New York Journal of Mathematics

New York J. Math. **30** (2024) 1177–1195.

Cohomology and the combinatorics of words for Magnus formations

Ido Efrat

ABSTRACT. For a prime number p and a free pro-p group G on a totally ordered basis X, we consider closed normal subgroups G^Φ of G which are generated by p-powers of iterated commutators associated with Lyndon words in the alphabet X. We express the profinite cohomology group $H^2(G/G^\Phi)$ combinatorically, in terms of the shuffle algebra on X. This partly extends existing results for the lower p-central and p-Zassenhaus filtrations of G.

CONTENTS

1. Introduction

The aim of this paper is to give a general connection between the cohomology of pro-p groups and the combinatorics of words. Here p is a fixed prime number, and we consider a free pro-p group G on a basis X. We further consider filtrations $G^\Phi = G^{\Phi(n)}$, $n = 1, 2, \dots$, of G by closed normal subgroups given in terms of powers of standard Lie generators with respect to X. The cohomology groups we study are $H^l(G/G^\Phi) = H^l(G/G^\Phi, \mathbb{Z}/p)$, $l = 1, 2$, with the trivial action on $\mathbb{Z}/p$. It is well known that the first cohomology group of a pro-p

Received February 12, 2024.

2010 *Mathematics Subject Classification.* Primary 12G05, Secondary 20J06, 68R15.

Key words and phrases. Profinite cohomology, combinatorics of words, Magnus formations, shuffle algebra, Lyndon words, shuffle relations, Massey products, lower p-central filtration, p-Zassenhaus filtration.

This work was supported by the Israel Science Foundation (grant No. 569/21).

ISSN 1076-9803/2024

group describes its generator structure, whereas the (much deeper) second cohomology group captures its relation structure [NSW08, Ch. III, §9]. We prove a general isomorphism theorem describing these lower cohomology groups in terms of Lyndon words and the shuffle algebra on X.

This isomorphism was proved in our earlier works [Ef17], [Ef20], and [Ef23] for the lower p-central filtration and the p-Zassenhaus filtration, which are special cases of the filtrations considered here. In fact, for $n = 2$ and the lower p-central filtration, the isomorphism was implicitly proved by Labute in his seminal work [L67] on the structure of pro-p Demuškin groups (following Serre [Se63]), and it serves as a major tool in the cohomology theory of pro-p groups; see e.g., [NSW08, Ch. III, §9].

More specifically, on the pro-p group side, we study a category of *pro-p Magnus formations* $\Phi = (\Lambda\colon G \to \mathbb{Z}_p\langle\langle X\rangle\rangle^{\times,1}, \tau, e)$ – to be described in more detail below – which is modeled after the Magnus representation of free groups ([Ma35], [Se02, Ch. I, §1.5], [L54, Ch. I, §4]). To any such formation we associate a closed normal subgroup G^Φ of G.

On the combinatorial side, we consider X also as an alphabet with a fixed total order. Let X^* be the set of words in X. The *shuffle algebra on X* is the free $\mathbb{Z}$-module on X^* with the *shuffle product* $\sqcup\!\sqcup$ (see §3). Dividing it by the submodule generated by all shuffle products $u \sqcup\!\sqcup v$ of nonempty words u, v, we obtain the *indecomposable quotient* $\mathrm{Sh}(X)_{\mathrm{indec}}$ of the shuffle algebra. It is this graded module which lies at the center of our combinatorial description of the cohomology. Namely, for a certain set I of positive integers associated with Φ, defined below, we prove:

Main Theorem. *For p sufficiently large, there is a canonical isomorphism*

$$\Big(\bigoplus_{s\in I} \mathrm{Sh}(X)_{\mathrm{indec},s}\Big) \otimes (\mathbb{Z}/p) \cong H^2(G/G^\Phi).$$

See Theorem 8.2.

As mentioned above, the isomorphism of the Main Theorem was earlier proved in some important cases:

(1) Labute [L67] proves this isomorphism when $G^\Phi = G^p[G,G]$ and $I = \{1,2\}$. Namely, the cosets of the words (x), $x \in X$, and (xy), where $x, y \in X$ and $x < y$, form a linear basis of the left-hand side of the isomorphism. Let φ_x, $x \in X$, be the basis of $H^1(G/G^\Phi)$ which is dual to X. Then, for p odd, the Bockstein elements $\mathrm{Bock}(\varphi_x)$ (see Example 8.4) and the cup products $\varphi_x \cup \varphi_y$, $x < y$, form a linear basis of $H^2(G/G^\Phi)$, giving the desired isomorphism.

(2) This was extended in [Ef17] and [Ef20] to the *lower p-central filtration* $G^{(n,p)}$, $n = 1, 2, \ldots$, of G. Recall that these closed subgroups of G are defined inductively by

$$G^{(1,p)} = G, \quad G^{(n+1,p)} = (G^{(n,p)})^p[G, G^{(n,p)}], \quad n \geq 1.$$

By constructing an appropriate linear basis of $H^2(G/G^{(n,p)})$, it was shown that the Main Theorem holds for $G^\Phi = G^{(n,p)}$, $n < p$, and $I = \{1, 2, \dots, n\}$. When $n = 2$ this recovers Labute's result.

(3) Let $G_{(n,p)}$, $n = 1, 2, \dots$, be the *p-Zassenhaus filtration* of G (also called the *modular dimension filtration* [DDSMS99, Ch. 11]; See in addition [MPQT21], [MPQT22]). Thus

$$G_{(1,p)} = G, \quad G_{(n,p)} = (G_{(\lceil n/p\rceil,p)})^p \prod_{k+l=n} [G_{(k,p)}, G_{(l,p)}], \quad n \geq 2.$$

In [Ef23] we prove the Main Theorem when $G^\Phi = G_{(n,p)}$, $n < p$, and $I = \{1, n\}$.

Moreover, the terms $G^{(n,p)}$ (resp., $G_{(n,p)}$) have canonical "approximate" generators given by *Lyndon words*. Recall that these are the nonempty words w in X^* which are smaller in the alphabetical order than all their proper suffixes. For each such word w, one associated its *Lie element* τ_w, which is an iterated commutator in the free pro-p group G (see Example 4.3). Then one has:

(i) The powers $\tau_w^{p^{n-i}}$, where w is a Lyndon word of length $1 \leq i \leq n$, generate $G^{(n,p)}$ modulo $G^{(n+1,p)}$ [Ef17, Th. 5.3].

(ii) When $n \geq p$, the powers $\tau_{(x)}^q = x^q$, where $x \in X$ and q is the smallest p-power $\geq n$, together with the Lie elements τ_w, where w is a Lyndon word of length n, generate $G_{(n,p)}$ modulo $(G_{(n,p)})^p[G, G_{(n,p)}]$ [Ef23, Th. 4.6].

Such approximations seem unavailable in more general cases, and instead, we simply work with subgroups G^Φ generated by p-powers of the τ_w. Thus we take an integer $n \geq 2$ and a map $j\colon \{1, 2, \dots, n\} \to \mathbb{Z}_{\geq 0}$. Set

$$I = \left\{1 \leq i \leq n \;\middle|\; ip^{j(i)} \leq i' p^{j(i')} \text{ for every } 1 \leq i' \leq i\right\}.$$

Let L consist of all Lyndon words in X^* with lengths in I, and let $\tau\colon L \to G$ be the map $w \mapsto \tau_w$. Then the *Magnus formation* Φ considered above is the triple (Λ, τ, e), where $\Lambda\colon G \to \mathbb{Z}_p\langle\langle X\rangle\rangle^{\times,1}$ is a continuous homomorphism into the group of 1-units in $\mathbb{Z}_p$, and $e(i) = p^{j(i)}$. We define G^Φ to be the closed subgroup of G generated by all powers $\tau_w^{e(i)}$, $w \in L$; See §4 for the definition of general Magnus formations. This indeed contains (i) and (ii) as special cases (Examples 8.6 and 8.7).

The idea of the proof of the Main Theorem theorem is to construct natural bases for both its sides: First, using results of Radford [Ra79] and, independently, Perrin and Viennot, we show that the cosets of the Lyndon words w with lengths in I form a linear basis of the left-hand side. Further, to each such word w we associate a cohomology element $\bar\rho_w^*(\alpha_w)$ in $H^2(G/G^\Phi)$. Using a "triangularity" property of Lyndon words (Definition 4.2(vi)), we show that these elements form a linear basis of $H^2(G/G^\Phi)$, which we call the *Lyndon basis*. Associating these bases one with each other yields the desired isomorphism.

The basis elements $\bar\rho_w^*(\alpha_w)$ belong to an intriguing set of cohomology elements in $H^2(G/G^\Phi)$, called the *unitriangular spectrum*. We recall from [Ef17] that these elements are defined as follows: Let $\mathbb{U}_i$ be the group of all unipotent and upper-triangular $(i+1)\times(i+1)$-matrices over $\mathbb{Z}/p^{j(i)+1}$, and let $\overline{\mathbb{U}}_i$ be its quotient by $\mathbb{Z}/p$ as naturally embedded in its center. The natural central extension $0 \to \mathbb{Z}/p \to \mathbb{U}_i \to \overline{\mathbb{U}}_i \to 1$ has a classifying cohomology element $\alpha_i \in H^2(\overline{\mathbb{U}}_i)$. For every continuous homomorphism $\bar\rho : G \to \overline{\mathbb{U}}_i$ one has the pullback $\bar\rho^*(\alpha_i)$ in $H^2(G)$. In particular, every word w of length i gives rise to a *Magnus representation* $\rho_w : G \to \mathbb{U}_i$ (§4), which induces a continuous homomorphism $\bar\rho_w : G/G^\Phi \to \overline{\mathbb{U}}_i$. For w Lyndon of length $i \in I$, we obtain the basis element $\bar\rho_w^*(\alpha_i)$.

In its extreme ends, the unitriangular spectrum contains Bockstein elements (for $i = 1$) and Massey product elements (when $j(i) = 0$) – see Examples 8.4 and 8.5. Bockstein elements are fairly well understood, whereas Massey product elements were extensively studied in recent years in Galois-theoretic situations (see e.g., [EfMa17], [GMT18], [HaW19], [HoW15], [LLSWW23], [MS23a], [MS23b], [MT16], as well as the references therein), and for number fields from the arithmetical topology perspective (e.g., in [Mo12], [Vo05], [KMT17]). However, the behavior of the inner elements of the spectrum in such situations is still not well understood, and we hope that the connections investigated in this paper will be applicable also in these other contexts.

I thank Darij Grinberg and the referee for helpful comments on previous versions of this paper.

2. Binomial maps

For the rest of the paper, we fix an integer $n \geq 2$. Let $e : \{1,2,\dots,n\} \to \mathbb{Z}_{\geq 1}$ be a map.

Definition 2.1. The map e is *binomial* if for all positive integers i, i', l such that $i'l \leq i \leq n$ and $1 \leq l \leq e(i')$ one has $e(i) | \binom{e(i')}{l}$.

The following lemma shows that this definition of binomial maps coincides with the one given at [CE16, Def. 3.6]:

Lemma 2.2. *The map e is binomial if and only if the following two conditions hold:*

(a) *For all positive integers i', l such that $i'l \leq n$ and $1 \leq l \leq e(i')$ one has $e(i'l) | \binom{e(i')}{l}$; and*

(b) *For every $1 \leq i' \leq i \leq n$ one has $e(i) | e(i')$.*

Proof. If e is binomial, then (a) and (b) hold by taking $i = i'l$ and $l = 1$, respectively. The inverse implication is immediate. □

We let I_e be the set of all $1 \leq i \leq n$ such that for every $1 \leq i' \leq i$ one has

$$i'e(i') \geq ie(i). \tag{2.1}$$

In particular, $1 \in I_e$.

Example 2.3. Let $a_1, \dots, a_{n-1}$ be positive integers. For $1 \le i \le n$ we set

$$e(i) = \gcd\Big\{\prod_{k\in K} a_k \;\Big|\; K \subseteq \{1, 2, \dots, n-1\},\ |K| = n-i\Big\}$$

(thus $e(n) = 1$). By [CE16, Examples 3.3, 3.8], e is binomial.

Now consider the special case where $a_k = p^{r_k}$ with p a prime number and $1 \le r_1 \le \cdots \le r_{n-1}$. Then $e(i) = p^{j(i)}$ with $j(i) = \sum_{k=1}^{n-i} r_k$. Since the map $x - \log_p x$ is increasing in $[1, \infty)$, for $1 \le i' \le i$ one has

$$\log_p(i/i') \le i - i' \le \sum_{k=n-i+1}^{n-i'} r_k = j(i') - j(i),$$

and (2.1) holds. Therefore $I_e = \{1, 2, \dots, n\}$ in this case.

In particular, when $a_k = \cdots = a_{n-1} = p$ we have $e(i) = p^{n-i}$.

Example 2.4. Let p be a prime number and let t be a positive integer. We set $j(i) = t\lceil \log_p(n/i)\rceil$ and $e(i) = p^{j(i)}$ for $1 \le i \le n$. Then j is weakly decreasing, so (b) of Lemma 2.2 holds. By [CE16, Example 3.9], e is binomial. Also note that $j(1) \ge t$, so $e(1) > 1$.

The set I_e is given by the following proposition. In the special case $t = 1$ it was proved in [Ef23, Lemma 4.1], and the proof in the general case is obtained by minor adjustments.

Proposition 2.5. *In the situation of Example 2.4, I_e consists of the integers $i_k = \lceil n/p^k\rceil$, where $k \ge 0$.*

Proof. The sequence i_k is weakly decreasing to 1. We may restrict ourselves to k such that $p^k \le n$. Then $(n/p^k)+1 \le n/p^{k-1}$, so $n/p^k \le i_k < n/p^{k-1}$. Hence $j(i_k) = tk$.

Since $n/p^k \le \lceil n/p^{k+1}\rceil p^t$, one has $i_k p^{tk} \le i_{k+1} p^{t(k+1)}$, i.e., the sequence $i_k p^{j_n(i_k)} = i_k p^{tk}$ is weakly increasing in the above range.

We also observe that if $i < i_{k-1}$, then $i < n/p^{k-1}$, i.e., $j(i) \ge tk$.

We now show that every $i \in I_e$ has the form i_k for some k. Since $n = i_0$, we may assume that $i < n$. Hence there is k in the above range such that $i_k \le i < i_{k-1}$. By the previous observation, $j(i) \ge tk$. Taking $i' = i_k$ in (2.1), we obtain that

$$i_k p^{j(i_k)} \ge i p^{j(i)} \ge i_k p^{tk} = i_k p^{j(i_k)}.$$

Hence $i = i_k$.

Conversely, we show that each i_k is in I_e. Take $1 \le i' < i_k$. There exists l in the above range such that $i_l \le i' < i_{l-1}$. Necessarily $l > k$, so $i_l p^{tl} \ge i_k p^{tk}$. As we have observed, $j(i') \ge tl$. Hence

$$i' p^{j(i')} \ge i_l p^{tl} \ge i_k p^{tk} = i_k p^{j(i_k)}. \qquad \square$$

3. Words

We refer to [Re93], [Lo83], and [GR20] as general sources on the combinatorics of words.

We fix a nonempty totally ordered set $(X, \leq)$, considered as an alphabet. Let X^* be the free unital monoid on X with the concatenation product. Its elements are considered as (associative) words in X, and the unit element 1 of X^* is the empty word. We write $|w|$ for the length of the word w. Let $\leq_{\mathrm{alp}}$ be the alphabetical (lexicographic) total order on X^*. The *length-alphabetical* total order $\preceq$ on X^* is defined by $w_1 \preceq w_2$ if and only if $|w_1| < |w_2|$, or both $|w_1| = |w_2|$ and $w_1 \leq_{\mathrm{alp}} w_2$.

A nonempty word $w \in X^*$ is called a *Lyndon word* if it is smaller in $\leq_{\mathrm{alp}}$ than all its proper right factors (i.e., suffixes). See [De10, §2.1] for an equivalent definition.

Every Lyndon word w of length ≥ 2 has a *standard factorization* as a concatenation $w = uv$ of Lyndon words u, v. Namely, v is the $\leq_{\mathrm{alp}}$-minimal nontrivial right factor of w which is a Lyndon word; equivalently, v is the longest nontrivial right factor of w which is a Lyndon word [Ef23, Lemm 2.2]. The set of all Lyndon words in X^* is a Hall set [Re93, Th. 5.1], and the above factorization coincides with the general notion of a standard factorization in Hall sets [Re93, §4.1].

Consider a unital commutative ring R. Let $R\langle\langle X\rangle\rangle$ denote the R-module of formal power series f with coefficients in R and over the set X of non-commuting variables. Thus $f = \sum_{w\in X^*} f_w w$ with $f_w \in R$. The concatenation induces on $R\langle\langle X\rangle\rangle$ via linearity the structure of an R-algebra. Let $R\langle X\rangle$ be the subalgebra of $R\langle\langle X\rangle\rangle$ consisting of all noncommutative polynomials in X, that is, all such power series f whose support

$$\mathrm{Supp}(f) = \{w \in X^* \mid f_w \neq 0\}$$

is finite. We identify a word $w \in X^*$ as a monomial in $R\langle X\rangle$.

For $f = \sum_{w\in X^*} f_w w \in R\langle\langle X\rangle\rangle$ and $g = \sum_{w\in X^*} g_w w \in R\langle X\rangle$ we define the *scalar product*

$$(f, g)_R = \sum_{w\in X^*} f_w g_w. \tag{3.1}$$

It is R-bilinear, and $(f, w)_R = f_w$ and $(w, g)_R = g_w$ for every w.

Next let $\star\colon X^* \times X^* \to R\langle X\rangle$ be a binary map such that the module $R\langle X\rangle$ is a unital associative R-algebra with respect to the induced R-bilinear map

$$\star\colon R\langle X\rangle \times R\langle X\rangle \to R\langle X\rangle,\ \ \Big(\sum_u f_u u\Big) \star \Big(\sum_v g_v v\Big) = \sum_{u,v} f_u g_v (u \star v),$$

and the unit element $1 \in X^*$. We further assume that for nonempty $u, v \in X^*$ the support $\mathrm{Supp}(u \star v)$ consists only of words w of length $1 \leq |w| \leq |u| + |v|$. We say that $f \in R\langle\langle X\rangle\rangle$ is *compatible with* $\star$ if for every nonempty words $u, v \in X^*$ one has

$$(f, u)_R \cdot (f, v)_R = (f, u \star v)_R. \tag{3.2}$$

The proof of the following fact is straightforward. Here $(u \star v)_s$ denotes the homogeneous part of degree s of $u \star v$.

Lemma 3.1. *Suppose that $f \in R\langle\langle X\rangle\rangle$ is compatible with $\star$, and let N be an ideal in R. Let u, v be nonempty words in X^* with $s = |u| + |v|$. If $(f, w)_R \in N$ for every nonempty $w \in X^*$ with $|w| < s$, then $(f, (u \star v)_s)_R \in N$.*

We will be especially interested in the *shuffle product* $u ш v$ and *infiltration product* $u \downarrow v$ of words $u, v \in X^*$ defined as follows (see [CFL58], [Re93, pp. 134–135]): Write $u = (x_1 \cdots x_r)$, $v = (x_{r+1} \cdots x_{r+t}) \in X^*$. Then

$$u ш v = \sum_\sigma (x_{\sigma^{-1}(1)} \cdots x_{\sigma^{-1}(r+t)}) \in R\langle X\rangle,$$

where σ ranges over all permutations of $1, 2, \dots, r+t$ such that $\sigma(1) < \cdots < \sigma(r)$ and $\sigma(r+1) < \cdots < \sigma(r+t)$.

Similarly, consider all surjective maps $\sigma : \{1, 2, \dots, r+t\} \to \{1, 2, \dots, k(\sigma)\}$, with $1 \le k(\sigma) \le r+t$, $\sigma(1) < \cdots < \sigma(r)$ and $\sigma(r+1) < \cdots < \sigma(r+t)$, and which satisfy the following weak form of injectivity: If $\sigma(i) = \sigma(j)$, then $x_i = x_j$. Then we set

$$u \downarrow v = \sum_\sigma (x_{\sigma^{-1}(1)} \cdots x_{\sigma^{-1}(k(\sigma))}) \in R\langle X\rangle. \tag{3.3}$$

By our assumption, $x_{\sigma^{-1}(i)}$ does not depend on the choice of the preimage $\sigma^{-1}(i)$. Thus $u ш v$ is the part of $u \downarrow v$ of degree $r+t$, that is, the partial sum corresponding to all such maps σ which are bijective.

For instance,

$$(xy) ш (x) = (xyx) + 2(xxy), \quad (xy) \downarrow (x) = (xyx) + 2(xxy) + (xy),$$
$$(xy) ш (xz) = (xyxz) + 2(xxyz) + 2(xxzy) + (xzxy),$$
$$(xy) \downarrow (xz) = (xyxz) + 2(xxyz) + 2(xxzy) + (xzxy) + (xyz) + (xzy).$$

The maps $R\langle X\rangle \times R\langle X\rangle \to R\langle X\rangle$ induced by ш and $\downarrow$ as above are commutative and associative [Lo83, p. 128, Prop. 6.3.15], and the assumption about $\mathrm{Supp}(u \star v)$ is clearly satisfied.

4. Magnus formations

The discussion in this section can be carried out both in the context of discrete groups and rings, as well as profinite groups and rings. Since we are motivated by profinite applications, and the discrete setting is easily obtained from the profinite one by obvious amendments, we carry the discussion in the latter setting.

Let R be a profinite commutative ring with unit 1_R. We equip $R\langle\langle X\rangle\rangle$ with the minimal topology for which the maps $(\cdot, w)_R : R\langle\langle X\rangle\rangle \to R$ are continuous for every $w \in X^*$. Then $R\langle\langle X\rangle\rangle$ is also a profinite ring, and both its subgroup $R\langle\langle X\rangle\rangle^\times$ of invertible elements and its subgroup $R\langle\langle X\rangle\rangle^{\times,1}$ of invertible elements f with $(f, 1)_R = 1_R$ are profinite groups [Ef14, §5].

Let G be a profinite group, and consider a continuous map

$$\Lambda\colon G \to R\langle\langle X\rangle\rangle^{\times,1}, \quad \Lambda(\sigma) = \sum_{w\in X^*} \epsilon_w(\sigma)w.$$

The maps $\epsilon_w\colon G \to R$, $\epsilon(\sigma) = (\Lambda(\sigma), w)_R$, are then continuous.

Let $\mathbb{U}_i(R)$ be the group of all $(i+1)\times(i+1)$-matrices over R which are *unitriangular*, i.e., unipotent and upper-triangular. It is a profinite group with respect to the natural (product) topology induced from R. For a word $w = (a_1a_2\cdots a_i) \in X^*$ of length i we define a map

$$\rho_{w,R}\colon G \to \mathbb{U}_i(R), \quad \rho_{w,R}(\sigma)_{kl} = \epsilon_{(a_k a_{k+1}\cdots a_{l-1})}(\sigma)$$

for $1 \le k \le l \le i+1$. It is continuous, and we call it the *Magnus representation* of G over R associated with w.

Proposition 4.1. *The following conditions are equivalent:*

(a) Λ *is a group homomorphism;*

(b) *For every $w \in X^*$ and $\sigma_1, \sigma_2 \in G$ one has*

$$\epsilon_w(\sigma_1\sigma_2) = \sum_{u,v\in X^*,\ w=uv} \epsilon_u(\sigma_1)\epsilon_v(\sigma_2),$$

where the summation is over all decompositions of w as a concatenation $w = uv$.

(c) *For every $w \in X^*$ the map $\rho_{w,R}$ is a group homomorphism.*

Proof. The implications (a)⇔(b)⇒(c) are straightforward. For (c)⇒(b) we look at the $(1, i+1)$-entry of $\rho_{w,R}$. □

Given $w \in X^*$, we write $o(w)$ for a general element of $R\langle\langle X\rangle\rangle$ whose support consists of words strictly larger than w with respect to the length-alphabetical order $\preceq$ (see §3), and composed of letters appearing in w.

The *lower central series* $G^{(i)}$, $i = 1, 2, \ldots$, of G is defined inductively by $G^{(1)} = G$ and $G^{(i+1)} = [G, G^{(i)}]$ (in the profinite sense). We recall that $n \ge 2$ is a fixed integer as in §2.

Definition 4.2. A (profinite) *Magnus formation* over R is a triple

$$\Phi = \big(\Lambda\colon G \to R\langle\langle X\rangle\rangle^{\times,1}, \tau\colon L \to G, e\colon \{1, 2, \ldots, n\} \to \mathbb{Z}_{\ge 1}\big),$$

such that:

(i) G is a profinite group;
(ii) Λ is a continuous group homomorphism;
(iii) L is a nonempty subset of X^*;
(iv) The words in L have lengths in $\{1, 2, \ldots, n\}$;
(v) τ is a map such that $\tau(w) \in G^{(i)}$ for every $w \in L$ of length i;
(vi) For every $w \in L$ one has $\Lambda(\tau(w)) = 1 + w + o(w)$ (*triangularity*);
(vii) The map e is binomial and is not identically 1.

Consider Magnus formations

$$\Phi_l = (\Lambda_l : G_l \to R\langle\langle X\rangle\rangle^{\times,1}, \tau_l : L_l \to G_l, e), \quad l = 1, 2,$$

over R, where $L_1 \subseteq L_2$. A *morphism* $\Phi_1 \to \Phi_2$ is a continuous group homomorphism $\gamma : G_1 \to G_2$ such that $\Lambda_1 = \Lambda_2 \circ \gamma$ and $\tau_2|_{L_1} = \gamma \circ \tau_1$.

Let $\star : X^* \times X^* \to R\langle X\rangle$ be a binary map as in §3. We say that the Magnus formation $\Phi = (\Lambda, \tau, e)$ is *compatible with* $\star$ if for every $\sigma \in G$ the series $\Lambda(\sigma)$ is compatible with $\star$, in the sense of §3.

We note that if $\gamma : \Phi_1 \to \Phi_2$ is a morphism of Magnus formations as above, and if Φ_2 is compatible with $\star$, then Φ_1 is also compatible with $\star$. The converse holds if $\gamma : G_1 \to G_2$ is surjective.

Example 4.3. Let p be a prime number, let G be the free pro-p group on the alphabet X as a basis [FJ23, §20.4], and take $R = \mathbb{Z}_p$. The *pro-p Magnus homomorphism* $\Lambda_{\mathbb{Z}_p} : G \to \mathbb{Z}_p\langle\langle X\rangle\rangle^{\times,1}$ is defined on the free generators $x \in X$ of G by $\Lambda_{\mathbb{Z}_p}(x) = 1 + x$ (note that $(1 + x)\sum_{k\geq 0}(-1)^k x^k = 1$, so indeed $1 + x \in \mathbb{Z}_p\langle\langle X\rangle\rangle^{\times,1}$).

For a Lyndon word w in X^* one defines its *Lie element* τ_w in G by induction on $|w|$ as follows: When $w = (x)$ has length 1, set $\tau_{(x)} = x$. Otherwise let $w = uv$ be the standard factorization of w (see §3), and set $\tau_w = [\tau_u, \tau_v]$.

Let $e : \{1, 2, \dots, n\} \to \mathbb{Z}_{\geq 1}$ be any binomial map which is not identically 1, and let L be a nonempty set of Lyndon words in X^* of lengths $\leq n$. We set $\tau : L \to S$ to be the map $w \mapsto \tau_w$. Then (v) holds by [Re93, Cor. 6.16], and (vi) holds by [Ef17, Prop. 4.4(c)]. Consequently, $(\Lambda_{\mathbb{Z}_p}, \tau, e)$ is a Magnus formation over $\mathbb{Z}_p$.

Moreover, this formation is compatible with the infiltration product $\downarrow$: Indeed, this was shown by Chen, Fox, and Lyndon in the discrete case for $R = \mathbb{Z}$ [CFL58, Th. 3.6], and the case $R = \mathbb{Z}_p$ follows (see also [Mo12, Prop. 8.6], [Re93, Proof of Th. 6.4], [Vo05, Prop. 2.25]).

5. The fundamental matrix

We consider a Magnus formation

$$\Phi = (\Lambda : G \to R\langle\langle X\rangle\rangle^{\times,1}, \tau : L \to G, e : \{1, 2, \dots, n\} \to \mathbb{Z}_{\geq 1})$$

over the profinite ring R. For $w \in L$ of length i let

$$\sigma_w = \tau(w)^{e(i)}.$$

Proposition 5.1. *Let $w \in X^*$ and $w' \in L$ have lengths i, i', respectively.*

(a) *If $1 \neq w < w'$, then $\epsilon_w(\sigma_{w'}) = 0$;*
(b) *If $w = w'$, then $\epsilon_w(\sigma_{w'}) = e(i)1_R$;*
(c) *If $1 \leq i \leq n$, then $\epsilon_w(\sigma_{w'}) \in e(i)R$;*
(d) *If w has letters not appearing in w', then $\epsilon_w(\sigma_{w'}) = 0$.*

Proof. By the triangularity property (Definition 4.2(vi)) and the binomial expansion formula,

$$\Lambda(\sigma_{w'}) = \Lambda(\tau(w'))^{e(i')} = (1 + w' + o(w'))^{e(i')} = 1 + e(i')w' + o(w').$$

This gives (a) and (b). Moreover,

$$\Lambda(\sigma_{w'}) = \Lambda(\tau(w'))^{e(i')} \in \Big(1 + \sum_{|u|\geq i'} Ru\Big)^{e(i')} \subseteq 1 + \sum_{1\leq l\leq e(i'),\, i'l\leq |v|} \binom{e(i')}{l} Rv.$$

If l satisfies $1 \leq l \leq e(i')$ and $i'l \leq i$, then the binomiality of e implies that $e(i) | \binom{e(i')}{l}$. Taking in the right sum $v = w$, we deduce (c).

Moreover, in the sums above we may restrict to words u, v whose letters appear in w'. This shows (d). □

Now fix an integer $m \geq 2$ such that for every positive integer e one has $\mathbb{Z}/m\mathbb{Z} \cong eR/meR$ via the group homomorphism $k \mapsto ke1_R$. In the applications, we will take $m = p$ prime and $R = \mathbb{Z}_p$, and this condition clearly holds.

For $1 \leq i \leq n$ let $\pi_i : R \to R/me(i)R$ be the natural epimorphism. For $w \in X^*$ and $w' \in L$ of lengths $1 \leq i, i' \leq n$, respectively, we set

$$\langle w, w' \rangle = \pi_i(\epsilon_w(\sigma_{w'})).$$

By Proposition 5.1(c), $\langle w, w' \rangle \in e(i)R/me(i)R$. Under the identification $\mathbb{Z}/m \cong e(i)R/me(i)R$, we may consider $\langle w, w' \rangle$ as an element of $\mathbb{Z}/m$.

We call the transposed (possibly infinite) matrix

$$\Big[\langle w, w' \rangle\Big]^T_{w,w'\in L},$$

where L is totally ordered by $\preceq$, the *fundamental matrix* of the Magnus formation Φ. From Proposition 5.1(a)(b) we deduce:

Corollary 5.2. *The fundamental matrix of a Magnus formation is unitriangular.*

Remark 5.3. This construction is functorial in the following sense: Consider Magnus formations

$$\Phi_l = (\Lambda_l : G_l \to R\langle\langle X\rangle\rangle^{\times,1}, \tau_l : L_l \to G_l, e : \{1, 2, \dots, n\} \to \mathbb{Z}_{\geq 1}),\ l = 1, 2,$$

over R, with $L_1 \subseteq L_2$. Let $\gamma : \Phi_1 \to \Phi_2$ be a morphism as in §4. For every $w' \in L_1$ of length i' we have

$$\Lambda_1(\tau_1(w')^{e(i')}) = \Lambda_2(\tau_2(w')^{e(i')}).$$

Hence the values of $\langle w, w' \rangle$ with respect to Φ_1 and to Φ_2 coincide.

6. Unitriangular representations

For an integer $i \geq 1$ and a profinite commutative unital ring R, we write Id for the identity matrix in the group $\mathbb{U}_i(R)$ of unitriangular $(i+1)\times(i+1)$-matrices over R (see §4). We also write E_{kl} for the $(i+1)\times(i+1)$-matrix over R which is 1 at entry (k,l), and is 0 elsewhere.

From now on we assume that $m = p$ is a prime number and $R = \mathbb{Z}_p$.

We record the following fact about the lower central series of $\mathbb{U}_i$, proved in [Ef23, Prop. 6.2(c)]:

Lemma 6.1. *For integers $i \geq i' \geq 1$ and $j, j' \geq 0$, one has $j' \geq j + \log_p(i/i')$ if and only if $(\mathbb{U}_i(\mathbb{Z}/p^{j+1})^{(i')})^{p^{j'}} \leq \mathrm{Id} + p^j\mathbb{Z}E_{1,i+1}$.*

Let $\Phi = (\Lambda : G \to \mathbb{Z}_p\langle\langle X\rangle\rangle^{\times,1}, \tau : L \to G, e)$ be a Magnus formation over $\mathbb{Z}_p$, where $e(i) = p^{j(i)}$ for some map $j : \{1,2,\dots,n\} \to \mathbb{Z}_{\geq 0}$. Let I_e be the subset of $\{1,2,\dots,n\}$ defined in §2.

Given a word $w \in X^*$ of length $1 \leq i \leq n$ we set

$$R_w = \mathbb{Z}/p^{j(i)+1} (= \mathbb{Z}/me(i)), \qquad \mathbb{U}_w = \mathbb{U}_i(R_w).$$

Let $\mathbb{U}_w^0$ be the subgroup $\mathrm{Id} + p^{j(i)}\mathbb{Z}E_{1,i+1}$ of $\mathbb{U}_w$. Then $\mathbb{U}_w^0 \cong \mathbb{Z}/p$, and $\mathbb{U}_w^0$ is central in $\mathbb{U}_w$. One has $\mathbb{U}_w^0 = (\mathbb{U}_w^{(i)})^{p^{j(i)}}$ [Ef23, Prop. 6.2(b)].

Let $\bar{\Lambda}_w : G \to R_w\langle\langle X\rangle\rangle^{\times,1}$ be the continuous homomorphism induced by Λ, and let $\rho_{w,R_w} : G \to \mathbb{U}_w$ be the continuous Magnus representation associated with $\bar{\Lambda}_w$, as in §4.

We define G^Φ to be the closed normal subgroup of G generated by all powers $\sigma_w = \tau(w)^{p^{j(i)}}$, where $w \in L$ and $i = |w|$.

Proposition 6.2. (a) *For a word $w \in X^*$ of length $i \in I_e$ one has $\rho_{w,R_w}(G^\Phi) \leq \mathbb{U}_w^0$.*

(b) *If in addition $w \in L$, then $\rho_{w,R_w}(G^\Phi) = \mathbb{U}_w^0$.*

Proof. (a) Since $\mathbb{U}_w^0$ is normal in $\mathbb{U}_w$, it suffices to show that $\rho_{w,R_w}(\sigma_{w'}) \in \mathbb{U}_w^0$ for every $w' \in L$. Let $i' = |w'|$.

Assume first that $i' \leq i$. Since $i \in I_e$, (2.1) holds, so $j(i') \geq j(i) + \log_p(i/i')$. Hence, by Lemma 6.1, $(\mathbb{U}_w^{(i')})^{p^{j(i')}} \leq \mathrm{Id} + p^{j(i)}\mathbb{Z}E_{1,i+1} = \mathbb{U}_w^0$. By condition (v) of Definition 4.2, $\tau(w') \in G^{(i')}$, and we deduce that

$$\rho_{w,R_w}(\sigma_{w'}) = \rho_{w,R_w}(\tau(w'))^{p^{j(i')}} \in (\mathbb{U}_w^{(i')})^{p^{j(i')}} \leq \mathbb{U}_w^0.$$

When $i < i'$ Proposition 5.1(a) implies that $\rho_{w,R_w}(\sigma_{w'}) = \mathrm{Id}$.

(b) By Proposition 5.1(b), $\rho_{w,R_w}(\sigma_w)_{1,i+1} = p^{j(i)}1_{R_w}$. In view of (a), $\rho_{w,R_w}(\sigma_w) = \mathrm{Id} + p^{j(i)}E_{1,i+1}$, which is a generator of $\mathbb{U}_w^0$. □

By Proposition 6.2(a), for w of length $i \in I_e$, the representation ρ_{w,R_w} induces a continuous homomorphism

$$\rho_w^0 : G^\Phi \to \mathbb{U}_w^0.$$

For every $w, w' \in L$ with $i = |w| \in I_e$ we have, under the identifications $\mathbb{U}_w^0 = p^{j(i)}\mathbb{Z}/p^{j(i)+1}\mathbb{Z} = \mathbb{Z}/p$, that

$$\rho_w^0(\sigma_{w'}) = \pi_i(\epsilon_w(\sigma_{w'})) = \langle w, w' \rangle. \tag{6.1}$$

Since $\mathbb{U}_w^0$ is central in $\mathbb{U}_w$, the homomorphism ρ_w^0 is G-invariant, that is, $\rho_w^0(\lambda\sigma\lambda^{-1}) = \rho_w^0(\sigma)$ for every $\sigma \in G^\Phi$ and $\lambda \in G$.

Let $\mathrm{Hom}(G^\Phi, \mathbb{Z}/p)$ denote the group of all continuous homomorphisms $\psi\colon G^\Phi \to \mathbb{Z}/p$. Let $\mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G$ be its subgroup consisting of all such homomorphisms which are G-invariant.

We will need the following fact in linear algebra [Ef17, Lemma 8.4]:

Lemma 6.3. *Let R be a commutative ring and let $(\cdot,\cdot)\colon A \times B \to R$ be a non-degenerate bilinear map of R-modules. Let $(\mathcal{L}, \leq)$ be a finite totally ordered set, and for every $w \in \mathcal{L}$ let $a_w \in A$, $b_w \in B$. Suppose that the matrix $\big((a_w, b_{w'})\big)_{w,w' \in \mathcal{L}}$ is invertible, and that a_w, $w \in \mathcal{L}$, generate A. Then a_w, $w \in \mathcal{L}$, is an R-linear basis of A, and b_w, $w \in \mathcal{L}$, is an R-linear basis of B.*

Specifically, for Φ as above, there is a well defined perfect bilinear map of $\mathbb{Z}/p$-linear spaces

$$(\cdot,\cdot)\colon G^\Phi/(G^\Phi)^p[G, G^\Phi] \times \mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G \to \mathbb{Z}/p, \quad (\bar{\sigma}, \psi) = \psi(\sigma) \tag{6.2}$$

[EfMi11, Cor. 2.2].

Proposition 6.4. *Suppose that the lengths of the words in L are in I_e. Then the maps ρ_w^0, $w \in L$, form a $\mathbb{Z}/p$-linear basis of* $\mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G$.

Proof. Assume first that L is finite. The left direct factor in (6.2) is generated by the cosets of $\sigma_{w'}$, $w' \in L$. By (6.1), the matrix $[(\bar{\sigma}_{w'}, \rho_w^0)]_{w,w' \in L}$ is the transpose of the fundamental matrix of Φ. By Corollary 5.2, it is invertible. Lemma 6.3 therefore implies the assertion in this case.

In the general case, write $L = \bigcup_\alpha L_\alpha$, where the L_α form a direct system of finite subsets of L. For every α let $\Phi_\alpha = (\Lambda, \tau|_{L_\alpha}, e)$ be the restricted Magnus formation. Thus G^{Φ_α} be the closed normal subgroup of G generated by the σ_w, $w \in L_\alpha$. Then G^Φ is generated by the G^{Φ_α}, and it follows that $\mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G = \varinjlim_\alpha \mathrm{Hom}(G^{\Phi_\alpha}, \mathbb{Z}/p)^G$. The assertion therefore follows from the finite case. $\square$

7. The isomorphism theorem

As before, let $m = p$ be a prime number, let $R = \mathbb{Z}_p$, and let $\Phi = (\Lambda\colon G \to \mathbb{Z}_p\langle\langle X\rangle\rangle^{\times,1}, \tau\colon L \to G, e)$ be a Magnus formation over $\mathbb{Z}_p$. We now assume further that Φ is compatible with a binary operation $\star$ as in §4. We denote the set of all words of length s in X^* by X^s. For $f \in \mathbb{Z}_p\langle X\rangle$ let f_s be its homogenous part of degree s. Let I_e be as in §2. Recall that for $w \in X^*$ of length in I_e, we may view ρ_w^0 as an element of $\mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G$.

Lemma 7.1. *For every nonempty words $u, v \in X^*$ with $s = |u| + |v| \in I_e$, one has*

$$\sum_{w\in X^s} (u \star v, w)_{\mathbb{Z}_p} \rho^0_w = 0.$$

Proof. First, we note that since $u \star v \in \mathbb{Z}_p\langle X\rangle$, the sum is well defined.

Let $w' \in L$. For $w \in X^*$ of length $1 \le i < s$ we have $ip^{j(i)} \ge sp^{j(s)}$, by (2.1), whence $j(i) > j(s)$. By Proposition 5.1(c), $\epsilon_w(\sigma_{w'}) \in p^{j(i)}\mathbb{Z}_p \subseteq p^{j(s)+1}\mathbb{Z}_p$. We apply Lemma 3.1 for the ideal $p^{j(s)+1}\mathbb{Z}_p$ of $\mathbb{Z}_p$ and $f = \Lambda(\sigma_{w'})$ to deduce that

$$(\Lambda(\sigma_{w'}), (u \star v)_s)_{\mathbb{Z}_p} \in p^{j(s)+1}\mathbb{Z}_p.$$

Therefore for the substitution pairing (6.2) we have, using (6.1),

$$\begin{aligned}
(\bar\sigma_{w'}, \sum_{w\in X^s} (u \star v, w)_{\mathbb{Z}_p} \rho^0_w) &= \sum_{w\in X^s} (u \star v, w)_{\mathbb{Z}_p} \rho^0_w(\bar\sigma_{w'}) \\
&= \sum_{w\in X^s} (u \star v, w)_{\mathbb{Z}_p} \pi_s(\epsilon_w(\sigma_{w'})) = \pi_s\Big(\sum_{w\in X^s} (u \star v, w)_{\mathbb{Z}_p} \epsilon_w(\sigma_{w'})\Big) \\
&= \pi_s\big((\Lambda(\sigma_{w'}), (u \star v)_s)_{\mathbb{Z}_p}\big) = 0.
\end{aligned}$$

Since the bilinear map (6.2) is non-degenerate, this gives the assertion. □

Suppose that $A = \bigoplus_{s\ge 0} A_s$ is a graded R-module, which is a (not necessarily graded) associative R-algebra with respect to a product map $\circ$. Let N be the R-submodule of A generated by the homogenous parts $(a\circ b)_{r+t}$ of the products $a\circ b$, where a, b are homogenous elements of A of degrees $r, t \ge 1$, respectively. It is a graded submodule, giving rise to a graded quotient R-module $A_{\mathrm{indec}} = A/N$, called the *indecomposable quotient* of A. Let $A_{\mathrm{indec},s}$ be the homogenous component of A_{indec} of degree s.

Now take the $\mathbb{Z}_p$-module $A = \bigoplus_{w\in X^*} \mathbb{Z}_p w$ with the product map $\star$ as in §3. We write $A^{(L)}_{\mathrm{indec}}$ for the submodule of A_{indec} generated by the images $\bar w$ of the words w in L.

Theorem 7.2. *Let Φ be a Magnus formation over $\mathbb{Z}_p$ as above which is compatible with $\star$. Suppose that the words in L have lengths in I_e. Then the map $\bar w \otimes 1 \mapsto \rho^0_w$, $w \in L$, induces an isomorphism of $\mathbb{Z}/p$-linear spaces*

$$A^{(L)}_{\mathrm{indec}} \otimes (\mathbb{Z}/p) \xrightarrow{\sim} \mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G.$$

Proof. There is a unique $\mathbb{Z}_p$-module homomorphism

$$h\colon \bigoplus_{s\in I_e} \bigoplus_{w\in X^s} \mathbb{Z}_p w \to \mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G.$$

such that $h(w) = \rho^0_w$ for $s \in I_e$ and $w \in X^s$. By Lemma 7.1, h is trivial on the homogenous components $(u \star v)_s$, where u, v are nonempty words and

$s = |u| + |v| \in I_e$. Therefore h factors via $\bigoplus_{s\in I_e} A_{\mathrm{indec},s}$. Since the lengths of the words in L are in I_e, the homomorphism h induces a $\mathbb{Z}/p$-linear map

$$\bar{h}\colon A^{(L)}_{\mathrm{indec}} \otimes (\mathbb{Z}/p) \to \mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G,$$

where $\bar{h}(\bar{w} \otimes 1) = \rho^0_w$ for $w \in L$.

Now the $\bar{w} \otimes 1$, where $w \in L$, span $A^{(L)}_{\mathrm{indec}} \otimes (\mathbb{Z}/p)$ as a $\mathbb{Z}/p$-linear space. Furthermore, by Proposition 6.4, their images ρ^0_w form a linear basis of the $\mathbb{Z}/p$-linear space $\mathrm{Hom}(G^\Phi, \mathbb{Z}/p)^G$. Therefore $\bar{h}$ is an isomorphism. □

Remark 7.3. This isomorphism is functorial in the following sense: Consider the setup of Remark 5.3 (with $m = p$ and $R = \mathbb{Z}_p$), and let $A = \bigoplus_{w\in X^*} \mathbb{Z}_p w$ be as above. Suppose that the Magnus formation Φ_2 (whence also the formation Φ_1) is compatible with the product map $\star$. Then γ induces a commutative square

$$\begin{tikzcd}
A^{(L_1)}_{\mathrm{indec}} \otimes (\mathbb{Z}/p) \arrow[r, "\sim"] \arrow[d] & \mathrm{Hom}(G_1^{\Phi_1}, \mathbb{Z}/p)^{G_1} \\
A^{(L_2)}_{\mathrm{indec}} \otimes (\mathbb{Z}/p) \arrow[r, "\sim"] & \mathrm{Hom}(G_2^{\Phi_2}, \mathbb{Z}/p)^{G_2}, \arrow[u]
\end{tikzcd}$$

where the right vertical map is the restriction.

8. The shuffle algebra

Our main examples concern the p-adic Magnus formations of Example 4.3, in connection with the shuffle algebra.

Every word $w \in X^*$ can be uniquely written as a concatenation $w = u_1^{k_1} \cdots u_t^{k_t}$, where $u_1 >_{\mathrm{alp}} \cdots >_{\mathrm{alp}} u_t$ are Lyndon words in X^*, $k_1 > \cdots > k_t$, and where u^k denotes the concatenation of u with itself k times [Re93, Cor. 4.7 and Th. 5.1]. Consider the noncommutative polynomials

$$Q_w = \frac{1}{k_1! \cdots k_t!} u_1^{ш k_1} ш \cdots ш u_t^{ш k_t} \in \mathbb{Q}\langle X\rangle,$$

where $u^{ш k}$ denotes the k-times shuffle product $u ш \cdots ш u$. The polynomial Q_w is homogenous of degree $|w| = k_1|u_1| + \cdots + k_t|u_t|$, and in fact, $Q_w \in \mathbb{Z}\langle X\rangle$ [Re93, Th. 6.1]. By a result of Radford [Ra79] and Perrin and Viennot (unpublished) – see again [Re93, Th. 6.1] – for every word $w \in X^*$ one has

$$Q_w = w + \sum_{v \le_{\mathrm{alp}} w} a_{v,w} v$$

for some nonnegative integers $a_{v,w}$, and where for all but finitely many v we have $a_{v,w} = 0$. We may restrict to v such that $|v| = |w|$. Hence for every positive integer s we have

$$\bigoplus_{w\in X^s} \mathbb{Z} Q_w = \bigoplus_{w\in X^s} \mathbb{Z} w. \tag{8.1}$$

Recall that the *shuffle $\mathbb{Z}$-algebra* $\mathrm{Sh}(X)$ over X is the $\mathbb{Z}$-module $\bigoplus_{w\in X^*}\mathbb{Z}w$ with the shuffle product $ш$ (§4). Let $\mathrm{Sh}(X)_{\mathrm{indec}}$ be its indecomposable quotient with respect to the product map $\circ = ш$. Since for words u, v with $s = |u|+|v|$ we have $(u \downarrow v)_s = u ш v$, the indecomposable quotient of $\bigoplus_{w\in X^*}\mathbb{Z}w$ with respect to $\circ = \downarrow$ is also $\mathrm{Sh}(X)_{\mathrm{indec}}$. The shuffle product $ш$ extends in an obvious way to the $\mathbb{Z}_p$-module $\bigoplus_{w\in X^*}\mathbb{Z}_p w$, giving rise to a $\mathbb{Z}_p$-shuffle algebra $\mathrm{Sh}(X)\otimes\mathbb{Z}_p$. We note that

$$\mathrm{Sh}(X)_{\mathrm{indec}}\otimes\mathbb{Z}_p = (\mathrm{Sh}(X)\otimes\mathbb{Z}_p)_{\mathrm{indec}}. \tag{8.2}$$

Proposition 8.1. *Let L be the set of all Lyndon words in X^* of length $s \ge 1$. Let r be a positive integer whose prime factors are larger than s. Then*

$$\mathrm{Sh}(X)_{\mathrm{indec},s}\otimes(\mathbb{Z}/r) = \mathrm{Sh}(X)^{(L)}_{\mathrm{indec},s}\otimes(\mathbb{Z}/r).$$

Proof. Take $w \in X^s$ with its decomposition $w = u_1^{k_1}\cdots u_t^{k_t}$ as above. As $k_1,\dots,k_t \le s$, the assumption on r implies that $k_1!\cdots k_t!$ is invertible in $\mathbb{Z}/r$. If in addition $w \notin L$, then $k_1!\cdots k_t! Q_w$ has trivial image in $\mathrm{Sh}(X)_{\mathrm{indec},s}$, and therefore Q_w has trivial image in $\mathrm{Sh}(X)_{\mathrm{indec},s}\otimes(\mathbb{Z}/r)$.

Therefore the images of $\sum_{w\in X^s}\mathbb{Z}Q_w$ and $\sum_{w\in L}\mathbb{Z}Q_w$ in $\mathrm{Sh}(X)_{\mathrm{indec},s}\otimes(\mathbb{Z}/r)$ coincide. But by (8.1), the former sum is $\sum_{w\in X^s}\mathbb{Z}w$, whereas by the construction of Q_w, the latter sum is $\sum_{w\in L}\mathbb{Z}w$. Hence these two images are the full $\mathrm{Sh}(X)_{\mathrm{indec},s}\otimes(\mathbb{Z}/r)$ and $\mathrm{Sh}(X)^{(L)}_{\mathrm{indec},s}\otimes(\mathbb{Z}/r)$, respectively. □

We now take $\Phi = (\Lambda\colon G \to \mathbb{Z}_p^{\times,1}, \tau\colon L \to G, e)$ to be a p-adic Magnus formation, as in Example 4.3. Thus G is a free pro-p group on basis X, and we recall that Φ is compatible with the infiltration product $\downarrow$. We further assume that the map e is given by $e(i) = p^{j(i)}$ for some map $j\colon \{1,2,\dots,n\}\to\mathbb{Z}_{\ge 0}$. The map j is weakly decreasing and is not identically 0, by Definition 4.2(vii). Thus $j(1)\ge 1$.

We can now prove the Main Theorem from the Introduction:

Theorem 8.2. *Suppose that $n < p$ and L is the set of all Lyndon words in X^* with length in I_e. Then there is a canonical isomorphism of $\mathbb{Z}/p$-linear spaces*

$$\Big(\bigoplus_{s\in I_e}\mathrm{Sh}(X)_{\mathrm{indec},s}\Big)\otimes(\mathbb{Z}/p)\xrightarrow{\sim} H^2(G/G^{\Phi}).$$

Proof. By (8.2), $\mathrm{Sh}(X)^{(L)}_{\mathrm{indec}}\otimes\mathbb{Z}_p \cong (\mathrm{Sh}(X)\otimes\mathbb{Z}_p)^{(L)}_{\mathrm{indec}}$. Hence, by Proposition 8.1 (with $r = p$),

$$\begin{aligned}\Big(\bigoplus_{s\in I_e}\mathrm{Sh}(X)_{\mathrm{indec},s}\Big)\otimes(\mathbb{Z}/p) &= \Big(\bigoplus_{s\in I_e}\mathrm{Sh}(X)^{(L)}_{\mathrm{indec},s}\Big)\otimes(\mathbb{Z}/p)\\ &= \mathrm{Sh}(X)^{(L)}_{\mathrm{indec}}\otimes(\mathbb{Z}/p) = (\mathrm{Sh}(X)\otimes\mathbb{Z}_p)^{(L)}_{\mathrm{indec}}\otimes(\mathbb{Z}/p).\end{aligned}$$

By Theorem 7.2 for $A = \mathrm{Sh}(X)\otimes\mathbb{Z}_p$ and $\downarrow$, the latter module is isomorphic to $\mathrm{Hom}(G^{\Phi},\mathbb{Z}/p)^G$ via the map $\bar{w}\otimes 1 \mapsto \rho^0_w$, for $w \in L$. Moreover, by the definition of the first cohomology group, $\mathrm{Hom}(G^\Phi,\mathbb{Z}/p)^G = H^1(G^\Phi)^G$. We deduce that

$$\Big(\bigoplus_{s\in I_e}\mathrm{Sh}(X)_{\mathrm{indec},s}\Big)\otimes(\mathbb{Z}/p)\cong H^1(G^\Phi)^G. \tag{8.3}$$

Now when $w=(x)$ is a word of length 1 we have $\sigma_w = x^{p^{j(1)}}\in G^p$. When w is a Lyndon word of length ≥ 2 we have $\tau_w\in G^{(2)}$, by Definition 4.2(v), whence also $\sigma_w\in G^{(2)}$. Thus G^Φ is contained in the Frattini subgroup $G^pG^{(2)} = G^p[G,G]$ of G. It follows that the inflation map $H^1(G/G^\Phi)\to H^1(G)$ is an isomorphism. Since G is a free pro-p group, $\mathrm{cd}_p(G)\leq 1$. The five term sequence in profinite cohomology [NSW08, Prop. 1.6.7] therefore implies that the transgression map

$$\mathrm{trg}\colon\ H^1(G^\Phi)^G\to H^2(G/G^\Phi)$$

is an isomorphism, and we combine it with (8.3). □

Remark 8.3. Explicitly, this isomorphism is given as follows: The left-hand side is generated by elements of the form $\bar{w}\otimes 1$, where w is a Lyndon word of length $s\in I_e$, and such a generator is mapped to $\mathrm{trg}(\rho^0_w)$. Let $\alpha_w\in H^2(\mathbb{U}_w/\mathbb{U}^0_w)$ correspond to the central extension

$$1\to\mathbb{U}^0_w(\cong\mathbb{Z}/p)\to\mathbb{U}_w\to\mathbb{U}_w/\mathbb{U}^0_w\to 1$$

under the Schreier correspondence [NSW08, Th. 1.2.4]. Let $\bar\rho_w\colon G/G^\Phi\to\mathbb{U}_w/\mathbb{U}^0_w$ be the homomorphism induced by $\rho_{w,R_w}\colon G\to\mathbb{U}_w$ (see Proposition 6.2(a)). By [Hoe68], $\mathrm{trg}(\rho^0_w)$ is the pullback $\bar\rho^*_w(\alpha_w)$ of α_w to $H^2(G/G^\Phi)$ along $\bar\rho_w$. It corresponds to the central extension

$$0\to\mathbb{Z}/p\to\mathbb{U}_w\times_{\mathbb{U}_w/\mathbb{U}^0_w}(G/G^\Phi)\to G/G^\Phi\to 1,$$

where the middle term is the fiber product.

We examine these cohomology elements in two special situations:

Example 8.4. Suppose that $w=(x)$ has length 1. Then α_w corresponds to the extension

$$0\to\mathbb{Z}/p\to\mathbb{Z}/p^{j(1)+1}\to\mathbb{Z}/p^{j(1)}\to 0.$$

The *Bockstein map* $\mathrm{Bock}\colon H^1(G/G^\Phi,\mathbb{Z}/p^{j(1)})\to H^2(G/G^\Phi)$ is the connecting homomorphism associated to this short exact sequence of trivial G/G^Φ-modules [NSW08, Th. 1.3.2]. The homomorphism $\bar\rho_w\colon G/G^\Phi\to\mathbb{U}_w/\mathbb{U}^0_w$ may be identified with the map $\bar\epsilon_{(x)}=\epsilon_{(x)}\ (\mathrm{mod}\ p^{j(1)})$. Then the pullback $\bar\rho^*_w(\alpha_w)$ is $\mathrm{Bock}(\bar\rho_w)=\mathrm{Bock}(\bar\epsilon_{(x)})$ [Ef17, Example 7.4(1)].

Example 8.5. Let $w=(a_1\cdots a_n)$ be a Lyndon word in X^* of length n, and suppose that $j(n)=0$. Then the pullbacks $\bar\rho^*_w(\alpha_w)$ are elements of the n-fold Massey product

$$\langle\cdot,,\dots,\cdot\rangle\colon\ H^1(G)^n\to H^2(G).$$

We refer, e.g., to [Ef14] for the definition of this map in the context of profinite cohomology, and recall that this is a multi-valued map, i.e., $\langle\varphi_1,\dots,\varphi_n\rangle$ is a *subset* of $H^2(G)$. Namely, in this case $R_w=\mathbb{Z}/p$, and $\mathbb{U}_w/\mathbb{U}^0_w$ is the group $\mathbb{U}_w$ with its $(1, n+1)$-entry deleted. Let $\bar{\Lambda}_w : G \to (\mathbb{Z}/p)\langle\langle X\rangle\rangle^{\times,1}$ be the homomorphism induced by Λ as in §6, and denote the coefficient of a word u in $\bar{\Lambda}_w(\sigma)$ by $\bar{\varepsilon}_u(\sigma)$. As shown by Dwyer [Dw75] in the discrete case (see [Ef14, Prop. 8.3] for the profinite case) the pullbacks $\bar{\rho}_w^*(\alpha_w)$ are elements of $\langle \bar{\varepsilon}_{(a_1)}, \dots, \bar{\varepsilon}_{(a_n)}\rangle$.

Finally, we specify Theorem 8.2 in the two special cases discussed in the Introduction:

Example 8.6. Consider the binomial map $e(i) = p^{n-i}$, as in Example 2.3. Then $I_e = \{1, 2, \dots, n\}$, and L contains all Lyndon words w of length $1 \leq i \leq n$. For a free pro-p group G on the basis X, let $K^{(n,p)}$ be its closed subgroup generated by all powers $\tau_w^{p^{n-i}}$ for such w. We obtain that when $n < p$,

$$\bigoplus_{s=1}^{n} \mathrm{Sh}(X)_{\mathrm{indec},s} \otimes (\mathbb{Z}/p) \xrightarrow{\sim} H^2(G/K^{(n,p)}).$$

The groups $K^{(n,p)}$ are closely related to the lower p-central filtration $G^{(n,p)}$, $n = 1, 2, \dots,$ of G. Namely, in [Ef17, Th. 5.3] it is shown (using Lie algebra techniques) that the subgroups $K^{(n,p)}, G^{(n,p)}$ coincide modulo $G^{(n+1,p)}$.

Example 8.7. For a positive integer t, we consider the binomial map $e(i) = p^{t\lceil \log_p(n/i)\rceil}$, as in Example 2.4. Assume that $n < p$. By Proposition 2.5, $I_e = \{1, n\}$. In the free pro-p group G on basis the X, let $K_{(n,p)}$ be the closed subgroup generated by all powers $x^{e(1)}$, $x \in X$, and by all Lie elements τ_w, where w is a Lyndon word of length n in X^*. We obtain that

$$\Big(\bigoplus_{x\in X}(\mathbb{Z}/p)\Big) \oplus \big(\mathrm{Sh}(X)_{\mathrm{indec},n} \otimes (\mathbb{Z}/p)\big) \xrightarrow{\sim} H^2(G/K_{(n,p)}).$$

When $t = 1$, the subgroups $K_{(n,p)}$ are closely related to the p-Zassenhaus filtration of G (see the Introduction). Namely, in [Ef23, Th. 4.6] it is shown using p-restricted Lie algebra techniques that the subgroups $K_{(n,p)}, G_{(n,p)}$ coincide modulo $(G_{(n,p)})^p[G, G_{(n,p)}]$.

References

[CE16] Chapman, M.; Efrat, I. Filtrations of the free group arising from the lower central series. *J. Group Theory* **19** (2016), no. 3, 405–433. MR3510836, Zbl 1356.20019, doi: 10.1515/jgth-2016-0508. 1180, 1181

[CFL58] Chen, K.-T.; Fox, R. H.; Lyndon, R. C. Free differential calculus. IV. The quotient groups of the lower central series. *Ann. of Math. (2)* **68** (1958), 81–95. MR0102539, Zbl 0142.22304, doi: 10.2307/1970044. 1183, 1185

[De10] Deligne, P. Le groupe fondamental unipotent motivique de $\mathbb{G}_m - \mu_N$, pour $N = 2, 3, 4, 6$ ou 8. *Publ. Math. l'IHÉS* **112** (2010), 101–141. MR2737978, Zbl 1218.14016, doi: 10.1007/s10240-010-0027-6. 1182

[DDSMS99] Dixon, J.D.; Du Sautoy, M.P.F.; Mann, A.; Segal, D. Analytic Pro-p Groups, 2nd Edition. Cambridge Studies in Advanced Mathematics 61. *Cambridge Univ. Press, Cambridge* 1999. xviii+368 pp. ISBN: 0-521-65011-9. MR1720368, Zbl 0934.20001, doi: 10.1017/CBO9780511470882. 1179

[Dw75] Dwyer, W.G. Homology, Massey products and maps between groups. *J. Pure Appl. Algebra* **6**, no. 2 (1975), 177–190. MR0385851, Zbl 0338.20057, doi: 10.1016/0022-4049(75)90006-7. 1193

[Ef14] Efrat, I. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Advances Math.* **263** (2014), 389–411. MR3239143, Zbl 1346.20027, doi: 10.1016/j.aim.2014.07.006. 1183, 1192, 1193

[Ef17] Efrat, I. The Cohomology of canonical quotients of free groups and Lyndon words. *Documenta Math.* **22** (2017), 973–997. MR3665398, Zbl 1437.20047. 1178, 1179, 1185, 1188, 1192, 1193

[Ef20] Efrat, I. The lower p-central series of a free profinite group and the shuffle algebra. *J. Pure Applied Math.* **224**, no. 6 (2020), 106260. MR4048520, Zbl 1506.20086, doi: 10.1016/j.jpaa.2019.106260. 1178

[Ef23] Efrat, I. The p-Zassenhaus filtration of a free profinite group and shuffle relations. *J. Inst. Math. Jussieu* **22**, no. 2 (2023), 961–983. MR4557910, Zbl 1517.12005, doi: 10.1017/S1474748021000426. 1178, 1179, 1181, 1182, 1187, 1193

[EfMa17] Efrat, I.; Matzri, E. Triple Massey products and absolute Galois groups. *J. Eur. Math Soc. (JEMS)* **19**, no. 12 (2017), 3629–3640. MR3730509, Zbl 1425.12004, doi: 10.4171/JEMS/748. 1180

[EfMi11] Efrat, I.; Mináč, J. On the descending central sequence of absolute Galois groups. *Amer. J. Math.* **133**, no. 6 (2011), 1503–1532. MR2863369, Zbl 1236.12003, doi: 10.1353/ajm.2011.0041. 1188

[FJ23] Fried, M. D.; Jarden, M. Field Arithmetic. 4th ed. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Vol. 11. *Springer*, 2023. xxxi+827 pp. ISBN: 978-3-031-28019-1; 978-3-031-28020-7. MR4647281, Zbl 1530.12003, doi: 10.1007/978-3-031-28020-7. 1185

[GR20] Grinberg, D.; Reiner, V. Hopf Algebras in Combinatorics, 2020. e-print: `https://arxiv.org/abs/1409.8356v7`. 1182

[GMT18] Guillot, P.; Mináč, J.; Topaz, A. Four-fold Massey products in Galois cohomology. With an appendix by Olivier Wittenberg. *Compos. Math.* **154**, no. 9 (2018), 1921–1959. MR3867288, Zbl 1455.12005, doi: 10.1112/s0010437x18007297. 1180

[HaW19] Harpaz, Y.; Wittenberg, O., The Massey vanishing conjecture for number fields. *Duke Math. J.* **172**, no. 1 (2023), 1–41. MR4533716, Zbl 1521.11070, doi: 10.1215/00127094-2022-0004. 1180

[Hoe68] Hoechsmann, K. Zum Einbettungsproblem. *J. reine angew. Math.* **229** (1968), 81–106. MR244190, Zbl 0185.11202, doi: 10.1515/crll.1968.229.81. 1192

[HoW15] Hopkins, M.; Wickelgren, K. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra* **219**, no. 5 (2015), 1304–1319. MR3299685, Zbl 1323.55014, doi: 10.1016/j.jpaa.2014.06.006. 1180

[KMT17] Kodani, H.; Morishita, M.; Terashima, Y. Arithmetic topology in Ihara theory. *Publ. Res. Inst. Math. Sci.* **53**, no. 4 (2017), 629–688. MR3716496, Zbl 1430.11082, doi: 10.4171/PRIMS/53-4-6. 1180

[L67] Labute, J. Classification of Demushkin groups. *Canad. J. Math.* **19** (1967), 106–132. MR210788, Zbl 0153.04202, doi: 10.4153/CJM-1967-007-8. 1178

[LLSWW23] Lam, Y.; Hay J.; Liu, Y.; Sharifi, R.; Wake, P.; Wang, J. Generalized Bockstein maps and Massey products. *Forum Math. Sigma* **11** (2023), Paper No. e5, 41. MR4537772, Zbl 7646054, doi: 10.1017/fms.2022.103. 1180

[L54] Lazard, M. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. École Norm. Sup. (3)* **71** (1954), 101–190. MR88496, Zbl 0055.25103. 1178

[Lo83] Lothaire, M. Combinatorics on Words. Encyclopedia of Mathematics and its Applications 17. *Addison-Wesley Publishing Co., Reading, MA*, 1983. xix+238 pp.; ISBN: 0-201-13516-7. MR675953, Zbl 0514.20045. 1182, 1183

[Ma35] MAGNUS, W. Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. *Math. Ann.* **111**, no. 1 (1935), 159–280. MR1512992, Zbl 0011.15201, doi: 10.1007/BF01472217. 1178

[MS23a] MERKURJEV, A.; SCAVIA, F. The Massey Vanishing Conjecture for fourfold Massey products modulo 2. e-print: https://arxiv.org/abs/2301.09290, 2023. 1180

[MS23b] MERKURJEV, A.; SCAVIA, F. Non-formality of Galois cohomology modulo all primes. e-print: https://arxiv.org/abs/2309.17004, 2023. 1180

[MPQT21] MINÁČ, J.; PASINI, F. W.; QUADRELLI, C.; TÂN, N. D. Koszul algebras and quadratic duals in Galois cohomology. *Adv. Math.* **380** (2021), Paper No. 107569, 49. MR4200471, Zbl 1483.12003, doi: 10.1016/j.aim.2021.107569. 1179

[MPQT22] MINÁČ, J.; PASINI, F. W.; QUADRELLI, C.; TÂN, N. D. Mild pro-p groups and the Koszulity conjectures. *Expo. Math.* **40**, no. 3, (2022), 432–455. MR4475389, Zbl 1527.16030, doi: 10.1016/j.exmath.2022.03.004. 1179

[MT16] MINÁČ, J.; TÂN, N. D. Triple Massey products vanish over all fields. *J. London Math. Soc.(2)* **94**, No. 3 (2016), 909–932. MR3614934, Zbl 1378.12002, doi: 10.1112/jlms/jdw064. 1180

[Mo12] MORISHITA, M. Knots and Primes. Universitext. *Springer, London*, 2012. xii+191 pp. ISBN: 978-1-4471-2157-2. MR2905431, Zbl 7814877, doi: 10.1007/978-1-4471-2158-9. 1180, 1185

[NSW08] NEUKIRCH, J.; SCHMIDT, A.; WINGBERG, K. Cohomology of Number Fields. 2nd edition. Grundlehren der mathematischen Wissenschaften 323. *Springer-Verlag, Berlin*, 2008. xvi+825 pp. ISBN: 978-3-540-37888-4. MR2392026, Zbl 1136.11001, doi: 10.1007/978-3-540-37889-1. 1178, 1192

[Ra79] RADFORD, D. E. A natural ring basis for the shuffle algebra and an application to group schemes. *J. Algebra* **58**, no. 2 (1979), 432–454. MR540649, Zbl 0409.16011, doi: 10.1016/0021-8693(79)90171-6. 1179, 1190

[Re93] REUTENAUER, CH. Free Lie Algebras. London Mathematical Society Monographs. New Series, 7. *Oxford Science Publications, The Clarendon Press, Oxford University Press, New York*, 1993. xviii+269 pp. ISBN: 0-19-853679-8. MR1231799, Zbl 0798.17001. 1182, 1183, 1185, 1190

[Se63] SERRE, J.-P. Structure de certains pro-p-groupes (d'après Demuškin). *Séminaire Bourbaki* Exp. 252 (1962/63). MR180466, Zbl 0121.04404. 1178

[Se02] SERRE, J.-P. Galois Cohomology. Springer Monographs in Mathematics *Springer-Verlag, Berlin*, 2002. x+210 pp. ISBN: 3-540-42192-0. MR1867431, Zbl 1004.12003. 1178

[Vo05] VOGEL, D. On the Galois group of 2-extensions with restricted ramification. *J. reine angew. Math.* **581** (2005), 117–150. MR2132673, Zbl 1143.11042, doi: 10.1515/crll.2005.2005.581.117. 1180, 1185

(Ido Efrat) EARL KATZ FAMILY CHAIR IN PURE MATHEMATICS, DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, P.O. BOX 653, BE'ER-SHEVA 8410501, ISRAEL
efrat@bgu.ac.il

This paper is available via http://nyjm.albany.edu/j/2024/30-52.html.