MODULES OF CONSTANT JORDAN TYPE FROM GALOIS EXTENSIONS OF LOCAL FIELDS

ALEXANDRE EIMER

Contents

Introduction 1
1. Background material & Outline 3
   1.1. Modules of constant Jordan type 3
   1.2. Local fields 4
   1.3. The main theorem 5
   1.4. Demuškin groups 6
   1.5. Unequal characteristics 7
   1.6. The stable module category and Heller shifts 7
2. The Heller shifts of $\mathbb{F}_p$ 9
   2.1. The modules $\omega_s(\mathbb{F}_p)$ 9
   2.2. The module $M_n$ 14
   2.3. Applications to Galois theory 19
3. The Heller shifts of $J$ 20
   3.1. The module $\omega(J)$ 20
   3.2. The modules $\omega_s(J)$ for $s \geq 2$ 23
4. Cohomology 26
5. Back to the main theorem 28
   5.1. Summary 29
   5.2. When $\xi_p^2$ is not in $k$ 29
   5.3. When $p = 2$ 30
Appendix A. Some invariants 30
References 32

Introduction

Suppose $K/k$ is a finite Galois extension, and let $G = Gal(K/k)$. The group $J(K) = \mathbb{K}^\times/K^\times$ of $p$-th power residue classes in $\mathbb{K}$, where $p$ is a prime number, can be seen as a $\mathbb{F}_p$-vector space, and indeed as an $\mathbb{F}_p G$-module with the usual Galois action. Understanding $J(K)$ as such a module can be very useful: see [BLMS07] or [AGKM01], for instance. In order to provide motivation with a simple-minded example, assume that the class of $a \in \mathbb{K}^\times$ in $J(K)$ is fixed by $G$; then $L = K[a^{1/p}]$ is Galois over $k$ (assuming that $k$ contains a primitive $p$-th root of unity). In this case $Gal(L/k)$ is an extension of $G$ by a central subgroup of order $p$. The elementary theory of $p$-groups shows that, at least in principle, all Galois extensions of $k$ whose group is a finite $p$-group can be constructed inductively in this manner, showing the potential usefulness of results about the $\mathbb{F}_p G$-module $J(K)$.

Little is known in general. In [MS03], J. MINÁČ and J. SWALLOW study the case when $G$ is a cyclic $p$-group (see the references therein for earlier work on the cyclic case). As far as we know, the literature does not contain significant results for other types of groups.
In this paper, we study some Kummer extensions, that is, extensions for which \( G \) is an elementary abelian \( p \)-group, assuming that \( k \) contains a primitive \( p \)-th root of unity. More specifically, we will assume that \( k \) is a local field, and that \( K = k^{\frac{1}{p}} = k[(k^*)^{1/p}] \) is its maximal Kummer extension.

Under these assumptions, our description of \( J(k^{\frac{1}{p}}) \) is fairly complete. When studying a module for an elementary abelian \( p \)-group in characteristic \( p \), the information one can hope for is the behaviour after restriction to an arbitrary shifted cyclic subgroup, and the cohomology groups. We address both.

We start with:

**Theorem (A).** Suppose \( k \) is a local field containing a primitive \( p \)-th root of unity, and put \( K = k^{\frac{1}{p}} \) as above. Put \( G = \text{Gal}(K/k) \) and \( J(K) = K^\times/K^{\times p} \). Then as an \( F_p G \)-module, \( J(K) \) is of constant Jordan type; moreover, its stable constant Jordan type is \([1]^2\).

See [Ben17] for information about modules of constant Jordan type (we recall the basics below, of course). These are actively studied at the moment, and it is perhaps a surprise to see examples arising from field theory. We also point out that modules of constant Jordan types are intimately related to vector bundles over projective spaces.

Before stating other results, we first illustrate our theorem with a concrete example. Consider \( p = 2 \) and \( k = \mathbb{Q}_2 \); it contains clearly the primitive 2\(^{nd} \) root of unity (most commonly known as \(-1\)). Here, as is well known, \( K = \mathbb{Q}_2[\sqrt{2}] = \mathbb{Q}_2[\sqrt{2}, \sqrt{-1}, \sqrt{3}] \) (information of this sort is not used by our methods, and we mention this for concreteness only). Here \( G = \text{Gal}(K/k) \cong C_2^3 \) and \( \dim_{F_2} J(K) = 10 \). We will explain in this article how to choose generators \( x_1, x_2, x_3 \) of \( G \) and how to construct a convenient basis of \( J(K) \) in order to describe the action. The module structure of \( G \) on \( J(K) \) can be given by three matrices, say \( M_1, M_2 \) and \( M_3 \) where \( M_i \) is the matrix of \( x_i - \text{id} \) in our basis; those matrices commute and are nilpotent. The theorem then says, in this particular case, that the matrix

\[
\begin{pmatrix}
 a & b & c \\
 b & c & a \\
 c & b & a
\end{pmatrix}
\]

where \( a, b, c \) are in an algebraic closure of \( F_2 \) (and the blanks are zero) has constant rank (namely 4), as long as \((a, b, c) \neq (0, 0, 0)\). Of course this may be verified directly.

The cohomology groups of \( J(K) \) are as follows:

**Theorem (B).** Under the hypotheses of Theorem A, we have the following isomorphisms:

\[
\begin{align*}
\hat{H}^0(G, J(K)) & \cong F_{p^{n-1+n(n-1)/2}}, \\
\hat{H}^1(G, J(K)) & \cong \hat{H}^3(G, F_p), \\
\hat{H}^s(G, J(K)) & \cong \hat{H}^{s+2}(G, F_p) \oplus \hat{H}^{s-2}(G, F_p) \quad \forall s \geq 2.
\end{align*}
\]

Both theorems will appear as consequences of the following key statement. To formulate it, we must recall that \( F_p G \)-modules are best studied in the *stable category*, in which \( \text{hom}(M, N) \) consists of all usual modules homomorphisms modulo those morphisms which factor through a projective module. This category is triangulated, and is thus endowed with an invertible endofunctor \( \Omega \), frequently called the *Heller shift*. At the heart of this paper is the next result, which we formulate in vague terms for now.
Theorem (C). Let \( p \) be a prime and \( G \) be an elementary abelian \( p \)-group. For all \( s \in \mathbb{Z} \) we construct an explicit module \( \omega_s(\mathbb{F}_p) \) which is stably isomorphic to \( \Omega^s(\mathbb{F}_p) \). Moreover, when \( G = \text{Gal}(\mathbb{K}/\mathbb{k}) \) and \( J = J(\mathbb{K}) \) as in Theorem A, we construct for all \( s \in \mathbb{Z} \) an explicit module \( \omega_s(J) \) which is stably isomorphic to \( \Omega^s(J) \). These modules fit in particular, when \( s \geq 1 \), into an exact sequence

\[
0 \longrightarrow \omega_{s+2}(\mathbb{F}_p) \longrightarrow \omega_s(J) \longrightarrow \omega_{s-2}(\mathbb{F}_p) \longrightarrow 0 .
\]

In order to establish these results, as befits Galois theory, we turn questions of field theory into questions of group theory. A bit more precisely, let \( \Gamma \) be a pro-\( p \)-group, and let \( \Phi(\Gamma) \) denote its Frattini subgroup, that is

\[
\Phi(\Gamma) = \Gamma^p(\Gamma, \Gamma) .
\]

Thus \( \Gamma/\Phi(\Gamma) \) is the largest quotient of \( \Gamma \) which is elementary abelian. After a little translation, our results will be about \( J = \Phi(\Gamma)/\Phi(\Phi(\Gamma)) \), seen as a \( \mathbb{F}_p \Gamma \)-module, where \( G = \Gamma/\Phi(\Gamma) \). We will investigate this when \( \Gamma \) is a free pro-\( p \)-group, and then in the case when \( \Gamma \) is the largest \( p \)-quotient of \( \text{Gal}(\mathbb{K}/\mathbb{k}) \), which is a Demužkin group, provided the fact that \( \mathbb{k} \) is a local field with a primitive \( p \)-th root of unity. For example, we prove that, in the free case, the module \( J \) is isomorphic to \( \Omega^2(\mathbb{F}_p) \), a fact which appears, when \( p = 2 \), in [CM08] and for any \( p \) in [Fri95]. We give various generalizations. It is hoped that some of them have an independent interest for group theorists.

Organization of the paper. In the first section, we recall some basic facts about modules of constant Jordan type and Kummer theory, in order to show how Theorem A follows from Theorem C; we also state a “Main Theorem”, more general (and more technical) than the above, covering for example the case when \( \mathbb{k} \) does not contain enough roots of unity. Then in section 2 we construct the modules \( \omega_s(\mathbb{F}_p) \), as part of Theorem C (this does not involve any Galois theory). Section 3 completes the picture with the modules \( \omega_s(J) \). Finally, the cohomology groups are computed in section 4. We conclude with a summary in section 5, where we make sure that all cases of the main theorem are accounted for.

1. Background material & Outline

This section serves as an extended, more technical introduction. First we recall basic facts about modules of constant Jordan type. Then we describe more precisely the Galois-theoretic situation which we are interested in, translating the results entirely into the language of groups. Then, we state the main result of the paper, which is a refinement of both Theorems A and B. Finally, we give some recollections about Heller shifts, which will be central throughout the rest of the paper.

1.1. Modules of constant Jordan type. In this very short introduction, we will closely follow the book [Ben17] by D. Benson. In this section, and in the rest of the paper, the letter \( p \) denotes a prime number, and the name \( E_n \) will refer to an elementary abelian \( p \)-group of rank \( n \) (that is, a group isomorphic to \( C_p^n \)), with a preferred basis written \( x_1, \ldots, x_n \); however unlike D. Benson, we will consider right modules instead of left modules, for reasons which will appear in §2; as we focus on modules over commutative rings, such a choice only influences the notation.

Modules of constant Jordan type were first introduced in [CFP08], and were designed in order to extend the possible techniques we had to study representations of cyclic \( p \)-groups over fields of characteristic \( p \). Indeed if \( M \) is an \( \mathbf{F}E_1 \)-module, where \( \mathbf{F} \) denotes a field of characteristic \( p \), the study of \( M \) reduces to the study of a nilpotent endomorphism, since, for all \( m \in M \), we clearly have that

\[
m \cdot (x_1 - \text{id})^p = m \cdot (x_1^p - \text{id}) = 0 .
\]
Thus the possible $\mathbb{F}E_1$-modules are classified by the possible Jordan types of nilpotent matrices. As nilpotent morphisms shall play a central rôle, we introduce some useful notation: if $x_i$ is one of the chosen generators for $E_n$, then we set $X_i = x_i - 1 \in \mathbb{F}E_n$ and more generally if $\gamma \in \mathbb{F}^*$, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}$, we write $X_\gamma = \sum_{j \leq s} \gamma_j X_j \in \mathbb{F}E_n$. Also, it will be useful to be able to talk about the Jordan type of a module:

**Definition.** Let $M$ be an $\mathbb{F}E_1$-module; the *canonical Jordan type* of $M$ is that of the endomorphism $m \mapsto m \cdot X_1$. If the number of Jordan blocks of size $i$ is $m_i$, we will say that the Jordan type is $[1]^{m_1} \ldots [p]^{m_p}$.

Despite the use of a preferred generator, the Jordan type of a module is well-defined: indeed, taking another generator of $E_1$, that is $x_1^k$ for a $k$ prime to $p$, the sizes of the blocks remain the same. If the blocks of dimension $p$ are omitted, we speak of *stable* Jordan type; the cyclic components of dimension $p$ are in fact only copies of $\mathbb{F}E_1$, hence projective.

The main idea is to restrain the $E_n$-modules not only to cyclic subgroups but to the so-called *cyclic shifted subgroups*. Now we can introduce the

**Definition.** A cyclic shifted subgroup $\Gamma$ of $E_n$ (over $\mathbb{F}$) is a subgroup of the units of $\mathbb{F}E_n$ generated by an element $g_\gamma = 1 + X_\gamma$, for some $\gamma \in \mathbb{F}^n$.

Given a cyclic shifted subgroup $\Gamma$ generated by $\gamma$, and an $\mathbb{F}E_n$-module $M$, the $\mathbb{F}E_1$-module obtained by letting a generator of $E_1$ act as $\gamma$ on $M$ is simply called the restriction of $M$ to $\Gamma$ and is denoted by $M|_{\Gamma}$.

**Definition.** Let $M$ be a finite type $\mathbb{F}E_n$-module. $M$ is said to have constant Jordan type $[a_1] \ldots [a_t]$ if for every cyclic shifted subgroup $\Gamma$ of $\mathbb{F}E_n$, the restricted module $M|_{\Gamma}$ has Jordan type $[a_1] \ldots [a_t]$.

When $M$ is an $\mathbb{F}E_n$-module (and $\mathbb{F}$ is not necessarily algebraically closed), we say that $M$ is of constant Jordan type if and only if $M \otimes_{\mathbb{F}} \mathbb{F}$ is of constant Jordan type. In the same fashion we define the *stable* Jordan type of a module $M$ simply by omitting the blocks of length $p$. It should be remarked that it is a non-trivial fact that the previous definition does not depend upon numerous factors -for instance the choice of a basis for $E_n$.

Examples of modules of constant Jordan type are provided by the various $\Omega^s(\mathbb{F})$ which are discussed below.

**1.2. Local fields.** Now, it is time to introduce the extensions which are at the heart of this article. A local field, for us, is a finite extension of some $\mathbb{Q}_\ell$ (where $\ell$ is prime). Let $k$ be a local field which contains a primitive $p$-th root of unity and let us fix $\tilde{k}$ an algebraic closure of $k$. We set $\mathcal{R}_1 = \{ \alpha \in \tilde{k} | \alpha^p \in k \}$ and then $k^\frac{1}{p} = k[\mathcal{R}_1]$. We recall that we aim to study $(k^\frac{1}{p})^\times / (\tilde{k}^\times)^p = J(k^\frac{1}{p})$ as a $Gal(k^\frac{1}{p} / k)$-module, and that we frequently write $K = k^\frac{1}{p}$.

The study of $J(K)$ will lead us to the study of some other extensions, as we shall see hereafter. Let us put $\mathcal{R}_2 = \{ \alpha \in \tilde{k} | \alpha^p \in K \}$, and $K^{(2)} = K[\mathcal{R}_2]$. We clearly have the following diagram of extensions.

$$
\begin{array}{c}
K^{(2)} \\
\downarrow \\
K \\
\downarrow \\
k
\end{array}
$$
According to the previous diagram we have the following exact sequence

\[ 0 \longrightarrow \text{Gal}(K^{(2)}/K) \longrightarrow \text{Gal}(K^{(2)}/k) \longrightarrow \text{Gal}(K/k) \longrightarrow 0. \]

Therefore it is abundantly clear that \( G := \text{Gal}(K/k) \) acts on \( \text{Gal}(K^{(2)}/K) \) by conjugation. Furthermore, as an \( \mathbb{F}_pG \)-module \( \text{Gal}(K^{(2)}/K) \) is related to \( J(K) \) via Kummer theory. Let us recall the basics.

Recall first that a field extension \( L/L_0 \) is an \( n \)-Kummer extension if it is simply a Galois extension such that \( \text{Gal}(L/L_0) \) is an abelian group of exponent dividing \( n \), and if \( L_0 \) contains a primitive \( n \)-th root of unity. As in Galois theory, there is a correspondence theorem.

**Theorem 1** (Kummer theory). Let \( L_0 \) be a field containing a primitive \( n \)-th root of unity and fix an algebraic closure \( \bar{L}_0 \) of \( L_0 \). The \( n \)-Kummer extensions \( L \) of \( L_0 \) contained in \( \bar{L}_0 \) are in 1-to-1 correspondence with the subgroups of \( L_0^*/L_0^{*n} \); moreover the correspondence maps the subgroup \( H \) to the field \( L_0[x^\frac{1}{n}], [x] \in H \), and is thus order-preserving. Finally, if a field \( K \) and a subgroup \( H \) are in correspondence, then \( \text{hom}(\text{Gal}(L/L_0), \mathbb{Z}/n\mathbb{Z}) \cong H \).

See [Gui18, Theorem 1.25]. From this theorem and the previous considerations we can deduce two key facts.

First, the groups \( \text{Gal}(K^{(2)}/K) \) and \( G = \text{Gal}(K/k) \) are simply elementary abelian \( p \)-groups and in particular \( \text{Gal}(K^{(2)}/K) \) is an \( \mathbb{F}_p \)-vector space.

Secondly, the theory applied to the base field \( K \) implies, by maximality, that \( K^{(2)} \) is in correspondence with \( J(K) \) (note that all \( p \)-Kummer extensions of \( K \) are contained in \( K^{(2)} \)). It follows that \( \text{hom}(\text{Gal}(K^{(2)}/K), \mathbb{F}_p) \) is isomorphic to \( J(K) \), and this is really an isomorphism as modules over \( \mathbb{F}_pG \): indeed this is the refinement brought by equivariant Kummer theory (see [Gui18, Theorem 1.26]).

A more elaborate result, which we call Tate duality (cf. [Gui18, Theorem 13.21]), states that \( J(K) \) is self-dual, as a module, as long as \( k \) contains a primitive \( p \)-th root of unity, which is fortunately the case here.

We summarize this discussion in the following lemma:

**Lemma 2.** There are isomorphisms of \( \mathbb{F}_pG \)-modules between \( \text{Gal}(K^{(2)}/K) \), \( J(K) \) and \( J(K)^* \).

From now on, we set \( J = J(K) \) and \( n = \dim_{\mathbb{F}_p} k^*/k^{*p} \), so that the rank of \( G \cong E_n \) is \( n \). According to the previous lemma, instead of trying to study \( J \), we can turn our attention to \( \text{Gal}(K^{(2)}/K) \) and use techniques from group theory.

In fact, let us write \( L(p) \) for the largest pro-\( p \) extension of the field \( L \) (contained in a fixed algebraic closure), and let us put \( G_L(p) = \text{Gal}(L(p)/L) \). It is not hard to see that the intermediate field \( K = k^{\frac{1}{2^p}} \) is in Galois correspondence with \( \Phi(G_k(p)) \) (recall that \( \Phi \) is used for Frattini subgroups). Similarly, \( K^{(2)} \) is in correspondence with \( \Phi(\Phi(G_k(p)) = \Phi(2)(G_k(p)) \), using the maximality conditions defining the extensions. We can therefore state the following lemma:

**Lemma 3.** There is an isomorphism \( J \cong \Phi(G_k(p))/\Phi(2)(G_k(p)) \), as modules over \( \mathbb{F}_pG \) where \( G = G_k(p)/\Phi(G_k(p)) \).

**1.3. The main theorem.** Thanks to the previous lemma, we have completely translated the problem arising from Galois theory into a group-theoretic one; not only does this formulation enable us to solve the problem, but we can now rephrase all results of this article in the following theorem.

**Theorem 4** (Main theorem). Let \( k \) be a local field and let \( \Gamma = G_k(p) \) be the Galois group of a maximal pro-\( p \)-extension; we write \( n \) for the minimal number of generators of \( \Gamma \), so that \( \Gamma/\Phi(\Gamma) = E_n \) is elementary abelian of rank \( n \). Put \( J = \Phi(\Gamma)/\Phi(2)(\Gamma) \).
Then $J$, as an $E_n$-module, is of constant Jordan type. Moreover its stable Jordan type is

- $[1]$ if $k$ does not contain a primitive $p^t$-root of unity,
- $[1]^2$ if $k$ contains a primitive $p^t$-root of unity.

Moreover, we have the following possibilities for the cohomology of $J$.

1. If $k$ does not contain a primitive $p^t$-root of unity, then for all $s \in \mathbb{Z}$:
   \[ \hat{H}^s(E_n, J) = \hat{H}^{s-2}(E_n, F_p). \]

2. If $\xi_p \in k$ and the residue field of $k$ is of characteristic prime to $p$, then $n = 2$ and for all $s \in \mathbb{Z}$:
   \[ \hat{H}^s(E_2, J) = \hat{H}^s(E_2, F_p) \oplus \hat{H}^{s}(E_2, F_p). \]

3. If $\xi_p \in k$ and the characteristic of the residue field of $k$ is $p$ then
   \[
   \begin{align*}
   \hat{H}^0(E_n, J) & \cong F_p^{n-1+n(n-1)/2}, \\
   \hat{H}^1(E_n, J) & \cong \hat{H}^3(E_n, F_p), \\
   \hat{H}^s(E_n, J) & \cong \hat{H}^{s+2}(E_n, F_p) \oplus \hat{H}^{s-2}(E_n, F_p) \quad \forall s \geq 2.
   \end{align*}
   \]

Note that in the case where $k$ does not contain a primitive $p^t$-root of unity, there is no such thing as Kummer theory; therefore there is no such thing as an isomorphism between $(k^{1/p})^\times/(k^{1/p})^\times_p$ and $\Phi(\Gamma)/\Phi^{(2)}(\Gamma)$, so that the formulation of the theorem is the only one available. It should be remarked that $J$ seems to detect some differences in the arithmetic of the field.

The rest of the paper is devoted to the proof of this theorem (which implies, in particular, the statements of Theorems A and B from the introduction, of course).

1.4. Demuškin groups. The Galois groups of maximal $p$-extensions of local fields are explicitly known: indeed if $L$ is a local field such that $\xi_p \in L$, then $G_L(p)$ is a Demuškin group. A presentation by generators and relations of such groups was given by J. Labute (see [Lab67]), which we recall first for $p \neq 2$:

   \[ D_{k,2s} = \langle x_1, \ldots, x_{2s} | x_1^{p^k}(x_1, x_2)(x_3, x_4) \ldots (x_{2s-1}, x_{2s}) = 1 \rangle, \]

where $k$ is the maximal integer such that $\xi_p^k \in L$ and $2s$ is the dimension of $J(L)$.

When $p = 2$, the relation in the Demuškin group changes. If the number of generators is odd, it becomes

   \[ D_{f,n=2s+1} = \langle x_1, \ldots, x_{2s+1} | x_1^{2f}(x_2, x_3)(x_4, x_5) \ldots (x_{2s}, x_{2s+1}) = 1 \rangle. \]

If the number of generators is however even, it becomes either

   \[ D_{f,n=2s} = \langle x_1, \ldots, x_{2s} | x_1^{2+2f}(x_1, x_2)(x_3, x_4) \ldots (x_{2s-1}, x_{2s}) = 1 \rangle, \]

or

   \[ D'_{f,n=2s} = \langle x_1, \ldots, x_{2s} | x_1^{2f}(x_1, x_2)x_3^{2f}(x_3, x_4) \ldots (x_{2s-1}, x_{2s}) = 1 \rangle. \]

In each case $f$ is an integer such that $f \geq 2$.

We complete this review of the possible descriptions for $G_L(p)$ with the case when $L$ does not contain a primitive $p^t$-root of unity: in this situation $G_L(p)$ is a free prop-$p$-group (Theorem 3, II, §5 in [Ser97]).
1.5. **Unequal characteristics.** Consider a prime number $\ell$ different from $p$, let us consider any finite extension $k$ of $Q_\ell$ such that $k$ contains a primitive $p^{th}$-root of unity $\xi_p$. In this case, we can already settle the statements of Theorem 5 by easy arguments. Let us do this at once, as a warm-up for the more involved computations to follow.

According to [Gui18, Lemma 4.10], any finite Galois extension $L$ of $k$ verifies:

$$\dim_{F_p} L^x/L^{x_p} = 2.$$ 

If we focus on the extension $k^{1/\ell}$, then we claim that $J(k^{1/\ell})$ as a $\text{Gal}(k^{1/\ell}/k)$-module is only but two copies of the trivial module. Indeed, the Galois group of the maximal pro-$p$-extension is the Demuškin group

$$G_k(p) = \langle x_1, x_2 | x_1^{p^k}(x_1, x_2) = 1 \rangle,$$

for some $k \geq 1$, as explained above. Let $\Phi = \Phi(G_k(p))$ and $\Phi^{(2)} = \Phi^{(2)}(G_k(p))$, so that we are interested in $J = \Phi/\Phi^{(2)}$ (see Lemma 3). Then $J$ is generated by $x_1^p$, $x_2^p$ and $(x_1, x_2) := x_1^{-1}x_2^{-1}x_1x_2$ as a module over $G = G_k(p)/\Phi$: this follows from the formulae about commutators that we give below (see §2.2.3 in particular), but can also be checked as an exercise. Given the relation defining $G_k(p)$, we see that $x_1^p$ and $x_2^p$ alone generate $J$.

Now write the relation in the form $x_2^{-1}x_1x_2 = x_1^{-p^k+1}$, so that

$$x_2^{-1}x_1x_2 = x_1^{-p^{k+1}}x_1^p,$$

and we see that conjugation by $x_2$ fixes $x_1^p$ modulo $\Phi^{(2)}$. The action of $x_2$ (as an element of $G$) on the module $J$ is thus trivial. As for $x_1$, we write

$$x_1^{-1}x_2^{-1}x_1 = x_1^p x_2^{-1}.$$

As we have established that $x_1^p$ and $x_2^{-1}$ commute modulo $\Phi^{(2)}$, we obtain

$$x_1^{-1}x_2^{-p}x_1 = x_1^{p^{k+1}}x_2^{-p} = x_2^{-p} \mod \Phi^{(2)},$$

and we conclude that $x_1$ acts trivially on $J$, too.

We summarize the situation as follows.

**Lemma 5.** Let $\ell$ be a prime number different from $p$. Suppose $k$ is a finite extension of $Q_\ell$ such that $\xi_p \in k$. We set $K = k^{1/\ell}$. Then

$$J(K) \cong F_p \times F_p,$$

as a $\text{Gal}(K/k)$-module.

Therefore the corresponding statements in Theorem 5 are true for trivial reasons. From now on, we will suppose that the characteristic of the residue field of $k$ is $p$, unless we explicitly assume otherwise.

When $p = 2$, the result remains true, as the main differences vanish modulo $\Phi^{(2)}$.

1.6. **The stable module category and Heller shifts.** We have to introduce some new modules: our key-argument is yet very simple (it is just a simple exact sequence), but we have to explain some classical notation and objects. Here we just follow [CTVEZ03] (p. 35 sq.), so we consider a finite group $G$ and a field $F$ (whose characteristic $p$ typically divides the order of $G$).

Let $M$ be an $FG$-module, let $\pi : P \rightarrow M$ an epimorphism from a projective module onto $M$. Its kernel denoted $\Omega(M)$ is called the Heller shift of $M$; it always exists, however it is only defined up to a projective module. That is why we have to introduce the stable module category $\text{mod}_{FG}$ whose objects are in fact $FG$-modules, and whose hom sets, written $\text{hom}$, are defined by

$$\text{hom}(M, N) = \text{hom}_{FG}(M, N)/P_{M,N}.$$
where $P_{M,N}$ is the subspace of morphisms which factor through a projective. Then $\Omega$ becomes a well-defined functor on the stable category.

We should immediately remark that we can iterate our construction and then introduce for instance $\Omega^2(M) = \Omega(\Omega(M))$ and so on. Dualizing this construction (i.e. taking the cokernel of a monomorphism from $M$ into a projective module) gives birth to $\Omega^{-1}(M)$ and then we can again iterate such a construction. We would like to emphasize the fact that $\Omega(M)$ is not well-defined in the category of modules but in the stable category; usually $\omega(M)$ will be our notation for some module whose image in $\text{mod}_{FG}$ is isomorphic to $\Omega(M)$, though we will repeat this for emphasis.

We will consider in particular the modules $\Omega^s(F)$ when $G$ is elementary abelian: a whole family of modules $\omega_s(F)$ which meet a precise condition will be given in §2. Then in §3 we shall do the same with modules $\omega_s(J)$, where $J$ is as above, which are stably isomorphic to $\Omega^s(J)$.

When all of this is done, the crucial statement will be the existence of a short exact sequence

\[
0 \longrightarrow \omega_3(F_p) \longrightarrow \omega(J) \longrightarrow \omega_{-1}(F_p) \longrightarrow 0.
\]

In the introduction this was part of Theorem C. Here we explore the immediate consequences.

The exactness of a sequence is not sufficient to conclude anything about the constant Jordan type in general, but luckily here we have automatically a bit more. Still following [Ben17], recall that a locally split exact sequence is a short exact sequence

\[
0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,
\]

whose restriction to every cyclic shifted subgroup is split. It is obvious, in this case, that if $M_1, M_3$ are modules of constant Jordan type, so is $M_2$. In fact, its Jordan type is the sum of the Jordan type of $M_1$ and that of $M_3$.

We should then recall D. BENSON’S theorem on negative Tate cohomology ([Ben17], p.99):

**Theorem 6** (Benson). Let $j,s$ be in $\mathbb{Z}$ and $s < 0$. Let $M$ be an $FE_n$-module such that there exists a short exact sequence of the form

\[
0 \longrightarrow \Omega^j(F) \longrightarrow M \longrightarrow \Omega^{j+s-1}(F) \longrightarrow 0.
\]

Then the previous short exact sequence is locally split exact.

We can therefore apply the previous theorem to the exact sequence (*) Now, it is a well-known result (see again [Ben17]) that a module which is stably isomorphic to $\Omega^j(F)$ is of constant Jordan type; in fact if $j$ is odd (resp. even) the stable Jordan type of $\Omega^j(F)$ is $[p-1]$ (resp. $[1]$). Hence $\omega(J)$ is of constant Jordan type and its stable Jordan type is $[p-1]²$; since a module $M$ is of constant Jordan type if and only if $\omega(M)$ is, and more precisely using Proposition 5.1.12 from [Ben17], we can conclude. We have shown:

**Lemma 7.** Theorem A follows from Theorem C. \(\square\)

We conclude this section with a discussion of the vector bundle associated with $J$ (any module of constant Jordan type defines such a bundle). More precisely, we can construct from $J$ a vector bundle over $\text{P}_F^{p-1}$ (the projective space over $F$) using a functor denoted $\mathcal{F}$ (see [Ben17] p.172 sq.); as the definition is quite technical we will not recall anything about it. Let $\mathcal{O}$ denote the structural sheaf of $\text{P}_F^{p-1}$ and $\mathcal{O}(k)$ denote $\mathcal{O}^{\otimes k}$ if $k$ is a positive integer, otherwise we set $\mathcal{O}(k) = (\mathcal{O}^*)^{\otimes k}$, where $\mathcal{O}^*$ is the usual dual sheaf.

**Corollary.** If the characteristic of the residue field of $k$ is equal to $p$, we have the following isomorphism:

\[
\mathcal{F}(J(k^\mathbb{C})) = \mathcal{O}(p) \oplus \mathcal{O}(-p),
\]
however if the residue field of $k$ is of characteristic prime to $p$, we have the isomorphism:

$$\mathcal{F}(J(k^{\mathbb{Z}})) = \mathcal{O} \oplus \mathcal{O}.$$  

Proof. If the residue field of $k$ has characteristic prime to $p$, then according to lemma 5, it appears that $J(k^{\mathbb{Z}}) = F_p \times F_p$. Therefore $\mathcal{F}(J) = \mathcal{O} \oplus \mathcal{O}$.

If the residue field of $k$ is not prime to $p$, then we shall remark that $Gal(k^{\mathbb{Z}}/k)$ is not an elementary abelian $p$-group of rank $2$: its rank is at least $3$. Therefore according to Benson ([Ben17] p. 194) the sequence we obtained by applying the exact functor $\mathcal{F}$ to the exact sequence (*) which is

$$0 \longrightarrow \mathcal{F}(\omega_3(F)) \longrightarrow \mathcal{F}(\omega(J)) \longrightarrow \mathcal{F}(\omega(F)) \longrightarrow 0,$$

splits, hence the conclusion. \qed

2. The Heller shifts of $\mathbf{F}_p$

In this section, $p$ is a prime number, $E_n$ is an elementary abelian $p$-group of rank $n$, and we write simply $F_p$ for the trivial $E_n$-module. We start by giving a presentation by generators and relations of a certain module $\omega_s(F_p)$, for $s \in \mathbb{Z}$, which is stably isomorphic to $\Omega^n(F_p)$. Then in the second part, we revisit $\omega_2(F_p)$ from a completely different viewpoint. Namely, we start from a free pro-$p$-group of rank $n$, denoted $F_n$, and consider $M_n = \Phi(F_n)/\Phi^2(F_n)$ as a module over $E_n = F_n/\Phi(F_n)$; working directly with commutators, we find a presentation for $M_n$ which turns out to be precisely the presentation for $\omega_2(F_p)$ considered earlier. As a result, $M_n$ is of course isomorphic to $\omega_2(F_p)$.

Thus we do not make any mention of Galois theory in the next paragraphs. However, the result about $M_n$ is a statement regarding free pro-$p$ groups from which we will deduce parts of Theorem 5 (in the case when the base field does not contain the $p^{th}$-roots of unity, when $G_k(p)$ is free). Also, the material in this section paves the way for a similar analysis, with the free group replaced by a general Demuškin group, in the next section.

We start our exposition by assuming that $p > 2$. The very minor modifications needed to deal with $p = 2$ will be given afterwards.

2.1. The modules $\omega_s(F_p)$

We start with the case $n = 1$. It is well known that there is a projective resolution of $F_p$ as an $F_p E_1 = F_p C_p$ module which is periodic, and indeed of the form

$$\cdots \longrightarrow F_p E_1 \xrightarrow{x \mapsto x \cdot X_1} F_p E_1 \xrightarrow{x \mapsto x \cdot X_1^{p-1}} F_p E_1 \xrightarrow{x \mapsto x \cdot X_1} F_p E_1 \longrightarrow \cdots$$

Let us be more precise. In degree $s \geq 0$ we take a copy $P_s$ of the free module of rank $1$, we take $P_{s-1} = F_p$, and define $D_s: P_s \rightarrow P_{s-1}$ by $D_s(x) = x \cdot X_1$ if $s$ is odd, and $D_s(x) = x \cdot X_1^{p-1}$ if $s$ is even and positive, while $D_0$ is the augmentation.

By definition, we see that $\omega_s(F_p) := \ker(D_{s+1}) = \text{Im}(D_s) \cong P_s/\ker(D_s)$ is a model for $\Omega^s(F_p)$. So $\omega_s(F_p)$ is a submodule of $P_{s+1}$, but more importantly for us, it is a quotient of $P_s$. It is thus “presented” as having one generator (the generator for $P_s$), and one relation (the image of the generator of $P_{s+1}$ under $D_{s+1}$, which generates all of $\text{Im}(D_{s+1}) = \ker(D_s)$).

We need some notation. It may appear surprising at first, but will generalize well to other values of $n$. So we consider the graded commutative ring $P_s = F_p E_1[\zeta, \eta]$, where the subring $F_p E_1$ is concentrated in degree 0, the degrees of $\zeta$ and $\eta$ are 2 and 1 respectively, and there are no relations apart from those imposed by graded-commutativity, that is $\eta^2 = 0$ and $\eta \zeta = \zeta \eta$. In other words, we have

$$P_s = H^*(E_1, F_p) \otimes_{F_p} F_p E_1.$$

From topological practice, we have acquired the habit of writing either $xy$ or $yx$ for the product of two elements $x$ and $y$ of $P_s$. 


The degree \( s \) summand in \( P_s \) is free of rank 1 over \( \mathbf{F}_p E_1 \), generated by \( \zeta^k \) if \( s = 2k \) and by \( \eta \zeta^k \) if \( s = 2k + 1 \). So we may take it as the module written \( P_s \) above, and thus we can consider the combined map

\[
D : P_s \to P_s
\]

obtained from the various boundary maps \( D_s \). We caution that \( D \) is not a derivation of the ring \( P \), as can be verified with the formulae \( D(\zeta^k) = \eta \zeta^{k-1} \cdot X_1^{p-1} \), \( D(\eta \zeta^k) = \zeta^k \cdot X_1 \).

The point of this is to come up with reasonable names for the generators of the modules \( \omega_*(\mathbf{F}_p) \). Thus to finish with the case \( n = 1 \), we see that \( \omega_{2k}(\mathbf{F}_p) \) is generated by \( D_{2k}(\zeta^h) \); as the module of relations \( \ker(D_{2k}) \) is also \( \text{Im}(D_{2k+1}) \), it is generated by \( D_{2k+1}(\eta \zeta^k) = \zeta^k \cdot X_1 \). Using the isomorphism \( \omega_{2k}(\mathbf{F}_p) \cong P_{2k}/\ker(D_{2k}) \) induced by \( D_{2k} \), we conclude that we have the following presentation by generators and relations:

\[
\omega_{2k}(\mathbf{F}_p) \cong \langle \zeta^k \mid \zeta^k \cdot X_1 = 0 \rangle.
\]

A similar reasoning leads to

\[
\omega_{2k+1}(\mathbf{F}_p) \cong \langle \eta \zeta^k \mid \eta \zeta^k \cdot X_1^{p-1} = 0 \rangle.
\]

We can turn to an arbitrary value of \( n \). Tensoring the resolution \( P_s \) previously given with itself \( n \) times (over \( \mathbf{F}_p \)), we obtain a resolution \( A_{s} \) of \( \mathbf{F}_p \), by the Künneth theorem. Moreover, the usual formula for the differential in a tensor product of complexes shows, by an immediate induction on \( n \), that we really have a resolution by \( \mathbf{F}_p E_{n} \)-modules.

We can identify \( A_s = \bigoplus \omega_{s}(\mathbf{F}_p) \) with the graded ring \( \mathbf{F}_p E_{n}[\zeta_1, \ldots, \zeta_n, \eta_1, \ldots, \eta_n] \). It is equipped with a self-map \( D \), obtained from the differentials. The module \( \omega_{s}(\mathbf{F}_p) := A_s/D(A_{s+1}) \) is stably isomorphic to \( \Omega^s(\mathbf{F}_p) \), by definition. Moreover, the \( \mathbf{F}_p E_{n} \)-module \( A_s \) is free, its generators being the monomials in the \( \zeta \) and \( \eta \) of the appropriate degree. Thus we have a presentation

\[
A_{s+1} \xrightarrow{D_{s+1}} A_s \xrightarrow{D_s} \omega_{s}(\mathbf{F}_p) \xrightarrow{D_s} 0.
\]

Hence \( \omega_{s}(\mathbf{F}_p) \) has a presentation, with generators indexed by the monomials in \( A_{s} \), and relations indexed by the monomials in \( A_{s+1} \). The technical point will be to compute the effect of the map \( D_{s+1} \), and this is the object of the proposition below. We point out that, in the sequel, the ring \( A_s \) will be essentially forgotten, but what will survive is a system of names for the generators and relations of various modules.

**Definition.** A multi-index is a tuple \( \nu = (\nu_1, \nu_2, \ldots) \) of nonnegative integers (in this paper, most multi-indices will be of length \( n \), the rank of \( E_n \)). The weight of \( \nu \) is then \( |\nu| = \nu_1 + \nu_2 + \cdots \). We define a \( C \)-index of weight \( s \) to be a pair \((h, z)\) of multi-indices of the same length verifying the following conditions:

1. \( h_i \in \{0, 1\} \) for each \( i \),
2. \( 2|z| + |h| = s \).

Further, if \( \nu \) is a multi-index, we define \( \text{supp}(\nu) = \{i \mid \nu_i \neq 0\} \).

As elements of \( A \) do not commute, we have to specify the following notation

\[
\eta^h \zeta^z = \eta_1^{h_1} \cdots \eta_n^{h_n} \zeta_1^{z_1} \cdots \zeta_n^{z_n}.
\]

We shall introduce some small notations, classical in the free differential calculus of Fox (see [Fox53]). Taking into account the weight of each generator, a basis of \( A \) is given by the monomial \( \eta^h \zeta^z \) where \((h, z)\) is a \( C \)-index. Let \( m \) be such a monomial, we define the following linear map:

\[
\begin{align*}
\frac{\partial^m}{\partial \eta_i} &= 0 \quad \text{if there is no } \eta_i \text{ in } m, \\
\frac{\partial^m}{\partial \zeta_i} &= m.
\end{align*}
\]
Note those are well defined, since we have defined these $\mathbf{F}_p$-linear applications on an $\mathbf{F}_p$-basis of $A$. In the same fashion, we introduce the following operators for every $i \in \{1, \ldots, n\}$, if

$$\zeta_i^{-1}: A_{s+2} \longrightarrow A_s$$

$$m \longrightarrow \zeta_i^{-1}(m) = \begin{cases} c & \text{if } m = \zeta_i m' \text{ for a monomial } m', \\ 0 & \text{otherwise.} \end{cases}$$

It will be easier to write simply $\zeta_i^{-1}m$ or $\eta m\zeta_i^{-1}$ for $\zeta_i(m)$. With this notation, the action of $D$ for $n = 1$ described above can be recast as

$$D(\zeta_i^k) = \eta \zeta_i^k \zeta_i^{-1} \cdot X_i^{p-1}, \quad D(\eta \zeta_i^k) = \frac{\partial(\eta \zeta_i^k)}{\partial \eta} \cdot X_1,$$

and thus for any monomial $m$ in $\eta_i$ and $\zeta_i$ we may state:

$$D(m) = \frac{\partial(m)}{\partial \eta} \cdot X_1 + \eta_i m \zeta_i^{-1} \cdot X_i^{p-1}.$$

The next proposition generalizes this to any value of $n$.

**Proposition 8.** Let $s \geq 0$. The module $\omega_s(\mathbf{F}_p)$, which is stably isomorphic to $\Omega^s(\mathbf{F}_p)$, has a presentation of the form

$$\omega_s(\mathbf{F}_p) \cong \langle \eta \zeta^s | \ Rel^{s+1}(h', z') \rangle$$

with generators $\eta \zeta^s$ indexed by the C-indices $(h, z)$ of weight $s$, and one relation $\Rel^{s+1}(h', z')$ for each C-index $(h', z')$ of weight $s + 1$, given by

$$\sum_{i=1}^{n} \left( \frac{\partial(\eta u \zeta^s)}{\partial \eta} \cdot X_i + \eta \eta u \zeta^s \zeta_i^{-1} \cdot X_i^{p-1} \right) = 0.$$

Moreover, for $s \geq 1$ there is an $\mathbf{F}_p E_n$-module $\omega_{s-1}(\mathbf{F}_p)$, which is stably isomorphic to $\Omega^{s-1}(\mathbf{F}_p)$, and has a presentation of the form

$$\omega_{s-1}(\mathbf{F}_p) \cong \langle \eta \zeta^s | \ Rel_{s-1}(h', z') \rangle$$

with generators $\eta \zeta^s$ indexed by the C-indices $(h, z)$ of weight $s$, and one relation $\Rel_{s-1}(h', z')$ for each C-index $(h', z')$ of weight $s - 1$, given by

$$\sum_{i=1}^{n} \left( \eta \zeta^s \eta_i \cdot X_i + \zeta_i \frac{\partial(\eta \zeta^s)}{\partial \eta} \cdot X_i^{p-1} = 0 \right).$$

Finally, there is a module $\omega_{-1}(\mathbf{F}_p)$, stably isomorphic to $\Omega^{-1}(\mathbf{F}_p)$, with presentation

$$\omega_{-1}(\mathbf{F}_p) \cong \langle \alpha | \prod_{1 \leq i \leq n} X_i^{p-1} = 0 \rangle.$$

**Proof.** Assume $s \geq 1$ first. Let us find an expression of the differential $D$ by induction on the rank of the elementary abelian group $n$. It is clear that the proposition holds for $n = 1$ according to what was recalled at the beginning of this subsection.

Let us assume that for every element of the form $c = \eta_1^{h_1} \cdots \eta_{n-1}^{h_{n-1}} \zeta_1^{z_1} \cdots \zeta_{n-1}^{-1} = \eta \zeta^s$, where $(h, z)$ is a C-index, we have

$$D(c) = \sum_{i=1}^{n-1} \left( \eta_i c \zeta_i^{-1} X_i^{p-1} + \frac{\partial c}{\partial \eta_i} X_i \right).$$

We now establish that the same formula holds with $n - 1$ replaced by $n$.

Continue with the element $c$, and let $(h_n, z_n) \in \{0, 1\} \times \mathbb{N} \setminus \{0, 0\}$, by using the classical definition of the differential of the tensor products of two resolutions, and the fact that
ζ_n is of degree 2 we get:
\[
D(\eta^h \zeta_n \bar{\zeta}_n \eta_n^h) = D(c \eta_n^h \zeta_n^2) \\
= D(c) \eta_n^h \zeta_n^{i} + \sum_{i=1}^{n-1} h_i c D(\eta_n^h \zeta_n^{i})
\]
Since \( h_n \in \{0, 1\} \), we may distinguish two cases according to the possible values of \( h_n \).

If \( h_n = 0 \), since \( \zeta_n \) is of weight 2, and using that \( D(\zeta_n^{i}) = \eta_n \zeta_n^{i-1} X_n^{p-1} \), we obtain
\[
D(\eta^h \zeta_n \bar{\zeta}_n \eta_n^h) = D(c \eta_n^h \zeta_n^{i}) = D(c) \zeta_n^{i} + \sum_{i=1}^{n-1} h_i \eta_n \zeta_n^{i-1} X_n^{p-1}.
\]

Again, since \( \zeta_n \) commutes with all elements the following relations implying the above operators are immediate, on every monomial \( m \):

\[
\begin{align*}
\zeta_n^{i} \frac{\partial \eta_n^m}{\partial \eta_n} &= \frac{\partial \zeta_n^m}{\partial \eta_n} = \frac{\partial \eta_n^m}{\partial \eta_n} \\
\zeta_n^{i-1}(m) &= \zeta_n^{i-1}(\zeta_n^{i-1}(m))
\end{align*}
\]

where \( i \in \{1, \ldots, n\} \) and \( j \neq n \). Therefore, by reordering the second term -which makes the factor \( (-1)^{i=1} \) disappear- we have in this case the expected formula:
\[
D(c \eta_n^{i} \zeta_n^{i}) = \eta_n \zeta_n^{i} X_n^{p-1} + \sum_{i=1}^{n-1} \frac{\partial c \zeta_n^{i}}{\partial \eta_n} X_i + \eta_n \zeta_n^{i} X_i^{p-1},
\]
which is what we expected according to (1).

If \( h_n = 1 \), some slight changes have to be made:
\[
D(c \eta_n^{i} \zeta_n^{i}) = D(c) \eta_n \zeta_n^{i} c + \sum_{i=1}^{n-1} \frac{\partial c \zeta_n^{i}}{\partial \eta_n} X_i + \eta_n \zeta_n^{i} X_i^{p-1}.
\]
Furthermore, we have the following equalities:
\[
\begin{align*}
\frac{\partial \eta_n^m}{\partial \eta_n} &= \frac{\partial \zeta_n^m}{\partial \eta_n} = \frac{\partial \eta_n^m}{\partial \eta_n} \\
\eta_n \zeta_n^{i-1}(m) &= \zeta_n^{i-1}(\eta_n m)
\end{align*}
\]

Again, if we set \( (h', z') = ((h, 1), (z, z_n)) \), then, on one hand, we clearly have:
\[
\frac{\partial \eta_n^{h} \zeta_n^{i}}{\partial \eta_n} = \frac{\partial c \eta_n^{i}}{\partial \eta_n} \eta_n \zeta_n^{i} \quad i \neq n,
\]
so that \( D(c) \zeta_n^{i} \) is equal to
\[
\sum_{i=1}^{n-1} \frac{\partial \eta_n^{h} \zeta_n^{i}}{\partial \eta_n} X_i + \sum_{i=1}^{n-1} \eta_n \frac{\partial \eta_n^{h} \zeta_n^{i}}{\partial \eta_n} \zeta_n^{i-1} X_i^{p-1}.
\]
Now, using the graded-commutativity, we obtain
\[
\eta_n^{h} \zeta_n^{i} = (-1)^{i=1} \eta_n \zeta_n^{i}.
\]
Therefore, it is clear that
\[
\frac{\partial \eta_n^{h} \zeta_n^{i}}{\partial \eta_n} = (-1)^{i=1} \eta_n \zeta_n^{i},
\]

hence the expected formula.

Since \( \omega_s(F_p) \) is just but the kernel of \( D_s \), we can deduce the proposition.

Now, what happens vis-à-vis \( \omega_{-s-1}(F_p) \) is quite similar to our argument: we can consider the dual resolution of the initial one. Using again the Künneth formula and doing the same computation, we can obtain an expression of the differential \( D \); but rather than considering the kernel of the differential, we compute the cokernel.
We have not given yet a description of $\omega_{-1}(F_p)$ and $\omega_0(F_p)$. In fact we can extend our description to $\omega_0(F_p)$, because our formulae make still sense in this situation and they give

$$\omega_0(F_p) = \langle \zeta^0 \eta^j \mid \zeta^0 \eta^j X_i = 0, \quad \forall i \in \{1, \ldots, n\} \rangle,$$

which is only but a pompous notation for $\omega_0(F_p)$.

Finally, it is a well-known fact that $I^*$ is stably isomorphic to $\Omega^{-1}(F_p)$, where $I$ is the augmentation ideal in the group algebra $F_pE_n$, and it is generated by one element, which should logically be denoted by $\zeta^0 \eta^0$, but in order to emphasize its specificity we will call it $\alpha$. Furthermore it verifies the only relation $\alpha \prod_{1 \leq i \leq n} X_i^{p-1} = 0$, and this concludes the proof.

**Example.** We shall give a precise description of two modules of those families: $\omega_1(F_p)$ and $\omega_{-2}(F_p)$. (The reader who wants a third example can have a glimpse at the last corollary to Lemma 11 at the very end of this section: its proof starts with a description of $\omega_2(F_p)$.)

The generators of $\omega_1(F_p)$ are simply the $\eta_i$ for $i \in \{1, \ldots, n\}$, and the relations are in fact of two kinds. The first kind consists in the relations $\text{Rel}^1(0, z_i = 1)$ (by $(0, z_i = 1)$ we mean in the obvious way the $C$-index $((0, \ldots, 1, \ldots, 0), (0, \ldots, 0))$ where the 1 is in $i$-th position), which are (for $i \in \{1, \ldots, n\}$)

$$\text{Rel}^1(0, z_i = 1): \quad \eta_i X_i^{p-1} = 0;$$

and then, using the same abbreviation, the second kind of relation is in fact (for $1 \leq i < j \leq n$)

$$\text{Rel}^1(h_i = h_j = 10, \ldots): \quad \eta_j X_i - \eta_i X_j = 0.$$

It should be noticed that $\omega_1(F_p)$ is in fact $I$, the augmentation ideal: a clear isomorphism is in fact given by the map sending $\eta_i$ to $X_i$.

What about $\omega_{-2}(F_p)$? The generators are elements of the form $\eta_i$ and there is a unique relation denoted $\text{Rel}_{-1}(0, 0)$ which is

$$\text{Rel}_{-1}(0, 0): \quad \eta_1 X_1 + \ldots + \eta_n X_n = 0.$$

**Remarks.** The following facts are noteworthy.

1. Let $d_{n,s} = \dim F_p H^s(E_n, F_p)$. Then $d_{n,s}$ is also the number of generators in our presentation of $\omega_s(F_p)$. It follows that this system of generators is minimal, which can also be deduced from the fact that all the relations belong to the radical (of the free module covering $\omega_s(F_p)$); one has

$$\tilde{H}^s(E_n, F_p) \cong \omega_s(F_p)/\text{Rad}(\omega_s(F_p)) \cong \text{hom}_{F_p E_n}(\omega_s(F_p), F_p).$$

2. The dimensions of the modules verify

$$\dim F_p \omega_{s+1}(F_p) = d_{n,s} p^n - \dim F_p \omega_s(F_p).$$

Finally, we should point out that the previous result remains true when $p = 2$; even the proof can be kept without any change! Yet it is a common place that the cohomology ring $H^*(C_2, F_2)$ is quite different from the cohomology ring of $H^*(C_p, F_p)$ with $p$ odd. Nevertheless again, all remains true, at the cost of being very silly, since nothing is well suited for $p = 2$. Indeed, for $p = 2$, taking into account the specificity of this case would lead us to make slight cosmetic changes in the description of $\omega_s(F_2)$ as an $F_2 E_n$-module: let us name it $\omega_s'(F_2)$ in this case. We would indeed name its generators $\eta^h = \eta_1^{h_1} \ldots \eta_n^{h_n}$ where the weight of $h = (h_1, \ldots, h_n)$ is $s$ and index its relations by the multi-indices of weight $s + 1$, relations who are in fact the following

$$\text{Rel}^s(h): \sum_{i=0}^n \frac{\partial h}{\partial \eta_i} X_i = 0.$$
However, there exists an isomorphism between this presentation and the one previously given, by setting

\[
\psi: \; \omega_s(F_2) \rightarrow \omega'_s(F_2)
\]

\[
\zeta \eta^h \rightarrow \eta_1^{2z_1 + h_1} \eta_2^{2z_2 + h_2} \ldots \eta_n^{2z_n + h_n}
\]

2.2. The module \(M_n\). We shall rediscover the module \(\omega_2(F_p)\) in a completely different way.

2.2.1. Notation & conventions. If \(G\) is a finitely generated pro-\(p\)-group, \(\Phi(G)\) denotes its Frattini subgroup, which means that \(\Phi(G) = G^p(G, G)\). By \((G, G)\) we mean of course the group generated by the commutators

\[
(g_1, g_2) = g_1^{-1} g_2^{-1} g_1 g_2, \forall g_1, g_2 \in G.
\]

Whenever \(H \leq G\), the group \(G\) acts by conjugation on \(H\), and we write

\[
h^g = g^{-1} h g, \; \forall h \in H, \forall g \in G.
\]

Thus \(G\) acts on \(M_G = \Phi(G)/\Phi^{(2)}(G)\) by conjugation, and since the action of \(\Phi(G)\) is trivial modulo \(\Phi^{(2)}(G)\), we will study the action of \(G/\Phi(G) \cong E_r\) for some \(r\). As \(M_G\) is an \(F_p\) vector space, it is, all in all, an \(F_pE_r\)-right module, with the elementary abelian group \(E_r\) identified as above.

On \(M_G\) we shall use an additive notation, i.e. we write

\[
[\alpha, \beta] = [\alpha] + [\beta], \; \forall \alpha, \beta \in \Phi(G),
\]

where \([\alpha]\) denotes the class of \(\alpha\) modulo \(\Phi^{(2)}(G)\). However, usually the additive notation makes it unnecessary to use brackets, and we may simply write \(\alpha + \beta\) for \(\alpha, \beta \in \Phi(G)\).

As for the action, our convention is to write \([\alpha]\cdot x\) for \([\alpha^x]\) (where \(\alpha \in \Phi(G)\) and \(x \in G\)), and more generally we write \([\alpha]\cdot \lambda\) where \(\lambda \in F_pE_r\). Moreover, we extend the convention we introduced in §1.1: if we have used a letter, say \(x\), to denote an element of \(G\), then we shall usually use the same letter \(x\) for its image in \(G/\Phi(G)\) and the capitalized letter \(X\) for \(x - 1 \in F_p(G/\Phi(G))\).

Here is an example of computation with all our conventions at work:

\[
\alpha \cdot X = \alpha^x - \alpha = x^{-1} \alpha x \alpha^{-1} = (x, \alpha^{-1}),
\]

for \(\alpha \in \Phi(G)\) and \(x \in G\).

This applies in particular to \(G = F_n\), the free pro-\(p\)-group on \(n\) generators. In this case we write \(M_n := \Phi(F_n)/\Phi^{(2)}(F_n)\). We shall give a presentation by generators and relations of \(M_n\) as an \(F_pE_n\)-module, where \(E_n = F_n/\Phi(F_n)\), and then remark that it coincides with the presentation previously given of \(\omega_2(F_p)\).

2.2.2. Some classical relations. Let \(G\) be a finitely generated pro-\(p\)-group. Let us recall some classical formulae about commutators, translated into relations about \(\Phi(G)/\Phi^{(2)}(G)\) as a module with an action of \(G\). When we specialize to \(G = F_n\) below, we shall see that we have in fact described all the relations, in the sense that we have a presentation.

Lemma 9. Let \(x, y, z\) be three elements of \(G\), then the following relation holds in \(\Phi^{(2)}(G)/\Phi(G)\):

\[
(y, x)Z + (x, z)Y + (z, y)X = 0,
\]

where \(X = x - 1\) (similarly for \(y\) and \(z\)). Furthermore we have:

\[
y^p \cdot X = (x, y)Y^{p-1}.
\]

Proof. We recall the Hall-Witt formula (cf. [DSMS99] or [Laz54]). Let \(x, y, z\) be three elements of a pro-\(p\)-group \(G\), then

\[
((x, y^{-1}), z)^y((y, z^{-1}), x)^z((z, x^{-1}), y)^z = 1.
\]
Indeed it is clear that
\[(x, y^{-1})^y = y^{-1}x^{-1}yxy^{-1}y = y^{-1}x^{-1}yx = (y, x).\]

We can deduce the following well-known relation, similar to the Jacobi relation in the realm of Lie algebras:
\[(y, x)Z + (x, z)Y + (z, y)X = 0 \pmod{\Phi^2(G)}.\]

Indeed using the Hall-Witt relation and the previous remark, we have:
\[
\begin{align*}
1 &= ((x, y^{-1}, z)^y((y, z^{-1}), x)^z((z, x^{-1}), y)^x) \\
&= ((x, y^{-1})^{-1}(x, y^{-1})^y((y, z^{-1})^{-1}(y, z^{-1})^y) x((z, x^{-1})^{-1}(z, x^{-1})^y)^x \\
&= ((x, y)^{-1}(y, x)^y)((z, y)^{-1}(z, y)^y)((x, z)^{-1}(x, z)^y).
\end{align*}
\]

The following equalities, which could be found in [DSMS99], will be useful:
\[
\begin{align*}
(x, yz) &= (x, z)(x, y)^z \\
(xy, z) &= (x, z)^y(y, z) \\
(y^n, x) &= (x, y)^{y^{n-1}}(x, y)y^{n-2} \ldots (x, y),
\end{align*}
\]

hence
\[(y^k, x) = \sum_{i=0}^{k-1} (x, y) \cdot y^i = (x, y) \cdot \sum_{i=0}^{k-1} y^i \pmod{\Phi^2(G)}.\]

Since in \(\mathbb{F}_p[T]\) the following polynomial identity holds
\[
\sum_{i=0}^{p-1} T^i = (T - 1)p^{-1},
\]
we get for \(k = p\) the following formula:
\[
(y^p, x) = (x, y) \cdot Y^{p-1}.
\]

Given that
\[
y^p \cdot X = (y^p)^x - y^p = x^{-1}y^px - y^p = y^{-p}x^{-1}y^px = (y^p, x),
\]
we obtain the expected relation:
\[
y^p \cdot X = (x, y)Y^{p-1}. \quad \square
\]

2.2.3. The free group. Now we specialize to \(G = \mathcal{F}_n\), the free pro-\(p\) group on \(n\) generators, which will be called \(\chi_1, \ldots, \chi_n\). The images of these in \(E_n = \mathcal{F}_n/\Phi(\mathcal{F}_n)\) will be called \(x_1, \ldots, x_n\). We write \(X_i = x_i - 1 \in \mathbb{F}_p E_n\).

According to the previous relations (5), the 2-commutators (i.e. the \((\chi_i, \chi_j)\)) and the \(\chi_i^p\) form a generating system for \(M_n\) as \(\mathbb{F}_p E_n\)-module. The first thing we note is that
\[
(\chi_i, \chi_j) = - (\chi_j, \chi_i).
\]

Simply because \(\chi_i\) commutes with \(\chi_i^p\), we certainly have
\[
\chi_i^p \cdot X_i = 0.
\]

Next, from the relation (4) of the lemma, we have
\[
\chi_j^p \cdot X_i = (\chi_i, \chi_j)X_j^{p-1}.
\]

And finally, from (3), we obtain:
\[
(\chi_k, \chi_j) \cdot X_i + (\chi_j, \chi_i) \cdot X_k + (\chi_i, \chi_k) \cdot X_j = 0.
\]

Ultimately, we shall prove that the four types of relations just given between the generators provide a presentation for \(M_n\), i.e. they generate the module of relations.

The strategy is as follows. First we note that it is enough to include the 2-commutators with \(i < j\), of course, so we have \(\binom{n}{2}\) commutators and \(n\) elements of the form \(\chi_i^p\). Let \(F_{n, p}\)
be the free $F_pE_n$-module on elements called $e_1, \ldots, e_n$ and $e_{i,j}$ for $i < j$. There is a short exact sequence

$$0 \longrightarrow K \longrightarrow F_{n,p} \overset{\psi}{\longrightarrow} M_n \longrightarrow 0,$$

where $\psi(e_i) = \chi_i^p$ and $\psi(e_{i,j}) = (\chi_i, \chi_j)$. We want to show that $K = \ker(\psi)$ is generated by the elements above. For this, we shall determine the dimension of $M_n$ (which is easy), so that we will know the dimension of $K$ over $F_p$. The work will consist in exhibiting carefully selected elements of $K$, all obtained from the above using the $F_pE_n$ action, which are linearly independent over $F_p$ and numerous enough for us to conclude that they span $K$.

2.2.4. A basis for $K$. The dimension of $M_n$ is well-known.

**Lemma 10.** With our notation:

$$\dim_{F_p} M_n = 1 + (n - 1) \cdot p^n.$$

**Proof.** According to [Koc02], example 6.3, we have that the minimal number of topological generators of $\Phi(F_n)$ - denoted $d(\Phi(F_n))$ - is equal to $p^n(n - 1) + 1$, therefore we can conclude by definition of the Frattini subgroup. □

When $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index, we set

$$X^\nu = X_1^{\nu_1}X_2^{\nu_2}\ldots X_n^{\nu_n}.$$

Note that the family $(X^\nu)_{\nu \in \mathcal{I}}$, where $\mathcal{I} = \{0, \ldots, p-1\}^n$ is an $F_p$ basis of the group algebra $F_pE_n$. We will write $\mathcal{E}$ for this basis. Now we proceed to introduce distinguished elements of $K$.

- The relations $R(i, m)$ and $R(i, j, m)$.

For each $1 \leq i \leq n$ and $m = (m_1, \ldots, m_n) \in \{0, \ldots, p-1\}^n$, a multi-index such that $m$ is different from $(0, \ldots, 0)$, we introduce

$$R(i, m) = \begin{cases} 
  e_i \cdot X_i^{m_i} \cdot \prod_{s \neq i} X_s^{m_s}, & \text{if } m_i \neq 0, \\
  e_i \cdot X_j^{m_j} \cdot \prod_{s \neq i, j} X_s^{m_s} + e_{(i,j)} \cdot X_i^{p-1}X_j^{m_j-1} \prod_{s \neq i,j} X_s^{m_s}, & \text{if } i < j, \\
  e_i \cdot X_j^{m_j} \cdot \prod_{s \neq j} X_s^{m_s} - e_{(j,i)} \cdot X_i^{p-1}X_j^{m_j-1} \prod_{s \neq i,j} X_s^{m_s}, & \text{if } i > j,
\end{cases}$$

where $j = \max\{s | m_s \neq 0\}$ in the second and third case and clearly $m_i = 0$. By virtue of the relation (4), we deduce that $R(i, m)$ is in the kernel of $\psi$. We have therefore found exactly

(7) \(n \cdot (p^n - 1)\)

vectors in the kernel so far.

By virtue of the same relation, we obtain that

(8) \((\chi_i, \chi_j)X_i^{p-1}X_j^{p-1} = \chi_i^pX_j^p = 0,\)

thus vectors of the form

$$R(i, j, m) = e_{(i,j)}X_j^{p-1}X_i^{p-1} \prod_{k<i} X_k^{m_k}$$

are in the kernel, for a total amount of

(9) \(\sum_{i=1}^n (n - i) \cdot p^{i-1}\)

vectors of those form.

- Relations of Jacobi type.
Let $\chi_i, \chi_j, \chi_k$ be three elements of our generating system of $\mathcal{F}_n$ with $i \leq j \leq k$. Because of (3) and the elementary properties on the commutators, we get:

\begin{equation}
(\chi_i, \chi_j)X_k = (\chi_i, \chi_k)X_j - (\chi_j, \chi_k)X_i.
\end{equation}

Thus elements of the form $e_{(i,j)}X_k - e_{(i,k)}X_j + e_{(j,k)}X_i$, where $i < j < k$, lie in the kernel. More generally, by multiplying the previous relation by $X^m$ verifying the following conditions

1. $m_k \neq p - 1$,
2. if $i > k$ then $m_i = 0$,

we deduce that vectors of the following form lie also in the kernel:

\[ e_{(i,j)} \cdot X^{m_k+1}_k \cdot \prod_{s < k} X^{m_s}_s + e_{(j,k)} \cdot X^{m_i+1}_i \cdot \prod_{s \neq i, s < k} X^{m_s}_s - e_{(i,k)} \cdot X^{m_j+1}_j \cdot \prod_{s \neq j, s < k} X^{m_s}_s, \]

where $m \in \{0, \ldots, p - 1\}^n$ is a multi-index such that $m$ is different from $(0, \ldots, 0)$.

Such vectors are denoted $\text{jac}_1(i, j, k, m)$; clearly $m_k \leq p - 2$, and their number is

\[ (p - 1) \cdot \sum_{k=0}^{n} \binom{k - 1}{2} \cdot p^{k-1}. \]

By multiplying (10) by $X_k^{p-1}$, we obtain the relation

\begin{equation}
(\chi_i, \chi_k)X_k^{p-1}X_j = (\chi_j, \chi_k)X_k^{p-1}X_i.
\end{equation}

Therefore, by multiplying by $X^m$ where $m$ verify the following conditions

1. $m_j \neq p - 1$,
2. if $i > j$, $m_i = 0$,

we get again vectors of the form

\[ e_{(i,k)}X_k^{p-1}X_j^{m_j+1} \prod_{s < j} X^{m_s}_s - e_{(j,k)}X_k^{p-1}X_i^{m_i+1} \prod_{s \neq i, s < j} X^{m_s}_s, \]

where $i < j < k$, which are in the kernel. Hence we have added in our kernel a total amount of

\[ (p - 1) \cdot \sum_{j=1}^{n} (j - 1)(n - j)p^{j-1} \]

vectors of this form, they are denoted by $\text{jac}_2(i, j, k, m)$.

From now on, we set

\[ F = \{R(i, m), R(i, j, m), \text{jac}_1(i, j, k, m), \text{jac}_2(i, j, k, m)\}, \]

with the conditions on $i, j, k, m$ given above.

**Lemma 11.** The system $F$ is a basis of $\ker \psi$.

**Proof.** All vectors contained in $F$ are in $\ker \psi$ by definition; we shall prove that they are linearly independent and that their number is equal to $\dim F_{n,p} - \dim M_n$.

**Linear independence.** Bear in mind that $\mathcal{E}$ is the basis of $F_{n,p}$ consisting of the $e_i \cdot X^\nu$ and the $e_{(i,j)} \cdot X^\nu$ where $\nu$ and $\mu$ are elements of $\{0, \ldots, p - 1\}^n$. Let us define an $F_{p}$-linear map $f: F_{n,p} \to F_{n,p}$ given on the vectors of $\mathcal{E}$ by

\[
\begin{aligned}
f(e_i \cdot X^m) &= R(i, m), \\
f(e_{(i,j)} \cdot X^{m_k+1}_k \cdot \prod_{s < k} X^{m_s}_s) &= \text{jac}_1(i, j, k, m), \\
f(e_{(i,k)}X_k^{p-1}X_j^{m_j+1} \prod_{s \neq j, s < k} X^{m_s}_s) &= \text{jac}_2(i, j, k, m),
\end{aligned}
\]

and fixing the other vectors of $\mathcal{E}$; note that among those remaining vectors are the $R(i, j, m)$ for instance. In order to number the vectors of the basis, we will use an order relation rather than cumbersome formulae from combinatorics.
We define a total order relation on the vectors of $E$ by imposing the following conditions:

1. $e_i \cdot \prod X^{\nu_s}_{s} \leq e_j \cdot \prod X^{\nu_s}_{s}$ if and only if $i < j$ or $i = j$ and either $|\nu| < |\mu|$ or if $|\nu| = |\mu|$ then we use the lexicographic order.
2. $e_{(i,j)} \cdot \prod X^{\nu_s}_{s} \leq e_{(k,l)} \cdot \prod X^{\mu_s}_{s}$ if and only if one of the following condition is true
   
   (a) $i < k$
   
   (b) if $i = k$ then one of the following must be true:
      
      (i) $j < l$,
      
      (ii) $|\nu| < |\mu|$,  
      
      (iii) $\nu \leq \mu$ where $\leq$ is the lexicographic order

3. $e_i \cdot \prod X^{\nu_s}_{s} \leq e_{(j,k)} \cdot \prod X^{\mu_s}_{s}$

The matrix associated to $f$ in the canonical basis, thus ordered, is lower triangular with 1's on the diagonal, as is readily checked (when defining the elements of $F$, we have always given the formulae so that the leftmost term is the lowest for the order relation).

So $f$ is invertible, and the image of the canonical basis under $f$ is another basis for $F_{n,p}$. This proves in particular that the elements of $F$ are linearly independent.

**Cardinality.** By using the formula previously given, we can get: $\dim_{F_p} \ker \psi = \binom{n}{2} p^n - 1$. However

\begin{equation}
(12) \quad (p - 1) \cdot \sum_{k=0}^{n-1} \left(\frac{k}{2}\right) p^k = \left(n - \frac{1}{2}\right) p^n - \sum_{k=1}^{n-1} (k - 1) \cdot p^k,
\end{equation}

in the same fashion

\begin{equation}
(13) \quad (p - 1) \cdot \sum_{j=1}^{n} (n - j)(j - 1)p^{j-1} = \sum_{j=1}^{n-1} (2j - n)p^j,
\end{equation}

by adding the previous equalities we get:

\begin{equation}
(12) + (13) = \left(n - \frac{1}{2}\right) p^n + \sum_{k=0}^{n-1} kp^k - \sum_{k=0}^{n-1} kp^{k-1} + \sum_{i=1}^{n} p^{i-1} - \sum_{i=1}^{n} p^i + \sum_{k=0}^{n-1} p^k
= \left(n - \frac{1}{2}\right) p^n + \sum_{k=0}^{n-1} kp^k - \sum_{k=0}^{n-2} (k + 1)p^k + \sum_{k=0}^{n-2} p^k + \sum_{k=0}^{n-1} p^k
= \left(n - \frac{1}{2}\right) p^n + p(1 - p^{n-1}) + \sum_{k=0}^{n-1} p^k - \sum_{k=0}^{n-2} p^k
= \left(n - \frac{1}{2}\right) p^n + n - 1.
\end{equation}

If we add this to (7), we obtain the desired cardinality. \qed

From this lemma we can deduce the following three corollaries.

**Corollary.** The system formed by the vectors $(\chi_i^p)_{i=1,\ldots,n}$ and the vectors $(\chi_i, \chi_j)X^\nu$ such that $\nu$ verifies the following conditions

1. $\max\{s | \nu_s \neq 0\} \leq j$
2. $\nu_i \neq p - 1$ or $\nu_j \neq p - 1$
3. if $\nu_j = p - 1$, then $\nu_k = 0$ for $k \in \{i + 1, \ldots, j - 1\}$

forms a basis of $M_n$.

**Proof.** Let

$$B = f(E) \setminus F,$$

where $E$ is our usual basis for $F_{n,p}$ and $f$ is the endomorphism defined in the proof of the lemma. Then $\psi(B)$ is a basis for $M_n$. However, a vector of $v \in E$ is in $f^{-1}(F)$ if and only if one of the following condition is true:

1. if $v = e_iX^\nu$ where $\nu \neq (0, \ldots, 0)$
2. if $v = e_{(i,j)}X_i^{p-1}X_j^{p-1} \prod_{k \notin \{i,j\}} X_s^{m_s}$.
(3) if \( v = e_{(i,j)}X_k^{m_k} \prod_{s < k} X_s^{m_s} \), where \( m_k \neq 0 \).

(4) if \( v = e_{(i,k)}X_k^{p-1}X_j^{m_j} \prod_{s \leq i < j} X_s^{m_s} \), where \( m_j \neq 0 \).

Negating this conditions, and keeping in mind that \( f(v) = v \) if \( v \) is not in \( f^{-1}(F) \), we obtain the announced result. \( \square \)

**Corollary.** The module \( M_n \) admits the following presentation by generators and relations:

- *its generators are the \( \chi_i^p \) and the \((\chi_i, \chi_j)\) where \( i \) and \( j \) are in \( \{1, \ldots, n\} \) and \( i < j \).
- *The relations are given by*
  1. \( \chi_i^p : X_i = 0 \),
  2. \( \chi_i^p : X_j = (\chi_j, \chi_i)X_i^{p-1} \) if \( i > j \),
  3. \( \chi_i^p : X_j = -(\chi_i, \chi_j)X_j^{p-1} \) if \( i < j \),
  4. \( (\chi_i, \chi_j)X_k + (\chi_j, \chi_k)X_i - (\chi_i, \chi_k)X_j = 0 \), where \( i < j < k \).

Notice that, alternatively, we could have used generators \((\chi_i, \chi_j)\) for \( i \neq j \) (rather than just \( i < j \)), add the relation \((\chi_i, \chi_j) = -(\chi_j, \chi_i)\), and then delete relation (3) which is now redundant with (2). Also (4) can then be re-written in a more symmetrical form.

**Proof.** Let \( R_n \) be the module defined by the presentation of the corollary. It should be remarked that there exists an obvious map of modules from \( R_n \) onto \( M_n \), for the relations verified in \( R_n \) are verified in \( M_n \) too: therefore it is clear that

\[
\dim_{F_p} M_n \leq \dim_{F_p} R_n.
\]

By looking closer to the proof of the previous corollary, we see that we only used the relations mentioned in the corollary in order to construct \( F \), therefore we can show exactly by re-writing the proof of the corollary that

\[
\dim_{F_p} R_n \leq \dim_{F_p} M_n.
\]

So the dimensions are equal, and the obvious epimorphism is an isomorphism. \( \square \)

**Corollary.** The module \( M_n \) is isomorphic to \( \omega_2(F_p) \).

**Proof.** The presentations of these two modules are in fact the same. Indeed, \( \omega_2(F_p) \), as introduced in the previous section, is generated (Proposition 8) by elements of the form

\[
(1) \eta_i \eta_j \text{ for } 1 \leq i < j \leq n
\]
\[
(2) \zeta_i \text{ for } i \in \{1, \ldots, n\}.
\]

The relations which are verified are in fact

\[
(1) \text{ If } 0 \leq i \leq n \text{ then } Rel(h_i = 1, z_i = 1): \zeta_i X_i = 0,
\]
\[
(2) \text{ If } j < i \text{ then } Rel(h_j = 1, z_i = 1): \zeta_i X_j - \eta_i \eta_j X_j^{p-1} = 0,
\]
\[
(3) \text{ If } j > i, \text{ then } Rel(h_j = 1, z_i = 1): \zeta_i X_j + \eta_i \eta_j X_j^{p-1} = 0,
\]
\[
(4) \text{ If } i < j < k, \text{ then } Rel(h_i = h_j = h_k = 1): \eta_i \eta_j \eta_k X_k + \eta_j \eta_k X_i - \eta_i \eta_k X_j = 0.
\]

Therefore the map sending \( \zeta_i \) on \( \chi_i^p \) and \( \eta_i \eta_j \) on \((\chi_i, \chi_j)\) is a map of modules and in fact an isomorphism. \( \square \)

### 2.3. Applications to Galois theory.

As a very quick conclusion to this section, we can prove parts of Theorem 5. Indeed, in the case when \( k \) does not contain the \( p \)-th roots of unity, the group \( \bar{G}_k(p) \) is free, as recalled in \( \S 1.4 \). Thus the module called \( J \) in the Main Theorem is precisely \( M_n \). As we have established that \( M_n \cong \Omega^2(F_p) \), we see that it is of constant Jordan type \([1]\) (cf \( \S 1.6 \)). Moreover, for all \( s \) we have

\[
\hat{H}^s(E_n, J) = \hat{H}^s(E_n, \Omega^2(F_p)) \cong \hat{H}^{s-2}(E_n, F_p),
\]

from which the cohomological statements of Theorem 5 are clear.
3. The Heller shifts of \( J \)

In this section, \( p \) is a prime and \( k \) is a local field whose residue field has characteristic \( p \) and such that it contains a primitive \( p^{th} \)-root of unity \( \xi_p \). We then put \( K = k^\mathbb{F}_p \). It has been seen in §1.2 that \( Gal(K/k) \) is a \( p \)-elementary abelian group of rank \( n \) which will be written \( E_n \). In this section we officially put \( J = \Phi(G_k(p))/\Phi^{(2)}(G_k(p)) \), keeping in mind from Lemma 3 and the preceding discussion that \( J \) is isomorphic to \( K^\times/K^{\times p} \) (and also to its dual) as an \( E_n \)-module.

Building on the previous section, we shall find presentations in terms of generators and relations for \( \omega_s(J) \), an \( E_n \)-module stably isomorphic to \( \Omega^s(J) \) (for \( s \geq 0 \)). We relate these modules to the previous ones by means of exact sequences, as announced in the introduction.

Throughout this section, we assume that \( p > 2 \) and that \( k \) contains a \( p^2 \)-th root of unity \( \xi_{p^2} \). The necessary modifications to cover the alternative cases (which are not more difficult to handle, only a little different) will be given later.

3.1. The module \( \omega(J) \). We start with a presentation of \( J \). We shall use freely the notation introduced in the previous section, and the reader should review the presentation for \( \omega_2(F_p) \) (from Proposition 8 or the last corollary to Lemma 11).

**Lemma 12.** The module \( J \) can be presented as:

\[
J \cong \omega_2(F_p)/(\Delta)
\]

where \( 1 \leq i < j \leq n \), and \( (h, z) \) runs through the \( C \)-indices of weight 3; as for \( \Delta \), it stands for the relation

\[
\eta_1 \eta_2 + \eta_3 \eta_4 + \ldots + \eta_{n-1} \eta_n = 0.
\]

**Proof.** The Demuškin group \( G_k(p) \cong D_{k,n} \) is the quotient of the free pro-\( p \)-group \( F_n \) by the relation

\[
\Delta : x_1^{p^i}(x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n) = 1,
\]

and \( k \geq 2 \) from our assumption that \( \xi_{p^2} \in k \) (see §1.4). It is clear that \( \Delta \in \Phi(F_n) \).

When \( G \) is a finitely generated pro-\( p \) group, and \( K \) is a closed subgroup, one sees easily that \( \Phi(G) \) maps onto \( \Phi(G/K) \) under the quotient map \( G \longrightarrow G/K \). Moreover, if \( K \subset \Phi(G) \), then \( \Phi(G/K) \) can be identified with \( \Phi(G)/K \). Clearly, if \( N \) denotes the smallest closed, normal subgroup containing \( \Delta \), we have \( N \subset \Phi(F_n) \) and so there is an exact sequence

\[
0 \longrightarrow N \longrightarrow \Phi(F_n) \longrightarrow \Phi(D_{k,n}) \longrightarrow 1.
\]

Now by the same reasoning, we see that \( \Phi^{(2)}(F_n) \) maps onto \( \Phi^{(2)}(D_{k,n}) \); it follows easily that there is another exact sequence

\[
0 \longrightarrow N/(N \cap \Phi^{(2)}(F_n)) \longrightarrow \Phi(F_n)/\Phi^{(2)}(F_n) \longrightarrow \Phi(D_{k,n})/\Phi^{(2)}(D_{k,n}) \longrightarrow 1.
\]

This says in other notation, using our identification of \( M_n \) with \( \omega_2(F_p) \), that the kernel of \( \omega_2(F_2) \longrightarrow J \) is generated, as \( F_p E_n \)-module, by \( \Delta \).

**Remark.** We should point out immediately that this presentation is not a minimal: indeed we could get rid of a generator among the subset \( \{ \eta_1 \eta_2, \ldots, \eta_{n-1} \eta_n \} \), for instance \( \eta_{n-1} \eta_n \), according to the relation \( \Delta \); however by excluding it, the relations loose a lot of their symmetry. Simple facts about the socle filtration can be shown, in the spirit of [AGKM01]; they may be still worthwhile, but as it is not the main subject of this article we relegate them to Appendix A.
Corresponding to this presentation is a short exact sequence

\[ 1 \longrightarrow \ker \pi_0 \overset{i_0}{\longrightarrow} F \overset{\pi_0}{\longrightarrow} J \longrightarrow 1, \]

where \( F \) is a free \( \mathbb{F}_p E_n \) module of rank \( d_{n,2} \) (recall that we write \( d_{n,s} = \dim_{\mathbb{F}_p} H^s(E_n, \mathbb{F}_p) \)). By definition, the module \( \ker \pi_0 \) is stably isomorphic to \( \Omega(J) \). We know a system of generators for \( \ker \pi_0 \), namely the \( \text{Rel}^3(z, h) \) and \( \Delta \), and our task, of course, is to find the “relations between the relations”.

Here is what the answer will be. In order to make the formulae less cumbersome, we introduce the following notation for the norm:

\[ N = \prod_{1 \leq i < n} X_i^{p-1} = \sum_{x \in E_n} x, \]
\[ N^j = \prod_{i \neq j} X_i^{p-1}. \]

We then define \( \omega(J) \) to be the module

\[ \omega(J) = \langle \eta_1 \zeta_i, \eta_1 \eta_2 \eta_3, \Delta \mid \text{Rel}^4(h, z), \Delta N = \sum_{i} \eta_2 \zeta_{i-1} \rangle, \]

where \((h, z)\) runs through the \( C \)-indices of weight \( 4 \), the indices \( i, j \) are in \( \{1, \ldots, n\} \), and \( 1 \leq i_1 < i_2 < i_3 \leq n \). As the notation of course suggests, we shall establish that \( \omega(J) \) is stably isomorphic to \( \Omega(J) \), and we shall accomplish this by showing that \( \omega(J) \) is (genuinely) isomorphic to \( \ker \pi_0 \).

We start by gathering basic information.

**Lemma 13.** Let the modules \( \omega(J) \) and \( \ker \pi_0 \) be as above.

1. The dimension of \( J \) over \( \mathbb{F}_p \) is \( 2 + (n - 2) \cdot p^n \).
2. There is an exact sequence

\[ 0 \longrightarrow \omega_3(\mathbb{F}_p) \overset{\varphi}{\longrightarrow} \omega(J) \overset{\psi}{\longrightarrow} \omega_{-1}(\mathbb{F}_p) \longrightarrow 0, \]

where \( \varphi \) maps \( \eta^i \zeta^j \in \omega_3(\mathbb{F}) \) to the element with the same name in \( \omega(J) \), while \( \psi \) maps \( \eta^i \zeta^j \in \omega(J) \) to \( 0 \) and maps \( \Delta \) to \( \alpha \) (with notation as in Proposition 8).
3. We have

\[ \dim_{\mathbb{F}_p} \omega(J) = \dim_{\mathbb{F}_p} \ker \pi_0 = \dim_{\mathbb{F}_p} \omega_3(\mathbb{F}_p) + p^n - 1. \]

**Proof.** (1) According to exercise 6 of §4.5 in [Ser97], if \( G \) is a Demuškin group, then for every open subgroup \( H \), if \( r_G \) (resp. \( r_H \)) denotes the rank of \( G \) (resp. \( H \)), we have the following formula:

\[ r_H - 2 = (G : H)(r_G - 2). \]

Applying this to \( H = \Phi(G_k(p)) \), which is an open subgroup ([DSMS99]), and using that \( r_H = \dim_{\mathbb{F}} H/\Phi(H) = \dim_{\mathbb{F}} J \), we obtain the result.

(2) From the definitions of the modules involved, it is clear that \( \varphi \) and \( \psi \) are well-defined and that \( \psi \) is surjective. That \( \varphi \) is injective follows easily by inspection, as the new relation in \( \omega(J) \) involves the new generator \( \Delta \). It is clear that \( \omega_3(\mathbb{F}_p) \subset \ker \psi \), and the induced map \( \omega(J)/\omega_3(\mathbb{F}_p) \longrightarrow \omega_{-1}(\mathbb{F}_p) \) has an inverse mapping \( \alpha \) to \( \Delta \), so \( \omega_3(\mathbb{F}_p) = \ker \psi \).

(3) From (2) we see that the dimension of \( \omega(J) \) is \( \dim_{\mathbb{F}_p} \omega_3(\mathbb{F}_p) + \dim_{\mathbb{F}_p} \omega_{-1}(\mathbb{F}_p) \), and \( \dim_{\mathbb{F}_p} \omega_{-1}(\mathbb{F}_p) = p^n - 1 \) as \( \omega_{-1}(\mathbb{F}_p) \cong I^a \), the dual of the augmentation ideal. On the other hand, (1) shows that \( \dim_{\mathbb{F}_p} \ker \pi_0 = \dim_{\mathbb{F}_p} F - \dim_{\mathbb{F}_p} J = \dim_{\mathbb{F}_p} F - (2 + (n - 2) p^n) \), and as the rank of the free module \( F \) is \( d_{n,2} \), we have \( \dim_{\mathbb{F}_p} F = d_{n,2} p^n \). Now we recall that

\[ \dim_{\mathbb{F}_p} \omega_3(\mathbb{F}_p) = d_{n,2} p^n - \dim_{\mathbb{F}_p} \omega_2(\mathbb{F}_p), \]

as pointed out at the end of §2.1; also \( \dim_{\mathbb{F}_p} \omega_2(\mathbb{F}_p) = 1 + (n - 1) p^n \) (for example this follows from the isomorphism \( \omega_2(\mathbb{F}_p) \cong M_n \) and Lemma 10, but of course may be computed directly). Rearranging terms, we get the announced result. \( \square \)
Proposition 14. The module $\omega(J)$ is isomorphic to $\ker \pi_0$, and thus is stably isomorphic to $\Omega(J)$.

Proof. We return to the surjective map $\pi_0: F \longrightarrow J$. Let the generators of the free module $F$ be labelled $\zeta_i$ and $\eta_i\bar{\eta}_j$, so that $\pi_0(\zeta_i) = \zeta_i$ and $\pi_0(\eta_i\bar{\eta}_j) = \eta_j\bar{\eta}_j$. According to Lemma 12, the module $\ker \pi_0$ is generated by the element $\varepsilon_\Delta := \sum_i \bar{\eta}_{2i-1} \bar{\eta}_{2i}$, and the elements which we now call $\varepsilon_{i\eta\zeta} \bar{\eta}$, obtained from the left-hand-side of equation $\text{Rel}^3(z, h)$ by “adding bars”. For example, as the relation $\text{Rel}^3(h_{2i} = 1, z_{2i-1} = 1)$ reads

$$-\zeta_{2i-1} X_{2i} + \eta_{2i-1} \eta_i X_{2i-1}^{p-1} = 0,$$

we have

$$\varepsilon_{\eta_2, \zeta_{2i-1}} = -\bar{\zeta}_{2i-1} X_{2i} + \bar{\eta}_{2i-1} \bar{\eta}_2 X_{2i-1}^{p-1}.$$

We attempt to define a map

$$\theta: \omega(J) \longrightarrow \ker \pi_0$$

which satisfies $\theta(\eta^h \zeta^z) = \varepsilon_{i\eta\zeta} \bar{\eta}$ and $\theta(\Delta) = \varepsilon_\Delta$. If we can merely prove that it is well-defined, then it will be surjective, and hence an isomorphism since we have computed above that the dimensions of the two modules are equal. Hence our task is to show that the elements $\varepsilon_{i\eta\zeta} \bar{\eta}$ and $\varepsilon_\Delta$ satisfy the relations described in our definition of $\omega(J)$.

Part of this has already been done, of course, since $J$ is a quotient of $\omega_2(F_p)$. More precisely, we have the following commutative diagram :

$$
\begin{array}{ccc}
0 & \longrightarrow & \omega_2(F_p) \\
\eta^h \zeta^z \mapsto \varepsilon_{i\eta\zeta} & = & \ker \pi_0 \\
\eta \bar{\eta}_j \mapsto 0 & \longrightarrow & F \\
\end{array}
\downarrow
\begin{array}{ccc}
\omega_2(F_p) & \longrightarrow & 0 \\
& \longrightarrow & J := \omega_2(F_p)/\langle \Delta \rangle \\
\end{array}
\downarrow
\begin{array}{ccc}
0 & \longrightarrow & \omega_2(F_p) \\
\end{array}
$$

We see that the submodule generated by the elements $\varepsilon_{i\eta\zeta} \bar{\eta}$ is a homomorphic image of $\omega_3(F_p)$ within $\ker \pi_0$. Since the relations $\text{Rel}^4(h', z')$ hold in $\omega_3(F_p)$, as established in the previous section, they must also hold in $\ker \pi_0$.

The nontrivial work occurs with the relation involving $\Delta$: we must prove that

$$\varepsilon_{i\eta\zeta} N - \sum_i \varepsilon_{\eta_2, \zeta_{2i-1}} \bar{N}_{2i-1} = 0.$$

Indeed:

$$\begin{align*}
\varepsilon_{i\eta\zeta} N - \sum_i \varepsilon_{\eta_2, \zeta_{2i-1}} \bar{N}_{2i-1} &= \sum_i \eta_{2i-1} \bar{\eta}_{2i} N - \sum_i (-\bar{\zeta}_{2i-1} X_{2i} \bar{N}_{2i-1} + \bar{\eta}_{2i-1} \bar{\eta}_2 X_{2i-1}^{p-1} \bar{N}_{2i-1}) \\
&= \sum_i \eta_{2i-1} \bar{\eta}_{2i} N - \sum_i \bar{\eta}_{2i-1} \bar{\eta}_2 X_{2i-1}^{p-1} \bar{N}_{2i-1} \\
&= 0,
\end{align*}$$

using $X_{2i} \bar{N}_{2i-1} = 0$ and $X_{2i-1}^{p-1} \bar{N}_{2i-1} = N$. \hfill $\square$

At this point, we should emphasize that we have found a module $\omega(J)$, stably isomorphic to $\Omega(J)$, and fitting in an exact sequence

$$
\begin{array}{ccc}
0 & \longrightarrow & \omega_3(J) \\
\longrightarrow & \longrightarrow & \omega(J) \\
\longrightarrow & \longrightarrow & \omega_4(J) \\
& \longrightarrow & 0
\end{array}
$$

We have explained in §1.6 (see the discussion surrounding Lemma 7) how this implies that $J$ has constant Jordan type, perhaps the single most important claim in this paper.

Remark. The careful reader may probably wonder why we had to study a presentation of $\Omega(J)$ instead of studying $J$; in fact one can show that $J$ fits into an exact sequence of the form

$$
\begin{array}{ccc}
0 & \longrightarrow & \omega_{-1}(F_p) \\
& \longrightarrow & \omega_2(F_p) \\
& \longrightarrow & J \\
& \longrightarrow & 0
\end{array}
$$

The epimorphism from $\omega_2(F)$ onto $J$ is only the one coming from $M_n$ to $J$. However, the proofs of the most interesting facts are not so straightforward, since this sequence is not locally split exact.
3.2. The modules $\omega_s(J)$ for $s \geq 2$. Now we shall give a precise depiction of the modules $\omega_s(J)$ when $s \geq 2$. As in the case of $\omega(J)$, we define the modules first, and subsequently prove that they are stably isomorphic to the appropriate Heller shifts.

So let $s \geq 2$. We define $\omega_s(J)$ with a presentation. The generators are named $\eta^h \zeta^z$ where $(h, z)$ is a $C$-index of weight $s + 2$, and $\mu^m \delta^d$ where $(m, d)$ is a $C$-index of weight $s - 2$.

The relations are:

(1) The relations $\text{Rel}^{s+3}(h'', z'')$ where $(h'', z'')$ is a $C$-index of weight $s + 3$; these involve only the generators $\eta^h \zeta^z$. (Recall that these relations were introduced in Proposition 8; they show up in the definition of $\omega_{s+2}(F_p)$.)

(2) Extra relations, involving the $\mu^m \delta^d$, which are indexed by the $C$-indices of weight $s - 1$ and denoted $\delta-\text{Rel}^{s-1}(m'', d'')$. They are given by:

(a) If $s$ is even and $(m'', d'') = (m''_{2i-1} = 1, d''_{2i-1} = \frac{s-2}{2})$ then the relation $\delta-\text{Rel}^{s-1}(m'', d'')$ is:

$$ \delta_{2i-1} X_{2i-1} = \eta_{2i-1} \eta_{2i} \zeta_{2i-1}^2 N^{2i-1}, $$

(b) if $s$ is odd and $(m'', d'') = (m'' = 0, d''_{2i-1} = \frac{s-1}{2})$ then the relation $\delta-\text{Rel}^{s-1}(m'', d'')$ is:

$$ \mu_{2i-1} \delta_{2i-1} X_{2i-1} = \eta_{2i} \zeta_{2i-1}^{s+1} N^{2i-1}. $$

(c) in all other cases for $(m'', d'')$, the relation $\delta-\text{Rel}^{s-1}(m'', d'')$ is:

$$ \sum_{i=1}^n \mu_i (\mu^m \delta^d) \delta_i^{-1} X_i^{p-1} + \frac{\partial (\mu^m \delta^d)}{\partial \mu_i} X_i = 0. $$

Where the operators $\frac{\partial}{\partial \mu_i}$ and $\delta_i^{-1}$ are defined in the same way as $\frac{\partial}{\partial \eta_{2i}}$ and $\zeta_i^{-1}$.

(These “generic” relations show up, in other notation, in the definition of $\omega_{s-2}(F_p)$; the other relations are “exceptional cases”.)

We point out that our presentation for $\omega(J)$ does not appear as a particular case of this one for $s = 1$. This will be reflected, in the next section, with the calculation of the cohomology groups of $J$, which have a regular behaviour for $s \geq 2$ only.

Example. If $s = 2$ then the module $\omega_2(J)$ is generated by elements of the form $\eta^h \zeta^z$ where $(h, z)$ is a $C$-index of weight 4 and $\mu^0 \delta^0$. As the relations between the elements $\eta^h \zeta^z$ are new, we will only describe the $\delta$-relations. They are of two types:

• The generic relations (sub-case (c)) are simply

$$ \delta-\text{Rel}^1(0, h_{2i} = 1): \quad \mu^0 \delta^0 X_{2i} = 0. $$

• The relations in the subcase (a) are a bit trickier:

$$ \delta-\text{Rel}^1(0, h_{2i-1} = 1): \quad \mu^0 \delta^0 X_{2i-1} = \eta_{2i-1} \eta_{2i} \zeta_{2i-1} N^{2i-1}. $$

It should be remarked that the expected module as a vector space (not and as a module) is just $\omega_2(F_p) \oplus F_p$, where the copy of $F_p$ is generated by $\mu^0 \delta^0$. Thus the module looks -at first glance- like $\omega_1(F_p) \oplus \omega_0(F_p)$; it would have been genuinely isomorphic to this direct sum if the relation called $\delta-\text{Rel}^1(0, m_{2i-1} = 1)$ had been $\mu^0 \delta^0 X_{2i-1} = 0$, which it is not. However, this relation indicates how to “glue” our copy of $\omega_{s-2=0}(F_p)$ (generated by what comes from the Demuškin relation) to the copy of $\omega_{s+2=4}(F_p)$ (which emerges from the $\mu^m \delta^d$-free relations). It is noteworthy that the cohomology will not detect this small difference between $\omega_s(J)$ and $\omega_{s+2}(F_p) \oplus \omega_{s-2}(F_p)$ as soon as $s$ is greater than two.
Since $\omega_s(J)$ comes with a presentation, we have exact sequences (for $s \geq 1$)
\begin{equation}
0 \longrightarrow \ker \pi_s \longrightarrow F^{(s)} \longrightarrow \omega_s(J) \longrightarrow 0,
\end{equation}
where $F^{(s)}$ is a free $F_pE_n$-module of rank $d_{n,s+2} + d_{n,s-2}$ (as usual $d_{n,s} = \dim_{F_p} H^s(E_n, F_p)$, which is also the number of $C$-indices of weight $s$). Here $\ker \pi_s$ is by definition stably isomorphic to $\Omega(\omega_s(J))$. We shall proceed by induction, assuming $\omega_s(J)$ to be stably isomorphic to $\Omega^s(J)$, and proving that $\ker \pi_s$ is isomorphic to $\omega_{s+1}(J)$.

We need some preliminaries, which are similar to those of Lemma 13.

**Lemma 15.** Let $s \geq 2$.

1. There is an exact sequence
\begin{equation*}
0 \longrightarrow \omega_{s+2}(F_p) \longrightarrow \omega_s(J) \longrightarrow \omega_{s-2}(F_p) \longrightarrow 0.
\end{equation*}

2. We have
\begin{equation*}
\dim_{F_p} \omega_s(J) = \dim_{F_p} \ker \pi_{s-1} = \dim_{F_p} \omega_{s+2}(F_p) + \dim_{F_p} \omega_{s-2}(F_p).
\end{equation*}

**Proof.** For (1), one must check that the monomorphism can be defined by
\begin{equation*}
\eta^h \zeta^z \mapsto \omega_s(J),
\end{equation*}
whereas the epimorphism can be defined by
\begin{equation*}
\omega_s(J) \longrightarrow \omega_{s-2}(F_p), \quad \eta^h \zeta^z \longrightarrow \mu^m \delta^d.
\end{equation*}

Exactness is proved by inspection, arguing as we did in Lemma 13. Similarly, the reader will establish (2) by adapting the arguments used in that same proof. $\square$

**Proposition 16.** The module $\omega_s(J)$ presented above is stably isomorphic to $\Omega^s(J)$, for all $s \geq 2$.

**Proof.** In this proof, the generators of the free modules $F^{(s)}$ (see (16)) will be named by adding bars on top of the chosen names for the generators of $\omega_s(F_p)$, that is, $\eta^h \zeta^z$ and $\bar{\mu}^m \bar{\delta}^d$. For $s = 1$, we have also the simpler $\bar{\delta}$. The map $\pi_s$ removes the bars.

**Step 1.** We start by showing that $\omega_2(F_p)$ is isomorphic to $\ker \pi_1$. We proceed much as in the proof of Proposition 14. The exact sequence (16) refers to the presentation of $\omega(J)$ given in its definition. Thus $\ker \pi_1$ is generated by elements which we call $\varepsilon_{\eta^h \zeta^z}$ (for $(h, z)$ of weight 4), corresponding to the relation $\text{Rel}^4(z, \bar{h})$, and $\varepsilon_{\delta^0}$ defined unsurprisingly by
\begin{equation*}
\varepsilon_{\delta^0} = \hat{\delta} \eta - \sum_{i=1}^j \tilde{\eta}_{2i} \zeta_{2i-1} N^{2i-1}.
\end{equation*}
(We take the relations involved in the definition of $\omega(J)$ and “add bars”.) Note that we use $\delta^0$ instead of the more logical $\delta^0_{(0,0)}$ (which would make a reference to the definition of $\omega_2(J)$, as a simplification.

It is enough to show that there is a well-defined module homomorphism $\omega_2(J) \longrightarrow \ker \pi_1$ with $\eta^h \zeta^z \mapsto \varepsilon_{\eta^h \zeta^z}$ and $\delta^0_{(0,0)} \mapsto \varepsilon_{\delta^0}$. In other words, we must show that the elements $\varepsilon_{\eta^h \zeta^z}$ and $\varepsilon_{\delta^0}$ satisfy the relations which were spelled out in the Example above. As in the proof of Proposition 14, we realize that the only non-trivial work is with the “$\delta$-relations”: we must show
\begin{equation*}
\varepsilon_{\delta^0} X_{2i} = 0 \quad \text{and} \quad \varepsilon_{\delta^0} X_{2i-1} = \varepsilon_{\eta_{2i-1} \eta_{2i-1} \zeta_{2i-1} N^{2i-1}}.
\end{equation*}
The first one follows from the relations $N X_{2i} = \tilde{N}^{2i-1} X_{2i} = 0$. And as for the second one, we compute:
\begin{equation*}
\varepsilon_{\delta^0} X_{2i-1} = - (\sum_{j} \tilde{\eta}_{2j} \zeta_{2j-1} \tilde{N}^{2j-1}) X_{2i-1}
\end{equation*}
\begin{equation*}
= - \tilde{\eta}_{2i-1} \zeta_{2i-1} \tilde{N}^{2i-1} X_{2i-1}.
\end{equation*}
On the other hand, as the relation $\text{Rel}^4(h_{2i} = h_{2i-1} = 1, z_{2i-1} = 1)$ states
\[ \eta_{2i} \zeta_{2i-1} X_{2i} - \eta_{2i-1} \zeta_{2i-1} X_{2i-1} = 0, \]
we have
\[ \varepsilon \eta_{2i} \zeta_{2i-1} X_{2i} - \eta_{2i-1} \zeta_{2i-1} X_{2i-1} = 0, \]
and so
\[ \varepsilon \eta_{2i} \zeta_{2i-1} X_{2i} - \eta_{2i-1} \zeta_{2i-1} X_{2i-1} = \varepsilon \varrho, X_{2i-1} \]
as we wanted. This completes the proof that $\omega_2(J) \cong \ker \pi_1$. In particular, $\omega_2(J)$ is stably isomorphic to $\Omega(\omega(J))$ and thus to $\Omega^2(J)$.

**Step 2.** Now we turn to the proof that, for all $s \geq 2$, the module $\omega_{s+1}(J)$ is isomorphic to $\ker \pi_s$, and so is stably isomorphic to $\Omega(\omega_s(J))$. When this is done, an immediate induction shows that $\omega_s(J)$ is stably isomorphic to $\Omega^s(J)$ for all $s \geq 2$, as announced.

The argument follows the same pattern yet again. There are elements $\varepsilon \eta^h \zeta^z$ and $\varepsilon \mu^m \delta^d$ in $\ker \pi_s$, obtained from the relations which are known to hold in $\omega_s(J)$, namely $\text{Rel}^{s+3}(z, h)$ and $\delta - \text{Rel}_{(h', z')}$ respectively, by "adding bars". We must show that there is a well-defined homomorphism $\omega_{s+1}(J) \longrightarrow \ker \pi_s$ with $\eta^h \zeta^z \mapsto \varepsilon \eta^h \zeta^z$ and $\mu^m \delta^d \mapsto \varepsilon \mu^m \delta^d$. Our task is to show that the relations in $\omega_{s+1}(J)$ are mapped to 0 by this homomorphism, and this is non-trivial only for the $\delta$-relations.

We perform the non-trivial calculations in the case when $s$ is even. The reader will provide similar arguments for the case when $s$ is odd.

Let us look more precisely at the relations implying $\mu_{2i-1} \delta_{2i-1}^2$. Indeed if the $\delta$-relation does not contain $\mu_{2i-1} \delta_{2i-1}^2$, this relation between the relations is not an "exceptional case" and does not imply an "exceptional case". Everything is as if we were studying the relations in $\omega_{s-2}(F_p)$ rather than $\omega_s(J)$, and of course we have already done that. So let us study more closely these relations which are in fact $\delta - \text{Rel}^s(h, z)$ where either $(h, z) = (h = 0, z_{2i-1} = \frac{x}{q})$ or $(h, z) = (h_{2i-1} = h_i = 1, z_{2i-1} = \frac{\xi_{2i-1}}{2q})$ where $j \neq 2i - 1$. Let us first focus on the second case. We would like to prove that, writing $\varepsilon(x)$ instead of $\varepsilon_x$ for better readability:
\[ \varepsilon \left( \mu_{2i-1} \delta_{2i-1}^2 \right) X_j - \varepsilon \left( \mu_{2i-1}^\delta \delta_{2i-1}^{s+2} \right) X_{2i-1} = 0. \]
Indeed:
\[ \varepsilon \left( \mu_{2i-1} \delta_{2i-1}^{s+2} \right) X_j - \varepsilon \left( \mu_{2i-1}^\delta \delta_{2i-1}^{s+2} \right) X_{2i-1} = \delta_{2i-1}^{s+2} X_{2i-1} - \eta_{2i-1} \eta_{2i} \zeta_{2i-1} \bar{N}^{s+2} X_{2i-1} - \bar{N}^{s+2} X_{2i-1} X_j = 0. \]
Therefore the relation is verified. Then let us take a closer look at the relations $\delta - \text{Rel}^s(h = 0, z_{2i-1} = \frac{x}{2})$, which should be:
\[ \varepsilon \left( \mu_{2i-1} \delta_{2i-1}^{s+2} \right) X_{2i-1} - \varepsilon \left( \eta_{2i-1} \zeta_{2i-1} \bar{N}^{s+2} \right) \bar{N}^{s+2} X_{2i-1} = 0. \]
Let us check:
\[ \varepsilon \left( \mu_{2i-1} \delta_{2i-1}^{s+2} \right) X_{2i-1} - \varepsilon \left( \eta_{2i-1} \zeta_{2i-1} \bar{N}^{s+2} \right) \bar{N}^{s+2} X_{2i-1} = \bar{N}^{s+2} \eta_{2i-1} \eta_{2i} \zeta_{2i-1} \bar{N} \bar{N}^{s+2} \eta_{2i-1} \eta_{2i} \zeta_{2i-1} \bar{N} = 0. \]
This concludes the proof.
4. COHOMOLOGY

In this shorter section we keep the notation as in the previous one. In particular, we still assume that \( p > 2 \) and that \( \xi_p \in k \). We turn our attention to the cohomology groups of \( J \).

**Lemma 17.** Let \( G \) be a finite \( p \)-group and \( V \) be a self-dual \( F_pG \)-module. Put \( \mathcal{N} = \sum_{g \in G} g \in F_pG \). For every integer \( s \), there is an isomorphism

\[
\hat{H}^s(G, V) \cong (\omega_s(V) \cap \ker(\mathcal{N}))/\text{Rad}(\omega_s(V)),
\]

for \( \omega_s(V) \) a module stably isomorphic to \( \Omega^s(V) \).

In this lemma, and its proof, we write \( M \cap \ker \mathcal{N} \) for the kernel of the map \( m \mapsto m \cdot \mathcal{N} \) on the (right) \( F_pG \)-module \( M \).

**Proof.** Indeed we have the following simple isomorphisms (of vector spaces):

\[
\begin{align*}
\hat{H}^s(G, V) &\cong \text{hom}(\Omega^s(F_p), V) \quad \text{(definition)} \\
&\cong \text{hom}(F_p, \Omega^{-s}(V)) \quad \text{(adjunction)} \\
&\cong \text{hom}(F_p, \Omega^s(V)^*) \quad \text{(self-duality)} \\
&\cong \hat{H}^0(G, \omega_s(V)^*) \quad \text{(definition)} \\
&\cong (\omega_s(V)^*)^G/(\omega_s(V)^* \cdot \mathcal{N}) \quad \text{(classical)}.
\end{align*}
\]

However, we claim that there is an isomorphism

\[
(\omega_s(V)^*)^G/(\omega_s(V)^* \cdot \mathcal{N}) \cong \omega_s(V) \cap \ker(\mathcal{N})/(\text{Rad}(\omega_s(V))).
\]

More generally, if \( M \) is any \( G \)-module, then \((M^G/M \cdot \mathcal{N})^* \cong M^* \cap \ker \mathcal{N}/\text{Rad}(M^*)\), as we proceed to show. Our first observation is that \((M^G/M \cdot \mathcal{N})^*\) is isomorphic to the kernel of the map

\[
f^*: (M^G)^* \longrightarrow (M \cdot \mathcal{N})^*,
\]

which is the transpose of the inclusion \( f: M \cdot \mathcal{N} \longrightarrow M^G \), and thus \( f^* \) is an epimorphism. As \( G \) is a \( p \)-group, \( M^*/\text{Rad}(M^*) \cong (M^G)^* \) (since \( M^*/\text{Rad}(M^*) \) is the largest quotient of \( M^* \) with trivial action, its dual must be the largest submodule of \( M \) with trivial action). It follows a little more precisely that, if \( g: M^G \longrightarrow M \) is the inclusion map, then the following sequence is exact:

\[
0 \longrightarrow \text{Rad}(M^*) \longrightarrow M^* \xrightarrow{g^*} (M^G)^* \longrightarrow 0.
\]

Thus let us consider \( f^* \circ g^* = \iota^* \), the transpose of the inclusion \( \iota: M \cdot \mathcal{N} \longrightarrow M \), and describe its kernel in two different ways. On the one hand, if \( \varphi: M \longrightarrow F_p \), then we have

\[
(\varphi \cdot \mathcal{N})(m) = \varphi \left( m \cdot \sum_g g^{-1} \right) = \varphi(m \cdot \mathcal{N}),
\]

for \( m \in M \). This shows that the restriction of \( \varphi \) to \( M \cdot \mathcal{N} \) is identically zero if and only if \( \varphi \cdot \mathcal{N} = 0 \). In other words, and in our current notation, we have \( \ker \iota^* = M^* \cap \ker \mathcal{N} \).

However, we also have

\[
\ker \iota^* = \ker f^* \circ g^* = (g^*)^{-1}(\ker f^*).
\]

Here the kernel of \( f^* \) is \((M^G/M \cdot \mathcal{N})^*\) as initially observed. As \( g^* \) is onto, with kernel \( \text{Rad}(M^*) \), we conclude that \( \ker \iota^*/\text{Rad}(M^*) \cong \ker f^* \), which was precisely our claim. This concludes the proof. \( \square \)

The following lemma is a classic, and will be very useful:
Lemma 18. Suppose we have an exact sequence of $\mathbf{F}_p G$-modules, where $G$ is a finite group:

$$0 \longrightarrow R \longrightarrow F \overset{\pi}{\longrightarrow} M \longrightarrow 0.$$ 

Assume that $F$ is free of rank $r$, with generators $x_1, \ldots, x_r$. If $R \subset \text{Rad}(F)$, then the elements $\pi(x_1), \ldots, \pi(x_r)$ form a minimal system of generators for $M$, and their images in $M/\text{Rad}(M)$ form a basis. \hfill $\Box$

For example, this applies to the modules $\omega_s(\mathbf{F}_p)$ for all $s \geq 0$, with the presentations we have provided. As a consequence, we have the equalities (which have already been mentioned)

$$\dim_{\mathbf{F}_p} \omega_s(\mathbf{F}_p)/\text{Rad}(\mathbf{F}_p) = \text{the number of generators in the presentation} = \text{the number of } C\text{-indices of weight } s = \dim_{\mathbf{F}_p} H^s(E_n, \mathbf{F}_p) = \delta_{n,s}.$$ 

Of course, one may alternatively argue that, since $\omega_s(\mathbf{F}_p)$ was constructed from a resolution of $\mathbf{F}_p$, there is an isomorphism $\omega_s(\mathbf{F}_p)/\text{Rad}(\omega_s(\mathbf{F}_p)) \cong H^s(E_n, \mathbf{F}_p)$, essentially from the definition of cohomology groups as Ext groups. However, it is cumbersome to argue in this fashion with $\omega_s(J)$, to which we turn. In this case, the last lemma applies as long as $s \geq 1$, but our presentation for $J$ appears as an exception.

So for $s \geq 1$, the dimension of $\omega_s(J)/\text{Rad}(\omega_s(J))$ is the number of generators in the presentation provided; for $s \geq 2$ it is $d_{n,s+2} + d_{s-2}$, and for $s = 1$ it is $d_{n,3} + 1$. For $s = 0$ on the other hand, one of the generators is superfluous, so one could find a presentation with $n - 1 + \binom{n}{2}$ generators, and this one is easily seen to be minimal, so the dimension of $J/\text{Rad}(J)$ is $n - 1 + \binom{n}{2}$.

Theorem 19. We have the following isomorphisms:

$$\hat{H}^0(E_n, J) \cong \mathbf{F}_p^{n-1+\binom{n}{2}}, \\
\hat{H}^1(E_n, J) \cong \hat{H}^3(E_n, \mathbf{F}_p), \\
\hat{H}^s(E_n, J) \cong \hat{H}^{s+2}(E_n, \mathbf{F}_p) \oplus \hat{H}^{s-2}(E_n, \mathbf{F}_p) \text{ for } s \geq 2.$$ 

Proof. We rely on Lemma 17. First we claim that, when $s = 0$ or $s \geq 2$, the action of $\mathcal{N}$ is zero on all of $\omega_s(J)$. Assuming this, Lemma 17 asserts that

$$\dim_{\mathbf{F}_p} \hat{H}^s(E_n, J) = \dim_{\mathbf{F}_p} \omega_s(J)/\text{Rad}(\omega_s(J)),$$

whence the result of the theorem for these values of $s$, by the discussion above.

We prove the claim, which for $s = 0$ is trivial, so assume $s \geq 2$. That $\eta^h \zeta^s \cdot \mathcal{N} = 0$ is easy to see, indeed if there exists $i \notin \text{supp}(h)$, then multiplying Rel$^{s+2}(\delta, \gamma_i(h))$ by $\hat{N}^i X^{p-2}$, we get that

$$\eta^h \zeta^s \cdot \mathcal{N} = 0.$$ 

If there is no such $i$, then consider instead Rel$^{s+3}(\delta, \Delta_1(h))$ and multiply it simply by $\hat{N}^1$. It is clear that $\mu^m \delta^d$ verify $\mu^m \delta^d \mathcal{N} = 0$, by the same kind of computation:

$$\mu_{2i-1} \delta_{2i-1} \mathcal{N} = \eta_{2i} \zeta \hat{N}^{2i-1} \hat{N}^{2i-1} = 0.$$ 

The case where we have to consider $(h = 0, z_{2i-1} = \frac{\zeta^{2i}}{2})$ is similar. This concludes the proof of the claim (see also the remark after the proof).

It remains only to treat the case $s = 1$. We recall that
\[ \omega(J) \cong \langle \eta_j \zeta_i, \eta_i \eta_j \eta_k, \delta \mid \text{Rel}^4(h, z), \Delta \mathcal{N} = \sum_i \eta_{2i} \zeta_i - 1 \mathcal{N}^{2i-1} \rangle. \]

Still relying in Lemma 17, we need to determine the kernel of \( \mathcal{N} \). It clearly appears that \( \Delta \mathcal{N} \neq 0 \); on the other hand, we claim that all other generators given in the presentation are killed by \( \mathcal{N} \). Indeed consider \( \eta^h \zeta^z \); if \( \text{supp}(h) = \{1, \ldots, n\} \), by considering the relation \( \text{Rel}(\gamma_1(z), \Delta_1(h)) \) and multiplying it \( \mathcal{N}^1 \), we have \( \eta^h \zeta^z \mathcal{N} = 0 \), otherwise take \( i \notin \text{supp}(h) \) and considering instead the relation \( \text{Rel}(z, \gamma_i(h)) \) multiplied by \( \mathcal{N}^i X_i^{p-2} \), we obtain the desired result.

Furthermore, since the presentation is minimal (as discussed above), the generators provide a basis of \( \omega(J)/\text{Rad}(\omega(J)) \), and so we conclude that \( \ker \mathcal{N}/\text{Rad}(\omega(J)) \) is spanned by the images of the \( \eta^h \zeta^z \). Their number is \( d_{n, 3} = \dim_{\mathbb{F}_p} H^3(E_n, \mathbb{F}_p) \). \( \square \)

**Remark.** There is an alternative way of conducting some of the computations in this proof, relying on the following well-known fact: if \( G \) is a finite \( p \)-group and \( M \) is an \( \mathbb{F}_p G \)-module, then any \( m \in M \) satisfying \( m \cdot \mathcal{N} \neq 0 \) generates a free \( \mathbb{F}_p G \)-module of rank 1. (This is classic, and is for example Lemma 1.31 in [Gui18]). The contrapositive tells us that, in order to show that \( m \cdot \mathcal{N} = 0 \), it is enough to find some \( \lambda \in \mathbb{F}_p G \) with \( \lambda \neq 0 \) and \( m \cdot \lambda = 0 \). It was easy enough, in the proof, to obtain \( m \cdot \mathcal{N} = 0 \) on the nose in the cases considered, but it would have been easier yet to merely find such a \( \lambda \).

### 5. Back to the main theorem

For convenience, let us recall the statement of our main theorem, originally given in §1.3:

**Theorem (Main theorem).** Let \( k \) be a local field and let \( \Gamma = G_k(p) \) be the Galois group of a maximal pro-\( p \)-extension; we write \( n \) for the minimal number of generators of \( \Gamma \), so that \( \Gamma/\Phi(\Gamma) = E_n \) is elementary abelian of rank \( n \). Put \( J = \Phi(\Gamma)/\Phi^{(2)}(\Gamma) \).

Then \( J \), as an \( E_n \)-module, is of constant Jordan type. Moreover its stable Jordan type is

- [1] if \( k \) does not contain a primitive \( p \)th-root of unity,
- [1] if \( k \) contains a primitive \( p \)th-root of unity.

Moreover, we have the following possibilities for the cohomology of \( J \):

1. If \( k \) does not contain a primitive \( p \)th root of unity, then for all \( s \in \mathbb{Z} \):
   \[ \hat{H}^s(E_n, J) = \hat{H}^{s-2}(E_n, \mathbb{F}_p) \].

2. If \( \xi_p \in k \) and the residue field of \( k \) is of characteristic prime to \( p \), then \( n = 2 \) and for all \( s \in \mathbb{Z} \):
   \[ \hat{H}^s(E_2, J) = \hat{H}^s(E_2, \mathbb{F}_p) \oplus \hat{H}^s(E_2, \mathbb{F}_p) \].

3. If \( \xi_p \in k \) and the characteristic of the residue field of \( k \) is \( p \) then
   \[
   \begin{align*}
   \hat{H}^0(E_n, J) & \cong \mathbb{F}_p^{n-1+n(n-1)/2}, \\
   \hat{H}^1(E_n, J) & \cong \hat{H}^3(E_n, \mathbb{F}_p), \\
   \hat{H}^s(E_n, J) & \cong \hat{H}^{s+2}(E_n, \mathbb{F}_p) \oplus \hat{H}^{s-2}(E_n, \mathbb{F}_p) \quad \forall s \geq 2.
   \end{align*}
   \]

We have now provided a proof for most statements. As the arguments are somewhat spread across the paper, we shall here give a summary to guide the reader. After that, we indicate how to complete the proof in the remaining cases which are not covered by the preceding work.
5.1. **Summary.** Assume first that \( k \) does not contain a primitive \( p \)-th root of unity. Then, as recalled in §1.4, the group \( \Gamma \) is free. We have explained in §2.3 how the main theorem is proved in this case when \( p > 2 \).

Assume from now on that \( \xi_p \in k \). First suppose that the residue field of \( k \) has characteristic \( \neq p \). This case of the main theorem was dealt with early in §1.5 for every prime.

We have reached the most interesting case, when \( \xi_p \in k \) and the residue field of \( k \) has characteristic \( p \). Now, the main theorem is exactly a combination of Theorem A and Theorem B from the Introduction (given the translations performed in §11). What is more, Lemma 7 states that Theorem A follows from Theorem C, and more precisely that the existence of an exact sequence of the form

\[
(*) \quad 0 \longrightarrow \omega_3(F) \longrightarrow \omega(J) \longrightarrow \omega_{-1}(F) \longrightarrow 0
\]

is enough to establish Theorem A. Assuming that \( p > 2 \) and that \( \xi_{p^2} \in k \) (rather than just \( \xi_p \in k \)), we have constructed this sequence in Lemma 13 (where the sequence appears for some module \( \omega(J) \)) and Proposition 14 (which identifies \( \omega(J) \) as stably isomorphic to \( \Omega(J) \), as requested). Under the same hypotheses, we have computed the cohomology, ie proved Theorem B, in Theorem 19.

Thus it remains to investigate the following situations :

- the case when \( \xi_p \in k \) but \( \xi_{p^2} \notin k \), for \( p > 2 \),
- the case \( p = 2 \); note that this case does not split into subcases according as \( \xi_{p^2} \in k \) or not, although it does split in some other way.

5.2. **When \( \xi_{p^2} \) is not in \( k \).** Assume that \( \xi_p \in k \) but \( \xi_{p^2} \notin k \), for some \( p > 2 \) (still assuming that the residue field of \( k \) is of characteristic \( p \)). We indicate briefly how the arguments must be adapted, without going into details. The altered presentation for \( G_k(p) \) (see §1.4) leads to an altered presentation for \( J \), to wit:

\[
J \cong \langle \zeta_i, \eta_i \eta_j \mid \text{Rel}^3(h, z), \zeta_i + \eta_i \eta_2 + \ldots + \eta_{n-1} \eta_n = 0 \rangle,
\]

where \((h, z)\) runs over all \( C \)-index of weight 3. This is obtained by a straightforward modification of Lemma 12.

Likewise, the Heller shifts of \( J \) are now presented differently. Indeed, for \( \omega(J) \) we have now:

\[
\langle \eta_j \zeta_1, \eta_i \eta_j \eta_k, \Delta \mid \text{Rel}(h, z), \Delta N = \eta_1 \zeta_1 X_1^{p-2} N^1 + \sum \eta_i \zeta_2 \eta_i (N^{2i-1}) \rangle,
\]

where \((h, z)\) is a \( C \)-index of weight 4. The statement of Lemma 13 remains valid as such, so in particular we have the exact sequence \((*)\) also in this case. The general strategy in the proof of Proposition 14 stays the same, requiring only minor computational changes.

All the Heller shifts are subsequently affected. The definition of \( \omega_s(J) \) for \( s \geq 2 \) involves now the same set of generators, but the set of relations must be altered as follows:

1. The relation denoted \( \delta_{\text{Rel}^{-1}}(h_1 = 1, z_1 = \frac{z_1 + 2}{2}) \) becomes

\[
\delta_1^{\frac{z_1}{2}} X_1 = \zeta_1^{\frac{z_1}{2}} N^1 + \eta_2 \eta_1 \zeta_2^\frac{z_1}{2} N^1.
\]

2. The relation denoted \( \delta_{\text{Rel}^{-1}}(h = 0, z_1 = \frac{z_1 + 1}{2}) \) becomes

\[
\mu_1 \delta_1^{\frac{z_1}{2}} X_1^{p-1} = \eta_1 \zeta_1^{\frac{z_1}{2}} N^1 + \zeta_1^{\frac{z_1}{2}} \eta_2 N^1.
\]

Again, the statement of Lemma 15 is not affected, and the proof of Proposition 16 necessitates only straightforward adjustments.

Finally, the new assumptions do not affect the statement of Theorem 19, and its proof can be reproduced *mutatis mutandis.*
5.3. **When** \( p = 2 \). Finally, we assume that \( p = 2 \) and that the residue field of \( k \) has characteristic 2 (as we assume that \( k \) is of characteristic 0, it contains \(-1\)). As recalled in §1.4, the presentation of the corresponding Demuškin groups is as follows. If the number of generators is odd, it becomes

\[
\mathcal{D}_{f,n=2s+1} = \langle x_1, \ldots, x_{2s+1} | x_1^2 (x_2, x_3)(x_4, x_5) \ldots (x_{2s}, x_{2s+1}) = 1 \rangle.
\]

If the number of generators is however even, it becomes either

\[
\mathcal{D}_{f,n=2s} = \langle x_1, \ldots, x_{2s} | x_1^2 (x_2, x_3)(x_4, x_5) \ldots (x_{2s-1}, x_{2s}) = 1 \rangle,
\]

or

\[
\mathcal{D}_{f,n=2s} = \langle x_1, \ldots, x_{2s} | x_1^2 (x_2, x_3)(x_4, x_5) \ldots (x_{2s-1}, x_{2s}) = 1 \rangle.
\]

In each case \( f \) is an integer such that \( f \geq 2 \). Therefore, as our work is always done modulo \( \Phi^{(2)}(\mathcal{D}_{f,2s}) \) (resp. \( \Phi^{(2)}(\mathcal{D}_{f,2s}) \)), there is formally no difference between the \( p \) odd case with \( \zeta_2, \zeta_2 \in k \) and the case \( p = 2 \) with \( 2s \) generators.

If the number of generators is odd, the relation is slightly changed. The presentation by generators and relations of \( J \) is in fact

\[
J \cong \langle \zeta_1, \eta_1 \eta_2 | \text{Rel}^2(h, z), \zeta_1 + \eta_2 \eta_3 + \eta_4 \eta_5 + \ldots + \eta_{2n+1} \eta_{2n+1} = 0 \rangle.
\]

It is crucial to remark that in this case the presentation of \( \omega(J) \) becomes

\[
\langle \eta_1 \zeta_1, \eta_1 \eta_2 \eta_3, \eta_4, \Delta | \text{Rel}^2(h, z), \Delta N = \eta_1 \zeta_1 \tilde{N}_1^4 + \sum \eta_{2i+1} \zeta_{2i} \tilde{N}_1^{2i} \rangle.
\]

This modification leads to the following modifications just as before in the presentation for \( \omega_s(J) \) for \( s \geq 2 \):

1. The relation denoted \( \delta - \text{Rel}^n-1(h_1 = 1, z_1 = \frac{\tilde{z}-2}{2}) \) becomes

\[
\delta \frac{\tilde{z}-2}{2} X_1 = \zeta_1^{2+2} \tilde{N}_1^4.
\]

2. The relation denoted \( \delta - \text{Rel}^n-1(h = 0, z_1 = \frac{\tilde{z}-1}{2}) \) becomes

\[
\mu_1 \delta \frac{\tilde{z}-1}{2} X_1^{p-1} = \eta_1 \zeta_1^{2+1} \tilde{N}_1^4.
\]

The proofs are again very similar.

**Appendix A. Some invariants**

In [AGKM01], ADEM, GAO, KARAGUEUZIAN and MINÁČ closely studied \( J \) when \( p = 2 \) with different techniques, since they had other motivations; nevertheless some of their results still hold. We should not adapt here their theorems and proofs, but only compute some of the numerous invariants they introduced in their paper, when \( p \neq 2 \).

Those invariants are in fact related to the socle layers of a module. Here, we denote \( \text{Soc}(N) \) the socle of a module \( N \), which is in fact the sum of all irreducible sub-modules of \( N \). The socle layer is defined inductively for a module \( N \) by:

\[
\left\{
\begin{array}{ll}
\text{Soc}(N) = \{0\} \\
\text{Soc}^{n+1}(N)/\text{Soc}^n(N) = \text{Soc}(N/\text{Soc}^{n-1}(N))
\end{array}
\right.
\]

Recall that we have in this case

\[
\{0\} \subset \text{Soc}(N) \subset \text{Soc}^2(N) \subset \ldots \subset \text{Soc}^r(N) = N.
\]

The integer \( r \) is called the (socle)-length of \( N \), and we will write \( r = l(N) \). For further details see [Ben95] p. 3 sq. In the same fashion, we recall the notion of cohomological \( p \)-dimension. For any group \( p \)-group \( G \), we set

\[
cd_p(G) = \inf \{ n | H^i(G, F_p) = 0, \forall i \geq n \}.
\]

Note that such integer does not always exist; however as mentioned earlier for a Demuškin group \( \mathcal{D}_{k,n} \), we have by definition \( cd_p(\mathcal{D}_{k,n}) = 2 \).
In [AGKM01], the proposition 5.2 implies that for any local field \( k \), we have
\[
\ell(\Phi(G_k(2))/\Phi^2(G_k(2))) + \text{cd}_2(G_k(2)) = n + 1.
\]

Where \( G_k(2) \) denotes the Galois group of a maximal pro-2-extension of \( k \).

Yet such formula can be extended, with the help of our presentations. Let us suppose again that \( p \neq 2 \).

**Proposition 20.** If \( k \) is a local field, then the following identity hold
\[
\ell(\Phi(G_k(p))/\Phi^2(G_k(p))) + \text{cd}_p(G_k(p)) = (p - 1)n + 1.
\]

**Proof.** As previously recalled either \( G_k(p) \) is a Demuškin group, or it is a free pro-\( p \)-group.

Let us begin by the most simple case, i.e. when \( G_k(p) \) is a free pro-\( p \)-group. According to 2.2.4, it appears that the radical length -denoted \( l(M) \) for a module- verify
\[
l(\omega_2(F)) = (p - 1) \cdot n.
\]

Therefore, since \( \text{cd}_p(F_n) = 1 \) (see [Ser97]), the announced equality is true. The second case is a bit trickier, for the sake of clarity we should assume that \( \xi_{p^i} \in k \), so that the Demuškin relation is modulo \( \Phi^{(2)} \):
\[
\Delta: \eta_1 \eta_2 + \eta_3 \eta_4 + \ldots + \eta_{n-1} \eta_n = 0.
\]

In order to prove this precise equalities we should find a basis: a generating system of \( J \) is given by the image of the basis of \( M_n \) by the obvious surjection, which we will call \( \psi \). However as we previously remarked thanks to the Demuškin relation we can get rid of \( \eta_{n-1} \eta_n \) and in fact all the \( \psi(\eta_{n-1} \eta_n X^n) \) where the multi index verify the conditions given in 2.2.4 in order to be in the given basis of \( M_n \). Yet, it is not sufficient. So, let us look to \( \Delta X_n^{p-1} X_{n-1}^{p-1} \), which is
\[
\eta_1 \eta_n X_n^{p-2} X_{n-1} X_2 - \eta_2 \eta_n X_n^{p-2} X_{n-1} X_1 + \ldots + \eta_{n-3} \eta_n X_n^{p-2} X_{n-1} X_{n-2} - \eta_{n-2} \eta_n X_n^{p-2} X_{n-1} X_{n-3} = 0.
\]

Note that in order to obtained this equality, we first used the fact that
\[
\eta_{n-1} \eta_n X_n^{p-1} X_{n-1}^{p-1} = 0,
\]
and the Jacobi relation. Now, we can get rid of
\[
\eta_{n-3} \eta_n X_n^{p-2} X_{n-1} X_{n-2}.
\]

Iterating this process it appears that a basis of \( J(K)^* \) is obtained by excluding the vectors \( \eta_i \eta_{p^i} X^n \) of the basis from 2.2.4 verifying the following conditions

1. If \( i = n - 1 \) there is no condition.
2. If \( i \neq n - 1 \), the following conditions have to be verified:
   (a) \( \nu_n = p - 2 \)
   (b) if \( i \) is even
      (i) \( \nu_{i-1} \neq 0 \).
      (ii) \( \forall j \in \{n - 1, n - 2, \ldots, i\}, \nu_j = p - 1 \).
   (c) if \( i \) is odd
      (i) \( \nu_{i+1} \neq 0 \).
      (ii) \( \forall j \in \{n - 1, \ldots, i + 1\}, \nu_j = p - 1 \).

Using this fact it appears that in this case
\[
l(\Phi(G_k(p))/\Phi^2(G_k(p)) = (p - 1)n - 1.
\]

Therefore the relation is true. \( \square \)
Set $J^*$ for $\Phi(G_k(p))/\Phi^2(G_k(p))$, no matter in which case we are. The other invariant introduced in [AGKM01] was in fact the dimension of $\text{Soc}^2(J)/\text{Soc}^1(J)$. (Note the disappearance of the asterisk!) However we have the following very classical isomorphism

$$\text{Soc}^2(N^*)/\text{Soc}^1(N^*) = (\text{Rad}(N)/\text{Rad}^2(N))^*.$$ 

Now, note that if we are in the case where $G_k(p)$ is a free pro-$p$-group, then according to the same proposition 2.2.4, a basis of the elements of $\text{Rad}(\omega_2(F))/\text{Rad}^2(\omega_2(F))$ is given by the following system of vectors

1. elements of the form $\eta_i\eta_jX_k$ where $k \leq j$,
2. elements of the form $\zeta_i \cdot X_j$ (which are $\eta_i\eta_jX_i^{p-1}$ or $-\eta_j\eta_iX_i^{p-1}$).

Therefore a simple computation shows us that

$$\dim_{F_p} \text{Soc}^2((\omega_2(F))/\text{Soc}^1(\omega_2(F)))^* = \frac{n(n-1)(n+4)}{3}.$$ 

What concerns the Demuškin group, we have to subtract from the previous basis according to the Demuškin relation (and the basis previously given) the elements of the form $\eta_{n-1}\eta_nX_j$ for any $j \in \{1, \ldots, n\}$, and the elements $\eta_{n-1}\eta_nX_{n-1}^{p-1}$ and $\eta_{n-1}\eta_nX_{n-1}$, so that we obtain

$$\dim_{F_p} \text{Soc}^2(J)/\text{Soc}(J) = \frac{(n-2)(n^2+5n+3)}{3}.$$ 

Note that in the last formula, when we set $n = 2$, we find that the dimension is $0$, which is not a great surprise, since when $n = 2$, $J$ is in fact isomorphic to $F_p \times F_p$.

References

[AGKM01] Alejandro Adem, Wenfeng Gao, Dikran B. Karagueuzian, and Jan Mináč. Field theory and the cohomology of some galois groups. *Journal of Algebra*, 235:608–635, 2001.

[Ben95] David Benson. Representation and cohomology, volume I. Cambridge University Press, 1995.

[Ben17] David J. Benson. Representations of elementary abelian $p$-groups and vector bundles. Cambridge University Press, 2017.

[BLMS07] Dave Benson, Nicole Lemire, Jan Minac, and John Swallow. Detecting pro-$p$-groups that are not absolute galois groups. *Journal für die reine und angewandte Mathematik*, 614:191–234, 2008.

[CFP08] Jon Carlson, Eric Friedlander, and Julia Pevtsova. Modules of constant jordan type. *Journal für die reine und angewandte Mathematik*, 614:191–234, 2008.

[CM08] Sunil K. Chebolu and Jan Minac. Auslander-reiten sequences as appetizers for homotopists and arithemeticians. On ArXiv, 2008.

[CTVEZ03] Jon F. Carlson, Lisa Townsley, Luis Valeri-Elizondo, and Mucheng Zhang. Cohomology Rings of Finite Groups. Kluwer Academics, 2003.

[DSMS99] J.D. Dixon, M.P.F. Du Sautoy, A. Mann, and D. Segal. *Analytical pro-p-groups*. Cambridge University Press, 1999.

[Fox53] Ralph Fox. Free differential calculus. i: Derivation in the free group ring. *Annals of Mathematics*, 57:547–560, 1953.

[Fri95] Michael Fried. Introduction to modular towers, 1995.

[Gui18] Pierre Guillot. A gentle course in Local Class Field Theory. Cambridge University Press, 2018.

[Koc02] Helmut Koch. *Galois Theory of $p$-Extensions*. Springer Verlag, 2002.

[Lab67] John Labute. Classification of demushkin groups. *Canadian Journal of Mathematics*, 19:106–132, 1967.

[Laz54] Michel Lazard. Sur les groupes nilpotents et les anneaux de lie. *Annales scientifiques de l’E.N.S.*, 71, 1954.

[MS03] Jan Minác and John Swallow. Construction and classification of some galois module structures. Sur ArXiv, Mai 2003.

[Ser97] Jean-Pierre Serre. *Cohomologie Galoisienne*. Springer Verlag, 1997.

Alexandre Eimer, Université de Strasbourg & CNRS, Institut de Recherche Mathématique Avancée, UMR 7501, F-67000 Strasbourg, France

E-mail address: eimer@math.unistra.fr