TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 369, Number 4, April 2017, Pages 2721–2745
http://dx.doi.org/10.1090/tran/6740
Article electronically published on September 1, 2016

ABELIAN-BY-CENTRAL GALOIS GROUPS OF FIELDS I: A FORMAL DESCRIPTION

ADAM TOPAZ

Abstract. Let K be a field whose characteristic is prime to a fixed positive integer n such that $\mu_n \subset K$, and choose $\omega \in \mu_n$ as a primitive n-th root of unity. Denote the absolute Galois group of K by $\mathrm{Gal}(K)$, and the mod-n central-descending series of $\mathrm{Gal}(K)$ by $\mathrm{Gal}(K)^{(i)}$. Recall that Kummer theory, together with our choice of ω, provides a functorial isomorphism between $\mathrm{Gal}(K)/\mathrm{Gal}(K)^{(2)}$ and $\mathrm{Hom}(K^\times, \mathbb{Z}/n)$. Analogously to Kummer theory, in this note we use the Merkurjev-Suslin theorem to construct a continuous, functorial and explicit embedding $\mathrm{Gal}(K)^{(2)}/\mathrm{Gal}(K)^{(3)} \hookrightarrow \mathrm{Fun}(K \smallsetminus \{0,1\}, (\mathbb{Z}/n)^2)$, where $\mathrm{Fun}(K \smallsetminus \{0,1\}, (\mathbb{Z}/n)^2)$ denotes the group of $(\mathbb{Z}/n)^2$-valued *functions* on $K \smallsetminus \{0,1\}$. We explicitly determine the functions associated to the image of commutators and n-th powers of elements of $\mathrm{Gal}(K)$ under this embedding. We then apply this theory to prove some new results concerning relations between elements in abelian-by-central Galois groups.

1. Introduction

In recent years, it has become increasingly evident that much of the arithmetic and geometric information which is encoded in very large Galois groups (e.g. maximal pro-p Galois groups and absolute Galois groups) is already encoded in much smaller quotients and specifically in so-called "abelian-by-central" quotients. Recall that the mod-n abelian-by-central Galois group of a field K is the maximal Galois group of K which is a central extension of an exponent-n abelian group by an exponent-n abelian group. In other words, the mod-n abelian-by-central Galois group of K is the quotient of its absolute Galois group associated to the third term in the mod-n central descending series.

One instance of this phenomenon comes from valuation theory. It has been known for several years that one can detect valuations of a given field using "large" Galois groups. More precisely, it was shown by Engler-Nogueira [EN94] and Efrat [Efr95] for $p = 2$, and by Engler-Koenigsmann [EK98] for $p > 2$ that one can detect inertia/decomposition groups of tamely-branching valuations in the maximal pro-p Galois group of a field K of characteristic different from p such that $\mu_p \subset K$. Also in the same direction, Koenigsmann [Koe03] shows how one can detect inertia/decomposition groups of valuations in absolute Galois groups of arbitrary fields. On the other hand, similar valuation-theoretic data is already encoded in abelian-by-central Galois groups. It was shown by Bogomolov-Tschinkel [BT02] and Pop

Received by the editors August 26, 2014 and, in revised form, April 20, 2015.
2010 *Mathematics Subject Classification.* Primary 12G05, 12F10, 20J06, 20E18.
Key words and phrases. Abelian-by-central, Galois groups, group cohomology, profinite groups.
This research was supported by NSF postdoctoral fellowship DMS-1304114.

[Pop10] that one can detect *abelian* inertia/decomposition groups of valuations using the pro-p abelian-by-central Galois group of a function field over an *algebraically closed field*. More recently, Efrat-Mináč [EM12] proved that the mod-p abelian-by-central Galois group encodes the existence (or non-existence) of a tamely-branching *p-Henselian* valuation in a field K of characteristic $\neq p$ such that $\mu_p \subset K$. Finally, it was shown by the author in Topaz [Top14] that the mod-p^n abelian-by-central Galois group (for arbitrary n) of a field K encodes abelian inertia/decomposition groups of almost *arbitrary* valuations, as long as $\operatorname{char} K \neq p$ and K contains sufficiently many roots of unity.

Further instances of this phenomenon arise from Galois cohomology. With mod-2 Galois cohomology, it was shown by Mináč-Spira [MS96] that the mod-2 abelian-by-central Galois group of a field K can be seen as a "Galois-theoretical analogue" of the Witt ring of quadratic forms of K. More recently, Chebolu-Efrat-Mináč [CEM12] proved that one can recover the mod-p^n Galois cohomology of a field K, endowed with the cup product and Bockstein morphism, as the *decomposable* part of the mod-p^n cohomology of the mod-p^n abelian-by-central Galois group, as long as K has characteristic different from p such that $\mu_{p^n} \subset K$; loc. cit. also gives a *non-functorial* construction which determines the mod-p^n abelian-by-central Galois group from the lower mod-p^n Galois cohomology groups of the field. See also Efrat-Mináč [EM11a] for related results in this direction. Along similar lines, the abelian-by-central Galois group and its natural *meta-abelian* generalizations encode a lot of information about important Galois modules which naturally arise from *strictly larger* quotients of the absolute Galois group via Kummer theory and Galois cohomology, as was shown by Mináč-Swallow-Topaz [MST14].

The strongest instance of this phenomenon, however, is a conjecture in birational anabelian geometry, which was first proposed by Bogomolov [Bog91] (see also Pop [Pop12] for a precise functorial formulation), whose goal is to recover a function field K of dimension ≥ 2 over an algebraically closed field from its pro-p abelian-by-central Galois group. If successful, this conjecture would go far beyond Grothendieck's original (birational) anabelian conjectures (see [Gro97]) since it deals with fields of *purely geometric* nature and with abelian-by-central Galois groups, which are "almost-abelian", as opposed to absolute Galois groups. While Bogomolov's conjecture is open in general, it has been proven for function fields of transcendence degree ≥ 2 over the *algebraic closure of a finite field* by Bogomolov-Tschinkel [BT08], [BT11] and by Pop [Pop03], [Pop10], [Pop12]. A weaker version of this conjecture, which uses large Galois groups instead of abelian-by-central ones, was also resolved for function fields over $\bar{\mathbb{Q}}$ in transcendence degree 2 by Silberstein [Sil12] and in transcendence degree ≥ 3 by Pop [Pop11]. It is also important to note that the abelian-by-central results in valuation theory mentioned above ([BT02] and [Pop10] in particular) play a central role in the proof of the known cases of this conjecture.

In this note, we begin an investigation of mod-n abelian-by-central Galois groups in general. The main result of this note uses the Merkurjev-Suslin theorem [MS82] to provide a *formal* description of mod-n abelian-by-central Galois groups and can be seen as an extension of Kummer theory to this non-abelian situation. This gives a *direct* and very *explicit* link between the arithmetic structure of a field $(K, +, \times)$ and the structure of its mod-n abelian-by-central Galois group without doing arithmetic in any proper extensions of K. More precisely, just as Kummer theory describes

the maximal mod-n *abelian* Galois group of a field K (which contains sufficiently many roots of unity) as the group of homomorphisms $K^\times \to \mathbb{Z}/n$, in this note we give a description of the "central" part (i.e. the *non-abelian* part) of the mod-n abelian-by-central Galois group in terms of special *functions* $K \smallsetminus \{0,1\} \to (\mathbb{Z}/n)^2$. This new description is functorial in K and is compatible with Kummer theory via taking commutators of pairs of elements and raising elements to n-th powers. See Theorem 1 below for the precise statement.

We use this formal description of the mod-n abelian-by-central Galois group to determine the existence of certain types of relations in such groups only by considering *Heisenberg quotients* – that is, homomorphisms from the mod-n abelian-by-central Galois group of a field to the Heisenberg group over $\mathbb{Z}/n$. Similar results in this direction were shown by Efrat-Mináč [EM11a], [EM11b] in the mod-p case. See Corollary 1.1, §3, §5 and Theorem 4 for more details.

Finally, using the results involving homomorphisms to the Heisenberg group, we conclude this note by observing that the notion of a *commuting-liftable* pair from [Top14] is equivalent to an *a priori* more general notion, which we call *weakly-commuting-liftable*, whenever one deals with mod-n abelian-by-central Galois groups of a field. This thereby generalizes the main results of loc. cit., which detect valuations using mod-p^n abelian-by-central Galois groups, to even more minimal situations. In addition to this observation, the main results of this note can be seen as a direct generalization of §7 of loc. cit. See §5.1 and Remark 5.2 of this paper for more details concerning commuting-liftable vs. weakly-commuting-liftable pairs.

1.1. **Notation and the main theorem.** Throughout the note, we will only consider continuous functions between discrete and/or profinite sets. We will use this convention with impunity and write "Hom" for the set of continuous homomorphisms, "Fun" for the set of continuous functions, "$f : A \to B$" for a continuous map A to B, etc.

Let K be a field and denote by $\mathrm{Gal}(K)$ its absolute Galois group. Let n be a positive integer which is relatively prime to $\operatorname{char} K$ and assume that $\mu_n \subset K$. Throughout the note we will deal with $\mathbb{Z}/n$ as our ring of coefficients, and we will denote it by Λ.

We recall that the mod-n central descending series of a profinite group $\mathfrak{G}$ is defined inductively as follows:

(1) $\mathfrak{G}^{(1)} = \mathfrak{G}$.
(2) $\mathfrak{G}^{(i+1)} = [\mathfrak{G}, \mathfrak{G}^{(i)}] \cdot (\mathfrak{G}^{(i)})^n$.

In other words, for $i \geq 1$, $\mathfrak{G}^{(i+1)}$ is precisely the left kernel of the canonical pairing

$$\mathfrak{G}^{(i)} \times \mathrm{Hom}_{\mathfrak{G}}(\mathfrak{G}^{(i)}, \Lambda) \to \Lambda$$

where $\mathfrak{G}$ acts on $\mathfrak{G}^{(i)}$ via conjugation, trivially on Λ, and $\mathrm{Hom}_{\mathfrak{G}}(\mathfrak{G}^{(i)}, \Lambda)$ denotes the set of $\mathfrak{G}$-equivariant homomorphisms $\mathfrak{G}^{(i)} \to \Lambda$. For $i \geq 1$, we denote $\mathfrak{G}^{(i)}/\mathfrak{G}^{(i+1)}$ by $\mathfrak{g}_i(\mathfrak{G})$. When $\mathfrak{G}$ is understood from context, we will simplify the notation and denote $\mathfrak{g}_i(\mathfrak{G})$ simply by $\mathfrak{g}_i$. Also in the case where $\mathfrak{G} = \mathrm{Gal}(K)$, the absolute Galois group of a field K as above, we denote $\mathfrak{g}_i(\mathrm{Gal}(K))$ by $\mathfrak{g}_i(K)$. We will generally use additive notation for $\mathfrak{g}_i$ (the exception to this is in Appendix A); in certain cases where we might want to consider $\mathfrak{g}_i$ as a multiplicative group, we will write $\mathfrak{G}^{(i)}/\mathfrak{G}^{(i+1)}$ instead of $\mathfrak{g}_i$.

For $\sigma, \tau \in \mathfrak{g}_1$, we define $[\sigma, \tau] := \tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}$ where $\tilde{\sigma}, \tilde{\tau} \in \mathfrak{G}/\mathfrak{G}^{(3)}$ are some lifts of $\sigma, \tau \in \mathfrak{g}_1 = \mathfrak{G}/\mathfrak{G}^{(2)}$. Since $\mathfrak{G}/\mathfrak{G}^{(3)} \twoheadrightarrow \mathfrak{G}/\mathfrak{G}^{(2)}$ is a central extension, $[\sigma, \tau]$ doesn't depend on the choice of lifts $\tilde{\sigma}, \tilde{\tau}$, and thus $[\bullet, \bullet] : \mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathfrak{g}_2$ is well-defined; it is well-known that $[\bullet, \bullet]$ is Λ-bilinear. For $\sigma \in \mathfrak{g}_1$, we define $\pi(\sigma) := \tilde{\sigma}^n$ where $\tilde{\sigma} \in \mathfrak{G}/\mathfrak{G}^{(3)}$ is some lift of $\sigma \in \mathfrak{g}_1 = \mathfrak{G}/\mathfrak{G}^{(2)}$. If no confusion is possible, we may also write $\pi\sigma := \pi(\sigma)$. As before, $\pi\sigma$ doesn't depend on the choice of lift $\tilde{\sigma}$, and thus $\pi : \mathfrak{g}_1 \to \mathfrak{g}_2$ is a well-defined map. The map π is not Λ-linear in general (e.g. if n is even), but $2 \cdot \pi : \mathfrak{g}_1 \to \mathfrak{g}_2$ is always Λ-linear.

Throughout the note we will work with a *fixed* primitive n-th root of unity $\omega \in \mu_n \subset K$. This choice of ω yields an isomorphism of G_K-modules $\mu_n \cong \Lambda$ by sending $\omega^i \in \mu_n$ to $i \in \Lambda$, which we tacitly use throughout. Kummer theory gives us a perfect pairing:

$$\mathfrak{g}_1(K) \times K^\times/n \to \mu_n,$$

defined by $(\sigma, x) \mapsto \sigma\sqrt[n]{x}/\sqrt[n]{x} \in \mu_n$. Therefore, we obtain an isomorphism $(\bullet)^\omega : \mathfrak{g}_1(K) \to \mathrm{Hom}(K^\times, \Lambda)$ using the Kummer pairing together with our fixed isomorphism $\mu_n \cong \Lambda$. Namely, for $\sigma \in \mathfrak{g}_1(K)$ and $x \in K^\times$, one has $\sigma^\omega(x) = i$ if and only if $\sigma\sqrt[n]{x}/\sqrt[n]{x} = \omega^i$.

For a discrete set S and a profinite set P, we denote by $\mathrm{Fun}(S, P)$ the set of functions $S \to P$. Obviously, any function $S \to P$ is continuous. Because P is profinite, $\mathrm{Fun}(S, P) = P^S$ obtains a natural profinite topology, and this agrees with the compact-open topology of $\mathrm{Fun}(S, P)$.

Let $f, g \in \mathrm{Hom}(K^\times, \Lambda)$ be given. We now introduce two functions $\Phi^\omega(f, g) : K \smallsetminus \{0, 1\} \to \Lambda^2$ and $\Psi^\omega(f) : K \smallsetminus \{0, 1\} \to \Lambda^2$, defined as follows:

(1) $\Phi^\omega(f, g)(x) = (f(x)g(1-x) - f(1-x)g(x),\ f(x)g(\omega) - f(\omega)g(x))$.
(2) $\Psi^\omega(f)(x) = \left(\binom{n}{2}f(x)f(1-x),\ \binom{n}{2}f(x)f(\omega) + f(x)\right)$.

As above, we endow $\mathrm{Fun}(K \smallsetminus \{0, 1\}, \Lambda^2)$ with the compact-open topology, and therefore $\mathrm{Fun}(K \smallsetminus \{0, 1\}, \Lambda^2) = (\Lambda^2)^{K \smallsetminus \{0,1\}}$ is canonically a profinite group. Thus, it makes sense to speak about closed subgroups of $\mathrm{Fun}(K \smallsetminus \{0, 1\}, \Lambda^2)$. We will denote by $\mathfrak{F}_K^\omega$ the closed subgroup of $\mathrm{Fun}(K \smallsetminus \{0, 1\}, \Lambda^2)$ which is topologically generated by the functions $\Phi^\omega(f, g)$ and $\Psi^\omega(f)$ as $f, g \in \mathrm{Hom}(K^\times, \Lambda)$ vary.

Suppose that $L|K$ is an extension of fields. Then the canonically induced map $\phi : \mathrm{Gal}(L) \to \mathrm{Gal}(K)$ restricts to homomorphisms $\phi^{(i)} : \mathrm{Gal}(L)^{(i)} \to \mathrm{Gal}(K)^{(i)}$ for all $i \geq 1$. In particular, we obtain induced homomorphisms $\phi_i : \mathfrak{g}_i(L) \to \mathfrak{g}_i(K)$. These induced maps, for $i = 1, 2$, are clearly compatible with $[\bullet, \bullet]$ and π in the sense that, for all $\sigma, \tau \in \mathfrak{g}_1(K)$, one has $\phi_2[\sigma, \tau] = [\phi_1\sigma, \phi_1\tau]$ and $\phi_2(\pi\sigma) = \pi(\phi_1\sigma)$.

On the other hand, it is clear from the definition that the restriction map $\mathrm{Fun}(L \smallsetminus \{0, 1\}, \Lambda^2) \to \mathrm{Fun}(K \smallsetminus \{0, 1\}, \Lambda^2)$, induced by the inclusion $K \subset L$, restricts to a homomorphism $\mathrm{res}_K : \mathfrak{F}_L^\omega \to \mathfrak{F}_K^\omega$ which sends $\Phi^\omega(f, g)$ to $\Phi^\omega(f|_{K^\times}, g|_{K^\times})$ and $\Psi^\omega(f)$ to $\Psi^\omega(f|_{K^\times})$, for all $f, g \in \mathrm{Hom}(L^\times, \Lambda)$. Thus $\mathfrak{F}_K^\omega$ is functorial in K as long as we endow each such K with the same fixed primitive n-th root of unity ω.

We are now ready to introduce the main theorem of the note, which relates the two profinite groups $\mathfrak{g}_2(K)$ and $\mathfrak{F}_K^\omega$ in a functorial way.

Theorem 1 (Main Theorem)**.** *Let K be a field whose characteristic is prime to n such that $\mu_n \subset K$. Choose $\omega \in \mu_n$ a fixed primitive n-th root of unity. Then there is a canonical isomorphism $\Omega_K : \mathfrak{g}_2(K) \to \mathfrak{F}_K^\omega$ which satisfies:*

(1) $\Omega_K([\sigma, \tau]) = \Phi^\omega(\sigma^\omega, \tau^\omega)$.
(2) $\Omega_K(\pi\sigma) = \Psi^\omega(\sigma^\omega)$.

Moreover, this isomorphism is functorial in K in the sense that if $L|K$ is a field extension, then the canonical map $\mathfrak{g}_2(L) \to \mathfrak{g}_2(K)$ corresponds to the restriction map $\mathfrak{F}_L^\omega \to \mathfrak{F}_K^\omega$ induced by $K \subset L$. Namely, the following diagram commutes:

$$\begin{array}{ccccc} \mathfrak{g}_2(L) & \xrightarrow{\Omega_L} & \mathfrak{F}_L^\omega & \xrightarrow{\text{incl.}} & \mathrm{Fun}(L \smallsetminus \{0,1\}, \Lambda^2) \\ \Big\downarrow{\scriptstyle \text{canon.}} & & \Big\downarrow{\scriptstyle \mathrm{res}_K} & & \Big\downarrow{\scriptstyle (K\subset L)^*} \\ \mathfrak{g}_2(K) & \xrightarrow[\Omega_K]{} & \mathfrak{F}_K^\omega & \xrightarrow[\text{incl.}]{} & \mathrm{Fun}(K \smallsetminus \{0,1\}, \Lambda^2) \end{array}$$

Theorem 1 shows that $\mathfrak{F}_K^\omega$ yields a *functorial formal description* of $\mathfrak{g}_2(K)$ in terms of *functions* on $K \smallsetminus \{0,1\}$ with values in Λ^2. Furthermore, this formal description is compatible with the Kummer isomorphism $(\bullet)^\omega : \mathfrak{g}_1(K) \to \mathrm{Hom}(K^\times, \Lambda)$ by identifying $[\sigma,\tau]$, resp. $\pi\sigma$, with $\Phi^\omega(\sigma^\omega, \tau^\omega)$, resp. $\Psi^\omega(\sigma^\omega)$, for $\sigma, \tau \in \mathfrak{g}_1(K)$. Theorem 1 is proved in §§4.1 and 4.2.

We also prove the following important corollary to Theorem 1, which gives an explicit and fairly restrictive condition on the types of relations that can occur between elements of the form $[\sigma,\tau]$ and $\pi\sigma$ in the group $\mathfrak{g}_2(K)$.

Corollary 1.1 (see Theorem 4)**.** *Let K be a field whose characteristic is prime to n such that $\mu_{2n} \subset K$. Choose $\omega \in \mu_n$ a fixed primitive n-th root of unity. Let $\sigma_i, \tau_i \in \mathfrak{g}_1(K)$ be a collection of elements which converges to 0 in $\mathfrak{g}_1(K)$. Let $a_i, b_i \in \Lambda$ be such that $2 \cdot a_i = \sigma_i^\omega(\omega)$ and $2 \cdot b_i = \tau_i^\omega(\omega)$. Since $\omega \in K^{\times 2}$ by assumption, such a_i, b_i always exist. Then the following are equivalent:*

(1) $\sum_i [\sigma_i, \tau_i] = \sum_i (b_i \cdot (2 \cdot \pi(\sigma_i)) - a_i \cdot (2 \cdot \pi(\tau_i)))$.
(2) $\sum_i [\sigma_i, \tau_i] \in \langle 2 \cdot \pi(\sigma_i), 2 \cdot \pi(\tau_i) \rangle_i$.
(3) $\sum_i [\sigma_i, \tau_i] \in 2 \cdot \pi(\mathfrak{g}_1(K))$.

In particular, the equivalence of (2) and (3) in Corollary 1.1 shows that a pair of elements $\sigma, \tau \in \mathfrak{g}_1(K)$ forms a *commuting-liftable* pair (i.e. $[\sigma,\tau] \in \langle 2 \cdot \pi\sigma, 2 \cdot \pi\tau \rangle$) if and only if σ, τ form a *weakly-commuting-liftable* pair (i.e. $[\sigma,\tau] \in 2 \cdot \pi(\mathfrak{g}_2(K))$). This observation thereby generalizes the various main results of [Top14]; see §5.1 for a more detailed discussion.

2. Cohomological minimal presentations

Most of the cohomological results in this section are fairly well-known for pro-p groups (and n a power of p), due to the existence of *minimal free pro-p presentations* and standard Frattini-type arguments which stem from the Burnside basis theorem. Such cohomological results, concerning pro-p groups of finite rank, go back to Labute [Lab67]; see also the exposition in [NSW08] around Propositions 3.9.13 and 3.9.14. For pro-p groups, these cohomological results were recently further studied by Efrat-Mináč in [EM11b], Section 2, and in [EM11a], Section 10. It is also important to note that in these approaches, in order to carry out the required cocycle calculations, one must choose a basis for H^1 which yields a minimal generating set for the corresponding pro-p group and fixes generators for the minimal free pro-p presentation.

When generalizing to arbitrary profinite groups, however, one no longer has access to these minimal free presentations. Also, the process of choosing a free presentation, and/or choosing a basis for H^1, makes statements about functoriality difficult or even impossible to prove in the usual category of profinite/pro-p groups.

In this section we discuss the main new ingredient introduced in this note. We introduce a *cohomological* analogue of a minimal free presentation for $\mathfrak{g}_2(\mathfrak{G})$, associated to an *arbitrary* profinite group $\mathfrak{G}$, which we denote by $\mathfrak{S}(\mathfrak{G})$. One of the main benefits of our construction is that $\mathfrak{S}(\mathfrak{G})$ is purely functorial in $\mathfrak{G}$.

Throughout this section we will work with a fixed profinite group $\mathfrak{G}$. Thus, we omit $\mathfrak{G}$ from the notation and denote $\mathfrak{g}_i(\mathfrak{G})$ by $\mathfrak{g}_i$. We will denote by $\mathrm{H}^*(\bullet) := \mathrm{H}^*(\bullet, \Lambda)$ the continuous-cochain cohomology of $\bullet$ with values in Λ. Throughout, we will also assume that $\mathfrak{g}_1 := \mathfrak{G}/\mathfrak{G}^{(2)}$ is isomorphic to $(\mathbb{Z}/n)^I$ for some indexing set I. Note that if K is a field whose characteristic is prime to n such that $\mu_n \subset K$, then $\mathfrak{g}_1(K) \cong (\mathbb{Z}/n)^I$, for some indexing set I, by Kummer theory; thus $\mathrm{Gal}(K)$ satisfies our added assumption.

Recall that Pontryagin duality yields a perfect pairing between $\mathrm{H}^1(\mathfrak{g}_1) = \mathrm{H}^1(\mathfrak{G})$ and $\mathfrak{g}_1$. We define $\mathfrak{K}(\mathfrak{G}) := \mathrm{H}^1(\mathfrak{g}_1)$. As with $\mathfrak{g}_i$, we will denote $\mathfrak{K}(\mathfrak{G})$ by $\mathfrak{K}$ throughout this section. Throughout the note, we will identify $\mathfrak{g}_1$ with $\mathrm{Hom}(\mathfrak{K}, \Lambda)$ via the canonical perfect pairing $\mathfrak{g}_1 \times \mathfrak{K} \to \Lambda$.

We recall that the Lyndon-Hochschild-Serre (LHS) spectral sequence associated to the extension $\mathfrak{G} \to \mathfrak{G}/\mathfrak{G}^{(2)} = \mathfrak{g}_1$,

$$\mathrm{H}^i(\mathfrak{g}_1, \mathrm{H}^j(\mathfrak{G}^{(2)})) \Rightarrow \mathrm{H}^{i+j}(\mathfrak{G}),$$

combined with the fact that $\inf : \mathrm{H}^1(\mathfrak{g}_1) \to \mathrm{H}^1(\mathfrak{G})$ is an isomorphism, yields the following exact sequence:

$$0 \to \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} \xrightarrow{d_2} \mathrm{H}^2(\mathfrak{g}_1) \xrightarrow{\inf} \mathrm{H}^2(\mathfrak{G}).$$

Above, d_2 denotes the differential on the E_2-page in the LHS-spectral sequence:

$$d_2 := d_2^{0,1} : \mathrm{E}_2^{0,1} \to \mathrm{E}_2^{2,0}.$$

Furthermore, we recall that the **Bockstein** homomorphism $\beta : \mathrm{H}^1(\mathfrak{g}_1) \to \mathrm{H}^2(\mathfrak{g}_2)$ is the connecting homomorphism in the cohomological long exact sequence associated to the short exact sequence of coefficient modules (recall that $\mathbb{Z}/n = \Lambda$):

$$1 \to \mathbb{Z}/n \xrightarrow{n} \mathbb{Z}/n^2 \to \mathbb{Z}/n \to 1.$$

We denote by $\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1$ the *completed* tensor product of $\mathfrak{g}_1$ with itself. In other words,

$$\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1 = \varprojlim \mathfrak{g}_1/N_1 \otimes \mathfrak{g}_1/N_2$$

where N_1 and N_2 vary over the open subgroups of $\mathfrak{g}_1$ and the tensor product is taken over Λ by considering $\mathfrak{g}_1/N_i$ as Λ-modules in the obvious way. One has a canonical map $\mathfrak{g}_1 \otimes \mathfrak{g}_1 \to \mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1$; if $\sigma, \tau \in \mathfrak{g}_1$, we will abuse the notation and write $\sigma \otimes \tau \in \mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1$ for the image of $\sigma \otimes \tau \in \mathfrak{g}_1 \otimes \mathfrak{g}_1$ under this map. It is easy to see that $\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1$ is Pontryagin dual to $\mathfrak{K} \otimes \mathfrak{K}$ via the pairing $(\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1) \times (\mathfrak{K} \otimes \mathfrak{K}) \to \Lambda$ given by

$$(\sigma \otimes \tau, x \otimes y) \mapsto \sigma(x)\tau(y)$$

and extended linearly. We will therefore sometimes denote elements f of $\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1$ as Λ-bilinear forms $\mathfrak{K} \times \mathfrak{K} \to \Lambda$, just as we denote elements g of $\mathfrak{g}_1$ as homomorphisms $\mathfrak{K} \to \Lambda$.

Denote by $\mathfrak{S}(\mathfrak{G})$ the subset of $(\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1) \times \mathfrak{g}_1$ defined by

$$\mathfrak{S}(\mathfrak{G}) = \left\{ (f, g) \ : \ \forall x \in \mathfrak{K}, \ f(x, x) = \binom{n}{2} \cdot g(x) \right\}.$$

As with $\mathfrak{g}_i$ and $\mathfrak{K}$, we will omit $\mathfrak{G}$ from the notation and denote $\mathfrak{S}(\mathfrak{G})$ by $\mathfrak{S}$ throughout this section. Clearly $\mathfrak{S}$ is a closed subgroup of $(\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1) \times \mathfrak{g}_1$. We also observe that the image of the projection $\mathfrak{S} \to \mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1$ is the subgroup of alternating Λ-bilinear forms on $\mathfrak{K} \times \mathfrak{K}$ with values in Λ.

Lemma 2.1. *In the notation above, one has a surjective map* $(\mathfrak{K} \otimes \mathfrak{K}) \oplus \mathfrak{K} \to \mathrm{H}^2(\mathfrak{g}_1)$ *defined by* $(x \otimes y) \oplus z \mapsto x \cup y + \beta z$ *(extended linearly). Moreover, the kernel of this surjective map is generated by all elements of the form* $(x \otimes x) \oplus (-\binom{n}{2} x)$ *as* $x \in \mathfrak{K}$ *varies. In particular, we obtain a canonical perfect pairing* $(\bullet, \bullet)_{\mathfrak{S}} : \mathfrak{S} \times \mathrm{H}^2(\mathfrak{g}_1) \to \Lambda$, *defined by*

(1) $((f, g), x \cup y)_{\mathfrak{S}} = f(x, y)$,
(2) $((f, g), \beta z)_{\mathfrak{S}} = g(z)$,

and extended linearly.

Proof. Observe that one has a perfect pairing

$$((\mathfrak{g}_1 \widehat{\otimes} \mathfrak{g}_1) \times \mathfrak{g}_1) \times ((\mathfrak{K} \otimes \mathfrak{K}) \oplus \mathfrak{K}) \to \Lambda$$

defined by $((f, g), (x \otimes y) \oplus z) \mapsto f(x, y) + g(z)$. Thus, it suffices to prove that the map $(\mathfrak{K} \otimes \mathfrak{K}) \oplus \mathfrak{K} \to \mathrm{H}^2(\mathfrak{g}_1)$, defined by $(x \otimes y) \oplus z \mapsto x \cup y + \beta z$, is surjective with kernel generated by all elements of the form $(x \otimes x) \oplus (-\binom{n}{2} \cdot x)$. The statement concerning the induced perfect pairing $(\bullet, \bullet)_{\mathfrak{S}}$ would follow immediately from this and the definition of $\mathfrak{S}$.

Recall our overarching assumption that $\mathfrak{g}_1 \cong (\mathbb{Z}/n)^I$ for some indexing set I. Now the required presentation of $\mathrm{H}^2((\mathbb{Z}/n)^I) \cong \mathrm{H}^2(\mathfrak{g}_1)$, as a quotient of $(\mathfrak{K} \otimes \mathfrak{K}) \oplus \mathfrak{K}$, is essentially well-known as it follows from the Künneth formula. We give a brief argument below.

In the case where $\mathfrak{g}_1 \cong \mathbb{Z}/n$ is cyclic, it is well-known that:

(1) $\mathrm{H}^1(\mathbb{Z}/n) = \langle x \rangle \cong \mathbb{Z}/n$, where x is the identity homomorphism $\mathbb{Z}/n \to \mathbb{Z}/n$,
(2) $\mathrm{H}^2(\mathbb{Z}/n) = \langle \beta x \rangle \cong \mathbb{Z}/n$ and
(3) $x \cup x = \binom{n}{2} \beta x$ in $\mathrm{H}^2(\mathbb{Z}/n)$.

Statements (1) and (2) above can be found in any standard book on group cohomology (see e.g. [NSW08], Chapter 1.7). Statement (3) is also well-known, but we note that it follows from Theorem 2 below if we take $\mathfrak{G} = \hat{\mathbb{Z}}$. Namely, $\mathrm{H}^2(\hat{\mathbb{Z}}) = 0$ and $\mathfrak{g}_1(\hat{\mathbb{Z}}) = \mathbb{Z}/n$; therefore $d_2 : \mathrm{H}^1(\hat{\mathbb{Z}}^{(2)})^{\mathbb{Z}/n} \to \mathrm{H}^2(\mathbb{Z}/n)$ is an isomorphism, etc. Thus the lemma is proven in the case where $\#I = 1$. The case where I is finite now follows from the Künneth formula for finite group cohomology, while the case where I is arbitrary follows from the finite I case using a limit argument. □

Lemma 2.2. *In the notation above, the surjective map* $\mathfrak{G}^{(2)} \twoheadrightarrow \mathfrak{g}_2$ *yields a canonical perfect pairing:*

$$(\bullet, \bullet)_{\mathfrak{g}_2} : \mathfrak{g}_2 \times \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} \to \Lambda.$$

The dual of $-d_2 : \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} \to \mathrm{H}^2(\mathfrak{g}_1)$, *via* $(\bullet, \bullet)_{\mathfrak{g}_2}$ *and the pairing* $(\bullet, \bullet)_{\mathfrak{S}}$ *of Lemma* 2.1 *yields a canonical surjective map* $-d_2^{\vee} : \mathfrak{S} \to \mathfrak{g}_2$ *which is defined by the equation* $(-d_2^{\vee}(s), \phi)_{\mathfrak{g}_2} = (s, -d_2\phi)_{\mathfrak{S}}$.

Proof. Recall that $\mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} = \mathrm{Hom}_{\mathfrak{G}}(\mathfrak{G}^{(2)}, \Lambda)$. Thus the first statement follows, using Pontryagin duality, from the definition of $\mathfrak{g}_2 = \mathfrak{G}^{(2)}/\mathfrak{G}^{(3)}$. Indeed, recall that $\mathfrak{G}^{(3)}$ is the left-kernel of the canonical pairing $\mathfrak{G}^{(2)} \times \mathrm{Hom}_{\mathfrak{G}}(\mathfrak{G}^{(2)}, \Lambda) \to \Lambda$. The surjectivity of $-d_2^{\vee} : \mathfrak{S} \to \mathfrak{g}_2$ is immediate, by Pontryagin duality, since $-d_2 : \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} \to \mathrm{H}^2(\mathfrak{g}_1)$ is injective. □

The next theorem and the corollary which follows it are the essential steps in describing the surjective map $-d_2^\vee : \mathfrak{S} \to \mathfrak{g}_2$ of Lemma 2.2 in a more explicit way. Before we state the theorem, we recall our convention that $\mathfrak{g}_1$ is identified with $\mathrm{Hom}(\mathfrak{K}, \Lambda)$; in particular, we write elements of $\mathfrak{g}_1$ as *functions* on $\mathfrak{K}$ with values in Λ.

Theorem 2. *In the notation above, let $u \in \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1}$ be given and consider $\eta := d_2 u$. Choose $x_i, y_i, z_j \in \mathfrak{K}$ such that $\eta = \sum_i x_i \cup y_i + \sum_j \beta z_j$ (this is always possible by Lemma 2.1). Then for all $\sigma, \tau \in \mathfrak{g}_1$, the following hold:*

(1) $-([\sigma,\tau], u)_{\mathfrak{g}_2} = \sum_i \sigma(x_i)\tau(y_i) - \sigma(y_i)\tau(x_i)$ *and*
(2) $-(\pi\sigma, u)_{\mathfrak{g}_2} = \binom{n}{2} \cdot \sum_i \sigma(x_i)\sigma(y_i) + \sum_j \sigma(z_j)$.

Proof. The proof of this theorem involves very explicit cocycle calculations which resemble the calculations in [NSW08], Propositions 3.9.13 and 3.9.14. For the sake of exposition, we defer the detailed proof of this theorem to Appendix A. □

Motivated by the viewpoint that $\mathfrak{S}$ should act as a sort-of free presentation for $\mathfrak{g}_2$, we are interested in finding elements of $\mathfrak{S}$ which map to $[\sigma,\tau]$ and $\pi\sigma$ via the surjective map $-d_2^\vee : \mathfrak{S} \to \mathfrak{g}_2$ described in Lemma 2.2. Therefore, we now introduce two types of elements in $\mathfrak{S}$ which will work in general:

(1) Let $\sigma, \tau \in \mathfrak{g}_1$ be given. Then $(\sigma \otimes \tau - \tau \otimes \sigma, 0) \in \mathfrak{S}$.
(2) Let $\sigma \in \mathfrak{g}_1$ be given. Then $(\binom{n}{2}\sigma \otimes \sigma, \sigma) \in \mathfrak{S}$.

The next corollary to Theorem 2 shows that these special elements of $\mathfrak{S}$ will work for our purposes by mapping to $[\sigma,\tau]$ and $\pi\sigma$.

Corollary 2.3. *In the notation above, consider the surjective map $-d_2^\vee : \mathfrak{S} \to \mathfrak{g}_2$ of Lemma 2.2, which is defined by $(-d_2^\vee(s), \phi)_{\mathfrak{g}_2} = (s, -d_2\phi)_{\mathfrak{S}}$. Then the following hold:*

(1) *For all $\sigma, \tau \in \mathfrak{g}_1$, one has $-d_2^\vee(\sigma \otimes \tau - \tau \otimes \sigma, 0) = [\sigma,\tau]$.*
(2) *For all $\sigma \in \mathfrak{g}_1$, one has $-d_2^\vee(\binom{n}{2}\sigma \otimes \sigma, \sigma) = \pi\sigma$.*

Proof. Let $\sigma, \tau \in \mathfrak{g}_1$ be given. It suffices to prove that for any $u \in \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1}$, the following two equalities hold:

(1) $([\sigma,\tau], u)_{\mathfrak{g}_2} = u([\sigma,\tau]) = ((\sigma \otimes \tau - \tau \otimes \sigma, 0), -d_2(u))_{\mathfrak{S}}$ and
(2) $(\pi\sigma, u)_{\mathfrak{g}_2} = u(\pi\sigma) = ((\binom{n}{2}\sigma \otimes \sigma, \sigma), -d_2(u))_{\mathfrak{S}}$.

But this is precisely Theorem 2 combined with the definition of $(\bullet,\bullet)_{\mathfrak{S}}$ from Lemma 2.1. □

Let R be an arbitrary *subset* of $\mathrm{H}^2(\mathfrak{g}_1)$ and consider the induced restriction homomorphism

$$\mathrm{res}_R : \mathfrak{S} \xrightarrow{s \mapsto (s,\bullet)_{\mathfrak{S}}} \mathrm{Hom}(\mathrm{H}^2(\mathfrak{g}_1), \Lambda) \xrightarrow{\text{restriction}} \mathrm{Fun}(R, \Lambda).$$

We denote the image of res_R by $\mathfrak{S}_R$. As before, we will keep $\mathfrak{G}$ implicit in the notation for $\mathfrak{S}_R$. Note that the kernel $R^\perp$ of $\mathfrak{S} \to \mathfrak{S}_R$ is precisely the annihilator of R with respect to $(\bullet,\bullet)_{\mathfrak{S}}$:

$$R^\perp = \{s \in \mathfrak{S} \ : \ \forall r \in R, \ (s,r)_{\mathfrak{S}} = 0\}.$$

Theorem 3. *In the notation above, let R be an arbitrary generating set for* $\ker(\mathrm{H}^2(\mathfrak{g}_1) \to \mathrm{H}^2(\mathfrak{G}))$. *Then R induces a canonical isomorphism $\Omega_R : \mathfrak{g}_2 \to \mathfrak{S}_R$ defined as follows:*

(1) *For $\sigma, \tau \in \mathfrak{g}_1$, $\Omega_R([\sigma,\tau]) = \mathrm{res}_R(\sigma \otimes \tau - \tau \otimes \sigma, 0)$.*
(2) *For $\sigma \in \mathfrak{g}_1$, $\Omega_R(\pi\sigma) = \mathrm{res}_R(\binom{n}{2}\sigma \otimes \sigma, \sigma)$.*

Proof. Recall the existence of the exact sequence

$$0 \to \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} \xrightarrow{d_2} \mathrm{H}^2(\mathfrak{g}_1) \xrightarrow{\inf} \mathrm{H}^2(\mathfrak{G})$$

and that, by Lemma 2.2, the dual of $-d_2$ yields a surjective map $-d_2^\vee : \mathfrak{S} \to \mathfrak{g}_2$. Also recall that, by Corollary 2.3, $-d_2^\vee$ satisfies the following equalities:

(1) $-d_2^\vee(\sigma \otimes \tau - \tau \otimes \sigma, 0) = [\sigma,\tau]$.
(2) $-d_2^\vee(\binom{n}{2}\sigma \otimes \sigma, \sigma) = \pi\sigma$.

By the definition of $\mathfrak{S}_R$, one has a canonical surjective map $\mathrm{res}_R : \mathfrak{S} \to \mathfrak{S}_R$. Thus, it suffices to prove that the kernel of $-d_2^\vee : \mathfrak{S} \to \mathfrak{g}_2$ is the same as the kernel of $\mathrm{res}_R : \mathfrak{S} \to \mathfrak{S}_R$. Indeed, we then can define $\Omega_R(\delta) := \mathrm{res}_R(\delta_1)$ where $\delta_1 \in \mathfrak{S}$ is chosen such that $-d_2^\vee(\delta_1) = \delta$.

As observed above, the kernel of $\mathrm{res}_R : \mathfrak{S} \to \mathfrak{S}_R$ is precisely $R^\perp$, the annihilator of R with respect to the pairing $(\bullet,\bullet)_{\mathfrak{S}}$. Since R generates the image of $d_2 : \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1} \to \mathrm{H}^2(\mathfrak{g}_1)$, we see that $R^\perp$ is precisely $(\mathrm{im}\, d_2)^\perp = (\mathrm{im}(-d_2))^\perp$. Since the map $-d_2^\vee : \mathfrak{S} \to \mathfrak{g}_2$ was defined to be the dual of $-d_2$, we obtain our claim: that the kernels of $-d_2^\vee$ and res_R are identical. □

Remark 2.4 (Functoriality). The isomorphism Ω_R is functorial in the following sense. Suppose that $\phi : \mathfrak{G} \to \mathfrak{H}$ is a homomorphism of profinite groups. Then ϕ induces canonical homomorphisms $\phi^{(i)} : \mathfrak{G}^{(i)} \to \mathfrak{H}^{(i)}$ for each $i \geq 1$. Therefore, ϕ induces canonical homomorphisms $\phi_i : \mathfrak{g}_i(\mathfrak{G}) \to \mathfrak{g}_i(\mathfrak{H})$ which are compatible with $\phi^{(i)}$. In particular, for all $\sigma, \tau \in \mathfrak{g}_1(\mathfrak{G})$, one has $\phi_2[\sigma,\tau] = [\phi_1\sigma, \phi_1\tau]$ and $\phi_2(\pi\sigma) = \pi(\phi_1\sigma)$. Moreover, the maps ϕ and ϕ_1 yield the following commutative diagram:

$$\begin{array}{ccc} \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G})) & \xrightarrow{\inf} & \mathrm{H}^2(\mathfrak{G}) \\ {\scriptstyle \phi_1^*}\uparrow & & \uparrow{\scriptstyle \phi^*} \\ \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{H})) & \xrightarrow[\inf]{} & \mathrm{H}^2(\mathfrak{H}) \end{array}$$

Suppose that $R(\mathfrak{G})$ denotes a generating set for $\ker(\mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G})) \to \mathrm{H}^2(\mathfrak{G}))$ and $R(\mathfrak{H})$ denotes a generating set for $\ker(\mathrm{H}^2(\mathfrak{g}_1(\mathfrak{H})) \to \mathrm{H}^2(\mathfrak{H}))$ in such a way so that the homomorphism $\phi_1^* : \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{H})) \to \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G}))$ restricts to a map $R(\mathfrak{H}) \to R(\mathfrak{G})$. We will show that ϕ_1^* induces a canonical map $\phi_1^{**} : \mathfrak{S}_{R(\mathfrak{G})} \to \mathfrak{S}_{R(\mathfrak{H})}$ which is compatible with ϕ_2 via Theorem 3. In other words, we will show that the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{g}_2(\mathfrak{G}) & \xrightarrow{\Omega_{R(\mathfrak{G})}} & \mathfrak{S}_{R(\mathfrak{G})} \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \phi_1^{**}} \\ \mathfrak{g}_2(\mathfrak{H}) & \xrightarrow[\Omega_{R(\mathfrak{H})}]{} & \mathfrak{S}_{R(\mathfrak{H})} \end{array} \tag{2.1}$$

and that it is compatible with $[\bullet,\bullet]$ and π similarly to Theorem 3.

To see this, first observe that the dual of $\phi_1^* : \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{H})) \to \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G}))$, via $(\bullet,\bullet)_{\mathfrak{S}}$, yields a homomorphism $(\phi_1^*)^\vee : \mathfrak{S}(\mathfrak{G}) \to \mathfrak{S}(\mathfrak{H})$. Furthermore, since ϕ_1^* restricts to a function $R(\mathfrak{H}) \to R(\mathfrak{G})$, we obtain a commutative diagram:

$$\begin{array}{ccc} \mathfrak{S}(\mathfrak{G}) & \xrightarrow{\mathrm{res}_{R(\mathfrak{G})}} & \mathrm{Fun}(R(\mathfrak{G}),\Lambda) \\ {\scriptstyle (\phi_1^*)^\vee}\downarrow & & \downarrow{\scriptstyle \phi_1^{**}} \\ \mathfrak{S}(\mathfrak{H}) & \xrightarrow[\mathrm{res}_{R(\mathfrak{H})}]{} & \mathrm{Fun}(R(\mathfrak{H}),\Lambda) \end{array} \tag{2.2}$$

Thus ϕ_1^{**} in (2.2) restricts to a canonical homomorphism $\phi_1^{**} : \mathfrak{S}_{R(\mathfrak{G})} \to \mathfrak{S}_{R(\mathfrak{H})}$ since these groups are the images of the horizontal maps in diagram (2.2). Namely, we obtain a commutative diagram:

$$\begin{array}{ccc} \mathfrak{S}(\mathfrak{G}) & \xrightarrow{\mathrm{res}_{R(\mathfrak{G})}} & \mathfrak{S}_{R(\mathfrak{G})} \\ {\scriptstyle (\phi_1^*)^\vee}\downarrow & & \downarrow{\scriptstyle \phi_1^{**}} \\ \mathfrak{S}(\mathfrak{H}) & \xrightarrow[\mathrm{res}_{R(\mathfrak{H})}]{} & \mathfrak{S}_{R(\mathfrak{H})} \end{array} \tag{2.3}$$

where the horizontal arrows are surjective.

On the other hand, the functoriality of the LHS-spectral sequence yields the following commutative diagram:

$$\begin{array}{ccc} \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1(\mathfrak{G})} & \xrightarrow{-d_2} & \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G})) \\ {\scriptstyle (\phi^{(2)})^*}\uparrow & & \uparrow{\scriptstyle \phi_1^*} \\ \mathrm{H}^1(\mathfrak{H}^{(2)})^{\mathfrak{g}_1(\mathfrak{H})} & \xrightarrow[-d_2]{} & \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{H})) \end{array} \tag{2.4}$$

We observe that $(\phi^{(2)})^*$ in diagram (2.4) is dual to ϕ_2 via the pairing $(\bullet,\bullet)_{\mathfrak{g}_2}$ (see Lemma 2.2). Thus, dualizing diagram (2.4) via the pairings $(\bullet,\bullet)_{\mathfrak{S}}$ and $(\bullet,\bullet)_{\mathfrak{g}_2}$ as in Lemma 2.2, we obtain the commutative diagram:

$$\begin{array}{ccc} \mathfrak{S}(\mathfrak{G}) & \xrightarrow{-d_2^\vee} & \mathfrak{g}_2(\mathfrak{G}) \\ {\scriptstyle (\phi_1^*)^\vee}\downarrow & & \downarrow{\scriptstyle \phi_2} \\ \mathfrak{S}(\mathfrak{H}) & \xrightarrow[-d_2^\vee]{} & \mathfrak{g}_2(\mathfrak{H}) \end{array} \tag{2.5}$$

whose horizontal arrows are surjective.

Lastly, the commutativity of diagram (2.1) follows from the fact that the kernel of $\mathrm{res}_{R(\bullet)}$ from diagram (2.3) is precisely the same as the kernel of $-d_2^\vee : \mathfrak{S}(\bullet) \to \mathfrak{g}_2(\bullet)$ from diagram (2.5), for $\bullet = \mathfrak{G}, \mathfrak{H}$, along with the definition of $\Omega_{R(\bullet)}$; see the proof of Theorem 3. Also, it follows from Corollary 2.3 and the proof of Theorem 3 that, for all $\sigma, \tau \in \mathfrak{g}_1(\mathfrak{G})$, the following hold:

(1) $\phi_1^{**}(\Omega_{R(\mathfrak{G})}[\sigma,\tau]) = \Omega_{R(\mathfrak{H})}(\phi_2[\sigma,\tau]) = \Omega_{R(\mathfrak{H})}([\phi_1\sigma,\phi_1\tau])$ and
(2) $\phi_1^{**}(\Omega_{R(\mathfrak{G})}(\pi\sigma)) = \Omega_{R(\mathfrak{H})}(\phi_2(\pi\sigma)) = \Omega_{R(\mathfrak{H})}(\pi(\phi_1\sigma))$.

3. The Heisenberg group

In this section we will explore an explicit example: the Heisenberg group over Λ. In particular, we will explicitly work through the consequences of Theorem 3, resp. Remark 2.4, for the Heisenberg group, resp. homomorphisms to the Heisenberg group.

3.1. **Recalling facts about the Heisenberg group.** We denote by $\mathcal{H}_\Lambda$ the Heisenberg group over Λ. Namely, $\mathcal{H}_\Lambda$ is the set of all 3×3 upper-triangular matrices with coefficients in the ring Λ, whose diagonal entries are 1. To simplify the notation we denote elements of $\mathcal{H}_\Lambda$ as follows:

$$h(a,b;c) := \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus, multiplication in $\mathcal{H}_\Lambda$ works as follows:

$$h(a,b;c) \cdot h(a',b';c') = h(a+a', b+b'; c+c'+ab').$$

A simple calculation shows that $\mathcal{H}_\Lambda^{(3)}$ is trivial, the map $h(0,0;c) \mapsto c$ yields an isomorphism $\mathfrak{g}_2(\mathcal{H}_\Lambda) \cong \Lambda$, and the map $h(a,b;c) \to (a,b)$ yields an isomorphism $\mathfrak{g}_1(\mathcal{H}_\Lambda) \cong \Lambda^2$. We will denote the image of $h(a,b;c)$ in $\mathfrak{g}_1(\mathcal{H}_\Lambda)$ by $h_1(a,b)$, and we will denote $h(0,0;c)$ by $h_2(c)$. A simple calculation shows that:

(1) $[h_1(a,b), h_1(a',b')] = h_2(ab' - a'b)$.
(2) $\pi(h_1(a,b)) = h_2(\binom{n}{2}ab)$.

Denote by e_1, e_2 the basis for $\mathfrak{K}(\mathcal{H}_\Lambda) = \mathrm{H}^1(\mathfrak{g}_1(\mathcal{H}_\Lambda))$ which is dual to $h_1(1,0)$, $h_1(0,1)$. In other words, the isomorphism $h_1^{-1} : \mathfrak{g}_1(\mathcal{H}_\Lambda) \to \Lambda^2$ is precisely the map (e_1, e_2). This allows us to describe the equivalence class of $\mathcal{H}_\Lambda$ as an extension of $\mathfrak{g}_1(\mathcal{H}_\Lambda) \cong \Lambda^2$ by $\mathfrak{g}_2(\mathcal{H}_\Lambda) \cong \Lambda$ as follows.

Lemma 3.1. *Consider $\mathcal{H}_\Lambda$ as an extension of $\mathfrak{g}_1(\mathcal{H}_\Lambda)$ by Λ via the isomorphism $h_2 : \Lambda \to \mathfrak{g}_2(\mathcal{H}_\Lambda)$. Then the class of $\mathcal{H}_\Lambda$ in $\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda))$ is given by $e_1 \cup e_2$.*

Proof. A 2-cocycle representing the equivalence class of $\mathcal{H}_\Lambda$ in $\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda))$ is given by the following formula:

$$(h_1(a,b), h_1(a',b')) \mapsto h(a,b;0) \cdot h(a',b';0) \cdot h(-(a+a'), -(b+b'); 0)^{-1} \in \mathfrak{g}_2(\mathcal{H}_\Lambda).$$

A simple calculation shows that

$$h(a,b;0) \cdot h(a',b';0) \cdot h(-(a+b'), -(b+b'); 0)^{-1} = h(0,0;ab').$$

Thus, this 2-cocycle representing the class of $\mathcal{H}_\Lambda$ in $\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda))$ is given by

$$\xi : (h_1(a,b), h_1(a',b')) \mapsto ab'.$$

Furthermore, since $e_i(h_1(a_1,a_2)) = a_i$ for $i = 1,2$, we see that the class of $\mathcal{H}_\Lambda$ is indeed equal to $e_1 \cup e_2 \in \mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda))$ since $e_1 \cup e_2$ is represented by the same cocycle ξ. □

By Lemma 3.1, we see that $e_1 \cup e_2 \in \ker(\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda)) \to \mathrm{H}^2(\mathcal{H}_\Lambda))$ (see e.g. Proposition 3.2 below). Moreover, the isomorphism $h_2^{-1} : \mathfrak{g}_2(\mathcal{H}_\Lambda) \to \Lambda$, which we can consider as an element of $\mathrm{H}^1(\mathcal{H}_\Lambda^{(2)})^{\mathfrak{g}_1(\mathcal{H}_\Lambda)}$, satisfies $-d_2(h_2^{-1}) = e_1 \cup e_2$ by Theorem 2 and the calculations above. Since h_2^{-1} generates $\mathrm{H}^1(\mathcal{H}_\Lambda^{(2)})^{\mathfrak{g}_1(\mathcal{H}_\Lambda)}$, we see that $e_1 \cup e_2$ is a generator for $\ker(\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\lambda)) \to \mathrm{H}^2(\mathcal{H}_\Lambda))$. In particular, Theorem 3

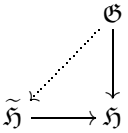
yields an isomorphism $\Omega_{e_1\cup e_2} : \mathfrak{g}_2(\mathcal{H}_\Lambda) \to \Lambda$ which satisfies the following properties for $\sigma, \tau \in \mathfrak{g}_1(\mathcal{H}_\Lambda)$:

(1) $\Omega_{e_1\cup e_2}([\sigma,\tau]) = \sigma(e_1)\tau(e_2) - \sigma(e_2)\tau(e_1)$.
(2) $\Omega_{e_1\cup e_2}(\pi\sigma) = \binom{n}{2}\sigma(e_1)\sigma(e_2)$.

3.2. **Recalling facts about embedding problems.** An embedding problem $\mathcal{E}$ is a pair of homomorphisms of profinite groups with the same codomain:

$$\mathcal{E} := (\widetilde{\mathfrak{H}} \to \mathfrak{H} \ ; \ \mathfrak{G} \to \mathfrak{H}).$$

A solution to the embedding problem $\mathcal{E}$ is a homomorphism $\mathfrak{G} \to \widetilde{\mathfrak{H}}$ which makes the following diagram commute:



If $\widetilde{\mathfrak{H}} \to \mathfrak{H}$ is a surjective homomorphism, which we consider as a group extension of $\mathfrak{H}$ by $\ker(\widetilde{\mathfrak{H}} \to \mathfrak{H})$, we denote the embedding problem $(\widetilde{\mathfrak{H}} \to \mathfrak{H}; \mathfrak{G} \to \mathfrak{H})$ simply by $(\widetilde{\mathfrak{H}}; \mathfrak{G} \to \mathfrak{H})$.

Proposition 3.2. *Let $\xi \in \mathrm{H}^2(\mathfrak{H}, A)$ represent two equivalent group extensions $\widetilde{\mathfrak{H}}, \widetilde{\mathfrak{H}}'$ of $\mathfrak{H}$ by A, and let $\phi : \mathfrak{G} \to \mathfrak{H}$ be a homomorphism. Then the following conditions are equivalent:*

(1) *$(\widetilde{\mathfrak{H}}; \phi)$ has a solution.*
(2) *$(\widetilde{\mathfrak{H}}'; \phi)$ has a solution.*
(3) *ξ is in the kernel of $\phi^* : \mathrm{H}^2(\mathfrak{H}, A) \to \mathrm{H}^2(\mathfrak{G}, A)$.*

Proof. Since $\widetilde{\mathfrak{H}}$ and $\widetilde{\mathfrak{H}}'$ are equivalent, one has a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \widetilde{\mathfrak{H}} & \longrightarrow & \mathfrak{H} & \longrightarrow & 1 \\ & & \| & & \downarrow \cong & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & \widetilde{\mathfrak{H}}' & \longrightarrow & \mathfrak{H} & \longrightarrow & 1 \end{array}$$

From this it is clear that (1) and (2) are equivalent.

Assume that $(\widetilde{\mathfrak{H}}; \phi)$ has a solution, say $\tilde{\phi}$. Recall that $\phi^*\xi$ has a representative group extension given by the fiber product $\widetilde{\mathfrak{H}} \times_{\mathfrak{H}} \mathfrak{G}$. The universal property of fiber products applied to $\tilde{\phi}$ yields a splitting of the short exact sequence

$$1 \to A \to \widetilde{\mathfrak{H}} \times_{\mathfrak{H}} \mathfrak{G} \to \mathfrak{G} \to 1.$$

Thus $\phi^*\xi$ is trivial as it is represented by a split extension.

Similarly, if $\phi^*\xi$ is trivial, then there is a splitting $\mathfrak{G} \to \widetilde{\mathfrak{H}} \times_{\mathfrak{H}} \mathfrak{G}$ of the short exact sequence above. Composing this splitting with the canonical map $\widetilde{\mathfrak{H}} \times_{\mathfrak{H}} \mathfrak{G} \to \widetilde{\mathfrak{H}}$ yields a solution to the embedding problem $(\widetilde{\mathfrak{H}}; \phi)$. □

By Proposition 3.2, it makes sense to define embedding problems of the form $(\xi; \phi)$, for $\xi \in \mathrm{H}^2(\mathfrak{H}, A)$ and $\phi : \mathfrak{G} \to \mathfrak{H}$. Saying that $(\xi; \phi)$ has a solution is equivalent to saying that $\phi^*\xi = 0$ in $\mathrm{H}^2(\mathfrak{G})$.

Proposition 3.3. *Let $\mathfrak{G}$ be a profinite group. Let $x, y \in \mathfrak{K}(\mathfrak{G}) = \mathrm{H}^1(\mathfrak{g}_1(\mathfrak{G}))$ be given and consider the homomorphism $(x, y) : \mathfrak{g}_1(\mathfrak{G}) \to \Lambda^2$ induced by x, y. Then the embedding problem*

$$\mathcal{E}_{x,y} := (\mathcal{H}_\Lambda \twoheadrightarrow \mathfrak{g}_1(\mathcal{H}_\Lambda) \xrightarrow{(e_1,e_2)} \Lambda^2 \ ; \ \mathfrak{G}/\mathfrak{G}^{(3)} \twoheadrightarrow \mathfrak{g}_1(\mathfrak{G}) \xrightarrow{(x,y)} \Lambda^2)$$

has a solution if and only if the image of $x \cup y$ vanishes in $\mathrm{H}^2(\mathfrak{G})$.

Proof. First assume that $\mathcal{E}_{x,y}$ has a solution. The fact that $x \cup y$ vanishes in $\mathrm{H}^2(\mathfrak{G})$ follows from Proposition 3.2 and the fact that $e_1 \cup e_2$ generates the kernel of $\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda)) \to \mathrm{H}^2(\mathcal{H}_\Lambda)$ (see the discussion which follows Lemma 3.1). Indeed, Proposition 3.2 implies that the image of $x \cup y$ vanishes in $\mathrm{H}^2(\mathfrak{G}/\mathfrak{G}^{(3)})$, and thus the image of $x \cup y$ also vanishes in $\mathrm{H}^2(\mathfrak{G})$.

Conversely, assume that the image of $x \cup y$ vanishes in $\mathrm{H}^2(\mathfrak{G})$. Then by Proposition 3.2 and Lemma 3.1, we obtain a solution $\phi_0 : \mathfrak{G} \to \mathcal{H}_\Lambda$ for the embedding problem:

$$\widetilde{\mathcal{E}}_{x,y} := (\mathcal{H}_\Lambda \twoheadrightarrow \mathfrak{g}_1(\mathcal{H}_\Lambda) \xrightarrow{(e_1,e_2)} \Lambda^2 \ ; \ \mathfrak{G} \twoheadrightarrow \mathfrak{g}_1(\mathfrak{G}) \xrightarrow{(x,y)} \Lambda^2).$$

However, since $\mathcal{H}_\Lambda^{(3)} = 0$, the solution ϕ_0 descends to a solution $\phi : \mathfrak{G}/\mathfrak{G}^{(3)} \to \mathcal{H}_\Lambda$ for our original embedding problem $\mathcal{E}_{x,y}$. □

3.3. **Relations induced by the Heisenberg group.** In this section we show how one can determine certain kinds of relations between elements of the form $[\sigma, \tau]$ and $\pi\sigma$ by looking at homomorphisms $\mathfrak{g}_1 \to \Lambda^2$ which lift to homomorphisms $\mathfrak{G}/\mathfrak{G}^{(3)} \to \mathcal{H}_\Lambda$. We briefly recall the notation introduced in Remark 2.4: for a homomorphism $\phi : \mathfrak{G} \to \mathfrak{H}$, one obtains induced homomorphisms $\phi_i : \mathfrak{g}_i(\mathfrak{G}) \to \mathfrak{g}_i(\mathfrak{H})$ which satisfy $\phi_2[\sigma, \tau] = [\phi_1\sigma, \phi_1\tau]$ and $\phi_2(\pi\sigma) = \pi(\phi_1\sigma)$ for all $\sigma, \tau \in \mathfrak{g}_1(\mathfrak{G})$.

Let us first make a couple of observations concerning convergence of elements in profinite groups. Let $\mathfrak{G}$ be an arbitrary profinite group and let $\sigma_i \in \mathfrak{G}$ be given, with a possibly infinite indexing set for i. Recall that the collection $(\sigma_i)_i$ *converges to* 1 provided that, for all open normal subgroups N of $\mathfrak{G}$, all but finitely many of the σ_i are contained in N. If $\mathfrak{G}$ is an abelian profinite group and $(\sigma_i)_i$ converges to 1, then one obtains a well-defined element $\prod_i \sigma_i$ of $\mathfrak{G}$, since the product is well-defined in every (continuous) finite quotient of $\mathfrak{G}$.

Assume that one is given a collection $(\sigma_i)_i$ of elements $\sigma_i \in \mathfrak{g}_1(\mathfrak{G})$. Then $(\sigma_i)_i$ converges to 0 in $\mathfrak{g}_1(\mathfrak{G})$ if and only if, for all $x \in \mathfrak{K}(\mathfrak{G}) = \mathrm{H}^1(\mathfrak{g}_1(\mathfrak{G}))$, all but finitely many of the $\sigma_i(x)$ are trivial. Furthermore, since $[\bullet, \bullet]$ and π are continuous, if $(\sigma_i, \tau_i, \gamma_j)_{i,j}$ converges to 0 in $\mathfrak{g}_1(\mathfrak{G})$, then $([\sigma_i, \tau_i], \pi(\gamma_j))_{i,j}$ converges to 0 in $\mathfrak{g}_2(\mathfrak{G})$.

Proposition 3.4. *Let $\mathfrak{G}$ be a profinite group with $\mathfrak{g}_1(\mathfrak{G})$ isomorphic to $(\mathbb{Z}/n)^I$ for some indexing set I. Let $x, y \in \mathfrak{K}(\mathfrak{G}) = \mathrm{H}^1(\mathfrak{g}_1(\mathfrak{G}))$ be given and consider the homomorphism $(x, y) : \mathfrak{g}_1(\mathfrak{G}) \to \Lambda^2$ induced by x, y. Suppose furthermore that the equivalent conditions of Proposition 3.3 hold and that $\phi : \mathfrak{G}/\mathfrak{G}^{(3)} \to \mathcal{H}_\Lambda$ is a solution to the embedding problem:*

$$\mathcal{E}_{x,y} := (\mathcal{H}_\Lambda \twoheadrightarrow \mathfrak{g}_1(\mathcal{H}_\Lambda) \xrightarrow{(e_1,e_2)} \Lambda^2 \ ; \ \mathfrak{G}/\mathfrak{G}^{(3)} \twoheadrightarrow \mathfrak{g}_1(\mathfrak{G}) \xrightarrow{(x,y)} \Lambda^2).$$

Let $\sigma_i, \tau_i \in \mathfrak{g}_1(\mathfrak{G})$ be given, and assume that the collection $(\sigma_i, \tau_i)_i$ converges to 0 in $\mathfrak{g}_1(\mathfrak{G})$. Then the following are equivalent:

(1) $\sum_i [\phi_1\sigma_i, \phi_1\tau_i] = 0$, *as elements of* $\mathfrak{g}_2(\mathcal{H}_\Lambda)$.
(2) $\sum_i (\sigma_i(x) \cdot \tau_i(y) - \sigma_i(y) \cdot \tau_i(x)) = 0$.

Proof. Recall that $e_1 \cup e_2$ generates $\ker(\mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda)) \to \mathrm{H}^2(\mathcal{H}_\Lambda))$. Moreover, if we denote by ϕ_1 the homomorphism $\mathfrak{g}_1(\mathfrak{G}) \to \mathfrak{g}_1(\mathcal{H}_\Lambda)$ defined by $\sigma \mapsto h_1(\sigma(x), \sigma(y))$, then the image of $e_1 \cup e_2$ under the induced map $\phi_1^* : \mathrm{H}^2(\mathfrak{g}_1(\mathcal{H}_\Lambda)) \to \mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G}))$ is precisely $x \cup y$. Our assumptions ensure that $x \cup y$ is contained in $\ker(\mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G})) \to \mathrm{H}^2(\mathfrak{G}))$. Therefore, we can choose R, a set of generators for $\ker(\mathrm{H}^2(\mathfrak{g}_1(\mathfrak{G})) \to \mathrm{H}^2(\mathfrak{G}))$, which contains $x \cup y$.

Consider the isomorphisms $\Omega_{e_1 \cup e_2} : \mathfrak{g}_2(\mathfrak{H}_\Lambda) \to \mathfrak{S}_{e_1 \cup e_2}$ and $\Omega_R : \mathfrak{g}_2(\mathfrak{G}) \to \mathfrak{S}_R$ of Theorem 3. Since $\phi_1^*(e_1 \cup e_2) = x \cup y \in R$, we obtain a canonical restriction map $\phi_1^{**} : \mathfrak{S}_R \to \mathfrak{S}_{e_1 \cup e_2}$ which is compatible with the canonical map $\phi_2 : \mathfrak{g}_2(\mathfrak{G}) \to \mathfrak{g}_2(\mathcal{H}_\Lambda)$ as discussed in Remark 2.4. Therefore, the restriction to $e_1 \cup e_2$, under the inclusion $e_1 \cup e_2 \mapsto x \cup y \in R$, of the element

$$\Omega_R\left(\sum_i [\sigma_i, \tau_i]\right) = \sum_i \Omega_R([\sigma_i, \tau_i]) = \sum_i \mathrm{res}_R(\sigma_i \otimes \tau_i - \tau_i \otimes \sigma_i, 0),$$

is trivial if and only if $\phi_2(\sum_i [\sigma_i, \tau_i]) = 0$ in $\mathfrak{g}_2(\mathcal{H}_\Lambda)$. In other words, $\phi_2(\sum_i [\sigma_i, \tau_i]) = 0$ if and only if

$$\sum_i \sigma_i(x)\tau_i(y) - \sigma_i(y)\tau_i(x) = 0.$$

This proves the proposition since $\phi_2(\sum_i [\sigma_i, \tau_i]) = \sum_i [\phi_1\sigma_i, \phi_1\tau_i]$. □

In §5, we will use Proposition 3.4 to explicitly describe certain kinds of relations among elements of the form $[\sigma, \tau]$ and $\pi\sigma$ in $\mathfrak{g}_2(K)$ for a field K whose characteristic is prime to n such that $\mu_n \subset K$; see Theorem 4 for the details.

4. Galois groups

The goal for this section will be to prove Theorem 1. Throughout this section K will be a field whose characteristic is prime to n such that $\mu_n \subset K$, and $\omega \in \mu_n$ will be a fixed primitive n-th root of unity. In many cases we will denote $\mathrm{H}^*(\mathrm{Gal}(K), \bullet)$ by $\mathrm{H}^*(K, \bullet)$ as is usual; when we wish to emphasize the connection with previous notation, we will still use the notation $\mathrm{H}^*(\mathrm{Gal}(K), \bullet)$. Continuing with the previous notation, our profinite group $\mathfrak{G}$ will be $\mathrm{Gal}(K)$ in the remainder of the note. Kummer theory yields a canonical perfect pairing

$$\mathfrak{g}_1(K) \times K^\times/n \to \mu_n.$$

Thus, we will identify $K^\times/n$ with $\mathfrak{K} = \mathrm{H}^1(\mathfrak{g}_1(K))$ via our choice of $\omega \in \mu_n$, as follows. For $x \in K^\times$, we denote by x_ω the homomorphism $\mathfrak{g}_1(K) \to \Lambda$ defined by $x_\omega(\sigma) = i$ if and only if $\sigma \sqrt[n]{x}/\sqrt[n]{x} = \omega^i$. Thus the map $x \mapsto x_\omega$ yields an isomorphism $K^\times/n \to \mathfrak{K} = \mathrm{H}^1(\mathfrak{g}_1(K))$. Lastly, as in §2, we identify $\mathfrak{g}_1(K)$ canonically with $\mathrm{Hom}(\mathfrak{K}, \Lambda)$. The connection with the notation of §§1.1 and 2 is as follows: for $\sigma \in \mathfrak{g}_1(K)$ and $x \in K^\times$, one has $x_\omega \in \mathfrak{K}$ and $\sigma^\omega(x) = \sigma(x_\omega)$.

The following lemma calculates the Bockstein map in Galois cohomology. This calculation seems to be fairly well-known: see [GS06], Lemma 7.5.10 and/or [EM11b], Proposition 2.6. We provide a precise proof of the lemma for the sake of completeness.

Lemma 4.1. *Let K be a field whose characteristic is prime to n such that $\mu_n \subset K$ and let $\omega \in \mu_n$ be a chosen primitive n-th root of unity. Let $\inf_K$ denote the inflation*

map $\mathrm{H}^2(\mathfrak{g}_1(K)) \to \mathrm{H}^2(\mathrm{Gal}(K))$. *One has the following equality in* $\mathrm{H}^2(\mathrm{Gal}(K))$ *for all* $x \in K^\times$*:*

$$\inf_K(\beta x_\omega) = \inf_K(\omega_\omega \cup x_\omega).$$

Proof. We denote by $\delta_i : \mathrm{H}^m(K, \mathbb{Z}/n(i)) \to \mathrm{H}^{m+1}(K, \mathbb{Z}/n(i))$ the connecting homomorphism associated to the short exact sequence of $\mathrm{Gal}(K)$-modules:

$$1 \to \mathbb{Z}/n(i) \to \mathbb{Z}/n^2(i) \to \mathbb{Z}/n(i) \to 1.$$

Observe that the isomorphism $\mathrm{H}^m(K, \Lambda) \to \mathrm{H}^m(K, \Lambda(i))$, induced by ω, is given by

$$\alpha \mapsto \alpha \cup (\underbrace{\omega \cup \cdots \cup \omega}_{i \text{ times}})$$

where we consider ω as an element of $\mu_n = \mathrm{H}^0(K, \Lambda(1))$. Furthermore, for $x \in \mu_n = \mathrm{H}^0(K, \Lambda(1))$, we observe that

$$x_\omega \cup \omega = \delta_1(x)$$

since the Kummer homomorphism $K^\times = \mathrm{H}^0(K, (K^{\mathrm{sep}})^\times) \to \mathrm{H}^1(K, \Lambda(1))$ is precisely the connecting homomorphism associated to

$$1 \to \mu_n \to (K^{\mathrm{sep}})^\times \xrightarrow{n} (K^{\mathrm{sep}})^\times \to 1.$$

To conclude the proof of the lemma, it suffices to prove the following claim: for all $\alpha \in \mathrm{H}^1(K, \Lambda)$, one has

$$\delta_0(\alpha) \cup \omega \cup \omega = \delta_1(\omega) \cup (\alpha \cup \omega).$$

Indeed, then one would have

$$\begin{aligned} \delta_0(\alpha) \cup \omega \cup \omega &= \delta_1(\omega) \cup (\alpha \cup \omega) \\ &= (\omega_\omega \cup \omega) \cup (\alpha \cup \omega) \\ &= (\omega_\omega \cup \alpha) \cup \omega \cup \omega \end{aligned}$$

which implies that $\delta_0(\alpha) = \omega_\omega \cup \alpha$.

To prove this claim, we calculate using the well-known elementary identities involving cup products and connecting homomorphisms (see e.g. [NSW08], Proposition 1.4.3):

$$\begin{aligned} \delta_0(\alpha) \cup \omega \cup \omega &= \delta_1(\alpha \cup \omega) \cup \omega \\ &= \delta_1(\omega \cup \alpha) \cup \omega \\ &= \delta_1(\omega) \cup (\alpha \cup \omega). \end{aligned}$$

Thus we obtain the claim and the lemma follows. □

Lemma 4.2. *Let* K *be a field whose characteristic is prime to* n *such that* $\mu_n \subset K$*, and let* $\omega \in \mu_n$ *be a primitive* n*-th root of unity. Then the kernel of* $\inf_K : \mathrm{H}^2(\mathfrak{g}_1(K)) \to \mathrm{H}^2(\mathrm{Gal}(K))$ *is generated by all elements of the form:*

(1) $x_\omega \cup (1-x)_\omega$,
(2) $x_\omega \cup \omega_\omega + \beta x_\omega$,

as $x \in K \smallsetminus \{0, 1\}$ *varies.*

Proof. By the Merkurjev-Suslin theorem [MS82], the composition

$$\mathrm{H}^1(\mathfrak{g}_1(K)) \otimes \mathrm{H}^1(\mathfrak{g}_1(K)) \xrightarrow{\cup} \mathrm{H}^2(\mathfrak{g}_1(K)) \xrightarrow{\inf} \mathrm{H}^2(\mathrm{Gal}(K))$$

is surjective, with kernel generated by all elements of the form $x_\omega \otimes (1-x)_\omega$. Thus, the lemma easily follows from Lemma 2.1 and Lemma 4.1. □

4.1. **The proof of Theorem 1 – construction of Ω_K.** For simplicity, we let $\mathbb{K}$ denote $K \smallsetminus \{0,1\}$. Furthermore, consider the set

$$R(K) := \{x_\omega \cup (1-x)_\omega\}_{x\in\mathbb{K}} \cup \{x_\omega \cup \omega_\omega + \beta x_\omega\}_{x\in\mathbb{K}} \subset H^2(\mathfrak{g}_1(K)).$$

Then one has a surjective function

$$\mathcal{M}_K : \mathbb{K} \sqcup \mathbb{K} \to R(K),$$

which is defined by sending x in the first $\mathbb{K}$ component to $x_\omega \cup (1-x)_\omega$ and x in the second $\mathbb{K}$ component to $x_\omega \cup \omega_\omega + \beta x_\omega$. By Lemma 4.2, $R(K)$ is a generating set for $\ker(\mathrm{H}^2(\mathfrak{g}_1(K)) \to \mathrm{H}^2(\mathrm{Gal}(K))$.

The surjective function $\mathcal{M}_K$ induces an *injective* homomorphism:

$$\mathcal{M}_K^* : \mathrm{Fun}(R(K), \Lambda) \hookrightarrow \mathrm{Fun}(\mathbb{K} \sqcup \mathbb{K}, \Lambda) = \mathrm{Fun}(\mathbb{K}, \Lambda)^2 = \mathrm{Fun}(\mathbb{K}, \Lambda^2).$$

Explicitly, this homomorphism sends a function $f : R(K) \to \Lambda$ to the function $\mathbb{K} \to \Lambda^2$ defined by

$$x \mapsto (f(x_\omega \cup (1-x)_\omega),\ f(x_\omega \cup \omega + \beta x_\omega)).$$

Now we consider the inclusion induced by $\Omega_{R(K)}$ of Theorem 3 composed with $\mathcal{M}_K^*$ from above:

$$\Omega_K : \mathfrak{g}_2(K) \xrightarrow{\Omega_{R(K)}} \mathfrak{S}_{R(K)} \subset \mathrm{Fun}(R(K), \Lambda) \xrightarrow{\mathcal{M}_K^*} \mathrm{Fun}(\mathbb{K}, \Lambda^2).$$

This map will induce our required isomorphism Ω_K between $\mathfrak{g}_2(K)$ and $\mathfrak{F}_K^\omega \subset \mathrm{Fun}(\mathbb{K}, \Lambda^2)$. Namely, it remains to prove that the image of Ω_K, as defined above, is precisely $\mathfrak{F}_K^\omega$. In other words, now we need to trace through the maps to describe $\Omega_K([\sigma,\tau])$ and $\Omega_K(\pi\sigma)$ as functions $\mathbb{K} \to \Lambda^2$.

Let $\sigma, \tau \in \mathfrak{g}_1(K)$ be given. We first recall that by Theorem 3:

(1) $\Omega_{R(K)}([\sigma,\tau]) = \mathrm{res}_{R(K)}(\sigma \otimes \tau - \tau \otimes \sigma, 0)$.
(2) $\Omega_{R(K)}(\pi\sigma) = \mathrm{res}_{R(K)}(\binom{n}{2}\sigma \otimes \sigma, \sigma)$.

Next we calculate $(\bullet,\bullet)_{\mathfrak{S}}$ from Lemma 2.1, applied to our special elements of $\mathfrak{S}$ and arbitrary elements of $R(K)$, while recalling that $\sigma(x_\omega) = \sigma^\omega(x)$ for all $\sigma \in \mathfrak{g}_1(K)$ and $x \in K^\times$. First, we calculate with $(\sigma \otimes \tau - \tau \otimes \sigma, 0) \in \mathfrak{S}$:

(1) $((\sigma \otimes \tau - \tau \otimes \sigma, 0), x_\omega \cup (1-x)_\omega)_{\mathfrak{S}} = \sigma^\omega(x)\tau^\omega(1-x) - \tau^\omega(x)\sigma^\omega(1-x)$ and
(2) $((\sigma \otimes \tau - \tau \otimes \sigma, 0), x_\omega \cup \omega_\omega + \beta x_\omega)_{\mathfrak{S}} = \sigma^\omega(x)\tau^\omega(\omega) - \tau^\omega(x)\sigma^\omega(\omega)$.

And now we calculate with $(\binom{n}{2}\sigma \otimes \sigma, \sigma) \in \mathfrak{S}$:

(1) $((\binom{n}{2}\sigma \otimes \sigma, \sigma), x_\omega \cup (1-x)_\omega)_{\mathfrak{S}} = \binom{n}{2}\sigma^\omega(x)\sigma^\omega(1-x)$ and
(2) $((\binom{n}{2}\sigma \otimes \sigma, \sigma), x_\omega \cup \omega_\omega + \beta x_\omega)_{\mathfrak{S}} = \binom{n}{2}\sigma^\omega(x)\sigma^\omega(\omega) + \sigma^\omega(x)$.

The final ingredient is the definition of $\mathcal{M}_K^*$, which sends a function $f : R(K) \to \Lambda$ to the function $x \mapsto (f(x_\omega \cup (1-x)_\omega), f(x_\omega \cup \omega_\omega + \beta x_\omega))$. Now it's a simple matter of putting everything together. Namely, for $\sigma, \tau \in \mathfrak{g}_1(K)$, $x \in \mathbb{K}$, and Ω_K as defined above, one has:

(1) $\Omega_K([\sigma,\tau])(x) = (\sigma^\omega(x)\tau^\omega(1-x) - \sigma^\omega(1-x)\tau^\omega(x),\ \sigma^\omega(x)\tau^\omega(\omega) - \sigma^\omega(\omega)\tau^\omega(x))$.
(2) $\Omega_K(\pi\sigma)(x) = (\binom{n}{2} \cdot \sigma^\omega(x)\sigma^\omega(1-x),\ \binom{n}{2}\sigma^\omega(x)\sigma^\omega(\omega) + \sigma^\omega(x))$.

Hence $\Omega_K([\sigma,\tau]) = \Phi^\omega(\sigma^\omega,\tau^\omega)$ and $\Omega_K(\pi\sigma) = \Psi^\omega(\sigma^\omega)$, by the definition of Φ^ω and Ψ^ω. Since $\mathfrak{g}_2(K)$ is (topologically) generated by elements of the form $[\sigma,\tau]$ and $\pi\sigma$ as $\sigma,\tau \in \mathfrak{g}_1(K)$ vary, $\mathfrak{F}_K^\omega$ is generated by $\Phi^\omega(f,g)$ and $\Psi^\omega(f)$ as $f,g \in \mathrm{Hom}(K^\times,\Lambda)$ vary, and $(\bullet)^\omega : \mathfrak{g}_1(K) \to \mathrm{Hom}(K^\times,\Lambda)$ is an isomorphism, we see that $\mathfrak{F}_K^\omega$ is indeed the image of Ω_K. Thus, the calculation above completes the proof that Ω_K is an isomorphism between $\mathfrak{g}_2(K)$ and $\mathfrak{F}_K^\omega$ which satisfies the requirements of Theorem 1.

4.2. **The proof of Theorem 1 – functoriality.** As noted above, $\mathfrak{g}_2(K)$ is topologically generated by elements of the form $[\sigma,\tau]$ and $\pi\sigma$, as $\sigma,\tau \in \mathfrak{g}_1(K)$ vary, while $\mathfrak{F}_K^\omega$ is (defined to be) topologically generated by $\Phi^\omega(f,g)$ and $\Psi^\omega(f)$, as $f,g \in \mathrm{Hom}(K^\times,\Lambda)$ vary. Also recall that the image of Ω_K is precisely $\mathfrak{F}_K^\omega$, so that $\Omega_K : \mathfrak{g}_2(K) \to \mathfrak{F}_K^\omega$ is our desired isomorphism. The functoriality in Theorem 1 now follows immediately from the fact that, for all fields K as in the theorem, Ω_K is an isomorphism which sends $[\sigma,\tau]$ to $\Phi^\omega(\sigma^\omega,\tau^\omega)$ and $\pi\sigma$ to $\Psi^\omega(\sigma^\omega)$.

More precisely, let us consider a situation where $K \hookrightarrow L$ is a field extension. Then one obtains a canonical map $\phi : \mathrm{Gal}(L) \to \mathrm{Gal}(K)$ which induces canonical maps $\phi_i : \mathfrak{g}_i(L) \to \mathfrak{g}_i(K)$ for $i = 1,2$, which are compatible with $[\bullet,\bullet]$ and π. That is, if $\sigma,\tau \in \mathfrak{g}_1(K)$, then $\phi_2([\sigma,\tau]) = [\phi_1\sigma,\phi_1\tau]$ and $\phi_2(\pi\sigma) = \pi(\phi_1\sigma)$. Furthermore, one has $\mathrm{res}_K(\Phi^\omega(f,g)) = \Phi^\omega(f|_{K^\times}, g|_{K^\times})$ and $\mathrm{res}_K(\Psi^\omega(f)) = \Psi^\omega(f|_{K^\times})$. Lastly, one has $(\phi_1\sigma)^\omega = (\sigma^\omega)|_{K^\times}$. Combining all these compatibility properties, along with the fact that Ω_K and Ω_L are both isomorphisms, we obtain the desired functoriality.

We now give an alternative proof of functoriality which uses the discussion of Remark 2.4. First, observe that the canonical homomorphism $\phi_1^* : \mathrm{H}^2(\mathfrak{g}_1(K)) \to \mathrm{H}^2(\mathfrak{g}_1(L))$ restricts to a map $R(K) \to R(L)$, where $R(K)$ and $R(L)$ are as defined in §4.1. Thus, as in Remark 2.4, we obtain a homomorphism $\phi_1^{**} : \mathfrak{S}_{R(L)} \to \mathfrak{S}_{R(K)}$ which is compatible with $\phi_2 : \mathfrak{g}_2(L) \to \mathfrak{g}_2(K)$ in the sense that the following diagram commutes:

$$\begin{array}{ccc} \mathfrak{g}_2(L) & \xrightarrow{\Omega_{R(L)}} & \mathfrak{S}_{R(L)} \\ \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_1^{**}} \\ \mathfrak{g}_2(K) & \xrightarrow[\Omega_{R(K)}]{} & \mathfrak{S}_{R(K)} \end{array}$$

and the following compatibility properties hold:

(1) $\phi_1^{**}(\Omega_{R(L)}([\sigma,\tau])) = \Omega_{R(K)}(\phi_2[\sigma,\tau]) = \Omega_{R(K)}([\phi_1\sigma,\phi_1\tau])$.
(2) $\phi_1^{**}(\Omega_{R(L)}(\pi\sigma)) = \Omega_{R(K)}(\phi_2(\pi\sigma)) = \Omega_{R(K)}(\pi(\phi_1\sigma))$.

If we define $\mathbb{L} := L \smallsetminus \{0,1\}$, then the map $R(K) \to R(L)$ is compatible with the embedding $\mathbb{K} \hookrightarrow \mathbb{L}$ in the sense that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{K} \sqcup \mathbb{K} & \xrightarrow{K \subset L} & \mathbb{L} \sqcup \mathbb{L} \\ \downarrow{\scriptstyle \mathcal{M}_K} & & \downarrow{\scriptstyle \mathcal{M}_L} \\ R(K) & \xrightarrow[\phi_1^*]{} & R(L) \end{array}$$

Thus, we obtain the following commutative diagram:

$$\begin{array}{ccccccc}
\mathfrak{g}_2(L) & \xrightarrow{\Omega_{R(L)}} & \mathfrak{S}_{R(L)} & \xrightarrow{\text{incl.}} & \mathrm{Fun}(R(L),\Lambda) & \xrightarrow{\mathcal{M}_L^*} & \mathrm{Fun}(\mathbb{L},\Lambda^2) \\
\downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_1^{**}} & & \downarrow{\scriptstyle \phi_1^{**}} & & \downarrow{\scriptstyle (K\subset L)^*} \\
\mathfrak{g}_2(K) & \xrightarrow[\Omega_{R(K)}]{} & \mathfrak{S}_{R(K)} & \xrightarrow[\text{incl.}]{} & \mathrm{Fun}(R(K),\Lambda) & \xrightarrow[\mathcal{M}_K^*]{} & \mathrm{Fun}(\mathbb{K},\Lambda^2)
\end{array}$$

and functoriality follows since Ω_L, resp. Ω_K, is the composition of the maps on the top, resp. bottom, row of the diagram above. This completes the proof of Theorem 1.

5. Relations in abelian-by-central Galois groups

Theorem 1 can be used to determine every relation that occurs among the elements $[\sigma,\tau]$ and $\pi\sigma$ within $\mathfrak{g}_2(K)$. Below is an example of a result which restricts the types of relations that occur in these Galois groups. The following theorem proves, among other things, that every relation in $\mathfrak{g}_2(K)/(2\cdot\pi(\mathfrak{g}_2(K)))$, between elements of the form $[\sigma,\tau]$, can be determined by looking only at homomorphisms from $\mathrm{Gal}(K)/(\mathrm{Gal}(K)^{(3)}\cdot\mathrm{Gal}(K)^{2n})$ to $\mathcal{H}_\Lambda$, the Heisenberg group over Λ.

First, we briefly recall some facts concerning convergence of elements in $\mathfrak{g}_1(K)$ and $\mathfrak{g}_2(K)$. Let K be a field whose characteristic is prime to n such that $\mu_n\subset K$, and choose $\omega\in\mu_n$ a primitive n-th root of unity. Let $\sigma_i,\tau_i,\gamma_j\in\mathfrak{g}_1(K)$ be given, with i,j varying over possibly infinite indexing sets. Assume that the collection $([\sigma_i,\tau_i],\pi(\gamma_j))_{i,j}$ converges to 0 in $\mathfrak{g}_2(K)$. Then the following three sums are well-defined elements of $\mathfrak{g}_2(K)$:

(1) $\sum_i[\sigma_i,\tau_i]+\sum_j\pi(\gamma_j)$.
(2) $\sum_i[\sigma_i,\tau_i]$.
(3) $\sum_j\pi(\gamma_j)$.

Moreover, recall that if $(\sigma_i,\tau_i,\gamma_j)_{i,j}$ converges to 0 in $\mathfrak{g}_1(K)$, then the collection $([\sigma_i,\tau_i],\pi(\gamma_j))_{i,j}$ converges to 0 in $\mathfrak{g}_2(K)$. The connection with Kummer theory is as follows: a collection $(\sigma_i)_i$ of elements $\sigma_i\in\mathfrak{g}_1(K)$ converges to 0 if and only if, for all $x\in K^\times$, all but finitely many of the $\sigma_i^\omega(x)$ vanish.

Recall that $\mathrm{Fun}(K\smallsetminus\{0,1\},\Lambda^2)$, endowed with the compact-open topology, is naturally an abelian profinite group. In this case, a collection $(f_i)_i$ of elements $f_i\in\mathrm{Fun}(K\smallsetminus\{0,1\},\Lambda^2)$ converges to 0 if and only if, for all $x\in K\smallsetminus\{0,1\}$, all but finitely many of the $f_i(x)$ vanish. In this case, the sum $\sum_i f_i$ yields a well-defined element of $\mathrm{Fun}(K\smallsetminus\{0,1\},\Lambda^2)$ which is the function defined by $x\mapsto\sum_i f_i(x)$. Since all but finitely many of the $f_i(x)$ are 0, the sum $\sum_i f_i(x)$ is a well-defined element in Λ^2.

Lastly, recall that the isomorphism $\Omega_K:\mathfrak{g}_2(K)\to\mathfrak{F}_K^\omega$ from Theorem 1 is an isomorphism of abelian profinite groups. In particular, Ω_K identifies $\mathfrak{g}_2(K)$ with a closed subgroup of $\mathrm{Fun}(K\smallsetminus\{0,1\},\Lambda^2)$. Thus, we see that the collection $([\sigma_i,\tau_i],\pi(\gamma_j))_{i,j}$ converges to 0 in $\mathfrak{g}_2(K)$ if and only if

$$(\Omega_K([\sigma_i,\tau_i]),\Omega_K(\pi(\gamma_j)))_{i,j}=(\Phi^\omega(\sigma_i^\omega,\tau_i^\omega),\Psi^\omega(\gamma_j^\omega))_{i,j}$$

converges to 0 in $\mathrm{Fun}(K\smallsetminus\{0,1\},\Lambda^2)$.

In Theorem 4 below, the various statements deal with possibly infinite sums. However, one of the assumptions of the theorem, that $(\sigma_i,\tau_i)_i$ converges to 0 in

$\mathfrak{g}_1(K)$, ensures that all of these possibly infinite sums are actually well-defined elements in their respective profinite groups, as discussed above. Because we use it in the statement of Theorem 4, we also recall the well-known fact that the map $2 \cdot \pi : \mathfrak{g}_1 \to \mathfrak{g}_2$ is Λ-linear; this fact also follows easily from Theorem 3.

Theorem 4. *Let K be a field whose characteristic is prime to n such that $\mu_{2n} \subset K$. Choose a primitive n-th root of unity $\omega \in \mu_n$. Let $\sigma_i, \tau_i \in \mathfrak{g}_1(K)$ be given with the indexing set for i possibly infinite, and assume that $(\sigma_i, \tau_i)_i$ converges to 0 in $\mathfrak{g}_1(K)$. Then the following are equivalent:*

(1) $\sum_i (\sigma_i^\omega(x) \cdot \tau_i^\omega(1-x) - \sigma_i^\omega(1-x) \cdot \tau_i^\omega(x)) = 0$ *for all* $x \in K \smallsetminus \{0,1\}$.
(2) $\sum_i [\sigma_i, \tau_i] = \sum_i (b_i \cdot (2 \cdot \pi(\sigma_i)) - a_i \cdot (2 \cdot \pi(\tau_i)))$ *where* $\sigma_i^\omega(\omega) = 2 \cdot a_i$ *and* $\tau_i^\omega(\omega) = 2 \cdot b_i$ *(such $a_i, b_i \in \Lambda$ exist since $\omega \in K^{\times 2}$).*
(3) $\sum_i [\sigma_i, \tau_i] \in \langle 2 \cdot \pi(\sigma_i), 2 \cdot \pi(\tau_i) \rangle_i$.
(4) $\sum_i [\sigma_i, \tau_i] \in 2 \cdot \pi(\mathfrak{g}_1(K))$.
(5) *For all homomorphisms $\phi \colon \mathrm{Gal}(K)/\mathrm{Gal}(K)^{(3)} \to \mathcal{H}_\Lambda$, one has $\sum_i [\phi_1 \sigma_i, \phi_1 \tau_i] = 0$, as elements of $\mathfrak{g}_2(\mathcal{H}_\Lambda)$.*
(6) $\sum_i (\sigma_i^\omega(x) \cdot \tau_i^\omega(y) - \sigma_i^\omega(y) \cdot \tau_i^\omega(x)) = 0$, *for all $x, y \in K^\times$ such that the image of $x_\omega \cup y_\omega$ vanishes in $\mathrm{H}^2(\mathrm{Gal}(K))$.*
(7) *For all $x \in K \smallsetminus \{0,1\}$, there exists some solution $\phi : \mathrm{Gal}(K)/\mathrm{Gal}(K)^{(3)} \to \mathcal{H}_\Lambda$ to the embedding problem $\mathcal{E}_{x,1-x}$, such that $\sum_i [\phi_1 \sigma_i, \phi_1 \tau_i] = 0$ as elements of $\mathfrak{g}_2(\mathcal{H}_\Lambda)$.*

Proof. To prove the equivalence of these statements, we will show the following implications: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1), (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (1) and (5) $\Rightarrow$ (7) $\Rightarrow$ (1).

Let us assume (1). Then by Theorem 1, one has

$$\Omega_K(\sum_i [\sigma_i, \tau_i])(x) = (0, \sum_i (\sigma_i^\omega(x) \tau_i^\omega(\omega) - \sigma_i^\omega(\omega) \tau_i^\omega(x))).$$

On the other hand, recall that $\Omega_K(2 \cdot \pi\sigma)(x) = (0, 2 \cdot \sigma^\omega(x))$. Since ω is a square in K, we obtain (2) as follows. Choose $a_i, b_i \in \Lambda$ such that $\sigma_i^\omega(\omega) = 2 \cdot a_i$ and $\tau_i^\omega(\omega) = 2 \cdot b_i$. Then the equation above implies that

$$\sum_i [\sigma_i, \tau_i] = \sum_i (b_i \cdot (2 \cdot \pi(\sigma_i)) - a_i \cdot (2 \cdot \pi(\tau_i))).$$

The implications (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are trivial.

Assume (4). Then, by Theorem 1, one has $\Omega_K(\sum_i [\sigma_i, \tau_i]) = (0, 2 \cdot \gamma_\omega)$ for some $\gamma \in \mathfrak{g}_1(K)$. But then (1) follows immediately from Theorem 1 since the first component of $\Omega_K(\sum_i [\sigma_i, \tau_i])(x)$ is precisely

$$\sum_i (\sigma_i^\omega(x) \cdot \tau_i^\omega(1-x) - \sigma_i^\omega(1-x) \cdot \tau_i^\omega(x)).$$

Thus (1), (2), (3) and (4) are equivalent.

Assume (4) and let $\phi : \mathrm{Gal}(K)/\mathrm{Gal}(K)^{(3)} \to \mathcal{H}_\Lambda$ be given as in (5). Recall that for all $\gamma \in \mathfrak{g}_1(\mathcal{H}_\Lambda)$, the element $2 \cdot \pi\gamma \in \mathfrak{g}_2(\mathcal{H}_\Lambda)$ is trivial. Therefore, $\phi_2(\sum_i [\sigma_i, \tau_i])$ is trivial. Thus we obtain (5).

The implication (5) $\Rightarrow$ (6) follows immediately from Proposition 3.4, recalling that for $\sigma \in \mathfrak{g}_1(K)$ and $x \in K^\times$ one has $\sigma^\omega(x) = \sigma(x_\omega)$. The implication (6) $\Rightarrow$ (1) is obvious since, for all $x \in K \smallsetminus \{0,1\}$, the image of $x_\omega \cup (1-x)_\omega$ is trivial in

$\mathrm{H}^2(\mathrm{Gal}(K))$. Lastly, (5) $\Rightarrow$ (7) is trivial, while (7) $\Rightarrow$ (1) is, again, simply applying Proposition 3.4. □

5.1. **Weakly-commuting-liftable pairs.** Let K be a field whose characteristic is relatively prime to n such that $\mu_{2n} \subset K$. We recall the definition of a CL-pair from [Top14]: a pair of elements $\sigma, \tau \in \mathfrak{g}_1(K)$ is called a **commuting-liftable** pair (or a **CL**-pair for short) provided that $[\sigma, \tau] \in \langle 2 \cdot \pi\sigma, 2 \cdot \pi\tau \rangle$. More generally, we will say that σ, τ are a **weakly-commuting-liftable** pair (or **WCL**-pair for short) provided that $[\sigma, \tau] \in 2 \cdot \pi(\mathfrak{g}_2(K))$. Clearly, any CL-pair is a WCL-pair, and thus the condition defining a WCL-pair is *a priori* weaker than the condition defining a CL-pair. The equivalence of (3) and (4) in Theorem 4 immediately implies the *equivalence* of the two notions.

Corollary 5.1. *Let K be a field whose characteristic is relatively prime to n such that $\mu_{2n} \subset K$. Let $\sigma, \tau \in \mathfrak{g}_1(K)$ be given. Then the following are equivalent:*

(1) *σ, τ form a CL-pair.*
(2) *σ, τ form a WCL-pair.*

Remark 5.2. Let ℓ be a prime and let $m \geq 1$ be given. For a field K consider $\mathcal{G}_K := \mathrm{Gal}(K(\ell)|K)$, the maximal pro-$\ell$ Galois group of K. Then, for any $M \gg m$, the main theorems in [Top14] show how to detect certain *minimized inertia and decomposition* subgroups of $\mathcal{G}_K/([\mathcal{G}_K, \mathcal{G}_K] \cdot \mathcal{G}_K^{\ell^m})$, using $\mathcal{G}_K/([\mathcal{G}_K, \mathcal{G}_K] \cdot \mathcal{G}_K^{\ell^M})$ endowed with the *subset of CL-pairs* in $(\mathcal{G}_K/([\mathcal{G}_K, \mathcal{G}_K] \cdot \mathcal{G}_K^{\ell^M}))^2$, as long as $\mathrm{char}\, K \neq \ell$ and $\mu_{2\ell^M} \subset K$. Moreover, if $m = 1$, then $M = 1$ suffices, and loc. cit. computes an explicit M which works in general, depending on ℓ and m. Using Corollary 5.1, we can replace *"CL-pairs"* with *"WCL-pairs"* in the above context. Since the defining condition for WCL-pairs is *weaker* than the condition for CL-pairs, we obtain an immediate strengthening of the main results of [Top14].

Appendix A. Cocycle calculations

The goal for this section will be to provide a complete and self-contained proof of Theorem 2. When dealing with finitely generated pro-p groups, the cocycle calculations that follow are fairly well-known and were carried out, using minimal free pro-p presentations and the Burnside basis theorem, by Labute [Lab67]; see also the exposition in [NSW08], Propositions 3.9.13 and 3.9.14. We generalize these calculations below by completely avoiding the use of minimal free presentations (which need not exist in general).

In this section we will use the notation of §2. Namely, $\mathfrak{G}$ is an arbitrary profinite group such that $\mathfrak{g}_1(\mathfrak{G}) \cong (\mathbb{Z}/n)^I$ for some indexing set I, $\mathfrak{g}_i := \mathfrak{g}_i(\mathfrak{G})$, and $\mathfrak{K} := \mathrm{H}^1(\mathfrak{g}_1, \Lambda) = \mathrm{H}^1(\mathfrak{G}, \Lambda)$. We also canonically identify $\mathfrak{g}_1$ with $\mathrm{Hom}(\mathfrak{K}, \Lambda)$ via the perfect pairing $\mathfrak{g}_1 \times \mathfrak{K} \to \Lambda$.

For $x \in \mathfrak{K}$ and $\sigma \in \mathfrak{g}_1$, we let $f_x(\sigma)$ denote the unique integer $0 \leq f_x(\sigma) < n$ such that $f_x(\sigma) \mod n = \sigma(x)$. For $x, y \in \mathfrak{K}$ and $\sigma, \tau \in \mathfrak{g}_1$, we define:

$$\mathrm{U}_{x,y}(\sigma, \tau) := \sigma(x) \cdot \tau(y)$$

and

$$\mathrm{B}_x(\sigma, \tau) := \begin{cases} 0, & \text{if } f_x(\sigma) + f_x(\tau) < n, \\ 1, & \text{if } f_x(\sigma) + f_x(\tau) \geq n. \end{cases}$$

It is immediately clear that $\mathrm{U}_{x,y} : \mathfrak{g}_1^2 \to \Lambda$ is a 2-cocycle which represents the class of $x \cup y$ in $\mathrm{H}^2(\mathfrak{g}_1)$. On the other hand, a simple calculation using the definition of the Bockstein map as the connecting homomorphism $\mathrm{H}^1(\mathfrak{g}_1) \to \mathrm{H}^2(\mathfrak{g}_1)$ associated to

$$1 \to \mathbb{Z}/n \xrightarrow{n} \mathbb{Z}/n^2 \to \mathbb{Z}/n \to 1$$

shows that $\mathrm{B}_x : \mathfrak{g}_1^2 \to \Lambda$ is a 2-cocycle which represents the class of $\beta x \in \mathrm{H}^2(\mathfrak{g}_1)$.

Before we proceed, let us make a couple of observations. First, if $\sigma(x) = \sigma'(x)$ and $\tau(y) = \tau'(y)$, then $\mathrm{U}_{x,y}(\sigma,\tau) = \mathrm{U}_{x,y}(\sigma',\tau')$. Similarly, if $\sigma(x) = \sigma'(x)$ and $\tau(x) = \tau'(x)$, then $\mathrm{B}_x(\sigma,\tau) = \mathrm{B}_x(\sigma',\tau')$. In the remainder of this section, we will write $\mathfrak{g}_1$ multiplicatively (contrary to our previous convention) in order to avoid confusion with multiplicative notation involving elements of $\mathfrak{G}$, which we will need below in the proof of Theorem 2.

Proposition A.1. *In the notation above, let $x, y \in \mathfrak{K}$ and $\sigma, \tau \in \mathfrak{g}_1$ be given. Then the following identities hold:*

(1) $\mathrm{U}_{x,y}(\sigma,\tau) + \mathrm{U}_{x,y}(\tau^{-1},\sigma\tau) - \mathrm{U}_{x,y}(\tau^{-1},\tau) = \sigma(x)\tau(y) - \sigma(y)\tau(x)$.
(2) $\sum_{i=0}^{n-1} \mathrm{U}_{x,y}(\sigma^i,\sigma) = \binom{n}{2}\sigma(x)\sigma(y)$.
(3) $\mathrm{B}_x(\sigma,\tau) + \mathrm{B}_x(\tau^{-1},\sigma\tau) - \mathrm{B}_x(\tau^{-1},\tau) = 0$.
(4) $\sum_{i=0}^{n-1} \mathrm{B}_x(\sigma^i,\sigma) = \sigma(x)$.

Proof. (1) One has

$$\begin{aligned}
&\mathrm{U}_{x,y}(\sigma,\tau) + \mathrm{U}_{x,y}(\tau^{-1},\sigma\tau) - \mathrm{U}_{x,y}(\tau^{-1},\tau) \\
&\quad = \sigma(x)\tau(y) - \tau(x)\cdot(\sigma(y)+\tau(y)) + \tau(x)\tau(y) \\
&\quad = \sigma(x)\tau(y) - \sigma(y)\tau(x).
\end{aligned}$$

(2) One has

$$\begin{aligned}
\sum_{i=0}^{n-1} \mathrm{U}_{x,y}(\sigma^i,\sigma) &= \sum_{i=0}^{n-1} i\cdot\sigma(x)\sigma(y) \\
&= \binom{n}{2}\cdot\sigma(x)\sigma(y).
\end{aligned}$$

(3) If $\tau(x) = 0$, it follows immediately from the definition that the expression $\mathrm{B}_x(\sigma,\tau) + \mathrm{B}_x(\tau^{-1},\sigma\tau) - \mathrm{B}_x(\tau^{-1},\tau)$ vanishes (all three terms in the expression are 0 in this case). Let us therefore assume that $\tau(x) \neq 0$ and thus $f_x(\tau) \neq 0$. In this case, one has $f_x(\tau^{-1}) = n - f_x(\tau)$ and so $\mathrm{B}_x(\tau^{-1},\tau) = 1$. If $f_x(\sigma) + f_x(\tau) < n$, then $\mathrm{B}_x(\sigma,\tau) = 0$ while $\mathrm{B}_x(\tau^{-1},\sigma\tau) = 1$ since

$$\begin{aligned}
f_x(\tau^{-1}) + f_x(\sigma\tau) &= (n - f_x(\tau)) + (f_x(\sigma) + f_x(\tau)) \\
&= n + f_x(\sigma) \geq n.
\end{aligned}$$

On the other hand, if $f_x(\sigma) + f_x(\tau) \geq n$, then $\mathrm{B}_x(\sigma,\tau) = 1$ while $\mathrm{B}_x(\tau^{-1},\sigma\tau) = 0$ since

$$\begin{aligned}
f_x(\tau^{-1}) + f_x(\sigma\tau) &= (n - f_x(\tau)) + (f_x(\sigma) + f_x(\tau) - n) \\
&= f_x(\sigma) < n.
\end{aligned}$$

In either case, we see that the expression $\mathrm{B}_x(\sigma,\tau) + \mathrm{B}_x(\tau^{-1},\sigma\tau) - \mathrm{B}_x(\tau^{-1},\tau)$ vanishes, as required.

(4) For $a', b' \in \mathbb{Z}_{\geq 0}$, define

$$\mathrm{B}(a', b') := \begin{cases} 0, & \text{if } a' + b' < n, \\ 1, & \text{if } a' + b' \geq n, \end{cases}$$

so that $\mathrm{B}(f_x(\sigma), f_x(\tau)) = \mathrm{B}_x(\sigma, \tau)$.

Define $a := f_x(\sigma)$. Let $g = \gcd(a, n)$ and let $e \in \mathbb{Z}$ be the integer such that $a = g \cdot e$. Observe that as i varies from 0 to $n-1$, the integer $f_x(\sigma^i)$ varies over $0, g, 2g, \ldots, (\frac{n}{g} - 1) \cdot g$ and each one of these integers occurs precisely g times. Now we may calculate:

$$\begin{aligned} \sum_{i=0}^{n-1} \mathrm{B}_x(\sigma^i, \sigma) &= \sum_{i=0}^{n-1} \mathrm{B}(f_x(\sigma^i), f_x(\sigma)) \\ &= g \cdot \sum_{j=0}^{\frac{n}{g}-1} \mathrm{B}(j \cdot g, e \cdot g). \end{aligned}$$

Note that the j such that $0 \leq j < \frac{n}{g}$ and $j \cdot g + e \cdot g \geq n$ (equivalently, $\mathrm{B}(j \cdot g, e \cdot g) = 1$) are precisely the j such that $\frac{n}{g} - e \leq j < \frac{n}{g}$; there are precisely e such integers j. The other j such that $0 \leq j < \frac{n}{g}$ (i.e. those j such that $j \cdot g + e \cdot g < n$) all satisfy $\mathrm{B}(j \cdot g, e \cdot g) = 0$. Thus

$$\sum_{j=0}^{\frac{n}{g}-1} \mathrm{B}(j \cdot g, e \cdot g) = e,$$

and therefore

$$\sum_{i=0}^{n-1} \mathrm{B}_x(\sigma^i, \sigma) = g \cdot e = a = \sigma(x).$$

This completes the proof of the proposition. □

We now prove Theorem 2.

Proof of Theorem 2. Let $\tilde{\sigma}$, resp. $\tilde{\tau} \in \mathfrak{G}$, be arbitrary elements, and denote their images in $\mathfrak{g}_1$ by σ, resp. τ. To simplify the notation, for $\tilde{\sigma}, \tilde{\tau}$ as above, we will define $\mathrm{U}_{x,y}(\tilde{\sigma}, \tilde{\tau}) := \mathrm{U}_{x,y}(\sigma, \tau)$ and $\mathrm{B}_z(\tilde{\sigma}, \tilde{\tau}) := \mathrm{B}_z(\sigma, \tau)$.

Let η be an element of $\ker(\mathrm{H}^2(\mathfrak{g}_1) \to \mathrm{H}^2(\mathfrak{G}))$. Choose a representation $\eta = \sum_i x_i \cup y_i + \sum_j \beta z_j$ with $x_i, y_i, z_j \in \mathfrak{K}$, as in Lemma 2.1. Consider $\xi : \mathfrak{G}^2 \to \Lambda$ defined by the formula

$$\xi : (\tilde{\sigma}, \tilde{\tau}) \mapsto \sum_i \mathrm{U}_{x_i, y_i}(\tilde{\sigma}, \tilde{\tau}) + \sum_j \mathrm{B}_{z_j}(\tilde{\sigma}, \tilde{\tau}).$$

Then ξ is a 2-cocycle which represents the inflation of η to $\mathfrak{G}$. Since the cohomology class of ξ is trivial in $\mathrm{H}^2(\mathfrak{G})$, there exists $u : \mathfrak{G} \to \Lambda$, a cochain such that $du = \rho$. In other words,

$$u(\tilde{\sigma}\tilde{\tau}) = u(\tilde{\sigma}) + u(\tilde{\tau}) - \xi(\tilde{\sigma}, \tilde{\tau}).$$

Furthermore, by adding a constant to u, we may assume without loss that $u(1) = 0$. Thus

$$u(\tilde{\sigma}^{-1}) = -u(\tilde{\sigma}) + \xi(\tilde{\sigma}^{-1}, \tilde{\sigma}).$$

The restriction of u to $\mathfrak{G}^{(2)}$ is the unique element $u \in \mathrm{H}^1(\mathfrak{G}^{(2)})^{\mathfrak{g}_1}$ such that $d_2 u = \eta$ (see e.g. [NSW08], Propositions 1.6.6 and 2.4.3). Thus, it suffices to calculate $u(\tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) = ([\sigma,\tau],u)_{\mathfrak{g}_2}$ and $u(\tilde{\sigma}^n) = (\pi\sigma,u)_{\mathfrak{g}_2}$.

First we calculate $u(\tilde{\sigma}^n)$:

$$\begin{aligned} u(\tilde{\sigma}^n) &= u(\tilde{\sigma}^{n-1}) + u(\tilde{\sigma}) - \xi(\tilde{\sigma}^{n-1},\tilde{\sigma}) \\ &= u(\tilde{\sigma}^{n-2}) + 2\cdot u(\tilde{\sigma}) - (\xi(\tilde{\sigma}^{n-2},\tilde{\sigma}) + \xi(\tilde{\sigma}^{n-1},\tilde{\sigma})) \\ &= \cdots = n\cdot u(\tilde{\sigma}) - \sum_{l=1}^{n-1} \xi(\tilde{\sigma}^l,\tilde{\sigma}) \\ &= -\sum_{l=1}^{n-1} \xi(\tilde{\sigma}^l,\tilde{\sigma}). \end{aligned}$$

Since $\xi(1,\tilde{\sigma}) = 0$, we get

$$u(\tilde{\sigma}^n) = -\sum_{l=0}^{n-1} \xi(\tilde{\sigma}^l,\tilde{\sigma}).$$

By Proposition A.1, we see that

$$u(\tilde{\sigma}^n) = -\left(\binom{n}{2}\cdot\sum_i \sigma(x_i)\sigma(y_i) + \sum_j \sigma(z_j)\right).$$

Now we calculate $u(\tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau})$:

$$\begin{aligned} u(\tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) &= u(\tilde{\sigma}^{-1}) + u(\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) - \xi(\tilde{\sigma}^{-1},\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) \\ &= u(\tilde{\sigma}^{-1}) + u(\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) - \xi(\tilde{\sigma}^{-1},\tilde{\sigma}) \\ &= -u(\tilde{\sigma}) + u(\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) + \xi(\tilde{\sigma}^{-1},\tilde{\sigma}) - \xi(\tilde{\sigma}^{-1},\tilde{\sigma}) \\ &= -u(\tilde{\sigma}) + u(\tilde{\tau}^{-1}) + u(\tilde{\sigma}\tilde{\tau}) - \xi(\tilde{\tau}^{-1},\tilde{\sigma}\tilde{\tau}) \\ &= -u(\tilde{\sigma}) - u(\tilde{\tau}) + u(\tilde{\sigma}\tilde{\tau}) + \xi(\tilde{\tau}^{-1},\tilde{\tau}) - \xi(\tilde{\tau}^{-1},\tilde{\sigma}\tilde{\tau}) \\ &= -u(\tilde{\sigma}) - u(\tilde{\tau}) + u(\tilde{\sigma}) + u(\tilde{\tau}) + \xi(\tilde{\tau}^{-1},\tilde{\tau}) - \xi(\tilde{\tau}^{-1},\tilde{\sigma}\tilde{\tau}) - \xi(\tilde{\sigma},\tilde{\tau}) \\ &= -(\xi(\tilde{\sigma},\tilde{\tau}) + \xi(\tilde{\tau}^{-1},\tilde{\sigma}\tilde{\tau}) - \xi(\tilde{\tau}^{-1},\tilde{\tau})). \end{aligned}$$

Again by Proposition A.1, we see that

$$u(\tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}) = -\left(\sum_i \sigma(x_i)\tau(y_i) - \sigma(y_i)\tau(x_i)\right).$$

This completes the proof of Theorem 2. □

Acknowledgments

The author warmly thanks Florian Pop and Ján Mináč for several discussions which motivated this work. The author also thanks both Ido Efrat and the referee for their kind encouragement and for helpful suggestions regarding the exposition.

References

[Bog91] Fedor A. Bogomolov, *On two conjectures in birational algebraic geometry*, Algebraic geometry and analytic geometry (Tokyo, 1990), ICM-90 Satell. Conf. Proc., Springer, Tokyo, 1991, pp. 26–52. MR1260938 (94k:14013) ↑2722

[BT02] Fedor Bogomolov and Yuri Tschinkel, *Commuting elements of Galois groups of function fields*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, pp. 75–120. MR1977585 (2004d:14021) ↑2721, 2722

[BT08] Fedor Bogomolov and Yuri Tschinkel, *Reconstruction of function fields*, Geom. Funct. Anal. **18** (2008), no. 2, 400–462, DOI 10.1007/s00039-008-0665-8. MR2421544 (2009g:11155) ↑2722

[BT11] Fedor Bogomolov and Yuri Tschinkel, *Reconstruction of higher-dimensional function fields* (English, with English and Russian summaries), Mosc. Math. J. **11** (2011), no. 2, 185–204, 406. MR2859233 (2012j:14034) ↑2722

[CEM12] Sunil K. Chebolu, Ido Efrat, and Ján Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Math. Ann. **352** (2012), no. 1, 205–221, DOI 10.1007/s00208-011-0635-6. MR2885583 ↑2722

[Efr95] Ido Efrat, *Abelian subgroups of pro-2 Galois groups*, Proc. Amer. Math. Soc. **123** (1995), no. 4, 1031–1035, DOI 10.2307/2160698. MR1242081 (95e:12007) ↑2721

[EK98] Antonio José Engler and Jochen Koenigsmann, *Abelian subgroups of pro-p Galois groups*, Trans. Amer. Math. Soc. **350** (1998), no. 6, 2473–2485, DOI 10.1090/S0002-9947-98-02063-7. MR1451599 (98h:12004) ↑2721

[EM11a] I. Efrat and J. Mináč, *Galois groups and cohomological functors*, Preprint (2011), available at `http://arxiv.org/abs/1103.1508`. ↑2722, 2723, 2725

[EM11b] Ido Efrat and Ján Mináč, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. **133** (2011), no. 6, 1503–1532, DOI 10.1353/ajm.2011.0041. MR2863369 ↑2723, 2725, 2734

[EM12] I. Efrat and J. Mináč, *Small Galois groups that encode valuations*, Acta Arith. **156** (2012), no. 1, 7–17. MR2997568 ↑2722

[EN94] Antonio José Engler and João Bosco Nogueira, *Maximal abelian normal subgroups of Galois pro-2-groups*, J. Algebra **166** (1994), no. 3, 481–505, DOI 10.1006/jabr.1994.1164. MR1280589 (95h:12004) ↑2721

[Gro97] Alexander Grothendieck, *Brief an G. Faltings* (German), Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 49–58. With an English translation on pp. 285–293. MR1483108 (99c:14023) ↑2722

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR2266528 (2007k:16033) ↑2734

[Koe03] Jochen Koenigsmann, *Encoding valuations in absolute Galois groups*, Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 33, Amer. Math. Soc., Providence, RI, 2003, pp. 107–132. MR2018554 (2004m:12012) ↑2721

[Lab67] J. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106–132. MR0210788 (35 #1674) ↑2725, 2740

[MS82] A. S. Merkurjev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136. ↑2722, 2736

[MS96] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. of Math. (2) **144** (1996), no. 1, 35–60. MR1405942 (97i:11038) ↑2722

[MST14] Ján Mináč, John Swallow, and Adam Topaz, *Galois module structure of (ℓ^n)th classes of fields*, Bull. Lond. Math. Soc. **46** (2014), no. 1, 143–154, DOI 10.1112/blms/bdt082. MR3161770 ↑2722

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 (2008m:11223) ↑2725, 2727, 2728, 2735, 2740, 2743

[Pop03] F. Pop, *Pro-l birational anabelian geometry over algebraically closed fields I*, Preprint (2003), available at http://arxiv.org/abs/math/0307076. ↑2722

[Pop10] Florian Pop, *Pro-ℓ abelian-by-central Galois theory of prime divisors*, Israel J. Math. **180** (2010), 43–68, DOI 10.1007/s11856-010-0093-y. MR2735055 (2012a:12010) ↑2722

[Pop11] F. Pop, *On Bogomolov's birational anabelian program II*, Preprint (2011), available at http://www.math.upenn.edu/~pop/Research/Papers.html. ↑2722

[Pop12] Florian Pop, *On the birational anabelian program initiated by Bogomolov I*, Invent. Math. **187** (2012), no. 3, 511–533, DOI 10.1007/s00222-011-0331-x. MR2891876 ↑2722

[Sil12] A. Silberstein, *Anabelian intersection theory I: The conjecture of Bogomolov-Pop and applications*, Preprint (2012), available at http://arxiv.org/abs/1211.4608. ↑2722

[Top14] A. Topaz, *Commuting-liftable subgroups of Galois groups II*, J. Reine Angew. Math. (to appear) (2014), available at http://www.arxiv.org/abs/1208.0583. ↑2722, 2723, 2725, 2740

Department of Mathematics, 970 Evans Hall #3840, University of California, Berkeley, Berkeley, California 94720-3840

E-mail address: atopaz@math.berkeley.edu

URL: http://math.berkeley.edu/~atopaz