{s_0w} & \text{for } w\in\widetilde{W} \text{ s.t. } \ell(s_0w)=\ell(w)+1,\\
& \alpha^+_{s_0w} & \longmapsto \beta^-_{1}\otimes\beta^0_{s_0w} & \text{for } w\in\widetilde{W} \text{ s.t. } \ell(s_0w)=\ell(w)+1,\\
& \alpha^-_{\omega} & \longmapsto \mathcal{R}_2\big(\alpha^-_\omega+\tau_{s_0}\cdot\alpha^+_{s_0^{-1}\omega}\big)-\tau_{s_0}\cdot\mathcal{R}_2\big(\alpha^+_{s_0^{-1}\omega}\big) & \text{for } \omega\in T^0/T^1,\\
& \alpha^+_{\omega} & \longmapsto \mathcal{R}_2\big(\alpha^+_\omega+\tau_{s_1}\cdot\alpha^-_{s_1^{-1}\omega}\big)-\tau_{s_1}\cdot\mathcal{R}_2\big(\alpha^-_{s_1^{-1}\omega}\big) & \text{for } \omega\in T^0/T^1.
\end{array}$$

Note that if we had defined $\mathcal{R}_2$ using multiplication on the right by τ_ω instead of multiplication on the left, we could have proved the above description immediately.

Lemma 4.5.7. *Let us consider the following $\mathcal{J}$-invariant k-subspace of E^2:*

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

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

$$\begin{tikzcd}
F^1E^2 \arrow[r, "\mathcal{R}_2|_{F^1E^2}"] \arrow[d, "\mathcal{J}"'] & E^1\otimes_{E^0}E^1 \arrow[d, "\mathcal{J}", "{\substack{\beta\otimes\beta'\\ \mapsto\\ -\mathcal{J}(\beta')\otimes\mathcal{J}(\beta)}}"'] \\
F^1E^2 \arrow[r, "\mathcal{R}_2|_{F^1E^2}"'] & E^1\otimes_{E^0}E^1.
\end{tikzcd}$$

Proof. Before beginning the computations, we first recall from (49) that the involutions $\mathcal{J}$ and Γ_ϖ commute on E^*. With this property, it is easy to show 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:

$$\begin{aligned}
(\mathcal{J} \circ \mathcal{R}_2)(\Gamma_\varpi(\alpha)) &= (\mathcal{J} \circ \Gamma_\varpi \circ \mathcal{R}_2)(\alpha) && \text{since } \mathcal{R}_2 \text{ commutes with } \Gamma_\varpi \text{ (Lemma 4.5.3)}\\
&= (\Gamma_\varpi \circ \mathcal{J} \circ \mathcal{R}_2)(\alpha) && \begin{array}{c}\text{since } \mathcal{J} \text{ and } \Gamma_\varpi \text{ commute on } E^1\\ \text{and hence on } E^1 \otimes_{E^0} E^1\end{array}\\
&= (\Gamma_\varpi \circ \mathcal{R}_2 \circ \mathcal{J})(\alpha) && \text{by assumption}\\
&= (\mathcal{R}_2 \circ \Gamma_\varpi \circ \mathcal{J})(\alpha) && \text{since } \mathcal{R}_2 \text{ commutes with } \Gamma_\varpi \text{ (Lemma 4.5.3)}\\
&= (\mathcal{R}_2 \circ \mathcal{J})(\Gamma_\varpi(\alpha)) && \text{since } \mathcal{J} \text{ and } \Gamma_\varpi \text{ commute on } E^2.
\end{aligned}$$

Now, let us consider the k-basis of F^1E^2 used in the definition of $\mathcal{R}_2$ (170). 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 all the elements in the left hand side of the following lines, since the other elements appearing in such k-basis of F^1E^2 can be obtained from these by applying Γ_ϖ.

$$\begin{array}{lll}
\tau_\omega \cdot \alpha^-_{(s_1s_0)^i} \xmapsto{\mathcal{R}_2} -\tau_\omega \cdot \beta^+_1 \otimes \beta^0_{(s_1s_0)^i} & & \text{for } i \in \mathbb{Z}_{\geqslant 1} \text{ and } \omega \in T^0/T^1,\\
\tau_\omega \cdot \alpha^0_{(s_1s_0)^i} \xmapsto{\mathcal{R}_2} \tau_\omega \cdot \beta^+_1 \otimes \beta^-_{(s_1s_0)^i} & & \text{for } i \in \mathbb{Z}_{\geqslant 1} \text{ and } \omega \in T^0/T^1,\\
\tau_\omega \cdot \alpha^+_{(s_1s_0)^i} \xmapsto{\mathcal{R}_2} -\tau_\omega \cdot \beta^0_{(s_1s_0)^i} \otimes \beta^-_1 & & \text{for } i \in \mathbb{Z}_{\geqslant 1} \text{ and } \omega \in T^0/T^1,\\
\tau_\omega \cdot \alpha^-_{s_0(s_1s_0)^i} \xmapsto{\mathcal{R}_2} -\tau_\omega \cdot \beta^0_{s_0(s_1s_0)^i} \otimes \beta^-_1 & & \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and } \omega \in T^0/T^1,\\
\tau_\omega \cdot \alpha^0_{s_0(s_1s_0)^i} \xmapsto{\mathcal{R}_2} -\tau_\omega \cdot \beta^-_1 \otimes \beta^+_{s_0(s_1s_0)^i} & & \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and } \omega \in T^0/T^1,\\
\tau_\omega \cdot \alpha^+_{s_0(s_1s_0)^i} \xmapsto{\mathcal{R}_2} \tau_\omega \cdot \beta^-_1 \otimes \beta^0_{s_0(s_1s_0)^i} & & \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and } \omega \in T^0/T^1.
\end{array}$$

We now apply the anti-involution $\mathcal{J}$ on both sides of the above lines, in order to check whether the new left hand side is sent to the new right hand side by $\mathcal{R}_2$: for the moment we only treat the case $\omega = 1$. For this computation we use the formulas for the action of $\mathcal{J}$ on E^1 and E^2 (see respectively (57) and (81)).

$$\begin{array}{l}
\alpha^-_{(s_0s_1)^i} \xmapsto{?} \beta^0_{(s_0s_1)^i} \otimes \beta^+_1,\\
\alpha^0_{(s_0s_1)^i} \xmapsto{?} -\beta^-_{(s_0s_1)^i} \otimes \beta^+_1 = -\beta^-_1 \otimes \beta^+_{(s_0s_1)^i},\\
\alpha^+_{(s_0s_1)^i} \xmapsto{?} \beta^-_1 \otimes \beta^0_{(s_0s_1)^i},\\
-\tau_{c_{-1}} \cdot \alpha^+_{s_0(s_1s_0)^i} \xmapsto{?} -\tau_{c_{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0(s_1s_0)^i},\\
-\tau_{c_{-1}} \cdot \alpha^0_{s_0(s_1s_0)^i} \xmapsto{?} -\tau_{c_{-1}} \cdot \beta^-_{s_0(s_1s_0)^i} \otimes \beta^-_1 = \tau_{c_{-1}} \cdot \beta^-_1 \otimes \beta^+_{s_0(s_1s_0)^i},\\
-\tau_{c_{-1}} \cdot \alpha^-_{s_0(s_1s_0)^i} \xmapsto{?} \tau_{c_{-1}} \cdot \beta^0_{s_0(s_1s_0)^i} \otimes \beta^-_1.
\end{array}$$

It is then immediate to see that the left hand side of the first six lines is sent to the right hand side of the respective lines.

Now it remains to treat the general case where ω is not necessarily equal to 1: to this end, it suffices to prove that if $\alpha \in E^2$ is such that $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ coincide at α, then they also coincide on $\tau_\omega \cdot \alpha$ for all $\omega \in T^0/T^1$. This can be shown as follows:

$$\begin{aligned}
(\mathcal{J} \circ \mathcal{R}_2)(\tau_\omega \cdot \alpha) &= \mathcal{J}(\tau_\omega \cdot \mathcal{R}_2(\alpha)) && \text{by Lemma 4.5.5, or immediate}\\
&= \mathcal{J}(\mathcal{R}_2(\alpha)) \cdot \tau_{\omega^{-1}}\\
&= \mathcal{R}_2(\mathcal{J}(\alpha)) \cdot \tau_{\omega^{-1}} && \text{by our assumption}\\
&= \mathcal{R}_2(\mathcal{J}(\alpha) \cdot \tau_{\omega^{-1}}) && \text{by Lemma 4.5.5}\\
&= (\mathcal{R}_2 \circ \mathcal{J})(\tau_\omega \cdot \alpha).
\end{aligned}$$

■

Remark 4.5.8. In view of the previous lemma, it is interesting to know how $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ behave on the subspace

$$F_0E^2 = \bigoplus_{\omega \in T^0/T^1} H^2(I, \mathbf{X}(\omega)).$$

We claim the following.

(i) The following equalities are true:

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

(ii) The two elements above are nonzero, and in particular the two composite maps $\mathcal{J} \circ \mathcal{R}_2$ and $\mathcal{R}_2 \circ \mathcal{J}$ do not coincide on F_0E^2.

(iii) One could change the definition of $\mathcal{R}_2$ on F_0E^2 only (let us call the new map $\mathcal{R}_2'$) in such a way that:

- $\star$ the map $\mathcal{R}_2'$ is again a section of the multiplication map (as a homomorphism of k-vector spaces); it commutes again with Γ_ϖ, as in Lemma 4.5.3; it is again a homomorphism of $k\left[T^0/T^1\right]$-bimodules, as in Lemma 4.5.5;
- $\star$ the map $\mathcal{R}_2'$ commutes with $\mathcal{J}$, this time on the whole E^2.

However, we will use the previous map $\mathcal{R}_2$ instead of $\mathcal{R}_2'$ in order not to make formulas more complicate.

Proof. Let us prove the three parts of the remark.

(i) In the following we will use repeatedly the formulas of Subsection 1.10.c: in particular, we will use some of the formulas for the action of E^0 on E^1 (namely, (61), (63) and (65)) and the formulas for the action of the anti-involution $\mathcal{J}$ on E^1 (57) and on E^2 (81). First of all, we compute

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

Now let us compute $(\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-)$: to this end, we recall from (171) that

$$\begin{aligned}
(\mathcal{R}_2)(\alpha_1^-) = -e_1 \cdot \beta_1^- \otimes \beta_{s_0}^0 &- e_{\underline{\mathrm{id}}} \cdot \beta_1^- \otimes \beta_{s_0}^+ \\
&- e_{\underline{\mathrm{id}}^2} \cdot \beta_{s_0}^0 \otimes \beta_1^- - \tau_{s_0 c_{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0.
\end{aligned}$$

More precisely, the sum of the first three terms is equal to $\mathcal{R}_2\big(\alpha_1^- + \tau_{s_0} \cdot \alpha_{\underline{s_0}^{-1}}^+\big)$, while the last summand is equal to $-\tau_{s_0} \cdot \mathcal{R}_2\big(\alpha_{\underline{s_0}^{-1}}^+\big)$. We now turn to the computation of $(\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-)$:

$$
\begin{aligned}
&(\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-) \\
&= \mathcal{J}\left(-e_1\beta_1^- \otimes \beta_{s_0}^0 - e_{\underline{\mathrm{id}}}\beta_1^- \otimes \beta_{s_0}^+ - e_{\underline{\mathrm{id}}^2}\beta_{s_0}^0 \otimes \beta_1^- - \tau_{s_0^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0\right) \\
&= \mathcal{J}\left(-\beta_1^- e_{\underline{\mathrm{id}}^2} \otimes \beta_{s_0}^0 - \beta_1^- e_{\underline{\mathrm{id}}^3} \otimes \beta_{s_0}^+ - \beta_{s_0}^0 e_{\underline{\mathrm{id}}^{-2}} \otimes \beta_1^- + \beta_{s_0^{-1}}^+ \otimes \beta_{s_0}^0\right) \\
&= \mathcal{J}\left(-\beta_1^- \otimes \beta_{s_0}^0 e_{\underline{\mathrm{id}}^{-2}} - \beta_1^- \otimes \beta_{s_0}^+ e_{\underline{\mathrm{id}}^{-1}} - \beta_{s_0}^0 \otimes \beta_1^- e_1 + \beta_{s_0^{-1}}^+ \otimes \beta_{s_0}^0\right) \\
&= \mathcal{J}\left(-\beta_1^- \otimes \beta_{s_0}^0 e_{\underline{\mathrm{id}}^{-2}} - \beta_1^- \otimes \beta_{s_0}^+ e_{\underline{\mathrm{id}}^{-1}} - \beta_{s_0}^0 \otimes \beta_1^- e_1 + \beta_{s_0^{-1}}^+ \otimes \beta_{s_0}^0\right) \\
&= e_{\underline{\mathrm{id}}^2}\mathcal{J}(\beta_{s_0}^0) \otimes \mathcal{J}(\beta_1^-) + e_{\underline{\mathrm{id}}}\mathcal{J}(\beta_{s_0}^+) \otimes \mathcal{J}(\beta_1^-) \\
&\qquad + e_1\mathcal{J}(\beta_1^-) \otimes \mathcal{J}(\beta_{s_0}^0) - \mathcal{J}(\beta_{s_0}^0) \otimes \mathcal{J}(\beta_{s_0^{-1}}^+) \\
&= -e_{\underline{\mathrm{id}}^2}\beta_{s_0^{-1}}^0 \otimes \beta_1^- - e_{\underline{\mathrm{id}}}\beta_{s_0^{-1}}^- \otimes \beta_1^- - e_1\beta_1^- \otimes \beta_{s_0^{-1}}^0 - \beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^- \\
&= -e_{\underline{\mathrm{id}}^2}\beta_{s_0}^0 \otimes \beta_1^- + e_{\underline{\mathrm{id}}}\beta_{s_0}^- \otimes \beta_1^- - e_1\beta_1^- \otimes \beta_{s_0}^0 - \beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^- \\
&= -e_{\underline{\mathrm{id}}^2}\beta_{s_0}^0 \otimes \beta_1^- - e_{\underline{\mathrm{id}}}\beta_1^- \otimes \beta_{s_0}^+ - e_1\beta_1^- \otimes \beta_{s_0}^0 - \beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^- \\
&= \mathcal{R}_2\big(\alpha_1^- + \tau_{s_0} \cdot \alpha_{s_0^{-1}}^+\big) - \beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^-.
\end{aligned}
$$

These computations show the equality

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

which is the first part of the statement in i). Note that the alternative description as

$$-\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0}$$

is easy to obtain with the usual formulas. Furthermore, the analogous description of

$$-(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^+) + (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^+)$$

can be easily obtained by applying Γ_ϖ (or rather $-\Gamma_\varpi$) to the above equality and recalling that Γ_ϖ commutes with $\mathcal{R}_2$ (see Lemma 4.5.3) and with $\mathcal{J}$ (see (49)).

(ii) Let us show that

(Claim) $$\beta_{s_0}^+ \otimes \beta_{s_0^{-1}}^0 \neq -\beta_{s_0^{-1}}^0 \otimes \beta_{s_0}^-.$$

To this end, it suffices to show that

(Claim) $$\beta_{s_0}^+ \cdot \zeta \cdot \beta_{s_0^{-1}}^0 \neq -\beta_{s_0^{-1}}^0 \cdot \zeta \cdot \beta_{s_0}^-,$$

since the following map is well defined (because $\zeta \in Z(E^0)$):

$$
\begin{aligned}
E^1 \otimes_{E^0} E^1 &\longrightarrow E^2 \\
\beta \otimes \beta' &\longmapsto \beta \cdot \zeta \cdot \beta'.
\end{aligned}
$$

In the following we will repeatedly use the formulas for the action of E^0 on E^1 (in particular, (61), (63), (66) and (65)). To multiply pairs of elements of

E^1 we refer instead to the definition of $\mathcal{R}_2$ (170). So let us start by (partially) computing $\beta^+_{s_0} \cdot \zeta \cdot \beta^0_{s_0^{-1}}$:

$$\begin{aligned}\beta^+_{s_0} \cdot \zeta \cdot \beta^0_{s_0^{-1}} &= \beta^+_{s_0} \cdot \Big(\beta^0_{s_0 s_1 s_0^{-1}} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_{s_1 s_0^{-1}}\Big)\\ &= -\tau_{s_0} \cdot \beta^-_1 \cdot \beta^0_{s_0 s_1 s_0^{-1}} + e_{\underline{\mathrm{id}}^3} \cdot \tau_{s_0} \cdot \beta^-_1 \cdot \beta^-_{s_1 s_0^{-1}}\\ &= -\tau_{s_0} \cdot \alpha^+_{s_0 s_1 s_0^{-1}} + e_{\underline{\mathrm{id}}^3} \cdot \tau_{s_0} \cdot \beta^-_1 \cdot \tau_{s_1 s_0^{-1}} \cdot \beta^-_1\\ &= \alpha^-_{s_1 s_0} + e_1 \cdot (\dots) + 0.\end{aligned}$$

Now let us compute $-\beta^0_{s_0^{-1}} \cdot \zeta \cdot \beta^-_{s_0}$:

$$\begin{aligned}-\beta^0_{s_0^{-1}} \cdot \zeta \cdot \beta^-_{s_0} &= -\beta^0_{s_0^{-1}} \cdot \Big(\beta^-_{s_1 c_{-1}} + e_1 \cdot (\dots) + e_{\underline{\mathrm{id}}^{-1}} \cdot (\dots) + e_{\underline{\mathrm{id}}^{-2}} \cdot (\dots)\Big)\\ &= \beta^0_{s_0^{-1}} \cdot \tau_{s_1 c_{-1}} \cdot \beta^+_1 + e_1 \cdot (\dots) + e_{\underline{\mathrm{id}}} \cdot (\dots) + e_{\underline{\mathrm{id}}^2} \cdot (\dots)\\ &= \beta^0_{s_0 s_1} \cdot \beta^+_1 + e_1 \cdot (\dots) + e_{\underline{\mathrm{id}}} \cdot (\dots) + e_{\underline{\mathrm{id}}^2} \cdot (\dots)\\ &= \alpha^-_{s_0 s_1} + e_1 \cdot (\dots) + e_{\underline{\mathrm{id}}} \cdot (\dots) + e_{\underline{\mathrm{id}}^2} \cdot (\dots).\end{aligned} \tag{173}$$

Now, since $q = p \geqslant 5$, we can choose $\lambda_0 \in \Gamma \smallsetminus \{1, \underline{\mathrm{id}}, \underline{\mathrm{id}}^2\}$ and, if by contradiction we had the equality $\beta^+_{s_0} \cdot \zeta \cdot \beta^0_{s_0^{-1}} = -\beta^0_{s_0^{-1}} \cdot \zeta \cdot \beta^-_{s_0}$, then, multiplying both terms on the left by e_{λ_0}, we would get the equality $e_{\lambda_0}\alpha^-_{s_1 s_0} = e_{\lambda_0}\alpha^-_{s_0 s_1}$, which is false.

(iii) We define

$$\begin{aligned}\mathcal{R}'_2(x) &\coloneqq \mathcal{R}_2(x) && \text{for all } x \in F^1E^2,\\ \mathcal{R}'_2(\tau_\omega \cdot \alpha^-_1) &\coloneqq \frac{1}{2}\tau_\omega \cdot \big(\mathcal{R}_2(\alpha^-_1) + \mathcal{J}(\mathcal{R}_2(\alpha^-_1))\big) && \text{for all } \omega \in T^0/T^1,\\ \mathcal{R}'_2(\tau_\omega \cdot \alpha^+_1) &\coloneqq \frac{1}{2}\tau_\omega \cdot \big(\mathcal{R}_2(\alpha^+_1) + \mathcal{J}(\mathcal{R}_2(\alpha^+_1))\big) && \text{for all } \omega \in T^0/T^1.\end{aligned}$$

It is clear that $\mathcal{R}'_2$ is a well defined homomorphism of k-vector spaces. Using that $\mathcal{J}$ commutes with the multiplication map (see (164)) and that both α^-_1 and α^+_1 are fixed by $\mathcal{J}$, it is also easy to see that $\mathcal{R}'_2$ is a section of the multiplication map $\mathcal{M}_2$. The fact that $\mathcal{R}'_2$ is a homomorphism of left $k[T^0/T^1]$-modules is clear from the definition.

Regarding the structure of right $k[T^0/T^1]$-modules, since the decomposition $F_0E^2 \oplus F^1E^2$ respects the action of $k[T^0/T^1]$, we only need to check what happens on F_0E^2. Recall from the proof of Lemma 4.5.5 that for all $u \in \mathbb{F}_p^\times$ one has

$$\tau_{\omega_u} \cdot \mathcal{R}_2(\alpha^-_1) = u^2\mathcal{R}_2(\alpha^-_1) \cdot \tau_{\omega_u}.$$

We compute

$$\begin{aligned}\mathcal{R}'_2(\tau_{\omega_u} \cdot \alpha^-_1) &\coloneqq \frac{1}{2}\tau_{\omega_u} \cdot \big(\mathcal{R}_2(\alpha^-_1) + \mathcal{J}(\mathcal{R}_2(\alpha^-_1))\big)\\ &= \frac{1}{2}\big(\tau_{\omega_u} \cdot \mathcal{R}_2(\alpha^-_1) + \mathcal{J}\big(\mathcal{R}_2(\alpha^-_1) \cdot \tau_{\omega_u^{-1}}\big)\big)\\ &= \frac{1}{2}\big(u^2\mathcal{R}_2(\alpha^-_1) \cdot \tau_{\omega_u} + \mathcal{J}\big(u^2\tau_{\omega_u^{-1}} \cdot \mathcal{R}_2(\alpha^-_1)\big)\big)\\ &= u^2\mathcal{R}'_2(\alpha^-_1) \cdot \tau_{\omega_u}.\end{aligned}$$

We have shown that

$$u^2\mathcal{R}_2'(\alpha_1^- \cdot \tau_{\omega_u}) = u^2\mathcal{R}_2'(\alpha_1^-) \cdot \tau_{\omega_u},$$

and this, together with the analogous computation for α_1^+, shows that $\mathcal{R}_2'\big|_{F_0E^2}$ is a homomorphism of right $k[T^0/T^1]$-modules, as we wanted.

Using the definition of $\mathcal{R}_2'$ and that $\mathcal{R}_2'\big|_{F_0E^2}$ is a homomorphism of $k[T^0/T^1]$-bimodules, with an easy computation one checks that $\mathcal{R}_2'\big|_{F_0E^2}$ (and hence $\mathcal{R}_2'$) commutes with $\mathcal{J}$. Also the fact that $\mathcal{R}_2'\big|_{F_0E^2}$ (and hence $\mathcal{R}_2'$) commutes with Γ_ϖ is easy to check, using the fact that Γ_ϖ commutes with $\mathcal{R}_2$ (Lemma 4.5.3) and with $\mathcal{J}$ (see (49)). ■

4.5.d Computation of the kernel in degree 2

Since $\mathcal{R}_2$ is a (set-theoretic) section of the multiplication map $\mathcal{M}_2$, it follows that for all $x \in E^2$ one has

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

In particular, we can produce elements in the kernel using the generators of E^2 as an E^0-bimodule (computed in Lemma 4.5.1). If $\mathcal{R}_2$ were a section of $\mathcal{M}_2$ as a map of E^0-bimodules, in this way we would obtain a set of generators of $\ker(\mathcal{M}_2)$. Unfortunately, we will see in Remark 4.5.14 that this is not the case, even though "few" generators are missing.

Lemma 4.5.9. *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^2 as an E^0-bimodule computed in Lemma 4.5.1, is the sub-E^0-bimodule of $E^1 \otimes_{E^0} E^1$ generated by the following elements.

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

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

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

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

Proof. The generators of E^2 as an E^0-bimodule computed in Lemma 4.5.1 are the following:

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

$$\begin{array}{ll}
\beta_1^+ \otimes \beta_{(s_1s_0)^i}^- & \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
\beta_1^+ \otimes \beta_{s_1(s_0s_1)^i}^- & \text{for } i \in \mathbb{Z}_{\geqslant 0}, \\
\beta_1^- \otimes \beta_{(s_0s_1)^i}^+ & \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\
\beta_1^- \otimes \beta_{s_0(s_1s_0)^i}^+ & \text{for } i \in \mathbb{Z}_{\geqslant 0}.
\end{array}$$

From the definition of $\mathcal{R}_2$ (170), 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 treat 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, 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 [OS21, 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 relating cup product and (opposite of the) Yoneda product (Corollary 1.9.3). But then we see that all such products are zero, because
$$\begin{aligned}
\tau_{s_0} \cdot \beta_1^+ &= 0, & \beta_1^+ \cdot \tau_{s_0} &= 0, \\
\tau_{s_1} \cdot \beta_1^- &= 0, & \beta_1^- \cdot \tau_{s_1} &= 0.
\end{aligned}$$

  So, again, 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 relating cup product and (opposite of the) Yoneda product (Corollary 1.9.3), and we see that it is zero (the other one can be computed exactly in the same way, or alternatively one can use Γ_ϖ or $\mathcal{J}$):
$$\begin{aligned}
\beta_{s_1}^0 \cdot \beta_{s_0}^0 &= (\beta_{s_1}^0 \cdot \tau_{s_0}) \smile (\tau_{s_1} \cdot \beta_{s_0}^0) \\
&= \beta_{s_1 s_0}^0 \smile (-\beta_{s_1 s_0}^0) \\
&= 0.
\end{aligned}$$

  So, again, 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. At the end of the proof of [OS21, Proposition 9.5] the following formula is computed (recall the definition of $\beta_{s_0}^{0,\star}$ from (71)):
$$\beta_{s_0}^{0,\star} \cdot \beta_{s_0}^{0,\star} = -e_1 \cdot \alpha_{s_0}^0$$
  (the formula claimed and proved there is actually $\beta_{s_0}^{0,\star} \cdot \beta_{s_0}^{0,\star} = e_1 \cdot \alpha_{s_0}^{0,\star}$, but in passing also the above formula is shown, and in any case one can use (88)). Now,

let us use the definition of $\beta^{0,\star}_{s_0}$ (i.e., $\beta^{0,\star}_{s_0} = -\beta^0_{s_0} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1$) to make this formula more explicit:

$$\begin{aligned}
-e_1 \cdot \alpha^0_{s_0} &= \beta^{0,\star}_{s_0} \cdot \beta^{0,\star}_{s_0} \\
&= \big(-\beta^0_{s_0} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1\big) \cdot \big(-\beta^0_{s_0} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1\big) \\
&= \beta^0_{s_0} \cdot \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \cdot \beta^0_{s_0} + \beta^0_{s_0} \cdot e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \cdot e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \\
&= \beta^0_{s_0} \cdot \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \cdot \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \cdot \beta^-_1 + e_{\underline{\mathrm{id}}^{-1}} \cdot e_{\underline{\mathrm{id}}^{-3}} \cdot \beta^-_1 \cdot \beta^-_1 \\
&= \beta^0_{s_0} \cdot \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \alpha^+_{s_0} - e_{\underline{\mathrm{id}}} \cdot \alpha^-_{s_0}
\end{aligned}$$

(here we have used the behaviour of properties of the left and right action of the idempotents (61); moreover, in the last step one can compute products explicitly, but actually we have already computed them – see the definition of $\mathcal{R}_2$ (170)). Now we can compute $\mathcal{R}_2(\beta^0_{s_0} \cdot \beta^0_{s_0})$:

$$\begin{aligned}
\mathcal{R}_2(\beta^0_{s_0} \cdot \beta^0_{s_0}) &= \mathcal{R}_2\Big(-e_{\underline{\mathrm{id}}^{-1}} \cdot \alpha^+_{s_0} + e_{\underline{\mathrm{id}}} \cdot \alpha^-_{s_0} - e_1 \cdot \alpha^0_{s_0}\Big) \\
&= -e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0} - e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta^-_1 + e_1 \cdot \beta^-_1 \otimes \beta^+_{s_0}.
\end{aligned}$$

We conclude that the value of $x - \mathcal{R}_2(\mathcal{M}_2(x))$ for $x = \beta^0_{s_0} \otimes \beta^0_{s_0}$ is

$$\beta^0_{s_0} \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta^-_1 - e_1 \cdot \beta^-_1 \otimes \beta^+_{s_0}.$$

Now it remains to compute the value of $x - \mathcal{R}_2(\mathcal{M}_2(x))$ for $x = \beta^0_{s_1} \otimes \beta^0_{s_1}$, but since $\Gamma_\varpi(\beta^0_{s_0}) = -\beta^0_{s_1}$ and since $\mathcal{R}_2$ is Γ_ϖ-invariant (Lemma 4.5.3), we see that such value can be obtained by applying Γ_ϖ to the last displayed equality. Hence we get

$$\beta^0_{s_1} \otimes \beta^0_{s_1} - e_{\underline{\mathrm{id}}} \cdot \beta^+_1 \otimes \beta^0_{s_1} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_1 - e_1 \cdot \beta^+_1 \otimes \beta^-_{s_1}. \qquad \blacksquare$$

Remark 4.5.10. Let us define K_2 as the sub-E^0-bimodule of $E^1 \otimes_{E^0} E^1$ generated by the following elements:

$$\begin{array}{lll}
\beta^-_1 \otimes \beta^-_1, & \beta^+_1 \otimes \beta^-_1, & \beta^0_{s_1} \otimes \beta^-_1, \\
\beta^-_1 \otimes \beta^+_1, & \beta^+_1 \otimes \beta^+_1, & \beta^0_{s_0} \otimes \beta^+_1, \\
\beta^+_1 \otimes \beta^0_{s_0}, & \beta^0_{s_1} \otimes \beta^0_{s_0}, & \\
\beta^-_1 \otimes \beta^0_{s_1}, & \beta^0_{s_0} \otimes \beta^0_{s_1}, &
\end{array}$$

$$\begin{aligned}
&\beta^0_{s_0} \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta^-_1 - e_1 \cdot \beta^-_1 \otimes \beta^+_{s_0}, \\
&\beta^0_{s_1} \otimes \beta^0_{s_1} - e_{\underline{\mathrm{id}}} \cdot \beta^+_1 \otimes \beta^0_{s_1} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_1 - e_1 \cdot \beta^+_1 \otimes \beta^-_{s_1}, \\
&\beta^+_{s_0} \otimes \beta^0_{s_0} + \beta^0_{s_0} \otimes \beta^-_{s_0} = -\tau_{s_0} \cdot \beta^-_1 \otimes \beta^0_{s_0} + \beta^0_{s_0} \otimes \beta^-_1 \cdot \tau_{s_0}, \\
&\beta^-_{s_1} \otimes \beta^0_{s_1} + \beta^0_{s_1} \otimes \beta^+_{s_1} = -\tau_{s_1} \cdot \beta^+_1 \otimes \beta^0_{s_1} + \beta^0_{s_1} \otimes \beta^+_1 \cdot \tau_{s_1}.
\end{aligned}$$

The first twelve elements were obtained in Lemma 4.5.9 (in particular, they lie in $\ker(\mathcal{R}_2)$), while the last two elements were obtained in Remark 4.5.8 and they are respectively equal to

$$\begin{gathered}
(\mathcal{R}_2 \circ \mathcal{J})(\alpha^-_1) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha^-_1), \\
-(\mathcal{R}_2 \circ \mathcal{J})(\alpha^+_1) + (\mathcal{J} \circ \mathcal{R}_2)(\alpha^+_1)
\end{gathered}$$

(in particular, they lie in $\ker(\mathcal{R}_2)$, too, since $\mathcal{J}$ and $\mathcal{M}_2$ commute by (164)).

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

Lemma 4.5.11. *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 4.5.10) are Γ_ϖ-invariant and $\mathcal{J}$-invariant. 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 (actually, regarding $\mathcal{J}$ one can avoid the computation by recalling that these last two elements were, by definition, of the form $x - \mathcal{J}(x)$ for suitable $x \in E^1 \otimes_{E^0} E^1$). It remains to study the behaviour of Γ_ϖ and $\mathcal{J}$ on the following two elements:

$$x_0 \coloneqq \beta^0_{s_0} \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta^-_1 - e_1 \cdot \beta^-_1 \otimes \beta^+_{s_0},$$
$$x_1 \coloneqq \beta^0_{s_1} \otimes \beta^0_{s_1} - e_{\underline{\mathrm{id}}} \cdot \beta^+_1 \otimes \beta^0_{s_1} - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_1 - e_1 \cdot \beta^+_1 \otimes \beta^-_{s_1}.$$

In the proof of Lemma 4.5.9, 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 (57) for the action of $\mathcal{J}$ on E^1 and the formula (61) for the action of the idempotents on E^1:

$$\begin{aligned}
\mathcal{J}(x_0) &= \mathcal{J}\left(\beta^0_{s_0} \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta^-_1 - e_1 \cdot \beta^-_1 \otimes \beta^+_{s_0}\right) \\
&= -\beta^0_{s_0^{-1}} \otimes \beta^0_{s_0^{-1}} + \beta^0_{s_0^{-1}} \otimes \beta^-_1 \cdot e_{\underline{\mathrm{id}}} + \beta^-_1 \otimes \beta^0_{s_0^{-1}} \cdot e_{\underline{\mathrm{id}}^{-1}} - \beta^-_{s_0^{-1}} \otimes \beta^-_1 \cdot e_1 \\
&= -\beta^0_{s_0} \otimes \beta^0_{s_0} + \beta^0_{s_0^{-1}} \otimes (e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1) + \beta^-_1 \otimes (e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0^{-1}}) - \beta^-_{s_0^{-1}} \otimes (e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_1) \\
&= -\beta^0_{s_0} \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0^{-1}} \otimes \beta^-_1 + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0^{-1}} - e_1 \cdot \beta^-_{s_0^{-1}} \otimes \beta^-_1 \\
&= -\beta^0_{s_0} \otimes \beta^0_{s_0} - e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta^-_1 - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_1 \otimes \beta^0_{s_0} + e_1 \cdot \beta^-_1 \otimes \beta^+_{s_0} \\
&= -x_0.
\end{aligned}$$

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 (49), and hence also on $T^*_{E^0}E^1$), getting that

$$\mathcal{J}(x_1) = \mathcal{J}(\Gamma_\varpi(x_0)) = \Gamma_\varpi(\mathcal{J}(x_0)) = \Gamma_\varpi(-x_0) = -x_1. \qquad \blacksquare$$

Lemma 4.5.12. *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 left E^0-modules.

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

(i) $\mathcal{R}_2(\tau_{s_0} \cdot \alpha^\sigma_{s_1 v}) \equiv \tau_{s_0} \cdot \mathcal{R}_2(\alpha^\sigma_{s_1 v})$ 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) $\mathcal{R}_2(\tau_{s_1} \cdot \alpha^\sigma_{s_1 v}) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha^\sigma_{s_1 v})$ 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 4.5.3 that Γ_ϖ commutes with $\mathcal{R}_2$ and in Lemma 4.5.11 that K_2 is Γ_ϖ-invariant, and so by applying Γ_ϖ to the equalities in (i), (ii) and (iii), we get:

(i') $\mathcal{R}_2(\tau_{s_1} \cdot \alpha^\sigma_{s_0w}) \equiv \tau_{s_1} \cdot \mathcal{R}_2(\alpha^\sigma_{s_0w})$ modulo K_2 for $w \in \widetilde{W}$ with $\ell(s_0w) = \ell(w)+1$ and for $\sigma \in \{-,0,+\}$ (as before, we already have equality in $E^1 \otimes_{E^0} E^1$);

(ii') $\mathcal{R}_2(\tau_{s_0} \cdot \alpha^\sigma_{s_0w}) \equiv \tau_{s_0} \cdot \mathcal{R}_2(\alpha^\sigma_{s_0w})$ modulo K_2 for $w \in \widetilde{W}$ with $\ell(s_0w) = \ell(w)+1$ and for $\sigma \in \{-,0,+\}$;

(iii') $\mathcal{R}_2(\tau_{s_i} \cdot \alpha^-_1) \equiv \tau_{s_i} \cdot \mathcal{R}_2(\alpha^-_1)$ modulo 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 4.5.5, or just by definition of $\mathcal{R}_2$ (170)).

All in all, this shows that the congruence

$$\mathcal{R}_2(x \cdot \alpha) \equiv x \cdot \mathcal{R}_2(\alpha) \mod K_2$$

is true for α running through a k-basis of E^2 and for $x \in \{\tau_{s_1}, \tau_{s_2}\}$. 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 the above congruence 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.

Now, it remains to prove (i), (ii) and (iii). In the following we will use multiple times the formulas in Subsection 1.10.c for E^1 (in particular, (57), (61), (63), (65) and (66)), and, less frequently, the formulas in Subsection 1.10.e for E^2 (in particular, (81), (85), (86) and (87)).

(i) We have to consider the following three lines in the new definition of $\mathcal{R}_2$ given in Remark 4.5.6:

$$\begin{aligned}
\alpha^-_{s_1v} &\longmapsto -\beta^+_1 \otimes \beta^0_{s_1v} && \text{for } v \in \widetilde{W} \text{ s.t. } \ell(s_1v) = \ell(v)+1,\\
\alpha^0_{s_1v} &\longmapsto \beta^+_1 \otimes \beta^-_{s_1v} && \text{for } v \in \widetilde{W} \text{ s.t. } \ell(s_1v) = \ell(v)+1,\\
\alpha^+_{s_1v} &\longmapsto \beta^0_{s_1} \otimes \beta^+_v && \text{for } v \in \widetilde{W} \text{ s.t. } \ell(s_1v) = \ell(v)+1.
\end{aligned} \tag{174}$$

We multiply both sides by τ_{s_0} and then we check that $\mathcal{R}_2$ actually sends the resulting left hand side to the resulting right hand side (so in this case we will see that it is not even necessary to mod out by K_2):

$$\begin{aligned}
0 &\xmapsto{\qquad ? \qquad} 0 \otimes \beta^0_{s_1v},\\
0 &\xmapsto{\qquad ? \qquad} 0 \otimes \beta^-_{s_1v},\\
-\alpha^-_{s_0s_1v} &\xmapsto{\ ?\ } -\beta^0_{s_0s_1} \otimes \beta^+_v = \beta^0_{s_0} \otimes \beta^-_{s_1v}.
\end{aligned}$$

The first two lines need no further comment, and looking at the definition of $\mathcal{R}_2$ in Remark 4.5.6, we also see that the left hand side of the third line is sent by $\mathcal{R}_2$ to the right hand side of the third line.

(ii) We now consider again the lines (174) above and this time we multiply both sides by τ_{s_1} and then we check that $\mathcal{R}_2$ actually sends the resulting left hand side to the resulting right hand side after considering the quotient modulo K_2. Since the relevant formulas are a bit different, we first treat the case $\ell(v) \geqslant 1$:

$$\begin{aligned} -\alpha^+_{c_{-1}v} - e_1 \cdot \alpha^-_{s_1v} &\xmapsto{\quad ? \quad} \beta^-_{s_1} \otimes \beta^0_{s_1v}, \\ -\alpha^0_{c_{-1}v} - e_1 \cdot \alpha^0_{s_1v} - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \alpha^+_{s_1v} &\xmapsto{?} -\beta^-_{s_1} \otimes \beta^-_{s_1v}, \\ -e_1 \cdot \alpha^+_{s_1v} &\xmapsto{\quad ? \quad} \tau_{s_1} \cdot \beta^0_{s_1} \otimes \beta^+_v. \end{aligned} \tag{175}$$

We first treat the last line: we claim that

$$\tau_{s_1} \cdot \beta^0_{s_1} \otimes \beta^+_v = -e_1 \cdot \beta^0_{s_1} \otimes \beta^+_v.$$

This is clear from the formula (66) that computes the product $\tau_{s_1} \cdot \beta^0_{s_1v}$ (we use that $\ell(s_1v) \geqslant 2$) and from the equality

$$\beta^0_{s_1} \otimes \beta^+_v = \begin{cases} \beta^0_{s_1v} \otimes \beta^+_1 & \text{if } \ell(v) \text{ is even,} \\ -\beta^0_{s_1v} \otimes \beta^-_1 & \text{if } \ell(v) \text{ is odd.} \end{cases}$$

To treat the first two lines, we first compute the following product:

$$\begin{aligned} \beta^-_{s_1} \cdot \tau_{s_1} &= \mathcal{J}\left(\tau_{s_1^{-1}} \cdot (-\beta^+_{s_1^{-1}})\right) \\ &= -\mathcal{J}\left(\tau_{s_1} \cdot \beta^+_{s_1}\right) \\ &= -\mathcal{J}\left(-\beta^-_{c_{-1}} - e_1 \cdot \beta^+_{s_1} + 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} + e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1}\right) \\ &= \mathcal{J}\left(\beta^-_{c_{-1}} + \beta^+_{s_1} \cdot e_{\underline{\mathrm{id}}^2} - 2\beta^0_{s_1} \cdot e_{\underline{\mathrm{id}}} - \beta^-_{s_1} \cdot e_1\right) \\ &= \beta^-_{c_{-1}} - e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1^{-1}} + 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1^{-1}} + e_1 \cdot \beta^+_{s_1^{-1}} \\ &= \beta^-_{c_{-1}} - e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} + e_1 \cdot \beta^+_{s_1}. \end{aligned}$$

We can now compute the right hand side of the first line in (175):

$$\begin{aligned} \beta^-_{s_1} \otimes \beta^0_{s_1v} &= -\beta^-_{s_1} \cdot \tau_{s_1} \otimes \beta^0_v \\ &= -\beta^-_{c_{-1}} \otimes \beta^0_v + e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^0_v + 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^0_v - e_1 \cdot \beta^+_{s_1} \otimes \beta^0_v \\ &= -\beta^-_{c_{-1}} \otimes \beta^0_v + e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^0_v + 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^0_v + e_1 \cdot \beta^+_1 \otimes \beta^0_{s_1v} \\ &= -\mathcal{R}_2(\alpha^+_{c_{-1}v}) - e_{\underline{\mathrm{id}}^{-2}} \cdot \tau_{s_1} \cdot \beta^+_1 \otimes \beta^0_{s_0} \cdot \tau_{s_0^{-1}v} \\ &\quad + 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^0_{s_0} \cdot \tau_{s_0^{-1}v} - e_1 \cdot \mathcal{R}(\alpha^-_{s_1v}); \end{aligned}$$

and hence we see that although the result is not exactly what expected, it actually becomes equal to $\mathcal{R}_2(-\alpha^+_{c_{-1}v} - e_1 \cdot \alpha^-_{s_1v})$ in the quotient $(E^1 \otimes_{E^0} E^1)/K_2$, as we wanted to show. It remains to treat the second line of (175): we compute

$$\begin{aligned} &- \beta^-_{s_1} \otimes \beta^-_{(s_1s_0)^i} \\ &\quad = \beta^-_{s_1} \cdot \tau_{s_1} \otimes \beta^+_v \\ &\quad = \beta^-_{c_{-1}} \otimes \beta^+_v - e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^+_v - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_v + e_1 \cdot \beta^+_{s_1} \otimes \beta^+_v \\ &\quad = \beta^-_{c_{-1}} \otimes \beta^+_v - e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^+_v - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_v - e_1 \cdot \beta^+_1 \otimes \beta^-_{s_1v} \\ &\quad = -\mathcal{R}(\alpha^0_{c_{-1}v}) - e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^+_v - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \mathcal{R}(\alpha^+_{s_1v}) - e_1 \cdot \mathcal{R}(\alpha^0_{s_1v}). \end{aligned}$$

This is the expected result, except for the presence of the term $\beta^-_{s_1} \otimes \beta^+_v$. We conclude the computation by showing that such term is actually 0: indeed, since v is of the form $s_0 \cdot v'$ for some $v' \in \widetilde{W}$ with $\ell(s_0 v') = \ell(v') + 1$, we have:

$$\begin{aligned}
\beta^-_{s_1} \otimes \beta^+_v &= -\beta^-_{s_1} \otimes (\tau_{s_0} \cdot \beta^-_{v'}) \\
&= -(\beta^-_{s_1} \cdot \tau_{s_0}) \otimes \beta^-_{v'} \\
&= 0.
\end{aligned}$$

We now treat the case $\ell(v) = 0$, i.e., without loss of generality $v = 1$. We recall that we have to consider the lines

$$\begin{aligned}
\alpha^-_{s_1} &\longmapsto -\beta^+_1 \otimes \beta^0_{s_1}, \\
\alpha^0_{s_1} &\longmapsto \beta^+_1 \otimes \beta^-_{s_1}, \\
\alpha^+_{s_1} &\longmapsto \beta^0_{s_1} \otimes \beta^+_1,
\end{aligned}$$

we have to multiply both sides by τ_{s_1} and see whether the resulting left hand side is sent to the resulting right hand side, at least modulo K_2. We first observe that from the definition of $\mathcal{R}_2(\alpha^+_1)$ (or rather from the definition of $\mathcal{R}_2(\tau_{c_{-1}} \cdot \alpha^+_1)$) it follows that

$$\mathcal{R}_2(\tau_{s_1} \cdot \alpha^-_{s_1}) = \tau_{s_1} \cdot \mathcal{R}_2(\alpha^-_{s_1}),$$

and hence we only need to consider the last two of the above three lines. Multiplying each side by τ_{s_1} on the left, we get

$$\begin{aligned}
-e_1 \cdot \alpha^0_{s_1} - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \alpha^+_{s_1} &\overset{?}{\longmapsto} \begin{aligned}[t] & e_1 \cdot \beta^+_{s_1} \otimes \beta^+_1 - 2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_1 \\ & -e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^+_1 + \beta^-_{c_{-1}} \otimes \beta^+_1, \end{aligned} \\
-e_1 \cdot \alpha^+_{s_1} &\overset{?}{\longmapsto} -e_1 \cdot \beta^0_{s_1} \otimes \beta^+_1 - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_{s_1} \otimes \beta^+_1.
\end{aligned}$$

Regarding the first line, we have

$$\begin{aligned}
e_1 \cdot \beta^+_{s_1} \otimes \beta^+_1 &= -e_1 \cdot \mathcal{R}_2(\alpha^0_{s_1}), \\
-2e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^0_{s_1} \otimes \beta^+_1 &= -2e_{\underline{\mathrm{id}}^{-1}} \cdot \mathcal{R}_2(\alpha^+_{s_1}), \\
-e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^-_{s_1} \otimes \beta^+_1 &= e_{\underline{\mathrm{id}}^{-2}} \cdot \tau_{s_1} \cdot \beta^+_1 \otimes \beta^+_1 \in K_2, \\
\beta^-_{c_{-1}} \otimes \beta^+_1 &\in K_2.
\end{aligned}$$

Regarding the second line, we have

$$\begin{aligned}
-e_1 \cdot \beta^0_{s_1} \otimes \beta^+_1 &= -e_1 \cdot \mathcal{R}_2(\alpha^+_{s_1}), \\
-e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^-_{s_1} \otimes \beta^+_1 &= e_{\underline{\mathrm{id}}^{-1}} \cdot \tau_{s_1} \cdot \beta^+_1 \otimes \beta^+_1 \in K_2.
\end{aligned}$$

(iii) It remains to check the congruences

$$\begin{aligned}
\mathcal{R}_2(\tau_{s_0} \cdot \alpha^+_1) &\overset{?}{\equiv} \tau_{s_0} \cdot \mathcal{R}_2(\alpha^+_1) \mod K_2, \\
\mathcal{R}_2(\tau_{s_1} \cdot \alpha^+_1) &\overset{?}{\equiv} \tau_{s_1} \cdot \mathcal{R}_2(\alpha^+_1) \mod K_2.
\end{aligned} \tag{176}$$

We start with the second one since it is easier:

$$\begin{aligned}
\tau_{s_1} \cdot \mathcal{R}_2(\alpha_1^+) &= \tau_{s_1} \cdot \Big(\mathcal{R}_2\big(\alpha_1^+ + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}}\big) - \tau_{s_1} \cdot \mathcal{R}_2\big(\alpha^-_{s_1^{-1}}\big)\Big) \\
&\equiv \mathcal{R}_2\big(\tau_{s_1} \cdot (\alpha_1^+ + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}})\big) + e_1 \cdot \tau_{s_1} \cdot \mathcal{R}_2\big(\alpha^-_{s_1^{-1}}\big) \mod K_2 \\
&\qquad \text{by (ii), since } \alpha_1^+ + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}} \in \textstyle\bigoplus_{\omega \in T^0/T^1} H^2(I, \mathbf{X}(\omega)) \\
&= \mathcal{R}_2\big(\tau_{s_1} \cdot (\alpha_1^+ + \tau_{s_1} \cdot \alpha^-_{s_1^{-1}})\big) + \mathcal{R}_2\big(e_1 \cdot \tau_{s_1} \cdot \alpha^-_{s_1^{-1}}\big) \\
&\qquad \text{again by (ii)} \\
&= \mathcal{R}_2(\tau_{s_1} \cdot \alpha_1^+).
\end{aligned}$$

This proves the second congruence in (176), and it remains to check the first one:

$$\begin{aligned}
\tau_{s_0} \cdot \mathcal{R}_2(\alpha_1^+) &= \tau_{s_0} \cdot \Big(e_1 \cdot \beta_1^+ \otimes \beta^0_{s_1} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^+_{s_1} \otimes \beta^+_1 \\
&\qquad + e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^0_{s_1} \otimes \beta^+_1 + \tau_{s_1^{-1}} \cdot \beta^+_1 \otimes \beta^0_{s_1}\Big) \\
&= 0 + 0 - e_{\underline{\mathrm{id}}^2} \cdot \beta^0_{s_0 s_1} \otimes \beta^+_1 + \tau_{s_0 s_1^{-1}} \cdot \beta^+_1 \otimes \beta^0_{s_1} \\
&= -e_{\underline{\mathrm{id}}^2} \cdot \mathcal{R}_2(\alpha^-_{s_0 s_1}) + \tau_{s_0 s_1^{-1}} \cdot \beta^+_1 \otimes \beta^0_{s_1} \\
&\equiv -e_{\underline{\mathrm{id}}^2} \cdot \mathcal{R}_2(\alpha^-_{s_0 s_1}) + \tau_{s_0} \cdot \beta^0_{s_1^{-1}} \otimes \beta^+_1 \cdot \tau_{s_1} \mod K_2 \\
&= -e_{\underline{\mathrm{id}}^2} \cdot \mathcal{R}_2(\alpha^-_{s_0 s_1}) - \beta^0_{s_0 s_1} \otimes \beta^+_1 \cdot \tau_{s_1^{-1}} \\
&= -e_{\underline{\mathrm{id}}^2} \cdot \mathcal{R}_2(\alpha^-_{s_0 s_1}) - \mathcal{R}_2(\alpha^-_{s_0 s_1}) \cdot \tau_{s_1^{-1}}.
\end{aligned}$$

It remains to compute (or rather rewrite) the second term:

$$\begin{aligned}
\mathcal{R}_2(\alpha^-_{s_0 s_1}) \cdot \tau_{s_1^{-1}} &= \mathcal{J}\big(\tau_{s_1} \cdot \mathcal{J}(\mathcal{R}_2(\alpha^-_{s_0 s_1}))\big) && \text{by Lemma 4.5.7} \\
&= \mathcal{J}\big(\tau_{s_1} \cdot \mathcal{R}_2(\mathcal{J}(\alpha^-_{s_0 s_1}))\big) \\
&= \mathcal{J}\big(\tau_{s_1} \cdot \mathcal{R}_2(\alpha^-_{s_1 s_0})\big) \\
&\equiv \mathcal{J}\big(\mathcal{R}_2(\tau_{s_1} \cdot \alpha^-_{s_1 s_0})\big) \mod K_2 && \text{by part (ii) and since } K_2 \text{ is } \mathcal{J}\text{-invariant} \\
&= \mathcal{J}\big(\mathcal{R}_2(-\alpha^+_{c_{-1} s_0} - e_1 \cdot \alpha^-_{s_1 s_0})\big) \\
&= \mathcal{R}_2\big(\mathcal{J}(-\alpha^+_{c_{-1} s_0} - e_1 \cdot \alpha^-_{s_1 s_0})\big) && \text{by Lemma 4.5.7} \\
&= \mathcal{R}_2\big(\alpha^-_{s_0} - \alpha^-_{s_0 s_1} \cdot e_1\big) \\
&= \mathcal{R}_2\big(\alpha^-_{s_0} - e_{\underline{\mathrm{id}}^2} \cdot \alpha^-_{s_0 s_1}\big) && \text{by (85)} \\
&= \mathcal{R}_2\big(-\tau_{s_0}\alpha^+_1 - e_{\underline{\mathrm{id}}^2} \cdot \alpha^-_{s_0 s_1}\big).
\end{aligned}$$

So, putting together the last two computations we see that

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

and this finishes the proof. ■

Proposition 4.5.13. *The kernel of the degree 2 multiplication map*

$$\mathcal{M}_2 \colon T^2_{E_0} E^1 = E^1 \otimes_{E^0} E^1 \longrightarrow E^2$$

is K_2 (defined in Remark 4.5.10).

Proof. When we have defined K_2 we have highlighted that $K_2 \subseteq \ker(\mathcal{M}_2)$. Therefore, it does make sense to consider the map $\overline{\mathcal{M}_2}$ induced by the multiplication map with domain $(E^1 \otimes_{E^0} E^1)/K_2$ and codomain E^2. So we have the following picture:

$$(E^1 \otimes_{E^0} E^1)/K_2 \underset{\overline{\mathcal{R}_2}}{\overset{\overline{\mathcal{M}_2}}{\rightleftarrows}} E^2.$$

By definition $\mathcal{R}_2$ is a section (as a map of k-vector spaces) of the surjection $\mathcal{M}_2$, and hence $\overline{\mathcal{R}_2}$ is a section of the surjection $\overline{\mathcal{M}_2}$, but now $\overline{\mathcal{R}_2}$ is not only a homomorphism of k-vector spaces but also a homomorphism of left E^0-modules (Lemma 4.5.12). Now we would like to show that $\overline{\mathcal{R}_2}$ is also a homomorphism of right E^0-modules. To this end, it is useful to consider the anti-involution: since K_2 is $\mathcal{J}$-invariant (Lemma 4.5.11), we can define an involution $\overline{\mathcal{J}}$ on $(E^1 \otimes_{E^0} E^1)/K_2$ induced by $\mathcal{J}$. It has the following property, analogously to $\mathcal{J}$:

$$\begin{aligned} \overline{\mathcal{J}}(x \cdot \overline{y}) &= \overline{\mathcal{J}}(\overline{y}) \cdot \mathcal{J}(x) \quad \text{for all } x \in E^0 \text{ and all } \overline{y} \in (E^1 \otimes_{E^0} E^1)/K_2, \\ \overline{\mathcal{J}}(\overline{y} \cdot x) &= \mathcal{J}(x) \cdot \overline{\mathcal{J}}(\overline{y}) \quad \text{for all } x \in E^0 \text{ and all } \overline{y} \in (E^1 \otimes_{E^0} E^1)/K_2. \end{aligned} \tag{177}$$

Furthermore, we claim that the following diagram is commutative:

$$\begin{tikzcd} E^2 \arrow[r, "\overline{\mathcal{R}_2}"] \arrow[d, "\mathcal{J}"] & (E^1 \otimes_{E^0} E^1)/K_2 \arrow[d, "\overline{\mathcal{J}}"] \\ E^2 \arrow[r, "\overline{\mathcal{R}_2}"] & (E^1 \otimes_{E^0} E^1)/K_2. \end{tikzcd}$$

Indeed, since $\mathcal{R}_2$ and $\mathcal{J}$ commute on F^1E^2 (Lemma 4.5.7), it is clear that the two composite maps of the diagram coincide on F^1E^2. It remains to show that they coincide on F_0E^2. Since $\mathcal{R}_2$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules, also $\overline{\mathcal{R}_2}$ is, and so, using also formulas (177), we see that both composite maps in the diagram transform multiplication on the left by τ_ω into multiplication on the right by $\tau_{\omega^{-1}}$ (where $\omega \in T^0/T^1$). Therefore, to check that the two composite maps coincide on F_0E^2, it suffices to check that they coincide at α_1^- and at α_1^+. But recall that the following two elements are among the generators of K_2 (see the definition of K_2 in Remark 4.5.10):

$$\begin{gathered} (\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^-) - (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^-), \\ -(\mathcal{R}_2 \circ \mathcal{J})(\alpha_1^+) + (\mathcal{J} \circ \mathcal{R}_2)(\alpha_1^+), \end{gathered}$$

and hence we see that the two composite maps of the diagram coincide at α_1^- and at α_1^+.

This concludes the proof that the above diagram is commutative, and now recall that we wanted to show that $\overline{\mathcal{R}_2}$ is also a homomorphism of right E^0-modules. To show our claim, we put together the fact that $\overline{\mathcal{R}_2}$ is a homomorphism of left E^0-modules, the formulas (177) for $\overline{\mathcal{J}}$ and the fact that the the above diagram is commutative. With these ingredients, we can compute the following chain of equalities, where $x \in E^0$ and $\alpha \in E^2$:

$$\begin{aligned}\overline{\mathcal{R}_2}(\alpha)\cdot x &= (\overline{\mathcal{J}} \circ \overline{\mathcal{J}})\big(\overline{\mathcal{R}_2}(\alpha)\cdot x\big)\\ &= \overline{\mathcal{J}}\big(\mathcal{J}(x)\cdot \overline{\mathcal{J}}(\overline{\mathcal{R}_2}(\alpha))\big)\\ &= \overline{\mathcal{J}}\big(\mathcal{J}(x)\cdot \overline{\mathcal{R}_2}(\mathcal{J}(\alpha))\big)\\ &= \overline{\mathcal{J}}\big(\overline{\mathcal{R}_2}(\mathcal{J}(x)\cdot \mathcal{J}(\alpha))\big)\\ &= \overline{\mathcal{R}_2}\big(\mathcal{J}(\mathcal{J}(x)\cdot \mathcal{J}(\alpha))\big)\\ &= \overline{\mathcal{R}_2}(\alpha\cdot x),\end{aligned}$$

completing the proof that $\overline{\mathcal{R}_2}$ is a homomorphism of right E^0-modules.

So far, we have shown that the surjective map $\overline{\mathcal{M}_2}$ admits a section $\overline{\mathcal{R}_2}$ as a homomorphism of E^0-bimodules. If we show that $\overline{\mathcal{R}_2} \circ \overline{\mathcal{M}_2} = \mathrm{id}_{(E^1 \otimes_{E^0} E^1)/K_2}$, then we are done, because we get that the multiplication map induces an isomorphism between $(E^1 \otimes_{E^0} E^1)/K_2$ and E^2. But, since $\overline{\mathcal{R}_2}$ is a homomorphism of E^0-bimodules, it suffices to check the equality $\overline{\mathcal{R}_2} \circ \overline{\mathcal{M}_2} = \mathrm{id}_{(E^1 \otimes_{E^0} E^1)/K_2}$ on a set of generators of $(E^1 \otimes_{E^0} E^1)/K_2$ as an E^0-bimodule. Namely, we can consider the (classes of) the generators of Lemma 4.5.1: if $y \in E^1 \otimes_{E^0} E^1$ is one of these, then by definition of K_2 we have

$$y - (\mathcal{R}_2 \circ \mathcal{M}_2)(y) \in K_2,$$

and hence in the quotient $(E^1 \otimes_{E^0} E^1)/K_2$ we have

$$\overline{y} = (\overline{\mathcal{R}_2} \circ \overline{\mathcal{M}_2})(\overline{y}),$$

as we wanted to show. ■

Remark 4.5.14. The elements listed in Lemma 4.5.9 do not suffice to generate $\ker(\mathcal{M}_2)$ as an E^0-bimodule. In particular, as explained before such lemma, the map $\mathcal{M}_2$ is not a homomorphism of E^0-bimodules.

Proof. Recall the notation χ_0 for the quadratic character. We consider the following map, which is well-defined because both e_{χ_0} and ζ lie in $Z(E^0)$:

$$\begin{aligned}\psi\colon\ E^1 \otimes_{E^0} E^1 &\longrightarrow E^2\\ x\otimes y &\longmapsto e_{\chi_0}\cdot x\cdot e_{\chi_0}\zeta\cdot y.\end{aligned}$$

Let us consider the elements in the list of Remark 4.5.10 (which, by the last proposition, generate $\ker(\mathcal{M}_2)$ as an E^0-bimodule). Recall that the elements in such list except the last two are exactly the elements listed in Lemma 4.5.9. We compute the image via ψ of all the elements in the list of Remark 4.5.10: since $e_{\chi_0}\cdot \beta_w^{\pm}\cdot e_{\chi_0}$ iz zero for all $w \in \widetilde{W}$ (see formulas (61)) we see that this reduces to compute the image via ψ of the following elements:

$$\begin{array}{llll}\beta^0_{s_1}\otimes\beta^-_1, & \beta^0_{s_0}\otimes\beta^+_1, & \beta^0_{s_1}\otimes\beta^0_{s_0}, & \beta^0_{s_0}\otimes\beta^0_{s_1},\\ \beta^0_{s_0}\otimes\beta^0_{s_0}, & \beta^0_{s_1}\otimes\beta^0_{s_1}, & \beta^0_{s_0}\otimes\beta^-_{s_0}, & \beta^0_{s_1}\otimes\beta^+_{s_1}.\end{array}$$

Moreover, from the fact that $\beta^{0,\star}_{s_i}$ (for $i \in \{0,1\}$) commutes with ζ (and with e_{χ_0}), looking at the definition of $\beta^{0,\star}_{s_i}$ (see (71)), it is not difficult to see that $\beta^0_{s_i}$ commutes with $e_{\chi_0}\zeta$. But then

$$\begin{aligned}\psi(\beta^0_{s_1}\otimes\beta^-_1) &= e_{\chi_0}\cdot\beta^0_{s_1}\cdot e_{\chi_0}\zeta\cdot\beta^-_1\\ &= e_{\chi_0}\zeta\cdot\beta^0_{s_1}\cdot\beta^-_1\\ &= 0,\end{aligned}$$

because we know that $\beta^0_{s_1} \cdot \beta^-_1 \in \ker(\mathcal{M}_2)$. Similarly, we see that ψ is zero at $\beta^0_{s_0} \otimes \beta^+_1$, $\beta^0_{s_1} \otimes \beta^0_{s_0}$ and at $\beta^0_{s_0} \otimes \beta^0_{s_1}$.

For the elements $\beta^0_{s_0} \otimes \beta^0_{s_0}$ and $\beta^0_{s_1} \otimes \beta^0_{s_1}$ the principle is similar, because, although they do not lie in $\ker(\mathcal{M})$, looking again at the list in Remark 4.5.10 from which they were obtained, we see that their product with e_{χ_0} on the left does lie in $\ker(\mathcal{M})$.

We have thus shown that the image via ψ of all the elements in the list in Remark 4.5.10 is zero, except at most the last two.

If we show that at least one of these two elements has nonzero image, than we have shown that the sub-bimodule generated by all the elements in the list except the last two (i.e., by the elements listed in Lemma 4.5.9) is strictly smaller that $\ker(\mathcal{M}_2)$, and we are done.

Hence, it suffices to show that $\psi\big(\beta^+_{s_0} \otimes \beta^0_{s_0} + \beta^0_{s_0} \otimes \beta^-_{s_0}\big)$ is nonzero (ie., by what we said before, that $\psi(\beta^0_{s_0} \otimes \beta^-_{s_0})$ is nonzero). In (173) we have computed that $\beta^0_{s_0^{-1}} \cdot \zeta \cdot \beta^-_{s_0}$ is nonzero and actually stays nonzero when multiplied on the left by e_{χ_0}. Hence the same is true for

$$\begin{aligned} \psi(\beta^0_{s_0} \otimes \beta^-_{s_0}) &= e_{\chi_0} \cdot \beta^0_{s_0} \cdot e_{\chi_0} \zeta \cdot \beta^-_{s_0} \\ &= e_{\chi_0} \tau_{c_{-1}} \cdot \beta^0_{s_0^{-1}} \cdot \zeta \cdot \beta^-_{s_0}. \end{aligned}$$

This conclues the proof of the remark. ∎

4.6 The kernel in degree 3

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. The elements $(\beta^-_w)_w$, $(\beta^0_w)_w$, $(\beta^+_w)_w$, $(\alpha^-_w)_w$, $(\alpha^0_w)_w$, $(\alpha^+_w)_w$, and $(\phi_w)_w$ are chosen as in Subsection 4.5.a.

Recall that we are considering the multiplication map

$$\mathcal{M} \colon T^*_{E^0} E^1 \longrightarrow E^*$$

and that in Subsection 4.5.c we have defined a section of its 2^{nd} graded piece $\mathcal{M}_2$ (as a map of k-vector spaces)

$$\mathcal{R}_2 \colon E^2 \longrightarrow T^2_{E^0} E^1$$

in order to compute $\ker(\mathcal{M}_2)$. We are going to work in the same way for the 3^{rd} graded piece $\mathcal{M}_3$.

4.6.a A section of the multiplication map in degree 3

In the proof of Lemma 4.1.1 and in Remark 4.1.2 (in particular, see Equations (155), (156) and (157)) we have obtained the following formulas:

$$\begin{aligned} \beta^-_1 \cdot \beta^0_{s_0(s_1 s_0)^i} \cdot \beta^-_1 &= -\beta^-_{s_0(s_1 s_0)^i} \smile \beta^0_{s_0(s_1 s_0)^i} \smile \beta^+_{s_0(s_1 s_0)^i}, \\ \beta^+_1 \cdot \beta^0_{s_1(s_0 s_1)^i} \cdot \beta^+_1 &= -\beta^+_{s_1(s_0 s_1)^i} \smile \beta^0_{s_1(s_0 s_1)^i} \smile \beta^-_{s_1(s_0 s_1)^i}, \\ \beta^-_1 \cdot \beta^0_{(s_0 s_1)^i} \cdot \beta^+_1 &= \beta^-_{(s_0 s_1)^i} \smile \beta^0_{(s_0 s_1)^i} \smile \beta^+_{(s_0 s_1)^i}, \\ \beta^+_1 \cdot \beta^0_{(s_1 s_0)^i} \cdot \beta^-_1 &= \beta^+_{(s_1 s_0)^i} \smile \beta^0_{(s_1 s_0)^i} \smile \beta^-_{(s_1 s_0)^i}. \end{aligned}$$

Recall that with our notation we have that, for all $w \in \widetilde{W}$ with $\ell(w) \geqslant 1$,

$$\phi_w = \beta_w^- \smile \beta_w^0 \smile \beta_w^+$$

(formula (165)), and hence we deduce the following formulas:

$$\begin{aligned}
\beta_1^- \cdot \beta^0_{s_0(s_1s_0)^i} \cdot \beta_1^- &= -\phi_{s_0(s_1s_0)^i}, \\
\beta_1^+ \cdot \beta^0_{s_1(s_0s_1)^i} \cdot \beta_1^+ &= \phi_{s_1(s_0s_1)^i}, \\
\beta_1^- \cdot \beta^0_{(s_0s_1)^i} \cdot \beta_1^+ &= \phi_{(s_0s_1)^i}, \\
\beta_1^+ \cdot \beta^0_{(s_1s_0)^i} \cdot \beta_1^- &= -\phi_{(s_1s_0)^i}.
\end{aligned}$$

This, together with the fact that $(\tau_{s_0} + e_1) \cdot \phi_{s_0^{-1}} = \phi_1$, shows that the following is a section of the multiplication map $T^3_{E^0} E^1 \longrightarrow E^3$, as a map of k-vector spaces (the last line is defined in terms of the lines above):

$$\begin{aligned}
\mathcal{R}_3\colon \qquad E^3 &\longrightarrow T^3_{E^0} E^1 = E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 \\
\tau_\omega \cdot \phi_{(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^+ \otimes \beta^0_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \phi_{(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^- \otimes \beta^0_{(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \phi_{s_0(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \phi_{s_1(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\
\tau_\omega \cdot \phi_1 &\longmapsto \tau_\omega \cdot (\tau_{s_0} + e_1) \cdot \mathcal{R}_3(\phi_{s_0^{-1}}) && \text{for } \omega \in T^0/T^1.
\end{aligned} \tag{178}$$

Lemma 4.6.1. *The map defined exactly as $\mathcal{R}_3$ but by putting multiplication by τ_ω (for $\omega \in T^0/T^1$) on the right everywhere instead of on the left everywhere is actually the same map as $\mathcal{R}_3$. In other words, the map $\mathcal{R}_3$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules.*

Proof. We proceed as in Lemma 4.5.5. Namely, we still use the notation ω_u for $u \in \mathbb{F}_p^\times$ as in (59) and (60) and we use the formulas describing the structure of E^1 and E^3 as $k\left[T^0/T^1\right]$-bimodules (i.e., respectively, the two formulas just mentioned and (89)) to "move τ_{ω_u} on the right" in the definition of $\mathcal{R}_3$ (178). More precisely, for the moment let us start by considering only the first four lines in the definition of $\mathcal{R}_3$:

$$\begin{aligned}
\tau_{\omega_u} \cdot \phi_{(s_1s_0)^i} &\longmapsto -\tau_{\omega_u} \cdot \beta_1^+ \otimes \beta^0_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ u \in \mathbb{F}_p^\times, \\
\tau_{\omega_u} \cdot \phi_{(s_0s_1)^i} &\longmapsto \tau_{\omega_u} \cdot \beta_1^- \otimes \beta^0_{(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ u \in \mathbb{F}_p^\times, \\
\tau_{\omega_u} \cdot \phi_{s_0(s_1s_0)^i} &\longmapsto -\tau_{\omega_u} \cdot \beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ u \in \mathbb{F}_p^\times, \\
\tau_{\omega_u} \cdot \phi_{s_1(s_0s_1)^i} &\longmapsto \tau_{\omega_u} \cdot \beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ u \in \mathbb{F}_p^\times.
\end{aligned}$$

By the formulas describing the structure of E^3 as a $k\left[T^0/T^1\right]$-bimodule we have that, for $w \in \widetilde{W}$ and for $u \in \mathbb{F}_p^\times$, the product $\tau_{\omega_u} \cdot \phi_w$ is either equal to $\phi_w \cdot \tau_{\omega_u}$ or to $\phi_w \cdot \tau_{\omega_u^{-1}}$ depending on the length of w: so we replace the left hand side of each of the four above lines accordingly, and similarly we start applying the formulas describing the structure of E^1 as a $k\left[T^0/T^1\right]$-bimodule on the right hand side, getting that:

$$\begin{aligned}
\phi_{(s_1s_0)^i}\cdot\tau_{\omega_u} &\longmapsto -u^2\beta_1^+\otimes(\tau_{\omega_u}\cdot\beta^0_{(s_1s_0)^i})\otimes\beta_1^-,\\
\phi_{(s_0s_1)^i}\cdot\tau_{\omega_u} &\longmapsto u^{-2}\beta_1^-\otimes(\tau_{\omega_u}\cdot\beta^0_{(s_0s_1)^i})\otimes\beta_1^+,\\
\phi_{s_0(s_1s_0)^i}\cdot\tau_{\omega_u^{-1}} &\longmapsto -u^{-2}\beta_1^-\otimes(\tau_{\omega_u}\cdot\beta^0_{s_0(s_1s_0)^i})\otimes\beta_1^-,\\
\phi_{s_1(s_0s_1)^i}\cdot\tau_{\omega_u^{-1}} &\longmapsto u^2\beta_1^+\otimes(\tau_{\omega_u}\cdot\beta^0_{s_1(s_0s_1)^i})\otimes\beta_1^+.
\end{aligned}$$

We continue the computation on the right, getting that

$$\begin{aligned}
\phi_{(s_1s_0)^i}\cdot\tau_{\omega_u} &\longmapsto -u^2\beta_1^+\otimes\beta^0_{(s_1s_0)^i}\otimes(\tau_{\omega_u}\cdot\beta_1^-),\\
\phi_{(s_0s_1)^i}\cdot\tau_{\omega_u} &\longmapsto u^{-2}\beta_1^-\otimes\beta^0_{(s_0s_1)^i}\otimes(\tau_{\omega_u}\cdot\beta_1^+),\\
\phi_{s_0(s_1s_0)^i}\cdot\tau_{\omega_u^{-1}} &\longmapsto -u^{-2}\beta_1^-\otimes\beta^0_{s_0(s_1s_0)^i}\otimes(\tau_{\omega_u^{-1}}\cdot\beta_1^-),\\
\phi_{s_1(s_0s_1)^i}\cdot\tau_{\omega_u^{-1}} &\longmapsto u^2\beta_1^+\otimes\beta^0_{s_1(s_0s_1)^i}\otimes(\tau_{\omega_u^{-1}}\cdot\beta_1^+).
\end{aligned}$$

And finally we obtain

$$\begin{aligned}
\phi_{(s_1s_0)^i}\cdot\tau_{\omega_u} &\longmapsto -u^2\beta_1^+\otimes\beta^0_{(s_1s_0)^i}\otimes u^{-2}\beta_1^-\cdot\tau_{\omega_u},\\
\phi_{(s_0s_1)^i}\cdot\tau_{\omega_u} &\longmapsto u^{-2}\beta_1^-\otimes\beta^0_{(s_0s_1)^i}\otimes u^2\beta_1^+\cdot\tau_{\omega_u},\\
\phi_{s_0(s_1s_0)^i}\cdot\tau_{\omega_u^{-1}} &\longmapsto -u^{-2}\beta_1^-\otimes\beta^0_{s_0(s_1s_0)^i}\otimes(u^{-1})^{-2}\beta_1^-\cdot\tau_{\omega_u^{-1}},\\
\phi_{s_1(s_0s_1)^i}\cdot\tau_{\omega_u^{-1}} &\longmapsto u^2\beta_1^+\otimes\beta^0_{s_1(s_0s_1)^i}\otimes(u^{-1})^2\beta_1^+\cdot\tau_{\omega_u^{-1}}.
\end{aligned}$$

This shows that, at least for the first four lines in the definition of $\mathcal{R}_3$ (178) we could have used multiplication by τ_{ω_u} on the right instead of on the left. Now we look at the last line:

$$\tau_{\omega_u}\cdot\phi_1\longmapsto\tau_{\omega_u}\cdot(\tau_{s_0}+e_1)\cdot\mathcal{R}_3(\phi_{s_0^{-1}})\qquad\text{for } u\in\mathbb{F}_p^\times.$$

We already know the behaviour of $\mathcal{R}_3(\phi_{s_0^{-1}})$ with respect to multiplication by τ_{ω_u}, and we can thus compute that the element $\phi_1\cdot\tau_{\omega_u}$, which is equal to $\tau_{\omega_u}\cdot\phi_1$, is mapped to

$$\begin{aligned}
\tau_{\omega_u}\cdot(\tau_{s_0}+e_1)\cdot\mathcal{R}_3(\phi_{s_0^{-1}}) &= (\tau_{s_0}+e_1)\cdot\tau_{\omega_u^{-1}}\cdot\mathcal{R}_3(\phi_{s_0^{-1}})\\
&= (\tau_{s_0}+e_1)\cdot\mathcal{R}_3(\phi_{s_0^{-1}})\cdot\tau_{\omega_u},
\end{aligned}$$

thus completing the proof. ■

We will see that the map $\mathcal{R}_3$ is not invariant for Γ_ϖ nor for $\mathcal{J}$, the problem being the last line (see Remark 4.9.14). However, it is possible to define a new section $\mathcal{R}_3'$ which is both Γ_ϖ-invariant and $\mathcal{J}$-invariant, as we will see in the next lemma.

Lemma 4.6.2. *Let us consider the map*

$$\begin{aligned}
\mathcal{R}_3'\colon E^3 &\longrightarrow T^3_{E^0}E^1 = E^1\otimes_{E^0}E^1\otimes_{E^0}E^1\\
\phi_w &\longmapsto \begin{cases}\mathcal{R}_3(\phi_w) & \text{if } \ell(w)\geqslant 1,\\ \frac{1}{4}\tau_w\cdot\Big(\mathcal{R}_3(\phi_1)+\Gamma_\varpi(\mathcal{R}_3(\phi_1)) \\ \qquad +\mathcal{J}(\mathcal{R}_3(\phi_1))+\Gamma_\varpi(\mathcal{J}(\mathcal{R}_3(\phi_1)))\Big) & \text{if } \ell(w)=0.\end{cases}
\end{aligned}$$

One has that $\mathcal{R}'_3$ is a section of the multiplication map $\mathcal{M}_3$ as a homomorphism of $k\left[T^0/T^1\right]$-bimodules and that it commutes with Γ_ϖ and with $\mathcal{J}$.

Proof. We have to prove four facts: that $\mathcal{R}'_3$ is a section of the multiplication map $\mathcal{M}_3$, that it is a homomorphism of $k\left[T^0/T^1\right]$-bimodules, that it commutes with Γ_ϖ and that it commutes with $\mathcal{J}$.

- Since $\mathcal{R}_3$ is a section of the multiplication map, $\mathcal{R}'_3$ is a section of the multiplication map as well, because the multiplication map commutes with Γ_ϖ and $\mathcal{J}$ (see (163) and (164)) and because $\Gamma_\varpi(\phi_1) = \phi_1 = \mathcal{J}(\phi_1)$.

- Let us prove that $\mathcal{R}'_3$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules. Using the formulas

$$\begin{aligned} \tau_\omega \cdot \Gamma_\varpi(x) &= \Gamma_\varpi(\tau_{\omega^{-1}} \cdot x), \\ \Gamma_\varpi(x) \cdot \tau_\omega &= \Gamma_\varpi(x \cdot \tau_{\omega^{-1}}), \\ \tau_\omega \cdot \mathcal{J}(x) &= \mathcal{J}(x \cdot \tau_{\omega^{-1}}), \\ \mathcal{J}(x) \cdot \tau_\omega &= \mathcal{J}(\tau_{\omega^{-1}} \cdot x) \end{aligned} \tag{179}$$

  (where $\omega \in T^0/T^1$ and $x \in E^*$ or $x \in T^*_{E^0}E^1$) it is easy to see that

$$\tau_\omega \cdot \mathcal{R}'_3(\phi_1) = \mathcal{R}'_3(\phi_1) \cdot \tau_\omega.$$

  Then, as in Lemma 4.6.1, we have that the map defined exactly as $\mathcal{R}'_3$ but by putting multiplication by τ_ω (for $\omega \in T^0/T^1$) on the right everywhere instead of on the left everywhere is actually the same map as $\mathcal{R}'_3$. In particular, the map $\mathcal{R}'_3$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules.

- Let us show that the map $\mathcal{R}'$ commutes with Γ_ϖ. We first look at the following lines in the definition of $\mathcal{R}'_3$ (equivalently, of $\mathcal{R}_3$):

$$\begin{aligned} \tau_\omega \cdot \phi_{(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^+ \otimes \beta^0_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\ \tau_\omega \cdot \phi_{(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^- \otimes \beta^0_{(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\ \tau_\omega \cdot \phi_{s_0(s_1s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\ \tau_\omega \cdot \phi_{s_1(s_0s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1. \end{aligned}$$

  We apply Γ_ϖ on both sides and we check that the left hand side is again sent to the right hand side by $\mathcal{R}'_3$ (equivalently, by $\mathcal{R}_3$).

$$\begin{aligned} \tau_{\omega^{-1}} \cdot \phi_{(s_0s_1)^i} &\overset{?}{\longmapsto} \tau_{\omega^{-1}} \cdot \beta_1^- \otimes \beta^0_{(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\ \tau_{\omega^{-1}} \cdot \phi_{(s_1s_0)^i} &\overset{?}{\longmapsto} -\tau_{\omega^{-1}} \cdot \beta_1^+ \otimes \beta^0_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\ \omega \in T^0/T^1, \\ \tau_{\omega^{-1}} \cdot \phi_{s_1(s_0s_1)^i} &\overset{?}{\longmapsto} \tau_{\omega^{-1}} \cdot \beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1, \\ \tau_{\omega^{-1}} \cdot \phi_{s_0(s_1s_0)^i} &\overset{?}{\longmapsto} -\tau_{\omega^{-1}} \cdot \beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1. \end{aligned}$$

  As expected, $\mathcal{R}'_3$ sends the left hand side to the right hand side. Furthermore, it is immediate to check that

$$\Gamma_\varpi(\mathcal{R}'_3(\phi_\omega)) = \mathcal{R}'_3(\Gamma_\varpi(\phi_\omega))$$

  for all $\omega \in T^0/T^1$.

- Let us show that the map $\mathcal{R}'$ commutes with $\mathcal{J}$. We again look at the following lines in the definition of $\mathcal{R}'_3$ (equivalently, of $\mathcal{R}_3$):

$$\begin{aligned}
\tau_\omega \cdot \phi_{(s_1 s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^+ \otimes \beta^0_{(s_1 s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\, \omega \in T^0/T^1,\\
\tau_\omega \cdot \phi_{(s_0 s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^- \otimes \beta^0_{(s_0 s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 1},\, \omega \in T^0/T^1,\\
\tau_\omega \cdot \phi_{s_0(s_1 s_0)^i} &\longmapsto -\tau_\omega \cdot \beta_1^- \otimes \beta^0_{s_0(s_1 s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\, \omega \in T^0/T^1,\\
\tau_\omega \cdot \phi_{s_1(s_0 s_1)^i} &\longmapsto \tau_\omega \cdot \beta_1^+ \otimes \beta^0_{s_1(s_0 s_1)^i} \otimes \beta_1^+ && \text{for } i \in \mathbb{Z}_{\geqslant 0},\, \omega \in T^0/T^1.
\end{aligned}$$

We apply $\mathcal{J}$ on both sides and we check that the left hand side is again sent to the right hand side by $\mathcal{R}'_3$ (equivalently, by $\mathcal{R}_3$):

$$\begin{aligned}
\phi_{(s_0 s_1)^i} \cdot \tau_{\omega^{-1}} &\xmapsto{\ ?\ } \beta_1^- \otimes \beta^0_{(s_0 s_1)^i} \otimes \beta_1^+ \cdot \tau_{\omega^{-1}} && \text{for } i \in \mathbb{Z}_{\geqslant 1},\, \omega \in T^0/T^1,\\
\phi_{(s_1 s_0)^i} \cdot \tau_{\omega^{-1}} &\xmapsto{\ ?\ } -\beta_1^+ \otimes \beta^0_{(s_1 s_0)^i} \otimes \beta_1^- \cdot \tau_{\omega^{-1}} && \text{for } i \in \mathbb{Z}_{\geqslant 1},\, \omega \in T^0/T^1,\\
\phi_{s_0(s_1 s_0)^i} \cdot \tau_{c_{-1}\omega^{-1}} &\xmapsto{?} -\beta_1^- \otimes (\beta^0_{s_0(s_1 s_0)^i} \cdot \tau_{c_{-1}}) \otimes \beta_1^- \cdot \tau_{\omega^{-1}} && \text{for } i \in \mathbb{Z}_{\geqslant 0},\, \omega \in T^0/T^1,\\
\phi_{s_1(s_0 s_1)^i} \cdot \tau_{c_{-1}\omega^{-1}} &\xmapsto{?} \beta_1^+ \otimes (\beta^0_{s_1(s_0 s_1)^i} \cdot \tau_{c_{-1}}) \otimes \beta_1^+ \cdot \tau_{\omega^{-1}} && \text{for } i \in \mathbb{Z}_{\geqslant 0},\, \omega \in T^0/T^1.
\end{aligned}$$

Using that $\mathcal{R}'_3$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules, we see that, as expected, $\mathcal{R}'_3$ sends the left hand side to the right hand side. Furthermore, using that $\mathcal{J}$ and Γ_ϖ commute (see (49)), it is immediate to check that

$$\mathcal{J}(\mathcal{R}'_3(\phi_1)) = \mathcal{R}'_3(\mathcal{J}(\phi_1)).$$

Using again that $\mathcal{R}'_3$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules and using the formulas (179), we also see that $\mathcal{J}(\mathcal{R}'_3(\phi_\omega)) = \mathcal{R}'_3(\mathcal{J}(\phi_1\omega))$ for all $\omega \in T^0/T^1$. ∎

Remark 4.6.3. For later use, let us compute explicitly the four summands in the definition of $\mathcal{R}'_3(\phi_1)$:

$$\begin{aligned}
\mathcal{R}_3(\phi_1) &= (\tau_{s_0} + e_1) \cdot \mathcal{R}_3(\phi_{s_0^{-1}})\\
&= (\tau_{s_0} + e_1) \cdot (-\beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-)\\
&= -(\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-,\\
\Gamma_\varpi(\mathcal{R}_3(\phi_1)) &= \Gamma_\varpi\big(-(\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-\big)\\
&= (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta_1^+,\\
\mathcal{J}(\mathcal{R}_3(\phi_1)) &= \mathcal{J}\big(-(\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-\big)\\
&= -\beta_1^- \otimes \beta^0_{s_0} \otimes \beta_1^- \cdot (\tau_{s_0^{-1}} + e_1),\\
\Gamma_\varpi(\mathcal{J}(\mathcal{R}_3(\phi_1))) &= \Gamma_\varpi\big(-\beta_1^- \otimes \beta^0_{s_0} \otimes \beta_1^- \cdot (\tau_{s_0^{-1}} + e_1)\big)\\
&= \beta_1^+ \otimes \beta^0_{s_1} \otimes \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1).
\end{aligned}$$

4.6.b Computation of the kernel in degree 3

Lemma 4.6.4. *Let $K_{2,3}$ be the sub-E^0-bimodule of $T^3_{E^0}E^1$ generated by the kernel of the degree 2 multiplication map, i.e.,*

$$K_{2,3} \coloneqq \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \subseteq T^3_{E^0}E^1,$$

where $\overline{(?)}$ *denotes the image of* $(?)$ *in* $T^3_{E^0}E^1$. *One has the following congruences:*

$$\Gamma_\varpi(\mathfrak{J}(\mathcal{R}_3(\phi_1))) \equiv \mathcal{R}_3(\phi_1) \mod K_{2,3},$$
$$\mathfrak{J}(\mathcal{R}_3(\phi_1)) \equiv \Gamma_\varpi(\mathcal{R}_3(\phi_1)) \mod K_{2,3}.$$

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, as shown in (163)). To show the first congruence, we first compute a couple of useful equalities and congruences:

$$\begin{aligned}(\tau_{s_0} + e_1) \cdot \beta_1^- \cdot \tau_{s_0} &= (\tau_{s_0} + e_1) \cdot \beta_{s_0}^- \\ &= -2e_{\underline{\mathrm{id}}}\beta^0_{s_0} + e_{\underline{\mathrm{id}}^2}\beta^+_{s_0} - \beta^+_{c_{-1}}.\end{aligned}$$

Since both $\beta^0_{s_0} \otimes \beta^0_{s_1}$ and $\beta^+_{s_0} \otimes \beta^0_{s_1} = -\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_1}$ lie in $\ker(\mathcal{M}_2)$, tensoring both sides of the last equality by $\beta^0_{s_1}$ we get the congruence

$$(\tau_{s_0} + e_1) \cdot \beta_1^- \cdot \tau_{s_0} \otimes \beta^0_{s_1} \equiv -\beta_1^+ \otimes \beta^0_{s_1^{-1}} \mod \ker(\mathcal{M}_2). \tag{180}$$

Now we apply Γ_ϖ to the last congruence, obtaining again a congruence since $\ker(\mathcal{M}_2)$ is Γ_ϖ-invariant:

$$-(\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot \tau_{s_1} \otimes \beta^0_{s_0} \equiv \beta_1^- \otimes \beta^0_{s_0^{-1}} \mod \ker(\mathcal{M}_2).$$

Now we apply $\mathfrak{J}$ (or rather $-\mathfrak{J}$) to the last congruence, obtaining again a congruence since $\ker(\mathcal{M}_2)$ is $\mathfrak{J}$-invariant:

$$-\mathfrak{J}(\beta^0_{s_0}) \otimes \mathfrak{J}\big((\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot \tau_{s_1}\big) \equiv \mathfrak{J}(\beta^0_{s_0^{-1}}) \otimes \mathfrak{J}(\beta_1^-) \mod \ker(\mathcal{M}_2),$$

i.e.,

$$\beta^0_{s_0} \otimes \tau_{s_1} \cdot \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1) \equiv -\beta^0_{s_0} \otimes \beta_1^- \mod \ker(\mathcal{M}_2). \tag{181}$$

We now get the desired congruence $\Gamma_\varpi(\mathfrak{J}(\mathcal{R}_3(\phi_1))) \equiv \mathcal{R}_3(\phi_1)$ modulo $K_{2,3}$, by putting together (180) and (181):

$$\begin{aligned}&\Gamma_\varpi(\mathfrak{J}(\mathcal{R}_3(\phi_1))) \\ &\quad = \beta_1^+ \otimes \beta^0_{s_1} \otimes \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1) \\ &\quad \equiv -\tau_{c_{-1}} \cdot (\tau_{s_0} + e_1) \cdot \beta_1^- \cdot \tau_{s_0} \otimes \beta^0_{s_1} \otimes \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1) \mod K_{2,3} \\ &\qquad\qquad \text{by (180)} \\ &\quad = \tau_{c_{-1}} \cdot (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \tau_{s_1} \cdot \beta_1^+ \cdot (\tau_{s_1^{-1}} + e_1) \\ &\quad \equiv -\tau_{c_{-1}} \cdot (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \beta_1^- \mod K_{2,3} \\ &\qquad\qquad \text{by (181)} \\ &\quad = \mathcal{R}_3(\phi_1).\end{aligned}$$

■

Lemma 4.6.5. *As in the last lemma, let* $K_{2,3}$ *be the sub-*E^0*-bimodule of* $T^3_{E^0}E^1$ *generated by the kernel of the degree* 2 *multiplication map, i.e.,*

$$K_{2,3} \coloneqq \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \subseteq T^3_{E^0}E^1,$$

where $\overline{(?)}$ *denotes the image of* $(?)$ *in* $T^3_{E^0}E^1$. *Furthermore, let* $K_{\mathrm{extra},3}$ *be the sub-left-*$k\left[T^0/T^1\right]$*-module generated by the following element:*

$$\begin{aligned}&\Gamma_\varpi(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1) \\ &\quad = (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-.\end{aligned}$$

One has that the kernel $\ker(\mathcal{M}_3)$ *of the multiplication map in degree* 3 *coincides with* $K_{2,3} + K_{\mathrm{extra},3}$. *Furthermore,* $K_{\mathrm{extra},3}$ *is also the sub-right-*$k\left[T^0/T^1\right]$*-module generated by the above element.*

Proof. The last claim is easy to see because we know from Lemma 4.6.1 that $\mathcal{R}_3$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules, and so for all $\omega \in T^0/T^1$ we have

$$\begin{aligned}\tau_\omega \cdot \big(\Gamma_\varpi(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1)\big) &= \Gamma_\varpi\big(\tau_{\omega^{-1}} \cdot \mathcal{R}_3(\phi_1)\big) - \tau_\omega \cdot \mathcal{R}_3(\phi_1) \\ &= \Gamma_\varpi\big(\mathcal{R}_3(\phi_{\omega^{-1}})\big) - \mathcal{R}_3(\phi_\omega) \\ &= \Gamma_\varpi\big(\mathcal{R}_3(\phi_1) \cdot \tau_{\omega^{-1}}\big) - \mathcal{R}_3(\phi_1) \cdot \tau_\omega \\ &= \big(\Gamma_\varpi(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1)\big) \cdot \tau_\omega.\end{aligned}$$

We now turn to the proof of the fact that $\ker(\mathcal{M}_3)$ coincides with $K_{2,3} + K_{\mathrm{extra},3}$. We reformulate this claim as follows: defining

$$V \coloneqq K_{2,3} + K_{\mathrm{extra},3} + \mathrm{Image}(\mathcal{R}_3') \subseteq T^3_{E^0}E^1,$$

we see that we have to prove that $V = T^3_{E^0}E^1$ (i.e., the inclusion from right to left): indeed assuming that we have already achieved this, we get that

$$K_{2,3} + K_{\mathrm{extra},3} + \mathrm{Image}(\mathcal{R}_3') = \ker(\mathcal{M}_3) \oplus \mathrm{Image}(\mathcal{R}_3'),$$

and this, together with the "easy inclusion" $K_{2,3}+K_{\mathrm{extra},3} \subseteq \ker(\mathcal{M}_3)$, shows that we have $K_{2,3}+K_{\mathrm{extra},3} = \ker(\mathcal{M}_3)$, as we wanted (for the inclusion $K_{\mathrm{extra},3} \subseteq \ker(\mathcal{M}_3)$, recall from Subsection 4.5.a that Γ_ϖ commutes with $\mathcal{M}$).

To reduce the amount of computations, we first make some preliminary observations.

a) We remark that one has the congruences

$$\Gamma_\varpi(\mathcal{J}(\phi_1)) \equiv \mathcal{R}_3(\phi_1) \equiv \Gamma_\varpi(\mathcal{R}_3(\phi_1)) \equiv \mathcal{J}(\mathcal{R}_3(\phi_1)) \mod K_{2,3} + K_{\mathrm{extra},3}.$$

Indeed the first and last congruence are even true modulo $K_{2,3}$ (Lemma 4.6.4), while the second congruence trivially holds by definition of $K_{\mathrm{extra},3}$. Looking at the definition of $\mathcal{R}_3'$, this shows that

$$\mathcal{R}_3'(\phi_1) \equiv \mathcal{R}_3(\phi_1) \mod K_{2,3} + K_{\mathrm{extra},3}. \tag{182}$$

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 $\mathcal{M}_2$.
- ⋆ The term $\mathrm{Image}(\mathcal{R}_3')$ is invariant for Γ_ϖ and $\mathcal{J}$ because these involutions commute with $\mathcal{R}_3'$ (Lemma 4.6.2).
- ⋆ The term $K_{\mathrm{extra},3}$ is visibly invariant for Γ_ϖ. Moreover, applying $\mathcal{J}$ to the difference $\Gamma_\varpi(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1)$ (using that Γ_ϖ and $\mathcal{J}$ commute, see (49)) we get $\Gamma_\varpi(\mathcal{J}(\mathcal{R}_3(\phi_1))) - \mathcal{J}(\mathcal{R}_3(\phi_1))$, which lies in $K_{2,3}+K_{\mathrm{extra},3}$ by part a). This, taking also into account the behaviour of $\mathcal{J}$ with respect to multiplication by τ_ω for $\omega \in T^0/T^1$, proves that $\mathcal{J}(K_{\mathrm{extra},3}) \subseteq K_{2,3} + K_{\mathrm{extra},3}$.

c) We further remark that V is a sub-$k\left[T^0/T^1\right]$-bimodule of $T^3_{E^0}E^1$: indeed the term $K_{2,3}$ is clearly even a sub-E^0-bimodule, the term $K_{\mathrm{extra},3}$ is by definition a sub-$k\left[T^0/T^1\right]$-bimodule and the term $\mathrm{Image}(\mathcal{R}_3')$ is a sub-$k\left[T^0/T^1\right]$-bimodule because $\mathcal{R}_3'$ is a homomorphism of $k\left[T^0/T^1\right]$-bimodules (Lemma 4.6.2).

Now we can start the actual proof of the lemma. Let us consider $x \in T^3_{E^0} E^1$ 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 $z' \in \mathrm{Image}(\mathcal{R}_2)$. Looking at the explicit definition of $\mathcal{R}_2$ (170), we see that every $z' \in \mathrm{Image}(\mathcal{R}_2)$ can be written as a sum of simple tensors of the following forms:

$$\begin{aligned}
&u \otimes \beta_1^- && \text{for some } u \in E^1,\\
&u \otimes \beta_1^+ && \text{for some } u \in E^1,\\
&u \otimes \beta_w^0 && \text{for some } u \in E^1 \text{ and for some } w \in \widetilde{W} \text{ with } \ell(w) \geqslant 1.
\end{aligned}$$

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 form lie in V:

i) $y \otimes u \otimes \beta_1^-$ for some $u \in E^1$,

ii) $y \otimes u \otimes \beta_{s_0 v}^0$ for some $u \in E^1$ and for some $v \in \widetilde{W}$ with $\ell(s_0 v) = \ell(v) + 1$,

because by applying Γ_ϖ to such elements we immediately obtain what is left. We treat separately elements of the forms i) and ii).

i) Let us start the proof that every element of the form

$$y \otimes u \otimes \beta_1^- \qquad \text{(for some } y, u \in E^1\text{)}$$

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 only treat the elements of the form $r \otimes \beta_1^-$ for $r \in \mathrm{Image}(\mathcal{R}_2)$, and, looking at the explicit definition of $\mathcal{R}_2$ (170), we can further assume that $r \otimes \beta_1^-$ is of one of the following forms:

$$\begin{aligned}
&\tau_\omega \beta_1^+ \otimes \beta^0_{(s_1 s_0)^i} \otimes \beta_1^-, \quad \tau_\omega \beta^+_{(s_1 s_0)^i} \otimes \beta_1^- \otimes \beta_1^-, \quad \tau_\omega \beta^0_{(s_1 s_0)^i} \otimes \beta_1^- \otimes \beta_1^-,\\
&\tau_\omega \beta^0_{(s_0 s_1)^i} \otimes \beta_1^+ \otimes \beta_1^-, \quad \tau_\omega \beta^-_{(s_0 s_1)^i} \otimes \beta_1^+ \otimes \beta_1^-, \quad \tau_\omega \beta_1^- \otimes \beta^0_{(s_0 s_1)^i} \otimes \beta_1^-\\
&\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1} \text{ and } \omega \in T^0/T^1,\\
&\tau_\omega \beta^0_{s_0 (s_1 s_0)^i} \otimes \beta_1^- \otimes \beta_1^-, \quad \tau_\omega \beta^-_{s_0 (s_1 s_0)^i} \otimes \beta_1^- \otimes \beta_1^-, \quad \tau_\omega \beta_1^- \otimes \beta^0_{s_0 (s_1 s_0)^i} \otimes \beta_1^-,\\
&\tau_\omega \beta_1^+ \otimes \beta^0_{s_1 (s_0 s_1)^i} \otimes \beta_1^-, \quad \tau_\omega \beta^+_{s_1 (s_0 s_1)^i} \otimes \beta_1^+ \otimes \beta_1^-, \quad \tau_\omega \beta^0_{s_1 (s_0 s_1)^i} \otimes \beta_1^+ \otimes \beta_1^-\\
&\qquad \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and } \omega \in T^0/T^1,\\
&\tau_\omega \tau_{s_0} \mathcal{R}_2\big(\alpha^+_{s_0^{-1}}\big) \otimes \beta_1^- = \tau_\omega \tau_{s_0} \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^- \qquad \text{for } \omega \in T^0/T^1,\\
&\tau_\omega \tau_{s_1} \mathcal{R}_2\big(\alpha^-_{s_1^{-1}}\big) \otimes \beta_1^- = -\tau_\omega \tau_{s_1} \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta_1^- \qquad \text{for } \omega \in T^0/T^1.
\end{aligned}$$

Since the two elements $\beta_1^- \otimes \beta_1^-$ and $\beta_1^+ \otimes \beta_1^-$ lie in $\ker(\mathcal{M}_2)$, we see that many of the above elements lie in V. As we have already remarked that V is a left-$k\left[T^0/T^1\right]$-submodule, we also see that there is no loss of generality in considering only the elements with $\omega = 1$. Therefore, we are reduced to showing that the following elements lie in V:

$$\begin{aligned}
&\beta_1^+ \otimes \beta^0_{(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\\
&\beta_1^- \otimes \beta^0_{(s_0s_1)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 1},\\
&\beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\\
&\beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^- && \text{for } i \in \mathbb{Z}_{\geqslant 0},\\
&\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-,\\
&\tau_{s_1} \cdot \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta_1^-.
\end{aligned} \tag{183}$$

Up to a sign, the first line (respectively, the third line) is exactly $\mathcal{R}'_3(\phi_{(s_0s_1)^i})$ (respectively, $\mathcal{R}'_3(\phi_{s_0(s_1s_0)^i})$), and hence they both lie in V. Moreover, we know that $\beta^0_{s_1} \otimes \beta_1^- \in \ker(\mathcal{M}_2)$, from which it follows that

$$\begin{aligned}
\beta^0_{(s_0s_1)^i} \otimes \beta_1^- &= -\tau_{(s_0s_1)^{i-1}s_0} \cdot \beta^0_{s_1} \otimes \beta_1^- \in \ker(\mathcal{M}_2) && \text{for all } i \in \mathbb{Z}_{\geqslant 1},\\
\beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^- &= \tau_{(s_1s_0)^i} \cdot \beta^0_{s_1} \otimes \beta_1^- \in \ker(\mathcal{M}_2) && \text{for all } i \in \mathbb{Z}_{\geqslant 0}.
\end{aligned}$$

Therefore, it follows that also the second, the fourth and the sixth line in (183) lie in V. It remains to consider the element $\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-$. First of all, we see that there is no harm in considering instead the element $(\tau_{s_0}+e_1)\cdot\beta_1^-\otimes\beta^0_{s_0^{-1}}\otimes\beta_1^- = -\mathcal{R}_3(\phi_1)$, since $e_1\cdot\beta_1^-\otimes\beta^0_{s_0^{-1}}\otimes\beta_1^- \in \mathrm{Image}(\mathcal{R}'_3) \subseteq V$. But we have seen in formula (182) 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 (183) lie in V.

ii) We have to consider the elements of the form

$$y \otimes u \otimes \beta^0_{s_0v} = y \otimes u \otimes \beta^0_{s_0} \cdot \tau_v \qquad \text{(for some } y, u \in E^1)$$

and prove that they lie in V. As before, we can consider the equality

$$y \otimes u \otimes \beta^0_{s_0v} = (y \otimes u - \mathcal{R}_2(\mathcal{M}_2(y \otimes u))) \otimes \beta^0_{s_0v} + \mathcal{R}_2(\mathcal{M}_2(y \otimes u)) \otimes \beta^0_{s_0v},$$

from which we see that we may only treat the elements of the form $r \otimes \beta^0_{s_0v}$ for $r \in \mathrm{Image}(\mathcal{R}_2)$, and, looking at the explicit definition of $\mathcal{R}_2$ (170), we can further assume that $r \otimes \beta^0_{s_0v}$ is of one of the following forms:

$$\begin{aligned}
&\beta_1^+ \otimes \beta^0_{(s_1s_0)^i} \otimes \beta^0_{s_0}\tau_v, \quad \beta_1^+ \otimes \beta^-_{(s_1s_0)^i} \otimes \beta^0_{s_0}\tau_v, \quad \beta^0_{(s_1s_0)^i} \otimes \beta_1^- \otimes \beta^0_{s_0}\tau_v,\\
&\beta^0_{(s_0s_1)^i} \otimes \beta_1^+ \otimes \beta^0_{s_0}\tau_v, \quad \beta_1^- \otimes \beta^+_{(s_0s_1)^i} \otimes \beta^0_{s_0}\tau_v, \quad \beta_1^- \otimes \beta^0_{(s_0s_1)^i} \otimes \beta^0_{s_0}\tau_v\\
&\qquad \text{for } i \in \mathbb{Z}_{\geqslant 1},\\
&\beta^0_{s_0(s_1s_0)^i} \otimes \beta_1^- \otimes \beta^0_{s_0}\tau_v, \quad \beta_1^- \otimes \beta^+_{s_0(s_1s_0)^i} \otimes \beta^0_{s_0}\tau_v, \quad \beta_1^- \otimes \beta^0_{s_0(s_1s_0)^i} \otimes \beta^0_{s_0}\tau_v,\\
&\beta_1^+ \otimes \beta^0_{s_1(s_0s_1)^i} \otimes \beta^0_{s_0}\tau_v, \quad \beta_1^+ \otimes \beta^-_{s_1(s_0s_1)^i} \otimes \beta^0_{s_0}\tau_v, \quad \beta^0_{s_1(s_0s_1)^i} \otimes \beta_1^+ \otimes \beta^0_{s_0}\tau_v\\
&\qquad \text{for } i \in \mathbb{Z}_{\geqslant 0},\\
&\tau_{s_0}\mathcal{R}_2\big(\alpha^+_{s_0^{-1}}\big) \otimes \beta^0_{s_0}\tau_v = \tau_{s_0}\beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta^0_{s_0}\tau_v,\\
&\tau_{s_1}\mathcal{R}_2\big(\alpha^-_{s_1^{-1}}\big) \otimes \beta^0_{s_0}\tau_v = -\tau_{s_1}\beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta^0_{s_0}\tau_v.
\end{aligned}$$

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:

$$\begin{aligned} &\beta_1^- \otimes x \otimes y && \text{for some } x, y \in E^1, \\ &\beta_1^+ \otimes x \otimes y && \text{for some } x, y \in E^1. \end{aligned}$$

This shows that most of the elements in the above list are in V. The remaining ones are:

$$\begin{aligned} &\beta^0_{(s_1 s_0)^i} \otimes \beta_1^- \otimes \beta^0_{s_0} \cdot \tau_v && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ &\beta^0_{(s_0 s_1)^i} \otimes \beta_1^+ \otimes \beta^0_{s_0} \cdot \tau_v && \text{for } i \in \mathbb{Z}_{\geqslant 1}, \\ &\beta^0_{s_0 (s_1 s_0)^i} \otimes \beta_1^- \otimes \beta^0_{s_0} \cdot \tau_v && \text{for } i \in \mathbb{Z}_{\geqslant 0}, \\ &\beta^0_{s_1 (s_0 s_1)^i} \otimes \beta_1^+ \otimes \beta^0_{s_0} \cdot \tau_v && \text{for } i \in \mathbb{Z}_{\geqslant 0}, \\ &\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta^0_{s_0} \cdot \tau_v, \\ &\tau_{s_1} \cdot \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta^0_{s_0} \cdot \tau_v. \end{aligned}$$

We recall from Lemma 4.5.9 that $\beta_1^+ \otimes \beta^0_{s_0} \in \ker(\mathcal{M}_2)$ and that the same is true for $\beta^0_{s_1} \otimes \beta^0_{s_0}$, and so it only remains to consider the following elements:

$$\beta^0_{(s_1 s_0)^i} \otimes \beta_1^- \otimes \beta^0_{s_0} \cdot \tau_v \qquad \text{for } i \in \mathbb{Z}_{\geqslant 1}, \tag{184}$$

$$\beta^0_{s_0 (s_1 s_0)^i} \otimes \beta_1^- \otimes \beta^0_{s_0} \cdot \tau_v \qquad \text{for } i \in \mathbb{Z}_{\geqslant 0}, \tag{185}$$

$$\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta^0_{s_0} \cdot \tau_v. \tag{186}$$

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 4.5.9):

$$\beta^0_{s_0} \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \otimes \beta^0_{s_0} + e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta^+_{s_0}.$$

Tensoring by $\tau_{s_0} \cdot \beta_1^-$ on the left we get

$$\begin{aligned} \tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \beta^0_{s_0} &+ \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \otimes \beta^0_{s_0} \\ &+ \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta_1^- - \tau_{s_0} \cdot \beta_1^- \otimes e_1 \cdot \beta_1^- \otimes \beta^+_{s_0} \\ &\in K_{2,3}. \end{aligned}$$

Since $\beta_1^- \otimes \beta_1^-$ lies in $\ker(\mathcal{R}_2)$, we can delete the two terms where this element appears, getting that

$$\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \beta^0_{s_0} + \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta_1^- \in K_{2,3}.$$

Since $K_{2,3}$ is an E^0-bimodule, we can multiply by τ_v on the right getting that:

$$\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \beta^0_{s_0} \cdot \tau_v + \tau_{s_0} \cdot \beta_1^- \otimes e_{\underline{\mathrm{id}}} \cdot \beta^0_{s_0} \otimes \beta_1^- \cdot \tau_v \in K_{2,3}.$$

If $\ell(v) \geqslant 1$ then v must be of the form $s_1 v'$ for some $v' \in \widetilde{W}$ such that lengths add up. In this case $\beta_1^- \cdot \tau_v = 0$, and so we see that $\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \beta^0_{s_0} \cdot \tau_v$ lies in $K_{2,3}$, and in particular to V, completing the proof that the element in (186) lies in V if $\ell(v) \geqslant 1$. Now it remains to treat the case $\ell(v) = 0$, and without loss of generality $v = 1$. But in part i) we have seen that the element

$\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^-$ lies in V, and hence also in this case we get that the element $\tau_{s_0} \cdot \beta_1^- \otimes \beta^0_{s_0} \otimes \beta^0_{s_0} \cdot \tau_v$ lies in V. Hence, we are done with (186).

It remains to prove that the elements in (184) and in (185) lie in V. We claim that $\beta^0_{s_0} \otimes \beta_1^- \otimes \beta^0_{s_0}$ lies in $K_{2,3}$. If we show this, then we are done because $K_{2,3}$ is a sub-E^0-bimodule, and so we get that the elements in the lines (184) and (185) lie in $K_{2,3}$ as well and hence also to V. So, let us show that $\beta^0_{s_0} \otimes \beta_1^- \otimes \beta^0_{s_0}$ lies in $K_{2,3}$.

$$\begin{aligned}
\beta^0_{s_0} \otimes \beta_1^- \otimes \beta^0_{s_0} &= \mathcal{R}_2(-\alpha^-_{s_0}) \otimes \beta^0_{s_0} \\
&= \mathcal{R}_2(\tau_{s_0} \cdot \alpha_1^+) \otimes \beta^0_{s_0} \\
&\equiv \big(\tau_{s_0} \cdot \mathcal{R}_2(\alpha_1^+)\big) \otimes \beta^0_{s_0} \quad \text{mod } K_{2,3} \\
&= \big(e_1 \cdot \beta_1^+ \otimes \beta^0_{s_1} + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta^+_{s_1} \otimes \beta_1^+ \\
&\qquad + e_{\underline{\mathrm{id}}^{-2}} \cdot \beta^0_{s_1} \otimes \beta_1^+ + \tau_{s_1^{-1}} \cdot \beta_1^+ \otimes \beta^0_{s_1}\big) \otimes \beta^0_{s_0} \\
&\qquad\qquad \text{(computed in (172))} \\
&\equiv 0 \quad \text{mod } K_{2,3},
\end{aligned}$$

where the last equivalence is true because both $\beta_1^+ \otimes \beta^0_{s_0}$ and $\beta^0_{s_1} \otimes \beta^0_{s_0}$ lie in $\ker(\mathcal{M}_2)$. This concludes the proof that all the elements of the forms (184) and (185) lie in V, and with it the proof that all the elements of the form ii) lie in V. ■

4.7 The kernel in degree 4

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. The elements $(\beta^-_w)_w$, $(\beta^0_w)_w$, $(\beta^+_w)_w$, $(\alpha^-_w)_w$, $(\alpha^0_w)_w$, $(\alpha^+_w)_w$, and $(\phi_w)_w$ are chosen as in Subsection 4.5.a.

Since $E^4 = 0$, the kernel of the multiplication map $\mathcal{M}_4 \colon T^4_{E^0} E^1 \longrightarrow E^4$ is of course the whole $T^4_{E^0} E^1$. As we computed generators for $\ker(\mathcal{M}_2)$ as an E^0-bimodule (Proposition 4.5.13), and we computed $\ker(\mathcal{M}_3)$ in terms of $\ker(\mathcal{M}_2)$ and an additional generator (Lemma 4.6.5), we now wish to compute $\ker(\mathcal{M}_4) = T^4_{E^0} E^1$ 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 bilateral ideal by its elements of degree 2 and 3.

Lemma 4.7.1. *Let $\mathcal{M} \colon T^*_{E^0} E^1 \longrightarrow E^*$ be the multiplication map, and let*

$$K_{3,4} \coloneqq \overline{\ker(\mathcal{M}_3) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_3)} \subseteq T^4_{E^0} E^1,$$

where $\overline{(?)}$ denotes the image of $(?)$ in $T^4_{E^0} E^1$. One has that $K_{3,4} = T^4_{E^0} E^1$ and, consequently, that $\ker(\mathcal{M})$ is generated as a bilateral ideal by its elements of degree 2 and 3.

Proof. We have to prove that every element of $T^4_{E^0} E^1$ 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 $y \in T^3_{E^0} E^1$. Let us consider the equality

$$x \otimes y = x \otimes (y - \mathcal{R}_3(\mathcal{M}_3(y))) + x \otimes \mathcal{R}_3(\mathcal{M}_3(y)),$$

in which the first summand on the right hand side lies in $K_{3,4}$, because clearly $y - \mathcal{R}_3(\mathcal{M}_3(y)) \in \ker(\mathcal{M}_3)$. We see that it suffices to prove our claim for elements of the form $x \otimes y'$ for $x \in E^1$ and $y' \in \mathrm{Image}(\mathcal{M}_3)$. Now looking at the explicit definition of $\mathcal{R}_3$ (178), we see that every $y' \in \mathrm{Image}(\mathcal{M}_3)$ 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 $z, t \in E^1$. We are thus reduced to showing that the elements of the following form lie in $K_{3,4}$:

$$\begin{aligned} &u \otimes \beta_1^- &&\text{for } u \in T^3_{E^0} E^1, \\ &u \otimes \beta_1^+ &&\text{for } u \in T^3_{E^0} E^1. \end{aligned}$$

Let $u \in T^3_{E^0} E^1$. Similarly to what we did before, we consider the equality

$$u \otimes \beta_1^\pm = (u - \mathcal{R}_3(\mathcal{M}_3(u))) \otimes \beta_1^\pm + \mathcal{R}_3(\mathcal{M}_3(u)) \otimes \beta_1^\pm,$$

where we see that the first summand on the right hand side lies in $K_{3,4}$. We are therefore reduced to proving that the following elements lie in $K_{3,4}$:

$$\begin{aligned} &u' \otimes \beta_1^- &&\text{for } u' \in \mathrm{Image}(\mathcal{M}_3), \\ &u' \otimes \beta_1^+ &&\text{for } u' \in \mathrm{Image}(\mathcal{M}_3). \end{aligned}$$

Again such every $u' \in \mathrm{Image}(\mathcal{M}_3)$ 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 $z', t' \in E^1$. We are thus reduced to showing that the following elements lie in $K_{3,4}$:

$$\begin{aligned} &z' \otimes t' \otimes \beta_1^- \otimes \beta_1^- &&\text{for } z', t' \in E^1, \\ &z' \otimes t' \otimes \beta_1^+ \otimes \beta_1^- &&\text{for } z', t' \in E^1, \\ &z' \otimes t' \otimes \beta_1^- \otimes \beta_1^+ &&\text{for } z', t' \in E^1, \\ &z' \otimes t' \otimes \beta_1^+ \otimes \beta_1^+ &&\text{for } z', t' \in E^1. \end{aligned}$$

But we recall from Lemma 4.5.9 that 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 $\ker(\mathcal{M}_2)$, and in particular all the elements in the above four lines lie in $K_{3,4}$. ■

4.8 Main result

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. The elements $(\beta_w^-)_w$, $(\beta_w^0)_w$, $(\beta_w^+)_w$, $(\alpha_w^-)_w$, $(\alpha_w^0)_w$, $(\alpha_w^+)_w$, and $(\phi_w)_w$ are chosen as in Subsection 4.5.a.

We are now going to state the main result of this chapter, consisting in a presentation of the Ext-algebra E^* in terms of the tensor algebra $T^*_{E^0} E^1$. All the "positive" results in the statement of this theorem have already been proved, whereas the "negative" result that the kernel of the multiplication map $\mathcal{M} \colon T^*_{E^0} E^1 \longrightarrow E^*$ is not generated in degree 2 has not been dealt with yet, and its proof will be deferred to the next section.

Theorem 4.8.1. *Let us consider the multiplication map*

$$\mathcal{M} \colon T^*_{E^0} E^1 \longrightarrow E^*.$$

The following properties hold.

(i) The multiplication map $\mathcal{M}$ is surjective.

(ii) The kernel of the multiplication map $\mathcal{M}$ is finitely generated as a bilateral ideal.

(iii) More precisely, one can choose a finite set of generators of $\ker(\mathcal{M})$ *lying only in degrees* 2 *and* 3.

(iv) Let $\mathcal{M}_i$ be the multiplication map in degree i for all $i \in \mathbb{Z}_{\geqslant 0}$, and let

$$K_{2,3} := \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \subseteq T^3_{E^0} E^1,$$

where $\overline{(?)}$ denotes the image of $(?)$ in $T^3_{E^0}E^1$. One has that $K_{2,3}$ has finite codimension as a k-vector space in $\ker(\mathcal{M}_3)$.

(v) The sub-bimodule $K_{2,3}$ is properly contained in $\ker(\mathcal{M}_3)$. *In particular,* $\ker(\mathcal{M})$ *is not generated as a bilateral ideal by its degree* 2 *part.*

Proof. The fact that $\mathcal{M}$ is surjective has been proved in Section 4.1. Furthermore, we have seen in Lemma 4.7.1 that the homogeneous ideal $\ker(\mathcal{M})$ is generated by its 2^{nd} and 3^{rd} graded pieces. In Proposition 4.5.13 we have seen that the 2^{nd} graded piece is finitely generated as an E^0-bimodule, and in Lemma 4.6.5 we have seen that $K_{2,3}$ has finite codimension as a k-vector space in $\ker(\mathcal{M}_3)$. The fact that $\ker(\mathcal{M})$ is finitely generated as a bilateral ideal and that we can choose a finite number of generators lying in degrees 2 and 3 follows from these results; for an explicit list of generators see the next remark. The claim that $K_{2,3}$ is properly contained in $\ker(\mathcal{M}_3)$ will be shown in Section 4.9 (more precisely, in Corollary 4.9.12). ■

Remark 4.8.2. The following is a set of generators of $\ker(\mathcal{M})$ as a bilateral ideal:

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

$$\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\mathrm{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+,$$
$$\beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\underline{\mathrm{id}}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-,$$
$$\beta_{s_0}^+ \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_{s_0}^-$$
$$\beta_{s_1}^- \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_{s_1}^+$$
$$(\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-.$$

Proof. By the above theorem or by Lemma 4.7.1 we only need to consider the 2^{nd} and 3^{rd} graded pieces of $\ker(\mathcal{M})$. And the generators have been computed in Proposition 4.5.13 and in Lemma 4.6.5. ■

4.9 The ideal $\ker(\mathcal{M})$ is not generated by its 2^{nd} graded piece

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. The elements $(\beta_w^-)_w$, $(\beta_w^0)_w$, $(\beta_w^+)_w$, $(\alpha_w^-)_w$, $(\alpha_w^0)_w$, $(\alpha_w^+)_w$, and $(\phi_w)_w$ are chosen as in Subsection 4.5.a.

With notation as in Theorem 4.8.1, we have to show that $K_{2,3}$ is properly contained in $\ker(\mathcal{M}_3)$ (and then, in particular, it will follow that $\ker(\mathcal{M})$ is not generated as a bilateral ideal by its degree 2 part).

We will adopt the following strategy: first of all instead of working with the full $E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1$ we will work with $e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma$ for $\gamma \in \Gamma$ "generic", and then we will prove that $e_\gamma K_{2,3} e_\gamma$ is properly contained in $e_\gamma \ker(\mathcal{M}_3) e_\gamma$.

To show this last fact, we will define a homomorphism of E^0-bimodules

$$\widetilde{\mathcal{M}} \colon e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma \longrightarrow \widetilde{E^3} \tag{187}$$

(for a suitable E^0-bimodule $\widetilde{E^3}$) which will be similar to the usual multiplication map with values in E^3 but which will have the following property: the image of $e_\gamma \ker(\mathcal{M}_3) e_\gamma$ will be nonzero, while the image of $e_\gamma K_{2,3} e_\gamma$ will be zero, thus proving the claimed statement.

We begin with the following lemma, which, although not strictly needed to prove our claim, helps in giving a clearer picture (and, moreover, it will be used to describe explicitly the quotient $e_\gamma \ker(\mathcal{M}_3) e_\gamma / e_\gamma K_{2,3} e_\gamma$).

Lemma 4.9.1. *There exists a unique homomorphism of E^0-bimodules Θ making the following diagram commute:*

$$\begin{tikzcd}
E^3 \arrow[r, "\text{quot.}"] \arrow[d, "\zeta \cdot (_)"'] & E^3/F_1 E^0 \cong {}^{\eth}\big((F^2 E^0)^{\vee,\text{finite}}\big)^{\eth} \arrow[ddl, dashed, "\exists! \Theta"] \\
E^3 \arrow[d, "\text{quot.}"'] & \\
E^3/k \cdot e_1 \phi_1 & \\
\ker(\mathcal{S}_3). \arrow[u, phantom, "\cong" rotate=90] &
\end{tikzcd}$$

Proof. Uniqueness is clear, but let us nevertheless assume that such a map Θ is given, in order to find an explicit formula. Let us start by computing the action of ζ on the elements of $F^2 E^3$: let $w \in \widetilde{W}$ be such that $\ell(s_1 w) = \ell(w) + 1$; we compute:

$$\begin{aligned}
\zeta \cdot \phi_{s_0 s_1 w} &= (\tau_{s_1} \cdot \tau_{s_0} + e_1 \tau_{s_0} + e_1) \cdot \phi_{s_0 s_1 w} \\
&= (\tau_{s_1} + e_1) \cdot \big(\phi_{c_{-1} s_1 w} - e_1 \phi_{s_0 s_1 w}\big) + e_1 \phi_{s_0 s_1 w} \\
&= \phi_w - e_1 \phi_{s_0 s_1 w} + e_1 \phi_{s_0 s_1 w} \\
&= \phi_w.
\end{aligned}$$

By applying the automorphism Γ_ϖ we also get that, for all $v \in \widetilde{W}$ be such that $\ell(s_0 v) = \ell(v) + 1$, one has

$$\zeta \cdot \phi_{s_1 s_0 v} = \phi_v.$$

If there exists a homomorphism of E^0-bimodules Θ as in the statement of the lemma, then we can compute its value on the k-basis $\big(\overline{\phi_w}\big)_{w \in \widetilde{W}^{\ell \geqslant 2}}$ of $E^3/F_1 E^0$. Indeed, looking at the commutative diagram we get:

$$\begin{aligned}
\Theta(\overline{\phi_{s_0 s_1 w}}) &= \overline{\zeta \cdot \phi_{s_0 s_1 w}} \\
&= \overline{\phi_w} && \text{for all } w \in \widetilde{W} \text{ such that } \ell(s_1 w) = \ell(w) + 1, \\
\Theta(\overline{\phi_{s_1 s_0 v}}) &= \overline{\zeta \cdot \phi_{s_1 s_0 v}} \\
&= \overline{\phi_v} && \text{for all } v \in \widetilde{W} \text{ such that } \ell(s_0 v) = \ell(v) + 1.
\end{aligned}$$

We have thus shown uniqueness of Θ and we also know how it must be defined if we hope to prove that indeed there exists a map with such properties. Namely, we first define Θ as a homomorphism of k-vector spaces:

$$\begin{array}{llcl}\Theta\colon & E^3/F_1E^0 & \longrightarrow & E^3/k\cdot e_1\phi_1 \\ & \overline{\phi_{s_0s_1w}} \\ & \text{(for } w\in\widetilde{W} \text{ such that } \ell(s_1w)=\ell(w)+1) & \longmapsto & \overline{\phi_w}, \\ & \overline{\phi_{s_1s_0w}} \\ & \text{(for } w\in\widetilde{W} \text{ such that } \ell(s_0w)=\ell(w)+1) & \longmapsto & \overline{\phi_v}.\end{array}$$

It is then clear that Θ is such that the diagram in the statement of the lemma commutes, and it remains to show that it is a homomorphism of E^0-bimodules. We start with the following computation, for $w\in\widetilde{W}$ with $\ell(s_0w)=\ell(w)+1$:

$$\begin{aligned}\Theta\left((\tau_{s_0}+e_1)\cdot\overline{\phi_{s_0s_1s_0w}}\right) &= \Theta\left(\overline{\phi_{c_{-1}s_1s_0w}}\right)\\ &= \overline{\phi_{c_{-1}w}}\\ &= (\tau_{s_0}+e_1)\cdot\overline{\phi_{s_0w}}\\ &= (\tau_{s_0}+e_1)\cdot\Theta\left(\overline{\phi_{s_0s_1s_0w}}\right).\end{aligned}$$

Exactly in the same way we would get the following equality, for all $w\in\widetilde{W}$ with $\ell(s_1w)=\ell(w)+1$:

$$\Theta\left((\tau_{s_1}+e_1)\cdot\overline{\phi_{s_1s_0s_1w}}\right) = (\tau_{s_1}+e_1)\cdot\Theta\left(\overline{\phi_{s_1s_0s_1w}}\right).$$

Now, let us treat the case of length 2: let $\omega\in T^0/T^1$; we compute

$$\begin{aligned}\Theta\left((\tau_{s_0}+e_1)\cdot\tau^\vee_{s_0s_1\omega}\big|_{F^2E^0}\right) &= \Theta\left(((\tau_{s_0}+e_1)\cdot\tau^\vee_{s_0s_1\omega})\big|_{F^2E^0}\right)\\ &= \Theta(0)\\ &= \overline{e_1\phi_1}\\ &= \overline{e_1\phi_\omega}\\ &= (\tau_{s_0}+e_1)\cdot\overline{\phi_\omega}\\ &= (\tau_{s_0}+e_1)\cdot\Theta\left(\tau^\vee_{s_0s_1\omega}\big|_{F^2E^0}\right).\end{aligned}$$

Exactly in the same way we would get

$$\Theta\left((\tau_{s_1}+e_1)\cdot\tau^\vee_{s_1s_0\omega}\big|_{F^2E^0}\right) = (\tau_{s_1}+e_1)\cdot\Theta\left(\tau^\vee_{s_1s_0\omega}\big|_{F^2E^0}\right).$$

Moreover, for all $\omega\in T^0/T^1$ and all $w\in\widetilde{W}$ with $\ell(w)\geqslant 2$, it is easy to see that

$$\Theta\left(\tau_\omega\cdot\overline{\phi_w}\right) = \tau_\omega\cdot\Theta(\overline{\phi_w}).$$

And finally, for all $i\in\{0,1\}$ and all $w\in\widetilde{W}$ with $\ell(s_iw)=\ell(w)+1$, it is easy to see that

$$\Theta\left(\tau_{s_i}\cdot\overline{\phi_w}\right) = 0 = \tau_{s_i}\cdot\Theta\left(\overline{\phi_w}\right).$$

These formulas show that Θ is a homomorphism of left E^0-modules. To show that it is also a homomorphism of right E^0-modules, one could remark that Θ can also described as

$$\begin{array}{llcl}\Theta\colon & E^3/F_1E^0 & \longrightarrow & E^3/k\cdot e_1\phi_1 \\ & \overline{\phi_{ws_0s_1}} \\ & \text{(for } w\in\widetilde{W} \text{ such that } \ell(ws_0)=\ell(w)+1) & \longmapsto & \overline{\phi_w}, \\ & \overline{\phi_{ws_1s_0}} \\ & \text{(for } v\in\widetilde{W} \text{ such that } \ell(ws_1)=\ell(v)+1) & \longmapsto & \overline{\phi_w},\end{array}$$

and then do analogous computations.

Alternatively, one can remark that since both F_1E^3 and $k \cdot e_1\phi_1$ are $\mathcal{J}$-invariant, the involutive anti-automorphism $\mathcal{J}$ defines involutive anti-automorphisms, which we will still denote by $\mathcal{J}$ both on E^3/F_1E^3 and on $E^3/k \cdot e_1\phi_1$. With these definitions, and denoting by r the quotient map $E^3 \longrightarrow E^3/F_1E^3$, one sees that

$$\begin{aligned}\Theta \circ \mathcal{J} \circ r &= \Theta \circ r \circ \mathcal{J} \\ &= \big(\zeta \cdot (\_)\big) \circ \mathcal{J} \\ &= \zeta \cdot \mathcal{J}(\_) \\ &= \mathcal{J}\big((\_) \cdot \zeta\big) \\ &= \mathcal{J}\big(\zeta \cdot (\_)\big) \\ &= \mathcal{J} \circ \Theta \circ r.\end{aligned}$$

This shows that Θ commutes with $\mathcal{J}$ on the whole E^3/F_1E^3. Moreover, we know that the formula

$$\mathcal{J}(x \cdot \varphi) = \mathcal{J}(\varphi) \cdot \mathcal{J}(x)$$

holds for all $x \in E^0$ and for all $\varphi \in E^3$, hence it also holds for $\varphi \in E^3/F_1E^3$ and for $\varphi \in E^3/k \cdot e_1\phi_1$. We then see that for all $x \in E^0$ and all $\varphi \in E^3/F_1E^3$ we have

$$\begin{aligned}\Theta(\varphi \cdot x) &= (\mathcal{J} \circ \Theta \circ \mathcal{J})(\varphi \cdot x) \\ &= (\mathcal{J} \circ \Theta)(\mathcal{J}(x) \cdot \mathcal{J}(\varphi)) \\ &= \mathcal{J}\big(\mathcal{J}(x) \cdot \Theta(\mathcal{J}(\varphi))\big) \\ &= \Theta(\varphi) \cdot x,\end{aligned}$$

completing the proof that Θ is also a homomorphism of right E^0-modules. ■

For the next lemma and for what will follow, recall the definitions of the maps f and g from (50) and (51) and the notations f_i and g_i for their graded pieces. Recall also the structure theorems Proposition 1.10.2 and Proposition 1.10.4.

Lemma 4.9.2. *Let $(E^1)' := \ker(f_1) \oplus \ker(g_1) \subseteq E^1$, and let us consider the decomposition of E^0-bimodules*

$$(E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)' = \bigoplus_{j,j',j'' \in \{f_1, g_1\}} \ker(j) \otimes_{E^0} \ker(j') \otimes_{E^0} \ker(j'').$$

One has that the composite homomorphism of E^0 bimodules

$$(E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)' \xrightarrow{\text{multipl.}} E^3 \xrightarrow{\text{quot.}} E^3/k \cdot e_1\phi_1 \cong \ker(\mathcal{S}_3)$$

is zero on the following direct summands:

$$\begin{aligned}&\ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1), &&\ker(g_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(g_1), \\ &\ker(f_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1), &&\ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(f_1).\end{aligned}$$

Moreover, for all $\gamma \in \Gamma$ with $\gamma \neq \{1\}$, the homomorphism of E^0 bimodules

$$e_\gamma (E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)' e_\gamma \xrightarrow{\text{multipl.}} e_\gamma E^3$$

is zero on the following direct summands:

$$\begin{aligned}&e_\gamma \ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1) e_\gamma, &&e_\gamma \ker(g_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(g_1) e_\gamma, \\ &e_\gamma \ker(f_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1) e_\gamma, &&e_\gamma \ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(f_1) e_\gamma, \\ &e_\gamma \ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1) e_\gamma.\end{aligned}$$

Proof. The second statement clearly follows from the first one except for the lest direct summand. For the proof of the first statement we will use that $\ker(g_3) = k{\cdot}e_1\phi_1$ (see [OS21, Preliminary Observation B) in the proof of Proposition 9.6]). Hence, we need to show the following facts:

$$\begin{aligned}
\ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1) &\subseteq \ker(g_3),\\
\ker(g_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(g_1) &\subseteq \ker(g_3),\\
\ker(f_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1) &\subseteq \ker(g_3),\\
\ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(f_1) &\subseteq \ker(g_3),\\
\ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1) &\subseteq e_1 E^3.
\end{aligned}$$

Let us prove each one of these inclusions.

- Let us treat $\ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1)$. Let $\beta_f, \beta'_f, \beta''_f \in \ker(f_1)$; we compute:

$$\begin{aligned}
\zeta \cdot \beta_f \cdot \beta'_f \cdot \beta''_f \cdot \zeta &= \zeta \cdot \beta_f \cdot (\zeta \cdot \beta'_f \cdot \zeta) \cdot \beta''_f \cdot \zeta\\
&= (\zeta \cdot \beta_f \cdot \zeta) \cdot \beta'_f \cdot (\zeta \cdot \beta''_f \cdot \zeta)\\
&= \beta_f \cdot \beta'_f \cdot \beta''_f.
\end{aligned}$$

  This shows that the image of the simple tensors in $\ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1)$ is contained in $\ker(g_3) = k \cdot e_1\phi_1$, and hence the same is true for the whole image of $\ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1)$, as we wanted.

- Let us treat $\ker(f_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1)$. Let $\beta_f \in \ker(f_1)$ and $\beta_g, \beta'_g \in \ker(g_1)$; we compute:

$$\begin{aligned}
\zeta \cdot \beta_f \cdot \beta_g \cdot \beta'_g \cdot \zeta &= \zeta \cdot \beta_f \cdot \beta_g \cdot \zeta \cdot \beta'_g\\
&= \zeta \cdot \beta_f \cdot \zeta \cdot \beta_g \cdot \beta'_g\\
&= \beta_f \cdot \beta_g \cdot \beta'_g,
\end{aligned}$$

  and so we conclude as before.

- One can treat the direct summand $\ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(f_1)$ exactly as the last one.

- Let us treat $\ker(g_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(g_1)$. Let $\beta_f \in \ker(f_1)$ and $\beta_g, \beta'_g \in \ker(g_1)$; we compute:

$$\begin{aligned}
\zeta \cdot \beta_g \cdot \beta_f \cdot \beta'_g \cdot \zeta &= \beta_g \cdot \zeta \cdot \beta_f \cdot \zeta \cdot \beta'_g\\
&= \beta_g \cdot \beta_f \cdot \beta'_g,
\end{aligned}$$

  and so we conclude as before.

- Let us treat $\ker(g_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(g_1)$.

  In [OS21, Proposition 9.2 and its proof] it is computed that

$$\begin{aligned}
&\beta^{0,\star}_{s_0} \cdot \beta^{0,\star}_{s_0} = e_1\alpha^{0,\star}_{s_0} = -e_1\alpha^0_{s_0},\\
&\beta^{0,\star}_{s_1} \cdot \beta^{0,\star}_{s_1} = e_1\alpha^{0,\star}_{s_1} = e_1\alpha^0_{s_1},\\
&\beta^{0,\star}_{s_0} \cdot \beta^{0,\star}_{s_1} = 0,\\
&\beta^{0,\star}_{s_1} \cdot \beta^{0,\star}_{s_0} = 0
\end{aligned}$$

(the rightmost equalities in the first two lines follow from (88)). One easily see that the four elements $\beta^{0,\star}_{s_0} \otimes \beta^{0,\star}_{s_0}$, $\beta^{0,\star}_{s_1} \otimes \beta^{0,\star}_{s_1}$, $\beta^{0,\star}_{s_0} \otimes \beta^{0,\star}_{s_1}$ and $\beta^{0,\star}_{s_1} \otimes \beta^{0,\star}_{s_0}$ generate $\ker(g_1) \otimes_{E^0} \ker(g_1)$ as an E^0-bimodule (or even as a left E^0-module), and that the k-vector space

$$\operatorname{span}_k\{e_1\alpha^{0,\star}_{s_0}, e_1\alpha^{0,\star}_{s_1}\} = \operatorname{span}_k\{e_1\alpha^{0}_{s_0}, e_1\alpha^{0}_{s_1}\}$$

is a sub-E^0-bimodule of $\ker(g_2)$ (actually sub-E^0-left module would suffice for our purposes, and that it is a sub-E^0-bimodule would then follow), thus showing that the image of the multiplication map

$$\ker(g_1) \otimes_{E^0} \ker(g_1) \longrightarrow \ker(g_2)$$

is exactly $\operatorname{span}_k\{e_1\alpha^{0}_{s_0}, e_1\alpha^{0}_{s_1}\}$. Finally, we see that for all $\beta \in \ker(g_1)$ the products $\beta \cdot e_1\alpha^0_{s_0}$ and $\beta \cdot e_1\alpha^0_{s_1}$ lie in e_1E^3, since β and e_1 commute (as $\beta \in \ker(g_1) \cong F^1E^0$). ■

Remark 4.9.3. For later use we record that

$$e_\gamma \ker(g_1) \cdot \ker(g_1) = 0$$

for all $\gamma \in \Gamma$ with $\gamma \neq \{1\}$, as we saw in the last part of the proof of the lemma.

In the next lemma we are going to define a homomorphism of E^0-bimodules

$$\widehat{\mathcal{M}} \colon e_\gamma(E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)'e_\gamma \longrightarrow E^3$$

that will be our starting point to define the homomorphism of E^0-bimodules $\widetilde{\mathcal{M}}$ whose existence was claimed in (187) when we outlined the strategy of our proof.

Lemma 4.9.4. *As in the last lemma, let $(E^1)' := \ker(f_1) \oplus \ker(g_1) \subseteq E^1$. Let $\gamma \in \Gamma$ with $\gamma \neq \{1\}$, and let us consider the decomposition of E^0-bimodules*

$$e_\gamma(E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)'e_\gamma = \bigoplus_{j,j',j'' \in \{f_1, g_1\}} e_\gamma \ker(j) \otimes_{E^0} \ker(j') \otimes_{E^0} \ker(j'')e_\gamma. \tag{188}$$

Let us define a homomorphism of E^0-bimodules

$$\widehat{\mathcal{M}} \colon e_\gamma(E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)'e_\gamma \longrightarrow E^3$$

in the following way:

$$\begin{aligned}
\widehat{\mathcal{M}} \colon e_\gamma \ker(f_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(g_1)e_\gamma &\longrightarrow E^3 \\
\beta \otimes \beta' \otimes \beta'' &\longmapsto \beta \cdot \zeta \cdot \beta' \cdot \beta'',
\end{aligned}$$

$$\begin{aligned}
\widehat{\mathcal{M}} \colon e_\gamma \ker(g_1) \otimes_{E^0} \ker(f_1) \otimes_{E^0} \ker(f_1)e_\gamma &\longrightarrow E^3 \\
\beta \otimes \beta' \otimes \beta'' &\longmapsto \beta \cdot \beta' \cdot \zeta \cdot \beta'',
\end{aligned}$$

$$\begin{aligned}
\widehat{\mathcal{M}} \colon e_\gamma \ker(f_1) \otimes_{E^0} \ker(g_1) \otimes_{E^0} \ker(f_1)e_\gamma &\longrightarrow E^3 \\
\beta \otimes \beta' \otimes \beta'' &\longmapsto \beta \cdot \zeta \cdot \beta' \cdot \beta'' = \beta \cdot \beta' \cdot \zeta \cdot \beta'',
\end{aligned}$$

and as the zero map on all the remaining terms of the decomposition (188).

One has that the following diagram is commutative:

$$\begin{tikzcd}
 & E^3 \arrow[d, "\zeta \cdot (_)"] \\
e_\gamma(E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)'e_\gamma \arrow[ur, "\widehat{\mathcal{M}}"] \arrow[r, "\mathcal{M}"'] & E^3.
\end{tikzcd}$$

Proof. First note that $\widehat{\mathcal{M}}$ is a well defined homomorphism of E^0-bimodules because $\zeta \in Z(E^0)$ (and hence one can define suitable E^0-bilinear maps).

The fact that the diagram is commutative on all the terms where we have defined $\widehat{\mathcal{M}}$ to be the zero map follows from the fact that there also the multiplication map is zero (Lemma 4.9.2). The fact that the diagram is commutative on the remaining three terms is true basically by definition of $\ker(g_1)$, also taking into account that multiplication by ζ on E^3 can be written equivalently on the left and on the right. ■

Lemma 4.9.5. *Let $\gamma \in \Gamma$ with $\gamma \neq \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$. One has that*

$$e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma = e_\gamma (E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)' e_\gamma,$$

where $(E^1)' := \ker(f_1) \oplus \ker(g_1) \subseteq E^1$ and where the equality means that the natural map from the right hand side to the left hand side is an isomorphism of E^0-bimodules.

Proof. Recall from Proposition 1.10.2 that we have the following exact sequence of E^0-bimodules:

$$0 \longrightarrow \ker(f_1) \oplus \ker(g_1) \longrightarrow E^1 \longrightarrow E^1/(\ker(f_1) \oplus \ker(g_1)) \longrightarrow 0,$$

where the quotient $E^1/(\ker(f_1) \oplus \ker(g_1))$ has a k-basis given by the classes of the following four elements of E^1:

$$\begin{aligned} &e_{\underline{\mathrm{id}}} \cdot \beta_1^+ \cdot e_{\underline{\mathrm{id}}^{-1}}, && e_{\underline{\mathrm{id}}} \cdot \beta_{s_1}^+ \cdot e_{\underline{\mathrm{id}}}, \\ &e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \cdot e_{\underline{\mathrm{id}}}, && e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_{s_0}^- \cdot e_{\underline{\mathrm{id}}^{-1}}. \end{aligned}$$

So, since $\gamma \neq \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}$, we see that

$$e_\gamma E^1 = e_\gamma (E^1)', \qquad E^1 e_\gamma = (E^1)' e_\gamma. \tag{189}$$

Moreover, let $\mu \in \widehat{T^0/T^1}$, let $w \in \widetilde{W}$ and let $\beta \in \{\beta_w^-, \beta_w^0, \beta_w^+\}$ (with $\ell(w) \geqslant 1$ if we are considering β_w^0). From formulas (61) we see that:

$$\beta e_\mu = \begin{cases} e_\mu \beta \\ e_{\mu^{-1}} \beta \\ e_{\mu \underline{\mathrm{id}}^2} \beta \\ e_{\mu^{-1} \underline{\mathrm{id}}^2} \beta \\ e_{\mu \underline{\mathrm{id}}^{-2}} \beta \\ e_{\mu^{-1} \underline{\mathrm{id}}^{-2}} \beta \end{cases}$$

It follows that, writing $\gamma = \{\lambda, \lambda^{-1}\}$ and defining

$$\Gamma_\gamma := \left\{ \{\lambda, \lambda^{-1}\}, \{\lambda \underline{\mathrm{id}}^2, \lambda^{-1} \underline{\mathrm{id}}^{-2}\}, \{\lambda \underline{\mathrm{id}}^{-2}, \lambda^{-1} \underline{\mathrm{id}}^2\} \right\},$$

for all $\beta \in E^1$ we have

$$\beta \cdot e_\gamma = \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) \cdot \beta \cdot e_\gamma. \tag{190}$$

Since $\gamma \neq \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$, for each $\gamma' \in \Gamma_\gamma$ we see that $\gamma' \neq \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}$. But then, as before, it follows that

$$E^1 \cdot \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) = (E^1)' \cdot \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big). \tag{191}$$

Putting together what we have found, we deduce the following:

$$
\begin{aligned}
&e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma \\
&\qquad = e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) \cdot E^1 e_\gamma && \text{by (190)} \\
&\qquad = e_\gamma E^1 \otimes_{E^0} E^1 \cdot \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) \otimes_{E^0} E^1 e_\gamma \\
&\qquad = e_\gamma (E^1)' \otimes_{E^0} (E^1)' \cdot \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) \otimes_{E^0} (E^1)' e_\gamma && \text{by (191) and (189)} \\
&\qquad = e_\gamma (E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) \cdot (E^1)' e_\gamma \\
&\qquad = e_\gamma (E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)' e_\gamma && \text{by (190).}
\end{aligned}
$$

■

We are now ready to define the map $\widetilde{\mathcal{M}}$ whose existence was claimed in (187).

Remark 4.9.6. Let $\gamma \in \Gamma$ with $\gamma \neq \{1\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$. We have the following commutative diagram:

$$
\begin{tikzcd}
& e_\gamma E^3 \arrow[r, "\text{quot.}"] \arrow[d, "\zeta \cdot (\_)"'] & e_\gamma \cdot E^3/F_1E^3 \arrow[dl, "\Theta"] \\
e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma \arrow[ur, "\widehat{\mathcal{M}}"] \arrow[r, "\mathcal{M}"'] \arrow[urr, bend left, "\widetilde{\mathcal{M}} \coloneqq (\text{quot.}) \circ \widehat{\mathcal{M}}"] & e_\gamma E^3.
\end{tikzcd}
$$

This is constructed as in the following way: we identify $e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma$ with $e_\gamma (E^1)' \otimes_{E^0} (E^1)' \otimes_{E^0} (E^1)' e_\gamma$ following Lemma 4.9.5 (this identification clearly preserves the multiplication map $\mathcal{M}$). The triangle on the left then makes sense and commutes by Lemma 4.9.4. Moreover, we can define Θ as in Lemma 4.9.1, modulo the fact that on the target we identify $e_\gamma \cdot E^3/k \cdot e_1 \phi_1$ with $e_\gamma E^3$. With this definition, the triangle on the right commutes by the quoted lemma.

Before using the map $\widetilde{\mathcal{M}}$ to prove that $\ker(\mathcal{M})$ is not generated by its 2^{nd} graded piece, we need some further lemmas.

Lemma 4.9.7. *Let $\gamma \in \Gamma$ with $\gamma \neq \{1\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$. The map*

$$\widehat{\mathcal{M}} \colon e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma \longrightarrow e_\gamma E^3$$

defined in Remark 4.9.6 satisfies the following properties, for $\beta, \beta', \beta'' \in E^1$:

$$
\widehat{\mathcal{M}}(e_\gamma \beta \otimes \beta' \otimes \beta'' e_\gamma) =
\begin{cases}
e_\gamma \beta \cdot \zeta \cdot \beta' \cdot \beta'' e_\gamma & \text{if } \beta \in \ker(f_1), \qquad (192) \\
e_\gamma \beta \cdot \beta' \cdot \zeta \cdot \beta'' e_\gamma & \text{if } \beta \in \ker(g_1), \qquad (193) \\
e_\gamma \beta \cdot \beta' \cdot \zeta \cdot \beta'' e_\gamma & \text{if } \beta'' \in \ker(f_1), \qquad (194) \\
e_\gamma \beta \cdot \zeta \cdot \beta' \cdot \beta'' e_\gamma & \text{if } \beta'' \in \ker(g_1). \qquad (195)
\end{cases}
$$

Proof. Let $\beta, \beta', \beta'' \in E^1$. First of all we remark that it suffices to prove the formulas only for $\beta, \beta', \beta'' \in (E^1)' \coloneqq \ker(f_1) \oplus \ker(g_1)$. Indeed, first recall from the proof of Lemma 4.9.5 (formula (190)) that we have

$$\beta'' e_\gamma = \Big(\sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} \Big) \cdot \beta'' e_\gamma,$$

where $\Gamma_\gamma := \big\{\{\lambda, \lambda^{-1}\}, \{\lambda\,\underline{\mathrm{id}}^2, \lambda^{-1}\,\underline{\mathrm{id}}^{-2}\}, \{\lambda\,\underline{\mathrm{id}}^{-2}, \lambda^{-1}\,\underline{\mathrm{id}}^2\}\big\}$. In particular,

$$e_\gamma\beta \otimes \beta' \otimes \beta'' e_\gamma = e_\gamma e_\gamma \beta \otimes \Big(\beta' \cdot \sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'}\Big) \otimes \beta'' e_\gamma e_\gamma,$$

with the same definition of Γ_γ as in the proof of that lemma. But now, again as in Lemma 4.9.5, we see that

$$\begin{aligned} e_\gamma\beta &\in (E^1)', \\ \beta' \cdot \sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'} &\in (E^1)', \\ \beta'' e_\gamma &\in (E^1)'. \end{aligned}$$

Hence, if we take the formulas (192) to (195) for granted for $(E^1)'$, we deduce that

$$\begin{aligned} \widehat{\mathcal{M}}(e_\gamma\beta \otimes \beta' \otimes \beta'' e_\gamma) &= \begin{cases} e_\gamma e_\gamma \beta \cdot \zeta \cdot \Big(\beta' \cdot \sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'}\Big) \cdot \beta'' e_\gamma e_\gamma & \text{if } \beta \in \ker(f_1) \\ e_\gamma e_\gamma \beta \cdot \Big(\beta' \cdot \sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'}\Big) \cdot \zeta \cdot \beta'' e_\gamma e_\gamma & \text{if } \beta \in \ker(g_1) \\ e_\gamma e_\gamma \beta \cdot \Big(\beta' \cdot \sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'}\Big) \cdot \zeta \cdot \beta'' e_\gamma e_\gamma & \text{if } \beta'' \in \ker(f_1) \\ e_\gamma e_\gamma \beta \cdot \zeta \cdot \Big(\beta' \cdot \sum_{\gamma' \in \Gamma_\gamma} e_{\gamma'}\Big) \cdot \beta'' e_\gamma e_\gamma & \text{if } \beta'' \in \ker(g_1) \end{cases} \\ &= \begin{cases} e_\gamma\beta \cdot \zeta \cdot \beta'' e_\gamma & \text{if } \beta \in \ker(f_1) \\ e_\gamma\beta \cdot \zeta \cdot \beta'' e_\gamma & \text{if } \beta \in \ker(g_1) \\ e_\gamma\beta \cdot \zeta \cdot \beta'' e_\gamma & \text{if } \beta'' \in \ker(f_1) \\ e_\gamma\beta \cdot \zeta \cdot \beta'' e_\gamma & \text{if } \beta'' \in \ker(g_1). \end{cases} \end{aligned}$$

Hence, without loss of generality, we may assume that $\beta, \beta', \beta'' \in (E^1)'$, and since all the expression involved are "trilinear", we may further assume that either $\beta \in \ker(f_1)$ or $\beta \in \ker(g_1)$ and the same for β' and β''.

So let us treat these eight cases:

- In the following cases the claimed formulas hold by the very definition of $\widehat{\mathcal{M}}$:

$$\begin{array}{lllll} \text{Case} & \beta \in \ker(f_1), & \beta' \in \ker(f_1) & \text{and} & \beta'' \in \ker(g_1), \\ \text{Case} & \beta \in \ker(g_1), & \beta' \in \ker(f_1) & \text{and} & \beta'' \in \ker(f_1), \\ \text{Case} & \beta \in \ker(f_1), & \beta' \in \ker(g_1) & \text{and} & \beta'' \in \ker(f_1). \end{array}$$

- Assume that $\beta \in \ker(f_1)$, that $\beta' \in \ker(f_1)$ and that $\beta'' \in \ker(f_1)$.

  We know from Lemma 4.9.2 that $e_\gamma\beta \cdot \beta' \cdot \beta'' e_\gamma$ is zero, and a fortiori

$$\zeta \cdot e_\gamma\beta \cdot \beta' \cdot \beta'' e_\gamma = 0 = e_\gamma\beta \cdot \beta' \cdot \beta'' e_\gamma \cdot \zeta.$$

  But it is easy to see that ζ commutes with $e_\gamma\beta \cdot \beta'$ and with $\beta' \cdot \beta'' e_\gamma$. Recalling that $\widehat{\mathcal{M}}(e_\gamma\beta \otimes \beta' \otimes \beta'' e_\gamma)$ is zero by definition of $\widehat{\mathcal{M}}$, we conclude that (192) and (194) are satisfied in this case.

- Assume that $\beta \in \ker(g_1)$, that $\beta' \in \ker(f_1)$ and that $\beta'' \in \ker(g_1)$.

  Again we know from Lemma 4.9.2 that $e_\gamma\beta \cdot \beta' \cdot \beta'' e_\gamma$ is zero. Since here ζ commutes with both $e_\gamma\beta$ and $\beta'' e_\gamma$ and since $\widehat{\mathcal{M}}(e_\gamma\beta \otimes \beta' \otimes \beta'' e_\gamma)$ is zero by definition of $\widehat{\mathcal{M}}$, we conclude that (193) and (195) are satisfied in this case.

- The case $\beta \in \ker(g_1)$, $\beta' \in \ker(g_1)$ and $\beta'' \in \ker(g_1)$ can be done exactly as the last one.

- The case $\beta \in \ker(f_1)$, $\beta' \in \ker(g_1)$ and $\beta'' \in \ker(g_1)$ and the case $\beta \in \ker(g_1)$, $\beta' \in \ker(g_1)$ and $\beta'' \in \ker(f_1)$ can be done similarly. Here one uses that

$$\begin{aligned}
0 &= e_\gamma\beta \cdot \beta' \cdot \beta'' e_\gamma \cdot \zeta = e_\gamma\beta \cdot \zeta \cdot \beta' \cdot \beta'' e_\gamma && \text{in the first case,}\\
0 &= \zeta \cdot e_\gamma\beta \cdot \beta' \cdot \beta'' e_\gamma = e_\gamma\beta \cdot \beta' \cdot \zeta \cdot \beta'' e_\gamma && \text{in the second case,}
\end{aligned}$$

  yielding that (192) and (195) are satisfied in the first case, while (193) and (194) are satisfied in the second case. ■

Lemma 4.9.8. *Let $\gamma \in \Gamma$ with $\gamma \neq 1$. The set of elements of $e_\gamma E^3$ which are annihilated on the left by both $\tau_{s_0s_1}$ and $\tau_{s_1s_0}$ coincides with $e_\gamma F^1 E^3$.*

Proof. It is clear that every element in $e_\gamma F^1 E^3$ is annihilated by both $\tau_{s_0s_1}$ and $\tau_{s_1s_0}$. Let us prove the converse. We assume that $\gamma = \{\lambda, \lambda^{-1}\}$ with $\lambda \neq \lambda^{-1}$ (the case $\lambda = \lambda^{-1}$ is similar). The following is a k-basis of $e_\gamma E^3$:

$$\begin{array}{lll}
e_\lambda\phi_1, & e_{\lambda^{-1}}\phi_1, & \\
e_\lambda\phi_{(s_0s_1)^i s_0}, & e_{\lambda^{-1}}\phi_{s_0(s_1s_0)^i} & \text{for } i \in \mathbb{Z}_{\geqslant 0},\\
e_\lambda\phi_{(s_1s_0)^i s_1}, & e_{\lambda^{-1}}\phi_{s_1(s_0s_1)^i} & \text{for } i \in \mathbb{Z}_{\geqslant 0},\\
e_\lambda\phi_{(s_0s_1)^i}, & e_{\lambda^{-1}}\phi_{(s_0s_1)^i} & \text{for } i \in \mathbb{Z}_{\geqslant 1},\\
e_\lambda\phi_{(s_1s_0)^i}, & e_{\lambda^{-1}}\phi_{(s_1s_0)^i} & \text{for } i \in \mathbb{Z}_{\geqslant 1}.
\end{array}$$

Let us consider $\phi \in e_\gamma E^3$ with the property that it is annihilated by both $\tau_{s_0s_1}$ and $\tau_{s_1s_0}$. Since we have already said that every element in $e_\gamma F^1 E^3$ is annihilated by both $\tau_{s_0s_1}$ and $\tau_{s_1s_0}$, we may assume that $\phi \in F^2E^2$ and prove that it must be 0. We write ϕ as

$$\phi = \sum_{i\in\mathbb{Z}_{\geqslant 1}} a_i e_\lambda \phi_{(s_0s_1)^i} + \sum_{i\in\mathbb{Z}_{\geqslant 1}} b_i e_\lambda \phi_{(s_1s_0)^i} + \sum_{i\in\mathbb{Z}_{\geqslant 1}} c_i e_\lambda \phi_{(s_0s_1)^i s_0} + \sum_{i\in\mathbb{Z}_{\geqslant 1}} d_i e_\lambda \phi_{(s_1s_0)^i s_1}$$

for suitable $a_i, b_i, c_i, d_i \in k$ (almost all of them equal to zero). We compute

$$\begin{aligned}
\tau_{s_0s_1} \cdot \phi &= + \sum_{i\in\mathbb{Z}_{\geqslant 1}} b_i e_\lambda \phi_{(s_1s_0)^{i-1}} + \sum_{i\in\mathbb{Z}_{\geqslant 1}} d_i e_\lambda \phi_{(s_1s_0)^{i-1}s_1},\\
\tau_{s_1s_0} \cdot \phi &= \sum_{i\in\mathbb{Z}_{\geqslant 1}} a_i e_\lambda \phi_{(s_0s_1)^{i-1}} + \sum_{i\in\mathbb{Z}_{\geqslant 1}} c_i e_\lambda \phi_{(s_0s_1)^{i-1}s_0},
\end{aligned}$$

from which we see that for all $i \in \mathbb{Z}_{\geqslant 1}$ all the coefficients a_i, b_i, c_i and d_i must be zero, as we wanted. ■

Lemma 4.9.9. *Let $\gamma \in \Gamma$ with $\gamma \neq \{1\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$. The map*

$$\widetilde{\mathcal{M}}\colon e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma \longrightarrow e_\gamma \cdot E^3/F_1E^3$$

defined in Remark 4.9.6 is zero on $e_\gamma K_{2,3} e_\gamma$, where

$$K_{2,3} \coloneqq \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} + \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \subseteq E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1.$$

Proof. Let $x \in e_\gamma \cdot \overline{E^1 \otimes_{E^0} \ker(\mathcal{M}_2)} \cdot e_\gamma$; we want to prove that $\widetilde{\mathcal{M}}(x) = 0$. The proof in the case that $x \in e_\gamma \overline{\ker(\mathcal{M}_2) \otimes_{E^0} E^1} e_\gamma$ is completely analogous, and this allows us to conclude more generally for $x \in K_{2,3}$.

Without loss of generality we may assume that x is of the form

$$x = e_\gamma \beta \otimes y e_\gamma \qquad \text{for } \beta \in E^1 \text{ and } y \in \ker(\mathcal{M}_2).$$

And, using that $e_\gamma E^1 = e_\gamma \ker(f_1) \oplus e_\gamma \ker(g_1)$ (see (189)), without loss of generality we may further assume that either $\beta \in \ker(f_1)$ or $\beta \in \ker(g_1)$. If we are in the case $\beta \in \ker(f_1)$, then applying the formulas in Lemma 4.9.7, we see that

$$\widehat{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma) = e_\gamma \beta \cdot \zeta \cdot \mathcal{M}_2(y e_\gamma) = e_\gamma \beta \cdot \zeta \cdot 0.$$

And so a fortiori $\widetilde{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma)$ is zero.

Now, it remains to treat the case $\beta \in \ker(g_1)$. Since $\ker(g_1)$ is generated by $\beta_{s_0}^{0,\star}$ and $\beta_{s_1}^{0,\star}$ as a *left* E^0-module, we may assume without loss of generality that β is equal either to $\beta_{s_0}^{0,\star}$ or to $\beta_{s_1}^{0,\star}$. We treat only the case $\beta = \beta_{s_0}^{0,\star}$, the other one being completely analogous. As in the proof of Lemma 4.9.2, we see that, as $\gamma \neq \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-3}\}$, one has

$$E^1 \otimes_{E^0} E^1 e_\gamma = (\ker(f_1) \oplus \ker(g_1)) \otimes_{E^0} E^1 e_\gamma.$$

We can therefore write xe_γ as a sum of simple tensors of the following form:

$$xe_\gamma = \sum_i \beta_{if} \otimes \beta_i e_\gamma + \sum_i \beta_{ig} \otimes \beta_i' e_\gamma$$
$$\text{for some } \beta_{if} \in \ker(f_1), \text{ some } \beta_{ig} \in \ker(f_1) \text{ and some } \beta_i, \beta_i' \in E^1.$$

We want to compute $\tau_{s_1 s_0} \cdot \widehat{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma)$ and $\tau_{s_0 s_1} \cdot \widehat{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma)$, and prove that they both lie in $F_1 E^3$. If we prove this, then Lemma 4.9.8 (together with the definition of $\widetilde{\mathcal{M}}$ in terms of $\widehat{\mathcal{M}}$) yields that $\widetilde{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma)$ is 0.

We start with the computation of $\tau_{s_0 s_1} \cdot \widehat{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma)$:

$$\begin{aligned}
&\tau_{s_0 s_1} \cdot \widehat{\mathcal{M}}(e_\gamma \beta \otimes y e_\gamma) \\
&\quad = \tau_{s_0 s_1} \cdot \widehat{\mathcal{M}}\Big(e_\gamma \beta_{s_0}^{0,\star} \otimes \Big(\textstyle\sum_i \beta_{if} \otimes \beta_i e_\gamma + \sum_i \beta_{ig} \otimes \beta_i' e_\gamma \Big)\Big) \\
&\quad = \textstyle\sum_i \tau_{s_0 s_1} \cdot e_\gamma \beta_{s_0}^{0,\star} \cdot \beta_{if} \cdot \zeta \cdot \beta_i e_\gamma + \sum_i \tau_{s_0 s_1} \cdot e_\gamma \beta_{s_0}^{0,\star} \cdot \beta_{ig} \cdot \zeta \cdot \beta_i' e_\gamma \\
&\qquad\qquad \text{by Lemma 4.9.7} \\
&\quad = \textstyle\sum_i \tau_{s_0 s_1} \cdot e_\gamma \beta_{s_0}^{0,\star} \cdot \beta_{if} \cdot \zeta \cdot \beta_i e_\gamma \\
&\qquad\qquad \text{since } e_\gamma \ker(g_1) \cdot \ker(g_1) = 0 \text{ (Remark 4.9.3)} \\
&\quad = \textstyle\sum_i \zeta \cdot e_\gamma \beta_{s_0}^{0,\star} \cdot \beta_{if} \cdot \zeta \cdot \beta_i e_\gamma \\
&\qquad\qquad \text{since } \tau_{s_1 s_0},\ e_1 \tau_{s_0},\ e_1 \tau_{s_1} \text{ and } e_1 \text{ all act by 0 on } e_\gamma \beta_{s_0}^{0,\star} \\
&\quad = \textstyle\sum_i e_\gamma \beta_{s_0}^{0,\star} \cdot \zeta \cdot \beta_{if} \cdot \zeta \cdot \beta_i e_\gamma \\
&\quad = \textstyle\sum_i e_\gamma \beta_{s_0}^{0,\star} \cdot \beta_{if} \cdot \beta_i e_\gamma \\
&\quad = e_\gamma \beta_{s_0}^{0,\star} \cdot \Big(\textstyle\sum_i \beta_{if} \cdot \beta_i e_\gamma + \sum_i \beta_{ig} \otimes \beta_i' e_\gamma \Big) \\
&\qquad\qquad \text{since } e_\gamma \ker(g_1) \cdot \ker(g_1) = 0 \text{ (Remark 4.9.3)} \\
&\quad = e_\gamma \beta_{s_0}^{0,\star} \cdot \mathcal{M}_2(x e_\gamma) \\
&\quad = 0.
\end{aligned}$$

Now we compute $\tau_{s_1s_0} \cdot \widehat{\mathcal{M}}(e_\gamma\beta \otimes ye_\gamma)$:

$$\begin{aligned}\tau_{s_1s_0} \cdot \widehat{\mathcal{M}}(e_\gamma\beta \otimes ye_\gamma) &= \widehat{\mathcal{M}}(e_\gamma\tau_{s_1s_0} \cdot \beta^{0,\star}_{s_0} \otimes ye_\gamma)\\ &= \widehat{\mathcal{M}}(0 \otimes ye_\gamma)\\ &= 0.\end{aligned}$$ ■

The next remark shows that the map $\widehat{\mathcal{M}}$ alone is not useful for our purposes, and that we really need the map $\widetilde{\mathcal{M}}$ (compare this with the strategy outlined at the beginning of the section).

Remark 4.9.10. With notation and assumptions as in the last lemma, we see that it is not true that $\widehat{\mathcal{M}}$ is zero on $e_\gamma K_{2,3}e_\gamma$. Indeed:

$$\begin{aligned}\widehat{\mathcal{M}}\big(e_\gamma\beta^{0,\star}_{s_0} \otimes \beta^-_1 \otimes \beta^+_1 e_\gamma\big) &= e_\gamma\beta^{0,\star}_{s_0} \cdot \beta^-_1 \cdot \zeta \cdot \beta^+_1 e_\gamma\\ &\qquad \text{by Lemma 4.9.7}\\ &= e_\gamma\beta^{0,\star}_{s_0} \cdot \beta^-_1 \cdot \tau_{s_0s_1} \cdot \beta^+_1 e_\gamma\\ &= -e_\gamma\beta^{0,\star}_{s_0} \cdot \alpha^0_{s_0s_1} e_\gamma\\ &\qquad \text{see, e.g., the definition of } \mathcal{R}_2 \text{ in (170)}\\ &= -e_\gamma\beta^{0,\star}_{s_0} \cdot \alpha^{0,\star}_{s_0s_1} e_\gamma\\ &\qquad \text{by (88) and since } e_\gamma \text{ and } \beta^{0,\star}_{s_0} \text{ commute}\\ &= -e_\gamma\tau_{s_0} \cdot \phi_{s_0s_1} e_\gamma\\ &\qquad \text{by (111)}\\ &= -e_\gamma\phi_{c_{-1}s_1} e_\gamma,\end{aligned}$$

and this is nonzero, even though $e_\gamma\beta^{0,\star}_{s_0} \otimes \beta^-_1 \otimes \beta^+_1 e_\gamma \in K_{2,3}$ because $\beta^-_1 \cdot \beta^+_1 = 0$.

Lemma 4.9.11. *Let $\gamma \in \Gamma$ with $\gamma \neq \{1\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$, and let*

$$x := (\tau_{s_1} + e_1) \cdot \beta^+_1 \otimes \beta^0_{s_1^{-1}} \otimes \beta^+_1 + (\tau_{s_0} + e_1) \cdot \beta^-_1 \otimes \beta^0_{s_0^{-1}} \otimes \beta^-_1.$$

One has that the map $\widetilde{\mathcal{M}}$ is nonzero at $e_\gamma xe_\gamma$.

Proof. We have to compute the values of $\widehat{\mathcal{M}}$ at $x_{\gamma,1} := e_\gamma(\tau_{s_1}+e_1)\cdot\beta^+_1 \otimes \beta^0_{s_1^{-1}} \otimes \beta^+_1 e_\gamma$ and at $x_{\gamma,0} := e_\gamma(\tau_{s_0}+e_1)\cdot\beta^-_1 \otimes \beta^0_{s_0^{-1}} \otimes \beta^-_1 e_\gamma$ and show that their sum does not lie in F_1E^3. Before starting we recall from Proposition 1.10.2 that the following elements lie in $\ker(f_1)$:

$$\beta^+_1 - 2e_{\underline{\mathrm{id}}}\beta^0_{s_0} - e_{\underline{\mathrm{id}}}\beta^+_{s_1s_0}, \qquad \beta^-_1 + 2e_{\underline{\mathrm{id}}^{-1}}\beta^0_{s_1} - e_{\underline{\mathrm{id}}^{-1}}\beta^-_{s_0s_1},$$

and therefore

$$e_\gamma\beta^+_1 \in \ker(f_1), \qquad e_\gamma\beta^-_1 \in \ker(f_1). \tag{196}$$

We start with the computation of $\widehat{\mathcal{M}}(x_{\gamma,1})$:

$$\begin{aligned}
\widehat{\mathcal{M}}(x_{\gamma,1}) &= \widehat{\mathcal{M}}\left(e_\gamma(\tau_{s_1}+e_1)\cdot\beta_1^+\otimes\beta^0_{s_1^{-1}}\otimes\beta_1^+e_\gamma\right)\\
&= \widehat{\mathcal{M}}\left(e_\gamma\tau_{s_1}\cdot\beta_1^+\otimes\beta^0_{s_1^{-1}}\otimes\beta_1^+e_\gamma\right)\\
&= \widehat{\mathcal{M}}\left(e_\gamma\tau_{s_1}\cdot e_\gamma\beta_1^+\otimes\beta^0_{s_1^{-1}}\otimes\beta_1^+e_\gamma\right)\\
&= e_\gamma\tau_{s_1}\cdot\beta_1^+\cdot\zeta\cdot\beta^0_{s_1^{-1}}\cdot\beta_1^+e_\gamma && \text{by Lemma 4.9.7, since } \tau_{s_1}e_\gamma\beta_1^+\in\ker(f_1) \text{ by (196)}\\
&= e_\gamma\tau_{s_1}\cdot e_\gamma\beta_1^+\cdot\zeta\cdot\alpha^+_{s_1^{-1}}e_\gamma && \text{see, e.g., (170)}\\
&= e_\gamma\tau_{s_1}\cdot e_\gamma\beta_1^+\cdot(\tau_{s_1s_0}+e_1\tau_{s_1}+e_1)\cdot\alpha^+_{s_1^{-1}}e_\gamma && \text{as } \beta_1^+\cdot\tau_{s_0}=0\\
&= e_\gamma\tau_{s_1}\cdot e_\gamma\beta_1^+\cdot\tau_{s_1s_0}\cdot\alpha^+_{s_1^{-1}}e_\gamma && \text{as } (\tau_{s_1}+e_1)\cdot\alpha^+_{s_1^{-1}}=0\\
&= e_\gamma\tau_{s_1}\cdot e_\gamma\beta_1^+\cdot\alpha^+_{s_1s_0s_1^{-1}}e_\gamma\\
&= e_\gamma\tau_{s_1}\cdot e_\gamma\phi_{s_1s_0s_1^{-1}}e_\gamma && \text{by (114)}\\
&= e_\gamma\phi_{s_0s_1}.
\end{aligned}$$

Now, to compute $\widehat{\mathcal{M}}(x_{\gamma,0})$, we first remark that $\widehat{\mathcal{M}}$ commutes with Γ_ϖ: indeed first of all, defining $(E^1)' \coloneqq \ker(f_1)\oplus\ker(g_1)$, one sees that it suffices to prove that the map

$$\widehat{\mathcal{M}}\colon e_\gamma(E^1)'\otimes_{E^0}(E^1)'\otimes_{E^0}(E^1)'e_\gamma \longrightarrow E^3$$

commutes with Γ_ϖ, since the identification

$$e_\gamma(E^1)'\otimes_{E^0}(E^1)'\otimes_{E^0}(E^1)'e_\gamma = e_\gamma E^1\otimes_{E^0}E^1\otimes_{E^0}E^1e_\gamma$$

of Lemma 4.9.5 commutes with Γ_ϖ. Then, since $\Gamma_\varpi(\zeta)=\zeta$, we see that the decomposition

$$e_\gamma(E^1)'\otimes_{E^0}(E^1)'\otimes_{E^0}(E^1)'e_\gamma = \bigoplus_{j,j',j''\in\{f_1,g_1\}} e_\gamma\ker(j)\otimes_{E^0}\ker(j')\otimes_{E^0}\ker(j'')e_\gamma$$

is preserved by Γ_ϖ, and so it suffices to prove the statement on each of these terms, and this can be immediately done by looking at the explicit definition of $\widehat{\mathcal{M}}$ on such term (and using again that $\Gamma_\varpi(\zeta)=\zeta$).

Therefore, we have seen that $\widehat{\mathcal{M}}$ commutes with Γ_ϖ, and so we can easily compute $\widehat{\mathcal{M}}(x_{\gamma,0})$ knowing already $\widehat{\mathcal{M}}(x_{\gamma,1})$:

$$\begin{aligned}
\widehat{\mathcal{M}}(x_{\gamma,0}) &= \widehat{\mathcal{M}}(-\Gamma_\varpi(x_{\gamma,1}))\\
&= \Gamma_\varpi(-\widehat{\mathcal{M}}(x_{\gamma,1}))\\
&= \Gamma_\varpi(-e_\gamma\phi_{s_0s_1})\\
&= -e_\gamma\phi_{s_1s_0}.
\end{aligned}$$

We see that the sum $\widehat{\mathcal{M}}(x_{\gamma,0})+\widehat{\mathcal{M}}(x_{\gamma,1})$ does not lie in F_1E^0, as we wanted. ∎

We are now able to prove the main result of this section, thus completing the proof of Theorem 4.8.1.

Corollary 4.9.12. *Let*

$$K_{2,3}\coloneqq \overline{\ker(\mathcal{M}_2)\otimes_{E^0}E^1}+\overline{E^1\otimes_{E^0}\ker(\mathcal{M}_2)}\subseteq T^3_{E^0}E^1,$$

as in Theorem 4.8.1. One has that the inclusion $K_{2,3}\subseteq\ker(\mathcal{M}_3)$ is not an equality.

Proof. There exists $\gamma \in \Gamma$ with $\gamma \neq \{1\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$; indeed, if $p \geqslant 7$ then this is clear because

$$\#\Gamma = \frac{p-1}{2} + 1 \geqslant 4.$$

If instead $p = 5$, then we see that $\{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\} = \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}$ and that we may choose $\gamma = \{\chi_0\}$, where χ_0 is the quadratic character.

In Lemma 4.9.9 we have seen that the map $\widetilde{\mathcal{M}}$ is zero on $e_\gamma K_{2,3} e_\gamma$, whereas in Lemma 4.9.11 we have seen that $\widetilde{\mathcal{M}}(e_\gamma x e_\gamma)$ is nonzero, where

$$x := (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^- .$$

Since $x \in \ker(\mathcal{M}_3)$ (see for example Remark 4.8.2, or for the proof Lemma 4.6.5), the result follows. ∎

Remark 4.9.13. Let $\gamma \in \Gamma$ with $\gamma \neq \{1\}, \{\underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}, \{\underline{\mathrm{id}}^3, \underline{\mathrm{id}}^{-3}\}$. It is possible to describe the "e_γ-component" of $\ker(\mathcal{M}_3)/K_{2,3}$. Let us refer to the following diagram, which we described in Remark 4.9.6:

$$\begin{tikzcd}
 & e_\gamma E^3 \arrow[r, "\text{quot.}"] \arrow[d, "\zeta \cdot (_)"'] & e_\gamma \cdot E^3/F_1E^3 \arrow[dl, "\Theta"] \\
e_\gamma E^1 \otimes_{E^0} E^1 \otimes_{E^0} E^1 e_\gamma \arrow[ur, "\widehat{\mathcal{M}}"] \arrow[urr, bend left, "\widetilde{\mathcal{M}} := (\text{quot.}) \circ \widehat{\mathcal{M}}"] \arrow[r, "\mathcal{M}"'] & e_\gamma E^3. &
\end{tikzcd}$$

We have the following facts.

(i) Let us define $\overline{K}_3^{(\gamma)} := e_\gamma \cdot (\ker(\mathcal{M}_3)/K_{2,3})$. One has:

$$\begin{aligned}
\overline{K}_3^{(\gamma)} &:= e_\gamma \cdot \Big(\ker(\mathcal{M}_3)/K_{2,3} \Big) \\
&\cong e_\gamma \cdot \Big(\ker(\mathcal{M}_3)/K_{2,3} \Big) \cdot e_\gamma \\
&\cong (e_\gamma \ker(\mathcal{M}_3) e_\gamma)/(e_\gamma K_{2,3} e_\gamma).
\end{aligned}$$

(ii) $e_\gamma K_{2,3} e_\gamma = \ker(\widetilde{\mathcal{M}})$.

(iii) $\overline{K}_3^{(\gamma)} \cong \ker(\Theta)$.

(iv) Explicitly, as a k-vector space

$$\overline{K}_3^{(\gamma)} \cong \begin{cases} ku_\lambda \oplus ku_{\lambda^{-1}} & \text{if } \gamma = \{\lambda, \lambda^{-1}\} \text{ with } \lambda \neq \lambda^{-1}, \\ ku_\lambda & \text{if } \gamma = \{\lambda\} \text{ (i.e., if } \gamma = \{\chi_0\}), \end{cases}$$

where u_λ and $u_{\lambda^{-1}}$ are indeterminates. Moreover, the structure of E^0-bimodule is the following: for $\mu \in \widehat{T^0/T^1}$ and for $\lambda \in \gamma$, the idempotent e_λ acts on u_μ as the Kronecker symbol $\delta_{\mu,\lambda}$ (both on the left and on the right), whereas both τ_{s_0} and τ_{s_1} act by 0 on u_μ (both on the left and on the right).

Proof. Let us prove the four statements.

(i) Let us set

$$x := (\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta^0_{s_1^{-1}} \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta^0_{s_0^{-1}} \otimes \beta_1^- .$$

and let us recall from Lemma 4.6.5 that $\ker(\mathcal{M}_3)/K_{2,3}$ is generated as a k-vector space by the elements $\tau_\omega \cdot x$ for $\omega \in T^0/T^1$, or, equivalently, by the elements $e_\mu x$ for $\mu \in \widehat{T^0/T^1}$. It is easy to see that $e_\mu x = x e_\mu = e_\mu x e_\mu$, and so the first isomorphism in (i) follows, and the second is clear.

(ii) We have proved in Lemma 4.9.9 that $e_\gamma K_{2,3} e_\gamma \subseteq \ker(\widetilde{\mathcal{M}})$, so it remains to prove the reverse inclusion. By the commutative diagram $\ker(\widetilde{\mathcal{M}}) \subseteq e_\gamma \ker(\mathcal{M}_3) e_\gamma$, and so, by what we have said above about $\ker(\mathcal{M}_3)/K_{2,3}$, we may write an element $y \in \ker(\widetilde{\mathcal{M}})$ as $y = z + a_\lambda e_\lambda x e_\lambda + a_{\lambda^{-1}} e_{\lambda^{-1}} x e_{\lambda^{-1}}$ for some $z \in e_\gamma K_{2,3} e_\gamma$ and some $a_\lambda, a_{\lambda^{-1}} \in k$. Let $\lambda' = \lambda$ or $\lambda' = \lambda^{-1}$. The computation we made in the proof of Lemma 4.9.11 then shows that

$$\begin{aligned} \widetilde{\mathcal{M}}(e_{\lambda'} x e_{\lambda'}) &= \widetilde{\mathcal{M}}(e_{\lambda'} e_\gamma x e_\gamma e_{\lambda'}) \\ &= e_{\lambda'} \cdot \overline{e_\gamma \phi_{s_0 s_1} - e_\gamma \phi_{s_1 s_0}} \\ &= e_{\lambda'} \cdot \overline{\phi_{s_0 s_1} - \phi_{s_1 s_0}}, \end{aligned}$$

where $\overline{(?)}$ means the class of (?) in $E^3/F_1 E^3$. Hence, we see that $\widetilde{\mathcal{M}}(e_\lambda x e_\lambda)$ and $\widetilde{\mathcal{M}}(e_{\lambda-1} x e_{\lambda^{-1}})$ are linearly independent if $\lambda \neq \lambda^{-1}$, respectively that $\widetilde{\mathcal{M}}(e_\lambda x e_\lambda)$ is nonzero if $\lambda = \lambda^{-1}$. Looking again at the equality

$$y = z + a_\lambda e_\lambda x e_\lambda + a_{\lambda^{-1}} e_{\lambda^{-1}} x e_{\lambda^{-1}},$$

we see that y must be equal to z, completing the proof of the inclusion $\ker(\widetilde{\mathcal{M}}) \subseteq e_\gamma K_{2,3} e_\gamma$.

(iii) The map $\widetilde{\mathcal{M}}$ restricted to $e_\gamma \ker(\mathcal{M}_3) e_\gamma$ has values in $\ker(\Theta)$ by the commutative diagram, and so. taking (ii) into account, we see that it induces an injective homomorphism of E^0-bimodules from $\overline{K}_3^{(\gamma)}$ to $\ker(\Theta)$. But this map is also surjective because, looking at the explicit description of Θ (proof of Lemma 4.9.1) one sees that $\ker(\Theta) = \operatorname{span}_k \left\{ e_\lambda \cdot \overline{\phi_{s_0 s_1} - \phi_{s_1 s_0}}, e_{\lambda^{-1}} \cdot \overline{\phi_{s_0 s_1} - \phi_{s_1 s_0}} \right\}$, and then we have shown in the preceding part of the proof that $e_\gamma K_{2,3} e_\gamma$ surjects onto this space.

(iv) The claimed explicit description follows from the explicit description of

$$\ker(\Theta) = \operatorname{span}_k \left\{ e_\lambda \cdot \overline{\phi_{s_0 s_1} - \phi_{s_1 s_0}}, e_{\lambda^{-1}} \cdot \overline{\phi_{s_0 s_1} - \phi_{s_1 s_0}} \right\}. \qquad \blacksquare$$

Remark 4.9.14. Before Lemma 4.6.2 we claimed without proof that the map $\mathcal{R}_3$ is not Γ_ϖ-invariant nor $\mathcal{J}$-invariant. As we now know that $K_{2,3}$ is properly contained in $\ker(\mathcal{M}_3)$ (Corollary 4.9.12), looking at the statement of Lemma 4.6.5 we see that

$$\Gamma_\varpi(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1) \notin K_{2,3}.$$

This clearly excludes the possibility that $\mathcal{R}_3(\phi_1)$ is Γ_ϖ-invariant (since $\Gamma_\varpi(\phi_1) = \phi_1$). But is also excludes the possibility that $\mathcal{R}_3(\phi_1)$ is $\mathcal{J}$-invariant: indeed, in Lemma 4.6.4 we have proved the congruence

$$\mathcal{J}(\mathcal{R}_3(\phi_1)) \equiv \Gamma_\varpi(\mathcal{R}_3(\phi_1)) \mod K_{2,3},$$

and so if we had $\mathcal{J}$-invariance, we would obtain that $\Gamma_\varpi(\mathcal{R}_3(\phi_1)) - \mathcal{R}_3(\phi_1) \in K_{2,3}$ (using also that $\mathcal{J}(\phi_1) = \phi_1$), contradicting what we said above.

4.10 The Ext-algebra in terms of generators and relations

Assumptions. We assume that $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $p \neq 2, 3$ (with the fixed choices of $\mathbf{T}$, of I, of the positive root and of the Chevalley system as in Section 1.5). Furthermore, we choose $\pi = p$. The elements $(\beta_w^-)_w$, $(\beta_w^0)_w$, $(\beta_w^+)_w$, $(\alpha_w^-)_w$, $(\alpha_w^0)_w$, $(\alpha_w^+)_w$, and $(\phi_w)_w$ are chosen as in Subsection 4.5.a.

In this section we will compute a presentation of E^* as a k-algebra, and, in particular, we will prove that E^* is finitely presented as a k-algebra. We will proceed as follows: we will compute a presentation of E^1 as an E^0-bimodule or, more precisely, as a left module over $E^0 \otimes_k (E^0)^{\mathrm{op}}$ (see Lemma 4.10.1) and we will compute a presentation of the Hecke algebra E^0 as a k-algebra (see Lemma 4.10.1). It is then easy to show that combining these two presentations one obtains a presentation of the tensor algebra $T^*_{E^0}E^1$ as a k-algebra (see Lemma 4.10.3). We will then put this together with the presentation of E^* as a quotient of $T^*_{E^0}E^1$ already seen in Remark 4.8.2, to finally achieve a presentation of E^* as a k-algebra (see Proposition 4.10.4).

Let us start by fixing once and for all a generator ω_0 of the cyclic group T^0/T^1:

$$T^0/T^1 = \langle \omega_0 \rangle, \tag{197}$$

and recall from (47) we denote by u_{ω_0} the unique element of $(\mathfrak{O}/\mathfrak{M})^\times$ such that

$$\omega_0 = \begin{pmatrix} u_{\omega_0}^{-1} & 0 \\ 0 & u_{\omega_0} \end{pmatrix}.$$

This definition actually makes sense also for $G = \mathrm{SL}_2(\mathfrak{F})$ where $\mathfrak{F}$ is an arbitrary locally compact non-archimedean field, and in Lemma 4.10.2 we will work under these more general assumptions.

In the next lemma we compute a presentation of E^1 as an E^0-bimodule (more precisely, as a left module over $E^0 \otimes_k (E^0)^{\mathrm{op}}$).

Lemma 4.10.1. *Let*

$$M := \bigoplus_{i=1}^{4} E^0 \otimes_k E^0,$$

endowed with the natural structure making it into a free $E^0 \otimes_k (E^0)^{\mathrm{op}}$-left-module of rank 4: call the canonical basis $\left(\widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0}\right)$. Let us consider the submodule N generated by the following elements:

$$\begin{aligned}
&\tau_{s_1} \cdot \widehat{\beta_1^-}, && \tau_{s_0} \cdot \widehat{\beta_1^+},\\
&\widehat{\beta_1^+} \cdot \tau_{s_0}, && \widehat{\beta_1^-} \cdot \tau_{s_1},\\
&(\tau_{s_0} + e_1) \cdot \widehat{\beta_1^-} \cdot (\tau_{s_0} + e_1) && (\tau_{s_1} + e_1) \cdot \widehat{\beta_1^+} \cdot (\tau_{s_1} + e_1)\\
&\qquad + 2e_{\underline{\mathrm{id}}}\widehat{\beta_{s_0}^0} + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^+}, && \qquad - 2e_{\underline{\mathrm{id}}^{-1}}\widehat{\beta_{s_1}^0} + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^-},\\
&\tau_{s_0} \cdot \widehat{\beta_{s_1}^0} + \widehat{\beta_{s_0}^0} \cdot \tau_{s_1}, && \tau_{s_1} \cdot \widehat{\beta_{s_0}^0} + \widehat{\beta_{s_1}^0} \cdot \tau_{s_0},\\
&(\tau_{s_0} + e_1) \cdot \widehat{\beta_{s_0}^0} + e_{\underline{\mathrm{id}}}\tau_{s_0} \cdot \widehat{\beta_1^-}, && (\tau_{s_1} + e_1) \cdot \widehat{\beta_{s_1}^0} - e_{\underline{\mathrm{id}}^{-1}}\tau_{s_1} \cdot \widehat{\beta_1^+},\\
&\widehat{\beta_{s_0}^0} \cdot (\tau_{s_0} + e_1) + e_{\underline{\mathrm{id}}^{-1}}\widehat{\beta_1^-} \cdot \tau_{s_0}, && \widehat{\beta_{s_1}^0} \cdot (\tau_{s_1} + e_1) - e_{\underline{\mathrm{id}}}\widehat{\beta_1^+} \cdot \tau_{s_1},\\
&\tau_{\omega_0} \cdot \widehat{\beta_1^-} - u_{\omega_0}^{-2}\widehat{\beta_1^-} \cdot \tau_{\omega_0}, && \tau_{\omega_0} \cdot \widehat{\beta_1^+} - u_{\omega_0}^{2}\widehat{\beta_1^+} \cdot \tau_{\omega_0},\\
&\tau_{\omega_0} \cdot \widehat{\beta_{s_0}^0} - \widehat{\beta_{s_0}^0} \cdot \tau_{\omega_0^{-1}}, && \tau_{\omega_0} \cdot \widehat{\beta_{s_1}^0} - \widehat{\beta_{s_1}^0} \cdot \tau_{\omega_0^{-1}}.
\end{aligned}$$

Denote by $\widetilde{\beta_1^-}$, $\widetilde{\beta_1^+}$, $\widetilde{\beta_{s_0}^0}$ and $\widetilde{\beta_{s_1}^0}$ respectively the images of $\widehat{\beta_1^-}$, $\widehat{\beta_1^+}$, $\widehat{\beta_{s_0}^0}$ and $\widehat{\beta_{s_1}^0}$ in M/N. One has an isomorphism of $E^0 \otimes_k (E^0)^{\mathrm{op}}$-left-modules

$$\begin{aligned}
M/N &\xrightarrow{\quad P \quad} E^1 \\
\widetilde{\beta_1^-} &\longmapsto \beta_1^-, \\
\widetilde{\beta_1^+} &\longmapsto \beta_1^+, \\
\widetilde{\beta_{s_0}^0} &\longmapsto \beta_{s_0}^0, \\
\widetilde{\beta_{s_1}^0} &\longmapsto \beta_{s_1}^0.
\end{aligned}$$

Proof. To show that we indeed have a well defined homomorphism of $E^0 \otimes_k (E^0)^{\mathrm{op}}$-left-modules it suffices to show that the elements of E^1 that we obtain from the elements in the list defining N by replacing $\widehat{\beta_1^-}$, $\widehat{\beta_1^+}$, $\widehat{\beta_{s_0}^0}$ and $\widehat{\beta_{s_1}^0}$ respectively by β_1^-, β_1^+, $\beta_{s_0}^0$ and $\beta_{s_1}^0$ are all zero. I.e., we want to say that the following elements are all zero:

$$\begin{aligned}
&\tau_{s_1} \cdot \beta_1^-, && \tau_{s_0} \cdot \beta_1^+, && (198)\\
&\beta_1^+ \cdot \tau_{s_0}, && \beta_1^- \cdot \tau_{s_1}, && (199)\\
&(\tau_{s_0} + e_1) \cdot \beta_1^- \cdot (\tau_{s_0} + e_1) && (\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot (\tau_{s_1} + e_1) && \\
&\qquad + 2e_{\underline{\mathrm{id}}}\beta_{s_0}^0 + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^+, && \qquad - 2e_{\underline{\mathrm{id}}^{-1}}\beta_{s_1}^0 + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^-, && (200)\\
&\tau_{s_0} \cdot \beta_{s_1}^0 + \beta_{s_0}^0 \cdot \tau_{s_1}, && \tau_{s_1} \cdot \beta_{s_0}^0 + \beta_{s_1}^0 \cdot \tau_{s_0}, && (201)\\
&(\tau_{s_0} + e_1) \cdot \beta_{s_0}^0 + e_{\underline{\mathrm{id}}}\tau_{s_0} \cdot \beta_1^-, && (\tau_{s_1} + e_1) \cdot \beta_{s_1}^0 - e_{\underline{\mathrm{id}}^{-1}}\tau_{s_1} \cdot \beta_1^+, && (202)\\
&\beta_{s_0}^0 \cdot (\tau_{s_0} + e_1) + e_{\underline{\mathrm{id}}^{-1}}\beta_1^- \cdot \tau_{s_0}, && \beta_{s_1}^0 \cdot (\tau_{s_1} + e_1) - e_{\underline{\mathrm{id}}}\beta_1^+ \cdot \tau_{s_1}, && (203)\\
&\tau_{\omega_0} \cdot \beta_1^- - u_{\omega_0}^{-2}\beta_1^- \cdot \tau_{\omega_0}, && \tau_{\omega_0} \cdot \beta_1^+ - u_{\omega_0}^{2}\beta_1^+ \cdot \tau_{\omega_0}, && (204)\\
&\tau_{\omega_0} \cdot \beta_{s_0}^0 - \beta_{s_0}^0 \cdot \tau_{\omega_0^{-1}}, && \tau_{\omega_0} \cdot \beta_{s_1}^0 - \beta_{s_1}^0 \cdot \tau_{\omega_0^{-1}}. && (205)
\end{aligned}$$

For line (198) see (63), for line (199) see (65). Regarding line (200), using again such results and also (61) and (66), we compute

$$\begin{aligned}
(\tau_{s_0} + e_1) \cdot \beta_1^- \cdot (\tau_{s_0} + e_1) &= \tau_{s_0} \cdot \beta_1^- \cdot \tau_{s_0} + e_1 \cdot \beta_1^- \cdot \tau_{s_0} + \tau_{s_0} \cdot \beta_1^- \cdot e_1 + e_1 \cdot \beta_1^- \cdot e_1 \\
&= \tau_{s_0} \cdot \beta_{s_0}^- + e_1\beta_{s_0}^- - e_{\underline{\mathrm{id}}^2}\beta_{s_0}^+ \\
&= \left(-e_1\beta_{s_0}^- - 2e_{\underline{\mathrm{id}}}\beta_{s_0}^0 + e_{\underline{\mathrm{id}}^2}\beta_{s_0}^+ - \beta_{c_{-1}}^+\right) + e_1\beta_{s_0}^- - e_{\underline{\mathrm{id}}^2}\beta_{s_0}^+ \\
&= -2e_{\underline{\mathrm{id}}}\beta_{s_0}^0 - \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^+.
\end{aligned}$$

Applying the automorphism Γ_ϖ, we also find that

$$\begin{aligned}
(\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot (\tau_{s_1} + e_1) &= \Gamma_\varpi\left((\tau_{s_0} + e_1) \cdot \beta_1^- \cdot (\tau_{s_0} + e_1)\right) \\
&= \Gamma_\varpi\left(-2e_{\underline{\mathrm{id}}}\beta_{s_0}^0 - \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^+\right) \\
&= 2e_{\underline{\mathrm{id}}^{-1}}\beta_{s_1}^0 - \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^-.
\end{aligned}$$

So this shows that the elements in the line (200) are zero. To show that the elements in line (201) are zero it suffices to use again the formulas (63) and (65). Similarly, for line (202) we use again (66) and for line (203) we use instead (67) and (68). Finally, for lines (204) and (205) we use (59) and (60).

Now, it remains to prove injectivity and surjectivity of our homomorphism P. Surjectivity is clear from the fact that the elements β_1^-, β_1^+, $\beta_{s_0}^0$ and $\beta_{s_1}^0$ generate E^1 as an E^0-bimodule (see Lemma 1.10.3). To prove injectivity, we adopt the following strategy: we fix a k-basis $\mathcal{B}$ of E^1, and, using surjectivity, for all $b \in \mathcal{B}$ we fix a preimage $m_b \in M/N$ (in other words we are constructing a section of P, as a homomorphism of k-vector spaces only). If we prove that the elements m_b generate M/N as a k-vector space then injectivity of P follows, because the family $(m_b)_{b\in\mathcal{B}}$ is made of linearly independent elements.

So, let us pursue the above strategy to prove injectivity. Let us consider the following list: on the second/third column we of course have a k-basis of E^1. It is also easy to see that the elements in the first column are mapped to the elements on the right column by P. Therefore, we are exactly in the setting outlined above, and it remains to prove that the elements in the first column generate M/N as a k-vector space.

$$
\begin{array}{llll}
\widetilde{\beta_{s_1}^0} \cdot \tau_{(s_0s_1)^j} \cdot \tau_\omega & \mapsto \beta_{s_1}^0 \cdot \tau_{(s_0s_1)^j} \cdot \tau_\omega & = \beta^0_{s_1(s_0s_1)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\beta_{s_0}^0} \cdot \tau_{s_1(s_0s_1)^j} \cdot \tau_\omega & \mapsto \beta_{s_0}^0 \cdot \tau_{s_1(s_0s_1)^j} \cdot \tau_\omega & = \beta^0_{s_0s_1(s_0s_1)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\beta_{s_0}^0} \cdot \tau_{(s_1s_0)^j} \cdot \tau_\omega & \mapsto \beta_{s_0}^0 \cdot \tau_{(s_1s_0)^j} \cdot \tau_\omega & = \beta^0_{s_0} \cdot \tau_{(s_1s_0)^j} \cdot \tau_\omega & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\beta_{s_1}^0} \cdot \tau_{s_0(s_1s_0)^j} \cdot \tau_\omega & \mapsto \beta_{s_1}^0 \cdot \tau_{s_0(s_1s_0)^j} \cdot \tau_\omega & = \beta^0_{s_1} \cdot \tau_{s_0(s_1s_0)^j} \cdot \tau_\omega & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\beta_1^-} \cdot \tau_\omega & \mapsto \beta_1^- \cdot \tau_\omega & = \beta^-_\omega & \omega \in T^0/T^1, \\
\widetilde{\beta_1^+} \cdot \tau_\omega & \mapsto \beta_1^+ \cdot \tau_\omega & = \beta^+_\omega & \omega \in T^0/T^1, \\
\widetilde{\beta_1^-} \cdot \tau_{(s_0s_1)^j} \cdot \tau_\omega & \mapsto \beta_1^- \cdot \tau_{(s_0s_1)^j} \cdot \tau_\omega & = \beta^-_{(s_0s_1)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 1}, \\
\widetilde{\beta_1^-} \cdot \tau_{s_0(s_1s_0)^j} \cdot \tau_\omega & \mapsto \beta_1^- \cdot \tau_{s_0(s_1s_0)^j} \cdot \tau_\omega & = \beta^-_{s_0(s_1s_0)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\beta_1^+} \cdot \tau_{(s_1s_0)^j} \cdot \tau_\omega & \mapsto \beta_1^+ \cdot \tau_{(s_1s_0)^j} \cdot \tau_\omega & = \beta^+_{(s_1s_0)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 1}, \\
\widetilde{\beta_1^+} \cdot \tau_{s_1(s_0s_1)^j} \cdot \tau_\omega & \mapsto \beta_1^+ \cdot \tau_{s_1(s_0s_1)^j} \cdot \tau_\omega & = \beta^+_{s_1(s_0s_1)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\tau_{(s_1s_0)^j} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega & \mapsto \tau_{(s_1s_0)^j} \cdot \beta_1^- \cdot \tau_\omega & = \beta^-_{(s_1s_0)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 1}, \\
\tau_{s_0(s_1s_0)^j} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega & \mapsto \tau_{s_0(s_1s_0)^j} \cdot \beta_1^- \cdot \tau_\omega & = -\beta^+_{s_0(s_1s_0)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}, \\
\tau_{(s_0s_1)^j} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega & \mapsto \tau_{(s_0s_1)^j} \cdot \beta_1^+ \cdot \tau_\omega & = \beta^+_{(s_0s_1)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 1}, \\
\tau_{s_1(s_0s_1)^j} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega & \mapsto \tau_{s_1(s_0s_1)^j} \cdot \beta_1^+ \cdot \tau_\omega & = -\beta^-_{s_1(s_0s_1)^j\omega} & \omega \in T^0/T^1,\ j \in \mathbb{Z}_{\geqslant 0}.
\end{array}
$$

It is easy to see that, in order to prove that the elements in the first column generate M/N as a k-vector space, 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 above:

$$
\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_w, \qquad \tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_w, \qquad \tau_v \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w, \qquad \tau_v \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w.
$$

We are going to prove this claim inductively. Namely, we will prove by induction on $\ell(v) + \ell(w)$ that the four elements above all lie in V. Let us treat the case $\ell(v) + \ell(w) = 0$. By definition of N the following equalities are clearly true:

$$
\begin{aligned}
&\tau_{\omega_0} \cdot \widetilde{\beta_1^-} = u_{\omega_0}^{-2} \widetilde{\beta_1^-} \cdot \tau_{\omega_0}, && \tau_{\omega_0} \cdot \widetilde{\beta_1^+} = u_{\omega_0}^{2} \widetilde{\beta_1^+} \cdot \tau_{\omega_0}, \\
&\tau_{\omega_0} \cdot \widetilde{\beta_{s_0}^0} = \widetilde{\beta_{s_0}^0} \cdot \tau_{\omega_0^{-1}}, && \tau_{\omega_0} \cdot \widetilde{\beta_{s_1}^0} = \widetilde{\beta_{s_1}^0} \cdot \tau_{\omega_0^{-1}}.
\end{aligned}
$$

But then we see inductively that for all $n \in \mathbb{Z}_{\geqslant 0}$ we have

$$\begin{aligned} \tau_{\omega_0^n} \cdot \widetilde{\beta_1^-} &= u_{\omega_0}^{-2n} \widetilde{\beta_1^-} \cdot \tau_{\omega_0^n}, & \tau_{\omega_0^n} \cdot \widetilde{\beta_1^+} &= u_{\omega_0}^{2n} \widetilde{\beta_1^+} \cdot \tau_{\omega_0^n}, \\ \tau_{\omega_0^n} \cdot \widetilde{\beta_{s_0}^0} &= \widetilde{\beta_{s_0}^0} \cdot \tau_{\omega_0^{-n}}, & \tau_{\omega_0^n} \cdot \widetilde{\beta_{s_1}^0} &= \widetilde{\beta_{s_1}^0} \cdot \tau_{\omega_0^{-n}}. \end{aligned} \tag{206}$$

Now we look again at the elements

$$\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_w, \qquad \tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_w, \qquad \tau_v \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w, \qquad \tau_v \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w$$

under our assumption that $\ell(v) + \ell(w) = 0$. Equivalently, we are assuming that $v, w \in T^0/T^1$. Since T^0/T^1 is cyclic generated by ω_0, we can apply formulas (206), which allows us to rewrite the element $\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_w$, up to a coefficient, in the form $\widetilde{\beta_1^-} \cdot \tau_\omega$ for a suitable $\omega \in T^0/T^1$, and now $\widetilde{\beta_1^-} \cdot \tau_\omega$ lies in V by definition of V. In the same way, we treat the elements $\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_w$, $\tau_v \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w$ and $\tau_v \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w$.

Now it remains to consider the induction step. We distinguish some different 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 $\widehat{\beta_1^+} \cdot \tau_{s_0}$ and $\widehat{\beta_1^-} \cdot \tau_{s_1}$ lie in N, we see that it suffices to treat the following cases:

  $$\begin{aligned} &\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_\omega && \text{for some } \omega \in T^0/T^1, \\ &\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_\omega && \text{for some } \omega \in T^0/T^1, \\ &\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0 w'} && \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_0 w') = \ell(w') + 1, \\ &\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1 w'} && \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_1 w') = \ell(w') + 1. \end{aligned}$$

  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 V, it suffices to consider the following cases:

  $$\begin{aligned} &\tau_{(s_1 s_0)^j \omega'} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega && \text{for some } j \in \mathbb{Z}_{\geqslant 0} \text{ and some } \omega, \omega' \in T^0/T^1, \\ &\tau_{s_0 (s_1 s_0)^j \omega'} \cdot \widetilde{\beta_1^-} \cdot \tau_\omega && \text{for some } j \in \mathbb{Z}_{\geqslant 0} \text{ and some } \omega, \omega' \in T^0/T^1, \\ &\tau_{(s_0 s_1)^j \omega'} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega && \text{for some } j \in \mathbb{Z}_{\geqslant 0} \text{ and some } \omega, \omega' \in T^0/T^1, \\ &\tau_{s_1 (s_0 s_1)^j \omega'} \cdot \widetilde{\beta_1^+} \cdot \tau_\omega && \text{for some } j \in \mathbb{Z}_{\geqslant 0} \text{ and some } \omega, \omega' \in T^0/T^1. \end{aligned}$$

  If $\omega' = 1$ then these elements are in V because they are in the list of generators of V, and we can reduce to this situation exactly as we did in the case $\ell(v) + \ell(w) = 0$.

  Now we have to treat the elements

  $$\begin{aligned} &\tau_v \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0} \cdot \tau_{w'} && \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_0 w') = \ell(w') + 1, \\ &\tau_v \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1} \cdot \tau_{w'} && \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_1 w') = \ell(w') + 1. \end{aligned}$$

  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 $\ell(v) \geqslant 1$. In this case, using again that both $\tau_{s_1} \cdot \widehat{\beta_1^-}$ and $\tau_{s_0} \cdot \widehat{\beta_1^+}$ lie in V, we are reduced to considering elements of the following forms:

  $$\begin{aligned} &\tau_{v'} \cdot \tau_{s_0} \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0} \cdot \tau_{w'} && \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_0 w') = \ell(w') + 1, \\ &\tau_{v'} \cdot \tau_{s_1} \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1} \cdot \tau_{w'} && \text{for some } w' \in \widetilde{W} \text{ such that } \ell(s_1 w') = \ell(w') + 1. \end{aligned}$$

Now we use that the two elements

$$(\tau_{s_0} + e_1) \cdot \widehat{\beta_1^-} \cdot (\tau_{s_0} + e_1) + 2e_{\underline{\mathrm{id}}}\widehat{\beta_{s_0}^0} + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^+},$$
$$(\tau_{s_1} + e_1) \cdot \widehat{\beta_1^+} \cdot (\tau_{s_1} + e_1) - 2e_{\underline{\mathrm{id}}^{-1}}\widehat{\beta_{s_1}^0} + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^-}$$

are both in N, and we combine this with the inductive hypothesis that all of the elements

$$\tau_{v''} \cdot \widetilde{\beta_1^-} \cdot \tau_{w''}, \qquad \tau_{v''} \cdot \widetilde{\beta_1^+} \cdot \tau_{w''}, \qquad \tau_{v''} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_{w''}, \qquad \tau_{v''} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_{w''}$$

lie in V for all $v'', w'' \in \widetilde{W}$ such that $\ell(v'') + \ell(w'') < \ell(v) + \ell(w)$. By combining these two facts, it is then easy to conclude that the elements $\tau_{v's_0} \cdot \widetilde{\beta_1^-} \cdot \tau_{s_0w'}$ and $\tau_{v's_1} \cdot \widetilde{\beta_1^+} \cdot \tau_{s_1w'}$ 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 $\ell(vs_i) = \ell(v) + 1$ and $\ell(s_iw) = \ell(w) + 1$.

  Making v explicit, we see that we are dealing with the following elements:

$$\begin{aligned}
\tau_{(s_0s_1)^i\omega} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w &\quad \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1,\ w \in \widetilde{W} \text{ with } \ell(s_0w) = \ell(w) + 1,\\
\tau_{s_1(s_0s_1)^i\omega} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w &\quad \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1,\ w \in \widetilde{W} \text{ with } \ell(s_0w) = \ell(w) + 1,\\
\tau_{(s_1s_0)^i\omega} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w &\quad \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1,\ w \in \widetilde{W} \text{ with } \ell(s_1w) = \ell(w) + 1,\\
\tau_{s_0(s_1s_0)^i\omega} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w &\quad \text{for } i \in \mathbb{Z}_{\geqslant 0},\ \omega \in T^0/T^1,\ w \in \widetilde{W} \text{ with } \ell(s_1w) = \ell(w) + 1.
\end{aligned}$$

  As usual, we see that we can assume without loss of generality that $\omega = 1$, and then, using repeatedly that the elements

$$\tau_{s_0} \cdot \widehat{\beta_{s_1}^0} + \widehat{\beta_{s_0}^0} \cdot \tau_{s_1}, \qquad \tau_{s_1} \cdot \widehat{\beta_{s_0}^0} + \widehat{\beta_{s_1}^0} \cdot \tau_{s_0}$$

  are in N, we rewrite the elements we are dealing with as

$$\begin{aligned}
\tau_{(s_0s_1)^i} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w &= \widetilde{\beta_{s_0}^0} \cdot \tau_{(s_1s_0)^i} \cdot \tau_w\\
&= \widetilde{\beta_{s_0}^0} \cdot \tau_{(s_1s_0)^iw}\\
&\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and for } w \in \widetilde{W} \text{ with } \ell(s_0w) = \ell(w) + 1,\\
\tau_{s_1(s_0s_1)^i} \cdot \widetilde{\beta_{s_0}^0} \cdot \tau_w &= -\widetilde{\beta_{s_1}^0} \cdot \tau_{s_0(s_1s_0)^i} \cdot \tau_w\\
&= -\widetilde{\beta_{s_1}^0} \cdot \tau_{s_0(s_1s_0)^iw}\\
&\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and for } w \in \widetilde{W} \text{ with } \ell(s_0w) = \ell(w) + 1,\\
\tau_{(s_1s_0)^i} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w &= \widetilde{\beta_{s_1}^0} \cdot \tau_{(s_0s_1)^i} \cdot \tau_w\\
&= \widetilde{\beta_{s_1}^0} \cdot \tau_{(s_0s_1)^iw}\\
&\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and for } w \in \widetilde{W} \text{ with } \ell(s_1w) = \ell(w) + 1,\\
\tau_{s_0(s_1s_0)^i} \cdot \widetilde{\beta_{s_1}^0} \cdot \tau_w &= -\widetilde{\beta_{s_0}^0} \cdot \tau_{s_1(s_0s_1)^i} \cdot \tau_w\\
&= -\widetilde{\beta_{s_0}^0} \cdot \tau_{s_1(s_0s_1)^iw}\\
&\qquad\qquad \text{for } i \in \mathbb{Z}_{\geqslant 0} \text{ and for } w \in \widetilde{W} \text{ with } \ell(s_1w) = \ell(w) + 1.
\end{aligned}$$

  So, up to a sign, we see that we have obtained elements in the list of generators of V.

- Now we consider the elements $\tau_v \cdot \widetilde{\beta^0_{s_i}} \cdot \tau_w$ (for $i \in \{0,1\}$) under the additional assumption that $\ell(s_i w) = \ell(w) - 1$.

  In this case, we use that the elements

$$\widehat{\beta^0_{s_0}} \cdot (\tau_{s_0} + e_1) + e_{\underline{\mathrm{id}}^{-1}} \widehat{\beta^-_1} \cdot \tau_{s_0}, \qquad \widehat{\beta^0_{s_1}} \cdot (\tau_{s_1} + e_1) - e_{\underline{\mathrm{id}}} \widehat{\beta^+_1} \cdot \tau_{s_1}$$

  lie in N. Indeed, we can do the following computation (we only treat the case $i = 0$, the other being completely analogous):

$$\begin{aligned}
\tau_v \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_w &= \tau_v \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_{s_0} \cdot \tau_{s_0^{-1}w} \\
&= \tau_v \cdot \left(-\widetilde{\beta^0_{s_0}} \cdot e_1 - e_{\underline{\mathrm{id}}^{-1}} \widetilde{\beta^-_1} \cdot \tau_{s_0} \right) \cdot \tau_{s_0^{-1}w} \\
&= -\tau_v \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_{s_0^{-1}w} e_1 - \tau_v e_{\underline{\mathrm{id}}^{-1}} \cdot \widetilde{\beta^-_1} \cdot \tau_w.
\end{aligned}$$

  Using the definitions of e_1 and $e_{\underline{\mathrm{id}}^{-1}}$, we see that we are dealing with terms of the form

$$\begin{aligned}
&\tau_v \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_{s_0^{-1}w\omega} && \text{for some } \omega \in T^0/T^1, \\
&\tau_{v\omega'} \cdot \widetilde{\beta^-_1} \cdot \tau_w && \text{for some } \omega' \in T^0/T^1.
\end{aligned}$$

  If we look at the element in the first line, we have $\ell(v) + \ell(s_0^{-1}w\omega) = \ell(v) + \ell(w) - 1$, and so we can apply the inductive hypothesis, while if we look at the element in the second line we have $\ell(v\omega') + \ell(w) = \ell(v) + \ell(w)$, and so we can use the fact that we have already studied the element $\tau_{v\omega'} \cdot \widetilde{\beta^-_1} \cdot \tau_w$. In conclusion, we see that $\tau_v \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_w$ lies in V.

- Now it remains to treat the elements $\tau_v \cdot \widetilde{\beta^0_{s_i}} \cdot \tau_w$ (for $i \in \{0,1\}$) under the additional assumption that $\ell(v s_i) = \ell(v) - 1$.

  This time the relevant elements in N are

$$(\tau_{s_0} + e_1) \cdot \widehat{\beta^0_{s_0}} + e_{\underline{\mathrm{id}}} \tau_{s_0} \cdot \widehat{\beta^-_1}, \qquad (\tau_{s_1} + e_1) \cdot \widehat{\beta^0_{s_1}} - e_{\underline{\mathrm{id}}^{-1}} \tau_{s_1} \cdot \widehat{\beta^+_1}$$

  and the proof is completely analogous to the last one. For completeness, we add the relevant computations:

$$\begin{aligned}
\tau_v \cdot \widetilde{\beta^0_{s_1}} \cdot \tau_w &= \tau_v \cdot \widetilde{\beta^0_{s_1}} \cdot \tau_{s_1} \cdot \tau_{s_1^{-1}w} \\
&= \tau_v \cdot \left(-\widetilde{\beta^0_{s_1}} \cdot e_1 + e_{\underline{\mathrm{id}}} \widetilde{\beta^+_1} \cdot \tau_{s_1} \right) \cdot \tau_{s_1^{-1}w} \\
&= -\tau_v \cdot \widetilde{\beta^0_{s_1}} \cdot e_1 \tau_{s_1^{-1}w} + \tau_v e_{\underline{\mathrm{id}}} \cdot \widetilde{\beta^+_1} \cdot \tau_w, \\
\tau_v \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_w &= \tau_{vs_0^{-1}} \cdot \tau_{s_0} \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_w \\
&= \tau_{vs_0^{-1}} \cdot \left(-e_1 \cdot \widetilde{\beta^0_{s_0}} - e_{\underline{\mathrm{id}}} \tau_{s_0} \cdot \widetilde{\beta^-_1} \right) \cdot \tau_w \\
&= -\tau_{vs_0^{-1}} e_1 \cdot \widetilde{\beta^0_{s_0}} \cdot \tau_w - \tau_v e_{\underline{\mathrm{id}}^{-1}} \cdot \widetilde{\beta^-_1} \cdot \tau_w, \\
\tau_v \cdot \widetilde{\beta^0_{s_1}} \cdot \tau_w &= \tau_{vs_1^{-1}} \cdot \tau_{s_1} \cdot \widetilde{\beta^0_{s_1}} \cdot \tau_w \\
&= \tau_{vs_1^{-1}} \cdot \left(-e_1 \cdot \widetilde{\beta^0_{s_1}} + e_{\underline{\mathrm{id}}^{-1}} \tau_{s_1} \cdot \widetilde{\beta^+_1} \right) \cdot \tau_w \\
&= -\tau_{vs_1^{-1}} e_1 \cdot \widetilde{\beta^0_{s_1}} \cdot \tau_w + \tau_v e_{\underline{\mathrm{id}}} \cdot \widetilde{\beta^+_1} \cdot \tau_w.
\end{aligned}$$

■

In the next lemma we compute a presentation of the Hecke algebra $E^0 = H$. Since the Ext-algebra is not involved, we prove this under slightly more general assumptions. We remark that Große-Klönne has instead computed a finite presentation of H in the case $G = \mathrm{GL}_n(\mathfrak{F})$ (see [GK20, §2.1]).

Lemma 4.10.2. *For this lemma only let us assume more generally that $G = \mathrm{SL}_2(\mathfrak{F})$, where $\mathfrak{F}$ is an arbitrary locally compact non-archimedean field (i.e., not necessarily $\mathfrak{F} = \mathbb{Q}_p$ with $p \neq 2, 3$). The pro-p Iwahori–Hecke algebra $H = E^0$ can be expressed by generators and relations as follows. Let us choose a generator ω_0 of the cyclic group T^0/T^1 (of order $q-1$). Let*

$$k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle$$

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 bilateral ideal of $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle$ generated by the following elements

$$\begin{aligned}
&\widehat{\tau_{\omega_0}}^{q-1} - 1, \\
&\widehat{\tau_{\omega_0}} \cdot \widehat{\tau_{s_0}} - \widehat{\tau_{s_0}} \cdot \widehat{\tau_{\omega_0}}^{q-2}, && \widehat{\tau_{\omega_0}} \cdot \widehat{\tau_{s_1}} - \widehat{\tau_{s_1}} \cdot \widehat{\tau_{\omega_0}}^{q-2}, \\
&\widehat{\tau_{s_0}}^2 - \sum_{i=0}^{q-2} \widehat{\tau_{\omega_0}}^i \cdot \widehat{\tau_{s_0}}, && \widehat{\tau_{s_1}}^2 - \sum_{i=0}^{q-2} \widehat{\tau_{\omega_0}}^i \cdot \widehat{\tau_{s_1}}.
\end{aligned}$$

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 $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I$. One has an isomorphism of k-algebras

$$\begin{aligned}
k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I &\longrightarrow H = E^0 \\
\widetilde{\tau_{\omega_0}} &\longmapsto \tau_{\omega_0}, \\
\widetilde{\tau_{s_0}} &\longmapsto \tau_{s_0}, \\
\widetilde{\tau_{s_1}} &\longmapsto \tau_{s_1}.
\end{aligned}$$

Proof. We do have a well defined homomorphism of k-algebras as in the statement, because the following relations holds in the pro-p Iwahori–Hecke algebra:

$$\begin{aligned}
&\tau_{\omega_0}^{q-1} = 1, \\
&\tau_{\omega_0} \cdot \tau_{s_0} = \tau_{s_0} \cdot \tau_{\omega_0^{-1}} = \tau_{s_0} \cdot \tau_{\omega_0}^{q-2}, && \tau_{\omega_0} \cdot \tau_{s_1} = \tau_{s_1} \cdot \tau_{\omega_0^{-1}} = \tau_{s_1} \cdot \tau_{\omega_0}^{q-2}, \\
&\tau_{s_0}^2 = -e_1 \tau_{s_0} = \sum_{i=0}^{q-2} \tau_{\omega_0}^i \cdot \tau_{s_0}, && \tau_{s_1}^2 = -e_1 \tau_{s_1} = \sum_{i=0}^{q-2} \tau_{\omega_0}^i \cdot \tau_{s_1}.
\end{aligned}$$

Since this homomorphism is clearly surjective, it remains to prove that it is injective. Similarly to Lemma 4.10.1, we adopt the following strategy: we fix a k-basis $\mathcal{B}$ of E^0, and, using surjectivity, for all $b \in \mathcal{B}$ we fix a preimage $r_b \in k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I$ (in other words we are constructing a section of our homomorphism, as a homomorphism of k-vector spaces only). If we prove that the elements r_b generate $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I$ as a k-vector space then injectivity follows, because the family $(r_b)_{b \in \mathcal{B}}$ is made of linearly independent elements.

So, let us pursue the above strategy to prove injectivity. Let us consider the following list: on the second column we of course have a k-basis of $H = E^0$. It is also easy to see that the elements in the first column are mapped to the elements on the right column by our k-algebra homomorphism $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I \longrightarrow H = E^0$.

Therefore, we are exactly in the setting outlined above, and it remains to prove that the elements in the first column generate $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I$ as a k-vector space.

$$\begin{array}{lcll}
\widetilde{\tau_{\omega_0}}^{\,i} & \longmapsto & \tau_{\omega_0^i} & \text{for } i \in \{0, \dots, q-2\}, \\
\widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_1}} \cdot (\widetilde{\tau_{s_0}} \cdot \widetilde{\tau_{s_1}})^j & \longmapsto & \tau_{s_1 (s_0 s_1)^j \omega_0^i} & \text{for } i \in \{0, \dots, q-2\} \text{ and } j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_0}} \cdot (\widetilde{\tau_{s_1}} \cdot \widetilde{\tau_{s_0}})^j & \longmapsto & \tau_{s_0 (s_1 s_0)^j \omega_0^i} & \text{for } i \in \{0, \dots, q-2\} \text{ and } j \in \mathbb{Z}_{\geqslant 0}, \\
\widetilde{\tau_{\omega_0}}^{\,i} \cdot (\widetilde{\tau_{s_0}} \cdot \widetilde{\tau_{s_1}})^j & \longmapsto & \tau_{(s_0 s_1)^j \omega_0^i} & \text{for } i \in \{0, \dots, q-2\} \text{ and } j \in \mathbb{Z}_{\geqslant 1}, \\
\widetilde{\tau_{\omega_0}}^{\,i} \cdot (\widetilde{\tau_{s_1}} \cdot \widetilde{\tau_{s_0}})^j & \longmapsto & \tau_{(s_1 s_0)^j \omega_0^i} & \text{for } i \in \{0, \dots, q-2\} \text{ and } j \in \mathbb{Z}_{\geqslant 1}.
\end{array}$$

So, let us prove that the elements in the first column generate $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle / I$ as a k-vector space. Let us denote by V the k-vector space that they generate. It suffices to prove that every element of the form

$$\widetilde{\tau_{w_1}} \cdots \widetilde{\tau_{w_n}}$$

lies in V for all $n \in \mathbb{Z}_{\geqslant 0}$ and $w_1, \dots, w_n \in \{\omega_0, s_0, s_1\}$. Using the relations

$$\begin{aligned}
&\widetilde{\tau_{\omega_0}}^{\,q-1} = 1, \\
&\widetilde{\tau_{\omega_0}} \cdot \widetilde{\tau_{s_0}} = \widetilde{\tau_{s_0}} \cdot \widetilde{\tau_{\omega_0}}^{\,q-2}, \qquad\qquad \widetilde{\tau_{\omega_0}} \cdot \widetilde{\tau_{s_1}} = \widetilde{\tau_{s_1}} \cdot \widetilde{\tau_{\omega_0}}^{\,q-2},
\end{aligned}$$

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 $i \in \{0, \dots, q-2\}$, for $m \in \mathbb{Z}_{\geqslant 0}$ and for $l_1, \dots, l_m \in \{0, 1\}$. We now prove that the element $\widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_m}}}$ 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. So we can assume that there is at least one such pair of indices. Then, we have

$$\begin{aligned}
\widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_m}}} &= \widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_j}}} \cdot \widetilde{\tau_{s_{l_{j+1}}}} \cdots \widetilde{\tau_{s_{l_m}}} \\
&= \widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_j}}} \cdot \widetilde{\tau_{s_{l_j}}} \cdots \widetilde{\tau_{s_{l_m}}} \\
&= \widetilde{\tau_{\omega_0}}^{\,i} \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_{j-1}}}} \cdot \left(\sum_{i'=0}^{q-2} \widetilde{\tau_{\omega_0}}^{\,i'} \cdot \widetilde{\tau_{s_{l_j}}} \right) \cdot \widetilde{\tau_{s_{l_{j+2}}}} \cdots \widetilde{\tau_{s_{l_m}}}.
\end{aligned}$$

Using distributivity and again the formulas involving $\widetilde{\tau_{\omega_0}}$, we obtain a sum of elements of the form

$$\widetilde{\tau_{\omega_0}}^{\,i''} \cdot \widetilde{\tau_{s_{l_1}}} \cdots \widetilde{\tau_{s_{l_{j-1}}}} \cdot \widetilde{\tau_{s_{l_j}}} \cdot \widetilde{\tau_{s_{l_{j+2}}}} \cdots \widetilde{\tau_{s_{l_m}}}$$

for some $i'' \in \{0, \dots, q-2\}$, and these elements lie in V by inductive hypothesis. ∎

For the next lemma, we need to introduce some notation.

Let us consider indeterminates $\widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0}$ and the ring of non-commutative polynomials $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle$. Let $\lambda \colon T^0/T^1 \longrightarrow k^\times$ be a group homomorphism. 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 recall the list of elements we used to represent $H = E^0$ as a quotient of the ring of non-commutative polynomials $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}} \right\rangle$ in Lemma 4.10.2; we rewrite it using ε_1 where appropriate (and we write p instead of q since we are working with $\mathbb{Q}_p$):

$$
\begin{aligned}
&\widehat{\tau_{\omega_0}}^{p-1} - 1, & & \\
&\widehat{\tau_{\omega_0}} \cdot \widehat{\tau_{s_0}} - \widehat{\tau_{s_0}} \cdot \widehat{\tau_{\omega_0}}^{p-2}, & &\widehat{\tau_{\omega_0}} \cdot \widehat{\tau_{s_1}} - \widehat{\tau_{s_1}} \cdot \widehat{\tau_{\omega_0}}^{p-2}, \\
&\widehat{\tau_{s_0}}^2 + \varepsilon_1 \cdot \widehat{\tau_{s_0}}, & &\widehat{\tau_{s_1}}^2 + \varepsilon_1 \cdot \widehat{\tau_{s_1}}.
\end{aligned}
\tag{207}
$$

Furthermore, let consider the following list of elements, obtaining from the list in Lemma 4.10.1 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 $\lambda \in \{1, \underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}$:

$$
\begin{aligned}
&\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) \\
&\qquad + 2\varepsilon_{\underline{\mathrm{id}}} \widehat{\beta_{s_0}^0} + \widehat{\tau_{\omega_0}}^{\frac{p-1}{2}} \cdot \widehat{\beta_1^+}, & &\qquad - 2\varepsilon_{\underline{\mathrm{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{\mathrm{id}}} \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^-}, & &(\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_{s_1}^0} - \varepsilon_{\underline{\mathrm{id}}^{-1}} \widehat{\tau_{s_1}} \cdot \widehat{\beta_1^+}, \\
&\widehat{\beta_{s_0}^0} \cdot (\widehat{\tau_{s_0}} + \varepsilon_1) + \varepsilon_{\underline{\mathrm{id}}^{-1}} \widehat{\beta_1^-} \cdot \widehat{\tau_{s_0}}, & &\widehat{\beta_{s_1}^0} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) - \varepsilon_{\underline{\mathrm{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{aligned}
\tag{208}
$$

Lemma 4.10.3. *Let R_{E^0,E^1} be the quotient ring of the ring of non-commutative polynomials*

$$k \left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle$$

modulo the bilateral ideal I_{E^0,E^1} generated by the elements in the lists (207) *and* (208). *For all $\sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}$ let us denote by $\widetilde{\sigma}$ the image of $\widehat{\sigma}$ in R_{E^0,E^1}. One has an isomorphism of k-algebras*

$$
\begin{aligned}
R_{E^0,E^1} &\longrightarrow T^*_{E^0} E^1 \\
\underset{(\text{for } \sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\})}{\widetilde{\sigma}} &\longmapsto \sigma.
\end{aligned}
$$

Proof. Let $\iota_0 \colon E^0 \longrightarrow T^*_{E^0} E^1$ and $\iota_1 \colon E^1 \longrightarrow T_{E^0} E^1$ be the canonical inclusions. It is easy to check that the triple $(T_{E^0} E^1, \iota_0, \iota_1)$ enjoys the following universal property: for all triples (R, ξ_0, ξ_1) consisting of a k-algebra R (associative, not necessarily commutative), a homomorphism of k-algebras $\xi_0 \colon E^0 \longrightarrow R$ and a homomorphism of left $E^0 \otimes_k (E^0)^{\mathrm{op}}$-modules $\xi_1 \colon E^1 \longrightarrow R$ (where R is a left $E^0 \otimes_k (E^0)^{\mathrm{op}}$-module via ξ_0), there exists a unique homomorphism of k-algebras $\eta \colon T^*_{E^0} E^1 \longrightarrow R$ making the following diagrams commute:

$$
\begin{tikzcd}
 & T^*_{E^0} E^1 \arrow[d, "\eta"] \\
E^0 \arrow[ur, "\iota_0"] \arrow[r, "\xi_0"'] & R,
\end{tikzcd}
\qquad
\begin{tikzcd}
 & T^*_{E^0} E^1 \arrow[d, "\eta"] \\
E^1 \arrow[ur, "\iota_1"] \arrow[r, "\xi_1"'] & R.
\end{tikzcd}
$$

Using the presentation of E^0 given in Lemma 4.10.2, we see that there is a well defined homomorphism of k-algebras

$$\begin{aligned} H = E^0 &\xrightarrow{\xi_0} R_{E^0,E^1} \\ \tau_{\omega_0} &\longmapsto \widetilde{\tau_{\omega_0}}, \\ \tau_{s_0} &\longmapsto \widetilde{\tau_{s_0}}, \\ \tau_{s_1} &\longmapsto \widetilde{\tau_{s_1}}. \end{aligned}$$

Furthermore, using the presentation of E^1 as a left $E^0 \otimes_k (E^0)^{\mathrm{op}}$-module given in Lemma 4.10.1, we also see that there is a homomorphism of left $E^0 \otimes_k (E^0)^{\mathrm{op}}$-modules (where R_{E^0,E^1} is a left $E^0 \otimes_k (E^0)^{\mathrm{op}}$-module via ξ_0)

$$\begin{aligned} E^1 &\xrightarrow{\xi_1} R_{E^0,E^1} \\ \beta_1^- &\longmapsto \widetilde{\beta_1^-}, \\ \beta_1^+ &\longmapsto \widetilde{\beta_1^+}, \\ \beta_{s_0}^0 &\longmapsto \widetilde{\beta_{s_0}^0}, \\ \beta_{s_1}^0 &\longmapsto \widetilde{\beta_{s_1}^0}. \end{aligned}$$

Hence, by the universal property mentioned above, we get a homomorphism of k-algebras

$$\begin{aligned} T_{E^0}^* E^1 &\longrightarrow R_{E^0,E^1} \\ \underset{(\text{for } \sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\})}{\sigma} &\longmapsto \widetilde{\sigma}. \end{aligned}$$

On the other side it makes sense to define a homomorphism of k-algebras in the opposite direction

$$\begin{aligned} R_{E^0,E^1} &\longrightarrow T_{E^0}^* E^1 \\ \underset{(\text{for } \sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\})}{\widetilde{\sigma}} &\longmapsto \sigma \end{aligned}$$

as in the statement of the lemma, because we can define a suitable homomorphism on the k-algebra $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle$ which is clearly zero on I_{E^0,E^1}. But we see that, with the above procedure, we have obtained an inverse of this homomorphism (using also that $\{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}$ is a set of generators of $T_{E^0}^* E^1$ as a k-algebra), thus concluding the proof of the lemma. ■

Now, let us introduce some notation in order to finally achieve a presentation of the algebra E^* by generators and relations.

We have already computed the following list of generators of the kernel of $\mathcal{M}$ as a bilateral ideal (Remark 4.8.2):

$$
\begin{array}{lll}
\beta_1^- \otimes \beta_1^-, & \beta_1^+ \otimes \beta_1^-, & \beta_{s_1}^0 \otimes \beta_1^-, \\
\beta_1^- \otimes \beta_1^+, & \beta_1^+ \otimes \beta_1^+, & \beta_{s_0}^0 \otimes \beta_1^+, \\
\beta_1^+ \otimes \beta_{s_0}^0, & \beta_{s_1}^0 \otimes \beta_{s_0}^0, & \\
\beta_1^- \otimes \beta_{s_1}^0, & \beta_{s_0}^0 \otimes \beta_{s_1}^0, & \\
\multicolumn{3}{l}{\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\mathrm{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- - e_1 \cdot \beta_1^- \otimes \beta_{s_0}^+,} \\
\multicolumn{3}{l}{\beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\underline{\mathrm{id}}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ - e_1 \cdot \beta_1^+ \otimes \beta_{s_1}^-,} \\
\multicolumn{3}{l}{\beta_{s_0}^+ \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_{s_0}^-,} \\
\multicolumn{3}{l}{\beta_{s_1}^- \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_{s_1}^+,} \\
\multicolumn{3}{l}{(\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1^{-1}}^0 \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0^{-1}}^0 \otimes \beta_1^-.}
\end{array}
$$

We express this only using the generators $\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0$ (and the idempotents, which can be easily expressed in terms of τ_{ω_0}): we delete the exponent -1 which appears in the last line (we can do this by multiplying with the invertible element $\tau_{c_{-1}}$) and we use the formulas

$$
\begin{array}{ll}
\tau_{s_0} \cdot \beta_1^- = -\beta_{s_0}^+, & \tau_{s_1} \cdot \beta_1^+ = -\beta_{s_1}^-, \\
\beta_1^- \cdot \tau_{s_0} = \beta_{s_0}^-, & \beta_1^+ \cdot \tau_{s_1} = \beta_{s_1}^+.
\end{array}
$$

Doing this, we deduce that the following is again a list of generators of the kernel of $\mathcal{M}$ as a bilateral ideal:

$$
\begin{array}{lll}
\beta_1^- \otimes \beta_1^-, & \beta_1^+ \otimes \beta_1^-, & \beta_{s_1}^0 \otimes \beta_1^-, \\
\beta_1^- \otimes \beta_1^+, & \beta_1^+ \otimes \beta_1^+, & \beta_{s_0}^0 \otimes \beta_1^+, \\
\beta_1^+ \otimes \beta_{s_0}^0, & \beta_{s_1}^0 \otimes \beta_{s_0}^0, & \\
\beta_1^- \otimes \beta_{s_1}^0, & \beta_{s_0}^0 \otimes \beta_{s_1}^0, & \\
\multicolumn{3}{l}{\beta_{s_0}^0 \otimes \beta_{s_0}^0 + e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_1^- \otimes \beta_{s_0}^0 + e_{\underline{\mathrm{id}}} \cdot \beta_{s_0}^0 \otimes \beta_1^- + e_1 \cdot \beta_1^- \otimes (\tau_{s_0} \cdot \beta_1^-),} \\
\multicolumn{3}{l}{\beta_{s_1}^0 \otimes \beta_{s_1}^0 - e_{\underline{\mathrm{id}}} \cdot \beta_1^+ \otimes \beta_{s_1}^0 - e_{\underline{\mathrm{id}}^{-1}} \cdot \beta_{s_1}^0 \otimes \beta_1^+ + e_1 \cdot \beta_1^+ \otimes (\tau_{s_1} \cdot \beta_1^+),} \\
\multicolumn{3}{l}{-\tau_{s_0} \cdot \beta_1^- \otimes \beta_{s_0}^0 + \beta_{s_0}^0 \otimes \beta_1^- \cdot \tau_{s_0},} \\
\multicolumn{3}{l}{-\tau_{s_1} \cdot \beta_1^+ \otimes \beta_{s_1}^0 + \beta_{s_1}^0 \otimes \beta_1^+ \cdot \tau_{s_1},} \\
\multicolumn{3}{l}{(\tau_{s_1} + e_1) \cdot \beta_1^+ \otimes \beta_{s_1}^0 \otimes \beta_1^+ + (\tau_{s_0} + e_1) \cdot \beta_1^- \otimes \beta_{s_0}^0 \otimes \beta_1^-.}
\end{array}
$$

Now, we consider the following list of elements of $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle$, list which is obtained from the above one by replacing β_1^- with $\widehat{\beta_1^-}$, by replacing β_1^+ with $\widehat{\beta_1^+}$, by replacing $\beta_{s_i}^0$ with $\widehat{\beta_{s_i}^0}$ for $i \in \{0,1\}$, by replacing τ_{s_i} with $\widehat{\tau_{s_i}}$ for

$i \in \{0,1\}$ and by replacing e_λ by ε_λ for $\lambda \in \{1, \underline{\mathrm{id}}, \underline{\mathrm{id}}^{-1}\}$:

$$
\begin{array}{lll}
\widehat{\beta_1^-} \cdot \widehat{\beta_1^-}, & \widehat{\beta_1^+} \cdot \widehat{\beta_1^-}, & \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^-}, \\
\widehat{\beta_1^-} \cdot \widehat{\beta_1^+}, & \widehat{\beta_1^+} \cdot \widehat{\beta_1^+}, & \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^+}, \\
\widehat{\beta_1^+} \cdot \widehat{\beta_{s_0}^0}, & \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_{s_0}^0}, & \\
\widehat{\beta_1^-} \cdot \widehat{\beta_{s_1}^0}, & \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_{s_1}^0}, & \\
\multicolumn{3}{l}{\widehat{\beta_{s_0}^0} \cdot \widehat{\beta_{s_0}^0} + \varepsilon_{\underline{\mathrm{id}}^{-1}} \cdot \widehat{\beta_1^-} \cdot \widehat{\beta_{s_0}^0} + \varepsilon_{\underline{\mathrm{id}}} \cdot \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^-} + \varepsilon_1 \cdot \widehat{\beta_1^-} \cdot \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^-},} \\
\multicolumn{3}{l}{\widehat{\beta_{s_1}^0} \cdot \widehat{\beta_{s_1}^0} - \varepsilon_{\underline{\mathrm{id}}} \cdot \widehat{\beta_1^+} \cdot \widehat{\beta_{s_1}^0} - \varepsilon_{\underline{\mathrm{id}}^{-1}} \cdot \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^+} + \varepsilon_1 \cdot \widehat{\beta_1^+} \cdot \widehat{\tau_{s_1}} \cdot \widehat{\beta_1^+},} \\
\multicolumn{3}{l}{\widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^-} \cdot \widehat{\tau_{s_0}} - \widehat{\tau_{s_0}} \cdot \widehat{\beta_1^-} \cdot \widehat{\beta_{s_0}^0},} \\
\multicolumn{3}{l}{\widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^+} \cdot \widehat{\tau_{s_1}} - \widehat{\tau_{s_1}} \cdot \widehat{\beta_1^+} \cdot \widehat{\beta_{s_1}^0},} \\
\multicolumn{3}{l}{(\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_1^+} \cdot \widehat{\beta_{s_1}^0} \cdot \widehat{\beta_1^+} + (\widehat{\tau_{s_0}} + \varepsilon_1) \cdot \widehat{\beta_1^-} \cdot \widehat{\beta_{s_0}^0} \cdot \widehat{\beta_1^-}.}
\end{array}
\tag{209}
$$

The set of elements in this list clearly has the following property: its image under the homomorphism of k-algebras

$$
\begin{array}{ccc}
k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle & \longrightarrow & T_{E_0}^* E^1 \\
\underset{(\text{for } \sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\})}{\widehat{\sigma}} & \longmapsto & \sigma
\end{array}
$$

is a set of generators of $\ker(\mathcal{M})$ as a bilateral ideal.

Proposition 4.10.4. *Let R_{E^*} be the quotient ring of the ring of non-commutative polynomials in seven indeterminates*

$$
k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle
$$

modulo the bilateral ideal I_{E^*} generated by the elements in the lists (207), (208) *and* (209)*. For all $\sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\}$, let us denote by $\widetilde{\sigma}$ the image of $\widehat{\sigma}$ in R_{E^*}. One has an isomorphism of k-algebras*

$$
\begin{array}{ccc}
R_{E^*} & \longrightarrow & E^* \\
\underset{(\text{for } \sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\})}{\widetilde{\sigma}} & \longmapsto & \sigma.
\end{array}
$$

In particular, E^* is a finitely presented k-algebra.

Proof. Let us consider the homomorphism of k-algebras

$$
\begin{array}{cccc}
\Phi\colon & k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle & \longrightarrow & T_{E_0}^* E^1 \\
& \underset{(\text{for } \sigma \in \{\tau_{\omega_0}, \tau_{s_0}, \tau_{s_1}, \beta_1^-, \beta_1^+, \beta_{s_0}^0, \beta_{s_1}^0\})}{\widehat{\sigma}} & \longmapsto & \sigma
\end{array}
$$

and the natural homomorphism of (graded) k-algebras

$$
\mathcal{M}\colon T_{E_0}^* E^1 \longrightarrow E^*.
$$

We know that both Φ and $\mathcal{M}$ are surjective (for Φ see Lemma 4.10.3 and for $\mathcal{M}$ see Section 4.1). So $\mathcal{M} \circ \Phi$ is surjective, and, in order to prove the lemma, it remains to show that the kernel is I_{E^*}. Let $x \in \ker(\mathcal{M} \circ \Phi)$. When we wrote the list (209), we said that the images of the elements in this list via Φ form a system of generators of $\ker(\mathcal{M})$ as a bilateral ideal. In particular, this means that $\Phi(x)$ (which lies in $\ker(\mathcal{M})$) can be written as

$$\Phi(x) = \sum_i a_i \cdot \Phi(x_i) \cdot b_i$$

for suitable elements $a_i, b_i \in T^*_{E_0} E^1$, and x_i in the list (209). Representing a_i as $\Phi(a_i')$ for some $a_i \in k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^-}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle$ and similarly for b_i, we see that

$$x - \sum_i a_i' \cdot x_i \cdot b_i' \in \ker(\Phi).$$

Since $\ker(\Phi)$ is generated by the elements in the lists (207) and (208) as a bilateral ideal (Lemma 4.10.3), we deduce that $x \in I_{E^*}$. This concludes the proof, because we have shown the inclusion $\ker(\mathcal{M} \circ \Phi) \subseteq I_{E^*}$, and the reverse inclusion is clear. ■

Remark 4.10.5. It is easy to see that the relation

$$(\tau_{s_1} + e_1) \cdot \beta_1^+ \cdot (\tau_{s_1} + e_1) - 2e_{\underline{\mathrm{id}}^{-1}} \beta_{s_1}^0 + \tau_{\omega_0}^{\frac{p-1}{2}} \cdot \beta_1^- = 0$$

(which we used in to produce the corresponding element in the list (208)) 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 proposition, it is then immediate to get a presentation of E^* as a quotient of $k\left\langle \widehat{\tau_{\omega_0}}, \widehat{\tau_{s_0}}, \widehat{\tau_{s_1}}, \widehat{\beta_1^+}, \widehat{\beta_{s_0}^0}, \widehat{\beta_{s_1}^0} \right\rangle$ (quotient modulo a finitely generated bilateral ideal) by replacing $\widehat{\beta_1^-}$ with

$$-\widehat{\tau_{\omega_0}}^{\frac{p-1}{2}} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) \cdot \widehat{\beta_1^+} \cdot (\widehat{\tau_{s_1}} + \varepsilon_1) + 2\widehat{\tau_{\omega_0}}^{\frac{p-1}{2}} \cdot \varepsilon_{\underline{\mathrm{id}}^{-1}} \widehat{\beta_{s_1}^0}$$

wherever it appears in the lists (207), (208) and (209).

Bibliography

[AS21] Konstantin Ardakov and Peter Schneider. The Bernstein center in natural characteristic. arXiv preprint arXiv:2105.06128, 2021.

[BD84] Joseph N. Bernstein and Pierre Deligne. Le “centre” de Bernstein. In *Representations des groups redutifs sur un corps local, traveaux en cours*, pages 1–32. Hermann, 1984.

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate texts in mathematics*. Springer, 2nd edition, 1991.

[Bou81] N. Bourbaki. *Groupes et algèbres de Lie. Chapitres 4 à 6*. Éléments de mathématiques. Masson, 1981.

[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.

[BT73] Armand Borel and Jacques Tits. Homomorphismes “abstraits” de groupes algebriques simples. *Annals of Mathematics*, 97(3):499–571, 1973.

[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.

[CGP15] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*, volume 26 of *New mathematical monographs*. Cambridge University Press, 2nd edition, 2015.

[Con12] Brian Conrad. Weil and Grothendieck approaches to adelic points. *L'Enseignement Mathématique*, 58(1):61–97, 2012.

[Con20] Brian Conrad. Algebraic groups II. Reductive groups over fields. AMS Open Math Notes OMN:201701.110663 (version: 2020-01-19), 2020.

[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.

[Har66] Robin Hartshorne. *Residues and duality*, volume 20 of *Lecture notes in mathematics*. Springer, 1966.

[Har16] Michael Harris. Speculations on the mod p representation theory of p-adic groups. *Annales de la Faculté des sciences de Toulouse: Mathématiques*, 25(2-3):403–418, 2016.

[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.

[Hum98] James E. Humphreys. *Linear algebraic groups*, volume 21 of *Graduate texts in mathematics*. Springer, 4th edition, 1998.

[Jan03] Jens C. Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical surveys and monographs*. American Mathematical Society, 2nd edition, 2003.

[Koz16] Karol Kozioł. Pro-p-Iwahori invariants for SL_2 and L-packets of Hecke modules. *International Mathematics Research Notices*, 2016(4):1090–1125, 2016.

[Koz18] Karol Kozioł. Hecke module structure on first and top pro-p-Iwahori cohomology. *Acta Arithmetica*, 186(4):349–376, 2018.

[Lam12] Tsit-Yuen Lam. *Lectures on modules and rings*, volume 189 of *Graduate texts in mathematics*. Springer, 2012.

[Laz65] Michel Lazard. Groupes analytiques p-adiques. *Publications Mathématiques de l'IHÉS*, 26:5–219, 1965.

[Lus89] George Lusztig. Affine Hecke algebras and their graded version. *Journal of the American Mathematical Society*, 2(3):599–635, 1989.

[Mil17] James S Milne. *Algebraic groups: the theory of group schemes of finite type over a field*, volume 170 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2017. Erratum at `https://www.jmilne.org/math/Books/iagerrata.html`.

[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 undangewandte Mathematik*, 635:149—185, 2009.

[Oll14] Rachel Ollivier. Compatibility between Satake and Bernstein isomorphisms in characteristic p. *Algebra & Number Theory*, 8(5):1071–1111, 2014.

[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.

[OS21] Rachel Ollivier and Peter Schneider. On the pro-p Iwahori Hecke Ext-algebra of $\mathrm{SL}_2(\mathbb{Q}_p)$. arXiv preprint arXiv:2104.13422, 2021.

[Sch09] Nicolas Alexander Schmidt. Generische pro-p Hecke-Algebren. Diplomarbeit, Humboldt-Universität zu Berlin, 2009.

[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*. Monogrphs 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.

[uu13] MathOverflow User user30180 (`https://mathoverflow.net/users/30180/user30180`). On the F-rational points of the derived group of a connected reductive algebraic group. MathOverflow, 2013. URL:`https://mathoverflow.net/q/133288` (version: 2013-06-10).

[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.

[Vig98] Marie-France Vignéras. Induced R-representations of p-adic reductive groups. *Selecta Mathematica New Series*, 4:549–623, 1998.

[Vig05] Marie-France Vignéras. Pro-p-Iwahori Hecke ring and supersingular $\mathbb{F}_p$-representations. *Mathematische Annalen*, 331:523–556, 2005. Erratum in 333:699–701, 2005.

[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.