THE LOWER $p$-CENTRAL SERIES OF A FREE PROFINITE GROUP AND THE SHUFFLE ALGEBRA

IDO EFRAT

Abstract. For a prime number $p$ and a free profinite group $S$ on the basis $X$, let $S^{(n,p)}$, $n = 1, 2, \ldots$, be the lower $p$-central filtration of $S$. For $p > n$, we give a combinatorial description of $H^2(S/S^{(n,p)}, \mathbb{Z}/p)$ in terms of the Shuffle algebra on $X$.

1. Introduction

For a fixed prime number $p$ and a profinite group $G$, the lower $p$-central filtration $G^{(n,p)}$, $n = 1, 2, 3, \ldots$, of $G$ is defined inductively by

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

Thus $G^{(n+1,p)}$ is the closed subgroup of $G$ generated by all powers $g^p$ and commutators $[g, h] = g^{-1}h^{-1}gh$, with $g \in G^{(n,p)}$ and $h \in G$. The subgroups $G^{(n,p)}$ are normal in $G$, and we denote $G^{[n,p]} = G/G^{(n,p)}$. We write $H^i(G) = H^i(G, \mathbb{Z}/p)$ for the profinite cohomology group of $G$ with respect to its trivial action on $\mathbb{Z}/p$.

In this paper we consider a free profinite group $S$ on the basis $X$. For $p > n$, we give an explicit combinatorial description of $H^2(S^{[n,p]}, \mathbb{Z}/p)$ in terms of the shuffle algebra $S_{\mathbb{Z}}(X)$ over $X$. To state it, denote the free monoid on $X$ by $X^*$, and consider its elements as associative words in the alphabet $X$. Let $\mathbb{Z}(X)$ be the free $\mathbb{Z}$-module over the basis $X^*$. The shuffle product of words $u = (x_1 \cdots x_r)$ and $v = (x_{r+1} \cdots x_{r+t})$ is defined by

$$uvw = \sum_\sigma (x_{\sigma(1)} \cdots x_{\sigma(r+t)}) \in \mathbb{Z}(X),$$

where $\sigma$ ranges over all permutations of $1, 2, \ldots, r + t$ such that $\sigma(1) < \cdots < \sigma(r)$ and $\sigma(r + 1) < \cdots < \sigma(r + t)$. This extends by linearity to an associative and commutative bilinear map $m$ on $\mathbb{Z}(X)$, and the shuffle algebra $S_{\mathbb{Z}}(X)$ is the resulting $\mathbb{Z}$-algebra.

2010 Mathematics Subject Classification. Primary 12G05; Secondary 68R15, 12F10, 12E30.

Key words and phrases. Shuffle algebra, lower $p$-central sequence, Galois cohomology, unipotent upper-triangular representations, Massey products, absolute Galois groups.
Next let $M$ be the submodule of $\mathbb{Z}\langle X \rangle$ generated by all products $uuv$ such that $u,v \in X^*$ are nonempty words. The $\mathbb{Z}$-module $\text{Sh}_\mathbb{Z}(X)_{\text{indec}} = \mathbb{Z}\langle X \rangle / M$ is called the indecomposable quotient of $\text{Sh}_\mathbb{Z}(X)$. The $\mathbb{Z}$-module $\text{Sh}_\mathbb{Z}(X)$, and therefore also its quotient $\text{Sh}_\mathbb{Z}(X)_{\text{indec}}$, are graded by the length $|w|$ of words $w$. Our main result states that, for $p$ sufficiently large, all relations in $H^2(S^{[n,p]})$ are formal consequences of shuffle relations:

**Main Theorem.** For every integer $n \geq 2$ and a prime number $p > n$ there is a canonical isomorphism

$$
\bigoplus_{s=1}^n \text{Sh}_\mathbb{Z}(X)_{\text{indec},s} \otimes (\mathbb{Z}/p) \xrightarrow{\sim} H^2(S^{[n,p]}).
$$

This isomorphism is based on a general construction of cohomological elements $\rho^* \gamma_{n,s}$ in $H^2(G)$, where $G$ is an arbitrary profinite group. These elements are constructed as certain pullbacks by unipotent upper-triangular representations $\rho$ of $G$, and we refer to §3 for their precise definition. They include Bockstein elements, cup products, and more generally, elements of Massey products in $H^2(G)$ (Examples 3.3 and 3.4). The case where $G = S^{[n,p]}$, for $S$ a free profinite group, is of a generic nature, but the cohomological elements $\rho^* \gamma_{n,s}$ are interesting also for profinite groups $G$ of arithmetical origin. In particular, in §8 we take $G$ to be the absolute Galois group of a field containing a root of unity of order $p$. Then the Merkurjev–Suslin theorem implies that each element of $H^2(G)$ decomposes as a sum of cup products. However the decomposition pattern of the $\rho^* \gamma_{n,s}$ is known explicitly only in very few cases, and these decompositions correspond to deep facts in Galois cohomology, which in turn provide restrictions on the possible group-theoretic structure of $G$ (see §8).

The proof of Theorem 1 leans heavily on our previous paper [Efr17], where we construct for every word $w \in X^*$ of length $\leq n$ an element $\alpha_{w,n}$ of $H^2(S^{[n,p]})$, and show that the elements $\alpha_{w,n}$, where $w$ is a Lyndon word, form a linear basis of $H^2(S^{[n,p]})$ (see §6 for details). The elements $\alpha_{w,n}$ are special instances of the above-mentioned pullbacks $\rho^* \gamma_{n,s}$, where the representation $\rho = \hat{\rho}^w$ is constructed in this case using Magnus theory (see §7). The existence of an epimorphism $\bigoplus_{s=1}^n \text{Sh}_\mathbb{Z}(X)_{\text{indec},s} \otimes (\mathbb{Z}/p) \xrightarrow{\sim} H^2(S^{[n,p]})$ is a formal consequence of the results of [Efr17]. It was further shown there, by an explicit computation, that this epimorphism is an isomorphism for $n = 2, p > 2$ and for $n = 3, p > 3$. Thus the present paper settles this problem in general, by proving the injectivity of the epimorphism for $p > n$. Note that for $n = p$ it need not be injective – see Example
The main new ingredient in the current paper, which leads to the proof of the injectivity, is the use of the Radford polynomials (discussed in §6).

When \( n = 2 \), the quotient \( S^{[2,p]} \) is an elementary abelian \( p \)-group. Then the Main Theorem recovers the known fact that for an elementary abelian \( p \)-group \( \bar{S} \), with \( p \) odd, one has \( H^1(\bar{S}) \oplus \wedge^2 H^1(\bar{S}) \cong H^2(\bar{S}) \) via the map which is the Bockstein homomorphism on the first direct summand, and is induced by the cup product on the second summand ([EMI11, §2D], [Top16, Fact 8.1]). In this sense our work traces back to the pioneering work of Labute on the duality between \( S^{(2,p)}/S^{(3,p)} \) and the second cohomology \([Lab67]\).

I thank Claudio Quadrelli, Jacob Stix, and Adam Topaz for discussions related to this work.

2. Upper-triangular unipotent matrices

For a unital commutative ring \( R \), let \( \mathbb{U}_s(R) \) denote the group of all upper-triangular unipotent \( (s+1) \times (s+1) \)-matrices over \( R \).

We consider integers \( n, s \) such that \( n \geq 2 \) and \( 1 \leq s \leq n \). Let \( R = \mathbb{Z}/p^{n-s+1} \) and \( \mathbb{U} = \mathbb{U}_s(R) \). We write \( I_{s+1} \) for the unit matrix in \( \mathbb{U} \), and \( E_{i,j} \) for the \( (s+1) \times (s+1) \)-matrix over \( R \) which is 1 at entry \( (i,j) \), and is 0 elsewhere.

**Lemma 2.1.** The lower \( p \)-central filtration of \( \mathbb{U} \) satisfies

(a) \( \mathbb{U}^{(n,p)} \cong \mathbb{Z}/p \);
(b) \( \mathbb{U}^{(n,p)} \) lies in the center of \( \mathbb{U} \);
(c) \( \mathbb{U}^{(n+1,p)} = 1 \).

**Proof.** (a) By [Efr17, Prop. 6.3(a)], \( \mathbb{U}^{(n,p)} = I_{s+1} + \mathbb{Z}p^{n-s}E_{1,s+1} \). Therefore there is an isomorphism

\[
\mathbb{U}^{(n,p)} \rightarrow \mathbb{Z}/p, \quad I_{s+1} + kp^{n-s}E_{1,s+1} \mapsto k \pmod{p}.
\]

(b) See [Efr17, Prop. 6.3(b)].

(c) By (a) and (b), \( \mathbb{U}^{(n+1,p)} = (\mathbb{U}^{(n,p)})^p[\mathbb{U}^{(n,p)}, \mathbb{U}] = 1 \). □

We obtain a central extension

\[
0 \rightarrow \mathbb{Z}/p \rightarrow \mathbb{U} \xrightarrow{\lambda} \mathbb{U}^{[n,p]} \rightarrow 1
\]

where \( \lambda \) is the canonical epimorphism. This extension corresponds to a cohomology element \( \gamma_{n,s} \in H^2(\mathbb{U}^{[n,p]}) \), in the sense of the Schreier correspondence (see e.g., [NSW08 Th. 1.2.4]).

Next we compute the exponent of \( \mathbb{U} \), based on an argument by W. Sawin [Saw18]. First we record a few elementary facts about binomial coefficients.
Proposition 2.2. (a) Let \( l, k \) be integers such that \( 1 \leq l \leq p^k \). Then \( p^k / \gcd(p^k, l) \) divides \( \binom{p^k}{l} \).

(b) Let \( l, k \) be integers such that \( 1 \leq l \leq p^k \) and \( l \) is a p-power. Then \( p^k / l \) is the maximal p-power dividing \( \binom{p^k}{l} \).

(c) Let \( t, k \) be integers such that \( 1 \leq t \leq p^k \), and let \( q \) be a p-power. Then \( q | \binom{p^k}{l} \), \( l = 1, 2, \ldots, t \), if and only if \( qp \log_p t | p^k \).

(d) For \( m \geq 1 \), one has \( p | \binom{m}{l} \), \( l = 1, 2, \ldots, m - 1 \), if and only if \( m \) is a p-power.

Proof. (a) Let \( v_p \) be the p-adic valuation. As \( \binom{p^k}{l} = \frac{p^k}{l} \binom{p^k - 1}{l - 1} \), we have \( v_p(\binom{p^k}{l}) \geq k - v_p(l) = v_p(p^k / \gcd(p^k, l)) \), and the assertion follows.

(b) See [RS80, Cor. 4.3].

(c) Suppose that \( q p \log_p t | p^k \). Since \( p \log_p t \) is the largest p-power \( \leq t \), for every \( 1 \leq l \leq t \) we have \( q \gcd(p^k, l)|p^k \), so by (a), \( q | \binom{p^k}{l} \).

Conversely, if \( q \) divides \( \binom{p^k}{l} \) for \( l = p \log_p t \), then by (b), \( q \) divides \( p^k / l \).

(d) See e.g., [Fin47]. Note that the “if” part is contained in (c).

Proposition 2.3 (Sawin). Let \( s \) be a positive integer and let \( q > 1 \) be a p-power. Then the group \( U = U_s(\mathbb{Z}/q) \) has exponent \( qp \log_p s \).

Proof. Let \( p^r = qp \log_p s \) and observe that \( p^r > s \).

Consider an arbitrary matrix \( I_{s+1} + N \) in \( U \), where \( N \) is upper-triangular with zeros on the main diagonal. Thus \( N^{s+1} = 0 \). For every \( k \geq 0 \) and for \( t = \min(s, p^k) \), the binomial expansion formula implies that

\[
(I_{s+1} + N)^{p^k} = \sum_{l=0}^{p^k} \binom{p^k}{l} N^l = \sum_{l=0}^{t} \binom{p^k}{l} N^l.
\]

For \( k = r \) we have \( t = s \), and Proposition 2.2(c) implies that \( (I_{s+1} + N)^{p^r} = I_{s+1} \). Therefore the exponent of \( U \) divides \( p^r \).

On the other hand, take \( k = r - 1 \). As neither \( qp \log_p s \) nor \( pq^k \) divides \( p^k = p^{r-1} \), we have \( qp \log_p t \not| p^k \). Proposition 2.2(c) therefore yields \( 1 \leq l \leq t (\leq s) \) such that \( q \not| \binom{p^k}{l} \). Take \( N \) to be the \((s + 1) \times (s + 1)\)-matrix which is 1 on the super-diagonal and is 0 elsewhere. Then for \( 1 \leq i \leq j \leq s + 1 \) we have \((N^m)_{ij} = 1\), if \( j - i = m \), and \((N^m)_{ij} = 0\) otherwise. It follows from (2.2) that \( (I_{s+1} + N)^{p^{r-1}} \neq I_{s+1} \). Consequently, the exponent of \( U \) is exactly \( p^r \).
3. Pullbacks

As before, let \( n, s \) be integers such that \( 1 \leq s \leq n \) and \( n \geq 2 \), and set \( \mathbb{U} = \mathbb{U}_s(R) \) where \( R = \mathbb{Z}/p^{n-s+1} \). Let \( \text{pr}_{ij} : \mathbb{U} \to R \) denote the projection on the \((i,j)\)-entry, \( i \leq j \).

**Definition 3.1.** Given a profinite group \( G \) and a continuous homomorphism \( \rho : G \to \mathbb{U}_{[n,p]} \), let \( \rho^* : H^2(\mathbb{U}_{[n,p]}) \to H^2(G) \) be the induced homomorphism on the cohomology. We write \( \rho^* \gamma_{n,s} \) for the pullback of \( \gamma_{n,s} \) to \( H^2(G) \) under \( \rho \). We define \( H^2(G)_{n,s} \) to be the subset of \( H^2(G) \) consisting of all such pullbacks.

**3.2. Remarks.**

1. The pullback \( \rho^*(\gamma_{n,s}) \in H^2(G) \) corresponds to the central extension \([\text{Led05}, \text{p. 33}]\)

\[
0 \to \mathbb{Z}/p \to \mathbb{U} \times_{\mathbb{U}_{[n,p]}} G \to G \to 1,
\]

where the fiber product is with respect to the projection \( \mathbb{U} \to \mathbb{U}_{[n,p]} \) and \( \rho \).

2. In particular, \( \rho^*(\gamma_{n,s}) = 0 \) if and only if \((3.1)\) splits, which means that the embedding problem

\[
\begin{array}{ccc}
0 & \to & \mathbb{Z}/p \\
\downarrow & & \downarrow \rho \\
\mathbb{U} & \to & \mathbb{U}_{[n,p]} \\
\end{array}
\]

is solvable, i.e., there is continuous homomorphism \( \hat{\rho} \) making it commutative. Compare \([\text{Hoe68}, \text{1.1}]\).

**Example 3.3.** Bockstein elements. The Bockstein map

\[
\text{Bock}_{p^{n-1},G} : H^1(G, \mathbb{Z}/p^n) \to H^2(G)
\]

is the connecting homomorphism arising from the short exact sequence of trivial \( G \)-modules

\[
0 \to \mathbb{Z}/p \to \mathbb{Z}/p^n \to \mathbb{Z}/p^{n-1} \to 0.
\]

Now take \( s = 1 \), so \( R = \mathbb{Z}/p^n \), \( \mathbb{U} = \mathbb{U}_2(\mathbb{Z}/p^n) \cong \mathbb{Z}/p^n \) via the map \( \text{pr}_{1,2} \), and \( \mathbb{U}_{[n,p]} \cong \mathbb{Z}/p^{n-1} \) (see Lemma 2.1(a)). Hence the continuous homomorphisms \( \rho : G \to \mathbb{U}_{[n,p]} \) may be identified with the elements of \( H^1(G, \mathbb{Z}/p^{n-1}) \); namely, \( \rho \) corresponds to \( \text{pr}_{1,2} \circ \rho \in H^1(G, \mathbb{Z}/p^n) \). By \([\text{Efr17}, \text{Example 7.4(1)}]\), one has

\[
\rho^* \gamma_{n,1} = \text{Bock}_{p^{n-1},G}(\text{pr}_{1,2} \circ \rho).
\]

Thus

\[
H^2(G)_{n,1} = \text{Im}(\text{Bock}_{p^{n-1},G}).
\]
Example 3.4. Massey products. Suppose that \( n = s \geq 2 \), so \( U = U_n(\mathbb{Z}/p) \). The subgroup \( H^2(G)_{n,n} \) turns out to be related to the \( n \)-fold Massey product \( \langle \cdot, \ldots, \cdot \rangle : H^1(G)^n \to H^2(G) \). For a review on Massey products in the context of profinite cohomology we refer e.g., to [Efr14], which follows [Dwy75, \S 2] in the discrete setting. We recall that for \( \chi_1, \ldots, \chi_n \in H^1(G) \), the Massey product \( \langle \chi_1, \ldots, \chi_n \rangle \) is a subset of \( H^2(G) \), with the following properties:

(i) The product \( \langle \chi_1, \ldots, \chi_n \rangle \) consists exactly of the pullbacks \( \rho^* \gamma_{n,n} \), where \( \rho : G \to U^{[n,n]} \) is a continuous homomorphism such that \( \chi_i = \text{pr}_{i,i+1} \circ \rho, \ i = 1, 2, \ldots, n \) [Efr17, Example 7.4(2)].

(ii) In particular, one has \( \langle \chi_1, \ldots, \chi_n \rangle \neq \emptyset \) if and only if there is a continuous homomorphism \( \rho : G \to U^{[n,p]} \) such that \( \chi_i = \text{pr}_{i,i+1} \circ \rho, \ i = 1, \ldots, n. \)

(iii) In view of (i) and Remark 3.2(2), one has \( 0 \in \langle \chi_1, \ldots, \chi_n \rangle \) if and only if there is a continuous homomorphism \( \hat{\rho} : G \to U \) such that \( \chi_i = \text{pr}_{i,i+1} \circ \hat{\rho}, \ i = 1, \ldots, n. \)

(iv) When \( n = 2 \) and \( \rho : G \to U^{[2,p]} \) is the unique homomorphism such that \( \chi_1 = \text{pr}_{1,2} \circ \rho \) and \( \chi_2 = \text{pr}_{2,3} \circ \rho \), one has \( \rho^* \gamma_{2,2} = \chi_1 \cup \chi_2. \)

(v) When \( n = 3 \), if \( \langle \chi_1, \chi_2, \chi_3 \rangle \) is nonempty, then it is a coset in \( H^2(G) \) of its indeterminacy
\[
\chi_1 \cup H^1(G) + \chi_3 \cup H^1(G) = \{ \chi_1 \cup \psi_1 + \chi_3 \cup \psi_3 \mid \psi_1, \psi_3 \in H^1(G) \}.
\]

From (i) we immediately deduce that \( H^2(G)_{n,n} \) is the union of all \( n \)-fold Massey products in \( H^2(G) \).

In particular, take \( n = s = 2 \). By (iv) above,
\[
H^2(G)_{2,2} = H^1(G) \cup H^1(G) = \{ \chi_1 \cup \chi_2 \mid \chi_1, \chi_2 \in H^1(G) \}.
\]

4. Examples

First we recall from [FJ08, \S 17.4] the following terminology and facts on free profinite groups. Let \( G \) be a profinite group and \( X \) a set. A map \( f : X \to G \) converges to 1, if for every open normal subgroup \( N \) of \( G \), the set \( X \setminus f^{-1}(N) \) is finite.

We say that a profinite group \( S \) is a free profinite group on basis \( X \) with respect to a map \( \iota : X \to S \) if

(i) \( \iota : X \to S \) converges to 1 and \( \iota(X) \) generates \( S \) as a profinite group;

(ii) For every profinite group \( G \) and a map \( f : X \to G \) converging to 1, there is a unique continuous homomorphism \( \hat{f} : S \to G \) such that \( f = \hat{f} \circ \iota \) on \( X \).
A free profinite group $S = S_X$ on $X$ exists, and is unique up to a continuous isomorphism. Moreover, $\iota$ is then injective, and one may identify $X$ with its image in $S$.

**Example 4.1.** Let $S$ be a free profinite group, let $m > n$, and let $G = S^{[m,p]}$. We show that then $\rho^* = 0$ for every continuous homomorphism $\rho: G \to \mathbb{U}^{[n,p]}$, so in particular $\rho^* \gamma_{n,s} = 0$ for every $1 \leq s \leq n$. Since $H^2(S) = 0$, the five term exact sequence in profinite cohomology [NSW08, Prop. 1.6.7] implies that the transgression map $\text{trg}: H^1(S^{(n,p)})^S \to H^2(S^{[n,p]})$ is surjective. The functoriality of $\text{trg}$ gives rise to a commutative square

$$
\begin{array}{ccc}
H^1(S^{(n,p)})^S & \rightarrow & H^2(S^{[n,p]}) \\
\downarrow \text{res} & & \downarrow \text{inf} \\
H^1(S^{(m,p)})^S & \rightarrow & H^2(S^{[m,p]})
\end{array}
$$

(see [EMi11, §2B]). By [CEM12, Lemma 5.4], the map $\text{res}: H^1(S^{(n,p)})^S \to H^1(S^{(n+1,p)})^S$ is trivial, and therefore so is the left vertical map. It follows that the right vertical inflation map is also trivial.

Now let $\rho: S^{[m,p]} \to \mathbb{U}^{[n,p]}$ be a continuous homomorphism. The projectivity of $S$ yields a continuous homomorphism $\hat{\rho}: S \to \mathbb{U}$ such that the left square in the following diagram commutes:

$$
\begin{array}{ccc}
S & \rightarrow & S^{[m,p]} \\
\downarrow \hat{\rho} & & \downarrow \rho \\
\mathbb{U} & \rightarrow & \mathbb{U}^{[n,p]}
\end{array}
$$

Now $\hat{\rho}(S^{(n,p)}) \leq \mathbb{U}^{(n,p)}$, so $\hat{\rho}(S^{(n,p)})$ is mapped trivially into $\mathbb{U}^{[n,p]}$. It follows that $\rho$ factors via a homomorphism $\hat{\rho}: S^{[n,p]} \to \mathbb{U}^{[n,p]}$, as in the diagram. Then $\rho^* = \text{inf} \circ \hat{\rho}^*$. Since $\text{inf}$ is trivial, $\rho^* = 0$.

**Example 4.2.** Let $G = \hat{\mathbb{Z}}^{[n,p]} = \mathbb{Z}/p^{n-1}$. As this is a one-relator $p$-group, one has $\dim_{F_p} H^2(G) = 1$ [NSW08, Cor. 3.9.5]. Take $2 \leq s \leq n$. When $p = 2$ we assume further that $3 \leq s \leq n$. An elementary calculation shows that then $n - s + 1 + [\log_p s] \leq n - 1$. Hence, by Proposition 2.3, the exponent of $\mathbb{U} = \mathbb{U}_s(\mathbb{Z}/p^{n-s+1})$ divides $p^{n-1}$. Therefore the embedding problem (3.2) is solvable for every homomorphism $\rho: G \to \mathbb{U}^{[n,p]}$. By Remark 3.2(2), $\rho^* \gamma_{n,s} = 0$.

By contrast, when $s = 1$ we have $\mathbb{U} \cong \mathbb{Z}/p^n$, $\mathbb{U}^{[n,p]} \cong \mathbb{Z}/p^{n-1}$. Taking $\rho$ to be an isomorphism, we see that (3.2) is not solvable, so $\rho^* \gamma_{n,1} \neq 0$. 

Finally, suppose that \( p = n = 2 \), so \( G = \mathbb{Z}/2 \). Then \( \gamma_{2,2} \) corresponds to the short exact sequence

\[
0 \to \mathbb{Z}/2 \to D_4 \to (\mathbb{Z}/2)^2 \to 0,
\]

where \( D_4 \) is the dihedral group of order 8 and the kernel is its unique normal subgroup of order 2. Let \( \tau \) be an element of order 4 in \( D_4 \), and \( \bar{\tau} \) its image in \((\mathbb{Z}/2)^2\). Define a homomorphism \( \rho: \mathbb{Z}/2 \to (\mathbb{Z}/2)^2 \) by \( \rho(1) = \bar{\tau} \). Then (3.2) is not solvable, whence \( \rho^* \gamma_{2,2} \neq 0 \).

5. The indecomposable quotient

Let \( R \) be a unital commutative ring, and let \( A = \bigoplus_{s=0}^{\infty} A_s \) be a graded \( R \)-algebra. Let \( A_+ = \bigoplus_{s=1}^{\infty} A_s \). The proof of the following lemma is straightforward.

**Lemma 5.1.** The following \( R \)-submodules of \( A \) coincide:

(i) The submodule of \( A \) generated by all products \( aa' \), where \( a, a' \in A_+ \);

(ii) The submodule of \( A \) generated by all products \( aa' \), where \( a, a' \in A_+ \) are homogenous;

(iii) The submodule of \( A \) generated by all products \( aa' \), where \( a, a' \) are elements of a given set \( T \) of homogenous elements in \( A_+ \) which generates it as an \( R \)-module.

We denote this \( R \)-submodule by \( D \), and call it the submodule of weakly decomposable elements of \( A \). Since \( D \) is generated by homogenous elements, the quotient \( A_{\text{indec}} = A/D \) has the structure of a graded \( R \)-module, which we call the indecomposable quotient of \( A \). Note that \( D_1 = \{0\} \), so the graded module morphism \( A \to A_{\text{indec}} \) is an isomorphism in degree 1.

In particular, let \( X \) be a set, let \( X^* \) be as before the free monoid on \( X \), and let \( \bigoplus_{w \in X^*} R w \) be the free \( R \)-module on \( X^* \), graded by the length map on \( X^* \). It can be completed to unital associative graded algebras in the following two ways:

(1) The free associative \( R \)-algebra \( R\langle X \rangle \) over \( X \): Here the product is the concatenation in \( X^* \) (simply denoted by \( (u, v) \mapsto uv \)) extended by \( R \)-linearity, and the unit element is the unit element 1 of \( X^* \), i.e., the empty word. The embedding \( R \to R\langle X \rangle \) induces an isomorphism \( R \cong R\langle X \rangle_{\text{indec}} \) of graded \( R \)-modules (both concentrated in degree 0).

(2) The shuffle \( R \)-algebra \( \text{Sh}_R(X) \) on \( X \): Here the product is the shuffle product \( (u, v) \mapsto umv \) on \( X^* \) (see the Introduction) extended by \( R \)-linearity, and the unit element is again 1 ∈ \( X^* \).
Whereas $R\langle X \rangle_{\text{indec}}$ has a trivial structure, the structure of $\text{Sh}_R(X)_{\text{indec}}$ is deep, as we shall see in the sequel.

The above two constructions are dual in a bialgebra context – see [LV12, §1.3.2] for details.

6. Words

We fix a nonempty set $X$, considered as an alphabet, and fix a total order on $X$. Then the free monoid $X^*$ on $X$ is totally ordered with respect to the alphabetical order $\leq$ induced by the total order on $X$. As before, we consider its elements as words in the alphabet $X$. Let $X^s$ denote the set of all words $w$ of length $|w| = s$. Thus $X^0 = \{1\}$.

A nonempty word $w \in X^*$ is called a Lyndon word if it is smaller with respect to $\leq$ than all its non-trivial proper right factors (i.e., suffixes). We denote the set of all Lyndon words of length $s$ on $X$ by $\text{Lyn}_s(X)$.

The number of Lyndon words of length $s$ over $X$ can be expressed in terms of Witt’s necklace function, defined for integers $s, m \geq 1$ by

$$\varphi_s(m) = \frac{1}{s} \sum_{d|s} \mu(d)m^{s/d}.$$ 

Here $\mu$ is the Möbius function, defined by $\mu(d) = (-1)^k$, if $d$ is a product of $k$ distinct prime numbers, and $\mu(d) = 0$ otherwise. We also define $\varphi_s(\infty) = \infty$. Then one has [Reu93, Cor. 4.14]

$$|\text{Lyn}_s(X)| = \varphi_s(|X|).$$

(6.1)

Every word $w \in X^*$ can be uniquely written as a concatenation $w = u_1^{i_1} \cdots u_k^{i_k}$ of Lyndon words $u_1 > \cdots > u_k$, where $i_1, \ldots, i_k \geq 1$, and $u^i$ denotes the concatenation of $i$ copies of $u$ [Reu93, Th. 5.1 and Cor. 4.7]. Note that then $|w| = i_1|u_1| + \cdots + i_k|u_k|$. We define a non-associative polynomial

$$Q_w = \frac{1}{i_1! \cdots i_k!} u_1^{wi_1} \cdots u_k^{wi_k}.$$ 

in $\mathbb{Q}\langle X \rangle$, where $u^{wi}$ is the shuffle product of $i$ copies of $u$.

6.1. Remarks. (1) The polynomial $Q_w$ is homogenous of the same degree $i_1|u_1| + \cdots + i_k|u_k|$ as $w$.
(2) The coefficients of $Q_w$ are in fact non-negative integers [Reu93, p. 128].
(3) When $w$ is a Lyndon word, $Q_w = w$.
(4) If $w$ is not a Lyndon word, then $i_1! \cdots i_k! Q_w$ is weakly decomposable in $\text{Sh}_Z(X)$. 
We will need the following result by Radford [Rad79] and Perrin and Viennot (unpublished); see [Reu93, Th. 6.1].

**Theorem 6.2.** For every word $w$ one has $Q_w = w + \sum_{v<w} a_{v,w} v$ for some non-negative integers $a_{v,w}$.

Note that in this sum we may restrict ourselves to words $v$ of the same length $s$ as $w$.

Assume for a moment that $X$ is finite, and let $[Q_w]_{w \in X^s}$ and $[w]_{w \in X^s}$ denote the column matrices with respect to the lexicographic order on $X^s$. Theorem 6.2 gives an upper-triangular unipotent matrix $M$ with entries in $\mathbb{Z}$ such that $[Q_w]_{w \in X^s} = M [w]_{w \in X^s}$. Since $M$ is invertible over $\mathbb{Z}$, and $X^s$ is a $\mathbb{Z}$-linear basis of the homogeneous component $\mathbb{Z}\langle X \rangle_s$ of $\mathbb{Z}\langle X \rangle$ of degree $s$, the polynomials $(Q_w)_{w \in X^s}$ also form a $\mathbb{Z}$-linear basis of $\mathbb{Z}\langle X \rangle_s$. Thus

$$\mathbb{Z}\langle X \rangle_s = \bigoplus_{u \in X^s} \mathbb{Z} u = \bigoplus_{w \in X^s} \mathbb{Z} Q_w,$$

and the polynomials $(Q_w)_{w \in X^s}$ form a $\mathbb{Z}$-linear basis of $\mathbb{Z}\langle X \rangle$. By a limit argument, the same holds also when $X$ is infinite.

For the following proposition, note that the structural graded module epimorphism $\text{Sh}_\mathbb{Z}(X) \to \text{Sh}_\mathbb{Z}(X)_{\text{indec}}$ induces for every $s \geq 0$ epimorphisms of $\mathbb{Z}$-modules

$$\mathbb{Z}\langle X \rangle_s = \text{Sh}_\mathbb{Z}(X)_s \to \text{Sh}_\mathbb{Z}(X)_{\text{indec}, s} \otimes (\mathbb{Z}/p)$$

on the $s$-homogenous components.

**Proposition 6.3.** Suppose that $1 \leq s < p$. Then the images of the Lyndon words of length $s$ generate the $\mathbb{Z}/p$-module $\text{Sh}_\mathbb{Z}(X)_{\text{indec}, s} \otimes (\mathbb{Z}/p)$.

**Proof.** Consider $w \in X^s$ with its unique presentation $w = u_1^{i_1} \cdots u_k^{i_k}$ as a concatenation of Lyndon words as above. Then $1 \leq i_1, \ldots, i_k \leq s < p$, so $i_1! \cdots i_k!$ is invertible modulo $p$. If in addition $w \notin \text{Lyn}_s(X)$, then $i_1! \cdots i_k! Q_w$ is weakly indecomposable in $\text{Sh}_\mathbb{Z}(X)$ (Remark 6.1(4)). Therefore in this case, $Q_w$ has a trivial image in $\text{Sh}_\mathbb{Z}(X)_{\text{indec}, s} \otimes (\mathbb{Z}/p)$.

Hence the $\mathbb{Z}$-modules $\sum_{w \in \text{Lyn}_s(X)} \mathbb{Z} Q_w$ and $\sum_{w \in X^s} \mathbb{Z} Q_w$ have the same image in $\text{Sh}_\mathbb{Z}(X)_{\text{indec}, s} \otimes (\mathbb{Z}/p)$. By (6.2), this image is all of $\text{Sh}_\mathbb{Z}(X)_{\text{indec}, s} \otimes (\mathbb{Z}/p)$. \qed

**Example 6.4.** In Proposition 6.3 one cannot omit the assumption that $s < p$. Indeed, suppose that $X = \{x\}$ consists of a single letter. Then for every $s$, the set $X^s$ consists solely of the concatenation power $(x)^s = (x \cdots x)$ ($s$ times). Therefore $\text{Sh}_\mathbb{Z}(X)_s = \mathbb{Z}\langle X \rangle_s \cong \mathbb{Z}$ for every $s$. 

Let $D$ be the module of weakly decomposable elements in $\text{Sh}_Z(X)$.

In degree 1 we have $D_1 = \{0\}$, so $\text{Sh}_Z(X)_{\text{indec},1} = \text{Sh}_Z(X)_1 \cong \mathbb{Z}$, whence $\text{Sh}_Z(X)_{\text{indec},1} \otimes (\mathbb{Z}/p) \cong \mathbb{Z}/p$.

In degree $s \geq 2$ the $\mathbb{Z}$-module $D_s$ is generated by the shuffles $(x)^i w(x)^{s-i} = (s\choose i)(x)^s$, $i = 1, 2, \ldots, s - 1$. Hence $D_s = \mathbb{Z} h(s)(x)^s$, where

$$h(s) = \gcd\left\{\left(\begin{array}{c}s \\ i\end{array}\right) \mid 1 \leq i \leq s - 1\right\},$$

implying that $\text{Sh}_Z(X)_{\text{indec},s} \cong \mathbb{Z}/h(s)$. Now one has $p|h(s)$ if and only if $s$ is a $p$-power (Proposition 2.2(d)). Therefore $\text{Sh}_Z(X)_{\text{indec},s} \otimes (\mathbb{Z}/p)$ is $\mathbb{Z}/p$ if $s$ is a $p$-power, and is 0 otherwise.

Moreover, we have $\text{Lyn}_1(X) = \{(x)\}$ and $\text{Lyn}_s(X) = \emptyset$ for $s \geq 2$. Therefore when $s > 1$ is a $p$-power, the images of the Lyndon words of length $s$ do not generate $\text{Sh}_Z(X)_{\text{indec},s} \otimes (\mathbb{Z}/p)$. In particular, the image of $\text{Lyn}_p(X)$ does not generate $\text{Sh}_Z(X)_{\text{indec},p} \otimes (\mathbb{Z}/p)$.

7. Shuffl e relations

Given a commutative unital ring $R$, let $R\langle\langle X\rangle\rangle$ be the ring of formal power series in the set $X$ of non-commuting variables and with coefficients from $R$. Let $R\langle\langle X\rangle\rangle^*\times$ be its group of invertible elements. Note that for $x \in X$ one has $(1 + x) \sum_{i=0}^{\infty} (-1)^i x^i = 1$, so $1 + x \in R\langle\langle X\rangle\rangle^*.$

Assuming further that $R$ is finite, $R\langle\langle X\rangle\rangle^*\times$ is a profinite group in a natural way [Efr14, §]. Let $S$ be the free profinite group on the basis $X$ (see §). There is a unique continuous homomorphism, $\Lambda_R \colon S \to R\langle\langle X\rangle\rangle^*\times$, called the profinite Magnus homomorphism, satisfying $\Lambda_R(x) = 1 + x$ for every $x \in X$; see [Efr14, §5] for its detailed construction. This construction is functorial, in the sense that for every ring homomorphism $\varphi \colon R \to R'$ with an induced group homomorphism $\bar{\varphi} \colon R\langle\langle X\rangle\rangle^* \to R'\langle\langle X\rangle\rangle^*\times$ one has $\bar{\varphi} \circ \Lambda_R = \Lambda_{R'}$.

As in [Efr17, Example 7.4], for every integers $n, s$ such that $1 \leq s \leq n$ and $n \geq 2$, and every word $w = (x_1 \cdots x_s) \in X^s$, we associate a cohomology element $\alpha_{w,n} \in H^2(S^{[n,p]})$ as follows:

Let again $U = \bigcup_s R$ where $R = \mathbb{Z}/p^{n-s+1}$. First we define a map $\rho_R^w \colon S \to U$ by setting the entry $(\rho_R^w(\sigma))_{ij}$, where $i < j$, to be the coefficient of the subword $(x_i \cdots x_{j-1})$ in the power series $\Lambda_R(\sigma)$. The map $\rho_R^w$ is a continuous group homomorphism [Efr14, Lemma 7.5]. It induces a homomorphism $\tilde{\rho}_R^w \colon S^{[n,p]} \to \mathbb{U}^{[n,p]}$. Let $(\tilde{\rho}_R^w)^* \colon H^2(\mathbb{U}^{[n,p]}) \to H^2(S^{[n,p]})$ be the induced homomorphism on the cohomology groups. For $\gamma_{n,s}$ as in §2

THE LOWER $p$-CENTRAL SERIES AND SHUFFLE RELATIONS

11
we obtain the pullback
\[ \alpha_{w,n} = (\overline{\rho}_R^{w})^*(\gamma_{n,s}) \in H^2(S^{[n,p]}). \]

Fixing a total order on \( X \), the main theorem of [Efr17] states:

**Theorem 7.1.** For \( n \geq 2 \), the cohomology elements \( \alpha_{w,n} \), where \( w \) ranges over all Lyndon words of length \( 1 \leq |w| \leq n \) in the alphabet \( X \), form an \( \mathbb{F}_p \)-linear basis of \( H^2(S^{[n,p]}) \).

For \( f \in \mathbb{Z}\langle X \rangle \) and \( w \in X^* \), let \( f_w \) be the coefficient of \( w \) in \( f \). By [Efr17] Th. 9.4, one has the following shuffle relations:

**Theorem 7.2.** Let \( u, v \in X^* \) be nonempty words with \( s = |u| + |v| \leq n \). Then
\[ \sum_{w \in X^s} (uwv)_w \alpha_{w,n} = 0. \]

We now prove our main result, and at the same time strengthen Proposition [6.3]

**Theorem 7.3.** Let \( p \) be a prime number and \( n \) an integer such that \( 2 \leq n < p \). Then:

(a) The map \( w \mapsto \alpha_{w,n} \) induces a \( \mathbb{Z}/p \)-module isomorphism
\[ \bigoplus_{s=1}^{n} \text{Sh}_\mathbb{Z}(X)_{\text{indec},s} \otimes (\mathbb{Z}/p) \cong H^2(S^{[n,p]}). \]

(b) For every \( 1 \leq s < p \), the images of the Lyndon words of length \( s \) form a linear basis of the \( \mathbb{Z}/p \)-module \( \text{Sh}_\mathbb{Z}(X)_{\text{indec},s} \otimes (\mathbb{Z}/p) \).

**Proof.** For \( 1 \leq s \leq n \), the map \( X^s \to H^2(S^{[n,p]}), \ w \mapsto \alpha_{w,n} \), extends by linearity to a \( \mathbb{Z} \)-module homomorphism
\[ \Phi_s: \mathbb{Z}\langle X \rangle_s = \bigoplus_{w \in X^s} \mathbb{Z}w \to H^2(S^{[n,p]}). \]

Thus for \( f \in \mathbb{Z}\langle X \rangle_s \) one has
\[ \Phi_s(f) = \Phi_s\left( \sum_{w \in X^s} f_w w \right) = \sum_{w \in X^s} f_w \alpha_{w,n}. \]

By Theorem [7.2], \( \Phi_s(uvw) = 0 \) for any nonempty words \( u, v \in X^* \) with \( s = |u| + |v| \). Consequently, \( \Phi_s \) factors via \( \text{Sh}_\mathbb{Z}(X)_{\text{indec},s} \). Therefore it induces a \( \mathbb{F}_p \)-linear map
\[ (7.1) \quad \bar{\Phi}_s: \text{Sh}_\mathbb{Z}(X)_{\text{indec},s} \otimes (\mathbb{Z}/p) \to H^2(S^{[n,p]}). \]
By Proposition 6.3, for every $s$ the image of $\text{Lyn}_s(X)$ spans $\text{Sh}_Z(X)_{\text{indec},s} \otimes (\mathbb{Z}/p)$. Furthermore, by Theorem 7.1, the cohomology elements $\Phi_s(\bar{w})$, where $1 \leq s \leq n$ and $\bar{w} \in L_s$, form an $\mathbb{F}_p$-linear basis of $H^2(S^{[n,p]})$. It follows that $\bigoplus_{s=1}^n \Phi_s: \bigoplus_{s=1}^n \text{Sh}_Z(X)_{\text{indec},s} \otimes (\mathbb{Z}/p) \to H^2(S^{[n,p]})$ is an isomorphism, and the image of $\text{Lyn}_s(X)$ in facts form a basis of $\text{Sh}_Z(X)_{\text{indec},s} \otimes (\mathbb{Z}/p)$ for every $1 \leq s \leq n$.

From Theorem 7.3(b) and (6.1) we deduce:

**Corollary 7.4.** For $1 \leq s < p$ one has

$$\dim_{\mathbb{F}_p}(\text{Sh}_Z(X)_{\text{indec},s} \otimes (\mathbb{Z}/p)) = \varphi_s(|X|).$$

The next example shows that in part (a) of Theorem 7.3 one cannot omit the assumption that $n < p$ (for part (b) this has already been shown in Example 6.4).

**Example 7.5.** Suppose that $X = \{x\}$. Then $S^{[n,p]} = \mathbb{Z}^{[n,p]} \cong \mathbb{Z}/p^{n-1}$, whence $\dim_{\mathbb{F}_p} H^2(S^{[n,p]}) = 1$. On the other hand, Example 6.4 shows that

$$\dim_{\mathbb{F}_p} \text{Sh}_Z(X)_{\text{indec},1} \otimes (\mathbb{Z}/p) = \dim_{\mathbb{F}_p} \text{Sh}_Z(X)_{\text{indec},p} \otimes (\mathbb{Z}/p) = 1,$$

so there is no isomorphism as in Theorem 7.3(a).

Explicitly, Example 4.2 shows that when $p \neq 2$ and $n \geq p$, one has $\alpha_{w,n} = (\rho_{\mathbb{Z}/p,\rho^{1-p}+1})^* \gamma_{n,p} = 0$ for words $w$ of length $p$. Thus $\Phi_p$ is trivial on the nonzero summand $\text{Sh}_Z(X)_{\text{indec},p} \otimes (\mathbb{Z}/p)$.

Now suppose that $p = n = 2$. We have $\text{Bock}_{2,G}(\chi) = \chi \cup \chi$ for every profinite group $G$ and every $\chi \in H^1(G)$ [EMIl1 Lemma 2.4]. Also, using the functoriality of the Magnus homomorphism we get $\text{pr}_{1,2} \circ \rho_{\mathbb{Z}/4}^{(x)} = \text{pr}_{1,2} \circ \rho_{\mathbb{Z}/2}^{(xx)} = \text{pr}_{3,4} \circ \rho_{\mathbb{Z}/2}^{(xx)}$. Combining this with Examples 3.3 and 3.4 we obtain that

$$\Phi_1(x) = (\rho_{\mathbb{Z}/4}^{(x)})^* \gamma_{2,1} = \text{Bock}_{2,\mathbb{Z}/2}(\text{pr}_{1,2} \circ \rho_{\mathbb{Z}/4}^{(x)})$$

$$= (\text{pr}_{1,2} \circ \rho_{\mathbb{Z}/4}^{(x)}) \cup (\text{pr}_{1,2} \circ \rho_{\mathbb{Z}/4}^{(x)}) = (\text{pr}_{1,2} \circ \rho_{\mathbb{Z}/2}^{(xx)}) \cup (\text{pr}_{3,4} \circ \rho_{\mathbb{Z}/2}^{(xx)})$$

$$= (\rho_{\mathbb{Z}/2}^{(xx)})^* \gamma_{2,2} = \Phi_2(x).$$

This shows that the map $\bigoplus_{s=1}^n \Phi_s$ is not injective in this case as well.

8. Absolute Galois groups

Let $F$ be a field containing a root of unity of order $p$, and let $G = G_F$ be the absolute Galois group of $F$. The Merkurjev–Suslin theorem implies that every element of $H^2(G)$ decomposes as a sum $\sum_i \chi_i \cup \chi_i'$ of cup products, $\chi_i, \chi_i' \in H^1(G)$. In particular, for every continuous homomorphism $\rho: G \to \mathbb{Z}/p\mathbb{Z}$,
the pullback \( \rho^* \gamma_{n,s} \) has such a decomposition. While the Merkurjev–Suslin theorem is in general non-explicit, in a few cases the decomposition pattern of the \( \rho^* \gamma_{n,s} \) is known, and in fact is related to some rather deep facts in Galois cohomology and to structural results on absolute Galois groups.

**Example 8.1.** Let \( n = 2, s = 1 \). Here \( \mathbb{U} = \mathbb{U}_1(\mathbb{Z}/p^2) \cong \mathbb{Z}/p^2 \) and \( \mathbb{U}^{[2,p]} \cong \mathbb{Z}/p \) via \( \text{pr}_{1,2} \). Denote the group of \( p \)-th roots of unity by \( \mu_p \). Fix an isomorphism \( i: \mu_p \cong \mathbb{Z}/p \), let \( i^*: H^1(G, \mu_p) \to H^1(G) = H^1(G, \mathbb{Z}/p) \) be the induced isomorphism, and let \( \zeta = i^{-1}(1) \). The Kummer map \( \kappa: F^\times = H^0(G, F^\times_{\text{sep}}) \to H^1(G, \mu_p) \) is the connecting homomorphism arising from the short exact sequence

\[
1 \to \mu_p \to F^\times_{\text{sep}} \xrightarrow{p} F^\times_{\text{sep}} \to 1
\]

of discrete \( G \)-modules. By [EMi11, Prop. 2.6],

\[
\text{Bock}_{p,G} \cup \text{id} = \text{id} \cup \kappa
\]

as maps \( H^1(G) \otimes H^0(G, \mu_p) \to H^2(G, \mu_p) \). By the functoriality of the cup product [NSW08, Prop. 1.4.2], this can be restated as

\[
\text{(8.1)} \quad \text{Bock}_{p,G} \cup \text{id} = \text{id} \cup (i^* \circ \kappa \circ i^{-1})
\]

as maps \( H^1(G) \otimes H^0(G) \to H^2(G) \). This cohomological identity was a main ingredient in the restriction on the group-theoretic structure of absolute Galois groups given in [EMi11, Main Theorem]. It can be expressed in terms of the pullbacks \( \rho^* \gamma_{2,1} \); namely, for every continuous homomorphism \( \rho: G \to \mathbb{U}^{[2,p]} \), Example 3.3 and (8.1) (applied on \( (\text{pr}_{1,2} \circ \rho) \otimes 1 \)) give

\[
\rho^* \gamma_{2,1} = \text{Bock}_{p,G}(\text{pr}_{1,2} \circ \rho) = (\text{pr}_{1,2} \circ \rho) \cup i^*(\kappa(\zeta)).
\]

Therefore, in the notation of Definition 3.1

\[
H^2(G)_{2,1} = H^1(G) \cup i^*(\kappa(\zeta)).
\]

**Example 8.2.** When \( n = s = 2 \), we generally have \( \rho^* \gamma_{2,2} = (\text{pr}_{1,2} \circ \rho) \cup (\text{pr}_{2,3} \circ \rho) \), by Example 3.4(iv).

**Example 8.3.** Let \( n = s = 3 \) and \( \mathbb{U} = \mathbb{U}_3(\mathbb{Z}/p) \). It was shown in [Mat14], [EM17] and [MT16] (following earlier works by Hopkins, Wickelgren [HW15], Mináč and Tán) that if a 3-fold Massey product in \( H^2(G) = H^2(G_F) \) is nonempty, then it contains \( 0 \). This imposes another restriction on the possible group-theoretic structure of absolute Galois groups - see [MT17, §7]. The following proposition interprets this fact in terms of the pullbacks \( \rho^* \gamma_{3,3} \):
Proposition 8.4. Let $\chi_1, \chi_2 \in H^1(G)$. The set $\chi_1 \cup H^1(G) + \chi_2 \cup H^1(G)$ consists exactly of all the pullbacks $\rho^* \gamma_{3,3}$, where $\rho : G \to \mathbb{U}^{[3, p]}$ is a continuous homomorphism such that $\chi_1 = \text{pr}_{1,2} \circ \rho$ and $\chi_2 = \text{pr}_{3,4} \circ \rho$.

Consequently, $H(G)_{3,3}$ is the set $H^1(G) \cup H^1(G) + H^1(G) \cup H^1(G)$ of all sums of two cup products.

Proof. Let $\rho$ be as in the first assertion. By Example 3.4(i), the Massey product $\langle \text{pr}_{1,2} \circ \rho, \text{pr}_{2,3} \circ \rho, \text{pr}_{3,4} \circ \rho \rangle$ contains $\rho^* \gamma_{3,3}$, and in particular, is nonempty. By the above result, it contains 0. In view of Example 3.4(iv), it coincides with its indeterminicity, and in particular
\[
\rho^* \gamma_{3,3} \in (\text{pr}_{1,2} \circ \rho) \cup H^1(G) + (\text{pr}_{3,4} \circ \rho) \cup H^1(G) = \chi_1 \cup H^1(G) + \chi_2 \cup H^1(G).
\]

For the converse, note that since $\chi_1, \chi_2 : G \to \mathbb{Z}/p$ are continuous homomorphisms, the map
\[
\rho' = \begin{bmatrix}
1 & \chi_1 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & \chi_2 \\
0 & 0 & 0 & 1
\end{bmatrix} : G \to \mathbb{U}
\]
is also a continuous homomorphism. This shows that $0 \in \langle \chi_1, 0, \chi_2 \rangle$ (Example 3.3(iii)), so again
\[
\langle \chi_1, 0, \chi_2 \rangle = \chi_1 \cup H^1(G) + \chi_2 \cup H^1(G).
\]
Hence, by Example 3.4(i), every element of $\chi_1 \cup H^1(G) + \chi_2 \cup H^1(G)$ has the form $\rho^* (\gamma_{3,3})$ for some continuous homomorphism $\rho : G \to \mathbb{U}^{[3, p]}$ such that $\chi_1 = \text{pr}_{1,2} \circ \rho$ and $\chi_2 = \text{pr}_{3,4} \circ \rho$.

The second assertion of the proposition follows from the first one. \qed

8.5. Remarks. (1) In the previous discussion one can replace $G_F$ by the maximal pro-$p$ Galois group $G_F(p) = \text{Gal}(F(p)/F)$ of $F$, where $F(p)$ is the maximal pro-$p$ Galois extension of $F$. Indeed, inf : $H^i(G_F(p)) \to H^i(G_F)$ is an isomorphism for every $i$ [CEM12, Remark 8.2]. Moreover, there is a relative Kummer map $F^\times \to H^1(G_F(p), \mu_p)$ which is a connecting homomorphism arising from the exponentiation by $p$ map $F(p)^\times \to F(p)^\times$, and it commutes with $\kappa$ and the inflation map $H^1(G_F(p), \mu_p) \to H^1(G_F, \mu_p)$.

(2) It will be interesting to find in the absolute Galois group case explicit decompositions of $\rho^* \gamma_{n,s}$ as a sum of cup products for other values of $n, s$.  

THE LOWER $p$-CENTRAL SERIES AND SHUFFLE RELATIONS 15
References

[CEM12] S. K. Chebolu, I. Efrat, and J. Mináč, Quotients of absolute Galois groups which determine the entire Galois cohomology, Math. Ann. 352 (2012), 205–221.

[Dwy75] W. G. Dwyer, Homology, Massey products, and maps between groups, J. Pure Appl. Algebra 6 (1975), 177–190.

[Efr14] I. Efrat, The Zassenhaus filtration, Massey products, and representations of profinite groups, Adv. Math. 263 (2014), 389–411.

[Efr17] I. Efrat, The cohomology of canonical quotients of free groups and Lyndon words, Documenta Math. 22 (2017), 973–997.

[EM17] I. Efrat and E. Matzri, Triple Massey products and absolute Galois groups, J. Eur. Math Soc. (JEMS) 19 (2017), 3629–3640.

[EMi11] I. Efrat and J. Mináč, On the descending central sequence of absolute Galois groups, Amer. J. Math. 133 (2011), 1503–1532.

[EMi17] I. Efrat and J. Mináč, Galois groups and cohomological functors, Trans. Amer. Math. Soc. 369 (2017), 2697–2720.

[Fin47] N. J. Fine, Binomial coefficients modulo a prime, Amer. Math. Monthly 54 (1947), 589–592.

[FJ08] M. D. Fried and M. Jarden, Field arithmetic, Third edition, Springer, Berlin, 2008.

[Hoe68] K. Hoechsmann, Zum Einbettungsproblem, J. reine angew. Math. 229 (1968), 81–106.

[HW15] M. Hopkins and K. Wickelgren, Splitting varieties for triple Massey products, J. Pure Appl. Algebra 219 (2015), 1304–1319.

[Lab67] J. P. Labute, Classification of Demushkin groups, Canad. J. Math. 19 (1967), 106–132.

[Led05] A. Ledet, Brauer Type Embedding Problems, Fields Institute Monographs, vol. 21, American Mathematical Society, Providence, RI, 2005.

[LV12] J.-L. Loday and B. Vallette, Algebraic operads, Springer, Heidelberg, 2012.

[Mat14] E. Matzri, Triple Massey products in Galois cohomology (2014), available at arXiv:1411.4146

[MT16] J. Mináč and N. D. Tân, Triple Massey products vanish over all fields, J. London Math. Soc. 94 (2016), 909–932.

[MT17] J. Mináč and N. D. Tân, Triple Massey products and Galois theory, J. Eur. Math. Soc. (JEMS) 19 (2017), 255–284.

[NSW08] J Neukirch, A. Schmidt, and K. Wingberg, Cohomology of Number Fields, Second edition, Springer, 2008.

[Rad79] D. E. Radford, A natural ring basis for the shuffle algebra and an application to group schemes, J. Algebra 58 (1979), 432–454.

[Reu93] C. Reutenauer, Free Lie algebras, London Mathematical Society Monographs. New Series, vol. 7, The Clarendon Press, Oxford University Press, New York, 1993. Oxford Science Publications.

[RS80] G.-C. Rota and B. Sagan, Congruences derived from group action, Europ. J. Combinatorics 1 (1980), 67–76.
[Saw18] W. Sawin, *Order of unipotent matrices over \( \mathbb{Z}/q\mathbb{Z} \)*, MathOverflow, 2018. URL: https://mathoverflow.net/q/294231 (version: 2018-03-02).

[Top16] A. Topaz, *Reconstructing function fields from rational quotients of mod-1 Galois groups*, Math. Ann. **366** (2016), 337–385.

Mathematics Department, Ben-Gurion University of the Negev, P.O. Box 653, Be’er-Sheva 84105, Israel

E-mail address: efrat@math.bgu.ac.il