The Cohomology of Canonical Quotients of Free Groups and Lyndon Words

Ido Efrat

Received: April 26, 2016
Revised: April 11, 2017

Communicated by Ulf Rehmann

Abstract. For a prime number p and a free profinite group S, let $S^{(n,p)}$ be the nth term of its lower p-central filtration, and $S^{[n,p]}$ the corresponding quotient. Using tools from the combinatorics of words, we construct a canonical basis of the cohomology group $H^2(S^{[n,p]},\mathbb{Z}/p)$, which we call the Lyndon basis, and use it to obtain structural results on this group. We show a duality between the Lyndon basis and canonical generators of $S^{(n,p)}/S^{(n+1,p)}$. We prove that the cohomology group satisfies shuffle relations, which for small values of n fully describe it.

2010 Mathematics Subject Classification: Primary 12G05, Secondary 20J06, 68R15
Keywords and Phrases: Profinite cohomology, lower p-central filtration, Lyndon words, Shuffle relations, Massey products

[1]

1. Introduction

Let p be a fixed prime number. For a profinite group G one defines the lower p-central filtration $G^{(n,p)}$, $n=1,2,\ldots$, inductively by

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

Thus $G^{(n+1,p)}$ is the closed subgroup of G generated by the powers h^p and commutators $[g,h]=g^{-1}h^{-1}gh$, where $g\in G$ and $h\in G^{(n,p)}$. We also set $G^{[n,p]}=G/G^{(n,p)}$.

Now let S be a free profinite group on the basis X, and let $n\geq 2$. Then $S^{[n,p]}$ is a free object in the category of pro-p groups G with $G^{(n,p)}$ trivial. As with any pro-p group, the cohomology groups $H^l(S^{[n,p]})=H^l(S^{[n,p]},\mathbb{Z}/p)$, $l=1,2$, capture the main information on generators and relations, respectively,

[1]This work was supported by the Israel Science Foundation (grant No. 152/13).

in a minimal presentation of $S^{[n,p]}$. The group $H^1(S^{[n,p]})$ is just the dual $(S^{[2,p]})^\vee \cong \bigoplus_{x\in X}\mathbb{Z}/p$, and it remains to understand $H^2(S^{[n,p]})$.

When $n=2$ the quotient $S^{[2,p]}$ is an elementary abelian p-group, and the structure of $H^2(S^{[2,p]})$ is well-known. Namely, for $p>2$ one has an isomorphism

$$H^1(S^{[2,p]})\oplus \bigwedge^2 H^1(S^{[2,p]}) \xrightarrow{\sim} H^2(S^{[2,p]}),$$

which is the Bockstein map on the first component, and the cup product on the second component. Furthermore, taking a basis χ_x, $x\in X$, of $H^1(S^{[2,p]})$ dual to X, there is a fundamental duality between pth powers and commutators in the presentation of S and Bockstein elements and cup products, respectively, of the χ_x (see [NSW08, Ch. III, §9] for details). These facts have numerous applications in Galois theory, ranging from class field theory ([Koc02], [NSW08]), the works by Serre and Labute on the pro-p Galois theory of p-adic fields ([Ser63], [Lab67]), the structure theory of general absolute Galois groups ([MS96], [EM11]), the birational anabelian phenomena ([Bog91], [Top16]), Galois groups with restricted ramification ([Vog05], [Sch10]), and mild groups ([Lab06], [For11], [LM11]), to mention only a few of the pioneering works in these areas.

In this paper we generalize the above results from the case $n=2$ to arbitrary $n\geq 2$. Namely, we give a complete description of $H^2(S^{[n,p]})$ in terms of a canonical linear basis of this cohomology group. This basis is constructed using tools from the *combinatorics of words* – in particular, the LYNDON WORDS in the alphabet X, i.e., words which are lexicographically smaller than all their proper suffixes (for a fixed total order on X). We call it the LYNDON BASIS, and use it to prove several structural results on $H^2(S^{[n,p]})$, and in particular to compute its size (see below).

The Lyndon basis constructed here can be most naturally described in terms of central extensions, as follows: For $1\leq s\leq n$ let $\mathbb{U}$ denote the group of all unipotent upper-triangular $(s+1)\times(s+1)$-matrices over the ring $\mathbb{Z}/p^{n-s+1}$. There is a central extension

$$0\to\mathbb{Z}/p\to\mathbb{U}\to\mathbb{U}^{[n,p]}\to 1$$

(Proposition 6.3). It corresponds to a cohomology element $\gamma_{n,s}\in H^2(\mathbb{U}^{[n,p]})$. For a profinite group G and a continuous homomorphism $\rho\colon G\to\mathbb{U}$ we write $\bar\rho\colon G^{[n,p]}\to\mathbb{U}^{[n,p]}$ for the induced homomorphism, and $\bar\rho^*\gamma_{n,s}$ for the pullback to $H^2(G^{[n,p]})$. Now for any word $w=(x_1\cdots x_s)$ in the alphabet X we define a homomorphism $\rho^w\colon S\to\mathbb{U}$ by setting the entry $(\rho^w(\sigma))_{ij}$ to be the coefficient of the subword $(x_i\cdots x_{j-1})$ in the power series $\Lambda(\sigma)$, where $\Lambda\colon S\to(\mathbb{Z}/p^{n-s+1})\langle\langle X\rangle\rangle^\times$ is the MAGNUS HOMOMORPHISM, defined on the generators $x\in X$ by $\Lambda(x)=1+x$ (see §3 and §6 for more details). The Lyndon basis is now given by:

MAIN THEOREM. *The pullbacks $\alpha_{w,n}=(\bar\rho^w)^*\gamma_{n,s}$, where w ranges over all Lyndon words of length $1\leq s\leq n$ in the alphabet X, form a linear basis of $H^2(S^{[n,p]})$ over $\mathbb{Z}/p$.*

We further show a duality between the Lyndon basis and certain canonical elements $\sigma_w \in S^{(n,p)}$, with w a Lyndon word of length $\leq n$, generalizing the above mentioned duality in the case $n = 2$ (see Corollary 8.3).

The cohomology elements $\bar{\rho}^*\gamma_{n,s}$ include the Bockstein elements (for $s = 1$), the cup products (for $n = s = 2$), and more generally, the elements of n-fold Massey products in $H^2(G^{[n,p]})$ (for $n = s \geq 2$); see Examples 7.4. The full spectrum $\bar{\rho}^*\gamma_{n,s}$, $1 \leq s \leq n$, appears to give new significant "external" objects in profinite cohomology, which to our knowledge have not been investigated so far in general.

Lyndon words are known to have tight connections with the SHUFFLE ALGEBRA, and indeed, the $\alpha_{w,n}$ for arbitrary words w of length $\leq n$ in X satisfy natural SHUFFLE RELATIONS (Theorem 9.4). In §10-§11 we show that for $n = 2, 3$ these shuffle relations fully describe $H^2(S^{[n,p]})$, provided that $p > 2$, $p > 3$, respectively (for $n = 2$ this was essentially known). Interestingly, related considerations arise also in the context of *multiple zeta values*, see e.g. [MP00], although we are not aware of a direct connection.

The Lyndon words on X form a special instance of *Hall sets*, which are well-known to have fundamental role in the structure theory of free groups and free Lie algebras (see [Reu93], [Ser92]). In addition, the Lyndon words have a TRIANGULARITY PROPERTY (see Proposition 4.4(b)). This property allows us to construct certain upper-triangular unipotent matrices that express a (semi-)duality between the σ_w and the cohomology elements $\alpha_{w,n}$.

We now outline the proof that the $\alpha_{w,n}$ form a linear basis of $H^2(S^{[n,p]})$. For simplicity we assume for the moment that X is finite. To each Lyndon word w of length $1 \leq s \leq n$ one associates in a canonical way an element τ_w of the s-th term of the lower central series of S (see §4). The cosets of the powers $\sigma_w = \tau_w^{p^{n-s}}$ generate $S^{(n,p)}/S^{(n+1,p)}$ (Theorem 5.3). Using the special structure of the lower p-central filtration of $\mathbb{U}$ we define for any two Lyndon words w, w' of length $\leq n$ a value $\langle w, w' \rangle_n \in \mathbb{Z}/p$ (see §6). The triangularity property of Lyndon words implies that the matrix $\big(\langle w, w' \rangle_n\big)$ is unipotent upper-triangular, whence invertible. Turning now to cohomology, we define a natural perfect pairing

$$(\cdot,\cdot)_n \colon S^{(n,p)}/S^{(n+1,p)} \times H^2(S^{[n,p]}) \to \mathbb{Z}/p.$$

Cohomological computations show that, for Lyndon words w, w' of length $\leq n$, one has $\langle w, w' \rangle_n = (\sigma_w, \alpha_{w',n})_n$. Hence the matrix $\big((\sigma_w, \alpha_{w',n})_n\big)$ is also invertible. We then conclude that the $\alpha_{w',n}$ form a basis of $H^2(S^{[n,p]})$ (Theorem 8.5). This immediately determines the dimension of the latter cohomology group, in terms of Witt's NECKLACE FUNCTION, which counts the number of Lyndon words over X of a given length (Corollary 8.6).

In the special case $n = 2$, the theory developed here generalizes the above description of $H^2(S^{[2,p]})$ in terms of the Bockstein map and cup products (see §10 for details). Namely, the matrix $(\langle w, w' \rangle_2)$ is the identity matrix, which gives the above duality between pth powers/commutators and Bockstein elements/cup products. Likewise, the shuffle relations just recover the basic fact that the cup product factors via the exterior product.

In §11 we describe our theory explicitly also for the (new) case $n = 3$.

While here we focus primarily on free profinite groups, it may be interesting to study the canonical elements $\bar{\rho}_*\gamma_{n,s}$ for more general profinite groups G, in particular, when $G = G_F$ is the absolute Galois group of a field F. For instance, when $n = 2$, they were used in [EM11] (following [MS96] and [AKM99]) and [CEM12] to describe the quotient $G_F^{[3,p]}$. Triple Massey products for G_F (which correspond to the case $n = s = 3$) were also extensively studied in recent years – see [EM15], [MT15b], [MT16], [MT17], and [Wic12] and the references therein.

I thank Claudio Quadrelli and the anonymous referee for their careful reading of this paper and for their very valuable comments and suggestions on improving the exposition.

2. Words

Let X be a nonempty set, considered as an alphabet. Let X^* be the free monoid on X. We view its elements as associative words on X. The length of a word w is denoted by $|w|$. We write $\emptyset$ for the empty word, and ww' for the concatenation of words w and w'.

Recall that a MAGMA is a set $\mathcal{M}$ with a binary operation $(\cdot,\cdot)\colon \mathcal{M}\times\mathcal{M}\to\mathcal{M}$. A morphism of magmas is a map which commutes with the associated binary operations. There is a FREE MAGMA $\mathcal{M}_X$ on X, unique up to an isomorphism; that is, $X\subseteq\mathcal{M}_X$, and for every magma $(\cdot,\cdot)\colon N\times N\to N$ and a map $f_0\colon X\to N$ there is a magma morphism $f\colon\mathcal{M}_X\to N$ extending f_0. See [Ser92, Ch. IV, §1] for an explicit construction of $\mathcal{M}_X$. The elements of $\mathcal{M}_X$ may be viewed as non-associative words on X.

The monoid X^* is a magma with respect to concatenation, so the universal property of $\mathcal{M}_X$ gives rise to a unique magma morphism $f\colon\mathcal{M}_X\to X^*$, called the FOLIAGE (or BRACKETS DROPPING) map, such that $f(x)=x$ for $x\in X$.

Let $\mathcal{H}$ be a subset of $\mathcal{M}_X$ and $\leq$ a total order on $\mathcal{H}$. We say that $(\mathcal{H},\leq)$ is a HALL SET IN $\mathcal{M}_X$, if the following conditions hold [Reu93, §4.1]:

(i) $X\subseteq\mathcal{H}$;
(ii) If $h=(h',h'')\in\mathcal{H}\setminus X$, then $h<h''$;
(iii) For $h=(h',h'')\in\mathcal{M}_X\setminus X$, one has $h\in\mathcal{H}$ if and only if
- $h',h''\in\mathcal{H}$ and $h'<h''$; and
- either $h'\in X$, or $h'=(v,u)$ where $u\geq h''$.

Given a Hall set $(\mathcal{H},\leq)$ in $\mathcal{M}_X$ we call $H=f(\mathcal{H})$ a HALL SET IN X^*.

Every $w\in H$ can be written as $w=f(h)$ for a *unique* $h\in\mathcal{H}$ [Reu93, Cor. 4.5]. If $w\in H\setminus X$, then we can uniquely write $h=(h',h'')$ with $h',h''\in\mathcal{H}$, and call $w=w'w''$, where $w'=f(h')$ and $w''=f(h'')$, the STANDARD FACTORIZATION of w [Reu93, p. 89].

Next we fix a total order $\leq$ on X, and define a total order $\leq_{\mathrm{alp}}$ (the ALPHABETICAL order) on X^* as follows: Let $w_1, w_2 \in X^*$. Then $w_1 \leq_{\mathrm{alp}} w_2$ if and only if $w_2 = w_1 v$ for some $v \in X^*$, or $w_1 = v x_1 u_1$, $w_2 = v x_2 u_2$ for some words v, u_1, u_2 and some letters $x_1, x_2 \in X$ with $x_1 < x_2$. Note that the restriction of $\leq_{\mathrm{alp}}$ to X^n is the lexicographic order.
In addition, we order $\mathbb{Z}_{\geq 0} \times X^*$ lexicographically with respect to the usual order on $\mathbb{Z}_{\geq 0}$ and the order $\leq_{\mathrm{alp}}$ on X^*. We then define a second total order $\preceq$ on X^* by setting

$$w_1 \preceq w_2 \iff (|w_1|, w_1) \leq (|w_2|, w_2) \tag{2.1}$$

with respect to the latter order on $\mathbb{Z}_{\geq 0} \times X^*$.
A nonempty word $w \in X^*$ is called a LYNDON WORD if it is smaller in $\leq_{\mathrm{alp}}$ than all its non-trivial proper right factors. Equivalently, no non-trivial rotation leaves w invariant, and w is lexicographically strictly smaller than all its rotations $\neq w$ ([CFL58, Th. 1.4], [Reu93, Cor. 7.7]). We denote the set of all Lyndon words on X by $\mathrm{Lyn}(X)$, and the set of all such words of length n (resp., $\leq n$) by $\mathrm{Lyn}_n(X)$ (resp., $\mathrm{Lyn}_{\leq n}(X)$). The set $\mathrm{Lyn}(X)$, totally ordered with respect to $\leq_{\mathrm{alp}}$, is a Hall set [Reu93, Th. 5.1].

EXAMPLE 2.1. The Lyndon words of length ≤ 4 on X are

$$\begin{aligned}
&(x) \text{ for } x \in X,\\
&(xy), (xxy), (xyy), (xxxy), (xxyy), (xyyy) \text{ for } x, y \in X,\ x < y,\\
&(xyz), (xzy), (xxyz), (xxzy), (xyxz), (xyyz), (xyzy), (xyzz),\\
&\qquad (xzyy), (xzyz), (xzzy) \text{ for } x, y, z \in X,\ x < y < z,\\
&(xyzt), (xytz), (xzyt), (xzty), (xtyz), (xtzy) \text{ for } x, y, z, t \in X,\ x < y < z < t
\end{aligned}$$

The NECKLACE MAP (also called the WITT MAP) is defined for integers $n, m \geq 1$ by

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

Here μ 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; Alternatively, $1/\zeta(s) = \sum_{n=1}^{\infty} \mu(n)/n^s$, where $\zeta(s)$ is the Riemann zeta function and s is a complex number with real part > 1. When $m = q$ is a prime power, $\varphi_n(q)$ also counts the number of irreducible monic polynomials of degree n over a field of q elements [Reu93, §7.6.2]. We also define $\varphi_n(\infty) = \infty$. One has [Reu93, Cor. 4.14]

$$|\mathrm{Lyn}_n(X)| = \varphi_n(|X|). \tag{2.2}$$

3. Power series

We fix a commutative unital ring R. Recall that a bilinear map $M \times N \to R$ of R-modules is NON-DEGENERATE if its left and right kernels are trivial, i.e., the induced maps $M \to \mathrm{Hom}(N, R)$ and $N \to \mathrm{Hom}(M, R)$ are injective. The bilinear map is PERFECT if these two maps are isomorphisms.

Let $R\langle X\rangle$ be the free associative R-algebra on X. We may view its elements as polynomials over R in the non-commuting variables $x \in X$. The additive group of $R\langle X\rangle$ is the free R-module on the basis X^*. We grade $R\langle X\rangle$ by total degree. Let $R\langle\langle X\rangle\rangle$ be the ring of all formal power series in the non-commuting variables $x \in X$ and coefficients in R. For $f \in R\langle\langle X\rangle\rangle$ we write f_w for the coefficient of f at $w \in X^*$. Thus $f = \sum_{w\in X^*} f_w w$. There are natural embedings $X^* \subseteq R\langle X\rangle \subseteq R\langle\langle X\rangle\rangle$, where we identify $w \in X^*$ with the series f such that $f_w = 1$ and $f_{w'} = 0$ for $w' \neq w$. There is a well-defined non-degenerate bilinear map of R-modules

$$R\langle\langle X\rangle\rangle \times R\langle X\rangle \to R, \quad (f,g) \mapsto \sum_{w\in X^*} f_w g_w; \tag{3.1}$$

See [Reu93, p. 17]. For every integer $n \geq 0$, it restricts to a non-degenerate bilinear map on the homogenous components of degree n.

We may identify the additive group of $R\langle\langle X\rangle\rangle$ with R^{X^*} via the map $f \mapsto (f_w)_w$. When R is equipped with a profinite ring topology (e.g. when R is finite), the product topology on R^{X^*} induces a profinite group topology on $R\langle\langle X\rangle\rangle$. Moreover, the multiplication map of $R\langle\langle X\rangle\rangle$ is continuous, making it a profinite ring. The group $R\langle\langle X\rangle\rangle^\times$ of all invertible elements in $R\langle\langle X\rangle\rangle$ is then a profinite group.

Next we recall from [FJ08, §17.4] the following terminology and facts on free profinite groups. Let G be a profinite group and X a set. A map $\psi\colon X \to G$ CONVERGES TO 1, if for every open normal subgroup N of G, the set $X\setminus\psi^{-1}(N)$ is finite. We say that a profinite group S is a FREE PROFINITE GROUP ON BASIS X with respect to a map $\iota\colon X \to S$ if

(i) $\iota\colon X \to S$ converges to 1 and $\iota(X)$ generates S as a profinite group;
(ii) For every profinite group G and a map $\psi\colon X \to G$ converging to 1, there is a unique continuous homomorphism $\hat{\psi}\colon S \to G$ such that $\psi = \hat{\psi}\circ\iota$ on X.

A free profinite group on X exists, and is unique up to a continuous isomorphism. We denote it by S_X. The map ι is then injective, and we identify X with its image in S_X.

We define the (profinite) MAGNUS HOMOMORPHISM $\Lambda_{X,R}\colon S_X \to R\langle\langle X\rangle\rangle^\times$ as follows (compare [Efr14, §5]):

Assume first that X is finite. For $x \in X$ one has $1 = (1+x)\sum_{i=0}^\infty (-1)^i x^i$ in $R\langle\langle X\rangle\rangle$, so $1+x \in R\langle\langle X\rangle\rangle^\times$. Hence, by (ii), the map $\psi\colon X \to R\langle\langle X\rangle\rangle^\times$, $x \mapsto 1+x$, uniquely extends to a continuous homomorphism $\Lambda_{X,R}\colon S_X \to R\langle\langle X\rangle\rangle^\times$.

Now suppose that X is arbitrary. Let Y range over all finite subsets of X. The map $\psi\colon X \to S_Y$, which is the identity on Y and 1 on $X\setminus Y$, converges to 1. Hence it extends to a unique continuous group homomorphism $S_X \to S_Y$. Also, there is a unique continuous R-algebra homomorphism $R\langle\langle X\rangle\rangle \to R\langle\langle Y\rangle\rangle$, which is the identity on Y and 0 on $X\setminus Y$. Then

$$S_X = \varprojlim S_Y, \quad R\langle\langle X\rangle\rangle = \varprojlim R\langle\langle Y\rangle\rangle, \quad R\langle\langle X\rangle\rangle^\times = \varprojlim R\langle\langle Y\rangle\rangle^\times.$$

We define $\Lambda_{X,R} = \varprojlim \Lambda_{Y,R}$. It is functorial in both X and R in the natural way. Note that $\Lambda_{X,R}(x) = 1 + x$ for $x \in X$.
In the sequel, X will be fixed, so we abbreviate $S = S_X$ and $\Lambda_R = \Lambda_{X,R}$.

For $\sigma \in S$ and a word $w \in X^*$ we denote the coefficient of w in $\Lambda_R(\sigma)$ by $\epsilon_{w,R}(\sigma)$. Thus

$$\Lambda_R(\sigma) = \sum_{w \in X^*} \epsilon_{w,R}(\sigma) w.$$

By the construction of Λ_R, we have $\epsilon_{\emptyset,R}(\sigma) = 1$. Since Λ_R is a homomorphism, for every $\sigma, \tau \in S$ and $w \in X^*$ one has

$$\epsilon_{w,R}(\sigma\tau) = \sum_{w=u_1u_2} \epsilon_{u_1,R}(\sigma)\epsilon_{u_2,R}(\tau). \tag{3.2}$$

We will also need the classical *discrete* version of the Magnus homomorphism. To define it, assume that X is finite, and let F_X be the free group on basis X. There is a natural homomorphism $F_X \to S_X$. The DISCRETE MAGNUS HOMOMORPHISM $\Lambda_{\mathbb{Z}}^{\mathrm{disc}} \colon F_X \to \mathbb{Z}\langle\langle X \rangle\rangle^\times$ is defined again by $x \mapsto 1 + x$. There is a commutative square

$$\begin{tikzcd} F_X \arrow[r] \arrow[d, "\Lambda_{\mathbb{Z}}^{\mathrm{disc}}"'] & S_X \arrow[d, "\Lambda_{\mathbb{Z}_p}"] \\ \mathbb{Z}\langle\langle X \rangle\rangle^\times \arrow[r, hook] & \mathbb{Z}_p\langle\langle X \rangle\rangle^\times. \end{tikzcd} \tag{3.3}$$

4. Lie algebra constructions

Recall that the LOWER CENTRAL FILTRATION $G^{(n,0)}$, $n = 1, 2, \ldots$, of a profinite group G is defined inductively by

$$G^{(1,0)} = G, \quad G^{(n+1,0)} = [G^{(n,0)}, G].$$

Thus $G^{(n+1,0)}$ is generated as a profinite group by all elements of the form $[\sigma, \tau]$ with $\sigma \in G^{(n,0)}$ and $\tau \in G$. One has $[G^{(n,0)}, G^{(m,0)}] \le G^{(n+m,0)}$ for every $n, m \ge 1$ (compare [Ser92, Part I, Ch. II, §3]).

PROPOSITION 4.1. *Let $S = S_X$ and let $\sigma \in S$. Then:*

(a) *$\sigma \in S^{(n,0)}$ if and only if $\epsilon_{w,\mathbb{Z}_p}(\sigma) = 0$ for every $w \in X^*$ with $1 \le |w| < n$;*

(b) *$\sigma \in S^{(n,p)}$ if and only if $\epsilon_{w,\mathbb{Z}_p}(\sigma) \in p^{n-|w|}\mathbb{Z}_p$ for every $w \in X^*$ with $1 \le |w| < n$.*

Proof. In the discrete case (a) and (b) are due to Grün and Magnus (see [Ser92, Part I, Ch. IV, th. 6.3]) and Koch [Koc60], respectively. The results in the profinite case follow by continuity.
For other approaches see [Mor12, Prop. 8.15], [CE16, Example 4.5], and [MT15a, Lemma 2.2(d)]. □

We will need the following profinite analog of [Fen83, Lemma 4.4.1(iii)].

LEMMA 4.2. *Let $\sigma \in S^{(n,0)}$ and $\tau \in S^{(m,0)}$, and let $w \in X^*$ have length $n+m$. Write $w = u_1u_2 = u_2'u_1'$ with $|u_1| = |u_1'| = n$ and $|u_2| = |u_2'| = m$. Then*

$$\epsilon_{w,\mathbb{Z}_p}([\sigma,\tau]) = \epsilon_{u_1,\mathbb{Z}_p}(\sigma)\epsilon_{u_2,\mathbb{Z}_p}(\tau) - \epsilon_{u_2',\mathbb{Z}_p}(\tau)\epsilon_{u_1',\mathbb{Z}_p}(\sigma).$$

Proof. By Proposition 4.1(a), we may write $\Lambda_{\mathbb{Z}_p}(\sigma) = 1 + P + O(n+1)$ and $\Lambda_{\mathbb{Z}_p}(\tau) = 1 + Q + O(m+1)$, where $P, Q \in \mathbb{Z}_p\langle\langle X\rangle\rangle$ are homogenous of degrees n, m, respectively, and where $O(r)$ denotes a power series containing only terms of degree $\geq r$. Then

$$\Lambda_{\mathbb{Z}_p}([\sigma,\tau]) = 1 + PQ - QP + O(n+m+1).$$

(compare e.g., [Mor12, Proof of Prop. 8.5]). By (3.2), it follows that

$$\begin{aligned}\epsilon_{w,\mathbb{Z}_p}([\sigma,\tau]) &= (PQ-QP)_w = P_{u_1}Q_{u_2} - Q_{u_2'}P_{u_1'}\\ &= \epsilon_{u_1,\mathbb{Z}_p}(\sigma)\epsilon_{u_2,\mathbb{Z}_p}(\tau) - \epsilon_{u_2',\mathbb{Z}_p}(\tau)\epsilon_{u_1',\mathbb{Z}_p}(\sigma).\end{aligned}$$

□

The commutator map induces on the graded ring $\bigoplus_{n=1}^{\infty} S^{(n,0)}/S^{(n+1,0)}$ a graded Lie algebra structure [Ser92, Part I, Ch. II, Prop. 2.3]. Let $\mathfrak{d}$ be the ideal in the $\mathbb{Z}_p$-algebra $\mathbb{Z}_p\langle\langle X\rangle\rangle$ generated by X. Then $\bigoplus_{n=1}^{\infty}\mathfrak{d}^n/\mathfrak{d}^{n+1}$ is a Lie algebra with the Lie brackets defined on homogenous components by $[\bar f, \bar g] = \overline{fg - gf}$ for $f \in \mathfrak{d}^n$, $g \in \mathfrak{d}^m$ [Ser92, p. 25]. By Proposition 4.1(a), $\Lambda_{\mathbb{Z}_p}$ induces a graded $\mathbb{Z}_p$-algebra homomorphism

$$\mathrm{gr}\,\Lambda_{\mathbb{Z}_p}\colon \bigoplus_{n=1}^{\infty} S^{(n,0)}/S^{(n+1,0)} \to \bigoplus_{n=1}^{\infty}\mathfrak{d}^n/\mathfrak{d}^{n+1},\ \sigma S^{(n+1,0)} \mapsto \sum_{|w|=n}\epsilon_{w,\mathbb{Z}_p}(\sigma) + \mathfrak{d}^{n+1}.$$

Then Lemma 4.2 means that gr $\Lambda_{\mathbb{Z}_p}$ is a Lie algebra homomorphism.

For $w \in \mathrm{Lyn}(X)$ we inductively define an element τ_w of S and a non-commutative polynomial $P_w \in \mathbb{Z}\langle X\rangle \subseteq \mathbb{Z}_p\langle X\rangle$ as follows:

- If $w = (x)$ has length 1, then $\tau_w = x$ and $P_w = x$;
- If $|w| > 1$, then we take the standard factorization $w = w'w''$ of w with respect to the Hall set $\mathrm{Lyn}(X)$ (see §2), and set

$$\tau_w = [\tau_{w'}, \tau_{w''}], \qquad P_w = P_{w'}P_{w''} - P_{w''}P_{w'}.$$

For $w \in \mathrm{Lyn}_n(X)$ one has $\tau_w \in S^{(n,0)}$. Moreover:

PROPOSITION 4.3. *Let $n \geq 1$. The cosets of τ_w, with $w \in \mathrm{Lyn}_n(X)$, generate $S^{(n,0)}/S^{(n+1,0)}$.*

Proof. See [Reu93, Cor. 6.16] for the discrete version. The profinite version follows by taking closure. □

Let $\leq_{\mathrm{alp}}$ and $\preceq$ be the total orders on X^* defined in §2. The importance of the Lyndon words in our context, beside forming a Hall set, is part (b) of the following Proposition, called the TRIANGULARITY property.

PROPOSITION 4.4. *Let $w \in \mathrm{Lyn}(X)$. Then*

(a) *$\Lambda_{\mathbb{Z}_p}(\tau_w) - 1 - P_w$ is a combination of words of length $> |w|$.*

(b) *$P_w - w$ is a combination of words of length $|w|$ which are strictly larger than w with respect to $\leq_{\mathrm{alp}}$.*

(c) *$\Lambda_{\mathbb{Z}_p}(\tau_w) - 1 - w$ is a combination of words which are strictly larger than w in $\preceq$.*

Proof. (a) Since $\mathrm{gr}\,\Lambda_{\mathbb{Z}_p}$ is a Lie algebra homomorphism, for $w \in \mathrm{Lyn}_n(X)$ we have by induction

$$(\mathrm{gr}\,\Lambda_{\mathbb{Z}_p})(\tau_w S^{(n+1,0)}) = P_w + \mathfrak{d}^{n+1},$$

and the assertion follows. See also [Reu93, Lemma 6.10(ii)].

(b) See [Reu93, Th. 5.1] and its proof.

(c) This follows from (a) and (b). □

5. Generators for $S^{(n,p)}/S^{(n+1,p)}$

Let π be an indeterminate over the ring $\mathbb{Z}/p$ and let $\mathbb{Z}/p[\pi]$ be the polynomial ring. Let $A_\bullet = \bigoplus_{n=1}^{\infty} A_n$ be a graded Lie $\mathbb{Z}/p$-algebra with Lie bracket $[\cdot,\cdot]$. Suppose that there is a map $\mathbb{Z}/p[\pi] \times A_\bullet \to A_\bullet$, $\quad (\alpha, \xi) \mapsto \alpha\xi$, which is $\mathbb{Z}/p$-linear in $\mathbb{Z}/p[\pi]$, such that $\pi\xi \in A_{s+1}$ for $\xi \in A_s$, and such that for every $\xi_1, \xi_2 \in A_s$,

$$\pi(\xi_1 + \xi_2) = \begin{cases} \pi\xi_1 + \pi\xi_2, & \text{if } p > 2 \text{ or } s > 1, \\ \pi\xi_1 + \pi\xi_2 + [\xi_1, \xi_2], & \text{if } p = 2,\ s = 1. \end{cases} \tag{5.1}$$

By induction, this extends to:

Lemma 5.1. *Let $r, k, s \geq 1$ and let $\xi_1, \ldots, \xi_k \in A_s$. Then*

$$\pi^r\Big(\sum_{i=1}^{k} \xi_i\Big) = \begin{cases} \sum_{i=1}^{k} \pi^r \xi_i, & \text{if } p > 2 \text{ or } s > 1, \\ \sum_{i=1}^{k} \pi^r \xi_i + \sum_{i<j} \pi^{r-1}[\xi_i, \xi_j], & \text{if } p = 2,\ s = 1. \end{cases}$$

We write $\langle T \rangle$ for the submodule of $A_\bullet$ generated by a subset T.

Lemma 5.2. *Let $n \geq 2$ and for each $1 \leq s \leq n$ let T_s be a subset of A_s. When $p = 2$ assume also that $[\tau_1, \tau_2] \in T_2 \cup \{0\}$ for every $\tau_1, \tau_2 \in T_1$. If the sets $\pi^{n-s}\langle T_s \rangle$, $s = 1, 2, \ldots, n$, generate A_n, then the sets $\pi^{n-s} T_s$, $s = 1, 2, \ldots, n$, also generate A_n.*

Proof. When $p > 2$ or $s > 1$ Lemma 5.1 shows that $\pi^{n-s}\langle T_s \rangle = \langle \pi^{n-s} T_s \rangle$. When $p = 2$ and $s = 1$, it shows that

$$\pi^{n-1}\langle T_1 \rangle \subseteq \langle \pi^{n-1} T_1 \rangle + \langle \pi^{n-2} T_2 \rangle \subseteq A_n.$$

Therefore the subgroup of A_n generated by the sets $\pi^{n-s} T_s$, $s = 1, 2, \ldots, n$, contains the sets $\pi^{n-s}\langle T_s \rangle$, $s = 1, 2, \ldots, n$, and hence equals A_n. □

Motivated by e.g., [Laz54], [Ser63], [Lab67], we now specialize to a graded Lie algebra defined using the lower p-central filtration. We refer to [NSW08, Ch. III, §8] for the following facts. For the free profinite group S on the basis X and for $n \geq 1$ we set $\mathrm{gr}_n(S) = S^{(n,p)}/S^{(n+1,p)}$. It is an elementary abelian p-group, which we write additively. The commutator map induces a map $[\cdot,\cdot]\colon \mathrm{gr}_n(S)\times \mathrm{gr}_m(S)\to \mathrm{gr}_{n+m}(S)$, which endows a graded Lie algebra structure on $\mathrm{gr}_\bullet(S)=\bigoplus_{n=1}^\infty \mathrm{gr}_n(S)$. The map $\tau\mapsto\tau^p$ maps $S^{(r,p)}$ into $S^{(r+1,p)}$, and induces a map $\pi_r\colon \mathrm{gr}_r(S)\to \mathrm{gr}_{r+1}(S)$. The map $(\pi^r,\xi)\mapsto \pi_r(\xi)$ for $\xi\in \mathrm{gr}_r(S)$ extends to a map $\mathbb{Z}/p[\pi]\times \mathrm{gr}_\bullet(S)\to \mathrm{gr}_\bullet(S)$ which is $\mathbb{Z}/p$-linear in the first component and which satisfies (5.1).

THEOREM 5.3. *Let $n\geq 1$. The cosets of $\tau_w^{p^{n-s}}$, with $1\leq s\leq n$ and $w\in \mathrm{Lyn}_s(X)$, generate $S^{(n,p)}/S^{(n+1,p)}$.*

Proof. The case $n=1$ is immediate, so we assume that $n\geq 2$. For every $1\leq s\leq n$ let T_s be the set of cosets of τ_w, $w\in \mathrm{Lyn}_s(X)$, in $\mathrm{gr}_s(S)$. By Proposition 4.3, $\langle T_s\rangle$ is the image of $S^{(s,0)}$ in $\mathrm{gr}_s(S)$. Hence $\pi^{n-s}\langle T_s\rangle$ consists of the cosets in $\mathrm{gr}_n(S)$ of the p^{n-s}-powers of $S^{(s,0)}$. One has

$$S^{(n,p)}=\prod_{s=1}^n (S^{(s,0)})^{p^{n-s}}$$

[NSW08, Prop. 3.8.6]. Thus the sets $\pi^{n-s}\langle T_s\rangle$, $s=1,2,\dots,n$, generate $\mathrm{gr}_n(S)$. Further, T_1 consists of the cosets of x, with $x\in X$, and T_2 consists of the cosets of commutators $[x,y]$ with $x<y$ in X. Moreover, when $p=2$ the cosets of $[x,y]$ and $[y,x]=[x,y]^{-1}$ in $\mathrm{gr}_2(S)$ coincide. Lemma 5.2 therefore implies that even the sets $\pi^{n-s}T_s$, $s=1,2,\dots,n$, generate $\mathrm{gr}_n(S)$, as required. $\square$

6. THE PAIRING $\langle w,w'\rangle_n$

For a commutative unitary ring R and a positive integer m, let $\mathbb{U}_m(R)$ be the group of all $m\times m$ upper-triangular unipotent matrices over R. We write I_m for the identity matrix in $\mathbb{U}_m(R)$, and E_{ij} for the matrix with 1 at entry (i,j) and 0 elsewhere. As above, X will be a totally ordered set.

For the following fact we refer, e.g., to [Efr14, Lemma 7.5]. We recall from §3 that $\epsilon_{u,R}(\sigma)$ is the coefficient of the word $u\in X^*$ in the formal power series $\Lambda_R(\sigma)\in R\langle\langle X\rangle\rangle^\times$.

PROPOSITION 6.1. *Given a profinite ring R and a word $w=(x_1\cdots x_s)$ in X^* there is a well defined homomorphism of profinite groups*

$$\rho_R^w\colon S\to \mathbb{U}_{s+1}(R),\quad \sigma\mapsto (\epsilon_{(x_i\cdots x_{j-1}),R}(\sigma))_{1\leq i<j\leq s+1}.$$

REMARK 6.2. In particular, for each $x\in X$ the map $\chi_{x,R}=\epsilon_{(x),R}\colon S\to R$ is a group homomorphism, where R is considered as an additive group. The homomorphisms $\chi_{x,R}$, $x\in X$, are dual to the basis X, in the sense that $\chi_{x,R}(x)=1$, and $\chi_{x,R}(y)=0$ for $x\neq y$ in X.

PROPOSITION 6.3. *Let $1\leq s\leq n$. For $R=\mathbb{Z}/p^{n-s+1}$ one has:*

(a) $\mathbb{U}_{s+1}(R)^{(n,p)}=I_{s+1}+\mathbb{Z}p^{n-s}E_{1,s+1}$.
(b) $\mathbb{U}_{s+1}(R)^{(n,p)}$ *is central in* $\mathbb{U}_{s+1}(R)$.

Proof. (a) We follow the argument of [MT15a, Lemma 2.4]. Take $X = \{x_1, \dots, x_s\}$ be a set of s elements, let $S = S_X$, and let $w = (x_1 \cdots x_s)$. The matrices $\rho_R^w(x_i) = I_{s+1} + E_{i,i+1}$, $i = 1, 2, \dots, s$, generate $\mathbb{U}_{s+1}(R)$ [Wei55, p. 55], so ρ_R^w is surjective. Therefore it maps $S^{(n,p)}$ onto $\mathbb{U}_{s+1}(R)^{(n,p)}$.
By Proposition 4.1(b), for $\sigma \in S^{(n,p)}$ and $u \in X^*$ of length $1 \le |u| \le s$ one has $\epsilon_{u,\mathbb{Z}_p}(\sigma) \in p^{n-|u|}\mathbb{Z}_p$.
If $|u| < s$, then $\epsilon_{u,\mathbb{Z}_p}(\sigma) \in p^{n-|u|}\mathbb{Z}_p \subseteq p^{n-s+1}\mathbb{Z}_p$. Hence $\epsilon_{u,R}(\sigma) = 0$ in this case.
If $|u| = s$, then $\epsilon_{u,\mathbb{Z}_p}(\sigma) \in p^{n-s}\mathbb{Z}_p$, so $\epsilon_{u,R}(\sigma) \in p^{n-s}R$.
Moreover, $\tau_w^{p^{n-s}} \in (S^{(s,0)})^{p^{n-s}} \le S^{(n,p)}$. By Proposition 4.4(c), $\Lambda_{\mathbb{Z}_p}(\tau_w) = 1 + w + f$, where f is a combination of words strictly larger than w in $\preceq$. Hence $\Lambda_{\mathbb{Z}_p}(\tau_w^{p^{n-s}}) = 1 + p^{n-s}w + g$, where g is also a combination of words strictly larger than w in $\preceq$, which implies that $\epsilon_{w,R}(\tau_w^{p^{n-s}}) = p^{n-s} \cdot 1_R$.
Consequently, $\mathbb{U}_{s+1}(R)^{(n,p)} = \rho_R^w(S^{(n,p)}) = I_{s+1} + \mathbb{Z}p^{n-s}E_{1,s+1}$.

(b) It is straightforward to see that $I_{s+1} + \mathbb{Z}E_{1,s+1}$ is central in $\mathbb{U}_{s+1}(R)$, so the assertion follows from (a). $\square$

See [Bor04, §2] for a related analysis of the lower p-central filtration of $\mathbb{U}_{s+1}(\mathbb{Z}/p^{n-s+1})$.
Consider the obvious isomorphism

$$\iota_{n,s}\colon p^{n-s}\mathbb{Z}/p^{n-s+1}\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p, \qquad ap^{n-s} \pmod{p^{n-s+1}} \mapsto a \pmod{p}.$$

In view of Proposition 6.3(a), we may define a group isomorphism

$$\iota_{n,s}^{\mathbb{U}}\colon \mathbb{U}_{s+1}(\mathbb{Z}/p^{n-s+1})^{(n,p)} \xrightarrow{\sim} \mathbb{Z}/p, \quad (a_{ij}) \mapsto \iota_{n,s}(a_{1,s+1}).$$

Next let $w, w' \in X^*$ be words of lengths $1 \le s, s' \le n$, respectively, where w is Lyndon. We have $\tau_w^{p^{n-s}} \in (S^{(s,0)})^{p^{n-s}} \le S^{(n,p)}$. By Proposition 4.1(b), $\epsilon_{w',\mathbb{Z}_p}(\tau_w^{p^{n-s}}) \in p^{n-s'}\mathbb{Z}_p$, and therefore $\epsilon_{w',\mathbb{Z}/p^{n-s'+1}}(\tau_w^{p^{n-s}}) \in p^{n-s'}\mathbb{Z}/p^{n-s'+1}\mathbb{Z}$. We set

$$\langle w, w' \rangle_n = \iota_{n,s'}(\epsilon_{w',\mathbb{Z}/p^{n-s'+1}}(\tau_w^{p^{n-s}})) \in \mathbb{Z}/p. \tag{6.1}$$

Alternatively,

$$\langle w, w' \rangle_n = \iota_{n,s'}^{\mathbb{U}}(\rho_{\mathbb{Z}/p^{n-s'+1}}^{w'}(\tau_w^{p^{n-s}})). \tag{6.2}$$

Let $\preceq$ be as in (2.1).

PROPOSITION 6.4. *Let w, w' be words in X^* of lengths $1 \le s, s' \le n$, respectively, with w Lyndon.*

(a) *If $w' \prec w$, then $\langle w, w' \rangle_n = 0$;*
(b) *$\langle w, w \rangle_n = 1$;*
(c) *If w' contains letters which do not appear in w, then $\langle w, w' \rangle_n = 0$;*
(d) *If $s < s' < 2s$, then $\langle w, w' \rangle_n = 0$.*

Proof. (a), (b) Proposition 4.4(c) implies that $\Lambda_{\mathbb{Z}_p}(\tau_w^{p^{n-s}}) - 1 - p^{n-s}w$ is a combination of words strictly larger than w with respect to $\preceq$, and the same therefore holds over the coefficient ring $\mathbb{Z}/p^{n-s'+1}$. Hence, if $w' \prec w$, then $\epsilon_{w',\mathbb{Z}/p^{n-s'+1}}(\tau_w^{p^{n-s}}) = 0$, so $\langle w, w'\rangle_n = 0$. If $w = w'$, then $\epsilon_{w,\mathbb{Z}/p^{n-s+1}}(\tau_w^{p^{n-s}}) = p^{n-s} \cdot 1_{\mathbb{Z}/p^{n-s+1}}$, whence $\langle w, w\rangle_n = 1$.

(c) Here we clearly have $\epsilon_{w',\mathbb{Z}/p^{n-s'+1}}(\tau_w^{p^{n-s}}) = 0$.

(d) Since $\tau_w \in S^{(s,0)}$, one may write $\Lambda_{\mathbb{Z}_p}(\tau_w) = 1 + P + O(s'+1)$, where P is a combination of words w'' of length $s \leq |w''| \leq s'$, and $O(s'+1)$ denotes a combination of words of length $\geq s'+1$ (Proposition 4.1(a)). Since $s' < 2s$, this implies that $\Lambda_{\mathbb{Z}_p}(\tau_w^{p^{n-s}}) = 1 + p^{n-s}P + O(s'+1)$. In particular, $\epsilon_{w',\mathbb{Z}_p}(\tau_w^{p^{n-s}}) \in p^{n-s}\mathbb{Z}_p$, and therefore

$$\epsilon_{w',\mathbb{Z}/p^{n-s'+1}}(\tau_w^{p^{n-s}}) \in p^{n-s}(\mathbb{Z}/p^{n-s'+1}) = \{0\},$$

since $s < s'$. Hence $\langle w, w'\rangle_n = 0$. □

7. Transgressions

Given a profinite group G and a discrete G-module A, we write as usual $C^i(G,A)$, $Z^i(G,A)$, and $H^i(G,A)$ for the corresponding group of continuous i-cochains, group of continuous i-cocycles, and the ith profinite cohomology group, respectively. For $x \in Z^i(G,A)$ let $[x]$ be its cohomology class in $H^i(G,A)$.

For a normal closed subgroup N of G, let $\mathrm{trg}\colon H^1(N,A)^G \to H^2(G/N, A^N)$ be the transgression homomorphism. It is the map $d_2^{0,1}$ of the Lyndon–Hochschild–Serre spectral sequence associated with G and N [NSW08, Th. 2.4.3]. We recall the explicit description of trg, assuming for simplicity that the G-action on A is trivial [NSW08, Prop. 1.6.6]: If $x \in Z^1(N,A)$, then there exists $y \in C^1(G,A)$ such that $y|_N = x$ and $(\partial y)(\sigma_1,\sigma_2)$ depends only on the cosets of σ_1,σ_2 modulo N, so that ∂y may be viewed as an element of $Z^2(G/N,A)$. For any such y one has $\mathrm{trg}([x]) = [\partial y]$.

We fix for the rest of this section a finite group $\mathbb{U}$ and a normal subgroup N of $\mathbb{U}$ satisfying:

(i) $N \cong \mathbb{Z}/p$; and
(ii) N lies in the center of $\mathbb{U}$.

We set $\bar{\mathbb{U}} = \mathbb{U}/N$, and let it act trivially on $\mathbb{U}$. We denote the image of $u \in \mathbb{U}$ in $\bar{\mathbb{U}}$ by $\bar{u}$. We may choose a section λ of the projection $\mathbb{U} \to \bar{\mathbb{U}}$ such that $\lambda(\bar{1}) = 1$. We define a map $\delta \in C^2(\bar{\mathbb{U}}, N)$ by

$$\delta(\bar{u},\bar{u}') = \lambda(\bar{u}) \cdot \lambda(\bar{u}') \cdot \lambda(\bar{u}\bar{u}')^{-1}.$$

It is normalized, i.e., $\delta(\bar{u},1) = \delta(1,\bar{u}) = 1$ for every $\bar{u} \in \bar{\mathbb{U}}$.

We also define $y \in C^1(\mathbb{U},N)$ by $y(u) = u\lambda(\bar{u})^{-1}$. Note that $y|_N = \mathrm{id}_N$.

LEMMA 7.1. *For every $u, u' \in \mathbb{U}$ one has*

$$\delta(\bar{u},\bar{u}') \cdot y(u) \cdot y(u') = y(uu').$$

Proof. Since $y(u)$ and $y(u')$ are in N, they are central in $\mathbb{U}$, so

$$\begin{aligned}\delta(\bar u,\bar u')\cdot y(u)\cdot y(u') &= \lambda(\bar u)\cdot\lambda(\bar u')\cdot\lambda(\bar u\bar u')^{-1}\cdot y(u)\cdot y(u')\\ &= y(u)\cdot\lambda(\bar u)\cdot y(u')\cdot\lambda(\bar u')\cdot\lambda(\bar u\bar u')^{-1}\\ &= uu'\lambda(\bar u\bar u')^{-1} = y(uu').\end{aligned}$$

□

For the correspondence between elements of H^2 and central extensions see e.g., [NSW08, Th. 1.2.4].

Proposition 7.2. *Using the notation above, the following holds.*

(a) $\delta\in Z^2(\bar{\mathbb{U}},N)$;

(b) *One has* $\mathrm{trg}(\mathrm{id}_N)=-[\delta]$ *for the transgression map* $\mathrm{trg}\colon H^1(N,N)^{\mathbb{U}}\to H^2(\bar{\mathbb{U}},N)$.

(c) *The cohomology class* $[\delta]\in H^2(\bar{\mathbb{U}},N)$ *corresponds to the equivalence class of the central extension*

$$1\to N\to\mathbb{U}\to\bar{\mathbb{U}}\to 1. \tag{7.1}$$

Proof. (a), (b): For $u,u'\in\mathbb{U}$ Lemma 7.1 gives

$$(\partial y)(u,u') = y(u)\cdot y(u')\cdot y(uu')^{-1} = \delta(\bar u,\bar u')^{-1}.$$

This shows that δ is a 2-cocycle, and that $(\partial y)(u,u')$ depends only on the cosets $\bar u,\bar u'$. Further, $\mathrm{id}_N\in Z^1(N,N)$. By the explicit description of the transgression above, $\mathrm{trg}(\mathrm{id}_N)=-[\delta]$.

(c) Consider the set $B=N\times\bar{\mathbb{U}}$ with the binary operation

$$(u,\bar v)*(u',\bar v') = (\delta(\bar v,\bar v')uu',\bar v\bar v').$$

The proof of [NSW08, Th. 1.2.4] shows that this makes B a group, and $[\delta]$ corresponds to the equivalence class of the central extension

$$1\to N\to B\to\bar{\mathbb{U}}\to 1. \tag{7.2}$$

Moreover, the map $h\colon\mathbb{U}\to B$, $u\mapsto(y(u),\bar u)$ is clearly bijective. We claim that it is a homomorphism, whence an isomorphism. Indeed, for $u,u'\in\mathbb{U}$ Lemma 7.1 gives:

$$\begin{aligned}h(u)*h(u') &= (y(u),\bar u)*(y(u'),\bar u') = (\delta(\bar u,\bar u')y(u)y(u'),\bar u\bar u')\\ &= (y(uu'),\bar u\bar u') = h(uu').\end{aligned}$$

We obtain that the central extension (7.2) is equivalent to the central extension (7.1). □

Next let $\bar G$ be a profinite group, and let $\bar\rho\colon\bar G\to\bar{\mathbb{U}}$ be a continuous homomorphism. Let $\iota\colon N\xrightarrow{\sim}\mathbb{Z}/p$ be a fixed isomorphism (see (i)). Set

$$\alpha=(\bar\rho^*\circ\iota_*)([\delta]) = -(\bar\rho^*\circ\iota_*\circ\mathrm{trg})(\mathrm{id}_N)\in H^2(\bar G,\mathbb{Z}/p), \tag{7.3}$$

where the second equality is by Proposition 7.2(b). Then α corresponds to the equivalence class of the central extension

$$0 \to \mathbb{Z}/p \xrightarrow{\iota^{-1}\times 1} \mathbb{U} \times_{\bar{\mathbb{U}}} \bar{G} \to \bar{G} \to 1, \tag{7.4}$$

where $\mathbb{U}\times_{\bar{\mathbb{U}}}\bar{G}$ is the fiber product with respect to the natural projection $\mathbb{U} \to \bar{\mathbb{U}}$ and to $\bar{\rho}$; See [Hoe68, Proof of 1.1].

Suppose further that there is a profinite group G, a closed normal subgroup M of G, and a continuous homomorphism $\rho\colon G \to \mathbb{U}$ such that $\bar{G} = G/M$, $\rho(M) \le N$, and $\bar{\rho}\colon \bar{G} \to \bar{\mathbb{U}}$ is induced from ρ. The functoriality of transgression yields a commutative diagram

$$\begin{tikzcd}
H^1(N,N)^{\mathbb{U}} \arrow[r, "\iota_*", "\sim"'] \arrow[d, "\mathrm{trg}"] & H^1(N,\mathbb{Z}/p)^{\mathbb{U}} \arrow[r, "\rho^*"] \arrow[d, "\mathrm{trg}"] & H^1(M,\mathbb{Z}/p)^G \arrow[d, "\mathrm{trg}"] \\
H^2(\bar{\mathbb{U}},N) \arrow[r, "\iota_*", "\sim"'] & H^2(\bar{\mathbb{U}},\mathbb{Z}/p) \arrow[r, "\bar{\rho}^*"] & H^2(\bar{G},\mathbb{Z}/p).
\end{tikzcd}$$

The image of $\mathrm{id}_N \in H^1(N,N)$ in $H^1(M,\mathbb{Z}/p)^G$ is

$$\theta = \iota \circ (\rho|_M) \in H^1(M,\mathbb{Z}/p). \tag{7.5}$$

By (7.3) and the commutativity of the diagram,

$$\alpha = -\operatorname{trg}(\theta) \in H^2(\bar{G},\mathbb{Z}/p) \tag{7.6}$$

REMARK 7.3. Suppose that $\bar{\mathbb{U}}$ is abelian and that $\bar{G}$ acts trivially on $\bar{\mathbb{U}}$. A 2-cocycle representing α is

$$(\bar{\sigma},\bar{\sigma}') \mapsto \iota(\lambda(\bar{\rho}(\bar{\sigma}))\cdot\lambda(\bar{\rho}(\bar{\sigma}'))\cdot\lambda(\bar{\rho}(\bar{\sigma}\bar{\sigma}'))^{-1}).$$

But $\lambda(\bar{\rho}(\bar{\sigma}))\cdot\lambda(\bar{\rho}(\bar{\sigma}'))\cdot\lambda(\bar{\rho}(\bar{\sigma}\bar{\sigma}'))^{-1}$ is a 2-cocycle representing the image of $\bar{\rho}$ under the connecting homomorphism $H^1(\bar{G},\bar{\mathbb{U}}) \to H^2(\bar{G},N)$ arising from (7.1). Thus α is the image of $\bar{\rho}$ under the composition

$$H^1(\bar{G},\bar{\mathbb{U}}) \to H^2(\bar{G},N) \xrightarrow{\iota_*} H^2(\bar{G},\mathbb{Z}/p).$$

EXAMPLE 7.4. We give several examples of the above construction with the group $\mathbb{U} = \mathbb{U}_{s+1}(\mathbb{Z}/p^{n-s+1})$ (where $1 \le s \le n$), a continuous homomorphism $\rho\colon G \to \mathbb{U}$, where G is a profinite group, and the induced homomorphism $\bar{\rho}\colon G^{[n,p]} \to \mathbb{U}^{[n,p]}$. Note that assumptions (i) and (ii) then hold for $N = \mathbb{U}^{(n,p)}$, by Proposition 6.3. We will be especially interested in the case where $G = S = S_X$ is a free profinite group, $M = S^{(n,p)}$, $\rho = \rho^w_{\mathbb{Z}/p^{n-s+1}}$ for a word $w \in X^*$ of length $1 \le s \le n$, and $\bar{\rho} = \bar{\rho}^w_{\mathbb{Z}/p^{n-s+1}}\colon S^{[n,p]} \to \mathbb{U}^{[n,p]}$ is the induced homomorphism. In this setup we write $\alpha_{w,n}$ for α.

(1) *Bocksteins.* For a positive integer m and a profinite group $\bar{G}$, the connecting homomorphism arising from the short exact sequence of trivial $\bar{G}$-modules

$$0 \to \mathbb{Z}/p \to \mathbb{Z}/pm \to \mathbb{Z}/m \to 0$$

is the BOCKSTEIN HOMOMORPHISM

$$\mathrm{Bock}_{m,\bar{G}}\colon H^1(\bar{G},\mathbb{Z}/m) \to H^2(\bar{G},\mathbb{Z}/p).$$

Let $\mathbb{U} = \mathbb{U}_2(\mathbb{Z}/p^n)$ (i.e., $s = 1$). There is a commutative diagram of central extensions

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{U}^{(n,p)} \arrow[r] \arrow[d, "\wr"'] & \mathbb{U} \arrow[r] \arrow[d, "\wr"'] & \mathbb{U}^{[n,p]} \arrow[r] \arrow[d, "\wr"'] & 1 \\
0 \arrow[r] & p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \arrow[r] & \mathbb{Z}/p^n \arrow[r] & \mathbb{Z}/p^{n-1} \arrow[r] & 0.
\end{tikzcd}$$

For a profinite group $\bar{G}$ and a homomorphism $\bar{\rho}\colon \bar{G} \to \mathbb{Z}/p^{n-1}$, Remark 7.3 therefore implies that $\alpha = \mathrm{Bock}_{p^{n-1},\bar{G}}(\bar{\rho})$.
In particular, for $x \in X$ take

$$\bar{\rho} = \bar{\rho}^{(x)}_{\mathbb{Z}/p^n}\colon \bar{G} = S^{[n,p]} \to \mathbb{U}_2(\mathbb{Z}/p^n)^{[n,p]}.$$

Identifying $\mathbb{U}_2(\mathbb{Z}/p^n)^{[n,p]} = \mathbb{Z}/p^{n-1}$, we obtain

$$\alpha_{(x),n} = \mathrm{Bock}_{p^{n-1},S^{[n,p]}}(\epsilon_{(x),\mathbb{Z}/p^{n-1}}).$$

(2) *Massey products.* Let $n = s \geq 2$, so $\mathbb{U} = \mathbb{U}_{n+1}(\mathbb{Z}/p)$. Let $\bar{G}$ be a profinite group, let $\bar{\rho}\colon \bar{G} \to \mathbb{U}^{[n,p]}$ be a continuous homomorphism, and let $\rho_{i,i+1}\colon \bar{G} \to \mathbb{Z}/p$ denote its projection on the $(i, i+1)$-entry, $i = 1, 2, \ldots, n$. By a result of Dwyer [Dwy75, Th. 2.6], the extension (7.4) then corresponds to a defining system for the n-fold Massey product

$$\langle \rho_{12}, \rho_{23}, \ldots, \rho_{n,n+1}\rangle \subseteq H^2(\bar{G}, \mathbb{Z}/p)$$

(see [Efr14, Prop. 8.3] for the profinite analog of this fact). Thus, for a fixed $\bar{G}$ and for homomorphisms $\bar{\rho}_1, \ldots, \bar{\rho}_n\colon \bar{G} \to \mathbb{Z}/p$, with $\bar{\rho}$ varying over all homomorphisms such that $\bar{\rho}_{i,i+1} = \bar{\rho}_i$, $i = 1, 2, \ldots, n$, the cohomology element α ranges over the elements of the Massey product $\langle \bar{\rho}_1, \ldots, \bar{\rho}_n\rangle$.
In particular, for $\bar{G} = S^{[n,p]}$ and for a word $w = (x_1 \cdots x_n) \in X^*$ of length n, the cohomology elements $\alpha_{w,n}$ range over the Massey product $\langle \epsilon_{(x_1),\mathbb{Z}/p}, \ldots, \epsilon_{(x_n),\mathbb{Z}/p}\rangle \subseteq H^2(S^{[n,p]}, \mathbb{Z}/p)$, where the $\epsilon_{(x_i),\mathbb{Z}/p}$ are viewed as elements of $H^1(S^{[n,p]}, \mathbb{Z}/p)$.

(3) *Cup products.* In the special case $n = s = 2$, the Massey product contains only the cup product. Hence for every profinite group $\bar{G}$ and a homomorphism $\bar{\rho}\colon \bar{G} \to \mathbb{U}_3(\mathbb{Z}/p)$ the cohomology element $\alpha \in H^2(\bar{G}, \mathbb{Z}/p)$ is the cup product $\bar{\rho}_{12} \cup \bar{\rho}_{23}$. In particular, for $w = (xy)$ we have

$$\alpha_{(xy),\mathbb{Z}/p} = \epsilon_{(x),\mathbb{Z}/p} \cup \epsilon_{(y),\mathbb{Z}/p} \in H^2(S^{[2,p]}, \mathbb{Z}/p).$$

8. Cohomological duality

Let $S = S_X$ be again a free profinite group on the totally ordered set X, and let it act trivially on $\mathbb{Z}/p$. Let $n \geq 2$, so $S^{(n,p)} \leq S^p[S,S]$. Then the inflation map $H^1(S^{[n,p]}, \mathbb{Z}/p) \to H^1(S, \mathbb{Z}/p)$ is an isomorphism. Further, $H^2(S, \mathbb{Z}/p) = 0$. By the five-term sequence of cohomology groups [NSW08, Prop. 1.6.7], $\mathrm{trg}\colon H^1(S^{(n,p)}, \mathbb{Z}/p)^S \to H^2(S^{[n,p]}, \mathbb{Z}/p)$ is an isomorphism.

There is a natural non-degenerate bilinear map

$$S^{(n,p)}/S^{(n+1,p)} \times H^1(S^{(n,p)},\mathbb{Z}/p)^S \to \mathbb{Z}/p, \quad (\bar\sigma,\varphi)\mapsto\varphi(\sigma)$$

(see [EM11, Cor. 2.2]). It induces a bilinear map

$$(\cdot,\cdot)_n\colon S^{(n,p)} \times H^2(S^{[n,p]},\mathbb{Z}/p) \to \mathbb{Z}/p, \quad (\sigma,\alpha)_n = -(\mathrm{trg}^{-1}(\alpha))(\sigma),$$

with left kernel $S^{(n+1,p)}$ and trivial right kernel.

Now let $w\in X^*$ be a word of length $1\leq s\leq n$. As in Examples 7.4, we apply the computations in Section 7 to the group $\mathbb{U}=\mathbb{U}_{s+1}(\mathbb{Z}/p^{n-s+1})$, the open normal subgroup $N=\mathbb{U}^{(n,p)}$, the homomorphism $\rho=\rho^w_{\mathbb{Z}/p^{n-s+1}}\colon S\to\mathbb{U}$, the induced homomorphism $\bar\rho=\bar\rho^w_{\mathbb{Z}/p^{n-s+1}}\colon S^{[n,p]}\to\mathbb{U}^{[n,p]}$, and the closed normal subgroup $M=S^{(n,p)}$ of S. We write $\theta_{w,n},\alpha_{w,n}$ for θ,α, respectively.

LEMMA 8.1. *For $\sigma\in S^{(n,p)}$ and a word $w\in X^*$ of length $1\leq s\leq n$ one has*

$$(\sigma,\alpha_{w,n})_n=\iota_{n,s}(\epsilon_{w,\mathbb{Z}/p^{n-s+1}}(\sigma)).$$

Proof. By (7.6) and (7.5),

$$(\sigma,\alpha_{w,n})_n=\theta_{w,n}(\sigma)=\iota^{\mathbb{U}}_{n,s}(\rho^w_{\mathbb{Z}/p^{n-s+1}}(\sigma))=\iota_{n,s}(\epsilon_{w,\mathbb{Z}/p^{n-s+1}}(\sigma)). \qquad \square$$

This and (6.1) give:

COROLLARY 8.2. *Let w,w' be words in X^* of lengths $1\leq s,s'\leq n$, respectively, with w Lyndon. Then*

$$(\tau_w^{p^{n-s}},\alpha_{w',n})_n=\langle w,w'\rangle_n.$$

Proposition 6.4(a)(b) now gives:

COROLLARY 8.3. *Let $\mathrm{Lyn}_{\leq n}(X)$ be totally ordered by $\preceq$. The matrix*

$$\Big((\tau_w^{p^{n-|w|}},\alpha_{w',n})_n\Big),$$

where $w,w'\in\mathrm{Lyn}_{\leq n}(X)$, is upper-triangular unipotent.

In general the above matrix need not be the identity matrix – see e.g., Proposition 11.2 below. Next we observe the following general fact:

LEMMA 8.4. *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 $(L,\leq)$ be a finite totally ordered set, and for every $w\in L$ let $a_w\in A$, $b_w\in B$. Suppose that the matrix $\big((a_w,b_{w'})\big)_{w,w'\in L}$ is invertible, and that a_w, $w\in L$, generate A. Then a_w, $w\in L$, is an R-linear basis of A, and b_w, $w\in L$, is an R-linear basis of B.*

Proof. Let $b\in B$, and consider $r_{w'}\in R$, with $w'\in L$. The assumptions imply that $b=\sum_{w'}r_{w'}b_{w'}$ if and only if $(a_w,b-\sum_{w'}r_{w'}b_{w'})=0$ for every w. Equivalently, the $r_{w'}$ solve the linear system $\sum_{w'}(a_w,b_{w'})X_{w'}=(a_w,b)$, for $w\in L$. By the invertibility, the latter system has a unique solution. This shows that b_w, $w\in L$, is an R-linear basis of B.

By reversing the roles of a_w,b_w, we conclude that the a_w, $w\in L$, form an R-linear basis of A. $\square$

Theorem 8.5. (a) *The cohomology elements* $\alpha_{w,n}$*, where* $w \in \mathrm{Lyn}_{\leq n}(X)$*, form a* $\mathbb{Z}/p$*-linear basis of* $H^2(S^{[n,p]}, \mathbb{Z}/p)$*.*

(b) *When* X *is finite, the cosets of the powers* $\tau_w^{p^{n-s}}$*,* $w \in \mathrm{Lyn}_{\leq n}(X)$*, form a basis of the* $\mathbb{Z}/p$*-module* $S^{(n,p)}/S^{(n+1,p)}$*.*

Proof. When X is finite, the set $\mathrm{Lyn}_{\leq n}(X)$ is also finite. By Theorem 5.3, the cosets a_w of $\tau_w^{p^{n-|w|}}$, where $w \in \mathrm{Lyn}_{\leq n}(X)$, generate the $\mathbb{Z}/p$-module $S^{(n,p)}/S^{(n+1,p)}$. We apply Lemma 8.4 with the $\mathbb{Z}/p$-modules $A = S^{(n,p)}/S^{(n+1,p)}$ and $B = H^2(S^{[n,p]}, \mathbb{Z}/p)$, the non-degenerate bilinear map $A \times B \to \mathbb{Z}/p$ induced by $(\cdot, \cdot)_n$, the generators a_w of A, and the elements $b_w = \alpha_{w,n}$ of B.
Corollary 8.3 implies that the matrix $(a_w, b_{w'})$ is invertible. Therefore Lemma 8.4 gives both assertions in the finite case.
The general case of (a) follows from the finite case by a standard limit argument. □

We call $\alpha_{w,n}$, $w \in \mathrm{Lyn}_{\leq n}(X)$, the Lyndon basis of $H^2(S^{[n,p]}, \mathbb{Z}/p)$.
Recall that the number of relations in a minimal presentation of a pro-p group G is given by $\dim H^2(G, \mathbb{Z}/p)$ [NSW08, Cor. 3.9.5]. In view of (2.2), Theorem 8.5 gives this number for $G = S^{[n,p]}$:

Corollary 8.6. *One has*

$$\dim_{\mathbb{F}_p} H^2(S^{[n,p]}, \mathbb{Z}/p) = \dim_{\mathbb{F}_p}(S^{(n,p)}/S^{(n+1,p)}) = \sum_{s=1}^{n} \varphi_s(|X|),$$

where φ_s *is the necklace map.*

9. The shuffle relations

We recall the following constructions from [CFL58], [Reu93, pp. 134–135]. Let $u_1, \dots, u_t \in X^*$ be words of lengths $s_1, \dots, s_t$, respectively. We say that a word $w \in X^*$ of length $1 \leq n \leq s_1 + \cdots + s_t$ is an infiltration of $u_1, \dots, u_t$, if there exist sets $I_1, \dots, I_t$ of respective cardinalities $s_1, \dots, s_t$ such that $\{1, 2, \dots, n\} = I_1 \cup \cdots \cup I_t$ and the restriction of w to the index set I_j is u_j, $j = 1, 2, \dots, t$. We then write $w = w(I_1, \dots, I_t, u_1, \dots, u_t)$. We write $\mathrm{Infil}(u_1, \dots, u_t)$ for the set of all infiltrations of $u_1, \dots, u_t$. The infiltration product $u_1 \downarrow \cdots \downarrow u_t$ of $u_1, \dots, u_t$ is the polynomial $\sum w$ in $\mathbb{Z}\langle X \rangle$, where the sum is over all such infiltrations, taken with multiplicity.
If in the above setting, the sets $I_1, \dots, I_t$ are pairwise disjoint, then $w(I_1, \dots, I_t, u_1, \dots, u_t)$ is called a shuffle of $u_1, \dots, u_t$. We write $\mathrm{Sh}(u_1, \dots, u_t)$ for the set of all shuffles of $u_1, \dots, u_t$. It consists of the words in $\mathrm{Infil}(u_1, \dots, u_t)$ of length $s_1 + \cdots + s_t$. The shuffle product $u_1 ш \cdots ш u_t$ is the polynomial $\sum w(I_1, \dots, I_t, u_1, \dots, u_t)$ in $\mathbb{Z}\langle X \rangle$, where the sum is over all shuffles of $u_1, \dots, u_t$, taken with multiplicity. Thus $u_1 ш \cdots ш u_t$ is the homogenous part of $u_1 \downarrow \cdots \downarrow u_t$ of (maximal) degree $s_1 + \cdots + s_t$. For

instance

$$(xy) \downarrow (xz) = (xyxz) + 2(xxyz) + 2(xxzy) + (xzxy) + (xyz) + (xzy),$$
$$(xy)\text{ш}(xz) = (xyxz) + 2(xxyz) + 2(xxzy) + (xzxy)$$
$$(x) \downarrow (x) = 2(xx) + (x), \quad (x)\text{ш}(x) = 2(xx).$$

We may view infiltration and shuffle products also as elements of $\mathbb{Z}_p\langle X\rangle$. Let $\mathrm{Shuffles}(X)$ be the $\mathbb{Z}$-submodule of $\mathbb{Z}\langle X\rangle$ generated by all shuffle products $u\text{ш}v$, with $\emptyset \neq u, v \in X^*$. Let $\mathrm{Shuffles}_n(X)$ be its homogenous component of degree n.

EXAMPLES 9.1. $\mathrm{Shuffles}_1(X) = \{0\}$,

$$\mathrm{Shuffles}_2(X) = \langle (xy) + (yx) \mid x, y \in X\rangle,$$
$$\mathrm{Shuffles}_3(X) = \langle (xyz) + (xzy) + (zxy) \mid x, y, z \in X\rangle.$$

Let $(\cdot,\cdot)$ be the pairing of (3.1) for the ring $R = \mathbb{Z}_p$. As before, $S = S_X$ is the free profinite group on the set X. The following fact is due to Chen, Fox, and Lyndon in discrete case [CFL58, Th. 3.6] (see also [Mor12, Prop. 8.6], [Reu93, Lemma 6.7]), as well as [Vog05, Prop. 2.25] in the profinite case.

PROPOSITION 9.2. *For every $\emptyset \neq u, v \in X^*$ and every $\sigma \in S$ one has*

$$\epsilon_{u,\mathbb{Z}_p}(\sigma)\epsilon_{v,\mathbb{Z}_p}(\sigma) = (\Lambda_{\mathbb{Z}_p}(\sigma), u \downarrow v).$$

COROLLARY 9.3. *Let u, v be nonempty words in X^* with $s = |u| + |v| \leq n$. For every $\sigma \in S^{(n,p)}$ one has $(\Lambda_{\mathbb{Z}_p}(\sigma), u\text{ш}v) \in p^{n-s+1}\mathbb{Z}_p$.*

Proof. If w is a nonempty word of length $|w| < s$, then by Proposition 4.1(b), $\epsilon_{w,\mathbb{Z}_p}(\sigma) \in p^{n-|w|}\mathbb{Z}_p \subseteq p^{n-s+1}\mathbb{Z}_p$. In particular, this is the case for $w = u$, $w = v$, and when $w \in \mathrm{Infil}(u, v) \setminus \mathrm{Sh}(u, v)$. It follows from Proposition 9.2 that $(\Lambda_{\mathbb{Z}_p}(\sigma), u\text{ш}v) \in p^{n-s+1}\mathbb{Z}_p$. □

We obtain the following SHUFFLE RELATIONS (see also [Vog04, Cor. 1.2.10] and [FS84, Th. 6.8]). We write X^s for the set of words in X^* of length s.

THEOREM 9.4. *For every $\emptyset \neq u, v \in X^*$ with $s = |u| + |v| \leq n$ one has*

$$\sum_{w\in X^s} (u\text{ш}v)_w \alpha_{w,n} = 0.$$

Proof. For $\sigma \in S^{(n,p)}$, Corollary 9.3 gives

$$\sum_{w\in X^s} (u\text{ш}v)_w \epsilon_{w,\mathbb{Z}_p}(\sigma) = \sum_{w\in X^*} (u\text{ш}v)_w \epsilon_{w,\mathbb{Z}_p}(\sigma) = (\Lambda_{\mathbb{Z}_p}(\sigma), u\text{ш}v) \in p^{n-s+1}\mathbb{Z}_p.$$

Therefore, by Lemma 6.2,

$$\begin{aligned}(\sigma, \sum_{w\in X^s} (u\text{ш}v)_w \alpha_{w,n})_n &= \sum_{w\in X^s} (u\text{ш}v)_w (\sigma, \alpha_{w,n})_n \\ &= \sum_{w\in X^s} (u\text{ш}v)_w\, \iota_{n,s}(\epsilon_{w,\mathbb{Z}/p^{n-s+1}}(\sigma)) \\ &= \iota_{n,s}\Big(\sum_{w\in X^s} (u\text{ш}v)_w \epsilon_{w,\mathbb{Z}/p^{n-s+1}}(\sigma)\Big) = 0.\end{aligned}$$

Now use the fact that $(\cdot,\cdot)_n\colon S^{(n,p)}\times H^2(S^{[n,p]},\mathbb{Z}/p)\to\mathbb{Z}/p$ has a trivial right kernel. $\square$

Corollary 9.5. *There is a canonical epimorphism*

$$\bigoplus_{s=1}^{n}\Big(\big(\bigoplus_{w\in X^s}\mathbb{Z}\big)/\operatorname{Shuffles}_s(X)\Big)\otimes(\mathbb{Z}/p)\to H^2(S^{[n,p]},\mathbb{Z}/p)$$

$$(\bar r_w)_w\mapsto\sum_w r_w\alpha_{w,n}.$$

Proof. By Theorem 9.4 this homomorphism is well defined. By Theorem 8.5(a), it is surjective. $\square$

Remark 9.6. In view of Lemma 6.2, the epimorphism of Corollary 9.5 and the canonical pairing $(\cdot,\cdot)_n$ induce a bilinear map

$$S^{(n,p)}\times\bigoplus_{s=1}^{n}\Big(\big(\bigoplus_{w\in X^s}\mathbb{Z}\big)/\operatorname{Shuffles}_s(X)\Big)\to\mathbb{Z}/p,$$

$$(\sigma,\overline{(r_w)}_w)=\sum_w r_w\iota_{n,s}(\epsilon_{w,\mathbb{Z}/p^{n-s+1}}(\sigma))$$

with left kernel $S^{(n+1,p)}$.

Example 9.7. We show that for every $x_1,x_2,\dots,x_k\in X$ one has

$$(x_1x_2\cdots x_k)+(-1)^{k-1}(x_k\cdots x_2x_1)\in\operatorname{Shuffles}_n(X).$$

We may assume that $x_1,x_2,\dots,x_k$ are distinct. For $1\le l\le k-1$ let $u_l=(x_l\cdots x_2x_1)$ and $v_l=(x_{l+1}\cdots x_k)$. We consider the polynomial $\sum_{l=1}^{k-1}(-1)^{l-1}u_l ш v_l$ in $\mathbb{Z}\langle X\rangle$. It is homogenous of degree k. If $w\in\operatorname{Sh}(u_l,v_l)$, then either:

(1) x_l appears before x_{l+1} in w, and then w appears with an opposite sign also in $\operatorname{Sh}(u_{l-1},v_{l-1})$; or
(2) x_{l+1} appears before x_l in w, and then w appears with opposite sign also in $\operatorname{Sh}(u_{l+1},v_{l+1})$.

The only exceptions are $w=(x_1x_2\cdots x_k)\in\operatorname{Sh}(u_1,v_1)$ and $w=(x_k\cdots x_2x_1)\in\operatorname{Sh}(u_{k-1},v_{k-1})$. This shows that

$$(x_1x_2\cdots x_k)+(-1)^k(x_k\cdots x_2x_1)=\sum_{l=1}^{k-1}(-1)^{l-1}u_l ш v_l.$$

For $1\le k\le n$ Corollary 9.5 therefore implies that

$$\alpha_{(x_1x_2\cdots x_k),n}=(-1)^{k-1}\alpha_{(x_k\cdots x_2x_1),n}.$$

10. Example: The case $n = 2$

Our results in this case are fairly well known, and are brought here in order to illustrate the general theory.

As before let $S = S_X$ with X totally ordered. Here $S^{(2,p)} = S^p[S,S]$ and $\bar{S} = S^{[2,p]}$ is the maximal elementary p-abelian quotient of S. We may identify $H^1(S,\mathbb{Z}/p) = H^1(\bar{S},\mathbb{Z}/p) \cong \bigoplus_{x\in X}\mathbb{Z}/p$. Let $\chi_{x,\mathbb{Z}/p} = \epsilon_{(x),\mathbb{Z}/p}$, $x \in X$, be the basis of $H^1(S,\mathbb{Z}/p)$ dual to X (see Remark 6.2).

The Lyndon words w of length ≤ 2 are (x), where $x \in X$, and (xy), where $x, y \in X$ and $x < y$. For these words we have $\tau_{(x)} = x$ and $\tau_{(xy)} = [x,y]$. By Examples 7.4(1)(3),

$$\alpha_{(x),2} = \mathrm{Bock}_{p,\bar{S}}(\chi_{x,\mathbb{Z}/p}), \quad \alpha_{(xy),2} = \chi_{x,\mathbb{Z}/p} \cup \chi_{y,\mathbb{Z}/p}.$$

Hence, by Theorem 8.5, $\mathrm{Bock}_{p,\bar{S}}(\chi_{x,\mathbb{Z}/p})$ and $\chi_{x,\mathbb{Z}/p} \cup \chi_{y,\mathbb{Z}/p}$, where $x < y$, form a $\mathbb{Z}/p$-linear basis of $H^2(\bar{S},\mathbb{Z}/p)$. Furthermore, when X is finite, the elements of the form x^p and $[x,y]$ with $x, y \in X$, $x < y$, form a $\mathbb{Z}/p$-linear basis of $S^{(2,p)}/S^{(3,p)}$. In view of Examples 9.1 and Corollary 9.5, the map $(\bar{r}_w) \mapsto \sum_w r_w \alpha_{w,2}$ induces an epimorphism

$$\bigoplus_{x\in X}\mathbb{Z}/p \oplus \Big(\big(\bigoplus_{x,y\in X}\mathbb{Z}\big)/\langle (xy)+(yx) \mid x,y\in X\rangle\Big) \otimes (\mathbb{Z}/p) \to H^2(\bar{S},\mathbb{Z}/p).$$

It coincides with the map

$$H^1(\bar{S},\mathbb{Z}/p) \oplus \bigwedge^2 H^1(\bar{S},\mathbb{Z}/p) \to H^2(\bar{S},\mathbb{Z}/p)$$

which is $\mathrm{Bock}_{p,\bar{S}}$ on the first component and $\cup$ on the second component. When $p \neq 2$ the direct sum is a free $\mathbb{Z}/p$-module on $\mathrm{Lyn}_{\leq 2}(X)$, and by comparing dimensions we see that the epimorphism is in fact an isomorphism (compare [EM11, Cor. 2.9(a)]). However when $p = 2$ one has $\mathrm{Bock}_{2,\bar{S}}(\chi) = \chi \cup \chi$ [EM11, Lemma 2.4], so the above epimorphism is not injective.

Next, Proposition 6.4 shows that the matrix $(\langle w, w'\rangle_2)$, where $w, w' \in \mathrm{Lyn}_{\leq 2}(X)$, is the identity matrix. In view of Corollary 8.2, it coincides with the matrix $\big((\tau_w^{p^{2-|w|}}, \alpha_{w',2})_2\big)$. Thus

$(x^p, \mathrm{Bock}_{p,\bar{S}}(\chi_{x,\mathbb{Z}/p}))_2 = 1$ for every $x \in X$,

$(x^p, \mathrm{Bock}_{p,\bar{S}}(\chi_{y,\mathbb{Z}/p}))_2 = 0$ for every $x, y \in X, x \neq y$,

$(x^p, \chi_{y,\mathbb{Z}/p} \cup \chi_{z,\mathbb{Z}/p})_2 = 0$ for every $x, y, z \in X$,

$([x,y], \mathrm{Bock}_{p,\bar{S}}(\chi_{z,\mathbb{Z}/p}))_2 = 0$ for every $x, y, z \in X$,

$([x,y], \chi_{z,\mathbb{Z}/p} \cup \chi_{t,\mathbb{Z}/p})_2 = 0$ for every $x, y, z, t \in X, (xy) \neq (zt), (tz)$,

$([x,y], \chi_{x,\mathbb{Z}/p} \cup \chi_{y,\mathbb{Z}/p})_2 = 1$ for every $x, y \in X$ with $x < y$.

This recovers well known facts from [Lab66, §2.3], [Koc02, §7.8] and [NSW08, Th. 3.9.13 and Prop. 3.9.14]

11. Example: The case $n = 3$.

Here $S^{(3,p)} = S^{p^2}[S,S]^p[S,[S,S]]$. We abbreviate $\bar{S} = S^{[3,p]}$. Recall that $\mathrm{Lyn}_{\leq 3}(X)$ consists of the words

$$\begin{aligned}&(x) \text{ for } x \in X,\\ &(xy), (xxy), (xyy) \text{ for } x, y \in X \text{ with } x < y,\\ &(xyz), (xzy) \text{ for } x, y, z \in X \text{ with } x < y < z.\end{aligned}$$

For these words

$$\tau_{(x)} = x, \quad \tau_{(xy)} = [x,y], \quad \tau_{(xxy)} = [x,[x,y]], \quad \tau_{(xyy)} = [[x,y],y],$$
$$\tau_{(xyz)} = [x,[y,z]], \quad \tau_{(xzy)} = [[x,z],y].$$

By Theorem 5.3, the cosets of

$$x^{p^3},\ [x,y]^p,\ [x,[x,y]],\ [[x,y],y],\ [x,[y,z]],\ [[x,z],y],$$

with x, y, z as above, generate $S^{(3,p)}/S^{(4,p)}$. When X is finite, they form a linear basis of $S^{(3,p)}/S^{(4,p)}$ over $\mathbb{Z}/p$ (Theorem 8.5(b)). Furthermore, Theorem 8.5(a) gives:

Theorem 11.1. *The following cohomology elements form a $\mathbb{Z}/p$-linear basis of $H^2(\bar{S}, \mathbb{Z}/p)$:*

$$\alpha_{(x),3},\ \alpha_{(xy),3},\ \alpha_{(xxy),3},\ \alpha_{(xyy),3},\ \alpha_{(xyz),3},\ \alpha_{(xzy),3},$$

where $x, y, z \in X$ and we assume that $x < y < z$.

By Examples 7.4, $\alpha_{(x),3} = \mathrm{Bock}_{p^2,\bar{S}}(\chi_{x,\mathbb{Z}/p^2})$, and for every $x, y, z \in X$, $\alpha_{(xyz),3}$ belongs to the triple Massey product $\langle \chi_{x,\mathbb{Z}/p}, \chi_{y,\mathbb{Z}/p}, \chi_{z,\mathbb{Z}/p} \rangle \subseteq H^2(\bar{S}, \mathbb{Z}/p)$.

We further recall that $\alpha_{(xy),3}$ is the pullback to $H^2(\bar{S}, \mathbb{Z}/p)$ under $\bar{\rho}^{(xy)}_{\mathbb{Z}/p^2} \colon \bar{S} \to \mathbb{U}_3(\mathbb{Z}/p^2)^{[3,p]}$ of the cohomology element in $H^2(\mathbb{U}_3(\mathbb{Z}/p^2)^{[3,p]}, \mathbb{Z}/p)$ corresponding to the central extension

$$0 \to \mathbb{Z}/p \to \mathbb{U}_3(\mathbb{Z}/p^2) \to \mathbb{U}_3(\mathbb{Z}/p^2)^{[3,p]} \to 1.$$

Alternatively, it has the following explicit description: By Proposition 6.3(a), $\mathbb{U}_3(\mathbb{Z}/p^2)^{(3,p)} = I_3 + \mathbb{Z}pE_{13}$, and let $\iota = \iota^{\mathbb{U}}_{3,2} \colon \mathbb{U}_3(\mathbb{Z}/p^2)^{(3,p)} \xrightarrow{\sim} \mathbb{Z}/p$ be the natural isomorphism. By (7.5) and (7.6), $\alpha_{(xy),3} = -\mathrm{trg}(\theta)$, where $\theta = \iota \circ (\rho^{(xy)}_{\mathbb{Z}/p^2}|_{S^{(3,p)}})$ and $\mathrm{trg} \colon H^1(S^{(3,p)}, \mathbb{Z}/p)^S \xrightarrow{\sim} H^2(\bar{S}, \mathbb{Z}/p)$ is the transgression isomorphism.

Next we compute the matrix $((\tau_w^{p^{3-|w|}}, \alpha_{w',3})_3) = (\langle w, w' \rangle_3)$, where $w, w' \in \mathrm{Lyn}_{\leq 3}(X)$:

Proposition 11.2. *For $w, w' \in \mathrm{Lyn}_{\leq 3}(X)$ one has*

$$\langle w, w' \rangle_3 = \begin{cases} 1, & \text{if } w = w';\\ -1, & \text{if } w = (xyz),\ w' = (xzy) \text{ for some } x, y, z \in X,\ x < y < z;\\ 0, & \text{otherwise.}\end{cases}$$

Proof. In view of Proposition 6.4, it is enough to show the assertion when $w \neq w'$, either $|w| = |w'|$ or $2|w| \leq |w'|$, and the letters of w' appear in w. Furthermore, when $|w| = |w'|$ we may assume that $w \leq_{\mathrm{alp}} w'$.
Thus when w has one of the forms $(x), (xy), (xyy), (xzy)$ (where $x < y < z$) there is nothing more to show.
When $w = (xxy)$ with $x < y$ we need to check only the word $w' = (xyy)$. Then Lemma 4.2 gives

$$\begin{aligned}\langle (xxy), (xyy)\rangle_3 &= \epsilon_{(xyy),\mathbb{Z}/p}([x,[x,y]]) \\ &= \epsilon_{(x),\mathbb{Z}/p}(x)\cdot\epsilon_{(yy),\mathbb{Z}/p}([x,y]) - \epsilon_{(y),\mathbb{Z}/p}(x)\cdot\epsilon_{(xy),\mathbb{Z}/p}([x,y]) \\ &= 1\cdot 0 - 0\cdot 1 = 0.\end{aligned}$$

When $w = (xyz)$ with $x < y < z$ we need to check only the word $w' = (xzy)$. Then Lemma 4.2 gives

$$\begin{aligned}\langle (xyz), (xzy)\rangle_3 &= \epsilon_{(xzy),\mathbb{Z}/p}([x,[y,z]]) \\ &= \epsilon_{(x),\mathbb{Z}/p}(x)\cdot\epsilon_{(zy),\mathbb{Z}/p}([y,z]) - \epsilon_{(y),\mathbb{Z}/p}(x)\cdot\epsilon_{(xz),\mathbb{Z}/p}([y,z]) \\ &= 1\cdot(-1) - 0\cdot 0 = -1.\end{aligned}$$

This completes the verification in all cases. □

In view of Examples 9.1, Corollary 9.5 gives rise to an epimorphism

(11.1)

$$\begin{aligned}&\bigoplus_{x\in X}\mathbb{Z}/p \oplus \Big(\big(\bigoplus_{x,y\in X}\mathbb{Z}(xy)\big)/\langle (xy)+(yx) \mid x,y\in X\rangle\Big)\otimes(\mathbb{Z}/p) \\ &\qquad \oplus \Big(\big(\bigoplus_{x,y,z\in X}\mathbb{Z}(xyz)\big)/\langle (xyz)+(xzy)+(zxy) \mid x,y,z\in X\rangle\Big)\otimes(\mathbb{Z}/p) \\ &\qquad \to H^2(\bar{S},\mathbb{Z}/p).\end{aligned}$$

Moreover, for $x, y, z \in X$, $x < y < z$, we have

$$\begin{aligned}(yx) &= (x)ш(y) - (xy) \\ 2(xx) &= (x)ш(x) \\ (xyx) &= (x)ш(xy) - 2(xxy) \\ (yxx) &= (x)ш(yx) - (xx)ш(y) + (xxy) \\ (yxy) &= (xy)ш(y) - 2(xyy) \\ (yyx) &= (yy)ш(x) - (y)ш(xy) + (xyy) \\ (yxz) &= (y)ш(xz) - (xyz) - (xzy) \\ (zxy) &= (z)ш(xy) - (xzy) - (xyz) \\ (yzx) &= (zx)ш(y) - (x)ш(zy) + (xzy) \\ (zyx) &= (yx)ш(z) - (x)ш(yz) + (xyz) \\ 3(xxx) &= (x)ш(xx).\end{aligned}$$

These congruences and Example 2.1 imply that

$$\sum_{w\in X^2}\mathbb{Z}w \equiv \sum_{w\in \mathrm{Lyn}_2(X)}\mathbb{Z}w + \text{ 2-torsion} \pmod{\mathrm{Shuffles}_2(X)},$$

$$\sum_{w\in X^3}\mathbb{Z}w \equiv \sum_{w\in \mathrm{Lyn}_3(X)}\mathbb{Z}w + \text{ 3-torsion} \pmod{\mathrm{Shuffles}_3(X)}.$$

Therefore, for $p>3$, the direct sum in (11.1) is the free $\mathbb{Z}/p$-module on the basis $\mathrm{Lyn}_{\leq 3}(X)$. Thus the epimorphism (11.1) maps the $\mathbb{Z}/p$-linear basis $1w$, $w\in\mathrm{Lyn}_{\leq 3}(X)$, bijectively onto the $\mathbb{Z}/p$-linear basis $\alpha_{w,3}$, $w\in\mathrm{Lyn}_{\leq 3}(X)$ (see Theorem 8.5). Consequently we have:

Theorem 11.3. *For $n=3$ and $p>3$, (11.1) is an isomorphism. Thus all relations in $H^2(S^{[3,p]},\mathbb{Z}/p)$ are consequences of the shuffle relations of Theorem 9.4.*

References

[AKM99] A. Adem, D. B. Karagueuzian, and J. Mináč, *On the cohomology of Galois groups determined by Witt rings*, Adv. Math. 148 (1999), 105–160.

[Bog91] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Proc. of Tokyo Satellite conference ICM-90 Analytic and Algebraic Geometry, 1991, pp. 26–52.

[Bor04] I. C. Borge, *A cohomological approach to the modular isomorphism problem*, J. Pure Appl. Algebra 189 (2004), 7–25.

[CE16] M. Chapman and I. Efrat, *Filtrations of the free group arising from the lower central series*, J. Group Theory 19 (2016), 405–433, special issue in memory of O. Melnikov.

[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.

[CFL58] K.-T. Chen, R. H. Fox, and R. C. Lyndon, *Free differential calculus. IV. The quotient groups of the lower central series*, Ann. Math. 68 (1958), 81–95.

[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.

[EM15] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math Soc. (2015), to appear, available at `arXiv: 1412.7265`.

[EM11] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. 133 (2011), 1503–1532.

[Fen83] R. A. Fenn, *Techniques of Geometric Topology*, London Math. Society Lect. Note Series, vol. 57, Cambridge Univ. Press, Cambridge, 1983.

[FS84] R. Fenn and D. Sjerve, *Basic commutators and minimal Massey products*, Canad. J. Math. 36 (1984), 1119–1146.

[FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag, Berlin, 2008.

[For11] P. Forré, *Strongly free sequences and pro-p groups of cohomological dimension* 2, J. reine angew. Math. 658 (2011), 173–192.

[Hoe68] K. Hoechsmann, *Zum Einbettungsproblem* 229 (1968), 81–106.

[Koc60] H. Koch, *Über die Faktorgruppen einer absteigenden Zentralreihe*, Math. Nach. 22 (1960), 159–161.

[Koc02] H. Koch, *Galois theory of p-extensions*, Springer, Berlin, 2002.

[Lab66] J. P. Labute, *Demuškin groups of rank* $\aleph_0$, Bull. Soc. Math. France 94 (1966), 211–244.

[Lab67] J. Labute, *Classification of Demuškin groups*, Can. J. Math. 19 (1967), 106–132.

[Lab06] J. Labute, *Mild pro-p groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. reine angew. Math. 596 (2006), 155–182.

[LM11] J. Labute and J. Mináč, *Mild pro-2-groups and 2-extensions of* $\mathbb{Q}$ *with restricted ramification*, J. Algebra 332 (2011), 136–158.

[Laz54] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) 71 (1954), 101–190.

[MS96] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. Math. 144 (1996), 35–60.

[MT15a] J. Mináč and N. D. Tân, *The Kernel Unipotent Conjecture and the vanishing of Massey products for odd rigid fields,* (with an appendix by Efrat, I., Mináč, J. and Tân, N. D.), Adv. Math. 273 (2015), 242–270.

[MT15b] J. Mináč and N. D. Tân, *Triple Massey products over global fields*, Doc. Math. 20 (2015), 1467–1480.

[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. 19 (2017), 255–284.

[MP00] H. N. Minh and M. Petitot, *Lyndon words, polylogarithms and the Riemann ζ function*, Discrete Math. 217 (2000), 273–292.

[Mor12] M. Morishita, *Knots and primes*, Universitext, Springer, London, 2012.

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

[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.

[Sch10] A. Schmidt, *Über pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine angew. Math. 640 (2010), 203–235.

[Ser63] J.-P. Serre, *Structure de certains pro-p-groupes (d'après Demuškin)*, Séminaire Bourbaki (1962/63), Exp. 252.

[Ser92] J.-P. Serre, *Lie Algebras and Lie Groups*, Springer, 1992.

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

[Vog04] D. Vogel, *Massey products in the Galois cohomology of number fields*, Ph.D. thesis, Universität Heidelberg, 2004.

[Vog05] D. Vogel, *On the Galois group of 2-extensions with restricted ramification*, J. reine angew. Math. 581 (2005), 117–150.

[Wei55] A. J. Weir, *Sylow p-subgroups of the general linear group over finite fields of characteristic p*, Proc. Amer. Math. Soc. 6 (1955), 454–464.

[Wic12] K. Wickelgren, *n-nilpotent obstructions to π_1 sections of $\mathbb{P}^1 - \{0,1,\infty\}$ and Massey products*, Galois-Teichmüller theory and arithmetic geometry, Adv. Stud. Pure Math., vol. 63, Math. Soc. Japan, Tokyo, 2012, pp. 579–600.

Ido Efrat
Department of Mathematics
Ben-Gurion University of the Negev
P.O. Box 653
Be'er-Sheva 84105
Israel
efrat@math.bgu.ac.il