Galois groups of maximal class-2 extensions

Berrevoets, Onno

Onno B. Berrevoets

Galois groups of maximal class-2 field extensions

Supervisor: em. prof. dr. H.W. Lenstra

August 28, 2020

Master thesis, Mathematisch Instituut, Universiteit Leiden

Contents

1 Introduction **2**

1.1 Summary 2

1.2 Acknowledgements 5

2 Preliminaries **6**

2.1 Profinite groups 6

2.2 Class-2 groups 9

2.3 Pontryagin duality 10

2.4 Class field theory 12

3 Cohomology of topological groups **14**

3.1 Continuous cohomology 14

3.2 Cup products 15

3.3 Quotient categories 16

3.4 2-Cocycles and Sectioned Central Extensions 17

3.5 Galois cohomology 24

3.6 Ext functors 25

3.7 Calculation of Ext^1 groups 28

4 Profinite groups **28**

4.1 Profinite products 28

4.2 Profinite tensor products 30

4.3 Profinite exterior squares 31

4.4 An injective morphism $\bigwedge^2 A \to \bigotimes^2 A$ 33

4.5 Cocycle squares 35

4.6 Restricted products 39

5 A split exact sequence **43**

5.1 Commutator pairing 43

5.2 Section of $\mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$ 43

5.3 Canonical splitting 44

6 Multiplier-free theorems **47**

6.1 Multiplier-free theorems 47

7 Maximal class-2 extensions of fields **50**

7.1 Generalities 50

7.2 Maximal class-2 tamely ramified extensions of local number fields 51

7.3 Maximal class-2 extension of $\mathbb{Q}_p$ for $p > 2$ 55

7.4 Maximal class-2 extension of $\mathbb{Q}_2$ 59

7.5 Maximal class-2 extension of $\mathbb{Q}$ 68

7.6 Decomposition groups in global class-2 group 72

7.7 Descriptions Ext-part with cocycles 74

Bibliography **76**

1 Introduction

1.1 Summary

Let K be a field and let K^{alg} be an algebraic closure of K. A profinite group G is of *class* 2 if its commutator subgroup $[G,G]$ is contained in its center $\mathrm{Z}(G)$. A Galois extension of fields is called a *class*-2 *extension* if the Galois group is of class 2. We denote the composite of all class-2 Galois extensions of K inside K^{alg} by K^{cl2}. Then K^{cl2} is itself a class-2 extension of K. In this thesis, we focus on the description of the structure of the Galois group $\mathrm{Gal}(K^{\mathrm{cl2}}/K)$ when K equals the field $\mathbb{Q}$ of rational numbers or the field $\mathbb{Q}_p$ of p-adic numbers for some prime p. For any profinite group G we denote by $G^{(2)}$ the topological closure of $[G,G]$ in G, and we denote by G^{ab} the quotient $G/G^{(2)}$.

Before we state the results for $K=\mathbb{Q}_p$, we introduce some notation. For any prime p, denote by Γ_p the Galois group $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p)$. Moreover, for any $n\in\mathbb{Z}_{>0}$, let $\mu_n\subset\mathbb{Q}_p^{\mathrm{alg}}$ be the set of roots of X^n-1. For any prime p we denote by $\mathbb{Z}_p\subset\mathbb{Q}_p$ the ring of p-adic integers and we denote by $\mathbb{F}_p$ the finite field of order p. We identify $\mathbb{F}_p^*$ with $\mu_{p-1}\subset\mathbb{Q}_p$. We denote by $\widehat{\mathbb{Z}}$ the ring of profinite integers. We now describe Γ_p, starting with the case where p is odd.

Theorem 1.1. *Let p be an odd prime. Consider the profinite abelian group*

$$I_p' := (1+p\mathbb{Z}_p)\times\mu_{(p-1)^2}\times(1+p\mathbb{Z}_p)$$

and the topological action of $\widehat{\mathbb{Z}}$ on I_p' defined by

$$1\star(x,\zeta,y)=(xy,\zeta^p,y).$$

Let $I_p'\rtimes\widehat{\mathbb{Z}}$ be the associated semi-direct product. We identify $\mathbb{Z}_p^*$ with $(1+p\mathbb{Z}_p)\times\mathbb{F}_p^*$. Then there is a short exact sequence

$$1\longrightarrow\mathbb{Z}_p^*\xrightarrow{t}I_p'\xrightarrow{u}\mathbb{Z}_p^*\longrightarrow 1$$

of profinite groups, where $t(x,\zeta)=(x,\zeta,1)$ and $u(x,\zeta,y)=(y,\zeta^{p-1})$ and there is an isomorphism

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}_p^* \arrow[r, "{(t,0)}"] \arrow[d, "\wr"] & I_p'\rtimes\widehat{\mathbb{Z}} \arrow[r, "{(u,\mathrm{id})}"] \arrow[d, "\wr"] & \mathbb{Z}_p^*\times\widehat{\mathbb{Z}} \arrow[r] \arrow[d, "\wr"] & 1 \\
1 \arrow[r] & \Gamma_p^{(2)} \arrow[r] & \Gamma_p \arrow[r] & \Gamma_p^{\mathrm{ab}} \arrow[r] & 1
\end{tikzcd}$$

of short exact sequences of profinite groups.

In section 7.3 we will provide an isomorphism of short exact sequences as in Theorem 1.1 with descriptions of the outer vertical isomorphisms. The local Artin map $\mathbb{Q}_p^*\to\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ induces the isomorphism $\mathbb{Z}_p^*\times\widehat{\mathbb{Z}}\xrightarrow{\sim}\Gamma_p^{\mathrm{ab}}$ in Theorem 1.1. It maps $\mathbb{Z}_p^*$ isomorphically to the inertia group $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{unr}})$ of Γ_p^{ab}, where $\mathbb{Q}_p^{\mathrm{unr}}$ denotes the maximal unramified extension of $\mathbb{Q}_p$. Let $\varphi\in\Gamma_p$ denote any Frobenius element. Then we have a well-defined isomorphism $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{unr}})\xrightarrow{\sim}\Gamma_p^{(2)}$ given by $\beta\mapsto[\varphi,\widetilde{\beta}]$ where $\widetilde{\beta}\in\Gamma_p$ is any extension of β, and this isomorphism does not depend on the choice of φ. The latter two isomorphisms combined yield the isomorphism $\mathbb{Z}_p^*\xrightarrow{\sim}\Gamma_p^{(2)}$ appearing in Theorem 1.1. Moreover, the isomorphism $I_p'\rtimes\widehat{\mathbb{Z}}\xrightarrow{\sim}\Gamma_p$ in this theorem maps I_p' isomorphically to the inertia group of Γ_p, which is abelian in this case.

We remark that the subgroup $(1+p\mathbb{Z}_p)\times\mu_{(p-1)^2}\times\{1\}$ of I'_p may be identified with

$$(\mathbb{Z}_p^*)^{\frac{1}{p-1}} := \{x\in\mathbb{Q}_p^{\mathrm{alg}} : x^{p-1}\in\mathbb{Z}_p^*\},$$

so that I'_p becomes equal to $(\mathbb{Z}_p^*)^{\frac{1}{p-1}}\times(1+p\mathbb{Z}_p)$. In these terms, the map t is just inclusion on the first factor, and u maps (x,y) to $(\varphi(x)/x)y$.

Next we pass to the case $p=2$. Then we replace the group $(\mathbb{Z}_p^*)^{\frac{1}{p-1}}$ just discussed by

$$\sqrt{1+4\mathbb{Z}_2} := \{x\in\mathbb{Q}_2^{\mathrm{alg}} : x^2\in 1+4\mathbb{Z}_2\}.$$

Notice that $\mathbb{Q}_2(\sqrt{1+4\mathbb{Z}_2})$ is the unique quadratic unramified extension of $\mathbb{Q}_2$ inside $\mathbb{Q}_2^{\mathrm{alg}}$, and that $\mathbb{Z}_2^*$ is a subgroup of index 2 in $\sqrt{1+4\mathbb{Z}_2}$. The following theorem gives a description of Γ_2, comparable to Theorem 1.1. Denote by $\varphi\in\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{unr}}/\mathbb{Q}_2)$ the Frobenius element.

Theorem 1.2. *Consider the topological action of* $1+4\mathbb{Z}_2$ *on* $\mu_2\times\sqrt{1+4\mathbb{Z}_2}$ *defined by*

$$5\star(\varepsilon,x) = (\frac{\varphi(x)}{x}\varepsilon,x).$$

Let $I'_2 := (\mu_2\times\sqrt{1+4\mathbb{Z}_2})\rtimes(1+4\mathbb{Z}_2)$ *be the associated semi-direct product. Let a topological action of* $\widehat{\mathbb{Z}}$ *on* I'_2 *be defined by*

$$1\star(\varepsilon,x,y) = (\varepsilon,\varphi(x)y,y)$$

and let $I'_2\rtimes\widehat{\mathbb{Z}}$ *be the associated semi-direct product. Then there is a short exact sequence*

$$1\longrightarrow\mu_2\times\mathbb{Z}_2^*\xrightarrow{t}I'_2\xrightarrow{u}\mathbb{Z}_2^*\longrightarrow 1$$

of profinite groups, where $t(\varepsilon,x)=(\varepsilon,x,1)$ *and* $u(\varepsilon,x,y)=(\varphi(x)/x)y$, *and there is an isomorphism*

$$\begin{tikzcd}
1 \arrow[r] & \mu_2\times\mathbb{Z}_2^* \arrow[r, "{(t,0)}"] \arrow[d, "\wr"] & I'_2\rtimes\widehat{\mathbb{Z}} \arrow[r, "{(u,\mathrm{id})}"] \arrow[d, "\wr"] & \mathbb{Z}_2^*\times\widehat{\mathbb{Z}} \arrow[r] \arrow[d, "\wr"] & 1 \\
1 \arrow[r] & \Gamma_2^{(2)} \arrow[r] & \Gamma_2 \arrow[r] & \Gamma_2^{\mathrm{ab}} \arrow[r] & 1
\end{tikzcd}$$

of short exact sequences of profinite groups.

In section 7.4 we will provide an isomorphism of short exact sequences as in Theorem 1.2 with descriptions of the outer vertical isomorphisms. Similarly to the case for odd p, the local Artin map $\mathbb{Q}_2^*\to\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2)$ induces the isomorphism $\mathbb{Z}_2^*\times\widehat{\mathbb{Z}}\xrightarrow{\sim}\Gamma_2^{\mathrm{ab}}$ in Theorem 1.2. It maps $\mathbb{Z}_2^*$ isomorphically to the inertia group $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2^{\mathrm{unr}})$ of Γ_2^{ab}. Let σ_5 and σ_{-1} in $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2^{\mathrm{unr}})$ correspond via this isomorphism to 5 and -1 in $\mathbb{Z}_2^*$ respectively, and let $\widetilde{\sigma_5}$ and $\widetilde{\sigma_{-1}}$ be extensions to Γ_2 of σ_5 and σ_{-1} respectively. Let $\varphi\in\Gamma_2$ denote a Frobenius element that is the identity map on μ_{2^n} for all $n\in\mathbb{Z}_{>0}$. Then we have a well-defined isomorphism $\mu_2\times\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2^{\mathrm{unr}})\xrightarrow{\sim}\Gamma_2^{(2)}$ given by $((-1)^a,\beta)\mapsto[\widetilde{\sigma_5},\widetilde{\sigma_{-1}}]^a[\varphi,\widetilde{\beta}]$ where $\widetilde{\beta}\in\Gamma_2$ is any extension of β and where a is any integer, and this isomorphism does not depend on our choice of φ. The latter two isomorphisms together induce the isomorphism $\mu_2\times\mathbb{Z}_2^*\xrightarrow{\sim}\Gamma_2^{(2)}$ appearing in Theorem 1.2. Moreover, the isomorphism $I'_2\rtimes\widehat{\mathbb{Z}}\xrightarrow{\sim}\Gamma_2$ in this theorem maps I'_2 isomorphically to the inertia group of Γ_2. This inertia group is close to being abelian: the commutator subgroup of I'_2 equals μ_2 and is central. Moreover, the center $\mathrm{Z}(I'_2)$ of I'_2 equals $\mu_2\times\mathbb{Z}_2^*\times(1+8\mathbb{Z}_2)$ and is of index 4 in I'_2. We remark that for any non-abelian profinite group G the center $\mathrm{Z}(G)$ is of index at least 4 in G.

We get a similar description of $\Gamma := \mathrm{Gal}(\mathbb{Q}^{\mathrm{cl2}}/\mathbb{Q})$ by combining the two previous theorems, and the result can be found in Theorem 7.34. Consider an inclusion $\mathbb{Q}^{\mathrm{alg}} \subset \mathbb{Q}_p^{\mathrm{alg}}$. Then $\mathbb{Q}_p^{\mathrm{cl2}}$ is the compositum of its subfields $\mathbb{Q}^{\mathrm{cl2}}$ and $\mathbb{Q}_p$, and this result can be found in section 7.6. Equivalently, the natural continuous homomorphism $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p) \to \Gamma$, that restricts automorphisms to $\mathbb{Q}^{\mathrm{cl2}}$, is injective. This thesis is inspired by [6], in which Galois groups of certain class-2 field extensions are described.

From now on, let K be an algebraic number field or a local number field. From class field theory, the Galois group of the extension K^{ab}/K is well-known. Due to the following result, Theorem 1.3, we can also describe the Galois group of $K^{\mathrm{cl2}}/K^{\mathrm{ab}}$ by using the results from class field theory and by using that $\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathbb{Q}/\mathbb{Z}) = 0$. For any group G we denote by $G^{(2)}$ the commutator subgroup $[G, G]$ of G and we denote by $G^{(3)}$ the subgroup $[G, G^{(2)}]$ of G. Similarly, for any profinite group G we denote by $G^{(2)}$ the topological closure of $[G, G]$ in G and we denote by $G^{(3)}$ the closure of $[G, G^{(2)}]$ in G. More information on these groups $G^{(n)}$ can be found in section 2.2.

Throughout this thesis we will use the convention that parentheses (...) give two meanings to a sentence: one with the contents in all parentheses, and one without these contents. For example, for any (topological) groups G_1 and G_2 we denote the set of (continuous) homomorphisms $G_1 \longrightarrow G_2$ by $\mathrm{Hom}(G_1, G_2)$, and by this we mean that $\mathrm{Hom}(G_1, G_2)$ denotes the hom-set of groups if G_1 and G_2 are groups and $\mathrm{Hom}(G_1, G_2)$ denotes the hom-set of topological groups if G_1 and G_2 are topological groups. For any (profinite) abelian groups A and B we say that a map $f : A \times A \to B$ is *alternating* if f is (continuous and) bilinear and $f(a, a) = 0$ for all $a \in A$. We denote by $\mathrm{Alt}^2(A, B)$ the abelian group of all (continuous) alternating maps $A \times A \to B$. For any (profinite) abelian group A we denote by $\bigwedge^2 A$ a (profinite) abelian group and by

$$- \wedge - : A \times A \to \bigwedge^2 A, \quad (a_1, a_2) \mapsto a_1 \wedge a_2$$

a (continuous) alternating map such that composition with $- \wedge -$ induces a representation $\mathrm{Hom}(\bigwedge^2 A, -) \cong \mathrm{Alt}^2(A, -)$ of the functor $\mathrm{Alt}^2(A, -)$. For any (profinite) group G there is a well-defined *commutator map* $[-, -] : \bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$ that maps $\overline{g_1} \wedge \overline{g_2}$ to $\overline{[g_1, g_2]}$ for any $g_1, g_2 \in G$. In section 4.3 we will further discuss the (profinite) group $\bigwedge^2 G$.

For a (topological) group G and a (topological) G-module A we denote by $\mathrm{H}^2(G, A)$ the second (continuous) cohomology group with coefficients in A. If A is a topological G-module, then $\mathrm{H}^2(G, A)$ will denote the continuous cohomology group, unless specified otherwise. The following result is proven in chapter 6.

Theorem 1.3. *Let G be a (profinite) group such that $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. Then the commutator map*

$$[-, -] : \bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$$

is an isomorphism.

For any global or local field K we have $\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathbb{Q}/\mathbb{Z}) = 0$ by a theorem of Tate that can be found in [14, p. 227, Thm. 4]. For the remaining part of this section, assume that K is equal to $\mathbb{Q}$ or $\mathbb{Q}_p$ for some prime p, and write $\Gamma := \mathrm{Gal}(K^{\mathrm{cl2}}/K)$. It follows from the theorem of Tate that $\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathbb{Q}/\mathbb{Z}) = 0$ holds. In particular, we get an isomorphism $\bigwedge^2 \Gamma^{\mathrm{ab}} \to \Gamma^{(2)}$ by Theorem 1.3. Via this isomorphism, we can view the class $[\Gamma]$ of the central extension $1 \to \Gamma^{(2)} \to \Gamma \to \Gamma^{\mathrm{ab}} \to 1$ as an element of $\mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}})$.

In order to describe the structure of the profinite group Γ, it suffices to determine the element $[\Gamma] \in \mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}})$. To do so, we describe $\mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}})$ more explicitly using the following theorem, of which the proof is an exercise in [3, Ch. 5.6] in the case of discrete abelian groups. The proof of this result can be found in section 5.2.

Theorem 1.4. *Let A, G be (profinite) abelian groups. Then the sequence*

$$0 \to \mathrm{Ext}^1(G, A) \to \mathrm{H}^2(G, A) \overset{\mathrm{cp}}{\to} \mathrm{Hom}(\bigwedge^2 G, A) \to 0$$

is a split exact sequence, where $\mathrm{Ext}^1(G, A) \to \mathrm{H}^2(G, A)$ is the inclusion map, and where cp *is the map*

$$\mathrm{cp} : \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A), \quad [1 \to A \to E \to G \to 1] \mapsto (g_1 \wedge g_2 \mapsto [s(g_1), s(g_2)]),$$

with s any (continuous) set-theoretic section of $E \to G$.

Let $(G_i)_{i \in I}$ be a collection of procyclic groups indexed by I, and let A be a profinite abelian group. Suppose that I is finite, or, suppose that A is the product of finite discrete groups. In section 5.3 we will exhibit an explicit retraction

$$\mathrm{ret}((G_i)_i, A) : \mathrm{H}^2(\prod_i G_i, A) \to \mathrm{Ext}^1(\prod_i G_i, A)$$

of the inclusion map $\mathrm{Ext}^1(\prod_i G_i, A) \to \mathrm{H}^2(\prod_i G_i, A)$. By factoring Γ^{ab} into a product of procyclic groups, we get an explicit splitting

$$(\mathrm{ret}, \mathrm{cp}) : \mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}}) \overset{\sim}{\to} \mathrm{Ext}^1(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}}) \times \mathrm{End}(\bigwedge^2 \Gamma^{\mathrm{ab}}).$$

Since $\mathrm{cp}[\Gamma] = \mathrm{id}$, it remains to determine the element $\mathrm{ret}[\Gamma] \in \mathrm{Ext}^1(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}})$. This will be done by using various properties of Ext^1 and number-theoretic properties of the field K.

We will now pose several questions that arose from this thesis. Inspired by [1], we ask whether it is possible for every prime p to describe roots of elements of $\mathbb{Q}_p^{\mathrm{ab}}$ that generate $\mathbb{Q}_p^{\mathrm{cl2}}$, and similarly we ask for a description of $\mathbb{Q}^{\mathrm{cl2}}$. Another interesting question is whether the Galois group $\mathrm{Gal}(K^{\mathrm{cl2}}/K)$ can be described for other local and global fields K. We also ask whether it is possible to describe Galois groups of maximal 'class-n' extensions of $\mathbb{Q}_p$ and $\mathbb{Q}$, where p is a prime.

1.2 Acknowledgements

I am extremely grateful to my advisor Hendrik Lenstra for his support and guidance. The completion of this thesis would not have been possible without his extensive help. I would also like to thank Martin Bright, Ronald van Luijk and Bart de Smit for serving on the exam committee. I thank Bart Eggen, Daan van Gent, Geerten Koers and Wessel van Woerden for proofreading this thesis.

2 Preliminaries

2.1 Profinite groups

All statements without proofs or references in this section can be found with proof in [11]. The topological closure of a subspace X is denoted by $\overline{X}$.

Remark 2.1. Let $(I, \leq)$ be a directed set, i.e., $(I, \leq)$ is a poset such that for all $i, k \in I$ there exists $k \in I$ such that $i, j \leq k$. Consider an inverse system

$$((X_i)_i, (f_{ij} : X_i \to X_j)_{j \leq i}, I)$$

of topological groups. The inverse limit is equal to the subgroup

$$\{(x_i)_{i \in I} \mid \forall i, j \in I, j \leq i \Rightarrow f_{ij}(x_i) = x_j\}$$

of the topological group $\prod_i X_i$ equipped with the subspace topology. △

Definition 2.2. A *profinite group/ring* is a topological group/ring that is isomorphic to the inverse limit of an inverse system of discrete finite groups/rings. △

A *morphism* between profinite groups is a continuous group homomorphism. This turns the class of profinite groups into a locally small category, i.e., for any profinite groups G_1, G_2 the hom-set $\mathrm{Hom}(G_1, G_2)$ is a set.

Example 2.3. Let $K \subset L$ be a, possibly infinite, Galois extension. Then $\mathrm{Gal}(L/K)$ equals the inverse limit

$$\mathrm{Gal}(L/K) = \varprojlim_{K \subset M \subset L} \mathrm{Gal}(M/K)$$

where M ranges over the finite Galois extensions of K contained in L. Hence, $\mathrm{Gal}(L/K)$ is a profinite group. △

Definition 2.4. Let G be a group. Then the *profinite completion* $\widehat{G}$ *of* G is the inverse limit of the inverse system $(G/N)_{N \in I}$ where I is the set of all normal subgroups N of G of finite index. △

Notice that in the definition above, $\widehat{G}$ is a profinite group, and the image of the natural homomorphism $G \to \widehat{G}$ is dense in $\widehat{G}$.

Example 2.5. Let p be a prime. For any $i, j \in \mathbb{Z}_{>0}$ such that $i \geq j$ we consider the natural ring homomorphism $\mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ given by $x + p^i\mathbb{Z} \mapsto x + p^j\mathbb{Z}$ for any $x \in \mathbb{Z}$. Then the inverse limit $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ is the *ring of p-adic integers* and is denoted by $\mathbb{Z}_p$.

For any integers $n, m \geq 1$ with $m \mid n$ we similarly have a map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. The inverse limit of the induced inverse system is the *ring of profinite integers* and is denoted by $\widehat{\mathbb{Z}}$. As a topological group, $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. △

Lemma 2.6. *Let G be a compact topological group and let $H \subset G$ be a subgroup of G. Then H is open if and only if it is closed and of finite index $(G : H)$.*

Proof. Since G equals the disjoint union of cosets of H, the result follows from compactness of G. □

It is clear that profinite groups and profinite rings are compact Hausdorff and totally disconnected, since they are subspaces of products of finite discrete spaces. The following proposition is a special case of [11, Thm. 2.1.3] and of [11, Thm. 5.1.2].

Proposition 2.7. *A topological group is a profinite group if and only if it is compact Hausdorff and totally disconnected. A topological ring is a profinite ring if and only if it is compact Hausdorff.*

The following lemma is a special case of [11, Thm. 2.1.3].

Lemma 2.8. *Let G be a profinite group. Then there exists a set $\mathcal{N}$ of open normal subgroups N of G such that $\bigcap \mathcal{N} = \{1\}$ and such that for each open neighbourhood V of 1 there exists $N \in \mathcal{N}$ with $N \subset V$.*

Since profinite groups are compact Hausdorff, we get the following result.

Lemma 2.9. *Let $f : G \to G'$ be a morphism of profinite groups. Then f is closed, and for any subset $X \subset G$ we have $f(\overline{X}) = \overline{f(X)}$. Moreover, if f is a bijection, then f is an isomorphism of profinite groups.*

As a corollary of Lemma 2.9, every injective morphism of profinite groups induces a homeomorphism to its image.

Corollary 2.10. *Let $\iota : G \to G'$ be an injective morphism of profinite groups. Then the induced map $G \to \iota[G]$ is an isomorphism of profinite groups.*

The following two lemmas give sufficient conditions for morphisms of profinite groups to have continuous set-theoretic sections and retractions.

Lemma 2.11. *Every surjective morphism $G \to G'$ of profinite groups has a continuous set-theoretic section.*

Proof. See [11, Prop. 2.2.2]. □

Lemma 2.12. *Every injective morphism $G \to G'$ of profinite groups has continuous set-theoretic retraction.*

Proof. Let $\iota : G \to G'$ be an injective morphism of profinite groups. Then $\iota[G]$ is a closed subgroup of G' by Lemma 2.9. The quotient map $q : G' \to G'/\iota[G]$ of topological spaces has a topological section $s : G'/\iota[G] \to G'$ by [15, Ch. 1.2, Prop. 1], and note that we can take s to be such that $s(\iota[G]) = 1$. Now $G' \to G,\ g' \mapsto \iota^{-1}(g'(sqg')^{-1})$ is a continuous set-theoretic retraction of ι. □

Quotients of profinite groups by closed normal subgroups are profinite groups, and arbitrary products of profinite groups are profinite groups [11, Prop. 2.2.1]. The following result is a specific case of [11, Cor. 1.1.8].

Lemma 2.13. *Let $(G_i)_{i\in I}$ be an inverse system of profinite groups, let G be the inverse limit and let $f_i : G \to G_i$ be the projection map for all $i \in I$. Let $X \subset G$ be a subset. Then $\lim_{\leftarrow} f_i(X) = \overline{X}$.*

Lemma 2.14. *The inverse limit of any inverse system $(X_i)_{i\in I}$ of compact Hausdorff non-empty topological spaces over a directed set I is non-empty.*

Proof. See [11, Lemma 1.1.4]. □

Definition 2.15. Let G be a profinite group. Then for any subset $X \subset G$ we call $\overline{\langle X \rangle}$ the *subgroup topologically generated by* X. If $\overline{\langle X \rangle} = G$, then we say that G is topologically generated by X. △

Definition 2.16. A profinite group G is called *procyclic* if it is isomorphic to the inverse limit of a system of cyclic groups. △

Lemma 2.17. *A profinite group G is procyclic if and only if it is topologically generated by $\{g\}$ for some $g \in G$.*

Proof. Let G be a profinite group. If $g \in G$ is such that $G = \overline{\{g\}}$, then it is clear that G is procyclic. Now suppose that G is procyclic. Then G is the inverse limit of an inverse system $((G_i)_i, (f_{ij})_{j \le i}, I)$ with each G_i a finite cyclic discrete group and with each f_{ij} surjective. For every i, we let X_i be the set of generators of G_i. Then $(X_i)_i$ forms an inverse system, and $\lim_{\leftarrow} X_i$ is non-empty by Lemma 2.14. □

Definition 2.18. Let R be a profinite ring. Then a *topological R-module* is an R-module M such that M is a topological group and the multiplication map $R \times M \to M$ is continuous. △

Definition 2.19. Let G be a profinite group and let X be a topological space. Then a *topological G-action* is a group action of G on X such that the induced map $G \times X \to X$ is continuous, where $G \times X$ has the product topology. △

Lemma 2.20. *Consider a profinite group G and an element $\theta \in G$. Then there exists a unique morphism $\widehat{\mathbb{Z}} \to G$ such that $1 \mapsto \theta$.*

Proof. See [11, Ch. 4.1]. □

Any profinite abelian group A can be viewed as a $\widehat{\mathbb{Z}}$-module: for any $\theta \in A$ and any $n \in \widehat{\mathbb{Z}}$ we let $n\theta \in A$ be the element $f(n)$ where $f : \widehat{\mathbb{Z}} \to A$ is the morphism from Lemma 2.20 with $1 \mapsto \theta$. Any morphism of profinite abelian groups is a morphism of $\widehat{\mathbb{Z}}$-modules.

Lemma 2.21. *Let I be a directed set. Then $\lim_{\leftarrow}$ is an exact functor from the category of inverse systems of profinite groups over I to the category of profinite groups.*

Proof. See [11, Prop 2.2.4]. □

Remark 2.22. Let $0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$ be a short exact sequence of abelian groups that is split. Then

$$(0 \to A/\iota^{-1}N \to B/N \to B/\pi N \to 0)_N,$$

where N ranges over the subgroups of B with finite index, is an inverse system of short exact sequences. Moreover, the set of all such $\iota^{-1}N$ is cofinal in the set of all subgroups of A of finite index, which follows from the fact that ι has a retraction. Hence, $\lim_{\leftarrow} A/\iota^{-1}N = \widehat{A}$. Similarly we have $\lim_{\leftarrow} C/\pi N = \widehat{C}$. Hence, by taking the inverse limit of the inverse system of exact sequences, we get by Lemma 2.21 an exact sequence

$$0 \to \widehat{A} \xrightarrow{\widehat{\iota}} \widehat{B} \xrightarrow{\widehat{\pi}} \widehat{C} \to 0. \qquad △$$

Write $\mathbb{N}_\infty := \mathbb{Z}_{\geq 0} \cup \{\infty\}$. Then $\mathbb{N}_\infty$ is a monoid with the usual addition on $\mathbb{Z}_{\geq 0}$ and with $\infty + n = n + \infty = \infty$ for all $n \in \mathbb{N}_\infty$. We extend the usual linear order $\leq$ on $\mathbb{Z}_{\geq 0}$ to $\mathbb{N}_\infty$ by defining $n \leq \infty$ for all $n \in \mathbb{N}_\infty$.

Definition 2.23. Let $\mathcal{P} \subset \mathbb{Z}_{>0}$ be the set of prime numbers. A *supernatural number* is a formal product $\prod_{p\in\mathcal{P}} p^{n(p)}$ where for each $p \in \mathcal{P}$ we have $n(p) \in \mathbb{N}_\infty$. $\triangle$

For a collection $(n_i = \prod_p p^{n_i(p)})_{i\in I}$ of supernatural numbers, we define

$$\operatorname{lcm}\{n_i : i \in I\} = \prod_p p^{\max\{n_i(p):i\in I\}},$$
$$\gcd\{n_i : i \in I\} = \prod_p p^{\min\{n_i(p):i\in I\}}.$$

We define the *order* $|G|$ of a profinite group G as $\operatorname{lcm}\{\#G/N : N \subset G \text{ open subgroup}\}$. Notice that for any profinite abelian group G the map $G \to G$, $x \mapsto n\cdot x$ is an isomorphism for every $n \in \mathbb{Z}_{>0}$ with $\gcd(|G|, n) = 1$, i.e., with $|G|$ and n coprime.

2.2 Class-2 groups

Definition 2.24. Let G be a group. Then we define $G^{(1)} := G$ and $G^{(i+1)} := [G, G^{(i)}]$ for all integers $i \geq 1$. We write $G^{\mathrm{ab}} := G/G^{(2)}$ for the abelianized group of G. $\triangle$

Definition 2.25. Let G be a topological group. Then we define $G^{(1)} := G$ and $G^{(i+1)} := \overline{[G, G^{(i)}]}$ for all integers $i \geq 1$, i.e., $G^{(i+1)}$ is the closure of $[G, G^{(i)}]$ in G. $\triangle$

Let G be a (topological) group. For every integer $i \geq 2$ and elements $g \in G$, $h \in G^{(i)}$ and an inner automorphism σ of G we have $\sigma[g, h] = [\sigma g, \sigma h]$, hence it follows inductively that $G^{(i)}$ is normal in G. In other words, for each integer $i \geq 1$ we have $[G, G^{(i)}] \subset G^{(i)}$, i.e., $G^{(i+1)} \subset G^{(i)}$. The series $G^{(1)} \supset G^{(2)} \supset \ldots$ is called the *lower central series* of G. Moreover, we denote by G^{ab} and G^{cl2} the (topological) quotient group $G/G^{(2)}$ and $G/G^{(3)}$ respectively.

Definition 2.26. Let G be a (topological) group. Then G is of *class-*2 if $G^{(3)} = 1$. $\triangle$

Notice that a (profinite) group is a class-2 group if and only if $[G, G] \subset \mathrm{Z}(G)$; in the profinite case this follows from the fact that $\mathrm{Z}(G) = \bigcap_{g\in G} \mathrm{C}_G(g)$ is closed in G, where $\mathrm{C}_G(g)$ is the centralizer of g in G. In particular, a profinite group is of class 2 if and only if the underlying group is of class 2. Some examples of class-2 groups are abelian groups, the dihedral group D_4 of order 8 and the quaternion group Q_8. Moreover, G^{cl2} is a class-2 group for any (topological) group G: the subgroup $G^{(3)}$ is the smallest (closed) normal subgroup N of G for which G/N is of class 2.

A map $f : G_1 \times G_2 \to H$ of (topological) groups is called *bilinear* if for every $g_1 \in G_1$ and $g_2 \in G_2$ the maps $f(g_1, -)$ and $f(-, g_2)$ are homomorphisms. Essentially, bilinear maps of (profinite) groups can be viewed as maps of (profinite) abelian groups: if such a map f is bilinear, then expanding $f(ab, cd)$ in two manners shows that the range $\operatorname{ran} f$ of f (topologically) generates an abelian subgroup, and f factors through $G_1^{\mathrm{ab}} \times G_2^{\mathrm{ab}}$. An exact sequence $0 \to A \xrightarrow{\iota} B \to C \to 0$ of (topological) groups is called *central* if $\iota[A] \subset \mathrm{Z}(B)$ (and ι induces a homeomorphism $A \to \iota[A]$).

Lemma 2.27. *Let G be a (profinite) group. Then the following statements are equivalent.*

(1) *G is of class 2,*

(2) *the commutator map $[-,-] : G \times G \to G^{(2)}$ is bilinear,*

(3) *there exists a central exact sequence $1 \to A \to G \to C \to 1$ of (profinite) groups with C abelian.*

Proof. We prove (1) ⇔ (2) in (i) and (1) ⇔ (3) in (ii).

(i) If G is of class 2, then the commutator map is linear in its first argument since for any $g, a, b \in G$ we have

$$[a, g][b, g] = a[b, g]ga^{-1}g^{-1} = [ab, g],$$

and one can similarly show that the commutator map is linear in its second argument. Now suppose that the commutator map is bilinear. Then $G^{(2)}$ is abelian, and the commutator map factors through $G^{\mathrm{ab}} \times G^{\mathrm{ab}}$. This shows that $[G, G^{(2)}] = 1$ and thus $[G, G] \subset \mathrm{Z}(G)$.

(ii) If G is a class-2 group, then $0 \to \mathrm{Z}(G) \to G \to G/\,\mathrm{Z}(G) \to 0$ is a central exact sequence with $G/\,\mathrm{Z}(G)$ abelian. If $0 \to A \xrightarrow{\iota} G \xrightarrow{\pi} C \to 0$ is a central exact sequence with C abelian, then $\pi[G, G] = 0$ and thus $[G, G] \subset \iota A \subset \mathrm{Z}(G)$. □

The following result can be routinely verified by using the equivalence (1) ⇔ (2) from Lemma 2.27.

Corollary 2.28. *Any product (possibly infinite) of (profinite) class-2 groups is again a class-2 group. Moreover, any quotient and any subgroup of a profinite class-2 group is again a class-2 group.*

Lemma 2.29. *Let G be a group. Let H be a subgroup of G and let $i \in \mathbb{Z}_{>0}$ be such that $G^{(i+1)} \subset H \subset G^{(i)}$. Then H is normal in G.*

Proof. From $H \subset G^{(i)}$ it follows that $[G, H] \subset G^{(i+1)}$. Hence, we have $[G, H] \subset H$ thus H is normal in G. □

2.3 Pontryagin duality

Definition 2.30. Let X, Y be topological spaces. For any compact subset $K \subset X$ and any open subset $U \subset Y$, let $V_{K,U}$ be the set of all continuous maps $f : X \to Y$ with $f(K) \subset U$. The *compact-open topology* on the set $C(X, Y)$ of continuous functions $X \to Y$ is the topology generated by the subbasis $(V_{K,U})_{K,U}$. The subspace topology on a subset of $C(X, Y)$ is also called the *compact-open topology* on that subset. △

Consider the topological group $\mathbb{T} := \mathbb{R}/\mathbb{Z}$. Let **LCAb** be the category of locally compact abelian groups. Let G be a locally compact abelian group. Then we define the *Pontryagin dual of* G to be $G^* := \mathrm{Hom}(G, \mathbb{T})$ with the compact-open topology. With this topology G^* is again a locally compact abelian group [11]. Moreover, for any morphism $\varphi : G_1 \to G_2$ of locally abelian groups, we define the *Pontryagin dual of* φ to be the morphism $G_2^* \to G_1^*$ defined by $f \mapsto f \circ \varphi$. It is easy to verify that this now induces a contravariant functor $* : \mathbf{LCAb} \to \mathbf{LCAb}$.

We denote the objects of a category $\mathcal{C}$ by $\mathrm{Ob}(\mathcal{C})$. For any $G \in \mathrm{Ob}(\mathbf{LCAb})$, we consider the morphism $\alpha_G : G \to G^{**}$ defined by $g \mapsto [f \mapsto f(g)]$. Then the theorem on Pontryagin duality states that for any $G \in \mathrm{Ob}(\mathbf{LCAb})$ the map α_G is an isomorphism. In other words, we get the following result.

Theorem 2.31 (Pontryagin duality)**.** *The functor $*$ induces an equivalence of categories between $\mathbf{LCAb}$ and $\mathbf{LCAb}^{\mathrm{op}}$. A natural isomorphism of the identity functor to $**$ is given by α_-.*

For example, for any finite discrete abelian group A we have $A^* \cong A$. Let p be a prime and denote by C_{p^∞} the discrete p-power torsion subgroup of $\mathbb{Q}/\mathbb{Z}$. Then the Pontryagin dual of the group $\mathbb{Z}_p$ equals $\mathbb{Z}_p^* = C_{p^\infty}$. The Pontryagin dual of the group $\widehat{\mathbb{Z}}$ equals $\mathbb{Q}/\mathbb{Z}$.

Let $\mathbf{PAb}$ and $\mathbf{DTAb}$ be the full subcategories of $\mathbf{LCAb}$ respectively consisting of all profinite abelian groups and all discrete abelian torsion groups. In order to apply Pontryagin duality on profinite groups, the following theorem is more useful.

Theorem 2.32 (Pontryagin duality for profinite groups)**.** *The functor $*$ induces a duality of categories between $\mathbf{PAb}$ and $\mathbf{DTAb}$. A corresponding natural isomorphism is induced by α_-. Moreover, if $G \in \mathrm{Ob}(\mathbf{PAb})$ or $G \in \mathrm{Ob}(\mathbf{DTAb})$, then $G^* = \mathrm{Hom}(G, \mathbb{T}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ where $\mathbb{Q}/\mathbb{Z}$ is taken to be discrete.*

As with any equivalence of categories, all limits and colimits are preserved under Pontryagin duality. Therefore, we see that the duality also preserves kernels and cokernels. Hence, the functor $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ is exact on sequences of profinite abelian groups.

Corollary 2.33. *Let G be a profinite abelian group. Then there exists a set I and a surjective morphism $\widehat{\mathbb{Z}}^I \to G$.*

Proof. We use Pontryagin duality to prove this Lemma. It suffices to show that the Pontryagin dual G^* can be embedded as a group into $(\mathbb{Q}/\mathbb{Z})^{(I)}$ for some set I. For any prime p, the p-torsion subgroup $G^*[p]$ is a vector space over $\mathbb{F}_p$ and thus we have $G^*[p] \cong (\frac{1}{p}\mathbb{Z}/\mathbb{Z})^{(I_p)}$ as groups for some set I_p. Now take $I = \coprod_p I_p$ and notice that the natural morphism $\varphi : \bigoplus_p G^*[p] \to (\mathbb{Q}/\mathbb{Z})^{(I)}$ is injective. Moreover, φ extends to a map $\widetilde{\varphi} : G^* \to (\mathbb{Q}/\mathbb{Z})^{(I)}$ since $(\mathbb{Q}/\mathbb{Z})^{(I)}$ is an injective abelian group. Finally, the morphism $\widetilde{\varphi}$ is also injective and this follows from the injectivity of φ. □

Corollary 2.34. *Denote by C the class of all profinite abelian groups that are projective in the category $\mathbf{PAb}$. Then C is closed under taking closed subgroups, (possibly infinite) products and inverse limits. Moreover, we have $\widehat{\mathbb{Z}} \in C$.*

Proof. In the category of abelian groups, injectivity is equivalent to divisibility. Using this, one can verify that injectivity in the category $\mathbf{DTAb}$ is preserved under quotients and direct sums and direct limits. Moreover, the abelian torsion group $\mathbb{Q}/\mathbb{Z}$ is injective. By Pontryagin duality, the corollary follows. □

Similarly to the Pontryagin duality, we denote the functor $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z}) : \mathbf{Ab} \to \mathbf{Ab}$ by $*$ and write $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ and $f^* = \mathrm{Hom}(f, \mathbb{Q}/\mathbb{Z})$ for any abelian group A and morphism f of abelian groups. Since $\mathbb{Q}/\mathbb{Z}$ is divisible and thus injective in $\mathbf{Ab}$, we find that $* : \mathbf{Ab} \to \mathbf{Ab}$ is exact.

Lemma 2.35. *Let A be a (profinite) abelian group. If we have $A^* = 0$, then $A = 0$.*

Proof. If A is a profinite abelian group and $A^* = 0$, then $A \cong A^{**} = 0$ by Pontryagin duality. Now let A be an abelian group without any topology. We will prove the contrapositive, so assume that $A \neq 0$. Consider any non-trivial cyclic subgroup B of A. Then we have $\mathrm{Hom}(B, \mathbb{Q}/\mathbb{Z}) \neq 0$. By injectivity of $\mathbb{Q}/\mathbb{Z}$ it now follows that $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \neq 0$ also holds. □

2.4 Class field theory

In this section we will recall theory from class field theory, which can be found in [10], [5] and [16]. We will first give the definition of a restricted product.

Definition 2.36. Let I be an index set, and let G_i be a locally compact abelian group for all $i \in I$. Let $I_\infty \subset I$ be a finite subset and let $H_i \subset G_i$ be a compact subgroup for all $i \in I \backslash I_\infty$. Then the *restricted product of* $(G_i)_i$ *with respect to* $(H_i)_i$ is defined to be the subgroup

$$G = \{(x_i) \in (G_i)_{i \in I} \mid \text{for all but finitely many } i \in I \backslash I_\infty \text{ we have } x_i \in H_i\}.$$

We equip G with the coarsest topology such that for any finite $S \subset I$ containing I_∞, any open subset U of the topological product $\prod_{i \in S} G_i \times \prod_{i \in I \backslash S} H_i$ is also open in G. Then G is a topological group. △

In the setting of the definition above, for any subset $U \subset G$ we have that U is open in G if and only if for all $x \in G$ the set $xU \cap (\prod_{i \in I_\infty} G_i \times \prod_{i \in I \backslash I_\infty} H_i)$ is open in the product $\prod_{i \in I_\infty} G_i \times \prod_{i \in I \backslash I_\infty} H_i$.

Let K be a number field. Let P be the set of places of K and let $P_\infty \subset P$ be the subset of infinite places of K.

Definition 2.37. The *adele ring of* K is defined to be the restricted product of the additive groups $(K_v)_{v \in P}$ with respect to rings of integers $(\mathcal{O}_v)_{v \in P \backslash P_\infty}$. The multiplication on the adele ring is defined to be componentwise and this turns it into a topological ring. We denote the adele ring of K by $\mathbf{A}_K$. △

Definition 2.38. The *idele group of* K is defined to be the restricted product of the multiplicative groups $(K_v^*)_{v \in P}$ with respect to the unit groups of the rings of integers $(\mathcal{O}_v^*)_{v \in P \backslash P_\infty}$. We denote the idele group of K by $\mathbf{J}_K$. △

Notice that we have an equality of groups $\mathbf{J}_K = \mathbf{A}_K^*$, but the topology of the idele group $\mathbf{J}_K$ is not induced by the subspace topology from $\mathbf{A}_K$. We can diagonally embed K as a discrete subgroup of $\mathbf{A}_K$ and similarly we can diagonally embed K^* in $\mathbf{J}_K$ as a discrete subgroup [10, Ch. 7, Thm. 1]. The *idele class group* of K is defined as the topological group $C_K := \mathbf{J}_K / K^*$. For a finite extension L/K of number fields, we have a canonical embedding $\mathbf{A}_K \to \mathbf{A}_L$. Together with the diagonal embedding $L \to \mathbf{A}_L$ this gives a canonical isomorphism $\mathbf{A}_K \otimes L \to \mathbf{A}_L$ of topological rings [5, Ch. 2.14]. Hence, $\mathbf{A}_L$ is a free module of finite rank over $\mathbf{A}_K$ and we get a norm map $\mathbf{A}_L \to \mathbf{A}_K$, which we will denote by $N_{L/K}$. It coincides with the norm map $N_{L/K} : L \to K$ on the diagonal of L and K in $\mathbf{A}_L$ and $\mathbf{A}_K$ respectively. More explicitly, the norm $N_{L/K} : \mathbf{A}_L \to \mathbf{K}$ maps an element $(x_w)_w \in \mathbf{A}_L$ to an element $(y_v)_v \in \mathbf{A}_K$ such that for any place v of K we have

$$y_v = \prod_{w \mid v} N_{L_w/K_v}(x_w).$$

This norm map $\mathbf{A}_L \to \mathbf{A}_K$ induces a norm map $N_{L/K} : C_L \to C_K$ of idele class groups.

Now suppose that L/K is an abelian extension and write $G := \mathrm{Gal}(L/K)$. For any prime $\mathfrak{p}$ of K that does not ramify in L, there is a unique element $\sigma \in G_{\mathfrak{p}} \subset G$, the Artin symbol $(L/K, \mathfrak{p})$, such that for all $x \in L$ and any prime $\mathfrak{q}$ of L that lies above $\mathfrak{p}$, we have $\sigma(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{q}$, where $N(\mathfrak{p})$ is the ideal norm of $\mathfrak{p}$. The Artin symbol does not depend on $\mathfrak{q}$. Let $\mathfrak{d}$ be the relative discriminant of L/K and write $I(\mathfrak{d})$ for the set of fractional $\mathcal{O}_K$ ideals relatively prime to $\mathfrak{d}$. Then by multiplication we can extend the Artin symbols to an *Artin map* $I(\mathfrak{d}) \to G$. This map is surjective and induces a related *global Artin map* that appears in a global result, Theorem 2.40. The relation between these two Artin maps can be found in [10, Ch. 10]. First we state the local class field theorem for non-Archimedean local number fields K, i.e., for fields K that are the finite extensions of $\mathbb{Q}_p$ for some prime p. This result can be found in [16, Ch. 13.4].

Theorem 2.39 (Local Class Field Theorem)**.** *Let K be a non-Archimedean local number field and fix an algebraic closure K^{alg} of K. Let Σ be the set of finite abelian extensions of K contained in K^{alg}. Let $\mathcal{D}$ be the set of open subgroups of K^* of finite index. Then the map*

$$\begin{aligned} \Sigma &\to \mathcal{D} \\ L &\mapsto N_{L/K}L^* \end{aligned}$$

is an inclusion-reversing bijection. For an extension $L \in \Sigma$ and the corresponding open subgroup $D := N_{L/K}L^*$ there is a local Artin isomorphism $K^*/N_{L/K}L^* \xrightarrow{\sim} \mathrm{Gal}(L/K)$, and it maps the unit group U of the valuation ring of K isomorphically to the inertia group $I_{L/K}$ of L/K and prime elements are mapped to the Frobenius coset modulo $I_{L/K}$.

Notice that for K a non-Archimedean local number field we have in fact that every subgroup of K^* of finite index is open. Hence, we find that the local Artin maps induce an isomorphism

$$\widehat{K^*} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

The following result can be found in [5, Ch. 14.5-14.6] and [10, Ch. 10-11].

Theorem 2.40 (Global Class Field Theorem)**.** *Let K be an algebraic number field and fix an algebraic closure K^{alg} of K. Let Σ be the set of finite abelian extensions of K contained in K^{alg}. Let $\mathcal{D}$ be the set of open subgroups of the idele class group C_K. Then the map*

$$\begin{aligned} \Sigma &\to \mathcal{D} \\ L &\mapsto N_{L/K}C_K \end{aligned}$$

is an inclusion-reversing bijection. For an extension $L \in \Sigma$ and the corresponding open subgroup $D := N_{L/K}C_K$ there is a global Artin isomorphism $C_K/D \xrightarrow{\sim} \mathrm{Gal}(L/K)$, and it maps K_v^* surjectively to the decomposition group $G_v = \mathrm{Gal}(L_w/K_v)$ for any place v of K. This induces the local Artin isomorphism

$$K_v^*/N_{L_w/K_v}L_w^* \xrightarrow{\sim} G_v \subset \mathrm{Gal}(L/K),$$

where $w \mid v$ is a place extending v.

Every open subgroup of C_K is of finite index in C_K [10, p. 212]. Hence, it follows from Theorem 2.40 that the global Artin map yields an isomorphism

$$\varprojlim C_K/N \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where N ranges over the open subgroups of C_K. In particular, for $K = \mathbb{Q}$ we get an isomorphism $\widehat{\mathbb{Z}}^* \cong \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ induced by the continuous morphism

$$\prod_p \mathbb{Z}_p^* \to C_{\mathbb{Q}}, \quad (x_p)_p \mapsto \overline{(x_v)_v}, \text{ where } x_v = \begin{cases} x_v & \text{if } v \text{ is finite,} \\ 1 & \text{if } v = \infty. \end{cases}$$

3 Cohomology of topological groups

3.1 Continuous cohomology

Let G, A be topological groups with A abelian, and suppose that A is a G-module. Then A is a *topological G-module* if the action of G on A induces a continuous map $G \times A \to A$, where $G \times A$ has the product topology. A morphism of topological G-modules is a continuous morphism of G-modules. This gives a category of topological G-modules. If G is profinite and A discrete, then A is a topological G-module if and only if $A = \bigcup_N A^N$, where N ranges over the open normal subgroups of G and where A^N is the subgroup of A of fixed points by N [11, Lemma 5.3.1]. We will omit the adjective "topological" when we refer to profinite or discrete topological G-modules. The theory as developed in this section can be found in general in [8] and for profinite groups G in [18].

For any $n \in \mathbb{Z}_{\geq 0}$ we consider the abelian group $\mathrm{C}^n(G, A)$ of continuous maps $G^n \to A$, where G^n has the product topology. For any $n \in \mathbb{Z}_{\geq 0}$ we define the *boundary map* $d_n : \mathrm{C}^n(G, A) \to \mathrm{C}^{n+1}(G, A)$ as the group homomorphism such that for each $f \in \mathrm{C}^n(G, A)$ and all $(g_1, \ldots, g_{n+1})^{n+1}$ we have

$$\begin{aligned}(d_n f)(g_1, \ldots, g_{n+1}) = g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ + (-1)^{n+1} f(g_1, \ldots, g_n).\end{aligned}$$

We define d_{-1} as the trivial map $0 \to \mathrm{C}^0(G, A)$. Fix $n \in \mathbb{Z}_{\geq 0}$. We define the *group of continuous n-cocycles* as the kernel of d_n and denote this group by $\mathrm{Z}^n(G, A)$. Moreover, we define the *group of continuous n-coboundaries* as the image of d_{n-1} and denote this group by $\mathrm{B}^n(G, A)$. By a direct calculation it can be shown that we have $\mathrm{B}^n(G, A) \subset \mathrm{Z}^n(G, A)$. We define the *$n$-th continuous cohomology group with coefficients in A* as the quotient $\mathrm{H}^n(G, A) := \mathrm{Z}^n(G, A)/\,\mathrm{B}^n(G, A)$. Observe that we can identify $\mathrm{H}^0(G, A)$ with the group of invariants A^G under G. Moreover, if G is discrete, then the continuous group cohomology above coincides with the usual group cohomology as found in [16].

Let G, G' be topological groups and let A, A' be a topological G-module and a topological G'-module respectively. Then we say continuous group homomorphisms $f : G' \to G$ and $g : A \to A'$ are *compatible* if for all $a \in A$ and $x \in G'$ we have $g(f(x)a) = xg(a)$. If $f : G' \to G$ and $g : A \to A'$ are compatible, then for each $n \in \mathbb{Z}_{\geq 0}$ we get a well-defined group homomorphism

$$(f, g)_n^* : \mathrm{H}^n(G, A) \to \mathrm{H}^n(G', A'), \quad [\omega] \mapsto [(x_1, \ldots, x_n) \mapsto (g \circ \omega)(f(x_1), \ldots, f(x_n))].$$

For any two topological abelian groups G, A we can view A as a topological G-module with trivial action of G on A. Denote the category of topological abelian groups by $\mathbf{TAb}$. By only considering trivial actions, we get a bifunctor $\mathrm{H}^n(-, -) : \mathbf{TAb} \times \mathbf{TAb} \to \mathbf{Ab}$ that maps $(f : G' \to G, g : A \to A')$ to $\mathrm{H}^n(f, g) = (f, g)_n^*$. Similarly, we get a bifunctor $\mathrm{Z}^n(-, -) : \mathbf{TAb} \times \mathbf{TAb} \to \mathbf{Ab}$ that maps $(f : G' \to G, g : A \to A')$ to

$$\mathrm{Z}^n(G, A) \to \mathrm{Z}^n(G', A'), \quad \omega \mapsto [(x_1, \ldots, x_n) \mapsto (g \circ \omega)(f(x_1), \ldots, f(x_n))].$$

Let G be a topological group. We call a short exact sequence $0 \to A \to B \to C \to 0$ of topological G-modules *well-adjusted* if $A \to B$ induces a homeomorphism of A onto its image and $B \to C$ admits a continuous set-theoretic section. The following result can be found in [8, Thm. 1.15], and a profinite variant can be found in [18, Thm 9.3.3], and in this result we call each homomorphism δ a *connecting homomorphism.*

Theorem 3.1. *Let G be a topological group. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a well-adjusted short exact sequence of topological G-modules.*

(a) *For each $n \geq 0$ there is a unique homomorphism $\delta : \mathrm{H}^n(G,C) \to \mathrm{H}^{n+1}(G,A)$ such that for all $a \in \mathrm{Z}^{n+1}(G,A)$, $b \in \mathrm{C}^n(G,B)$, and $c \in \mathrm{Z}^n(G,C)$ satisfying $f \circ a = d_n b$ and $g \circ b = c$ we have $\delta[c] = [a]$.*

(b) *The sequence*

$$0 \longrightarrow \mathrm{H}^0(G,A) \xrightarrow{(\mathrm{id}_G,f)_0^*} \mathrm{H}^0(G,B) \xrightarrow{(\mathrm{id}_G,g)_0^*} \mathrm{H}^0(G,C) \xrightarrow{\delta} \mathrm{H}^1(G,A) \xrightarrow{(\mathrm{id}_G,f)_1^*} \dots$$

$$\dots \xrightarrow{\delta} \mathrm{H}^n(G,A) \xrightarrow{(\mathrm{id}_G,f)_n^*} \mathrm{H}^n(G,B) \xrightarrow{(\mathrm{id}_G,g)_n^*} \mathrm{H}^n(G,C) \xrightarrow{\delta} \mathrm{H}^{n+1}(G,A) \xrightarrow{(\mathrm{id}_G,f)_{n+1}^*} \dots$$

is exact.

Another important exact sequence is the inflation-restriction sequence for profinite groups. Let N be a closed normal subgroup of a profinite group G. Let A be a topological G-module. Then the inclusion morphism $\iota : N \to G$ is compatible with the identity map id_A on A. For any $n \in \mathbb{Z}_{\geq 0}$ we get a *restriction map*

$$\mathrm{Res} : \mathrm{H}^n(G,A) \to \mathrm{H}^n(N,A)$$

defined as the map $(\iota, \mathrm{id}_A)_n^*$. Moreover, for any $x \in G$ the morphisms $N \to N, y \mapsto xyx^{-1}$ and $A \to A, a \mapsto xa$ are compatible and they give a morphism $\mathrm{H}^n(N,A) \to \mathrm{H}^n(N,A)$. This endows $\mathrm{H}^n(N,A)$ with a G/N-module structure. The image of the restriction map $\mathrm{H}^n(G,A) \to \mathrm{H}^n(N,A)$ lies in the group of G/N-invariants $\mathrm{H}^n(N,A)^{G/N}$.

The topological group A^N of N-invariants is naturally a topological G/N-module. The quotient map $\pi : G \to G/N$ and the inclusion map $\iota' : A^N \to A$ are compatible. Hence, for any $n \in \mathbb{Z}_{\geq 0}$ we get an *inflation map*

$$\mathrm{Inf} : \mathrm{H}^n(G/N, A^N) \to \mathrm{H}^n(G,A)$$

defined as the map $(\pi, \iota')_n^*$. The following result gives inflation-restriction sequences and can be found in [18, Prop. 10.3.1] for profinite groups and in [16, Ch. 7.6], [7] for discrete groups G.

Theorem 3.2. *Let G be a (profinite) group, let A be a (discrete) G-module and let N be a (closed) normal subgroup of G. Suppose that $n > 0$ is an integer such that $\mathrm{H}^i(N,A) = 0$ for all $1 \leq i \leq n-1$. Then there is an exact sequence*

$$0 \to \mathrm{H}^n(G/N, A^N) \xrightarrow{\mathrm{Inf}} \mathrm{H}^n(G,A) \xrightarrow{\mathrm{Res}} \mathrm{H}^n(N,A)^{G/N} \to \mathrm{H}^{n+1}(G/N, A^N) \xrightarrow{\mathrm{Inf}} \mathrm{H}^{n+1}(G,A).$$

3.2 Cup products

For a profinite group G and discrete G-modules A and B we view $A \otimes B$ as a discrete G-module with the action defined by $g(a \otimes b) = ga \otimes gb$ where $g \in G$, $a \in A$, $b \in B$ [11, Ch. 7.9].

A proof of the following result can be found in [11, Ch. 7, Prop. 5]. A formulation with Tate-cohomology for finite groups G can be found in [16, Ch. 8.3] and in [12, Ch. 9.7]. The bilinear maps $-\cup-$ in this result are called *cup products.*

Proposition 3.3. *Let G be a profinite group. There exists a unique family of bilinear maps*

$$-\cup- : \mathrm{H}^n(G,A)\times \mathrm{H}^m(G,B)\to \mathrm{H}^{n+m}(G,A\otimes B),\quad (a,b)\mapsto a\cup b,$$

defined for all $n,m\in\mathbb{Z}_{\geq 0}$ and all discrete G-modules A and B, such that the following four properties hold.

(1) *The bilinear maps $-\cup-$ are natural in A and B.*

(2) *For $n=m=0$ the bilinear map $-\cup-$ equals the bilinear map*

$$A^G\times B^G\to (A\otimes B)^G,\quad (a,b)\mapsto a\otimes b.$$

(3) *Let B be a discrete G-module. Consider an exact sequence*

$$0\to A\to A'\to A''\to 0$$

of discrete G-modules. If the induced sequence

$$0\to A\otimes B\to A'\otimes B\to A''\otimes B\to 0$$

is exact, then for all $a''\in\mathrm{H}^n(G,A'')$ and $b\in\mathrm{H}^m(G,B)$ we have

$$(\delta a'')\cup b=\delta(a''\cup b)\quad \textit{in}\ \ \mathrm{H}^{n+m+1}(G,A\otimes B),$$

where δ denotes the connecting homomorphism from section 3.1.

(4) *Let A be a discrete G-module. Consider an exact sequence*

$$0\to B\to B'\to B''\to 0$$

of discrete G-modules. If the induced sequence

$$0\to A\otimes B\to A\otimes B'\to A\otimes B''\to 0$$

is exact, then for all $a\in\mathrm{H}^n(G,A)$ and $b''\in\mathrm{H}^m(G,B'')$ we have

$$a\cup(\delta b'')=(-1)^n\delta(a\cup b'')\quad \textit{in}\ \ \mathrm{H}^{n+m+1}(G,A\otimes B),$$

where δ denotes the connecting homomorphism from section 3.1.

3.3 Quotient categories

In this subsection we define the quotient of a category by some equivalence relation.

Let $\mathcal{C}$ be a category. Then a class $R\subset\{\text{isomorphisms of }\mathcal{C}\}$ is an *isomorphism equivalence class of* $\mathcal{C}$ if it has the following three properties:

(i) for any $X\in\mathrm{Ob}(\mathcal{C})$ we have $1_X\in R$,

(ii) R is closed under composition in $\mathcal{C}$,

(iii) for any $f\in R$ we have $f^{-1}\in R$.

Notice that R induces an equivalence relation $\sim_R$ on $\mathrm{Ob}(\mathcal{C})$ given by $X\sim_R Y$ if and only if $\mathrm{Hom}_{\mathcal{C}}(X,Y)\cap R$ is non-empty. Moreover, R induces an equivalence relation $\approx_R$ on $\mathrm{Hom}(\mathcal{C})$ given by $f\approx_R g$ if and only if there exist $\sigma,\tau\in R$ such that $(\sigma,\tau)\in\mathrm{Arr}_{\mathcal{C}}(f,g)$, where $\mathrm{Arr}_{\mathcal{C}}$ is the arrow category of $\mathcal{C}$.

Definition 3.4. Let $\mathcal{C}$ be a category and let R be an isomorphism equivalence class of $\mathcal{C}$. Then the *quotient category of* $\mathcal{C}$ *by* R is a category $\mathcal{C}/R$ and a functor $\mathcal{Q} : \mathcal{C} \to \mathcal{C}/R$ satisfying the following requirements:

(1) $\forall X, Y \in \mathrm{Ob}(\mathcal{C}), [\exists \sigma \in R : \sigma \in \mathrm{Hom}_{\mathcal{C}}(X, Y)] \Longrightarrow \mathcal{Q}(X) = \mathcal{Q}(Y)$,

(2) $\forall f, g \in \mathrm{Hom}(\mathcal{C}), [\exists \sigma, \tau \in R : (\sigma, \tau) \in \mathrm{Arr}_{\mathcal{C}}(f, g)] \Longrightarrow \mathcal{Q}(f) = \mathcal{Q}(g)$,

and such that for every other category $\mathcal{Y}$ and functor $\mathcal{Q}' : \mathcal{C} \to \mathcal{Y}$ satisfying (1) and (2), there exists a unique functor $\mathcal{F} : \mathcal{C}/R \to \mathcal{Y}$ such that $\mathcal{F}\mathcal{Q} = \mathcal{Q}'$. △

In the definition above we call $\mathcal{Q}$ the *quotient functor.* Notice that the quotient category by an isomorphism equivalence class is unique up to unique isomorphism that commutes with the quotient functors. Under some assumptions we can also prove existence of such a quotient category. Let X be a class with an equivalence relation $\sim$ on X. Then a *class of representative sets of* $(X, \sim)$ is a class $Y \subset X$ such that

(1) for all $y \in Y$ the equivalence class $[y]_\sim \cap Y$ of y is a set,

(2) for all $x \in X$ there exists $y \in Y$ such that $x \sim y$. Notice that such an element y does not have to be unique.

Proposition 3.5. *Let* $\mathcal{C}$ *be a locally small category and let* R *be an isomorphism equivalence class of* $\mathcal{C}$ *inducing an equivalence relation* $\sim_R$ *on* $\mathrm{Ob}(\mathcal{C})$*. Suppose that*

(i) *there exists a class of representative sets of* $(\mathrm{Ob}(\mathcal{C}), \sim_R)$*,*

(ii) *for all* $X, Y \in \mathrm{Ob}(\mathcal{C})$ *we have* $\#(\mathrm{Hom}_{\mathcal{C}}(X, Y) \cap R) \leq 1$*.*

Then the quotient category $\mathcal{C}/R$ *exists.*

Proof. We will construct $\mathcal{C}/R$. Let Z be a class of representative sets of $(\mathrm{Ob}(\mathcal{C}), \sim_R)$. We define the objects $\mathrm{Ob}(\mathcal{C}/R)$ of $\mathcal{C}/R$ to be the quotient class $Z/{\sim_R}$. Consider the equivalence relation $\approx_R$ on $\mathrm{Hom}(\mathcal{C})$ induced by R. Now for any $X, Y \in \mathrm{Ob}(\mathcal{C}/R)$ we define

$$\mathrm{Hom}_{\mathcal{C}/R}(X, Y) := \Big(\bigcup_{x \in X} \bigcup_{y \in Y} \mathrm{Hom}_{\mathcal{C}}(x, y) \Big) / \approx_R .$$

The composition $[g] \circ [f]$ of $[f] \in \mathrm{Hom}_{\mathcal{C}/R}(X, Y)$ and $[g] \in \mathrm{Hom}_{\mathcal{C}/R}(Y, Z)$ is defined to be $[g \circ \sigma \circ f]$ for any $\sigma : \mathrm{codom}(f) \to \mathrm{dom}(g)$ in R. It follows from (ii) that this is independent of σ and of the chosen representatives of $[f]$ and $[g]$. Associativity of the composition is clear. □

Under assumption of the global axiom of choice, condition (i) in Proposition 3.5 is always fulfilled due to Scott's trick [9, p. 65]. However, in our applications we will not rely on the global axiom of choice.

3.4 2-Cocycles and Sectioned Central Extensions

In this subsection we will establish an equivalence of categories between (continuous) 2-cocycles and (continuous) central extensions with set-theoretic sections. We also compare several concepts in both categories. For example, the second cohomology group in terms of 2-cocycles can be translated in terms of such extensions. For simplicity, we only consider topological G-modules A with trivial action of G on A. A correspondence where non-trivial actions of G-modules A without topology are taken into account, is given in [4, Ch. 14.4].

We will first give some definitions of related concepts.

(i) We make the second cohomology group from section 3.1 more explicit by describing the cocycles and coboundaries. Let G, A be topological groups of which A is abelian. A continuous 2-cocycle is a continuous map $\omega : G\times G \to A$ such that for all $x, y, z \in G$ we have

$$\omega(y,z) - \omega(xy,z) + \omega(x,yz) - \omega(x,y) = 0.$$

A continuous map $b : G\times G \to A$ is a continuous 2-coboundary if for some continuous map $f : G \to A$ and for all $x, y \in G$ we have

$$b(x,y) = f(x) + f(y) - f(xy).$$

(ii) Let G, A be topological groups of which A is abelian. A *continuous central extension* of G by A is an exact sequence of topological groups

$$1 \to A \to E \to G \to 1$$

such that A is central in E and such that $A \to E$ induces a homeomorphism of A with $\operatorname{im}(A \to E)$. Such an extension is usually just denoted by E. For any surjective morphism $E \to G$ of topological groups with $\ker(E \to G) \subset \mathrm{Z}(E)$ we associate $E \to G$ to the natural central extension $\ker(E \to G) \rightarrowtail E \twoheadrightarrow G$. A *(continuous) sectioned central extension* of G by A is a continuous central extension E together with a continuous set-theoretic section $E \leftarrow G$ of the map $E \to G$, and such that $A \to E$ induces a homeomorphism $A \to \operatorname{im}(A \to E)$. A G-morphism of $E_1 \to E_2$ of two continuous sectioned central extensions E_1, E_2 of G by A_1, A_2 respectively is a morphism $E_1 \to E_2$ of topological groups such that the following diagrams

$$\begin{tikzcd}
1 \arrow[r] & A_1 \arrow[r] & E_1 \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A_2 \arrow[r] & E_2 \arrow[r] & G \arrow[r] & 1
\end{tikzcd}
\qquad
\begin{tikzcd}
E_1 \arrow[d] & G \arrow[l] \arrow[d, "\mathrm{id}"] \\
E_2 & G \arrow[l]
\end{tikzcd}$$

commute. This defines the category $\mathbf{PreZ^E}(G)$ of sectioned central extensions with objects (A, E, ι, π, s) that represent a central extension $A \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$ with section $s : G \to E$.

Let G be a topological group. We will define the category $\mathbf{Z^2}(G)$ of continuous 2-cocycles. The objects are pairs (A, ω) where A is an abelian topological group and $\omega : G \times G \to A$ is a continuous cocycle. A morphism between two objects (A_1, ω_1), (A_2, ω_2) is a morphism $f : A_1 \to A_2$ of topological groups such that the following diagram

$$\begin{tikzcd}
A_1 \arrow[r, "f"] & A_2 \\
G \times G \arrow[u, "\omega_1"] \arrow[ur, "\omega_2"'] &
\end{tikzcd}$$

commutes.

Let G be a topological group. We will define the category $\mathbf{Z^E}(G)$ of continuous sectioned central extension classes as a quotient category of $\mathbf{PreZ^E}(G)$. Consider the class $R(G)$ of those morphisms $(A_1 \rightarrowtail E_1 \twoheadrightarrow G) \to (A_2 \rightarrowtail E_2 \twoheadrightarrow G)$ of $\mathbf{PreZ^E}(G)$ that satisfy $A_1 = A_2$ and for which the induced morphism $A_1 \to A_2$ is the identity morphism. Notice that any element of $R(G)$ is an isomorphism and that for any two objects $E_1, E_2 \in \mathbf{PreZ^E}(G)$ there is at most one morphism $E_1 \to E_2$ in $R(G)$. Moreover, it can be verified that $R(G)$ is an isomorphism equivalence class of $\mathbf{PreZ^E}(G)$. Let $\sim_R$ be the equivalence relation induced by $R(G)$ on $\mathrm{Ob}(\mathbf{PreZ^E}(G))$. We consider the class $X(G)$ of those central extensions $(A, E, \iota, \pi, s) \in \mathrm{Ob}(\mathbf{PreZ^E}(G))$ for which the underlying set of E equals $A \times G$. Then $X(G)$ is a class of representative sets of the equivalence relation $R(G)$ induced by $R(G)$. Hence, by Proposition 3.5 we conclude that the quotient category $\mathbf{Z^E}(G) := \mathbf{PreZ^E}(G)/R(G)$ exists. Denote the quotient functor by $\mathcal{Q}_{\mathrm{SCE}}$ and notice that for any two morphisms $f_i : (A_i \rightarrowtail E_i \twoheadrightarrow G) \to (A'_i \rightarrowtail E'_i \twoheadrightarrow G)$ in $\mathrm{Hom}(\mathbf{PreZ^E}(G))$ with $i = 1, 2$ we have

$$\mathcal{Q}_{\mathrm{SCE}}(f_1) = \mathcal{Q}_{\mathrm{SCE}}(f_2) \Longleftrightarrow [A_1 = A_2,\ A'_1 = A'_2 \text{ and } f_1, f_2 \text{ induce the same map } A_1 \to A'_1].$$

Theorem 3.6. *Let G be a topological group. Then the categories $\mathbf{Z^2}(G)$ and $\mathbf{Z^E}(G)$ are isomorphic.*

Proof. We will define two functors $F_1 : \mathbf{Z^E}(G) \to \mathbf{Z^2}(G)$ and $F_2 : \mathbf{Z^2}(G) \to \mathbf{Z^E}(G)$ that are inverses of each other.

F_1 Let $1 \to A \to E \to G \to 1$ be a continuous sectioned central extension class with continuous set-theoretic section $s : G \to E$. Then $\omega : G \times G \to A$ defined by $(x, y) \mapsto s(x)s(y)s(xy)^{-1}$ is a continuous cocycle map. This construction of ω does not depend on the choice of the representative of the extension class, and defines $F_1(E)$ for any object $E \in \mathbf{Z^E}(G)$.

Now let $1 \to A_i \to E_i \to G \to 1$ be objects of $\mathbf{Z^E}(G)$, and let $f : E_1 \to E_2$ be a morphism in $\mathbf{Z^E}(G)$. Then f induces a morphism $F_1(f) : A_1 \to A_2$ of abelian topological groups.

F_2 Let $\omega : G \times G \to A$ be a continuous cocycle map. We define $A \times_\omega G$ as topological space as $A \times G$ endowed with the product topology and with the group operation $(a, x)(b, y) = (\omega(x, y)ab, xy)$. This turns $A \times_\omega G$ into a topological group. We also consider the morphisms $A \to A \times_\omega G$ given by $a \mapsto (a\omega(1, 1)^{-1}, 1)$ and $\pi : A \times_\omega G \to G$ given by $(a, x) \mapsto x$. Moreover, we consider a continuous set-theoretic section $G \to E$ of π given by $x \mapsto (1, x)$. Now E is a sectioned central extension of G by A, and we define $F_2(\omega)$ to be the class of E.

Let $f : (A_1, \omega_1) \to (A_2, \omega_2)$ be a morphism in $\mathbf{Z^2}(G)$. Then we define $F_2(f)$ to be the morphism $A_1 \times_{\omega_1} G \to A_2 \times_{\omega_2} G$ defined by $(a, g) \mapsto (f(a), g)$.

It can be verified that F_1F_2 and F_2F_1 equal the identity functors on $\mathbf{Z^2}(G)$ and $\mathbf{Z^E}(G)$ respectively. We will only elaborate why F_2F_1 is the identity on the objects of $\mathbf{Z^E}(G)$. Let $[(A, E, \pi, \iota, s)]$ be a sectioned central extension class. Applying F_2F_1 yields a central extension $(A, A \times_\omega G, \iota', \pi', s')$ and it can be verified that the following maps are inverse morphisms in $\mathbf{PreZ^E}(G)$:

$$\begin{array}{cc} E \to A \times_\omega G & A \times_\omega G \to E \\ x \mapsto (\iota^{-1}(x(s\pi x)^{-1}), \pi x) & (a, g) \mapsto \iota(a)s(g). \end{array}$$

Hence, E and $A \times_\omega G$ represent the same object in $\mathbf{Z^E}(G)$. □

A stronger version of the following corollary can be found in [8, Prop. 1.9].

Corollary 3.7. *Let $\xi : 0 \to A \to E \to G \to 0$ be a central exact sequence of topological groups. Then ξ is well-adjusted if and only if there is a homeomorphism $\varphi : E \to A \times G$*

for which the diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{id}"] & E \arrow[r] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & A \times G \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

commutes, where $A \to A \times G$ is the map $a \mapsto (a, 1)$ and $A \times G \to G$ is the map $(a, x) \mapsto x$.

Proof. If such a homeomorphism φ exists, then it is clear that ξ is well-adjusted. By Theorem 3.6 it suffices to prove the existence of φ in the case that ξ is the exact sequence $0 \to A \to A \times_\omega G \to G \to 0$ for some cocycle $\omega \in \mathrm{Z}^2(G, A)$. In this case, the map $\varphi : A \times_\omega G \to A \times G$ given by $(a, x) \mapsto (a\omega(1, 1), x)$ suffices. □

We will now start comparing several concepts in terms of 2-cocycles and sectioned central extensions. The correspondence between the 2-cocycles and sectioned central extensions yields the following result, which gives an interpretation of the second cohomology group in terms of sectioned central extensions.

Let G, A be topological groups and let A be abelian. We will present the analog of the group of 2-cocycles in terms of sectioned central extensions. Let $\mathrm{Z}^{\mathrm{E}}(G, A)$ be the group whose objects are objects $[(A, E, \iota, \pi, s)] \in \mathbf{Z^E}(G)$, and where the group operation is induced by the *Baer sum*: let $[(A, E_i, \iota_i, \pi_i, s_i)]$ be sectioned central extensions of G by A for $i = 1, 2$, then the Baer sum of E_1, E_2 is the sectioned central extension

$$E_1 + E_2 := E_1 \times_G E_2 / \{(\iota_1(a)), \iota_2(a)^{-1}) \mid a \in A\}$$

of G by A, where $E_1 \times_G E_2$ is the fiber product of E_1, E_2 over G. The morphism $A \to E_1 + E_2$ is given by $a \mapsto \overline{(\iota_1(a), 1)}$; the morphism $E_1 + E_2 \to G$ is given by $\overline{(x, y)} \mapsto \pi_1(x)$; the section $G \to E_1 + E_2$ is given by $g \mapsto \overline{(s_1(g), s_2(g))}$. Any two elements as in the diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota"] & E \arrow[r, "\pi"'] & G \arrow[l, bend right, "s"'] \arrow[r] & 1
\end{tikzcd}$$

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "-\iota"] & E \arrow[r, "\pi"'] & G \arrow[l, bend right, "s"'] \arrow[r] & 1
\end{tikzcd}$$

are inverses to each other in $\mathrm{Z}^{\mathrm{E}}(G, A)$. Notice that by Corollary 3.7 for profinite abelian groups G, A every element of $\mathrm{Z}^{\mathrm{E}}(G, A)$ is profinite.

We will show that $\mathrm{Z}^{\mathrm{E}}(-, -)$ is functorial in both arguments, in fact, it is a bifunctor, as will follow from Proposition 3.10 since $\mathrm{Z}^2(-, -)$ is a bifunctor. From the same proposition it follows that $\mathrm{Z}^{\mathrm{E}}(-, -)$ is additive in the second argument.

Definition 3.8. Let $g : A \to A'$ be a morphism of topological abelian groups. Consider a sectioned central extension $\xi = (A, E, \iota, \pi, s) \in \mathbf{PreZ^E}(G)$. Since ι is central, the pushout $E' := A' \sqcup_A E$ of ι and g exists in the category of topological groups. Then the diagram

$$\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[d, "g"] & E \arrow[r, "\pi"] \arrow[d] & G \\
A' \arrow[r, "\iota'"] & E' &
\end{tikzcd}$$

commutes. The zero map $A' \to G$ and π together induce a map $\pi' : E' \to G$ by the universal property of the pushout. Then $1 \to A' \to E' \to G \to 1$ is a central extension. It comes with a section $G \to E'$ that equals the composition $G \xrightarrow{s} E \to E'$. We now define $g\xi$ to be the object $(A', E', \iota', \pi', s') \in \mathbf{PreZ^E}(G)$. Moreover, we define $g\mathcal{Q}_{\mathrm{SCE}}(\xi) := \mathcal{Q}_{\mathrm{SCE}}(g\xi)$, and this does not depend on the choice of ξ. $\triangle$

For any morphism $g : A \to A'$ of topological abelian groups, and any topological group G, we define $\mathrm{Z^E}(G, g)$ as the map

$$\mathrm{Z^E}(G, g) : \mathrm{Z^E}(G, A) \to \mathrm{Z^E}(G, A'), \quad \xi \mapsto g\xi.$$

This yields a functor $\mathrm{Z^E}(G, -) : \mathbf{TAb} \to \mathbf{TAb}$, where $\mathbf{TAb}$ denotes the category of topological abelian groups.

Definition 3.9. Let $f : G' \to G$ be a morphism of topological groups. Consider a sectioned central extension $\xi = (A, E, \iota, \pi, s) \in \mathbf{PreZ^E}(G)$. We define E' as the pullback $A \times_G G'$ and we get the following commutative diagram.

$$\begin{tikzcd}
A \arrow[r, "\iota"] & E \arrow[r, "\pi"] & G \\
& E' \arrow[u] \arrow[r, "\pi'"] & G' \arrow[u, "f"']
\end{tikzcd}$$

The zero map $A \to G'$ and the map ι together induce a map $\iota' : A \to E'$ by the universal property of the pullback. The resulting sequence $1 \to A \to E' \to G' \to 1$ is exact and $A \to E'$ is central. Moreover, it comes together with a section $s' : G' \to E'$ induced by the two maps $s \circ f : G' \to E$ and $\mathrm{id} : G' \to G'$. We define ξf to be the object $(A, E', \iota', \pi', s') \in \mathbf{PreZ^E}(G')$. Moreover, we define $\mathcal{Q}_{\mathrm{SCE}}(\xi)f := \mathcal{Q}_{\mathrm{SCE}}(\xi f)$, and this does not depend on the choice of ξ. $\triangle$

For any morphism $f : G' \to G$ of topological groups, and any topological abelian group A, we define $\mathrm{Z^E}(f, A)$ as the map

$$\mathrm{Z^E}(f, A) : \mathrm{Z^E}(G, A) \to \mathrm{Z^E}(G', A), \quad \xi \mapsto \xi f.$$

This yields a functor $\mathrm{Z^E}(-, A) : \mathbf{TGrp} \to \mathbf{TGrp}$, where $\mathbf{TGrp}$ denotes the category of topological groups.

We define $\mathrm{B^E}(G, A)$ to be the subgroup of $\mathrm{Z^E}(G, A)$ consisting of all sectioned central extensions E for which there exists a section morphism $G \to E$ of topological groups of the map $E \to G$. We define $\mathrm{H^E}(G, A)$ as the quotient $\mathrm{Z^E}(G, A) / \mathrm{B^E}(G, A)$. Notice we get functors $\mathrm{H^E}(G, -), \mathrm{H^E}(-, A) : \mathbf{Ab} \to \mathbf{Ab}$ induced by $\mathrm{Z^E}(G, -)$, $\mathrm{Z^E}(-, A)$ respectively. Then $\mathrm{H^E}(-, -)$ is a bifunctor, as follows from Proposition 3.10. Moreover, if G is abelian, then we define $\mathrm{Ext^E}(G, A)$ as the subgroup of $\mathrm{H^E}(G, A)$ given by classes that are represented by abelian extensions E.

Proposition 3.10. *Let G, A be topological groups of which A is abelian. The isomorphism of categories $\mathbf{Z^2}(G) \cong \mathbf{Z^E}(G)$ induces a group isomorphism $\psi : \mathrm{Z}^2(G, A) \xrightarrow{\sim} \mathrm{Z^E}(G, A)$ that is natural in G and A. Moreover, we have $\psi[\mathrm{B}^2(G, A)] = \mathrm{B^E}(G, A)$ and a natural morphism $\mathrm{H}^2(G, A) \cong \mathrm{H^E}(G, A)$.*

Proof. It is clear that the induced map ψ is bijective. It can be verified that for any $\omega_1, \omega_2 \in \mathrm{Z}^2(G, A)$ we have $F_1(F_2(\omega_1) + F_2(\omega_2)) = \omega_1 + \omega_2$. From this it follows that ψ is a group isomorphism. In order to show that this isomorphism is natural in G and A, one can verify by a direct calculation that for any continuous homomorphisms $f : G' \to G$ and $g : A \to A'$ of topological abelian groups and any $E \in \mathrm{Z^E}(G, A)$ we have $F_1(\mathrm{Z^E}(G, g)(E)) = \mathrm{Z}^2(G, g)(F_1(E))$ and $F_1(\mathrm{Z^E}(f, A)(E)) = \mathrm{Z}^2(f, A)(F_1(E))$.

It is left to show that $\psi[\mathrm{B}^2(G,A)] = \mathrm{B}^{\mathrm{E}}(G,A)$. Let $\omega \in \mathrm{Z}^2(G,A)$. Then we have $\psi(\omega) \in \mathrm{B}^{\mathrm{E}}(G,A)$ if and only if there exists a continuous section morphism s of $\pi : A \times_\omega G \to G$. Hence, we have $\psi(\omega) \in \mathrm{B}^{\mathrm{E}}(G,A)$ if and only if there exists a continuous map $f : G \to A$ such that

$$\widetilde{f} : G \to A \times_\omega G, \quad x \mapsto (f(x)^{-1}, x)$$

is a homomorphism. Such a map $\widetilde{f}$ is a homomorphism if and only if for all $x, y \in G$ we have $\omega(x,y) = f(x)f(y)f(xy)^{-1}$. We conclude that $\psi[\mathrm{B}^2(G,A)] = \mathrm{B}^{\mathrm{E}}(G,A)$ and thus $\mathrm{H}^2(G,A) \cong \mathrm{H}^{\mathrm{E}}(G,A)$. □

Using the correspondence above, it can be shown that elements $E_1, E_2 \in \mathrm{Z}^{\mathrm{E}}(G,A)$ are in the same coset of $\mathrm{B}^{\mathrm{E}}(G,A)$ precisely when there exist morphisms of topological groups $E_1 \rightleftarrows E_2$ such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & E_1 \arrow[r] \arrow[d, shift right] & G \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & E_2 \arrow[r] \arrow[u, shift right] & G \arrow[r] & 1
\end{tikzcd}$$

commutes. Hence, the class in $\mathrm{H}^{\mathrm{E}}(G,A)$ of a central extension does not depend on the appended set-theoretic section. We thus see that $\mathrm{H}^{\mathrm{E}}(G,A)$ becomes the group of well-adjusted central extensions of G by A.

Let A, G be topological abelian groups. We call a sectioned central extension $A \rightarrowtail E \twoheadrightarrow G$ *commutative* if E is abelian, and in this case we also call $\mathcal{Q}_{\mathrm{SCE}}(E) \in \mathbf{Z^E}(G)$ commutative. This definition of commutativity for $\mathcal{Q}_{\mathrm{SCE}}(E)$ does not depend on E. We call a cocycle $\omega : G \times G \to A$ *commutative* if for all $x, y \in G$ we have $\omega(x,y) = \omega(y,x)$. We consider the induced full subcategories $\mathbf{CZ^E}(G)$ of $\mathbf{Z^E}(G)$ and $\mathbf{CZ^2}(G)$ of $\mathbf{Z^2}(G)$ with exactly those objects that are commutative. We define $\mathrm{CZ}^{\mathrm{E}}(G,A) \subset \mathrm{Z}^{\mathrm{E}}(G,A)$ and $\mathrm{CZ}^2(G,A) \subset \mathrm{Z}^2(G,A)$ as the subgroups of all commutative elements, and we denote by $\mathrm{Ext}^1(G,A)$ the quotient $\mathrm{CZ}^2(G,A)/\,\mathrm{B}^2(G,A) \subset \mathrm{H}^2(G,A)$. The correspondence between cocycles and extensions yields the following result, induced by the functors constructed in the proof of Theorem 3.6.

Theorem 3.11. *Let G be a topological abelian group. Then the categories $\mathbf{CZ^E}(G)$ and $\mathbf{CZ^2}(G)$ are isomorphic.*

Proof. One can verify that for any commutative cocycle $\omega \in \mathbf{CZ^2}(G)$ the extension $F_1(\omega)$ is commutative. Moreover, one can verify that for any commutative extension $\xi \in \mathbf{CZ^E}(G)$ the cocycle $F_2(\xi)$ is commutative. The result now follows from Theorem 3.6. □

Theorem 3.11 and Proposition 3.10 yield a natural isomorphism $\mathrm{Ext}^E(G,A) \cong \mathrm{Ext}^1(G,A)$.

Let G be a discrete abelian group. We define the category $\mathbf{DCZ^E}(G)$ as the full subcategory of $\mathbf{CZ^E}(G)$ with only those objects represented by extensions $A \rightarrowtail E \twoheadrightarrow G$ for which A is discrete. Similarly, we define the category $\mathbf{DCZ^2}(G)$ as the full subcategory of $\mathbf{CZ^2}(G)$ with only those objects represented by cocycles $G \times G \to A$ for which A is discrete. A group G without topology can be viewed as a discrete group, and thus also gives categories $\mathbf{DCZ^E}(G)$ and $\mathbf{DCZ^2}(G)$. Now let G be a profinite abelian group. Similary, by restricting the objects to those where A is profinite, we get the full subcategories $\mathbf{PCZ^E}(G)$, $\mathbf{PCZ^2}(G)$ of $\mathbf{CZ^E}(G)$, $\mathbf{CZ^2}(G)$ respectively. Theorem 3.11 has discrete and profinite analogues: for a discrete group G the categories $\mathbf{DCZ^E}(G)$ and $\mathbf{DCZ^2}(G)$ are isomorphic, and for a profinite group G the categories $\mathbf{PCZ^E}(G)$ and $\mathbf{PCZ^2}(G)$ are isomorphic.

Lemma 3.12. *Consider a commutative diagram of profinite groups*

$$\begin{tikzcd}
E \arrow[r, "\pi"] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, "h"] & 1 \\
E' \arrow[r, "\pi'"] & G' \arrow[r] & 1
\end{tikzcd}$$

with each row exact, and with h injective. Then for every continuous set-theoretic section s of π, there exists a continuous set-theoretic section s' of π' such that the diagram

$$\begin{tikzcd}
E \arrow[d, "\varphi"] & G \arrow[l, "s"'] \arrow[d, "h"] \\
E' & G' \arrow[l, "s'"]
\end{tikzcd}$$

commutes.

Proof. Let s be a continuous set-theoretic section of π. By Lemma 2.11, there exists a continuous set-theoretic section t of π'. Consider the continuous map $\delta : G \to E'$ defined by $g \mapsto (\varphi s g)^{-1}(thg)$. Notice that $\pi'\delta$ is the trivial map. By Lemma 2.12 there exists a continuous set-theoretic retraction r of h. Now $s' : G' \to E'$ defined by $g' \mapsto (tg')(\delta r g')^{-1}$ is a continuous set-theoretic section of π'. Compatibility of s with s' is easily verified. □

Proposition 3.13. *Consider a commutative diagram of profinite groups*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "f"] & E \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "h"] & 1 \\
1 \arrow[r] & A' \arrow[r] & E' \arrow[r] & G' \arrow[r] & 1
\end{tikzcd}$$

with each row a central extension. Suppose that h is injective. Then we have an equality $\mathrm{H}^{\mathrm{E}}(\mathrm{id}, f)[E] = \mathrm{H}^{\mathrm{E}}(h, \mathrm{id})[E']$.

Proof. Choose compatible continuous set-theoretic sections s and s' as in Lemma 3.12. Let ω and ω' be the cocycles corresponding to s and s' respectively, via Theorem 3.6. Now it can be routinely verified that $\mathrm{Z}^2(\mathrm{id}, f)(\omega) = \mathrm{Z}^2(h, \mathrm{id})(\omega')$, so the result follows from Proposition 3.10. □

The next proposition shows that Pontryagin duality distributes over Baer sums of profinite groups. Notice that the Baer sum of two profinite abelian groups is again profinite.

Proposition 3.14. *Let A, B be profinite abelian groups. Then for any abelian extensions $E_1, E_2 \in \mathrm{Z}^{\mathrm{E}}(A, B)$, we have $(E_1 + E_2)^* = E_1^* + E_2^*$ as extensions in $\mathrm{Z}^{\mathrm{E}}(B^*, A^*)$.*

Proof. Consider extensions $A \overset{\iota_i}{\to} E_i \overset{\pi_i}{\to} B$ for $i = 1, 2$, where E_1, E_2 are profinite abelian groups. Notice that we have

$$E_1^* + E_2^* = \mathrm{coker}(B^* \overset{(\pi_1^*, -\pi_2^*)}{\to} \ker(E_1^* \times E_2^* \overset{\iota_1^* - \iota_2^*}{\to} A^*))$$
$$(E_1 + E_2)^* = \ker(\mathrm{coker}(B^* \overset{(\pi_1^*, -\pi_2^*)}{\to} E_1^* \times E_2^*) \overset{\iota_1^* - \iota_2^*}{\to} A^*).$$

The natural map

$$\mathrm{coker}(B^* \to \ker(E_1^* \times E_2^* \to A^*)) \to \ker(\mathrm{coker}(B^* \to E_1^* \times E_2^*) \to A^*)$$

is a continuous bijection and thus an isomorphism of profinite abelian groups. It gives an equality $E_1^* + E_2^* = (E_1 + E_2)^*$ as extensions in $\mathrm{Z}^{\mathrm{E}}(B^*, A^*)$. □

3.5 Galois cohomology

We can apply cohomology to Galois extensions. Let L/K be a Galois extension of fields and consider the topological group $G := \mathrm{Gal}(L/K)$. Let A be a discrete topological G-module. Then for all $n \in \mathbb{Z}_{>0}$ we have a natural isomorphism $\mathrm{H}^n(G, A) \cong \lim_{\rightarrow} \mathrm{H}^n(G/N, A^N)$, where the direct limit homomorphisms are the inflation maps. Then G acts naturally on the multiplicative group L^*, turning L^* into a discrete topological G-module. Our interest lies in the cohomology groups $\mathrm{H}^n(G, L^*)$ for $n \in \mathbb{Z}_{\geq 0}$. The cohomology group $\mathrm{H}^0(G, L^*)$ is equal to the group of G-invariants of L^*, i.e., we have $\mathrm{H}^0(G, L^*) = K^*$. Moreover, the first cohomology group $\mathrm{H}^1(G, L^*)$ is also explicitly known. The following result can be found in [16, Ch. 10, Prop. 2].

Theorem 3.15 (Hilbert's Theorem 90)**.** *Let L/K be a Galois extension of fields. Then $\mathrm{H}^1(\mathrm{Gal}(L/K), L^*) = 0$.*

Let $K_1 \subset K_2$ be an extension of fields and consider two Galois field extensions L_1/K_1, L_2/K_2 with Galois groups G_1, G_2 respectively. Suppose that there is a K_1-morphism $f : L_1 \to L_2$. We get a morphism $f' : G_2 \to G_1$ induced by restricting automorphisms $\sigma \in G_2$ to $f(L_1) \cong L_1$. Then f and f' are compatible morphisms and for every $n \in \mathbb{Z}_{\geq 0}$ they induce homomorphisms $f_n : \mathrm{H}^n(G_1, L_1^*) \to \mathrm{H}^n(G_2, L_2^*)$. We see that the assignment of $\mathrm{H}^n(\mathrm{Gal}(L/K), L^*)$ to a Galois field extension L/K is functorial in L and K. The homomorphisms f_n do not depend on the choice of the embedding $L_1 \to L_2$ [16]. In particular, if there is an isomorphism $L_1 \xrightarrow{\sim} L_2$ that maps K_1 isomorphically to K_2, then $\mathrm{H}^n(G_1, L_1^*)$ and $\mathrm{H}^n(G_2, L_2^*)$ are canonically isomorphic.

Let K be a field and let K^{sep} be a separable closure of K. Then the *Brauer group of* K is the cohomology group $\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}*})$ and by the previous remarks it does not depend on the chosen separable closure up to canonical isomorphism. We denote this group by $\mathrm{Br}(K)$. For every morphism $K_1 \to K_2$ of fields, we get a homomorphism $\mathrm{Br}(K_1) \to \mathrm{Br}(K_2)$ by the previous remarks. In fact, $K \mapsto \mathrm{Br}(K)$ is a covariant functor **Field** → **Ab**. By Theorem 3.2 and Theorem 3.15 we get the following result.

Proposition 3.16. *Let k be a field and let K be a separable closure of k. Write $G :=$ $\mathrm{Gal}(K/k)$. Let N be a closed normal subgroup of G. Then there is an exact sequence*

$$0 \to \mathrm{H}^2(G/N, K^{*N}) \overset{\mathrm{Inf}}{\to} \mathrm{Br}(k) \overset{\mathrm{Res}}{\to} \mathrm{Br}(K^N)^{G/N} \to \mathrm{H}^3(G/N, K^{*N}) \overset{\mathrm{Inf}}{\to} \mathrm{H}^3(G, K^*).$$

A more general version of the following theorem can be found in [16, Ch. 13.3, Prop. 6].

Theorem 3.17. *Let K be a finite extension of $\mathbb{Q}_p$ for some prime p. Then the Brauer group $\mathrm{Br}(K)$ is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$.*

We will now define the norm-residue symbols. Let K be a finite extension of $\mathbb{Q}_p$ for some prime p and let $n \in \mathbb{Z}_{>0}$. Assume that $X^n - 1$ splits over K and denote by $\mu_n \subset K$ the group of n^{th} roots of unity. It follows from Kummer theory [16, Ch. 10.3] that for any $a \in K^*$ we get a well-defined homomorphism

$$\varphi_a : G \to \mu_n, \quad \varphi_a(\sigma) = \sigma(\zeta)/\zeta \quad \text{where } \zeta \in K^{\mathrm{sep}} \text{ is any root of } X^n - a.$$

Now we choose a primitive n^{th} root of unity in μ_n, and identify μ_n with $\mathbb{Z}/n\mathbb{Z}$ and the tensor product $\mu_n \otimes \mu_n$ over $\mathbb{Z}$ with μ_n. Write $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$. The short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow K^{\mathrm{sep}*} \xrightarrow{\nu} K^{\mathrm{sep}*} \longrightarrow 1$$

with ν given by $x \mapsto x^n$, induces by Theorem 3.1 and by Theorem 3.15 an exact sequence

$$0 \to \mathrm{H}^2(G, \mu_n) \xrightarrow{\iota} \mathrm{Br}(K) \xrightarrow{\cdot n} \mathrm{Br}(K).$$

We now define the *norm-residue symbol* of $a, b \in K^*$ to be $(a, b) := \iota(\varphi_a \cup \varphi_b)$, where $\cup$ denotes the cup product from section 3.2. Denote by $\mathrm{Br}(K)[n]$ the n-torsion of $\mathrm{Br}(K)$. For abelian groups A and B we call a map $f : A \times A \to B$ *non-degenerate* if for every non-zero $a \in A$ the homomorphisms $f(a, -), f(-, a) : A \to B$ are both not the zero map.

Theorem 3.18. *The map*

$$K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mathrm{Br}(K)[n], \qquad (aK^{*n}, bK^{*n}) \mapsto (a, b)$$

is a well-defined non-degenerate bilinear map.

Proof. This follows from Proposition 5 and Proposition 7 in [16, Ch. 14.2]. □

3.6 Ext functors

A category $\mathcal{C}$ is called *pre-additive* if for all objects $X, Y \in \mathrm{Ob}(\mathcal{C})$ the hom-set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is endowed with an abelian group structure, such that for any diagram in $\mathcal{C}$

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & C \arrow[r, "h"] & D \end{tikzcd}$$

we have $(g_1 + g_2) \circ f = (g_1 \circ f) + (g_2 \circ f)$ and $h \circ (g_1 + g_2) = (h \circ g_1) + (h \circ g_2)$, where $\circ$ and $+$ are respectively the composition and addition operators. A covariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ of pre-additive categories is called *additive* if for any objects $A, B \in \mathcal{C}$ the functor induces a group homomorphism $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}A, \mathcal{F}B)$. For pre-additive categories $\mathcal{C}, \mathcal{D}$ we say that a contravariant functor $\mathcal{C} \to \mathcal{D}$ is additive if it induces an additive functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$. The definition of a *cohomological δ-functor* can be found in [12] and in [17].

For any abelian group A the right-derived functors of the left-exact functor $\mathrm{Hom}(A, -)$ define the ext-functors:

$$\mathrm{ext}^i(A, -) := \mathrm{R}^i \mathrm{Hom}(A, -), \quad i \in \mathbb{Z}_{\geq 0}.$$

Moreover, if A, B are abelian groups, then we have [12, Thm. 6.67] [17, Thm. 2.7.6] an isomorphism

$$\mathrm{ext}^i(A, B) \cong (\mathrm{R}^i \mathrm{Hom}(-, B))(A), \quad i \in \mathbb{Z}_{\geq 0}.$$

Hence, we can endow $(\mathrm{ext}^i(-, B))_i$ with a cohomological δ-functor structure. Given an abelian group G and a short exact sequence $0 \to A \to B \to C \to 0$ of abelian groups, we denote for any $k \in \mathbb{Z}_{\geq 0}$ by

$$\delta : \mathrm{ext}^k(G, C) \to \mathrm{ext}^{k+1}(G, A), \qquad \delta : \mathrm{ext}^k(A, G) \to \mathrm{ext}^{k+1}(C, G)$$

the connecting homomorphisms given by the properties of $(\mathrm{ext}^i(G, -))_i$ and $(\mathrm{ext}^i(-, G))_i$ as cohomological δ-functors respectively.

We define ext-functors for discrete abelian torsion groups by setting

$$\mathrm{ext}^1(A, B) := \mathrm{ext}^1(A_{\mathrm{grp}}, B_{\mathrm{grp}})$$

for any discrete abelian torsion groups A and B with underlying groups A_{grp} and B_{grp} respectively. Moreover, we define ext-functors for profinite abelian groups by setting $\mathrm{ext}^1(A,B) := \mathrm{ext}^1(B^*,A^*)$ for any profinite abelian groups A, B, where A^*, B^* are the Pontryagin duals of A, B respectively. We remark that for all (profinite) abelian groups A, B with A projective or B injective, we have $\mathrm{ext}^1(A,B) = 0$.

We have the following important properties of ext-functors for abelian groups and of ext-functors for profinite abelian groups.

Theorem 3.19. *Let A, B be (profinite) abelian groups. Then the following holds.*

(a) *For all $i \in \mathbb{Z}_{\geq 2}$ we have we have $\mathrm{ext}^i(A,B) = 0$.*

(b) $\mathrm{ext}^*(A,-)$ *and* $\mathrm{ext}^*(-,B)$ *are covariant and contravariant cohomological δ-functors respectively.*

Proof. The proof of the statements for abelian groups can be found in [12] and in [17]. For profinite abelian groups, (a) follows immediately by applying Pontryagin duality. Hence, it is left to prove (b) for profinite abelian groups. Let Γ be a profinite abelian group and let $0 \to A \to B \to C \to 0$ be an exact sequence of profinite abelian groups. Then we get an exact sequence of abelian torsion groups $0 \to C^* \to B^* \to A^* \to 0$. It gives a diagram

$$\begin{tikzcd}
\mathrm{Hom}(\Gamma^*, C^*) \arrow[r] & \mathrm{Hom}(\Gamma^*, B^*) \arrow[r] & \mathrm{Hom}(\Gamma^*, A^*) \arrow[r] & \mathrm{ext}^1(\Gamma^*, C^*) \arrow[r] & \dots \\
\mathrm{Hom}(C,\Gamma) \arrow[r] \arrow[u, "\wr"] & \mathrm{Hom}(B,\Gamma) \arrow[r] \arrow[u, "\wr"] & \mathrm{Hom}(A,\Gamma) \arrow[r, dashed] \arrow[u, "\wr"] & \mathrm{ext}^1(C,\Gamma) \arrow[r] \arrow[u, "\mathrm{id}"] & \dots
\end{tikzcd}$$

where the dashed line indicate the existence of a unique map to make the diagram commutative. It can be verified that this yields an exact sequence as desired. The exact sequence for profinite abelian groups in the other argument can be constructed similarly. □

Let A, B be (profinite) abelian groups. Recall from section 3.4 that $\mathrm{Ext}^{\mathrm{E}}(A,B)$ is the subgroup of abelian extensions in $\mathrm{H}^{\mathrm{E}}(A,B)$. We will construct maps $\Theta, \Theta' : \mathrm{ext}^1(A,B) \to \mathrm{Ext}^{\mathrm{E}}(A,B)$. Consider an extension class $[E] \in \mathrm{Ext}^{\mathrm{E}}(A,B)$. The short exact sequence $0 \to B \to E \to A \to 0$ then yields, since $(\mathrm{ext}^i(A,-))_i$ is a cohomological δ-functor, exact sequences

$$\mathrm{Hom}(A,E) \to \mathrm{Hom}(A,A) \xrightarrow{\delta} \mathrm{ext}^1(A,B),$$
$$\mathrm{Hom}(E,B) \to \mathrm{Hom}(B,B) \xrightarrow{\delta} \mathrm{ext}^1(A,B).$$

We now define $\Theta([E]) := \delta(\mathrm{id}_A)$ and $\Theta'([E]) := \delta(\mathrm{id}_B)$. Then Θ is a well-defined map [17, Ch. 3.4]. Similarly, it follows that Θ' is well-defined. We don't know whether Θ is the same map as Θ', but we will not need this information.

Theorem 3.20. *Let A, B be (profinite) abelian groups. Then $\Theta : \mathrm{ext}^1(A,B) \to \mathrm{Ext}^{\mathrm{E}}(A,B)$ and $\Theta' : \mathrm{ext}^1(A,B) \to \mathrm{Ext}^{\mathrm{E}}(A,B)$ are isomorphisms that are natural in B and A respectively.*

Proof. We will only prove that the isomorphism $\Theta : \mathrm{ext}^1(A,B) \to \mathrm{Ext}^{\mathrm{E}}(A,B)$ is natural in B. Dually, it follows similarly that the isomorphism $\Theta' : \mathrm{ext}^1(A,B) \to \mathrm{Ext}^{\mathrm{E}}(A,B)$ is natural in A. If A, B are profinite abelian groups, then by Proposition 3.14 we get a natural isomorphism $\mathrm{Ext}^{\mathrm{E}}(A,B) \xrightarrow{\sim} \mathrm{Ext}^{\mathrm{E}}(B^*,A^*)$ by applying Pontryagin duality, and this map makes the diagram

$$\begin{tikzcd}
\mathrm{ext}^1(A,B) \arrow[r, "\Theta"] \arrow[d, "\mathrm{id}"] & \mathrm{Ext}^{\mathrm{E}}(A,B) \arrow[d, "\wr"] \\
\mathrm{ext}^1(B^*,A^*) \arrow[r, "\Theta"] & \mathrm{Ext}^{\mathrm{E}}(B^*,A^*)
\end{tikzcd}$$

commute. Hence, it suffices to prove the theorem for abelian groups without topology. In [17, Cor. 3.4.5] it is proved that $\Theta : \mathrm{ext}^1(A,B) \to \mathrm{Ext}^{\mathrm{E}}(A,B)$ is an isomorphism of groups. We will only prove the naturality of Θ in the second argument for abelian groups.

Let A, B, B' be abelian groups and let $f : B \to B'$ be a morphism. Let $[E] \in \mathrm{Ext}^{\mathrm{E}}(A,B)$ and let $[E'] \in \mathrm{Ext}^{\mathrm{E}}(A,B')$ be equal to $\mathrm{Ext}^{\mathrm{E}}(A,f)([E])$. We then have a morphism of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "f"] & E \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & B' \arrow[r] & E' \arrow[r] & A \arrow[r] & 0
\end{tikzcd}$$

and this shows, by the fact that ext^1 is a cohomological δ-functor, that the diagram

$$\begin{tikzcd}
\mathrm{Hom}(A,E) \arrow[r] & \mathrm{Hom}(A,A) \arrow[r, "\delta"] \arrow[d, "\mathrm{id}"] & \mathrm{ext}^1(A,B) \arrow[d, "\mathrm{ext}^1(A{,}f)"] \\
\mathrm{Hom}(A,E) \arrow[r] & \mathrm{Hom}(A,A) \arrow[r, "\delta"] & \mathrm{ext}^1(A,B')
\end{tikzcd}$$

commutes. From this it follows that $\Theta(\mathrm{Ext}^{\mathrm{E}}(A,f)([E])) = \mathrm{ext}^1(A,f)(\Theta([E]))$. Hence, the isomorphism Θ is natural in the second argument. □

Since $\mathrm{Ext}^{\mathrm{E}}$ and Ext^1 are naturally isomorphic bifunctors by the theory from section 3.4, we get the following theorem.

Theorem 3.21.

(a) *Let $0 \to A \to B \to C \to 0$ be an exact sequence of (profinite) abelian groups. Let G be a (profinite) abelian group. Then there exist connecting homomorphisms δ such that the following sequences are exact.*

$$\begin{aligned}
0 \to \mathrm{Hom}(G,A) \to \mathrm{Hom}(G,B) \to \mathrm{Hom}(G,C) &\xrightarrow{\delta} \mathrm{Ext}^1(G,A) \to \\
&\mathrm{Ext}^1(G,B) \to \mathrm{Ext}^1(G,C) \to 0, \\
0 \to \mathrm{Hom}(C,G) \to \mathrm{Hom}(B,G) \to \mathrm{Hom}(A,G) &\xrightarrow{\delta} \mathrm{Ext}^1(C,G) \to \\
&\mathrm{Ext}^1(B,G) \to \mathrm{Ext}^1(A,G) \to 0.
\end{aligned}$$

(b) *Let A, B be (profinite) abelian groups. If A is projective, or, if B is injective, then we have* $\mathrm{Ext}^1(A,B) = 0$.

Proof. $\mathrm{Ext}^{\mathrm{E}}$ and Ext^1 are naturally isomorphic bifunctors by the theory from section 3.4. Hence, part (a) follows from Theorem 3.19 and Theorem 3.20. Part (b) follows from Theorem 3.20 and the fact that for all (profinite) abelian groups A, B with A projective or B injective we have $\mathrm{ext}^1(A,B) = 0$. □

3.7 Calculation of Ext^1 groups

In this section we will state a couple of lemmas that will help describing Ext^1-groups more explicitly.

Lemma 3.22. *Let $n \in \mathbb{Z}_{>0}$. Let A, B be profinite abelian groups with A finite, and assume that $\exp(A) \mid n$. Let $\pi : B \to B/nB$ be the quotient map. Then*

$$\mathrm{Ext}^1(A, \pi) : \mathrm{Ext}^1(A, B) \xrightarrow{\sim} \mathrm{Ext}^1(A, B/nB)$$

is an isomorphism of abelian groups.

Proof. The exact sequence $B \xrightarrow{\cdot n} B \to B/nB \to 0$ yields an exact sequence

$$\mathrm{Ext}^1(A, B) \xrightarrow{\cdot n} \mathrm{Ext}^1(A, B) \longrightarrow \mathrm{Ext}^1(A, B/nB) \longrightarrow 0,$$

by right-exactness and additivity of $\mathrm{Ext}^1(A, -)$. The map $\mathrm{Ext}^1(A, B) \xrightarrow{\cdot n} \mathrm{Ext}^1(A, B)$ equals

$$n \cdot \mathrm{Ext}^1(\mathrm{id}, B) = \mathrm{Ext}^1(n \cdot \mathrm{id}, B) = \mathrm{Ext}^1(0, B) = 0,$$

where we use the additivity of $\mathrm{Ext}^1(-, B)$ and the equality $A[n] = A$. It follows that $\mathrm{Ext}^1(A, B) \to \mathrm{Ext}^1(A, B/nB)$ is an isomorphism. □

Lemma 3.23. *Let $n \in \mathbb{Z}_{>0}$ be an integer. Let A, B be finite abelian groups with exponent equal to n and suppose that A is cyclic. The map $\Xi : \mathrm{Ext}^1(A, B) \to \mathrm{Hom}(A, B)$ that sends an extension $B \rightarrowtail E \twoheadrightarrow A$ to the map $x \mapsto s(x)^n$, where s is a set-theoretic section of $E \twoheadrightarrow A$, is an isomorphism of groups that does not depend on the choice of s.*

Proof. First of all, one can verify that for any extension $B \rightarrowtail E \twoheadrightarrow A$ and any set-theoretic section s of $E \to A$, the map $x \mapsto s(x)^n$ is a homomorphism $A \to B$ that does not depend on the chosen section s. Moreover, it can be verified by using Baer sums that Ξ is indeed a group homomorphism. It is also injective: if x generates A and if s is a set-theoretic section of $E \to A$ such that $s(x)^n = 1$, then $x^k \mapsto s(x)^k$ with $k \in \mathbb{Z}$ gives a section homomorphism $A \to E$. Surjectivity follows from computing the order of $\mathrm{Ext}^1(A, B)$ by using a projective resolution $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to A \to 0$. □

Lemma 3.24. *Let A, B be profinite abelian groups of which A is finite. Suppose that the orders of A and B are coprime. Then $\mathrm{Ext}^1(A, B) = 0$ and $\mathrm{Ext}^1(B, A) = 0$.*

Proof. We will only prove that $\mathrm{Ext}^1(A, B) = 0$. The other part is analogous. Write $n := \#A$. By additivity of Ext^1 in both arguments, we have $f := \mathrm{Ext}^1(n \cdot \mathrm{id}_A, B) = \mathrm{Ext}^1(A, n \cdot \mathrm{id}_B)$. Moreover, $n \cdot \mathrm{id}_A$ is the zero map and $n \cdot \mathrm{id}_B$ is an isomorphism. Hence $f = 0$ and f is an isomorphism on $\mathrm{Ext}^1(A, B)$. We conclude that $\mathrm{Ext}^1(A, B) = 0$. □

4 Profinite groups

In this section we will treat several constructions of universal objects in the category of (abelian) profinite groups: products, tensor products, and exterior squares. Moreover, we will define restricted products of collections of functors.

4.1 Profinite products

Notice that products exist in the category of profinite groups: the product $\prod_i G_i$ of the collection $(G_i)_i$ in the category of topological groups is compact, Hausdorff and totally disconnected, and thus a profinite group by Proposition 2.7. The projection maps from the product are profinite morphisms.

In the setting of the definition above, any open normal subgroup N of $\prod_i G_i$ has an open subset of the form $\prod_i V_i$ where $V_i \subset G_i$ equals G_i for all but finitely many $i \in I$. By Lemma 2.8 each V_i contains an open normal subgroup of G_i. Hence, there exists an open normal subgroup of finite index $\prod_i N_i$ of $\prod_i G_i$ contained in N. We therefore conclude that

$$\prod_{i\in I} G_i = \varprojlim \prod_{i\in I}(G_i/N_i),$$

where the inverse limit ranges over collections $(N_i)_i$ such that N_i is an open normal subgroup of G_i for all $i \in I$, and $N_i = G_i$ for all but finitely many i. For a profinite group G and a set X we denote by G^X the product $\prod_{x\in X} G$. For any collection $(f_i : G_i \to G)_i$ of morphisms of profinite groups indexed by a set I, we write $f_i \to 0$ if for each open normal subgroup $N \subset G$ the set $\{i \in I : \operatorname{im} f_i \not\subset N\}$ is finite. The following lemma is useful for defining morphisms of profinite groups out of a product of profinite groups.

Lemma 4.1. *Let $(F_i)_{i\in I}$ be a collection of profinite groups and let G also be a profinite group. Then the natural map $\varphi : \operatorname{Hom}(\prod_i F_i, G) \to \prod_i \operatorname{Hom}(F_i, G)$ is injective and its range equals*

$$\left\{ (f_i)_{i\in I} \;\middle|\; \begin{array}{cc} (1) & \forall i \in I, f_i \in \operatorname{Hom}(F_i, G), \\ (2) & \forall i, j \in I, i \neq j \Rightarrow [\operatorname{im} f_i, \operatorname{im} f_j] = 1, \\ (3) & f_i \to 0 \end{array} \right\}.$$

Proof. If $f, g \in \prod_i F_i$ are such that $\varphi(f) = \varphi(g)$, then the closed set $X := \{x \in \prod_i F_i \mid f(x) = g(x)\}$ contains $\prod_{j\in J} F_j$ for every finite subset $J \subset I$, hence $X = \prod_i F_i$ and φ is injective. Let H be the subset of $\prod_{i\in I} \operatorname{Hom}(F_i, G)$ of elements satisfying properties (1), (2), (3). It is not difficult to verify that $\operatorname{ran}(\varphi) \subset H$. In order to prove the inclusion $\operatorname{ran}(\varphi) \supset H$, consider any element $(f_i)_i \in H$. For any open normal subgroup $N \lhd G$ the map $f_N : \prod_i F_i \to G/N$ defined by $(x_i)_i \mapsto \prod_i f_i(x_i)$ is well-defined and a group morphism. These maps are compatible and the inverse limit $f := \lim_{\longleftarrow} f_N$ is an element of $\operatorname{Hom}(\prod_i F_i, G)$ such that $\varphi(f) = (f_i)_i$. □

The following lemma is useful in order to prove universal properties of several constructions.

Lemma 4.2. *Let G be a profinite group, let X be a discrete set, and let $f : G \to X$ be a continuous map. Then there exist an open normal subgroup $N \subset G$ such that f factors through G/N.*

Proof. See [11, Lemma 1.1.16] or [18, Lemma 1.2.6]. □

More concretely, we will use Lemma 4.2 in the following form.

Corollary 4.3. *Let G_1, G_2 be profinite groups and let X be a discrete set. Let $f : G_1 \times G_2 \to X$ be a continuous map. Then there exist open normal subgroups $N_1 \subset G_1$, $N_2 \subset G_2$ such that f factors through $G_1/N_1 \times G_2/N_2$. If in addition $G := G_1 = G_2$ holds, then f factors through $G/N \times G/N$ for some open normal subgroup N of G.*

4.2 Profinite tensor products

In this section we will describe the profinite tensor products over $\widehat{\mathbb{Z}}$. For any profinite abelian groups A, B, the profinite tensor product over $\widehat{\mathbb{Z}}$ will be a profinite abelian group $A \otimes B$ together with a continuous bilinear map $-\otimes- : A \times B \to A \otimes B$ such that composition with $-\otimes-$ yields a representation $\mathrm{Hom}(A \otimes B, -) \to \mathrm{Bil}(A, B, -)$ of the functor that maps a profinite abelian group C to the set $\mathrm{Bil}(A, B, C)$ of continuous bilinear maps $A \times B \to C$. A general theory of profinite tensor products of profinite modules over profinite algebras can be found in [11, Ch. 5.5].

We define the profinite tensor product as the inverse limit of tensor products of finite abelian groups.

Definition 4.4. Let G_1, G_2 be profinite abelian groups. Let $(I, \leq)$ be the directed set of all pairs (N_1, N_2) such that N_i is an open subgroup of G_i for $i = 1, 2$, and with $(N_1, N_2) \leq (N_1', N_2')$ if and only if $N_i \subset N_i'$ for $i = 1, 2$. Then the *tensor product* of G_1 and G_2 over $\mathbb{Z}$ is defined to be

$$G_1 \otimes G_2 := \varprojlim \, (G_1/N_1) \otimes (G_2/N_2),$$

together with the inverse limit $- \otimes - : G_1 \times G_2 \to G_1 \otimes G_2$ of the natural compositions

$$G_1 \times G_2 \to G_1/N_1 \times G_2/N_2 \to G_1/N_1 \otimes G_2/N_2$$

where the limit ranges over I in both cases. △

We denote by $g_1 \otimes g_2 \in G_1 \otimes G_2$ the image of $(g_1, g_2) \in G_1 \times G_2$ under the map $- \otimes -$. From the commutative diagram

$$\begin{tikzcd}
G_1 \otimes G_2 \arrow[r] & G_1/N_1 \otimes G_2/N_2 \\
G_1 \times G_2 \arrow[r] \arrow[u] & G_1/N_1 \times G_2/N_2 \arrow[u]
\end{tikzcd}$$

it follows that $\{g_1 \otimes g_2 \mid g_1 \in G_1, g_2 \in G_2\}$ topologically generates $G_1 \otimes G_2$.

The profinite tensor product has the following universal property.

Lemma 4.5. *Let G_1, G_2, A be profinite abelian groups. Then for all continuous bilinear maps $G_1 \times G_2 \to A$ there exists a unique morphism $G_1 \otimes G_2 \to A$ of profinite groups such that the following diagram commutes.*

$$\begin{tikzcd}
G_1 \otimes G_2 \arrow[r, dashed, "\exists!"] & A \\
G_1 \times G_2 \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proof. Uniqueness of this morphism $G_1 \otimes G_2 \to A$ follows from the fact that the set of pure tensors of $G_1 \otimes G_2$ topologically generates $G_1 \otimes G_2$. We prove (i) existence for finite A and (ii) existence for all A. Let $\varphi : G_1 \times G_2 \to A$ be a continuous bilinear map.

(i) Suppose that A is finite. Then by Corollary 4.3 there exist open normal subgroups $N_1 \subset G_1$ and $N_2 \subset G_2$ such that φ factors through $G_1/N_1 \times G_2/N_2$. The factor $G_1/N_1 \times G_2/N_2 \to A$ induces a morphism $G_1 \otimes G_2 \to (G_1/N_1) \otimes (G_2/N_2) \to A$ of profinite groups that satisfies the diagram.

(ii) For any open subgroup M of A we get a morphism $G_1 \otimes G_2 \to A/M$ by (i). These morphisms are compatible and the inverse limit $G_1 \otimes G_2 \to A$ satisfies the diagram. □

It is clear that for any two profinite abelian groups G_1, G_2 there is an isomorphism of profinite groups $G_1 \otimes G_2 \cong G_2 \otimes G_1$. Moreover, for any $g_1 \in G_1,\ g_2 \in G_2$ and $x \in \widehat{\mathbb{Z}}$ we have $x(g_1 \otimes g_2) = (xg_1) \otimes g_2 = g_1 \otimes (xg_2)$.

Lemma 4.6. *For any profinite abelian group A we have $\widehat{\mathbb{Z}} \otimes A \cong A$ as profinite groups.*

Proof. Inverse morphisms between A and $\widehat{\mathbb{Z}} \otimes A$ are induced by the maps

$$\begin{aligned} \widehat{\mathbb{Z}} \times A &\to A & \qquad A &\to \widehat{\mathbb{Z}} \otimes A \\ (x, a) &\mapsto xa & a &\mapsto 1 \otimes a. \end{aligned}$$

□

Lemma 4.7. *Let I, J be closed ideals of $\widehat{\mathbb{Z}}$. Then we have $\widehat{\mathbb{Z}}/I \otimes \widehat{\mathbb{Z}}/J \cong \widehat{\mathbb{Z}}/(I + J)$.*

Proof. The continuous bilinear map $\widehat{\mathbb{Z}}/I \times \widehat{\mathbb{Z}}/J \to \widehat{\mathbb{Z}}/(I+J)$ given by $(x, y) \mapsto xy$ induces a morphism $\varphi : \widehat{\mathbb{Z}}/I \otimes \widehat{\mathbb{Z}}/J \to \widehat{\mathbb{Z}}/(I + J)$. The kernel of the morphism $\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}/I \otimes \widehat{\mathbb{Z}}/J$ defined by $x \mapsto x \otimes 1$ contains $I + J$ and thus factors through a morphism $\psi : \widehat{\mathbb{Z}}/(I + J) \to \widehat{\mathbb{Z}}/I \otimes \widehat{\mathbb{Z}}/J$. Notice that φ and ψ are inverse maps to each other, thus proving the lemma. □

4.3 Profinite exterior squares

In this section we will describe the profinite exterior squares over $\widehat{\mathbb{Z}}$. For abelian groups A we denote by $\bigwedge^2 A$ the group $(A \otimes A)/\langle a \otimes a \mid a \in A\rangle$. A map $f : G \times G \to A$, with G and A (profinite) abelian groups, is called *alternating* if it is bilinear and for all $g \in G$ we have $f(g, g) = 0$. For any profinite abelian group A the exterior square will be a profinite abelian group $\bigwedge^2 A$ together with a continuous alternating map $- \wedge - : A \times A \to \bigwedge^2 A$ such that composition with $- \wedge -$ yields a representation $\mathrm{Hom}(\bigwedge^2 A, -) \to \mathrm{Alt}^2(A, -)$ of the functor that maps a profinite abelian group B to the set $\mathrm{Alt}^2(A, B)$ of continuous alternating maps $A \times A \to B$.

Definition 4.8. Let G be a profinite abelian group. Then the *exterior square* of G is defined to be the inverse limit $\bigwedge^2 G := \lim_{\leftarrow} \bigwedge^2 G/N$ together with the inverse limit $G \times G \to \bigwedge^2 G$ of the natural compositions

$$G \times G \to G/N \times G/N \to \bigwedge^2 G/N$$

where N ranges over all open normal subgroups of G in both cases. △

We denote by $g_1 \wedge g_2 \in \bigwedge^2 G$ the image of $(g_1, g_2) \in G \times G$ under $- \wedge -$. Notice that $\{g_1 \wedge g_2 \mid g_1, g_2 \in G\}$ topologically generates $\bigwedge^2 G$.

Lemma 4.9. *Let G, A be profinite abelian groups. Then for all continuous alternating maps $G \times G \to A$ there exists a unique morphism $\bigwedge^2 G \to A$ of profinite groups such that* *the following diagram commutes.*

$$\begin{tikzcd}
\bigwedge^2 G \arrow[r, dashed, "\exists!"] & A \\
G \times G \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proof. The proof is completely analogous to the proof of Lemma 4.5. □

The alternating map $- \wedge - : G \times G \to \bigwedge^2 G$ naturally induces a morphism $G \otimes G \to \bigwedge^2 G$. We see that $\bigwedge^2$ is a functor $\mathbf{PAb} \to \mathbf{PAb}$ if we define for every $f \in \mathrm{Hom}(A, B)$ the map $\bigwedge^2 f : \bigwedge^2 A \to \bigwedge^2 B$ by $a \wedge a' \mapsto f(a) \wedge f(a')$, where $\mathbf{PAb}$ is the category of profinite abelian groups.

Lemma 4.10. *Let G be a profinite abelian group. The morphism $G \otimes G \to \bigwedge^2 G$ is surjective and the kernel is topologically generated by $\{g \otimes g \mid g \in G\}$.*

Proof. Let π be the morphism $G \otimes G \to \bigwedge^2 G$. Surjectivity of π follows from the fact that the natural morphism and the trivial morphism $\bigwedge^2 G \rightrightarrows \mathrm{coker}(\pi)$ are equal due to Lemma 4.9: they induce the same map $G \times G \to \mathrm{coker}(\pi)$. Denote by N the subgroup of $G \otimes G \to \bigwedge^2 G$ topologically generated by $\{g \otimes g \mid g \in G\}$. It is clear that $N \subset \ker \pi$. By Lemma 4.9 the composition $G \times G \to G \otimes G \to (G \otimes G)/N$ induces a morphism $f : \bigwedge^2 G \to (G \otimes G)/N$. Now $f \circ \pi$ equals the quotient morphism $G \otimes G \to (G \otimes G)/N$ and thus we have $\ker \pi = N$. □

Corollary 4.11. *For any profinite abelian group G we have $\bigwedge^2 G \cong (G \otimes G)/\overline{\langle g \otimes g \mid g \in G \rangle}$.*

Lemma 4.12. *Let $(G_i)_{i \in I}$ be a collection of profinite abelian groups indexed by a linear order $(I, \leq)$. Then the following map is an isomorphism:*

$$\overset{2}{\bigwedge} \prod_{i \in I} G_i \xrightarrow{\sim} \Big(\prod_i \overset{2}{\bigwedge} G_i \Big) \times \Big(\prod_{i<j} G_i \otimes G_j \Big)$$
$$(g_i)_i \wedge (g_i')_i \longmapsto ((g_i \wedge g_i')_i,\ (g_i \otimes g_j' - g_i' \otimes g_j)_{i<j}).$$

Proof. For every $k \in I$, let ι_k be the natural imbedding $G_k \to \prod_i G_i$. For all $j, k \in I$ we consider the map

$$G_j \times G_k \to \overset{2}{\bigwedge} (\prod_i G_i), \quad (g, g') \mapsto \iota_j(g) \wedge \iota_k(g').$$

These maps induce morphisms

$$f_{jk} : G_j \otimes G_k \to \overset{2}{\bigwedge} (\prod_i G_i) \quad \text{for all } i, j \in I \text{ with } j < k,$$
$$f_{jj} : \overset{2}{\bigwedge} G_j \to \overset{2}{\bigwedge} (\prod_i G_i) \quad \text{for all } j \in I.$$

Using Lemma 2.2 it can be shown that the collection of maps $(f_{ij})_{i \leq j}$ induces a morphism of profinite abelian groups

$$f : \Big(\prod_i \bigwedge^2 G_i\Big) \times \Big(\prod_{i<j} G_i \otimes G_j\Big) \longrightarrow \bigwedge^2 \prod_{i\in I} G_i.$$

The morphism of profinite abelian groups stated in the lemma is the inverse map of f, as can be easily verified. □

Corollary 4.13. *Let G be a profinite abelian group. Then G is procyclic if and only if $\bigwedge^2 G = 0$.*

Proof. If G is finite and cyclic, then it is clear that $\bigwedge^2 G = 0$. Hence, if G is procyclic we have $\bigwedge^2 G = \lim_{\leftarrow} \bigwedge^2 G/N = 0$. Now suppose that G is such that $\bigwedge^2 G = 0$. Then for any open subgroup N we have $\bigwedge^2 G/N = 0$, and by the structure theorem for finitely generated abelian groups it follows that G/N is cyclic. □

Lemma 4.14. *Let $(G_i)_{i\in I}$ be a collection of abelian groups indexed by a linear order $(I, \leq)$. Then the following map is an isomorphism:*

$$\bigwedge^2 \bigoplus_{i\in I} G_i \xrightarrow{\sim} \Big(\bigoplus_i \bigwedge^2 G_i\Big) \times \Big(\bigoplus_{i<j} G_i \otimes G_j\Big)$$
$$(g_i)_i \wedge (g_i')_i \longmapsto ((g_i \wedge g_i')_i,\ (g_i \otimes g_j' - g_i' \otimes g_j)_{i<j}).$$

Proof. The proof is analogous to the proof of Lemma 4.12. □

Remark 4.15. Let $1 \to A \xrightarrow{\iota} G \xrightarrow{v} \widehat{\mathbb{Z}} \to 1$ be a central short exact sequence of profinite abelian groups with A procyclic. This sequence splits because $\widehat{\mathbb{Z}}$ is projective. Let $\psi : G \xrightarrow{\sim} \widehat{\mathbb{Z}} \times A$ be an isomorphism of profinite groups such that $\psi\iota$ is the natural inclusion $A \to \widehat{\mathbb{Z}} \times A$ and such that $v\psi^{-1}$ is the natural projection $\widehat{\mathbb{Z}} \times A \to \widehat{\mathbb{Z}}$. We have $\bigwedge^2 A = 0$ and $\bigwedge^2 \widehat{\mathbb{Z}} = 0$ by Lemma 4.13, hence from Lemma 4.12 it follows that $\bigwedge^2(\widehat{\mathbb{Z}} \times A) \to A$ defined by $(x_1, a_1) \wedge (x_2, a_2) \mapsto a_2^{x_1} a_1^{-x_2}$ is an isomorphism. Precomposing this isomorphism with $\bigwedge^2 \psi$ yields an isomorphism $\widetilde{\psi} : \bigwedge^2 G \to A$. This isomorphism $\widetilde{\psi}$ does not depend on the choice of ψ, because it equals the morphism of profinite groups

$$\bigwedge^2 G \to A, \quad \text{defined by} \quad x \wedge y \mapsto \iota^{-1} \frac{y^{v(x)}}{x^{v(y)}}.$$

Its inverse $A \to \bigwedge^2 G$ is given by $a \mapsto \varphi \wedge \iota a$, where $\varphi \in G$ is such that $v(\varphi) = 1$. △

Example 4.16. Let $p > 2$ be a prime number. By Remark 2.22 the exact sequence $1 \to \mathbb{Z}_p^* \to \mathbb{Q}_p^* \xrightarrow{v} \mathbb{Z} \to 0$, where v denotes the valuation map, induces an exact sequence $1 \to \mathbb{Z}_p^* \to \widehat{\mathbb{Q}_p^*} \to \widehat{\mathbb{Z}} \to 0$. Hence, it follows from Remark 4.15 that $\bigwedge^2 \widehat{\mathbb{Q}_p^*}$ is canonically isomorphic to $\mathbb{Z}_p^*$. The canonical isomorphism $\mathbb{Z}_p^* \to \bigwedge^2 \widehat{\mathbb{Q}_p^*}$ is given by $x \mapsto \pi \wedge x$, where π is a prime element of $\mathbb{Q}_p$. △

4.4 An injective morphism $\bigwedge^2 A \to \bigotimes^2 A$

For any (profinite) abelian group A the map $A \times A \to \bigotimes^2 A$, $(x, y) \mapsto x \otimes y - y \otimes x$ induces a morphism $\sigma_A : \bigwedge^2 A \to \bigotimes^2 A$ by the universal property of $\bigwedge^2 A$. In this section we will show that σ_A is injective for all (profinite) abelian groups A.

Lemma 4.17. *Let A_1, A_2 be abelian groups for which $\sigma_{A_1}, \sigma_{A_2}$ are injective morphisms. Then $\sigma_{A_1 \oplus A_2}$ is injective.*

Proof. Via the isomorphism of Lemma 4.14 and the distributive property of the tensor product, the morphism $\sigma_{A_1 \oplus A_2}$ corresponds to the morphism

$$\begin{aligned}\bigwedge^2 A_1 \oplus \bigwedge^2 A_2 \oplus (A_1 \otimes A_2) &\longrightarrow \bigotimes^2 A_1 \oplus \bigotimes^2 A_2 \oplus (A_1 \otimes A_2) \oplus (A_2 \otimes A_1),\\ (x_1 \wedge y_1, x_2 \wedge y_2, z_1 \otimes z_2) &\longmapsto (x_1 \otimes y_1 - y_1 \otimes x_1, x_2 \otimes y_2 - y_2 \otimes x_2, z_1 \otimes z_2, -z_2 \otimes z_1).\end{aligned}$$

From this it is clear that $\sigma_{A_1 \oplus A_2}$ is also injective. □

Lemma 4.18. *Let A be a finitely generated abelian group. Then σ_A is injective.*

Proof. For any cyclic group C we have $\bigwedge^2 C = 0$ and thus in this case σ_C is injective. By the structure theorem on finitely generated abelian groups, A is a finite product of cyclic groups. Now it follows inductively from Lemma 4.17 that σ_A is injective. □

Proposition 4.19. *Let A be an abelian group. Then σ_A is injective.*

Proof. Consider the set I of finitely generated subgroups of A. Then A equals $\lim_{\to N \in I} N$ and thus we have $\bigwedge^2 A = \lim_{\to N \in I} \bigwedge^2 N$ and $\bigotimes^2 A = \lim_{\to N \in I} \bigotimes^2 N$ [2, Ch. 3]. For any $N \in I$ the map $\sigma_N : \bigwedge^2 N \to \bigotimes N$ is injective by Lemma 4.18, hence the direct limit $\sigma_A : \bigwedge^2 A \to \bigotimes^2 A$ of $(\sigma_N)_{N \in I}$ is injective since taking direct limits is exact in any abelian category. □

Proposition 4.20. *Let A be a profinite abelian group. Then σ_A is injective.*

Proof. For each open subgroup $N \subset A$ the morphism $\sigma_{A/N} : \bigwedge^2(A/N) \to (A/N) \otimes (A/N)$ is injective by Lemma 4.19. Moreover, it follows from the universal property of the exterior square that the diagram

$$\begin{tikzcd}\bigwedge^2 A \arrow[r, "\sigma_A"] \arrow[d] & A \otimes A \arrow[d] \\ \bigwedge^2(A/N) \arrow[r, "\sigma_{A/N}"] & A/N \otimes A/N\end{tikzcd}$$

commutes for all open subgroups $N \subset A$. So the inverse limit of the maps $\sigma_{A/N}$ over all open subgroups N in fact equals the map σ_A. Since $\sigma_{A/N}$ is injective for each N and because the inverse limit functor is left exact, it follows that σ_A is injective. □

Remark 4.21. Let R be a commutative ring and let M be an R-module. We can analogously define the R-module morphism

$$\sigma_M : \bigwedge^2 M \to \bigotimes^2 M, \quad x \wedge y \mapsto x \otimes y - y \otimes x,$$

where we take the exterior product and tensor product in the category of R-modules. However, this map σ_M is not injective in all cases. For example, let R be the ring $\mathbb{F}_2[X, Y, Z]$ and consider the R-ideal $I := (X, Y, Z)$. Then in $\bigotimes^2 I$ we have the equalities

$$X \otimes YZ = XY \otimes Z = Y \otimes XZ = YZ \otimes X,$$

and thus we conclude that $\sigma_I(X \wedge YZ) = 0$. Consider the ideal $J := (X^2, Y^2, Z^2)$ of R. The map $I \times I \to R/J$ defined by $(f, g) \mapsto \overline{fg}$ is an alternating R-bilinear map and thus induces a morphism $\bigwedge^2 I \to R/J$ that sends $X \wedge YZ$ to the non-zero element

$\overline{XYZ} \in R/J$. Hence, $X \wedge YZ \neq 0$ and σ_I is not injective. We can turn R into a finite ring with 2^8 elements by replacing it by R/J. △

4.5 Cocycle squares

In this section we will describe the the cocycle square of abelian groups and of profinite abelian groups. For any abelian group A the cocycle square of A will be an abelian group $\bigodot^2 A$ together with a cocycle map $- \odot - : A \times A \to \bigodot^2 A$ such that composition with $- \odot -$ yields a representation $\operatorname{Hom}(\bigodot^2 A, -) \to \mathrm{Z}^2(A, -)$ of the functor that maps an abelian group B to the set $\mathrm{Z}^2(A, B)$ of cocycle maps $A \times A \to B$, where A acts trivially on B. See section 3.1 for the definition of cocycle maps. The profinite cocycle square will have a similar universal property additionally involving the topology. The notation and theorems from section 3.4 are assumed to be known.

Definition 4.22. Let G be an abelian group, written multiplicatively. Let F be the free abelian group on the symbols $g_1 \odot g_2$ where $g_1, g_2 \in G$. Consider the subgroup

$$N := \langle y \odot z - xy \odot z + x \odot yz - x \odot y \mid x, y, z \in G \rangle.$$

Then we define the *cocycle square* to be the group $\bigodot^2 G := F/N$ together with the cocycle map

$$- \odot - : G \times G \to \bigodot^2 G, \quad (g_1, g_2) \mapsto g_1 \odot g_2.$$

△

Lemma 4.23. *Let G, A be abelian groups. Then for all cocycle maps $G \times G \to A$ there exists a unique group homomorphism $\bigodot^2 G \to A$ such that the following diagram commutes.*

$$\begin{tikzcd}
\bigodot^2 G \arrow[r, dashed, "\exists!"] & A \\
G \times G \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proof. Uniqueness of the homomorphism follows from the universal property of the free abelian group F on the formal symbols $g_1 \odot g_2$ where $g_1, g_2 \in G$. Now let $c : G \times G \to A$ be a cocycle map. Then there exists a homomorphism $f : F \to A$ such that c equals the composition $G \times G \to F \to A$. The kernel of f contains $\ker(F \to \bigodot^2 G)$ and thus we get a homomorphism $\bigodot^2 G \to A$ that fits the diagram stated in the lemma. □

Lemma 4.24. *Let G, A be abelian groups and let $\omega : G \times G \to A$ be a cocycle. Define $f : G \times G \to A$ by $f(x, y) = \omega(x, y) - \omega(y, x)$ for all $(x, y) \in G \times G$. Then f is bilinear.*

Proof. Let $x, y, z \in G$. Then we have

$$\begin{aligned}
\omega(xy, z) - \omega(x, yz) &= \omega(y, z) - \omega(x, y), \\
\omega(x, yz) - \omega(zx, y) &= \omega(x, z) - \omega(z, y), \\
\omega(zx, y) - \omega(z, xy) &= \omega(x, y) - \omega(z, x).
\end{aligned}$$

Adding these three equations yields

$$\omega(xy, z) - \omega(z, xy) = \omega(y, z) + \omega(x, z) - \omega(z, y) - \omega(z, x),$$

and thus $f(xy, z) = f(y, z) + f(x, z)$. This proves that f is linear in its first argument. Since for all $g, g' \in G$ we have $f(g', g) = -f(g, g')$, it follows that f is also linear in its second argument. □

For any abelian group G consider the natural map $\kappa_G : \bigwedge^2 G \to \bigodot^2 G$ defined by $x \wedge y \mapsto x \odot y - y \odot x$, and notice that this is a homomorphism by Lemma 4.24. The natural composition $\bigwedge^2 G \to \bigodot^2 G \to \bigotimes^2 G$ is injective by Proposition 4.19. Hence, κ_G is injective. We view $\bigwedge^2 G$ as a subgroup of $\bigodot^2 G$ via κ_G. Notice that the natural map $G \times G \to \bigodot^2 G / \bigwedge^2 G$ is a commutative cocycle.

Lemma 4.25. *Let G be an abelian group. Then $G \times G \to \bigodot^2 G / \bigwedge^2 G$ is the initial object in $\mathbf{DCZ^2}(G)$.*

Proof. Denote the map $G \times G \to \bigodot^2 G / \bigwedge^2 G$ by ω. Let A be an abelian group and let $c : G \times G \to A$ be a commutative cocycle. Then c induces a group morphism $\bigodot^2 G \to A$. The composition $\bigwedge^2 G \to \bigodot^2 G \to A$ is the zero map since it induces the trivial cocycle $G \times G \to A$. Hence, we get a homomorphism $\bigodot^2 G / \bigwedge^2 G \to A$ and this is a morphism $\omega \to c$ of commutative cocycles. Now it follows from Lemma 4.23 that there is exactly one morphism $\omega \to c$. □

Denote the natural map $G \to \mathbb{Z}[G]$ by $[-]$. From the theory in section 3.4 it follows that the initial commutative cocycle $G \times G \to \bigodot^2 G / \bigwedge^2 G$ corresponds to a sectioned central extension. The following lemma shows that the corresponding extension is $\mathbb{Z}[G] \to G, [x] \mapsto x$ with section $[x] \mapsfrom x$.

Lemma 4.26. *Let G be an abelian group. The initial object in $\mathbf{DCZ^E}(G)$ is the sectioned central extension $\mathbb{Z}[G] \to G$.*

Proof. Consider a central extension $\pi : E \to G$ with a section $s : E \leftarrow G$. By the universal property of $\mathbb{Z}[G]$ as a free abelian group, there is a unique morphism $\psi : \mathbb{Z}[G] \to E$ of groups such that for any $g \in G$ we have $\psi([g]) = s(g)$. Hence, there is at most one morphism in $\mathrm{Hom}_{\mathbf{DCZ^E}(G)}(\mathbb{Z}[G], E)$ and it remains to verify that ψ makes the diagram

$$\begin{tikzcd}
\mathbb{Z}[G] \arrow[r] \arrow[d, "\psi"] & G \\
E \arrow[ur, "\pi"] &
\end{tikzcd}$$

commute, where $\mathbb{Z}[G] \to G$ is the natural morphism of groups. This follows from the universal property of $\mathbb{Z}[G]$ as a free abelian group since $[-] : G \to \mathbb{Z}[G]$ is a section of both $\pi \circ \psi$ and of the natural map $\mathbb{Z}[G] \to G$. □

The following proposition tells us more about the structure of $\bigodot^2 G$ for an abelian group G.

Proposition 4.27. *Let G be an abelian group. Then there is an exact sequence*

$$0 \to \bigwedge^{2} G \to \bigodot^{2} G \to \mathbb{Z}[G] \to G \to 0$$

where the third and fourth morphisms are respectively defined by

$$x \odot y \mapsto [x] + [y] - [xy], \qquad [x] \mapsto x.$$

Proof. By Lemma 4.25 and Lemma 4.26 it follows that in the isomorphism of categories $\mathbf{DCZ^2}(G) \cong \mathbf{DCZ^E}(G)$ from section 3.4 the commutative cocycle $G \times G \to \bigodot^2 G / \bigwedge^2 G$ corresponds to the commutative sectioned central extension $\mathbb{Z}[G] \to G$. Hence, we get the exact sequence

$$0 \to \bigodot^{2} G / \bigwedge^{2} G \to \mathbb{Z}[G] \to G \to 0.$$

It can be verified that the corresponding maps are as stated in the proposition. □

Corollary 4.28. *Let G be an abelian group. Then the group morphism $\bigwedge^2 G \to \bigodot^2 G$, given by $x \wedge y \mapsto x \odot y - y \odot x$ has a group-theoretic retraction.*

Proof. Propositition 4.27 gives an exact sequence

$$0 \to \bigwedge^{2} G \to \bigodot^{2} G \to \ker(\mathbb{Z}[G] \to G) \to 0.$$

Since $\ker(\mathbb{Z}[G] \to G)$ is free, we conclude that the short exact sequence splits. Hence, we get the desired result. □

We also need a profinite cocycle square. Unfortunately, the cocycle square of finite groups that we have constructed cannot always be equipped with a topology that turns it into a profinite group. For example, by Proposition 4.27 we conclude that for a cyclic group C_n of order n we have $\bigodot^2 C_n \cong \mathbb{Z}^n$.

Recall that for any group G we denote by $\widehat{G}$ the profinite completion $\lim_{\leftarrow N} G/N$ where N ranges over the normal subgroups of G of finite index. We first consider the finite case of the profinite cocycle square. We use the finite case to define the profinite cocycle square for all profinite abelian groups in Definition 4.31.

Definition 4.29. Let G be a finite profinite group. Let G_{grp} be the underlying group of G. We define the *cocycle square of* G to be $\bigodot^2 G := \widehat{\bigodot^2 G_{\mathrm{grp}}}$, together with the natural cocycle map $G \times G \to \bigodot^2 G$ that equals the composition

$$G \times G \to \bigodot^{2} G_{\mathrm{grp}} \to \bigodot^{2} G. \qquad \triangle$$

Note that the natural map $- \odot - : G \times G \to \bigodot^2 G$ is a continuous cocycle map.

Lemma 4.30. *Let G, A be finite profinite abelian groups. Then for all cocycle maps $G \times G \to A$ there exists a unique morphism $\bigodot^2 G \to A$ of profinite groups such that the following diagram commutes.*

$$\begin{tikzcd}
\bigodot^2 G \arrow[r, dashed, "\exists!"] & A \\
G \times G \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proof. Uniqueness of the map follows from the fact that the image of the map $G \times G \to \bigodot^2 G$ topologically generates $\bigodot^2 G$. Let G_{grp} be the underlying group of G. Let ω be a cocycle map $G \times G \to A$ and consider the induced homomorphism $f : \bigodot^2 G_{\mathrm{grp}} \to A$. Then the map $\bigodot^2 G_{\mathrm{grp}} \to A$ yields a group homomorphism $(\bigodot^2 G_{\mathrm{grp}})/\ker f \to A$. Since $\ker f$ is of finite index in $\bigodot^2 G_{\mathrm{grp}}$, we now get a morphism of profinite groups $h : \bigodot^2 G \to A$. It is not hard to verify that $h[-,-] = \omega$. □

Now we can give the definition of the profinite cocycle square for all profinite abelian groups.

Definition 4.31. Let G be a profinite abelian group. We define the *cocycle square of G* to be $\lim_{\leftarrow N} \bigodot^2(G/N)$, together with the inverse limit $- \odot - : G \times G \to \bigodot^2 G$ of the continuous cocycle maps $G/N \times G/N \to \bigodot^2(G/N)$, where N ranges over the open normal subgroups of G and $\bigodot^2(G/N)$ is the profinite cocycle square of G/N in both cases. △

Again, note that the natural map $- \odot - : G \times G \to \bigodot^2 G$ is a continuous cocycle map.

Lemma 4.32. *Let G, A be profinite abelian groups. Then for all continuous cocycle maps $G \times G \to A$ there exists a unique morphism $G \times G \to A$ of profinite groups such that the following diagram commutes.*

$$\begin{tikzcd}
\bigodot^2 G \arrow[r, dashed, "\exists!"] & A \\
G \times G \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proof. The proof of this lemma is very similar to the proof of the universal property for the profinite tensor product (Lemma 4.5). □

Corollary 4.33. *Let G, A be profinite abelian groups. Then the universal property of the cocycle square induces an isomorphism $\mathrm{Z}^2(G, A) \cong \operatorname{Hom}(\bigodot^2 G, A)$ of groups.*

Let G be a profinite abelian group. Then $G \times G \to \bigodot^2 G$ defined by $(x, y) \mapsto x \odot y - y \odot x$ is a continuous map, and it is alternating by Lemma 4.24. Hence, it induces a natural morphism $\kappa_G : \bigwedge^2 G \to \bigodot^2 G$ of profinite groups. Composing κ_G with the natural morphism $\bigodot^2 G \to \bigotimes^2 G$ is injective by Proposition 4.20, and thus we conclude that κ_G is injective. We can now view $\bigwedge^2 G$ as a closed subgroup of $\bigodot^2 G$ via κ_G due to Lemma 2.10.

Lemma 4.34. *Let G be an abelian group. Then $G \times G \to \bigodot^2 G / \bigwedge^2 G$ is the initial object in $\mathbf{PCZ^2}(G)$.*

Proof. This proof is completely similar to the proof of Lemma 4.25. □

Let R be a profinite commutative ring. For any profinite group A we write $R[[A]]$ for the profinite R-algebra $R = \lim_{\leftarrow} R[A/N]$ where N ranges over the open subgroups of A. The inverse limit of the maps $R[A/N] \to A/N, [x] \mapsto x$ gives a natural morphism $R[[A]] \to A$ of profinite abelian groups.

The universal profinite commutative cocycle $G \times G \to \bigodot^2 G / \bigwedge^2 G$ corresponds to a profinite sectioned central extension, by the theory in section 3.4. The following lemma shows that the corresponding extension is $\widehat{\mathbb{Z}}[[G]] \to G$, with a section $[-]$ that is the inverse limit of the maps $G/N \to \widehat{\mathbb{Z}}[G/N],\ x \mapsto [x]$.

Lemma 4.35. *Let G, A be profinite abelian groups. Then for all continuous maps $G \to A$ there exists a unique morphism $\widehat{\mathbb{Z}}[[G]] \to A$ of profinite groups such that the diagram*

$$\begin{tikzcd}
\widehat{\mathbb{Z}}[[G]] \arrow[r, dashed, "\exists!"] & A \\
G \arrow[u] \arrow[ur] &
\end{tikzcd}$$

commutes.

Proof. We prove (i) uniqueness and (ii) existence.

(i) Suppose that f_1, f_2 are morphisms $\widehat{\mathbb{Z}}[[G]] \to A$ that fit the diagram. Then for any open normal subgroup $M \subset G$, the set $\ker(f_1 - f_2)$ is mapped surjectively to $\widehat{\mathbb{Z}}[G/M]$ by the map $\widehat{\mathbb{Z}}[[G]] \to \widehat{\mathbb{Z}}[G/M]$, as can be seen by using Lemma 2.13. Applying Lemma 2.13 again yields $\ker(f_1 - f_2) = \lim_{\leftarrow} \widehat{\mathbb{Z}}[G/N]$ and thus $f_1 = f_2$.

(ii) If G and A are both finite, then the result follows from Lemma 2.20 and Lemma 4.1. Now we consider the case that only A is finite. Let $G \to A$ be a continuous map. Then $G \to A$ factors through G/M for some open subgroup $M \subset G$. The map $G/M \to A$ now induces a morphism $\widehat{\mathbb{Z}}[G/M] \to A$ and this yields a morphism $\widehat{\mathbb{Z}}[[G]] \to A$ that fits the diagram. If A is not finite, then for any open subgroup $M \subset A$ the composition $G \to A \to A/M$ induces a morphism $\widehat{\mathbb{Z}}[[G]] \to A/M$. These morphisms are compatible when M varies, and thus they induce a morphism $\widehat{\mathbb{Z}}[[G]] \to A$ that fits the diagram. □

Lemma 4.36. *Let G be a profinite group. Then the extension $\widehat{\mathbb{Z}}[[G]] \to G$ with section $x \mapsto [x]$ is the initial object in $\mathbf{PCZ^E}(G)$.*

Proof. This can be similarly proved as Lemma 4.26 but this time by relying on Lemma 4.35. □

Proposition 4.37. *Let G be a profinite abelian group. Then there is an exact sequence*

$$0 \to \bigwedge^2 G \to \bigodot^2 G \to \widehat{\mathbb{Z}}[[G]] \to G \to 0$$

where the third and fourth morphisms are respectively defined by

$$x \odot y \mapsto [x] + [y] - [xy], \qquad [x] \mapsto x.$$

Proof. This follows from Lemma 4.34 and Lemma 4.36, analogously to the proof of Proposition 4.27. □

Corollary 4.38. *Let G be a profinite abelian group. Then the morphism $\bigwedge^2 G \to \bigodot^2 G, x \wedge y \mapsto x \odot y - y \odot x$ has a retraction of profinite groups.*

Proof. By Lemma 4.37 we get a short exact sequence

$$0 \to \bigwedge^2 G \to \bigodot^2 G \to \ker(\widehat{\mathbb{Z}}[[G]] \to \widehat{\mathbb{Z}}) \to 0.$$

Since $\lim_{\leftarrow} \widehat{\mathbb{Z}}[G/N]$ is projective by Corollary 2.34, we get the desired result. □

4.6 Restricted products

In this section we will define restricted products. The aim of this section is to show that $\mathrm{Ext}^1(\prod_i G_i, A)$ is naturally isomorphic to the restricted product $\prod'_i \mathrm{Ext}^1(G_i, A)$ for any profinite abelian groups $(G_i)_i$ and A.

Definition 4.39. Let $(F_i)_{i \in I}$ be a collection of covariant functors $\mathbf{PAb} \to \mathbf{Ab}$ indexed by a set I. For any open subgroup N of a profinite abelian group A with quotient map $\pi_{A,N} : A \to A/N$, we consider the homomorphism

$$\widetilde{\pi_{A,N}} : \prod_i F_i(A) \to \prod_i F_i(A/N), \; (x_i)_i \mapsto (F_i(\pi_{A,N})(x_i))_i.$$

We now define the *restricted product of* $(F_i)_i$ as the functor $\prod'_i F_i : \mathbf{PAb} \to \mathbf{Ab}$ for which

$$\prod_i{}' F_i(A) = \bigcap_N \widetilde{\pi_{A,N}}^{-1}(\bigoplus_i F_i(A/N)), \quad \text{for any } A \in \mathrm{Ob}(\mathbf{PAb}),$$
$$\prod_i{}' F_i(f) = ((x_i)_i \mapsto (F_i(f)(x_i))_i), \quad \text{for any } f \in \mathrm{Hom}(\mathbf{PAb}),$$

where we take $\bigoplus_i F_i(A/N) \subset \prod_i F_i(A/N)$ via the natural inclusion. △

In the definition above, we sometimes write $\prod'_i(F_i(A))$ instead of $(\prod'_i F_i)(A)$ when the meaning is clear from context. Notice that the natural inclusions $\prod'_i F_i(A) \to \prod_i F_i(A)$ yield a natural transformation $\prod'_i F_i \to \prod_i F_i$. Moreover, any collection of natural transformations $(\eta_i : F_i \to G_i)_i$ of functors $\mathbf{PAb} \to \mathbf{Ab}$, induces a natural transformation $\prod'_i F_i \to \prod'_i G_i$ by componentwise application of the transformations η_i. Hence, for any index set I, we see that the restricted product is a functor $\prod' : \mathrm{Fun}(\mathbf{PAb}, \mathbf{Ab})^I \to \mathrm{Fun}(\mathbf{PAb}, \mathbf{Ab})$.

Lemma 4.40. *The restricted product functor* $\prod' : \mathrm{Fun}(\mathbf{PAb}, \mathbf{Ab})^I \to \mathrm{Fun}(\mathbf{PAb}, \mathbf{Ab})$ *is left exact for any index set* I*.*

Proof. Let $(0 \to E_i \xrightarrow{f_i} F_i \xrightarrow{h_i} H_i)_i$ be a collection of exact sequence of functors $\mathbf{PAb} \to \mathbf{Ab}$ indexed by a set I. Let $0 \to E \xrightarrow{f} F \xrightarrow{h} H$ be the restricted product of this exact sequence. Then exactness at E is clear. Let A be a profinite abelian group. Then $\mathrm{im}\, f(A) \subset \ker h(A)$ is easily verified. It is left to prove that $\ker h(A) \subset \mathrm{im}\, f(A)$. Let $(x_i)_i \in \ker h(A)$. Then for any i we have $x_i \in \ker h_i(A) = \mathrm{im}\, f_i(A)$, and we choose $e_i \in E_i(A)$ to be such that $f_i(A)(e_i) = x_i$. For any finite quotient $q : A \to A/N$ of A we have $F_i(q)(x_i) = 0$ for allmost all i, and it follows from the commutative diagram

$$\begin{tikzcd}
E_i(A) \arrow[r, tail, "f_i(A)"] \arrow[d, "E_i(q)"] & F_i(A) \arrow[d, "F_i(q)"] \\
E_i(A/N) \arrow[r, tail, "f_i(A/N)"] & F_i(A/N)
\end{tikzcd}$$

that $E_i(q)(e_i) = 0$ for almost all i. Hence, we have $(e_i)_i \in E$ and this element is mapped to $(x_i)_i$ by $f(A)$. □

We say that a functor $F : \mathbf{PAb} \to \mathbf{Ab}$ *preserves products of finite groups* if for any product $\prod_i A_i$ of finite discrete abelian groups with projection maps $\pi_j : \prod_i A_i \to A_j$ the map

$$(F(\pi_i))_i : F(\prod_i A_i) \to \prod_i F(A_i)$$

is an isomorphism. If the map $(F(\pi_i))_i : F(\prod_i A_i) \to \prod_i (A_i)$ is an isomorphism for all collections $(A_i)_i$ of profinite abelian groups, then we simply say that F *preserves products.* The functors that preserve products (of finite groups) together with the natural transformations form an abelian category.

Lemma 4.41. *Let* $(F_i)_i$ *be a collection of functors* $\mathbf{PAb} \to \mathbf{Ab}$ *that preserves products of finite groups. Then* $\prod'_i F_i$ *preserves products of finite groups.*

Proof. Let $(A_j)_{j \in J}$ be a collection of finite discrete abelian groups. Write $F := \prod'_i F_i$. For any $j \in J$, let $\pi_j : \prod_i A_i \to A_j$ be the projection map, and consider the map

$$\widetilde{\pi_j} : \prod_i F_i(A) \to \prod_i F_i(A_j), \quad (x_i)_i \mapsto (F_i(\pi_j)(x_i))_i.$$

The set of finite intersections of kernels $\ker(A \to A_j)$ is cofinal in the set of all open subgroups of A. Hence, we have

$$F(A) = \bigcap_j \widetilde{\pi_j}^{-1} \bigoplus_i F_i(A_j) = \bigcap_j \widetilde{\pi_j}^{-1} F(A_j). \tag{1}$$

Moreover, since each F_i preserves products we have an isomorphism

$$\prod_i F_i(A) \to \prod_j \prod_i F_i(A_j), \qquad x \mapsto (\widetilde{\pi_j}(x))_j$$

and the restriction to $F(A)$ induces by equation (1) the isomorphism

$$F(A) \xrightarrow{\sim} \prod_j F(A_j), \quad x \mapsto (F(\pi_j)(x))_j. \qquad \square$$

Proposition 4.42. *Let $(0 \to E_i \to F_i \to H_i \to 0)_i$ be a collection of exact sequences of functors* **PAb** $\to$ **Ab** *indexed by a set I. Suppose that F_i and H_i preserve products of finite groups for all i. Let A be a product of finite discrete abelian groups. Then the induced sequence*

$$0 \to \prod_i{}' E_i(A) \to \prod_i{}' F_i(A) \to \prod_i{}' H_i(A) \to 0$$

is exact.

Proof. For any i, let h_i be the natural transformation $F_i \to H_i$, and let $h : F \to H$ be the restricted product of the collection $(F_i \overset{h_i}{\to} H_i)_i$. Since restricted products are left exact functors by Lemma 4.40, it is left to prove that $h(A)$ is surjective. Write $A = \prod_j A_j$ with each A_j a finite discrete abelian group, and for any j let $\pi_j : A \to A_j$ be the projection map. Then by naturality of h the diagram

$$\begin{tikzcd}
F(A) \arrow[r, "h(A)"] \arrow[d, "(F(\pi_j))_j"', "\wr"] & H(A) \arrow[d, "(H(\pi_j))_j"', "\wr"] \\
\prod_j F(A_j) \arrow[r, two heads, "(h(A_j))_j"] & \prod_j H(A_j)
\end{tikzcd}$$

commutes. The vertical arrows are isomorphisms by Lemma 4.41, and the bottom horizontal arrow is surjective by finiteness of all A_j and by surjectivity of $(F_i)_i \to (H_i)_i$. It follows that $h(A)$ is surjective. $\square$

Lemma 4.43. *Let G be a profinite abelian group. Then the functors* $\mathrm{Ext}^1(G, -)$*,* $\mathrm{H}^2(G, -)$*,* $\mathrm{Z}^2(G, -)$ *and* $\mathrm{Hom}(G, -)$ *preserve products.*

Proof. It is clear that $\mathrm{Hom}(G, -)$ preserves products: this follows from the universal property of products. Similarly it follows that $\mathrm{Z}^2(G, -)$ preserves products. For any product $\prod_i A_i$ of profinite abelian groups, the isomorphism $\mathrm{Z}^2(G, \prod_i A_i) \overset{\sim}{\longleftrightarrow} \prod_i \mathrm{Z}^2(G, A_i)$ maps (collections of) commutative cocycles to (collections of) commutative cocycles, and maps (collections of) coboundaries to (collections of) coboundaries. It follows that $\mathrm{Ext}^1(G, -)$ and $\mathrm{H}^2(G, -)$ also preserve products. $\square$

Lemma 4.44. *Let $(G_i)_i$, G and A be profinite abelian groups. Let $(f_i : G_i \to G)_i$ be a collection of morphisms of profinite groups such that $f_i \to 0$ (cf. section 4.1). Then the image of the morphisms*

$$(\operatorname{Hom}(f_i, A))_i : \operatorname{Hom}(G, A) \to \prod_i \operatorname{Hom}(G_i, A),$$
$$(\operatorname{Ext}^1(f_i, A))_i : \operatorname{Ext}^1(G, A) \to \prod_i \operatorname{Ext}^1(G_i, A),$$
$$(\mathrm{H}^2(f_i, A))_i : \mathrm{H}^2(G, A) \to \prod_i \mathrm{H}^2(G_i, A)$$

is contained in

$$\prod_i{}' \operatorname{Hom}(G_i, A), \quad \prod_i{}' \operatorname{Ext}^1(G_i, A), \quad \prod_i{}' \mathrm{H}^2(G_i, A)$$

respectively.

Proof. For Hom this follows from the fact that for any $\varphi \in \operatorname{Hom}(G, A)$ and any finite quotient $q : A \to A/N$ the composition $G \to A \to A/N$ factors through a finite quotient of G. The analogous result similarly follows for $(\mathrm{Z}^2(f_i, A))_i$ and this also proves the result for Ext^1 and H^2 by describing the corresponding maps in terms of cocycle classes. □

Theorem 4.45. *Let $(G_i)_{i\in I}$ and A be profinite abelian groups and suppose that A is the product of finite discrete groups. For every $j \in I$, consider the natural inclusion $\iota_j : G_j \hookrightarrow \prod_i G_i$. Then the map*

$$\operatorname{Ext}^1(\prod_i G_i, A) \to \prod_i{}' \operatorname{Ext}^1(G_i, A), \quad x \mapsto (\operatorname{Ext}^1(\iota_i, A)(x))_i$$

is an isomorphism of abelian groups. This isomorphism is natural in all G_i's and in A.

Proof. The map $\operatorname{Ext}^1(\prod_i G_i, A) \to \prod_i' \operatorname{Ext}^1(G_i, A)$ is well-defined due to Lemma 4.44. For every $i \in I$, let $0 \to K_i \to \widehat{\mathbb{Z}}^{J_i} \to G_i \to 0$ be a projective resolution, which is possible by Corollary 2.33. Write $G := \prod_i G_i$, $J := \bigsqcup_i J_i$ and $K := \prod_i K_i$, and notice that for every $i \in I$ the natural inclusions give a morphism

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] & \widehat{\mathbb{Z}}^J \arrow[r] & G \arrow[r] & 0 \\
0 \arrow[r] & K_i \arrow[r] \arrow[u] & \widehat{\mathbb{Z}}^{J_i} \arrow[r] \arrow[u] & G_i \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

of short exact sequences. Hence, for every $i \in I$ we get the following commutative diagram.

$$\begin{tikzcd}
\operatorname{Hom}(K, A) \arrow[r, "\delta"] \arrow[d] & \operatorname{Ext}^1(G, A) \arrow[d] \\
\operatorname{Hom}(K_i, A) \arrow[r, "\delta"] & \operatorname{Ext}^1(G_i, A)
\end{tikzcd}$$

Taking restricted products, we obtain a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}(\widehat{\mathbb{Z}}^J, A) \arrow[r] \arrow[d, "\wr"] & \operatorname{Hom}(K, A) \arrow[r, "\delta"] \arrow[d, "\wr"] & \operatorname{Ext}^1(G, A) \arrow[r] \arrow[d] & 0 \\
\prod'_i \operatorname{Hom}(\widehat{\mathbb{Z}}^{J_i}, A) \arrow[r] & \prod'_i \operatorname{Hom}(K_i, A) \arrow[r, "(\delta)_i"] & \prod'_i \operatorname{Ext}^1(G_i, A) \arrow[r] & 0
\end{tikzcd}$$

by applying the long exact sequences of Ext. Indeed, the last objects of the rows are 0 because $\mathrm{Ext}^1(P, B) = 0$ whenever P is projective. Moreover, the two leftmost vertical arrows are group isomorphisms due to Lemma 4.1. The top row is clearly exact, and the bottom row is exact by Proposition 4.42 and Lemma 4.43. Now bijectivity of the map $\mathrm{Ext}^1(G, A) \to \prod_i' \mathrm{Ext}^1(G_i, A)$ is clear. The desired naturality follows from the fact that Ext^1 is a bifunctor. □

5 A split exact sequence

In this chapter we will show that for any abelian groups G, A we have got a split exact sequence

$$0 \to \mathrm{Ext}^1(G, A) \to \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A) \to 0,$$

where the action of G on A is trivial. This is an exercise by K.S. Brown in [3, Ch. 5.6]. We will also show a similar statement for profinite abelian groups.

5.1 Commutator pairing

In this section we describe a natural homomorphism $\mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$, where G and A are (profinite) abelian groups and G acts trivially on A. For abelian groups G and A we say that a map $f : G \times G \to A$ is *alternating* if it is bilinear and for all $g \in G$ we have $f(g, g) = 0$. By the theory in section 3.4, we identify $\mathrm{H}^2(G, A)$ with $\mathrm{H}^{\mathrm{E}}(G, A)$.

Consider an exact sequence

$$0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 0$$

of (profinite) groups where E is a central extension of G by A and where G is abelian. Then by Lemma 2.27 we have that E is of class 2, and the (continuous) commutator map $E \times E \to E^{(2)}$ is bilinear. Since G is abelian, we have $E^{(2)} \subset \iota[A]$ and get an induced (continuous) commutator map $c : E \times E \to A$. From $\iota[A] \subset \mathrm{Z}(E)$ it follows that c factors over the map $(\pi, \pi) : E \times E \to G \times G$, and the induced commutator map $G \times G \to A$ is continuous because the map $E \times E \to G \times G$ is open and surjective. It is clear that this commutator map is alternating. Hence, we get an induced morphism $[-, -] : \bigwedge^2 G \to A$ of (profinite) groups and it maps $g_1 \wedge g_2$ to $\iota^{-1}[e_1, e_2]$ where $\pi(e_i) = g_i$ for $i = 1, 2$. It is not hard to verify that this map $[-, -]$ depends only on the isomorphism class of the central extension. By the theory from section 3.4, we get a map $\mathrm{cp}(G, A) : \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$ called the *commutator pairing* that maps every central extension to such a commutator map. When it is clear from context what is meant, we simply write cp instead of $\mathrm{cp}(G, A)$.

In order to prove that $\mathrm{cp}(G, A)$ is a homomorphism, we translate $\mathrm{H}^2(G, A)$ and the map in terms of cocycles classes with the theory from section 3.4. Let $\omega : G \times G \to A$ be a cocycle. Then the cocycle class $[\omega] \in \mathrm{H}^2(G, A)$ corresponds to the central extension $0 \to A \to A \times_\omega G \to G \to 0$. It follows that the map $\mathrm{cp}(G, A)$ sends $[\omega]$ to the element of $\mathrm{Hom}(\bigwedge^2 G, A)$ defined by $[g_1 \wedge g_2 \mapsto \omega(g_1, g_2) - \omega(g_2, g_1)]$. This map is clearly a homomorphism.

5.2 Section of $\mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$

In this section we will prove that the homomorphism $\mathrm{cp} : \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$ has a group section in the case that A, G are abelian groups. This result is an exercise in

[3, Ch 5.6]. We will also show that for profinite abelian groups A, G the homomorphism $\mathrm{cp} : \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$ has a group section. The notation and theory of section 4.5 will be considered as known.

Proposition 5.1. *Let A, G be (profinite) abelian groups. Then the commutator pairing $\mathrm{cp}(G, A) : \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$ has a section that is natural in A.*

Proof. Let $\kappa_G : \bigwedge^2 G \to \bigodot^2 G$ defined by $x \wedge y \mapsto x \odot y - y \odot x$ be the injective homomorphism as in section 4.5. Denote by Φ the corresponding natural transformation $\mathrm{Hom}(\kappa_G, -)$ of $\mathrm{Hom}(\bigodot^2 G, -)$ to $\mathrm{Hom}(\bigwedge^2 G, -)$, and write $\Phi_B := \Phi(B)$ for any (profinite) abelian group B. Any (profinite) abelian group B gives a diagram

$$\begin{tikzcd}
\mathrm{Z}^2(G, B) \arrow[d] & \mathrm{Hom}(\bigodot^2 G, B) \arrow[l, "\sim"'] \arrow[d, "\Phi_B"] \\
\mathrm{H}^2(G, B) \arrow[r, "\mathrm{cp}"] & \mathrm{Hom}(\bigwedge^2 G, B)
\end{tikzcd}$$

and its commutativity can be verified by using the theory from section 5.1. Let $u := \Phi_{\bigodot^2 G}(\mathrm{id}_{\bigodot^2 G})$, i.e., u sends an element $x \wedge y$ to $x \odot y - y \odot x$. Then for any (profinite) abelian group B and any $f : \bigodot^2 G \to B$ we have $\Phi_B(f) = f \circ u$, which can either be seen by Yoneda's Lemma, or by a direct calculation. By Corollary 4.28 or Corollary 4.38 there exists a morphism $v : \bigodot^2 G \to \bigwedge^2 G$ such that $v \circ u = \mathrm{id}_{\bigwedge^2 G}$. Now the map

$$\mathrm{Hom}(\bigwedge^2 G, B) \to \mathrm{Hom}(\bigodot^2 G, B), \qquad g \mapsto g \circ v$$

is a section of Φ_B, and this results in a section of $\mathrm{H}^2(G, B) \to \mathrm{Hom}(\bigwedge^2 G, B)$ that is natural in B. □

Theorem 5.2. *Let G be (profinite) abelian groups. Then for any (profinite) abelian group A the sequence*

$$0 \to \mathrm{Ext}^1(G, A) \to \mathrm{H}^2(G, A) \overset{\mathrm{cp}}{\to} \mathrm{Hom}(\bigwedge^2 G, A) \to 0$$

is a split exact sequence, where $\mathrm{Ext}^1(G, A) \to \mathrm{H}^2(G, A)$ is the inclusion map. Moreover, we can choose the sections of cp *to be natural in A.*

Proof. It is easy to verify that the sequence is exact at $\mathrm{Ext}^1(G, A)$ and at $\mathrm{H}^2(G, A)$. It now follows from Proposition 5.1 that the sequence is split-exact with a section of cp that is natural in A. □

Corollary 5.3. *Let A, G be (profinite) abelian groups and suppose that G is (pro)cyclic. Then $\mathrm{Ext}^1(G, A) = \mathrm{H}^2(G, A)$.*

Proof. By Lemma 4.13 we have $\bigwedge^2 G = 0$. Hence, the result follows from 5.2. □

5.3 Canonical splitting

In this section we will exhibit a retraction of the map $\mathrm{Ext}^1(G, A) \to \mathrm{H}^2(G, A)$ for profinite abelian groups G, A where $G = \prod_i G_i$ is the product of procyclic groups G_i. This retraction will be natural in all G_i and A, and explicitly given. In order to define this retraction, we reduce G to the procyclic case G_i by using restricted products and relying on Theorem 4.45. The results in this section can be compared with Theorem 5.2, which does give retractions, but these retractions are not explicitly constructed and are not natural in G.

Remark 5.4. Let $(G_i)_{i\in I}$ and A be profinite abelian groups. Suppose that A is the product of finite discrete abelian groups, or, suppose that I is finite. For every j, let $\iota_i : G_j \to \prod_i G_i$ be the natural injection. Then there is a natural homomorphism $(\mathrm{H}^2(\iota_i, A)) : \mathrm{H}^2(\prod_i G_i, A) \to \prod'_i \mathrm{H}^2(G_i, A)$ defined by $x \mapsto (\mathrm{H}^2(\iota_i, A)(x))_i$. This is well-defined by Lemma 4.44. Similarly, we also have a homomorphism

$$\mathrm{Hom}(\bigwedge^2 \prod_i G_i, A) \xrightarrow{(\mathrm{Hom}(\bigwedge^2 \iota_i, A))_i} \prod_i{}' \mathrm{Hom}(\bigwedge^2 G_i, A).$$

The defined maps yield a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ext}^1(\prod_i G_i, A) \arrow[r] \arrow[d, "\wr"', "(\mathrm{Ext}^1(\iota_i,A))_i"] & \mathrm{H}^2(\prod_i G_i, A) \arrow[r] \arrow[d, "(\mathrm{H}^2(\iota_i,A))_i"] & \mathrm{Hom}(\bigwedge^2 \prod_i G_i, A) \arrow[r] \arrow[d, "(\mathrm{Hom}(\bigwedge^2 \iota_i,A))_i"] & 0 \\
0 \arrow[r] & \prod'_i \mathrm{Ext}^1(G_i, A) \arrow[r] & \prod'_i \mathrm{H}^2(G_i, A) \arrow[r] & \prod'_i \mathrm{Hom}(\bigwedge^2 G_i, A) \arrow[r] & 0
\end{tikzcd}$$

and the rows are exact by Theorem 5.2 and, if A is the product of finite discrete groups, Theorem 4.42. The leftmost vertical arrow is an isomorphism due to Theorem 4.45, or, due to the additivity of $\mathrm{Ext}^1(-, A)$. Moreover, the diagram is natural in A and, if the index set I is fixed, also in each G_i. △

Proposition 5.5. *Let $(G_i)_{i\in I}$ be a collection of procyclic groups and let A be a profinite abelian group. Suppose that A is the product of finite discrete groups, or, suppose that I is finite. Then the diagram in Remark 5.4 gives a diagram*

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ext}^1(\prod_i G_i, A) \arrow[r] \arrow[d, "\wr"', "(\mathrm{Ext}^1(\iota_i,A))_i"] & \mathrm{H}^2(\prod_i G_i, A) \arrow[r] \arrow[d, "(\mathrm{H}^2(\iota_i,A))_i"] & \mathrm{Hom}(\bigwedge^2 \prod_i G_i, A) \arrow[r] & 0 \\
0 \arrow[r] & \prod'_i \mathrm{Ext}^1(G_i, A) \arrow[r, "\sim"] & \prod'_i \mathrm{H}^2(G_i, A) \arrow[r] & 0 &
\end{tikzcd}$$

in which the rows are exact. Moreover, the composition

$$\mathrm{H}^2(\prod_i G_i, A) \longrightarrow \prod_i{}' \mathrm{H}^2(G_i, A) \longrightarrow \prod_i{}' \mathrm{Ext}^1(G_i, A) \longrightarrow \mathrm{Ext}^1(\prod_i G_i, A)$$

is a retraction of the map $\mathrm{Ext}^1(\prod_i G_i, A) \to \mathrm{H}^2(\prod_i G_i, A)$. This retraction is natural in A and, if the index set I is fixed, also in each G_i.

Proof. By Lemma 4.13 we have $\prod'_i \mathrm{Hom}(\bigwedge^2 G_i, A) = 0$ and this shows that we get the desired diagram. It follows from the commutativity of the diagram that the composition, as stated in the lemma, is indeed a retraction of the map $\mathrm{Ext}^1(\prod_i G_i, A) \to \mathrm{H}^2(\prod_i G_i, A)$. □

Denote by $\mathrm{ret}((G_i)_i, A)$ the retraction that is given by Proposition 5.5. We thus get a natural isomorphism as stated in the next proposition. Recall from section 5.1 the definition of the map $\mathrm{cp}(G, A) : \mathrm{H}^2(G, A) \to \mathrm{Hom}(\bigwedge^2 G, A)$ for any profinite abelian groups G, A. We sometimes simply write ret instead of $\mathrm{ret}((G_i)_i, A)$ when the meaning of the map is clear from context.

Proposition 5.6. *Let $(G_i)_{i\in I}$ be a collection of procyclic groups and let A be a profinite abelian group. Suppose that A is the product of finite discrete groups, or, suppose that I*

is finite. Then

$$\big(\operatorname{ret}, \operatorname{cp}\big) : \mathrm{H}^2(\prod_i G_i, A) \xrightarrow{\sim} \operatorname{Ext}^1(\prod_i G_i, A) \oplus \operatorname{Hom}(\bigwedge^2 \prod_i G_i, A)$$

is an isomorphism of groups that is natural in A and, if the index set I is fixed, also in each G_i.

The following lemma generalizes the naturality of the retraction maps ret.

Lemma 5.7. *Let $f : G' \to G$ be a morphism of profinite groups, and suppose that $G = \prod_{i \in I} G_i$ and $G' = \prod_{j \in J} G'_j$ are factorizations into procyclic groups. Let A be a profinite abelian group. Suppose that A is the product of finite discrete groups, or, suppose that I and J are finite. Assume that for each $j \in J$ one of the two following conditions holds: G'_j is projective, or, there exists $i \in I$ such that $f[G'_j] \subset G_i$, where we view G_i as a subgroup of G via the natural inclusion map. Then the diagram*

$$\begin{tikzcd}
\mathrm{H}^2(G, A) \arrow[r, "\mathrm{H}^2(f,A)"] \arrow[d, "\operatorname{ret}"] & \mathrm{H}^2(G', A) \arrow[d, "\operatorname{ret}"] \\
\operatorname{Ext}^1(G, A) \arrow[r, "\operatorname{Ext}^1(f,A)"] & \operatorname{Ext}^1(G', A)
\end{tikzcd}$$

commutes.

Proof. Let J' be the subset of J of all j for which G'_j is not projective. By Theorem 4.45 we have $\operatorname{Ext}^1(G', A) \cong \prod_{j \in J} \operatorname{Ext}^1(G'_j, A) = \prod_{j \in J'} \operatorname{Ext}^1(G'_j, A)$. Now the result follows from naturality in each G'_j with $j \in J'$. □

In our applications, most of the groups G_i will be projective, leading to the following practical result.

Proposition 5.8. *Let G, A be profinite abelian groups. Suppose that $C \subset G$ is a procyclic closed subgroup such that G/C is projective and such that G/C is a product of procyclic groups indexed by I. Let $\iota : C \to G$ be the inclusion map. Suppose that A is the product of finite discrete groups, or, suppose that I is finite. Then $\operatorname{Ext}^1(\iota, A)$ and*

$$(\mathrm{H}^2(\iota, A), \operatorname{cp}) : \mathrm{H}^2(G, A) \longrightarrow \operatorname{Ext}^1(C, A) \times \operatorname{Hom}(\bigwedge^2 G, A)$$

are isomorphisms. Moreover, we have $\mathrm{H}^2(\iota, A) = \operatorname{Ext}^1(\iota, A) \circ \operatorname{ret}((G_i)_{i \in I}, A)$ for every factorization $G = \prod_j G_i$ with $0 \in I$ and $C = G_0$ and all G_i procyclic.

Proof. Notice that $\mathrm{H}^2(\iota, A)$ indeed maps to $\operatorname{Ext}^1(C, A)$, since $\mathrm{H}^2(C, A) = \operatorname{Ext}^1(C, A)$ by Corollary 5.3. By assumption we have $G = C \times P$ for some projective subgroup $P \subset G$: the sequence $1 \to C \to G \to G/C \to 1$ splits because G/C is projective. This shows that $\operatorname{Ext}^1(\iota, A)$ is an isomorphism. The remaining statements follow from the commutative diagram

$$\begin{tikzcd}
\operatorname{Ext}^1(G, A) \arrow[r, hook] \arrow[d, "\operatorname{Ext}^1(\iota,A)"', "\wr"] & \mathrm{H}^2(G, A) \arrow[d, "\mathrm{H}^2(\iota,A)"] \\
\operatorname{Ext}^1(C, A) \arrow[r, hook, "\sim"] & \mathrm{H}^2(C, A)
\end{tikzcd}$$

and Proposition 5.6. □

Notice that in the setting of Proposition 5.8 the retraction $\operatorname{ret}((G_i)_{i\in I}, A)$ does not depend on the factorization $G = \prod_i G_i$.

For certain products $G = \prod_i G_i$, the following proposition gives an element ξ of $\mathrm{H}^2(G, \bigwedge^2 G)$ such that $(\operatorname{ret}, \operatorname{cp})\xi = (0, \mathrm{id})$.

Proposition 5.9. *Consider a profinite abelian group $G = \prod_{i\in I} G_i$ with each G_i procyclic and with $(I, <)$ a totally ordered set. Suppose that $\bigwedge^2 G$ is the product of finite discrete groups, or, suppose that I is finite. For every $j \in I$, let $\iota_j : G_j \to G$ be the natural inclusion map. Then the map*

$$\omega : G \times G \to \bigwedge^2 G, \quad ((\alpha_i)_i, (\beta_i)_i) \mapsto \sum_{i<i'} \iota_i(\alpha_i) \wedge \iota_{i'}(\beta_{i'})$$

is a well-defined continuous cocycle such that $(\operatorname{ret}, \operatorname{cp})[\omega] = (0, \mathrm{id})$.

Proof. For all $((\alpha_i)_i, (\beta_i)_i) \in G \times G$, the sum $\sum_{i<i'} \iota_i(\alpha_i) \wedge \iota_{i'}(\beta_{i'})$ is a finite sum in $\bigwedge^2 \prod_i (G_i/N_i)$, where N_i are open subgroups of G_i with $N_i = G_i$ for almost all i. Hence, ω is well-defined and continuous. It can be routinely verified that ω is a cocycle map. In section 5.1 we see that $\operatorname{cp}[\omega] : \bigwedge^2 G \to \bigwedge^2 G$ is given by $x \wedge y \mapsto \omega(x, y) - \omega(y, x) = x \wedge y$. Finally, it is easily verified that for every i and all $x, y \in G_i$ we have $\omega(\iota_i(x), \iota_i(y)) = 0$. Hence, for all i we have $\mathrm{H}^2(\iota_i, \mathrm{id})[\omega] = 0$, and we conclude that $\operatorname{ret}[\omega] = 0$. □

6 Multiplier-free theorems

In this section we will consider the map $[-,-] : \bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$ defined by $\overline{g_1} \wedge \overline{g_2} \mapsto [g_1, g_2]G_3$, for any group G. We will show that the map $[-,-]$ is an isomorphism of groups for a group G that satisfies $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. We prove a similar statement for profinite groups. The proofs of the two statements are similar.

6.1 Multiplier-free theorems

Remark 6.1. We will show that the commutator map

$$[-,-] : \bigwedge^2 G^{\mathrm{ab}} \to [G, G]/G^{(3)}, \quad \overline{g_1} \wedge \overline{g_2} \mapsto \overline{[g_1, g_2]}$$

is well-defined in the case that G is a group or a profinite group. So consider such a G. Then

$$1 \to G^{(2)}/G^{(3)} \to G/G^{(3)} \to G/G^{(2)} \to 1$$

is a central extension. Hence, from section 5.1 it follows that we get a map $\bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$ defined by $\overline{g_1} \wedge \overline{g_2} \mapsto \overline{[g_1, g_2]}$. △

Let G be a (profinite) group and let $f : \bigotimes^2 G^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$ be a (continuous) homomorphism. Then the map $\omega : G \times G \to \mathbb{Q}/\mathbb{Z}$ defined by $(x, y) \mapsto f(\overline{x} \otimes \overline{y})$ is a (continuous) cocycle: for all $x, y, z \in G$ we have

$$\begin{aligned} &\omega(y, z) - \omega(xy, z) + \omega(x, yz) - \omega(x, y) \\ &= f(\overline{y} \otimes \overline{z} - (\overline{x} + \overline{y}) \otimes \overline{z} + \overline{x} \otimes (\overline{y} + \overline{z}) - \overline{x} \otimes \overline{y}) \\ &= f(0) = 0. \end{aligned}$$

Definition 6.2. Let G be a (profinite) group acting trivially on the discrete abelian group

$\mathbb{Q}/\mathbb{Z}$. We define the homomorphisms

$$\begin{aligned}\Theta_G &: \mathrm{Hom}(\bigotimes^2 G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Z}^2(G, \mathbb{Q}/\mathbb{Z}) \quad \text{(without topology)},\\ \Theta_G &: \mathrm{Hom}(\bigotimes^2 G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Z}^2(G, \mathbb{Q}/\mathbb{Z}) \quad \text{(with topology)}\end{aligned}$$

as the maps that send f to the cocycle $(x, y) \mapsto f(\overline{x} \otimes \overline{y})$. We denote by $\overline{\Theta_G}$ the composition of Θ_G with the quotient map $\mathrm{Z}^2(G, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z})$. △

Lemma 6.3. *Let G be a (profinite) group. Let $b : G \to \mathbb{Q}/\mathbb{Z}$ be a (continuous) map and consider the (continuous) cocycle $\omega : G \times G \to \mathbb{Q}/\mathbb{Z}$ defined by $(x, y) \mapsto b(x) + b(y) - b(xy)$. Suppose that $\omega \in \mathrm{im}(\Theta_G)$. Then b has the following properties.*

(i) *We have $b(1) = 0$.*

(ii) *Let $g_1, g_2 \in G$. Then $b(g_1 g_2) - b(g_2 g_1) = b([g_1, g_2])$.*

(iii) *Let $g \in G$ and $c \in G^{(2)}$. Then $b(gc) = b(g) + b(c) = b(cg)$.*

(iv) *We have $b|_{G_3} = 0$.*

Proof. Let $f \in \mathrm{Hom}(\bigotimes^2 G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})$ be a (continuous) morphism such that $\Theta_G(f) = \omega$. Then for all $x, y \in G$ we have

$$f(\overline{x} \otimes \overline{y}) = b(x) + b(y) - b(xy). \tag{2}$$

(i) This follows from applying (2) on $x = y = 1$.

(ii) For all $g_1, g_2 \in G$ we have $0 = f(\overline{[g_1, g_2]} \otimes \overline{g_2 g_1}) = b([g_1, g_2]) + b(g_2 g_1) - b(g_1 g_2)$ by (2).

(iii) For all $g \in G$ and $c \in G^{(2)}$ we have $0 = f(\overline{g} \otimes \overline{c}) = b(g) + b(c) - b(gc)$ by (2) and similarly we have $0 = f(\overline{c} \otimes \overline{g}) = b(c) + b(g) - b(cg)$.

(iv) For each $c \in [G, G]$ and $g \in G$ we have $b([g, c]) = b(gc) - b(cg) = 0$ by (ii) and (iii). By (iii) we see that the restriction of b to $G^{(2)}$ is a (continuous) group homomorphism and we conclude that the kernel contains $G^{(3)}$. □

The following lemma gives an explicit surjective homomorphism from $\mathrm{im}(\overline{\Theta_G}) \subset \mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z})$ to $\mathrm{Hom}(K, \mathbb{Q}/\mathbb{Z})$ for any (profinite) group G. Recall from section 4.4 that $\sigma_G : \bigwedge^2 G^{\mathrm{ab}} \to \bigotimes^2 G^{\mathrm{ab}}$ is the map $x \wedge y \mapsto x \otimes y - y \otimes x$. Recall from section 2.3 that the functor $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$, denoted by $*$, is exact on sequences of abelian groups because $\mathbb{Q}/\mathbb{Z}$ is injective, and that the Pontryagin functor $*$, defined as $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ with $\mathbb{Q}/\mathbb{Z}$ discrete, is exact on sequences of profinite abelian groups by Pontryagin duality.

Lemma 6.4. *Let G be a (profinite) group and let $\iota : K \to \bigwedge^2 G^{\mathrm{ab}}$ be the kernel of the commutator map*

$$[-,-] : \bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}.$$

Consider the homomorphism

$$\psi := (\sigma_{G^{\mathrm{ab}}} \circ \iota)^* = \mathrm{Hom}(\sigma_{G^{\mathrm{ab}}} \circ \iota, \mathbb{Q}/\mathbb{Z}) : \mathrm{Hom}(\bigotimes^2 G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(K, \mathbb{Q}/\mathbb{Z}).$$

Then the map

$$\mathrm{im}\,\overline{\Theta_G} \to \mathrm{Hom}(K, \mathbb{Q}/\mathbb{Z}), \quad \overline{\Theta_G}(f) \mapsto \psi(f)$$

is a well-defined surjective homomorphism.

Proof. First of all, the surjectivity follows from the fact that ψ is injective: ι is injective and $\sigma := \sigma_{G^{\mathrm{ab}}}$ is injective by Proposition 4.19 or Proposition 4.20. Hence, it is left to prove that $\ker \overline{\Theta_G} \subset \ker \psi$, in order to conclude that $\operatorname{im} \overline{\Theta_G} \to \operatorname{Hom}(K, \mathbb{Q}/\mathbb{Z})$ is well-defined. By applying the functor $*$ introduced in section 2.3, we have the following commutative diagram, in which the rows are exact, and for every $f \in \ker \overline{\Theta_G}$ we will construct an element $\widetilde{F} \in (G^{(2)}/G^{(3)})^*$ such that $[-,-]^* \widetilde{F} = \sigma^* f$.

$$\begin{tikzcd}
0 \arrow[r] & (G^{(2)}/G^{(3)})^* \arrow[r, "{[-,-]^*}"] & (\bigwedge^2 G^{\mathrm{ab}})^* \arrow[r, "\iota^*"] & K^* \arrow[r] & 0 \\
0 \arrow[r] & \ker \overline{\Theta_G} \arrow[r, hook] & (\bigotimes^2 G^{\mathrm{ab}})^* \arrow[u, "\sigma^*"] & &
\end{tikzcd}$$

Consider an element $f \in \ker \overline{\Theta_G}$. Then for some (continuous) map $F : G \to \mathbb{Q}/\mathbb{Z}$ we have $f(\overline{x} \otimes \overline{y}) = F(x) + F(y) - F(xy)$ for all $x, y \in G$. Now $-F|_{G^{(2)}}$ is a homomorphism by (ii) of Lemma 6.3. Moreover, $-F|_{G^{(2)}}$ factors over $G^{(2)} \to G^{(2)}/G^{(3)}$ with a (continuous) map $\widetilde{F} : G^{(2)}/G^{(3)} \to \mathbb{Q}/\mathbb{Z}$ by (iv) of Lemma 6.3. Finally, by Lemma 6.3, we have for all $g_1, g_2 \in G$ that

$$\widetilde{F}([g_1, g_2]G_3) = F(g_2 g_1) - F(g_1 g_2) = f(\overline{g_1} \otimes \overline{g_2}) - f(\overline{g_2} \otimes \overline{g_1}) = \sigma^* f(\overline{g_1} \wedge \overline{g_2}).$$

Hence, we have $[-,-]^* \widetilde{F} = \sigma^* f$. This yields

$$\psi(f) = \iota^* \sigma^*(f) = \iota^*[-,-]^*(\widetilde{F}) = 0,$$

and thus $f \in \ker \psi$. □

Theorem 6.5. *Let G be a (profinite) group such that $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$. Then the commutator map*

$$[-,-] : \bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$$

is an isomorphism.

Proof. It is clear that the commutator map is surjective, so by Lemma 2.9 it is left to prove the injectivity of this map. From $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$ it follows that $\overline{\Theta_G}$ is the zero map. Hence, due to Lemma 6.4, we find that $\operatorname{Hom}(K, \mathbb{Q}/\mathbb{Z}) = 0$. We conclude that $K = 0$ by Lemma 2.35. □

Remark 6.6. A different proof of Theorem 6.5 can probably be obtained by means of the inflation-restriction sequence. Let G be a group, and let N be a subgroup of G. Assume that $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$, with G acting trivially on the group $\mathbb{Q}/\mathbb{Z}$. Since $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$, the inflation-restriction sequence yields the sequence

$$0 \to \mathrm{H}^1(G/N, \mathbb{Q}/\mathbb{Z}) \overset{\mathrm{Inf}}{\to} \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \overset{\mathrm{Res}}{\to} \mathrm{H}^1(N, \mathbb{Q}/\mathbb{Z})^{G/N} \overset{\tau}{\to} \mathrm{H}^2(G/N, \mathbb{Q}/\mathbb{Z}) \to 0,$$

and this corresponds to the exact sequence

$$0 \to \operatorname{Hom}(G/N, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}_{G/N}(N, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(G/N, \mathbb{Q}/\mathbb{Z}) \to 0,$$

where $\operatorname{Hom}_{G/N}(N, \mathbb{Q}/\mathbb{Z})$ is the subgroup of $\operatorname{Hom}(N, \mathbb{Q}/\mathbb{Z})$ consisting of all homomorphisms $f \in \operatorname{Hom}(N, \mathbb{Q}/\mathbb{Z})$ satisfying $f(gng^{-1}) = f(n)$ for all $g \in G$ and $n \in N$. We remark that for any group G' the abelian group $\operatorname{Hom}(G', \mathbb{Q}/\mathbb{Z})$ is isomorphic to $\operatorname{Hom}(G'/[G', G'], \mathbb{Q}/\mathbb{Z})$

since $\mathbb{Q}/\mathbb{Z}$ is abelian. By injectivity of $\mathbb{Q}/\mathbb{Z}$, the cokernel of the natural map

$$\mathrm{Hom}(G/(N\cdot[G,G]),\mathbb{Q}/\mathbb{Z})\to\mathrm{Hom}(G/[G,G],\mathbb{Q}/\mathbb{Z})$$

equals $\mathrm{Hom}(N/(N\cap[G,G]),\mathbb{Q}/\mathbb{Z})$ and we have

$$\mathrm{Hom}_{G/N}(N,\mathbb{Q}/\mathbb{Z})=\mathrm{Hom}(N/[G,N],\mathbb{Q}/\mathbb{Z}).$$

Hence, the latter exact sequence yields a short exact sequence

$$0\to\mathrm{Hom}(N/(N\cap[G,G]),\mathbb{Q}/\mathbb{Z})\to\mathrm{Hom}(N/[G,N],\mathbb{Q}/\mathbb{Z})\to\mathrm{H}^2(G/N,\mathbb{Q}/\mathbb{Z})\to 0.$$

It follows that $\mathrm{H}^2(G/N,\mathbb{Q}/\mathbb{Z})=0$ if and only if $N\cap[G,G]=[G,N]$. Now take $N=[G,G]$. Then the map τ thus induces an isomorphism

$$\tau':\mathrm{Hom}(G^{(2)}/G^{(3)},\mathbb{Q}/\mathbb{Z})\xrightarrow{\sim}\mathrm{H}^2(G^{\mathrm{ab}},\mathbb{Q}/\mathbb{Z}).$$

Since $\mathbb{Q}/\mathbb{Z}$ is injective, we have $\mathrm{Ext}^1(G^{\mathrm{ab}},\mathbb{Q}/\mathbb{Z})=0$, hence, the commutator pairing is an isomorphism $\mathrm{cp}:\mathrm{H}^2(G^{\mathrm{ab}},\mathbb{Q}/\mathbb{Z})\xrightarrow{\sim}\mathrm{Hom}(\bigwedge^2 G^{\mathrm{ab}},\mathbb{Q}/\mathbb{Z})$ by Theorem 5.2. The author of this thesis believes that the composition

$$\mathrm{cp}\circ\tau':\mathrm{Hom}(G^{(2)}/G^{(3)},\mathbb{Q}/\mathbb{Z})\to\mathrm{Hom}(\bigwedge^2 G^{\mathrm{ab}},\mathbb{Q}/\mathbb{Z})$$

is the map induced by the commutator map $[-,-]:\bigwedge^2 G^{\mathrm{ab}}\to G^{(2)}/G^{(3)}$, and this would show that this commutator map is an isomorphism. △

7 Maximal class-2 extensions of fields

7.1 Generalities

Throughout this section, let K be a field, and let K^{alg} be an algebraic closure of K. Write $G_K:=\mathrm{Gal}(K^{\mathrm{sep}}/K)$. In this section we will establish auxiliary results in order to determine in the upcoming sections the Galois group of maximal class-2 extensions of $\mathbb{Q}$ and $\mathbb{Q}_p$

Lemma 7.1. *The compositum of a collection of class-2 extensions of K is again a class-2 extension of K.*

Proof. Consider a collection $(L_\alpha)_\alpha$ of class-2 extensions of K. The compositum of Galois field extensions is again Galois and the embedding

$$\mathrm{Gal}(\prod_\alpha L_\alpha/K)\to\prod_\alpha\mathrm{Gal}(L_\alpha/K)$$
$$\sigma\mapsto(\sigma|_{L_\alpha})_\alpha$$

shows that $\mathrm{Gal}(\prod_\alpha L_\alpha/K)$ is a class-2 group by Lemma 2.28. □

Proposition 7.2. *The field K has a unique maximal class-2 field extension inside K^{alg}.*

Proof. The composite of all class-2 field extensions of K in K^{alg} is the unique maximal class-2 field extension in K^{alg}. □

We denote the maximal class-2 field extension of the field K by $K^{\mathrm{cl2}}\subset K^{\mathrm{alg}}$. In the remaining part of this section we write $\Gamma:=\mathrm{Gal}(K^{\mathrm{cl2}}/K)$. Since $\Gamma^{(2)}$ is the smallest closed normal subgroup N of Γ for which Γ/N is abelian, it follows that $\mathrm{Gal}(K^{\mathrm{cl2}}/K^{\mathrm{ab}})=\Gamma^{(2)}$ and $\mathrm{Gal}(K^{\mathrm{ab}}/K)=\Gamma^{\mathrm{ab}}$. Similarly, using the notation from section 2.2, it follows that Γ

equals G_K^{cl2}.

The following result is based on suggestions made by J.T. Tate and the proof can be found in [14]. We let G_K act trivially on the discrete abelian group $\mathbb{Q}/\mathbb{Z}$.

Theorem 7.3. *Suppose that K is a local field or a global field. Then $\mathrm{H}^2(G_K, \mathbb{Q}/\mathbb{Z}) = 0$.*

Proof. By the theorem in [14, Ch. 2.6, Thm. 4] we have $\mathrm{H}^2(G_K, \mathbb{C}^*) = 0$, where $\mathbb{C}^*$ is discrete. This theorem is proven in [14, p. 232-237, Thm. 4] by showing that $\mathrm{H}^2(G_K, \mathbb{Q}/\mathbb{Z}) = 0$. □

Recall from section 6.1 that for any profinite group G we have defined a commutator map $[-,-] : \bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$.

Proposition 7.4. *Suppose that K is a local field or a global field. Then the commutator map*

$$[-,-] : \bigwedge^2 \Gamma^{\mathrm{ab}} \to \Gamma^{(2)}, \quad \overline{x} \wedge \overline{y} \mapsto [x, y]$$

is an isomorphism.

Proof. We have $\mathrm{H}^2(G_K, \mathbb{Q}/\mathbb{Z}) = 0$ by Theorem 7.3. Hence, it follows from Theorem 6.5 that the commutator map $[-,-] : \bigwedge^2 G_K^{\mathrm{ab}} \to G_K^{(2)}/G_K^{(3)}$ is an isomorphism. Since $G_K^{\mathrm{cl2}} = \Gamma$, we have canonical isomorphisms $G_K^{\mathrm{ab}} \cong \Gamma^{\mathrm{ab}}$ and $G_K^{(2)}/G_K^{(3)} \cong \Gamma^{(2)}$, and it now follows that also the commutator map $[-,-] : \bigwedge^2 \Gamma^{\mathrm{ab}} \to \Gamma^{(2)}$ is an isomorphism. □

The exact sequence

$$1 \to \mathrm{Gal}(K^{\mathrm{cl2}}/K^{\mathrm{ab}}) \to \mathrm{Gal}(K^{\mathrm{cl2}}/K) \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to 1$$

corresponds to a central exact sequence

$$1 \to \bigwedge^2 \Gamma^{\mathrm{ab}} \to \Gamma \to \Gamma^{\mathrm{ab}} \to 1,$$

which represents an element $[\Gamma]$ in $\mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}})$. Recall that by Theorem 5.2 the sequence

$$0 \to \mathrm{Ext}^1(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}}) \to \mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}}) \overset{\mathrm{cp}}{\to} \mathrm{End}(\bigwedge^2 \Gamma^{\mathrm{ab}}) \to 0 \qquad (3)$$

is split exact, and one can verify that $[\Gamma] \in \mathrm{H}^2(\Gamma^{\mathrm{ab}}, \bigwedge^2 \Gamma^{\mathrm{ab}})$ is mapped to id $\in \mathrm{End}(\bigwedge^2 \Gamma^{\mathrm{ab}})$ by cp.

7.2 Maximal class-2 tamely ramified extensions of local number fields

Let p be a prime number. Let $\mathbb{Q}_p \subset K$ be a finite field extension and let K^{alg} be an algebraic closure of K. Let k be the residue field of K and let k^{alg} be the residue class field of K^{alg}. Write $q := \#k$. Let K^{tr} be the maximal tamely ramified extension of K inside K^{alg}. Write $\Delta := \mathrm{Gal}(K^{\mathrm{tr}}/K)$. Let π_K be a prime element of K. For every $n \in \mathbb{Z}_{>0} \backslash p\mathbb{Z}$ write $K_n := K(\sqrt[n]{\pi_K})$ where $\sqrt[n]{\pi_K} = \{x \in K^{\mathrm{alg}} : x^n = \pi_K\}$. Then $K^{\mathrm{tr}} = \bigcup_{n : p \nmid n} K_n$. For every $n \in \mathbb{Z}_{>0} \backslash p\mathbb{Z}$ we write $\mu_n \subset k^{\mathrm{alg}}$ for the set of zeroes of $X^n - 1$, and notice that the canonical map $K^{\mathrm{alg}} \to k^{\mathrm{alg}}$ maps the group of n^{th} roots of unity in K^{alg} isomorphically to μ_n. For any positive integers $m \mid n$ taking $(n/m)^{\mathrm{th}}$ powers yields a map $\mu_n \to \mu_m$. The inverse limit $\widehat{\mu} := \lim_{\leftarrow n} \mu_n$ with n ranging over all positive integers coprime to p, is the *Tate-module in characteristic p*. For every $\zeta = (\zeta_n)_n \in \widehat{\mu}$ and every $\sigma \in \Delta$ we write $\sigma(\zeta) = (\sigma(\zeta_n))_n$ and notice that this defines an action of Δ on $\widehat{\mu}$. We denote by $K^{\mathrm{unr}} \subset K^{\mathrm{tr}}$ the maximal unramified extension of K inside K^{alg}.

The following result follows from [16, Ch. 4, Cor. 1].

Lemma 7.5. *Let $K \subset L$ be a totally and tamely ramified Galois field extension of finite degree. Let ℓ be the residue field of L, and let $\mathfrak{m}_L$ be the maximal ideal of the valuation ring of L. Let π_L be a prime element of L. Then* $\mathrm{Gal}(L/K)$ *is cyclic and*

$$\mathrm{Gal}(L/K) \to \ell^*, \quad \sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L} \mod \mathfrak{m}_L$$

is an injective group homomorphism that does not depend on the choice of π_L.

Lemma 7.6. *For every $n \in \mathbb{Z}_{>0} \backslash p\mathbb{Z}$, let π_n be a prime element of K_n. Let $\mathfrak{m}_n$ be the maximal ideal of the valuation ring of K_n. Then*

$$\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \to \widehat{\mu}, \quad \sigma \mapsto \Big(\frac{\sigma(\pi_n)}{\pi_n} \mod \mathfrak{m}_n\Big)_n$$

is an isomorphism of profinite groups that does not depend on the choice of prime elements $(\pi_n)_n$.

Proof. For every $n \in \mathbb{Z}_{>0} \backslash p\mathbb{Z}$ we get the following diagram of fields

$$\begin{tikzcd}
& K_nK^{\mathrm{unr}} \arrow[ddl, dash] \arrow[dr, dash] & \\
& & K^{\mathrm{unr}} \arrow[ddl, dash] \\
K_n \arrow[dr, dash] & & \\
& K^{\mathrm{unr}} \cap K_n \arrow[d, dash] & \\
& K &
\end{tikzcd}$$

and since K_n/K is a Galois extension, the restriction map

$$\mathrm{Gal}(K_nK^{\mathrm{unr}}/K^{\mathrm{unr}}) \to \mathrm{Gal}(K_n/(K^{\mathrm{unr}} \cap K_n))$$

is an isomorphism. Notice that $K_n/(K^{\mathrm{unr}} \cap K_n)$ is totally and tamely ramified of degree n since $X^n - \pi_K$ is an Eisenstein polynomial over the valuation ring of $K^{\mathrm{unr}} \cap K_n$, and since for any root α of $X^n - \pi_K$ we have $K_n = (K^{\mathrm{unr}} \cap K_n)(\alpha)$. By Lemma 7.5 we now have a canonical isomorphism

$$\mathrm{Gal}(K_n/(K^{\mathrm{unr}} \cap K_n)) \to \mu_n$$

for every such n. Hence, the composition of the previous two isomorphisms yields a canonical isomorphism $\psi_n : \mathrm{Gal}(K_nK^{\mathrm{unr}}/K^{\mathrm{unr}}) \to \mu_n$ for every $n \in \mathbb{Z}_{>0} \backslash p\mathbb{Z}$. It can be verified that the inverse limit

$$\varprojlim \psi_n : \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \xrightarrow{\sim} \widehat{\mu}$$

is the same map as defined in the statement of this lemma. □

Let $\psi : \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \to \widehat{\mu}$ be the isomorphism from Lemma 7.6. Notice that ψ respects the conjugation action of Δ on $\mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{unr}})$ and the natural action of Δ on $\widehat{\mu}$. Fix a Frobenius automorphism φ of K^{tr}/K. The extensions $K \subset K^{\mathrm{unr}} \subset K^{\mathrm{tr}}$ give a canonical short exact sequence

$$1 \to \widehat{\mu} \to \Delta \xrightarrow{v} \widehat{\mathbb{Z}} \to 1$$

of profinite groups. The action $\Delta \to \mathrm{Aut}(\widehat{\mu})$ factors through $\widehat{\mathbb{Z}}$ and this yields a well-defined topological action of $\widehat{\mathbb{Z}}$ on $\widehat{\mu}$ defined by defined by $1 \star \zeta = \varphi(\zeta) = \zeta^q$. Let $\widehat{\mu} \rtimes \widehat{\mathbb{Z}}$ be the associated semi-direct product. It follows that we get an isomorphism $\Delta \cong \widehat{\mu} \rtimes \widehat{\mathbb{Z}}$, as stated in the following proposition.

Proposition 7.7. *There is an isomorphism $\Delta \to \widehat{\mu} \rtimes \widehat{\mathbb{Z}}$ such that the diagram*

$$\begin{tikzcd}
1 \arrow[r] & \widehat{\mu} \arrow[r] \arrow[d, "\mathrm{id}"] & \Delta \arrow[r] \arrow[d, "\wr"] & \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & \widehat{\mu} \arrow[r] & \widehat{\mu} \rtimes \widehat{\mathbb{Z}} \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & 1
\end{tikzcd}$$

commutes, where $\widehat{\mu} \to \widehat{\mu} \rtimes \widehat{\mathbb{Z}}$ and $\widehat{\mu} \rtimes \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ are the natural inclusion and projection map respectively.

Proof. Take the isomorphism $\Delta \to \widehat{\mu} \rtimes \widehat{\mathbb{Z}}$ defined by $\sigma \mapsto (\psi(\sigma\varphi^{-v(\sigma)}), v(\sigma))$. □

Define $\mathbb{Z}_{p'} := \prod_{r \neq p} \mathbb{Z}_r$, where r ranges over all primes different from p. Notice that $\widehat{\mu}$ is a free profinite $\mathbb{Z}_{p'}$-module of rank 1 that is generated as a $\mathbb{Z}_{p'}$-module by any topological group generator of $\widehat{\mu}$.

Lemma 7.8. *Identify Δ with $\widehat{\mu} \rtimes \widehat{\mathbb{Z}}$. Then we have $\Delta^{(i+1)} = \widehat{\mu}^{(q-1)^i} \rtimes \{0\}$ for any integer $i \geq 1$.*

Proof. Let H be a $\widehat{\mathbb{Z}}$-submodule of $\widehat{\mu}$, where $\widehat{\mathbb{Z}}$ acts continuously on $\widehat{\mu}$ by $1 \star \zeta = \zeta^q$. Then the topological closure $\overline{[\Delta, H]}$ of $[\Delta, H]$ is the smallest closed normal subgroup N of H for which Δ acts trivially on H/N by conjugation, i.e., for which the q^{th}-powering action of $1 \in \widehat{\mathbb{Z}}$ on H/N is trivial. Hence, we have $\overline{[\Delta, H]} = H^{q-1}$. It now remains to prove the base case $\Delta^{(2)} = \widehat{\mu}^{q-1}$ for induction on i. By Corollary 5.3 the central exact sequence

$$0 \to \widehat{\mu}/\overline{[\Delta, \widehat{\mu}]} \to \Delta/\overline{[\Delta, \widehat{\mu}]} \to \widehat{\mathbb{Z}} \to 0$$

shows that $\Delta/\overline{[\Delta, \widehat{\mu}]}$ is abelian, and thus $\Delta^{(2)} = \overline{[\Delta, \widehat{\mu}]}$. By our earlier observations, taking $H = \widehat{\mu}$ now yields $\Delta^{(2)} = \widehat{\mu}^{q-1}$. □

Let K^{ab} and K^{cl2} be the maximal abelian and maximal class two extension of K inside K^{alg} respectively, and define $K^{\mathrm{trab}} := K^{\mathrm{tr}} \cap K^{\mathrm{ab}}$ and $K^{\mathrm{trcl2}} := K^{\mathrm{tr}} \cap K^{\mathrm{cl2}}$. Then we have $\mathrm{Gal}(K^{\mathrm{trab}}/K) = \Delta^{\mathrm{ab}}$ and $\mathrm{Gal}(K^{\mathrm{trcl2}}/K) = \Delta^{\mathrm{cl2}} = \Delta/\Delta^{(3)}$. Notice that for any $n \in \mathbb{Z}_{>0} \backslash p\mathbb{Z}$ we have $\widehat{\mu}/\widehat{\mu}^n = \mu_n$. Hence, we find by Lemma 7.8 that $\Delta^{\mathrm{ab}} \cong \mu_{q-1} \times \widehat{\mathbb{Z}}$, and $\Delta^{\mathrm{cl2}} \cong \mu_{(q-1)^2} \rtimes \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}}$ acts on $\mu_{(q-1)^2}$ by $1 \star \zeta = \zeta^q$. By tracking the previously stated isomorphisms, we get the following result, which we state due to its similarity with Theorem 7.18 and Theorem 7.20.

Proposition 7.9. *Let h_1 be the inverse of the isomorphism*

$$\mathrm{Gal}(K^{\mathrm{trcl2}}/K^{\mathrm{trab}}) \to \mu_{q-1}, \quad \sigma \mapsto \frac{\sigma(\pi_{(q-1)^2})}{\pi_{(q-1)^2}} \mod \mathfrak{m}_{(q-1)^2}.$$

Also consider the well-defined isomorphism of profinite groups

$$h_2 : \mu_{q-1} \times \widehat{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{trab}}/K),$$
$$\widehat{\mu}/\widehat{\mu}^{q-1} \times \widehat{\mathbb{Z}} \ni (\zeta \bmod \widehat{\mu}^{q-1}, x) \mapsto (\psi^{-1}(\zeta)\varphi^x)\big|_{K^{\mathrm{trab}}}.$$

Moreover, we also consider the maps $\mu_{q-1} \to \mu_{(q-1)^2} \rtimes \widehat{\mathbb{Z}}$ *defined by* $\zeta \mapsto (\zeta, 0)$ *and* $\mu_{(q-1)^2} \rtimes \widehat{\mathbb{Z}} \to \mu_{q-1} \times \widehat{\mathbb{Z}}$ *defined by* $(\zeta, x) \mapsto (\zeta^{q-1}, x)$*. Then there exists an isomorphism* $\mu_{(q-1)^2} \rtimes \widehat{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{trcl2}}/K)$ *such that the diagram*

$$\begin{tikzcd}
1 \arrow[r] & \mu_{q-1} \arrow[r] \arrow[d, "h_1"] & \mu_{(q-1)^2} \rtimes \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "\wr"] & \mu_{q-1} \times \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "h_2"] & 1 \\
1 \arrow[r] & \Delta^{(2)}/\Delta^{(3)} \arrow[r] & \Delta^{\mathrm{cl2}} \arrow[r] & \Delta^{\mathrm{ab}} \arrow[r] & 1
\end{tikzcd}$$

commutes, i.e., the diagram shows an isomorphism of exact sequences.

We will also give a cohomological description of $\mathrm{Gal}(K^{\mathrm{trcl2}}/K)$ using the theory from section 5.3. First we need the following lemma and its corollary Corollary 7.12.

Lemma 7.10. *The commutator map* $[-,-] : \bigwedge^2 \Delta^{\mathrm{ab}} \to \Delta^{(2)}/\Delta^{(3)}$ *is an isomorphism.*

Proof. From $\Delta^{\mathrm{ab}} \cong \mu_{q-1} \times \widehat{\mathbb{Z}}$ and Lemma 4.12 we find that $\bigwedge^2 \Delta^{\mathrm{ab}} \cong \mu_{q-1}$, since μ_{q-1} and $\widehat{\mathbb{Z}}$ are procyclic. The group $\Delta^{(2)}/\Delta^{(3)} \cong \mu_{q-1}$ also has order $q-1$. Since the commutator map is surjective, it follows that it is an isomorphism. □

Remark 7.11. Lemma 7.10 can also be proven in a different way, namely by showing that $\mathrm{H}^2(\Delta, \mathbb{Q}/\mathbb{Z}) = 0$ and applying Theorem 6.5. In order to show that $\mathrm{H}^2(\Delta, \mathbb{Q}/\mathbb{Z}) = 0$, define Δ_n as the group with presentation $\langle \phi, \tau \mid \phi\tau\phi^{-1} = \tau^q,\ \phi^n = 1 \rangle$ for each $n \in \mathbb{Z}_{>0}$ and notice that $\Delta = \lim_{\leftarrow} \Delta_n$. It follows that $\lim_{\rightarrow} \mathrm{H}^2(\Delta_n, \mathbb{Q}/\mathbb{Z}) = \mathrm{H}^2(\Delta, \mathbb{Q}/\mathbb{Z})$ since $\mathbb{Q}/\mathbb{Z}$ is discrete [15]. Hence, it suffices to show that $\mathrm{H}^2(\Delta_n, \mathbb{Q}/\mathbb{Z}) = 0$ for each n. Notice that Δ_n is isomorphic to $\mathbb{F}_{q^n}^* \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Let

$$1 \to \mathbb{Q}/\mathbb{Z} \xrightarrow{\iota} E \to \Delta_n \to 1$$

be a central extension of Δ_n, and let $\widetilde{\phi}$, $\widetilde{\tau} \in E$ be lifts of $\phi, \tau \in \Delta_n$ to E such that ϕ has order n and τ has order $q^n - 1$, which is possible because $\mathbb{Q}/\mathbb{Z}$ is divisible. Let $b \in \mathbb{Q}/\mathbb{Z}$ be such that $\widetilde{\phi}\widetilde{\tau}\widetilde{\phi}^{-1} = \widetilde{\tau}^q \iota b$. We calculate

$$\widetilde{\tau} = \widetilde{\phi}^n \widetilde{\tau} \widetilde{\phi}^{-n} = \widetilde{\tau}^{q^n} (\iota b)^{(q^n-1)/(q-1)} = \widetilde{\tau} (\iota b)^{(q^n-1)/(q-1)},$$

and thus we find that $b \in \frac{q-1}{q^n-1}\mathbb{Z}/\mathbb{Z}$. It follows that we can modify the choice of $\widetilde{\tau}$ such that $\widetilde{\phi}\widetilde{\tau}\widetilde{\phi}^{-1} = \widetilde{\tau}^q$. This yields a section of $E \to \Delta_n$, hence $\mathrm{H}^2(\Delta_n, \mathbb{Q}/\mathbb{Z}) = 0$. △

From now on, write $C := \mathrm{Gal}(K^{\mathrm{trab}}/K^{\mathrm{unr}})$. Moreover, from now on we will assume that φ is a Frobenius element in Δ^{cl2}. Then the short exact sequence $1 \to C \to \Delta^{\mathrm{ab}} \to \widehat{\mathbb{Z}} \to 1$ is split-exact, and C is a cyclic group of order $q-1$. The following corollary gives a natural isomorphism $C \to \Delta^{(2)}/\Delta^{(3)}$.

Corollary 7.12. *The map* $C \to \mathrm{Gal}(K^{\mathrm{trcl2}}/K^{\mathrm{trab}})$ *defined by* $\gamma \mapsto [\varphi, \widetilde{\gamma}]$*, with* $\widetilde{\gamma}$ *an extension of* γ *to* K^{trcl2}*, is an isomorphism of groups that does not depend on the choice of the Frobenius element* $\varphi \in \Delta^{\mathrm{cl2}}$*.*

Proof. By Example 4.15 we have an isomorphism $C \to \bigwedge^2 \Delta^{\mathrm{ab}}$ induced by $C \to \bigwedge^2(\widehat{\mathbb{Z}} \times \widehat{\mu})$ defined by $\gamma \mapsto \varphi \wedge \gamma$, and the resulting isomorphism $C \to \bigwedge^2 \Delta^{\mathrm{ab}}$ does not depend on the choice of φ. The result now follows from 7.10. □

We already described the structure of Δ^{cl2} explicitly. The following theorem gives an alternative description of the extension $[\Delta^{\mathrm{cl2}}] \in \mathrm{H}^2(\Delta^{\mathrm{ab}}, \Delta^{(2)}/\Delta^{(3)})$, namely by describing the Ext-part and Hom-part of

$$\mathrm{H}^2(\Delta^{\mathrm{ab}}, \Delta^{(2)}/\Delta^{(3)}) \cong \mathrm{Ext}^1(\Delta^{\mathrm{ab}}, \Delta^{(2)}/\Delta^{(3)}) \times \mathrm{Hom}(\bigwedge^2 \Delta^{\mathrm{ab}}, \Delta^{(2)}/\Delta^{(3)}),$$

where the isomorphism is as described in Proposition 5.8. We need a few definitions. First notice that $\mathrm{H}^2(C,C) = \mathrm{Ext}^1(C,C)$ by Theorem 5.2. Moreover, by Lemma 7.10 we have a natural isomorphism $[-,-] : \bigwedge^2 \Delta^{\mathrm{ab}} \xrightarrow{\sim} \Delta^{(2)}/\Delta^{(3)}$. Recall from section 5.1 that cp is the commutator pairing. Let $f : C \to \Delta^{(2)}/\Delta^{(3)}$ be the natural isomorphism from Corollary 7.12, and let $\iota : C \to \Delta^{\mathrm{ab}}$ be the inclusion map. Consider the isomorphism $\Xi : \mathrm{Ext}^1(C,C) \to \mathbb{Z}/(q-1)\mathbb{Z}$ defined by Lemma 3.23, where we identify $\mathrm{Hom}(C,C)$ with $\mathbb{Z}/(q-1)\mathbb{Z}$.

Theorem 7.13. *The map*

$$(\mathrm{H}^2(\iota, f^{-1}), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}) : \mathrm{H}^2(\Delta^{\mathrm{ab}}, \Delta^{(2)}/\Delta^{(3)}) \xrightarrow{\sim} \mathrm{Ext}^1(C,C) \times \mathrm{End}(\Delta^{(2)}/\Delta^{(3)})$$

is an isomorphism that maps $[\Delta^{\mathrm{cl2}}]$ *to* $(\xi,\ \mathrm{id})$*, for some* $\xi \in \mathrm{Ext}^1(C,C)$*. Then* ξ *is the class of the extension* $1 \to C \xrightarrow{f} \mathrm{Gal}(K^{\mathrm{trcl2}}/K^{\mathrm{unr}}) \to C \to 1$*, where* $\mathrm{Gal}(K^{\mathrm{trcl2}}/K^{\mathrm{unr}}) \to C$ *is the projection map. Moreover, we have* $\Xi(\xi) = 1 \mod q-1$*.*

Proof. It follows from Proposition 5.8 that the map

$$(\mathrm{H}^2(\iota, f^{-1}), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}) : \mathrm{H}^2(\Delta^{\mathrm{ab}}, \Delta^{(2)}/\Delta^{(3)}) \xrightarrow{\sim} \mathrm{Ext}^1(C,C) \times \mathrm{End}(\Delta^{(2)}/\Delta^{(3)})$$

is an isomorphism. It can be routinely verified that $\mathrm{cp}[\Delta^{\mathrm{cl2}}] = [-,-]$. Moreover, by applying Proposition 3.13 we see that ξ is the class $[\mathrm{Gal}(K^{\mathrm{trcl2}}/K^{\mathrm{unr}})] \in \mathrm{Ext}^1(C,C)$. It remains to verify that $\Xi(\xi) = 1 \mod q-1$. Let $\psi : \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \to \widehat{\mu}$ be the natural isomorphism from Lemma 7.6. For any $\gamma \in C$ with extension $\widetilde{\gamma} \in \mathrm{Gal}(K^{\mathrm{trcl2}}/K^{\mathrm{unr}})$ we have

$$\psi(\varphi\widetilde{\gamma}\varphi^{-1}) = \varphi(\psi(\widetilde{\gamma})) = \psi(\widetilde{\gamma})^q = \psi(\widetilde{\gamma}^q),$$

and thus

$$f(\gamma) = [\varphi, \widetilde{\gamma}] = \widetilde{\gamma}^{q-1}.$$

This shows that $\Xi(\xi) = 1 \mod q-1$. □

7.3 Maximal class-2 extension of $\mathbb{Q}_p$ for $p > 2$

Let p be an odd prime. We use the same notation from section 7.2, applied to the specific case $K = \mathbb{Q}_p$. In this section, we will determine the structure of the Galois group $\Gamma_p := \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p)$. We will deduce a cohomological characterization of Γ_p from Theorem 7.13. Moreover, this cohomological description will yield a more detailed version of Theorem 1.1. Recall that we have defined $\Delta = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tr}}/\mathbb{Q}_p)$ and $C = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{trab}}/\mathbb{Q}_p^{\mathrm{unr}})$. Moreover, we write $B := \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{unr}})$ and we denote by I_p and I_p^{tr} the inertia groups $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p^{\mathrm{unr}})$ and $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{trcl2}}/\mathbb{Q}_p)$ respectively. Let $\varphi \in \Gamma_p$ be a Frobenius element. Recall that $f : C \to \Delta^{(2)}/\Delta^{(3)}$ is the isomorphism from Corollary 7.12. The relevant field extensions and groups are shown in Figure 1, where h is an isomorphism $B \to \Gamma_p^{(2)}$ that is yet to be defined. The unnamed field equals the composite of $\mathbb{Q}_p^{\mathrm{trcl2}}$ and $\mathbb{Q}_p^{\mathrm{ab}}$ inside $\mathbb{Q}_p^{\mathrm{cl2}}$, and is added to visualize the factorization of $\Gamma_p^{(2)}$ into a pro-p subgroup and a subgroup of order $p-1$.

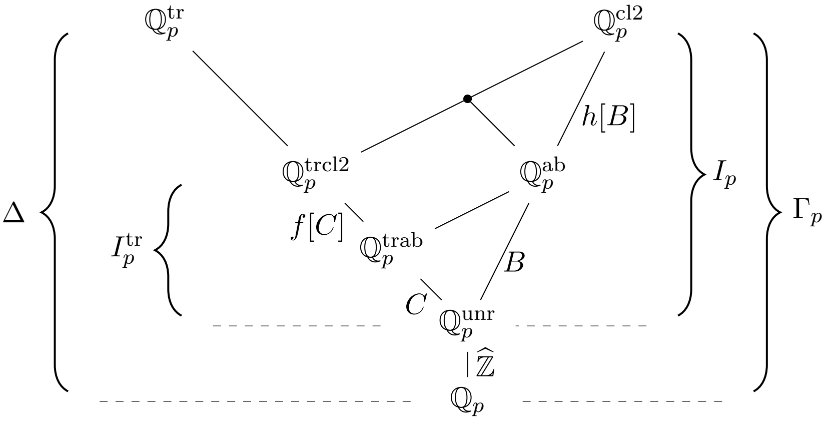

$\mathbb{Q}_p^{\mathrm{tr}}$
$\mathbb{Q}_p^{\mathrm{cl2}}$
$h[B]$
$\mathbb{Q}_p^{\mathrm{trcl2}}$
$\mathbb{Q}_p^{\mathrm{ab}}$
I_p
Δ
I_p^{tr}
$f[C]$
$\mathbb{Q}_p^{\mathrm{trab}}$
Γ_p
B
C
$\mathbb{Q}_p^{\mathrm{unr}}$
$\widehat{\mathbb{Z}}$
$\mathbb{Q}_p$

Figure 1: Hasse diagram of Galois field extensions. The unnamed field is the composite of $\mathbb{Q}_p^{\mathrm{trcl2}}$ and $\mathbb{Q}_p^{\mathrm{ab}}$. Moreover, we have $f[C] = \Delta^{(2)}/\Delta^{(3)}$ and $h[B] = \Gamma_p^{(2)}$.

By Lemma 7.4 the commutator map gives an isomorphism $\bigwedge^2 \Gamma_p^{\mathrm{ab}} \to \Gamma_p^{(2)}$. By local class field theory, the inertia group B of $\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p$ is isomorphic to the procyclic group $\mathbb{Z}_p^*$, and the short exact sequence

$$1 \to B \to \Gamma_p^{\mathrm{ab}} \to \widehat{\mathbb{Z}} \to 1$$

is split-exact, where $B \to \Gamma_p^{\mathrm{ab}}$ and $\Gamma_p^{\mathrm{ab}} \to \widehat{\mathbb{Z}}$ are the inclusion and quotient map respectively. Now Example 4.16 shows that the map $B \to \bigwedge^2 \Gamma_p^{\mathrm{ab}}$ defined by $\beta \mapsto \varphi|_{\mathbb{Q}_p^{\mathrm{ab}}} \wedge \beta$ is an isomorphism of profinite groups that does not depend on the choice of φ. Hence, we get the following result. We denote the map $B \to \Gamma_p^{(2)}$ in the following Lemma by h.

Lemma 7.14. *The map*

$$h : B \to \Gamma_p^{(2)}, \quad \beta \mapsto [\varphi, \widetilde{\beta}]$$

with $\widetilde{\beta} \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p^{\mathrm{unr}})$ any extension of β, is an isomorphism of profinite groups that does not depend on the choice of the Frobenius element $\varphi \in \Gamma_p^{\mathrm{cl2}}$.

Notice that for any profinite abelian group G we have $\mathrm{H}^2(B, G) = \mathrm{Ext}^1(B, G)$ by Corollary 5.3, and in particular we see that I_p is abelian. The inertia group B of $\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p$ is canonically isomorphic to $\mathbb{Z}_p^*$ by the local Artin isomorphism. Recall that C has order $p-1$ by section 7.2. Since $\mathbb{Z}_p^* = \mathbb{F}_p^* \times (1 + p\mathbb{Z}_p)$, the local Artin isomorphism now gives a canonical isomorphism $C \cong \mathbb{F}_p^*$. Hence, we have a canonical inclusion map $\iota : C \to B$ and projection map $\pi : B \to C$, and we have $\pi\iota = \mathrm{id}$.

Remark 7.15. The isomorphism $C \cong \mathbb{F}_p^*$ induced by the local Artin map is the multiplicative inverse of the isomorphism $C \cong \mu_{p-1}$ introduced in section 7.2: this follows from the remark in [16, Ch. 14.7]. The actual choice of the isomorphism $C \cong \mathbb{F}_p^*$ is actually not important, because they give the same isomorphism $\mathrm{Ext}^1(C, C) \cong \mathrm{Ext}^1(\mathbb{F}_p^*, \mathbb{F}_p^*)$ for both cases. △

Before we state and prove the cohomological description of Γ_p, we need to introduce more notation. Let $h : B \xrightarrow{\sim} \Gamma_p^{(2)}$ and $f : C \to \Delta^{(2)}/\Delta^{(3)}$ be the natural isomorphisms given by Lemma 7.14 and Corollary 7.12 respectively. Let $\kappa : B \hookrightarrow \Gamma_p^{\mathrm{ab}}$ be the natural embedding.

Recall from Remark 6.1 that $[-,-]$ denotes the commutator map $\bigwedge^2 G^{\mathrm{ab}} \to G^{(2)}/G^{(3)}$ for any profinite group G. Recall that $\mathrm{cp} : \mathrm{H}^2(\Gamma_p^{\mathrm{ab}}, \Gamma_p^{(2)}) \to \mathrm{Hom}(\bigwedge^2 \Gamma_p^{\mathrm{ab}}, \Gamma_p^{(2)})$ is the commutator pairing from section 5.1. Let $\Xi : \mathrm{Ext}^1(C,C) \to \mathbb{Z}/(p-1)\mathbb{Z}$ be the map induced by Lemma 3.23. Intuitively, Theorem 7.16 states that $[\Gamma_p]$ is the unique element $[E] \in \mathrm{H}^2(\Gamma_p^{\mathrm{ab}}, \Gamma_p^{(2)})$ such that $\mathrm{cp}[E] = \mathrm{id}$ and such that $\mathrm{H}^2(\kappa\iota, h^{-1}\pi)[E]$ is the class of the extension $1 \to C \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{trcl2}}/\mathbb{Q}_p^{\mathrm{unr}}) \to C \to 1$ in the 'tame part' $\mathrm{Ext}^1(C,C)$. This extension class in $\mathrm{Ext}^1(C,C)$ was previously described in Theorem 7.13.

Theorem 7.16. *The map*

$$\big(\mathrm{H}^2(\kappa, h^{-1}), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}\big) : \mathrm{H}^2(\Gamma_p^{\mathrm{ab}}, \Gamma_p^{(2)}) \xrightarrow{\sim} \mathrm{Ext}^1(B,B) \times \mathrm{End}(\Gamma_p^{(2)})$$

is an isomorphism that maps $[\Gamma_p]$ to (ξ, id) for some $\xi \in \mathrm{Ext}^1(B,B)$. Moreover, the map

$$\Xi \circ \mathrm{Ext}^1(\iota, \pi) : \mathrm{Ext}^1(B,B) \to \mathbb{Z}/(p-1)\mathbb{Z}$$

is an isomorphism that maps ξ to $1 \mod p-1$.

Proof. Since $\Gamma_p^{\mathrm{ab}} \cong B \times \widehat{\mathbb{Z}} \cong C \times \mathbb{Z}_p \times \widehat{\mathbb{Z}}$, it follows from Proposition 5.8 that

$$\big(\mathrm{H}^2(\kappa, h^{-1}), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}\big)$$

and $\mathrm{Ext}^1(\iota, B)$ are isomorphisms, and one can verify that it maps $[\Gamma_p]$ to (ξ, id) for some $\xi \in \mathrm{Ext}^1(B,B)$. Moreover, $\mathrm{Ext}^1(C,\pi)$ is an isomorphism because $\mathrm{Ext}^1(C, \mathbb{Z}_p) = 0$ by Lemma 3.24. It follows that $\mathrm{Ext}^1(\iota,\pi)$ is indeed an isomorphism. It is left to show that $\Xi \circ \mathrm{Ext}^1(\iota,\pi)$ maps ξ to $1 \mod p-1$. From Proposition 3.13 it follows that ξ equals the class of the extension

$$1 \to B \xrightarrow{h} I_p \xrightarrow{q} B \to 1,$$

where q is the projection map. It remains to prove that $\mathrm{Ext}^1(\iota,\pi)$ maps ξ to the class of the extension

$$1 \to C \xrightarrow{f} I_p^{\mathrm{tr}} \xrightarrow{q'} C \to 1,$$

where q' is the projection map: by Theorem 7.13 we then can conclude that $(\Xi \circ \mathrm{Ext}^1(\iota,\pi))(\xi)$ equals $1 \mod p-1$. Notice that indeed $\mathrm{Ext}^1(\iota,\pi)(\xi) = [I_p^{\mathrm{tr}}]$, by applying Proposition 3.13 twice to the commutative diagram,

$$\begin{tikzcd}
1 \arrow[r] & B \arrow[r, "h"] & I_p \arrow[r, "q"] & B \arrow[r] & 1 \\
1 \arrow[r] & B \arrow[u, "\mathrm{id}"] \arrow[r, "{(h,0)}"] \arrow[d, "\pi"] & I_p \times_B C \arrow[u] \arrow[r] \arrow[d] & C \arrow[u, "\iota"'] \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & C \arrow[r, "f"] & I_p^{\mathrm{tr}} \arrow[r, "q'"] & C \arrow[r] & 1
\end{tikzcd}$$

where the map $I_p \times_B C \to I_p^{\mathrm{tr}}$ is the natural composition $I_p \times_B C \to I_p \to I_p^{\mathrm{tr}}$, and the other maps out of $I_p \times_B C$ are the pullback morphisms. □

Remark 7.17. Notice that the exact sequence $1 \to I_p \to \Gamma_p \xrightarrow{v_p} \widehat{\mathbb{Z}} \to 1$ gives a topological action of $\widehat{\mathbb{Z}}$ defined by $v_p(\gamma) \star \sigma = \gamma\sigma\gamma^{-1}$ for any $\sigma \in I_p$ and $\gamma \in \Gamma_p$: this action is well-defined because I_p is abelian. Alternatively, this action is given by $x \star \sigma = \varphi^x \sigma \varphi^{-x}$

for all $x \in \widehat{\mathbb{Z}}$ and $\sigma \in I_p$. The associated semi-direct product $I_p \rtimes' \widehat{\mathbb{Z}}$ now fits in a diagram

$$\begin{tikzcd}
1 \arrow[r] & I_p \arrow[r] \arrow[d, "\mathrm{id}"] & \Gamma_p \arrow[r] \arrow[d, "\wr"] & \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & I_p \arrow[r] & I_p \rtimes' \widehat{\mathbb{Z}} \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & 1
\end{tikzcd}$$

that commutes. $\triangle$

In the following theorem, we use the notation from above. Let $h^{(2)} : \mathbb{Z}_p^* \xrightarrow{\sim} \Gamma_p^{(2)}$ be the composition

$$h^{(2)} : \mathbb{Z}_p^* \xrightarrow{\sim} B \xrightarrow{h} \Gamma_p^{(2)},$$

where $\mathbb{Z}_p^* \xrightarrow{\sim} B$ is induced by the local Artin map. Let

$$h^{\mathrm{ab}} : \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} \to \Gamma_p^{\mathrm{ab}}$$

be the isomorphism induced by the local Artin map $\widehat{\mathbb{Q}_p^*} \to \Gamma_p^{\mathrm{ab}}$ by writing $\widehat{\mathbb{Q}_p^*} = \mathbb{Z}_p^* \times \pi^{\widehat{\mathbb{Z}}}$, with π the prime element corresponding to the Frobenius element $\varphi|_{\mathbb{Q}_p^{\mathrm{ab}}}$. In the remaining part of this section, we will identify B with $\mathbb{Z}_p^*$ via the local Artin map.

Theorem 7.18. *Consider the profinite group $I_p' := (1 + p\mathbb{Z}_p) \times \mu_{(p-1)^2} \times (1 + p\mathbb{Z}_p)$ and the topological action of $\widehat{\mathbb{Z}}$ on I_p' defined by*

$$1 \star (x, \zeta, y) = (xy, \zeta^p, y).$$

Let $\Gamma_p' := I_p' \rtimes \widehat{\mathbb{Z}}$ be the associated semi-direct product. We identify $\mathbb{Z}_p^*$ with $(1+p\mathbb{Z}_p) \times \mathbb{F}_p^*$. Then there is a short exact sequence

$$1 \longrightarrow \mathbb{Z}_p^* \xrightarrow{t_p} I_p' \xrightarrow{u_p} \mathbb{Z}_p^* \longrightarrow 1$$

of profinite groups, where $t_p(x, \zeta) = (x, \zeta, 1)$ and $u_p(x, \zeta, y) = (y, \zeta^{p-1})$. Moreover, there exists an isomorphism $\Gamma_p' \to \Gamma_p$ such that

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}_p^* \arrow[r, "(t_p{,}0)"] \arrow[d, "h^{(2)}"] & \Gamma_p' \arrow[r, "(u_p{,}\mathrm{id})"] \arrow[d, "\wr"] & \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "h^{\mathrm{ab}}"] & 1 \\
1 \arrow[r] & \Gamma_p^{(2)} \arrow[r] & \Gamma_p \arrow[r] & \Gamma_p^{\mathrm{ab}} \arrow[r] & 1
\end{tikzcd}$$

is an isomorphism of exact sequences, and it maps I_p' isomorphically to the inertia group I_p of Γ_p.

Proof. Let $\Xi : \mathrm{Ext}^1(C, C) \to \mathbb{Z}/(p-1)\mathbb{Z}$ be the isomorphism induced by Lemma 3.23. By Theorem 7.16 we have that the isomorphism $\Xi \circ \mathrm{Ext}^1(\iota, \pi)$ maps the extension class ξ represented by $1 \to B \xrightarrow{h} I_p \xrightarrow{q} B \to 1$ to $1 \bmod p-1$. It can be routinely verified that the extension class of ξ'

$$1 \to \mathbb{Z}_p^* \xrightarrow{t_p} I_p' \xrightarrow{u_p} \mathbb{Z}_p^* \to 1.$$

is also mapped to $1 \bmod p-1$ by $\Xi \circ \mathrm{Ext}^1(\iota, \pi)$. Hence, we have $\xi = \xi'$. It follows that there exists an isomorphism $\eta : I'_p \xrightarrow{\sim} I_p$ such that the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}_p^* \arrow[r, "t_p"] \arrow[d, "\mathrm{id}"] & I'_p \arrow[r, "u_p"] \arrow[d, "\eta"] & \mathbb{Z}_p^* \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & B \arrow[r, "h"] & I_p \arrow[r, "q"] & B \arrow[r] & 1
\end{tikzcd}$$

is an isomorphism of exact sequences. Consider the action of $\widehat{\mathbb{Z}}$ on I'_p induced via η by the action of $\widehat{\mathbb{Z}}$ on I_p from Remark 7.17, and let $I'_p \rtimes' \widehat{\mathbb{Z}}$ be the associated semi-direct product. Then it is clear that the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & B \arrow[r, "(t_p{,}0)"] \arrow[d, "\mathrm{id}"] & I'_p \rtimes' \widehat{\mathbb{Z}} \arrow[r, "(u_p{,}\mathrm{id})"] \arrow[d, "(\eta{,}\mathrm{id})"] & B \times \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & B \arrow[r, "(h{,}0)"] & I_p \rtimes' \widehat{\mathbb{Z}} \arrow[r, "(q{,}\mathrm{id})"] & B \times \widehat{\mathbb{Z}} \arrow[r] & 1
\end{tikzcd}$$

is an isomorphism of exact sequences, where the bottom sequence is easily seen to be isomorphic to $1 \to \Gamma_p^{(2)} \to \Gamma_p \to \Gamma_p^{\mathrm{ab}} \to 1$. It now suffices to prove that $I'_p \rtimes' \widehat{\mathbb{Z}} = \Gamma'_p$, i.e., it suffices to prove that the action of $\widehat{\mathbb{Z}}$ on I'_p as defined in this proof is the same as the one stated in the theorem we are proving.

The action of $\widehat{\mathbb{Z}}$ on I_p is given by $1 \star \sigma = [\varphi, \sigma]\sigma$. Let ι_1, ι_2, ι_3 be the natural inclusions of $1+p\mathbb{Z}_p$, $\mu_{(p-1)^2}$ and $1+p\mathbb{Z}_p$ into I'_p respectively and let π_1, π_2, π_3 be the natural projections of I'_p onto $1+p\mathbb{Z}_p$, $\mu_{(p-1)^2}$ and $1+p\mathbb{Z}_p$ respectively. Let $\sigma \in I_p$. Write $e := \eta^{-1}\sigma$ and $e_i := \pi_i(e)$ for $i = 1, 2, 3$. Let $\sigma_i \in I_p$ be such that $\eta^{-1}\sigma_i = \iota_i e_i$ for $i = 1, 2, 3$. Then $\sigma = \sigma_1\sigma_2\sigma_3$ gives

$$1 \star \sigma = [\varphi, \sigma_1][\varphi, \sigma_2][\varphi, \sigma_3]\sigma.$$

Since we have $\sigma_1 \in h[B]$ and $h[B] = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p^{\mathrm{ab}})$ is central in Γ_p, we find that $[\varphi, \sigma_1] = 1$. Notice that $q(\sigma_2) = e_2^{p-1}$, and by definition of h we have $h(q(\sigma_2)) = [\varphi, \sigma_2]$. It follows that $h(e_2^{p-1}) = [\varphi, \sigma_2]$ and thus $\eta^{-1}[\varphi, \sigma_2] = \iota_2 e_2^{p-1}$. Similarly, from $q(\sigma_3) = e_3$ and $h(q(\sigma_3)) = [\varphi, e_3]$ it follows that $\eta^{-1}[\varphi, \sigma_2] = \iota_3 e_3$. Now we see that the action of $\widehat{\mathbb{Z}}$ on I'_p induced by the action of $\widehat{\mathbb{Z}}$ on I_p, is given by

$$1 \star e = \eta^{-1}(1 \star \sigma) = \eta^{-1}\big([\varphi, \sigma_1][\varphi, \sigma_2][\varphi, \sigma_3]\sigma\big) = \iota_2(e_2^{p-1})\iota_3(e_3)e.$$

It follows that the two described actions of $\widehat{\mathbb{Z}}$ on I'_p are indeed the same, and thus we have $I'_p \rtimes' \widehat{\mathbb{Z}} = \Gamma'_p$. □

7.4 Maximal class-2 extension of $\mathbb{Q}_2$

In this section we will describe the Galois group $\Gamma_2 := \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/\mathbb{Q}_2)$. There are two reasons why we need to distinguish this case from the case $\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p$ with p odd: the first reason is that the inertia group of $\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2$ is not procyclic, and the second reason is that we cannot use the theory from section 7.2 because we have $\mathbb{Q}_2^{\mathrm{trcl2}} = \mathbb{Q}_2^{\mathrm{unr}}$, where we use the notation from section 7.2. We denote by I_2 the inertia group of the extension $\mathbb{Q}_2^{\mathrm{cl2}}/\mathbb{Q}_2$. Let $\sqrt{-1} \in \mathbb{Q}_2^{\mathrm{ab}}$ be a square root of -1. By local class field theory, we have

$$\mathbb{Q}_2^{\mathrm{ab}} = \mathbb{Q}_2^{\mathrm{unr}} \otimes_{\mathbb{Q}_2} \mathbb{Q}_2(\sqrt{-1}) \otimes_{\mathbb{Q}_2} \mathbb{Q}_2(\zeta_{2^\infty} + \zeta_{2^\infty}^{-1})$$

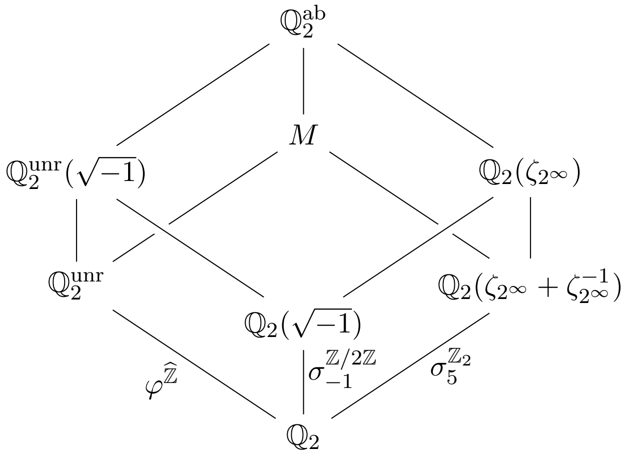
where

$$\zeta_{2^\infty} + \zeta_{2^\infty}^{-1} := \{\alpha + \alpha^{-1} \mid \exists n \in \mathbb{Z}_{>0} : \alpha^{2^n} = 1\} \subset \mathbb{Q}_2^{\mathrm{alg}}.$$

Moreover, we have $\mathbb{Q}_2(\sqrt{-1}) \otimes_{\mathbb{Q}_2} \mathbb{Q}_2(\zeta_{2^\infty} + \zeta_{2^\infty}^{-1}) = \mathbb{Q}_2(\zeta_{2^\infty})$. We define M as the composite $\mathbb{Q}_2^{\mathrm{unr}}\mathbb{Q}_2(\zeta_{2^\infty} + \zeta_{2^\infty}^{-1})$ inside $\mathbb{Q}_2^{\mathrm{ab}}$. Denote by μ_2 the subgroup $\{\pm 1\}$ of $\mathbb{Z}_2^*$. From the local Artin map we get a canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^\infty})/\mathbb{Q}_2) \cong \mathbb{Z}_2^* = \mu_2 \times (1 + 4\mathbb{Z}_2).$$

Let $\varphi \in \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{unr}}/\mathbb{Q}_2)$ be the Frobenius element of $\mathbb{Q}_2^{\mathrm{unr}}/\mathbb{Q}_2$. Notice that 5 generates $1+4\mathbb{Z}_2$ as its 2-adic logarithm is a unit in $\mathbb{Z}_2$. Let $\sigma_5 \in \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^\infty} + \zeta_{2^\infty}^{-1})/\mathbb{Q}_2) \cong 1+4\mathbb{Z}_2$ be the element corresponding to $5 \in 1 + 4\mathbb{Z}_2$. Let $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2) = \mu_2$ be the generator of $\mathrm{Gal}(\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2)$. This gives the following diagram.


$\mathbb{Q}_2^{\mathrm{ab}}$
M
$\mathbb{Q}_2^{\mathrm{unr}}(\sqrt{-1})$
$\mathbb{Q}_2(\zeta_{2^\infty})$
$\mathbb{Q}_2^{\mathrm{unr}}$
$\mathbb{Q}_2(\sqrt{-1})$
$\mathbb{Q}_2(\zeta_{2^\infty} + \zeta_{2^\infty}^{-1})$
$\varphi^{\widehat{\mathbb{Z}}}$
$\sigma_{-1}^{\mathbb{Z}/2\mathbb{Z}}$
$\sigma_5^{\mathbb{Z}_2}$
$\mathbb{Q}_2$

Let $\widetilde{\varphi}, \widetilde{\sigma_5}, \widetilde{\sigma_{-1}} \in \Gamma_2$ be the extensions of φ, σ_5, σ_{-1} respectively that are the identity map when restricted to $\mathbb{Q}_2(\zeta_{2^\infty})$, $\mathbb{Q}_2^{\mathrm{unr}}(\sqrt{-1})$, M respectively. Then $\widetilde{\sigma_5}$ acts on the roots of $X^{2^n} - 1$ in $\mathbb{Q}_2^{\mathrm{ab}}$ by taking 5th roots [16, Ch. 14.7]. Consider the group $A := \Gamma_2^{(2)}/(\Gamma_2^{(2)})^2$. Let $\iota : \mu_2 \to \Gamma_2^{\mathrm{ab}}$ be the inclusion map, and let $\pi : \Gamma_2^{(2)} \to A$ be the quotient map. Recall that the commutator map $[-,-] : \bigwedge^2 \Gamma_2^{\mathrm{ab}} \to \Gamma_2^{(2)}$ is an isomorphism due to Proposition 7.4. Let

$$\Xi : \mathrm{Ext}^1(\mu_2, A) \xrightarrow{\sim} \mathrm{Hom}(\mu_2, A)$$

be the isomorphism described in Lemma 3.23, and notice that $\mathrm{Ext}^1(\mu_2, A) = \mathrm{H}^2(\mu_2, A)$ due to Corollary 5.3. Let

$$\mathrm{cp} : \mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)}) \longrightarrow \mathrm{End}(\Gamma_2^{(2)})$$

be the commutator pairing from section 5.1. Eventually, we will prove the following theorem, namely Theorem 7.19, in this section. Intuitively, Theorem 7.19 states that class $[\Gamma_2]$ is the unique extension class ξ in $\mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)})$ such that

(i) ξ is mapped by the commutator pairing to $\mathrm{id} \in \mathrm{End}(\Gamma_2^{(2)})$,

(ii) ξ is mapped by $\mathrm{H}^2(\iota, \pi)$ to the class of an extension

$$1 \longrightarrow A \longrightarrow E \longrightarrow \mu_2 \longrightarrow 1$$

in which the coset of $[\widetilde{\varphi}, \widetilde{\sigma_5}]$ in A is mapped to an element $x^2 \in E$ with x a lift of $-1 \in \mu_2$ to E.

Theorem 7.19. *The map*

$$\big(\Xi \circ \mathrm{H}^2(\iota, \pi), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\, \mathrm{cp}\big) : \mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)}) \xrightarrow{\sim} \mathrm{Hom}(\mu_2, A) \times \mathrm{End}(\Gamma_2^{(2)})$$

is an isomorphism that maps $[\Gamma_2]$ *to* (f, id)*, where* $f(-1) = [\widetilde{\varphi}, \widetilde{\sigma_5}] \bmod (\Gamma_2^{(2)})^2$.

We will now describe $\Gamma_2^{(2)}$ in terms of the automorphisms $\widetilde{\varphi}$, $\widetilde{\sigma_{-1}}$, $\widetilde{\sigma_5}$. Using Lemma 4.12, we see that the isomorphism $[-,-] : \bigwedge^2 \Gamma_2^{\mathrm{ab}} \to \Gamma_2^{(2)}$ in Proposition 7.4 is induced by the three morphisms

$$\begin{aligned} (1 + 4\mathbb{Z}_2) \otimes \mu_2 &\longrightarrow \Gamma_2^{(2)}, \quad 1 \otimes -1 \longmapsto [\widetilde{\sigma_5}, \widetilde{\sigma_{-1}}], \\ \widehat{\mathbb{Z}} \otimes \mu_2 &\longrightarrow \Gamma_2^{(2)}, \quad 1 \otimes -1 \longmapsto [\widetilde{\varphi}, \widetilde{\sigma_{-1}}], \\ \widehat{\mathbb{Z}} \otimes \mathbb{Z}_2 &\longrightarrow \Gamma_2^{(2)}, \quad 1 \otimes 1 \longmapsto [\widetilde{\varphi}, \widetilde{\sigma_5}]. \end{aligned}$$

This shows that we have the equality

$$\Gamma_2^{(2)} = [\widetilde{\sigma_5}, \widetilde{\sigma_{-1}}]^{\mathbb{Z}/2\mathbb{Z}} \times [\widetilde{\varphi}, \widetilde{\sigma_{-1}}]^{\mathbb{Z}/2\mathbb{Z}} \times [\widetilde{\varphi}, \widetilde{\sigma_5}]^{\mathbb{Z}_2}.$$

By Proposition 7.4 we get an isomorphism of groups

$$h^{(2)} : \mu_2 \times \mathbb{Z}_2^* \xrightarrow{\sim} \Gamma_2^{(2)}, \quad ((-1)^x, (-1)^y 5^z) \mapsto [\widetilde{\sigma_5}, \widetilde{\sigma_{-1}}]^x [\widetilde{\varphi}, \widetilde{\sigma_{-1}}]^y [\widetilde{\varphi}, \widetilde{\sigma_5}]^z,$$

where $x, y \in \mathbb{Z}/2\mathbb{Z}$ and $z \in \mathbb{Z}_2$. Furthermore, we consider the isomorphism

$$h^{\mathrm{ab}} : \mathbb{Z}_2^* \times \widehat{\mathbb{Z}} \to \Gamma_2^{\mathrm{ab}}, \quad ((-1)^x 5^y, z) \mapsto \widetilde{\sigma_{-1}}|_{\mathbb{Q}_2^{\mathrm{ab}}}^x \, \widetilde{\sigma_5}|_{\mathbb{Q}_2^{\mathrm{ab}}}^y \, \widetilde{\varphi}|_{\mathbb{Q}_2^{\mathrm{ab}}}^z ,$$

where $x, y \in \mathbb{Z}/2\mathbb{Z}$ and $z \in \widehat{\mathbb{Z}}$. We also define the subgroup

$$\sqrt{1 + 4\mathbb{Z}_2} := \{x \in \mathbb{Q}_2^{\mathrm{alg}*} : x^2 \in 1 + 4\mathbb{Z}_2\}$$

of $\mathbb{Q}_2^{\mathrm{alg}*}$. We remark that $\mathbb{Q}_2(\sqrt{1 + 4\mathbb{Z}_2})$ is the unique quadratic unramified extension of $\mathbb{Q}_2$ inside $\mathbb{Q}_2^{\mathrm{alg}}$, and that $\mathbb{Z}_2^*$ is a subgroup of index 2 in $\sqrt{1 + 4\mathbb{Z}_2}$. We prove the following theorem later in this section.

Theorem 7.20. *Consider the topological action of* $1 + 4\mathbb{Z}_2$ *on* $\mu_2 \times \sqrt{1 + 4\mathbb{Z}_2}$ *defined by*

$$5 \star (\varepsilon, x) = (\frac{\varphi(x)}{x} \varepsilon, x).$$

Let $I_2' := (\mu_2 \times \sqrt{1 + 4\mathbb{Z}_2}) \rtimes (1 + 4\mathbb{Z}_2)$ *be the associated semi-direct product. Let a topological action of* $\widehat{\mathbb{Z}}$ *on* I_2' *be defined by*

$$1 \star (\varepsilon, x, y) = (\varepsilon, \varphi(x) y, y)$$

and let $\Gamma_2' := I_2' \rtimes \widehat{\mathbb{Z}}$ *be the associated semi-direct product. Then there is a short exact sequence*

$$1 \longrightarrow \mu_2 \times \mathbb{Z}_2^* \xrightarrow{t} I_2' \xrightarrow{u} \mathbb{Z}_2^* \longrightarrow 1$$

of profinite groups, where $t(\varepsilon, x) = (\varepsilon, x, 1)$ *and* $u(\varepsilon, x, y) = (\varphi(x)/x) y$*, and there is an isomorphism*

$$\begin{tikzcd} 1 \arrow[r] & \mu_2 \times \mathbb{Z}_2^* \arrow[r, "t"] \arrow[d, "h^{(2)}"] & \Gamma_2' \arrow[r, "u"] \arrow[d, "\wr"] & \mathbb{Z}_2^* \times \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "h^{\mathrm{ab}}"] & 1 \\ 1 \arrow[r] & \Gamma_2^{(2)} \arrow[r] & \Gamma_2 \arrow[r] & \Gamma_2^{\mathrm{ab}} \arrow[r] & 1 \end{tikzcd}$$

of short exact sequences of profinite groups, and it maps I_2' *isomorphically to the inertia group* I_2 *of* Γ_2.

Recall that we denote by Ξ the isomorphism $\mathrm{Ext}^1(\mu_2, A) \to \mathrm{Hom}(\mu_2, A)$ as described in Lemma 3.23.

Lemma 7.21. *The map*

$$\big(\Xi \circ \mathrm{H}^2(\iota,\pi), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}\big) : \mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)}) \xrightarrow{\sim} \mathrm{Hom}(\mu_2, A) \times \mathrm{End}(\Gamma_2^{(2)})$$

is an isomorphism.

Proof. Since $\Gamma_2^{\mathrm{ab}} \cong \mu_2 \times (1+4\mathbb{Z}_2) \times \widehat{\mathbb{Z}}$, it follows from Proposition 5.8 that

$$\big(\mathrm{H}^2(\iota,\mathrm{id}), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}\big) : \mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)}) \xrightarrow{\sim} \mathrm{Ext}^1(\mu_2, \Gamma_2^{(2)}) \times \mathrm{End}(\Gamma_2^{(2)})$$

is an isomorphism. Notice that $\mathrm{Ext}^1(\mathrm{id},\pi) : \mathrm{Ext}^1(\mu_2, \Gamma_2^{(2)}) \to \mathrm{Ext}^1(\mu_2, A)$ is an isomorphism by Lemma 3.22. Since we have $\mathrm{Ext}^1(\mathrm{id},\pi)\,\mathrm{H}^2(\iota,\mathrm{id}) = \mathrm{H}^2(\iota,\pi)$ and since Ξ is an isomorphism, the result follows. □

Define P as the compositum of all quadratic extensions of $\mathbb{Q}_2^{\mathrm{ab}}$ in $\mathbb{Q}_2^{\mathrm{cl2}}$. We remark that we have $\mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}}) = A$. Define S as the compositum of all quadratic extensions of M in $\mathbb{Q}_2^{\mathrm{cl2}}$. Notice that S and P are both Galois over $\mathbb{Q}_2$ since the groups $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/S)$ and $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/P)$ are both central in Γ_2. Moreover, we have $S \subset P$: if K is a quadratic extension of M, then the compositum $K\mathbb{Q}_2^{\mathrm{ab}}$ is of degree 1 or 2 over $\mathbb{Q}_2^{\mathrm{ab}}$. Notice that we have the following equality

$$\mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}}) = [\widetilde{\sigma_5}, \widetilde{\sigma_{-1}}]|_P^{\mathbb{Z}/2\mathbb{Z}} \times [\widetilde{\varphi}, \widetilde{\sigma_{-1}}]|_P^{\mathbb{Z}/2\mathbb{Z}} \times \left([\widetilde{\varphi}, \widetilde{\sigma_5}]^{\mathbb{Z}_2}/[\widetilde{\varphi}, \widetilde{\sigma_5}]^{2\mathbb{Z}_2}\right).$$

Moreover, for $\mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}}) = A$ we get an isomorphism

$$\begin{aligned} \overline{h^{(2)}} : \qquad & \mu_2 \times (\mathbb{Z}_2^*/\overline{\langle 5^2\rangle}) \xrightarrow{\sim} A, \\ & ((-1)^x, (-1)^y 5^z \overline{\langle 5^2\rangle}) \mapsto [\widetilde{\sigma_5}, \widetilde{\sigma_{-1}}]|_P^x\, [\widetilde{\varphi}, \widetilde{\sigma_{-1}}]|_P^y\, [\widetilde{\varphi}, \widetilde{\sigma_5}]|_P^z \end{aligned}$$

induced by $h^{(2)}$.

Notice that P/M is abelian by Corollary 5.3 since $\mathbb{Q}_2^{\mathrm{ab}}/M$ is cyclic. From Lemma 3.23 it follows that in order to describe the extension class

$$[\mathrm{Gal}(P/M)] \in \mathrm{Ext}^1(\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/M), \mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}}))$$

it suffices to express $\widetilde{\sigma_{-1}}^2$ in terms of $[\widetilde{\varphi}, \widetilde{\sigma_{-1}}]$, $[\widetilde{\sigma_5}, \widetilde{\sigma_{-1}}]$, $[\widetilde{\varphi}, \widetilde{\sigma_5}]$, modulo $[\widetilde{\varphi}, \widetilde{\sigma_5}]^{2\mathbb{Z}_2}$. We get a diagram of fields as seen in Figure 2.

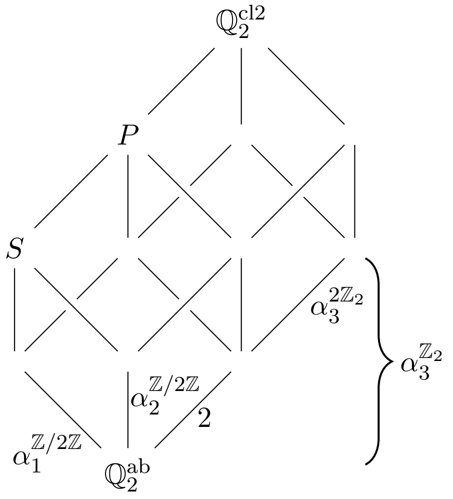

$\mathbb{Q}_2^{\mathrm{cl2}}$
P
S
$\alpha_3^{2\mathbb{Z}_2}$
$\alpha_3^{\mathbb{Z}_2}$
$\alpha_2^{\mathbb{Z}/2\mathbb{Z}}$
2
$\alpha_1^{\mathbb{Z}/2\mathbb{Z}}$
$\mathbb{Q}_2^{\mathrm{ab}}$

Figure 2: diagram of fields with $\alpha_1 := [\widetilde{\varphi}, \widetilde{\sigma_{-1}}]$, $\alpha_2 := [\widetilde{\sigma_{-1}}, \widetilde{\sigma_5}]$, $\alpha_3 := [\widetilde{\varphi}, \widetilde{\sigma_5}]$. In Lemma 7.22 we prove that the field S is placed correctly in this Hasse diagram.

Lemma 7.22. *We have an equality $S = P^{\langle \widetilde{\sigma_{-1}}|_P^2 \rangle}$ of fields.*

Proof. Since $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M) = \langle \widetilde{\sigma_{-1}} \rangle \Gamma_2^{(2)}$ we find that $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M)^2 = \langle \widetilde{\sigma_{-1}}^2 \rangle (\Gamma_2^{(2)})^2$. Now the result follows from the fact that P and S correspond as intermediate extensions of $\mathbb{Q}_2 \subset \mathbb{Q}_2^{\mathrm{cl2}}$ to the groups $(\Gamma_2^{(2)})^2$ and $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M)^2$ respectively. □

Write $G := \mathrm{Gal}(M/\mathbb{Q}_2)$, and notice that for any $\sigma \in G$ we have $\sigma(\pm M^{*2}) = \pm M^{*2}$, so that G acts naturally on $M^*/\pm M^{*2}$.

Lemma 7.23. *Let $\alpha \in M^*$, and let $\sqrt{\alpha} \in \mathbb{Q}_2^{\mathrm{alg}}$ be a root of $X^2 - \alpha$. We have the following equivalences*

$$M(\sqrt{\alpha}) \subset S \iff \mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha}) \subset S \iff \mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})/\mathbb{Q}_2 \text{ is Galois} \iff \alpha \in (M^*/\pm M^{*2})^G.$$

Proof. The first equivalence is clear since $\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})$ is the compositum of $\mathbb{Q}_2^{\mathrm{ab}}$ and $M(\sqrt{\alpha})$ in $\mathbb{Q}_2^{\mathrm{cl2}}$. We will now prove the second equivalence. If $\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})/\mathbb{Q}_2$ is Galois, then $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})/\mathbb{Q}_2^{\mathrm{ab}})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})/\mathbb{Q}_2)$ that is central because its cardinality equals 2. Hence, if $\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})/\mathbb{Q}_2$ is Galois, then $\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha}) = M(i, \sqrt{\alpha}) \subset S$. Any intermediate field E of the extension $\mathbb{Q}_2^{\mathrm{ab}} \subset \mathbb{Q}_2^{\mathrm{cl2}}$ is Galois over $\mathbb{Q}_2$, so the second equivalence is proven. Finally, we prove the third equivalence. Due to Kummer theory, we have an equality

$$W := \langle -1, \alpha \rangle M^{*2}/M^{*2} = (\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha})^{*2} \cap M^*)/M^{*2}$$

of subgroups of M^*/M^{*2}, since $\mathbb{Q}_2^{\mathrm{ab}}(\sqrt{\alpha}) = M(\sqrt{-1}, \sqrt{\alpha})$. Moreover, by Kummer theory, we have that $M(\sqrt{-1}, \sqrt{\alpha})/\mathbb{Q}_2$ is Galois if and only if W is a G-submodule of M^*/M^{*2}. The result follows. □

Recall from section 3.1 the definition of the connecting homomorphisms.

Lemma 7.24. *The connecting homomorphism*

$$\delta : (M^*/\pm M^{*2})^G \to \mathrm{H}^1(G, \pm M^{*2}),$$

induced by the exact sequence $1 \to \pm M^{*2} \to M^* \to M^*/\pm M^{*2} \to 1$ of G-modules, is an isomorphism.

Proof. The short exact sequence above induces by Theorem 3.1 a long exact sequence

$$0 \to (\pm M^{*2})^G \to (\mathbb{Q}_2^*)^G \to (M^*/\pm M^{*2})^G \to \mathrm{H}^1(G, \pm M^{*2}) \to \mathrm{H}^1(G, M^*).$$

Notice that the G-invariants of $\pm M^{*2}$ and of M^* both equal $\mathbb{Q}_2^*$, and that $\mathrm{H}^1(G, M^*) = 0$ by Theorem 3.15. The result follows. □

Lemma 7.25. *We have $[P : S] \cdot \# \mathrm{H}^1(G, M^{*2}) = 2$.*

Proof. From Lemma 7.23 and Kummer theory it follows that $\#(M^*/\pm M^{*2})^G = [S : \mathbb{Q}_2^{\mathrm{ab}}]$. Hence, we have

$$[P : S] \cdot \#(M^*/\pm M^{*2})^G = 8. \tag{4}$$

Since $\mathrm{H}^1(G, -)$ is an additive functor, $\pm M^{*2} = \langle \pm 1 \rangle \times M^{*2}$ gives

$$\mathrm{H}^1(G, \pm M^{*2}) \cong \mathrm{H}^1(G, \langle -1 \rangle) \times \mathrm{H}^1(G, M^{*2}).$$

The action of G on $\langle -1 \rangle$ is trivial, and thus $\mathrm{H}^1(G, \langle -1 \rangle) \cong \mathrm{Hom}(G, \langle -1 \rangle)$. It follows from

$G = \widetilde{\varphi}|_M^{\widehat{\mathbb{Z}}} \times \widetilde{\sigma_5}|_M^{\mathbb{Z}_2}$ that we have $\#\operatorname{Hom}(G, \langle -1 \rangle) = 4$. Using Lemma 7.24 we conclude that

$$\#(M^*/\pm M^{*2})^G = 4 \cdot \#\operatorname{H}^1(G, M^{*2}),$$

and together with (4), this proves the result. □

The following result simplifies the statement of Lemma 7.25.

Proposition 7.26. *We have* $\operatorname{H}^1(G, M^{*2}) = 0$.

Proof. The map $M^* \to M^{*2},\ x \mapsto x^2$ induces a short exact sequence of G-modules

$$0 \to \mu_2 \to M^* \to M^{*2} \to 0.$$

By taking cohomology groups and applying Theorem 3.15, we obtain the following exact sequence:

$$0 \to \operatorname{H}^1(G, M^{*2}) \to \operatorname{H}^2(G, \mu_2) \xrightarrow{\psi} \operatorname{H}^2(G, M^*).$$

Since $G \cong \mathbb{Z}_2 \times \widehat{\mathbb{Z}}$ we see that $\operatorname{Ext}^1(G, \mu_2) = 0$ because $\mathbb{Z}_2$ and $\widehat{\mathbb{Z}}$ are projective and because Ext^1 is additive. Theorem 5.2 now shows that $\operatorname{H}^2(G, \mu_2) \cong \mathbb{Z}/2\mathbb{Z}$:

$$\operatorname{H}^2(G, \mu_2) \cong \operatorname{Hom}(\bigwedge^2 G, \mu_2) \cong \operatorname{Hom}(\mathbb{Z}_2, \mu_2) = \mathbb{Z}/2\mathbb{Z}.$$

Hence, it suffices to prove that ψ is non-trivial.

Consider the composition $\psi' := \operatorname{Inf} \circ \psi : \operatorname{H}^2(G, \mu_2) \to \operatorname{Br}(\mathbb{Q}_2)$. From the exact sequence $0 \to \mu_2 \to M^* \to M^{*2} \to 0$ we find that

$$\mathbb{Q}_2^* \xrightarrow{2} M^{*2} \cap \mathbb{Q}_2^* \to \operatorname{H}^1(G, \mu_2) \to 0$$

is exact by taking cohomology groups and applying Theorem 3.15. Hence, we have a canonical isomorphism

$$\operatorname{H}^1(G, \mu_2) \cong (M^{*2} \cap \mathbb{Q}_2^*)/\mathbb{Q}_2^{*2} = \langle 2, -3 \rangle \mathbb{Q}_2^{*2}/\mathbb{Q}_2^{*2}.$$

We denote by $G_{\mathbb{Q}}$ the Galois group $\operatorname{Gal}(\mathbb{Q}_2^{\mathrm{sep}}/\mathbb{Q}_2)$. Recall from section 3.1 and section 3.2 that we denote inflation maps and cup products by Inf and $\cup$ respectively. Then we get a commutative diagram

$$\begin{tikzcd}
\operatorname{H}^1(G, \mu_2) \times \operatorname{H}^1(G, \mu_2) \arrow[r, "\cup"] \arrow[d, "(\operatorname{Inf},\operatorname{Inf})"] & \operatorname{H}^2(G, \mu_2) \arrow[r, "\psi"] \arrow[d, "\operatorname{Inf}"] & \operatorname{H}^2(G, M^*) \arrow[d, "\operatorname{Inf}"] \\
\operatorname{H}^1(G_{\mathbb{Q}_2}, \mu_2) \times \operatorname{H}^1(G_{\mathbb{Q}_2}, \mu_2) \arrow[r, "\cup"] \arrow[d] & \operatorname{H}^2(G_{\mathbb{Q}_2}, \mu_2) \arrow[r] \arrow[d] & \operatorname{Br}(\mathbb{Q}_2) \\
\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \arrow[r, "{(-,-)}"] & \operatorname{Br}(\mathbb{Q}_2)[2] &
\end{tikzcd}$$

where the top left square commutes due to [11, Prop. 7.9.5] and the bottom square commutes due to our definition of the norm-residue symbols $(-,-)$ in section 3.5. We have $\operatorname{Br}(\mathbb{Q}_2)[2] = \mathbb{Z}/2\mathbb{Z}$ by Theorem 3.17 and $(-,-) : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \to \operatorname{Br}(\mathbb{Q}_2)[2]$ is a non-degenerate bilinear map due to Theorem 3.18. Now it follows from $\dim_{\mathbb{F}_2}(\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}) = 3$ and $\dim_{\mathbb{F}_2}(\langle 2, -3 \rangle \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}) = 2$, that for some $\alpha, \beta \in \operatorname{H}^1(G, \mu_2)$ we have $\psi'(\alpha \cup \beta) \neq 0$. We conclude that ψ is non-trivial. □

Corollary 7.27. *We have* $[P : S] = 2$.

Proof. This follows immediately from Lemma 7.25 and Proposition 7.26. □

Let $\sqrt[4]{2}$ and $\sqrt[4]{3}$ in $\mathbb{Q}_2^{\mathrm{alg}}$ be square roots of $\sqrt{2}$ and $\sqrt{3}$ respectively. With Hensel's Lemma, one can verify that $x2^n \in \mathbb{Q}_2^*$ with $x \in \mathbb{Z}_2^*$ is a square in $\mathbb{Q}_2^*$ if and only if $x \equiv 1 \mod 8$ and $n \equiv 0 \mod 2$ both hold. From this it follows that $\mathbb{Q}_2(\sqrt{\mathbb{Q}_2^*})$ equals $\mathbb{Q}_2(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$ and this field is of degree 8 over $\mathbb{Q}$.

Lemma 7.28. *We have* $S = M(\sqrt{-1}, \sqrt[4]{2}, \sqrt[4]{-3})$.

Proof. By Lemma 7.23 and Kummer theory, it follows that it suffices to prove that $\sqrt{2}$, $\sqrt{-3}$ are generators of the group $(M^*/\pm M^{*2})^G$. By Lemma 7.24 and Proposition 7.26 we have

$$(M^*/\pm M^{*2})^G \cong \mathrm{H}^1(G, \pm M^{*2}) = \mathrm{H}^1(G, \mu_2) = \mathrm{Hom}(G, \mu_2),$$

where we use the additivity of $\mathrm{H}^1(G, -)$. Notice that $\mathrm{Hom}(G, \mu_2)$ is generated by the maps $f_{\sqrt{2}} : \sigma \mapsto \sigma(\sqrt{2})/\sqrt{2}$ and $f_{\sqrt{-3}} : \sigma \mapsto \sigma(\sqrt{-3})/\sqrt{-3}$. Then $\sqrt{2}$ and $\sqrt{-3}$ in $(M^*/\pm M^{*2})^G$ correspond to the maps $f_{\sqrt{2}}$ and $f_{\sqrt{-3}}$ respectively, and thus generate $(M^*/\pm M^{*2})^G$. □

Notice that we have

$$M \cap \mathbb{Q}_2(\sqrt{-1}, \sqrt[4]{2}, \sqrt[4]{-3}) = \mathbb{Q}_2(\sqrt{2}, \sqrt{-3}),$$

and the field S equals the composite field $M\mathbb{Q}_2(\sqrt{-1}, \sqrt[4]{2}, \sqrt[4]{-3})$ by Lemma 7.28. Since

$$[S : M] = 8 = [\mathbb{Q}_2(\sqrt{-1}, \sqrt[4]{2}, \sqrt[4]{-3}) : \mathbb{Q}_2(\sqrt{2}, \sqrt{-3})]$$

we conclude that $S = M \otimes_{\mathbb{Q}_2(\sqrt{2},\sqrt{-3})} \mathbb{Q}_2(\sqrt{-1}, \sqrt[4]{2}, \sqrt[4]{-3})$.

Lemma 7.29. *We have* $\widetilde{\sigma_{-1}}^2 = [\widetilde{\varphi}, \widetilde{\sigma_5}]$.

Proof. By Lemma 7.22 and Lemma 7.27 we see that $\widetilde{\sigma_{-1}}$ is the unique non-trivial element in $\mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}})$ that is the identity automorphism on S. Hence, it suffices to prove that $[\widetilde{\varphi}, \widetilde{\sigma_5}]|_S = \mathrm{id}_S$. By Lemma 7.28 it now suffices to verify that $\sqrt[4]{2}$, $\sqrt[4]{-3}$ are fixed points of $[\widetilde{\varphi}, \widetilde{\sigma_5}]$. The following table displays the sign of $\tau(\alpha)/\alpha$ for $\tau \in \{\widetilde{\sigma_5}, \widetilde{\varphi}\}$ and $\alpha \in \{\sqrt{-1}, \sqrt{2}, \sqrt{-3}\}$.

	$\widetilde{\sigma_5}$	$\widetilde{\varphi}$
$\sqrt{-1}$	$+$	$+$
$\sqrt{2}$	$-$	$+$
$\sqrt{-3}$	$+$	$-$

Since $[\widetilde{\varphi}, \widetilde{\sigma_5}]$ is independent of the choice of lifts of σ_5 and φ, we may assume without loss of generality that the following table represents the outcomes $\tau(\alpha)/\alpha$ of the input $\alpha = \sqrt[4]{2}, \sqrt[4]{-3}$ under $\tau = \widetilde{\sigma_5}, \widetilde{\varphi}$.

	$\widetilde{\sigma_5}$	$\widetilde{\varphi}$
$\sqrt[4]{2}$	$\sqrt{-1}$	1
$\sqrt[4]{-3}$	1	$\sqrt{-1}$

Now we can calculate that

$$[\widetilde{\varphi}, \widetilde{\sigma_5}](\sqrt[4]{2}) = \sqrt[4]{2}, \qquad [\widetilde{\varphi}, \widetilde{\sigma_5}](\sqrt[4]{-3}) = \sqrt[4]{-3}.$$

Hence, it follows that $[\widetilde{\varphi}, \widetilde{\sigma_5}]|_S = \mathrm{id}_S$ and $\widetilde{\sigma_{-1}}^2 = [\widetilde{\varphi}, \widetilde{\sigma_5}]$. □

Proof Theorem 7.19. By Lemma 7.21 we know that

$$\big(\Xi \circ \mathrm{H}^2(\iota, \pi), \mathrm{Hom}([-,-]^{-1}, \mathrm{id})\,\mathrm{cp}\big) : \mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)}) \xrightarrow{\sim} \mathrm{Hom}(\mu_2, A) \times \mathrm{End}(\Gamma_2^{(2)})$$

is an isomorphism. As noted in section 7.1, the map

$$\mathrm{Hom}([-,-]^{-1},\mathrm{id})\,\mathrm{cp} : \mathrm{H}^2(\Gamma_2^{\mathrm{ab}},\Gamma_2^{(2)}) \to \mathrm{End}(\Gamma_2^{(2)})$$

maps $[\Gamma_2]$ to the identity map. It remains to show that $\Xi\circ\mathrm{H}^2(\iota,\pi)[\Gamma_2]$ is the homomorphism $\mu_2 \to A$ defined by $-1 \mapsto [\widetilde{\varphi},\widetilde{\sigma_5}]$. Applying Proposition 3.13 shows that $\mathrm{H}^2(\iota,\pi)[\Gamma_2]$ is the class of the extension

$$1 \to \mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}}) \to \mathrm{Gal}(P/M) \to \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/M) \to 1.$$

Now it follows from Lemma 7.29 that $\Xi \circ \mathrm{H}^2(\iota,\pi)[\Gamma_2]$ maps -1 to $[\widetilde{\varphi},\widetilde{\sigma_5}]$. □

Proof Theorem 7.20. This proof will be similar to the proof of Theorem 7.18. Notice that from Proposition 3.13 it follows that $\mathrm{H}^2(\iota,\pi)[\Gamma_2]$ is the class of the extension $[\mathrm{Gal}(P/M)] \in \mathrm{Ext}^1(\mu_2, A)$. Let $\psi : \sqrt{1+4\mathbb{Z}_2} \to \mu_2$ be the morphism $x \mapsto \varphi(x)/x$. We denote by $\overline{\psi} : \sqrt{1+4\mathbb{Z}_2}/\overline{\langle 5^2\rangle} \to \mu_2$ the map induced by ψ. From Theorem 7.19 it follows that there exists an isomorphism

$$\mu_2 \times \left(\sqrt{1+4\mathbb{Z}_2}\ /\ \overline{\langle 5^2\rangle}\right) \xrightarrow{\sim} \mathrm{Gal}(P/M)$$

such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \times (\mathbb{Z}_2^*/\overline{\langle 5^2\rangle}) \arrow[r, "\text{inclusion}"] \arrow[d, "\overline{h^{(2)}}"] & \mu_2 \times \left(\sqrt{1+4\mathbb{Z}_2}/\overline{\langle 5^2\rangle}\right) \arrow[r, "0\oplus\overline{\psi}"] \arrow[d, "\wr"] & \mu_2 \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & \mathrm{Gal}(P/\mathbb{Q}_2^{\mathrm{ab}}) \arrow[r] & \mathrm{Gal}(P/M) \arrow[r] & \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/M) \arrow[r] & 1
\end{tikzcd}$$

commutes. From the previous diagram we find that there exists an isomorphism $\eta : \mu_2 \times \mathbb{Z}_2^* \to \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M)$ such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \times \mathbb{Z}_2^* \arrow[r, "\text{inclusion}"] \arrow[d, "h^{(2)}"] & \mu_2 \times \sqrt{1+4\mathbb{Z}_2} \arrow[r, "0\oplus\psi"] \arrow[d, "\eta"', "\wr"] & \mu_2 \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & \Gamma_2^{(2)} \arrow[r] & \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M) \arrow[r] & \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/M) \arrow[r] & 1
\end{tikzcd}$$

commutes: by applying the isomorphisms $\mathrm{Ext}^1(\mathrm{id},\overline{h^{(2)}}^{-1}\pi h^{(2)})$ and $\mathrm{Ext}^1(\mathrm{id},\pi)$ to the extension classes of the top row and bottom row of this diagram respectively, we obtain the extension classes of the top row and bottom row of the penultimate diagram respectively.

Now we will describe the extension class $[I_2] \in \mathrm{H}^2(\mathrm{Gal}(M/\mathbb{Q}_2^{\mathrm{unr}}),\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M))$ of

$$1 \to \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M) \to \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/\mathbb{Q}_2^{\mathrm{unr}}) \to \mathrm{Gal}(M/\mathbb{Q}_2^{\mathrm{unr}}) \to 1.$$

The action of I_2 on $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M)$ by conjugation factors through $\mathrm{Gal}(M/\mathbb{Q}_2^{\mathrm{unr}})$ since $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M)$ is abelian. The induced topological action of $\mathrm{Gal}(M/\mathbb{Q}_2^{\mathrm{unr}})$ on $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{cl2}}/M)$ by conjugation is given by $\widetilde{\sigma_5}|_M \star \gamma = [\widetilde{\sigma_5},\gamma]\gamma$. It induces via η an action of $1+4\mathbb{Z}_2$ on $\mu_2 \times \sqrt{1+4\mathbb{Z}_2}$. We let $(\varepsilon, x) \in \mu_2 \times \sqrt{1+4\mathbb{Z}_2}$, write $x = (-1)^a\sqrt{5}^b$ with $a \in \mathbb{Z}/2\mathbb{Z}$ and $b \in \mathbb{Z}_2$, write $\gamma := \eta(1,\sqrt{5}^b)$, and we find that this action of $1+4\mathbb{Z}_2$ on $\mu_2 \times \sqrt{1+4\mathbb{Z}_2}$ is given by

$$5 \star (\varepsilon, x) = \eta^{-1}([\widetilde{\sigma_5},\gamma]\gamma)(\varepsilon,(-1)^a) = \eta^{-1}([\widetilde{\sigma_5},\widetilde{\sigma_{-1}}]^b\gamma)(\varepsilon,(-1)^a) = (\frac{\varphi(x)}{x}\varepsilon, x).$$

We conclude that this action coincides with the action of $1+4\mathbb{Z}_2$ on $\mu_2 \times \sqrt{1+4\mathbb{Z}_2}$ defining

I_2'. Hence, there exists an isomorphism $\eta' : I_2' \to I_2$ such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \times \mathbb{Z}_2^* \arrow[r, "t"] \arrow[d, "h"] & I_2' \arrow[r, "u"] \arrow[d, "\eta'"', "\wr"] & \mathbb{Z}_2^* \arrow[r] \arrow[d, "h^{\mathrm{ab}}|_{\mathbb{Z}_2^*}"] & 1 \\
1 \arrow[r] & \Gamma_2^{(2)} \arrow[r] & I_2 \arrow[r] & \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2^{\mathrm{unr}}) \arrow[r] & 1
\end{tikzcd}$$

commutes.

Now we will describe the extension $[\Gamma_2] \in \mathrm{H}^2(\Gamma_2^{\mathrm{ab}}, \Gamma_2^{(2)})$. Consider the section s defined by $\varphi \mapsto \widetilde{\varphi}$ of the quotient map $\Gamma_2 \to \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{unr}}/\mathbb{Q}_2)$. The induced action of $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{unr}}/\mathbb{Q}_2)$ on I_2 by conjugation, now induces via η' an action of $\widehat{\mathbb{Z}}$ on I_2'. We find that this action is given by

$$1 \star (\varepsilon, x, y) = (\varepsilon, \varphi(x), y) :$$

write $x = (-1)^a \sqrt{5}^b$ and $y = 5^c$ with $a \in \mathbb{Z}/2\mathbb{Z}$ and $b, c \in \mathbb{Z}_2$ and write $\gamma := \eta'(1, \sqrt{5}^b, 1)$ and $\gamma' := \eta'(1, 1, y)$, and notice that we have

$$\begin{aligned}
1 \star (\varepsilon, x, y) &= (\varepsilon, (-1)^a, 1)\eta'^{-1}([\widetilde{\varphi}, \gamma]\gamma)\eta'^{-1}([\widetilde{\varphi}, \gamma']\gamma) \\
&= (\varepsilon, (-1)^a, 1)\eta'^{-1}([\widetilde{\varphi}, \widetilde{\sigma_{-1}}]^b\gamma)\eta'^{-1}([\widetilde{\varphi}, \widetilde{\sigma_5}]^c\gamma') \\
&= (\varepsilon, (-1)^a, 1)(1, \varphi(x), 1)(1, y, y).
\end{aligned}$$

Hence, the associated semi-direct product $I_2' \rtimes \widehat{\mathbb{Z}}$ equals Γ_2'. We conclude that there exists an isomorphism $\Gamma_2' \xrightarrow{\sim} \Gamma_2$ such that the diagram as stated in the theorem commutes. □

Theorem 7.20 shows that the extension class $[I_2] \in \mathrm{H}^2(\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}, \mathbb{Q}_2^{\mathrm{unr}}), \Gamma_2^{(2)})$ is mapped by the isomorphism $\mathrm{H}^2(h^{\mathrm{ab}}, (h^{(2)})^{-1})$ to the extension class $[I_2'] \in \mathrm{H}^2(\mathbb{Z}_2^*, \mu_2 \times \mathbb{Z}_2^*)$ of the extension

$$1 \to \mu_2 \times \mathbb{Z}_2^* \xrightarrow{t} I_2' \xrightarrow{u} \mathbb{Z}_2^* \to 1.$$

In the remaining part of this section, we will define a map ret, as in Proposition 5.5, and describe the 'Ext-part' $\mathrm{ret}[I_2'] \in \mathrm{Ext}^1(\mathbb{Z}_2^*, \mathbb{Z}_2^*)$ of the extension class $[I_2']$. This will be used in section 7.5 in order to describe the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cl2}}/\mathbb{Q})$. The following proposition describes $\mathrm{ret}[I_2']$.

Proposition 7.30. *Define $J_2' := \mu_2 \times \sqrt{1 + 4\mathbb{Z}_2} \times (1 + 4\mathbb{Z}_2)$. Then the element* $\mathrm{ret}[I_2']$ *in* $\mathrm{Ext}^1(\mathbb{Z}_2^*, \mu_2 \times \mathbb{Z}_2^*)$ *equals the extension class of*

$$1 \longrightarrow \mu_2 \times \mathbb{Z}_2^* \xrightarrow{t_2} J_2' \xrightarrow{u_2} \mathbb{Z}_2^* \longrightarrow 1,$$

where $t_2(\varepsilon, x) = (\varepsilon, x, 1)$ and $u_2(\varepsilon, x, y) = (\varphi(x)/x)y$.

Proof. Write $\mathbb{Z}_2^* = \mu_2 \times (1 + 4\mathbb{Z}_2)$ and consider the projection maps $p_1 : \mathbb{Z}_2^* \to \mu_2$ and $p_2 : \mathbb{Z}_2^* \to (1 + 4\mathbb{Z}_2)$. By the definition of the retraction map ret in Proposition 5.5, it suffices to prove that $\mathrm{Ext}^1(p_i, \mathrm{id})[J_2'] = \mathrm{H}^2(p_i, \mathrm{id})[I_2']$ for $i = 1, 2$. For $i = 2$ this is clear: since $1 + 4\mathbb{Z}_2$ is projective and procyclic, we have

$$\mathrm{H}^2(1 + 4\mathbb{Z}_2, \mu_2 \times \mathbb{Z}_2^*) \cong \mathrm{Ext}^1(1 + 4\mathbb{Z}_2, \mu_2 \times \mathbb{Z}_2^*) = 0.$$

Let $i : \mu_2 \to \mathbb{Z}_2^*$ be the inclusion map. It follows from the equation above that $\mathrm{Ext}^1(\mathrm{id}, p_1)$ and $\mathrm{H}^2(\mathrm{id}, p_1)$ are isomorphisms with inverses $\mathrm{Ext}^1(\mathrm{id}, i)$ and $\mathrm{H}^2(\mathrm{id}, i)$ respectively. Consider the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \times \mathbb{Z}_2^* \arrow[r, "t"] & I_2' \arrow[r, "u"] & \mathbb{Z}_2^* \arrow[r] & 1 \\
1 \arrow[r] & \mu_2 \times \mathbb{Z}_2^* \arrow[r] \arrow[u, "\mathrm{id}"] \arrow[d, "\mathrm{id}"'] & \mu_2 \times \sqrt{1+4\mathbb{Z}_2} \arrow[r, "\alpha"] \arrow[u] \arrow[d] & \mu_2 \arrow[r] \arrow[u, "i"'] \arrow[d, "i"] & 1 \\
1 \arrow[r] & \mu_2 \times \mathbb{Z}_2^* \arrow[r, "t_2"] & J_2' \arrow[r, "u_2"] & \mathbb{Z}_2^* \arrow[r] & 1
\end{tikzcd}$$

where the unnamed maps are the inclusion maps, and where $\alpha(\varepsilon, x) = \varphi(x)/x$. Then it follows from Proposition 3.13 that $\mathrm{Ext}^1(p_i, \mathrm{id})[J_2']$ and $\mathrm{H}^2(p_i, \mathrm{id})[I_2']$ both equal the extension class of the middle short exact sequence in the diagram above. □

7.5 Maximal class-2 extension of $\mathbb{Q}$

In this section, we will describe $\mathrm{ret}[\Gamma] \in \mathrm{Ext}^1(\Gamma^{\mathrm{ab}}, \Gamma^{(2)})$ where Γ is the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cl2}}/\mathbb{Q})$ and where ret is a specific retraction of $\mathrm{Ext}^1(\Gamma^{\mathrm{ab}}, \Gamma^{(2)}) \to \mathrm{H}^2(\Gamma^{\mathrm{ab}}, \Gamma^{(2)})$. We describe this extension by using the local results, see Theorem 7.18 and Theorem 7.20, on the extension $[\Gamma_p] \in \mathrm{H}^2(\Gamma_p^{\mathrm{ab}}, \Gamma_p^{(2)})$ where Γ_p denotes the Galois group $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p)$ for a prime p. The description of $\mathrm{ret}[\Gamma]$ together with Proposition 5.9 will lead to a description of $[\Gamma] \in \mathrm{H}^2(\Gamma^{\mathrm{ab}}, \Gamma^{(2)})$.

We fix algebraic closures $\mathbb{Q}^{\mathrm{alg}}$ of $\mathbb{Q}$ and $\mathbb{Q}_p^{\mathrm{alg}}$ of $\mathbb{Q}_p$ for every prime p. Moreover, we fix an embedding $\mathbb{Q}^{\mathrm{alg}} \subset \mathbb{Q}_p^{\mathrm{alg}}$ for every prime p. By standard Galois theory, for every finite Galois extension $L/\mathbb{Q}$ with $L \subset \mathbb{Q}^{\mathrm{alg}}$, the extension $L\mathbb{Q}_p/\mathbb{Q}_p$ is Galois, and restriction to L gives a natural injective homomorphism $\mathrm{Gal}(L\mathbb{Q}_p/\mathbb{Q}_p) \to \mathrm{Gal}(L/\mathbb{Q})$. Hence, we have $\mathbb{Q}^{\mathrm{ab}} \subset \mathbb{Q}_p^{\mathrm{ab}}$ and $\mathbb{Q}^{\mathrm{cl2}} \subset \mathbb{Q}_p^{\mathrm{cl2}}$. For every prime p we get a Hasse diagram as in Figure 3.

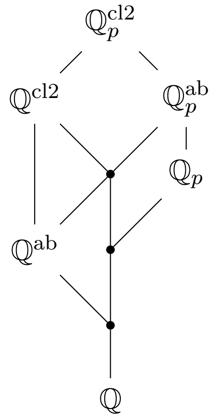

$\mathbb{Q}_p^{\mathrm{cl2}}$
$\mathbb{Q}^{\mathrm{cl2}}$
$\mathbb{Q}_p^{\mathrm{ab}}$
$\mathbb{Q}_p$
$\mathbb{Q}^{\mathrm{ab}}$
$\mathbb{Q}$

Figure 3: Hasse diagram where each unnamed field is the intersection of its parent fields.

Notice that the restriction to $\mathbb{Q}^{\mathrm{cl2}}$ gives a natural homomorphism $r_p : \Gamma_p \to \Gamma$ that maps onto the decomposition group of Γ corresponding to the valuation $|-|_p$ on $\mathbb{Q}^{\mathrm{cl2}}$ induced by $\mathbb{Q}^{\mathrm{alg}} \subset \mathbb{Q}_p^{\mathrm{alg}}$. It is clear that $r_p[\Gamma_p^{(2)}] \subset \Gamma^{(2)}$. Let $r_p^{\mathrm{ab}} : \Gamma_p^{\mathrm{ab}} \to \Gamma^{\mathrm{ab}}$ and $r_p^{(2)} : \Gamma_p^{(2)} \to \Gamma^{(2)}$ be the homomorphisms induced by r_p. We write $I_p := \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}_p^{\mathrm{unr}})$ and $B_p := \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{unr}})$. Then the diagram

$$\begin{tikzcd}
1 \arrow[r] & \Gamma_p^{(2)} \arrow[r] \arrow[d, "\mathrm{id}"] & I_p \arrow[r] \arrow[d, hook] & B_p \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & \Gamma_p^{(2)} \arrow[r] \arrow[d, "r_p^{(2)}"] & \Gamma_p \arrow[r] \arrow[d, "r_p"] & \Gamma_p^{\mathrm{ab}} \arrow[r] \arrow[d, "r_p^{\mathrm{ab}}"] & 1 \\
1 \arrow[r] & \Gamma^{(2)} \arrow[r] & \Gamma \arrow[r] & \Gamma^{\mathrm{ab}} \arrow[r] & 1
\end{tikzcd}$$

Figure 4: relation local and global extensions.

commutes. By the Global Class Field Theorem we have a commutative diagram

$$\begin{tikzcd}
\widehat{\mathbb{Q}_p^*} \arrow[r, "\sim", "A_p"'] \arrow[d, tail, "\kappa_p"] & \Gamma_p^{\mathrm{ab}} \arrow[d, "r_p^{\mathrm{ab}}"] \\
\widehat{\mathbb{Z}}^* \arrow[r, "\sim", "A"'] & \Gamma^{\mathrm{ab}}
\end{tikzcd}$$

with the horizontal isomorphisms the global and local Artin maps which we denote by $A : \widehat{\mathbb{Z}}^* \to \Gamma^{\mathrm{ab}}$ and $A_p : \widehat{\mathbb{Q}_p^*} \to \Gamma_p^{\mathrm{ab}}$ respectively, and with κ_p the injective morphism

$$\mathbb{Z}_p^* \times p^{\widehat{\mathbb{Z}}} \longrightarrow \prod_q \mathbb{Z}_q^*, \quad (u, p^n) \longmapsto (x_q)_q, \text{ where } \quad x_q = \begin{cases} u & \text{if } q = p, \\ p^{-n} & \text{if } q \neq p. \end{cases}$$

By the Local Class Field Theorem we have $A_p[\mathbb{Z}_p^*] = B_p$. Hence, we can view $[I_p]$, $[\Gamma_p]$, $[\Gamma]$ as elements of $\mathrm{H}^2(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$, $\mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$, $\mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ respectively, via the isomorphisms $\mathrm{H}^2(A_p|_{\mathbb{Z}_p^*}, ([-,-] \bigwedge^2 A_p)^{-1})$, $\mathrm{H}^2(A_p, ([-,-] \bigwedge^2 A_p)^{-1})$, $\mathrm{H}^2(A, ([-,-] \bigwedge^2 A)^{-1})$ respectively, where $[-,-]$ is the commutator map from Remark 6.1.

By Lemma 4.12 we have

$$\bigwedge^2 \widehat{\mathbb{Z}}^* \cong (\bigwedge^2 \mathbb{Z}_2^*) \times \prod_{2 \leq p < q} \mathbb{Z}_p^* \otimes \mathbb{Z}_q^*$$

and thus $\bigwedge^2 \widehat{\mathbb{Z}}^*$ is the product of finite groups. By Proposition 5.5, viewing $\widehat{\mathbb{Z}}^*$ as a product $\{\pm 1\} \times (1 + 4\mathbb{Z}_2) \times \prod_{p>2} \mathbb{Z}_p^*$ of procyclic groups gives a retraction

$$\mathrm{ret} : \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*) \to \mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$$

of the inclusion map $\mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*) \to \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$. Moreover, this same factorization of $\widehat{\mathbb{Z}}^*$ yields an explicit profinite group Γ_0 with $[\Gamma_0] \in \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ such that $\mathrm{cp}[\Gamma_0] = \mathrm{id}$ and $\mathrm{ret}[\Gamma_0] = 0$, by Proposition 5.9. Similarly, for every prime p we get retractions

$$\mathrm{ret} : \mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*}) \to \mathrm{Ext}^1(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*}), \quad \mathrm{ret} : \mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Z}}^*) \to \mathrm{Ext}^1(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Z}}^*)$$

and

$$\mathrm{ret} : \mathrm{Ext}^1(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Q}_p^*}) \to \mathrm{H}^2(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Q}_p^*}), \quad \mathrm{ret} : \mathrm{Ext}^1(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Z}}^*) \to \mathrm{H}^2(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Z}}^*),$$

based on the factorization $\widehat{\mathbb{Q}_2^*} = \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \times 2^{\widehat{\mathbb{Z}}}$ for $p = 2$ and $\widehat{\mathbb{Q}_p^*} = \mathbb{Z}_p^* \times p^{\widehat{\mathbb{Z}}}$ for p odd.

Lemma 7.31. *We have* $[\Gamma] = \mathrm{ret}[\Gamma] + [\Gamma_0]$ *in* $\mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$.

Proof. We have $\mathrm{cp}[\Gamma] = \mathrm{id}$ by section 7.1. Hence, ret and cp map $\mathrm{ret}[\Gamma] + [\Gamma_0] - [\Gamma]$ to the zero element of $\mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ and $\mathrm{End}(\bigwedge^2 \widehat{\mathbb{Z}}^*)$ respectively. The result now follows from Proposition 5.6. □

The following lemma expresses $\mathrm{ret}[\Gamma]$ in terms of the local extensions $\mathrm{ret}[I_p]$. For every prime p, denote by ι_p the inclusion map $\mathbb{Z}_p^* \hookrightarrow \mathbb{Q}_p^*$.

Lemma 7.32. *The isomorphism* $\mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*) \to \prod_p' \mathrm{Ext}^1(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ *from Theorem 4.45 maps* $\mathrm{ret}[\Gamma]$ *to the element*

$$\big(\mathrm{Ext}^1(\mathbb{Z}_p^*, \bigwedge^2 \kappa_p)\,\mathrm{ret}[I_p]\big)_p \in \prod_p{}' \mathrm{Ext}^1(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Z}}^*).$$

Proof. From the commutative diagram in Figure 4 and Proposition 3.13, it follows that $\mathrm{H}^2(\iota_p, \mathrm{id})[\Gamma_p] = [I_p]$ and $\mathrm{H}^2(\kappa_p, \mathrm{id})[\Gamma] = \mathrm{H}^2(\mathrm{id}, \bigwedge^2 \kappa_p)[\Gamma_p]$. Now from the commutative diagram

$$\begin{tikzcd}
{[I_p] \in \mathrm{H}^2(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Q}_p^*})} \arrow[r, "\mathrm{H}^2(\mathrm{id}, \bigwedge^2 \kappa_p)"] & \mathrm{H}^2(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Z}}^*) \\
{[\Gamma_p] \in \mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*})} \arrow[u, "\mathrm{H}^2(\iota_p, \mathrm{id})"] \arrow[r, "\mathrm{H}^2(\mathrm{id}, \bigwedge^2 \kappa_p)"] & \mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Z}}^*) \arrow[u, "\mathrm{H}^2(\iota_p, \mathrm{id})"'] \\
{[\Gamma] \in \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)} \arrow[ur, "\mathrm{H}^2(\kappa_p, \mathrm{id})"'] &
\end{tikzcd}$$

we conclude that $\mathrm{H}^2(\kappa_p \iota_p, \mathrm{id})[\Gamma] = \mathrm{H}^2(\mathrm{id}, \bigwedge^2 \kappa_p)[I_p]$. From the naturality of the retraction maps ret as in Lemma 5.7, it follows that

$$\mathrm{Ext}^1(\kappa_p \iota_p, \mathrm{id})\,\mathrm{ret}[\Gamma] = \mathrm{Ext}^1(\mathrm{id}, \bigwedge^2 \kappa_p)\,\mathrm{ret}[I_p]. \qquad \square$$

We will now describe $\mathrm{ret}[I_p]$ for each prime p. Denote by μ_2 the subgroup $\{\pm 1\}$ of $\mathbb{Z}_2^*$. For $p = 2$ we consider the extension

$$1 \longrightarrow \mu_2 \times \mathbb{Z}_2^* \xrightarrow{t_2} J_2' \xrightarrow{u_2} \mathbb{Z}_2^* \longrightarrow 1,$$

as in Proposition 7.30, i.e., $J_2' = \mu_2 \times \sqrt{1 + 4\mathbb{Z}_2} \times (1 + 4\mathbb{Z}_2)$ and $t_2(\varepsilon, x) = (\varepsilon, x, 1)$ and $u_2(\varepsilon, x, y) = (\varphi(x)/x)y$. Then it follows from Proposition 7.30 that $\mathrm{ret}[I_2]$ equals $[J_2']$. For p odd we consider the exact sequence

$$1 \longrightarrow \mathbb{Z}_p^* \xrightarrow{t_p} I_p' \xrightarrow{u_p} \mathbb{Z}_p^* \longrightarrow 1$$

as in Theorem 7.18, i.e., $I_p' = (1 + p\mathbb{Z}_p) \times \mu_{(p-1)^2} \times (1 + p\mathbb{Z}_p)$ and if we identify $\mathbb{Z}_p^*$ with $(1 + p\mathbb{Z}_p) \times \mathbb{F}_p^*$, then $t_p(x, \zeta) = (x, \zeta, 1)$ and $u_p(x, \zeta, y) = (y, \zeta^{p-1})$. It follows from Theorem 7.18 that $\mathrm{ret}[I_p]$ equals $[I_p']$ since I_p' is abelian. In order to unify notation, we write $J_p' := I_p'$ for p odd.

We will now construct an extension $[P] \in \mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$, and we will show in Theorem 7.33 the equality $[P] = \mathrm{ret}[\Gamma]$. Let $h_2 : \bigwedge^2 \widehat{\mathbb{Q}_2^*} \to \mu_2 \times \mathbb{Z}_2^*$ be the isomorphism induced by the isomorphism

$$\bigwedge^2 \widehat{\mathbb{Q}_2^*} \xrightarrow{\sim} \big(\bigwedge^2 \mathbb{Z}_2^*\big) \times (\mathbb{Z}_2^* \otimes \widehat{\mathbb{Z}})$$

from Lemma 4.12 with $\widehat{\mathbb{Q}_2^*} = \mathbb{Z}_2^* \times 2^{\widehat{\mathbb{Z}}}$. For odd p, we let $h_p : \bigwedge^2 \widehat{\mathbb{Q}_p^*} \to \mathbb{Z}_p^*$ be the canonical isomorphism from Example 4.16. Let $h : \prod_p \bigwedge^2 \widehat{\mathbb{Q}_p^*} \to \mu_2 \times \widehat{\mathbb{Z}}^*$ be the isomorphism induced by the isomorphisms h_p. Write $J' := \times \prod_p J'_p$. By Lemma 4.1 the maps t_p and u_p and $\bigwedge^2 \kappa_p$ induce maps

$$\begin{aligned} t := (t_p)_p : &\qquad \mu_2 \times \widehat{\mathbb{Z}}^* \to J', \\ u := (u_p)_p : &\qquad J' \to \widehat{\mathbb{Z}}^*, \\ \bigwedge^2 \kappa := (\bigwedge^2 \kappa_p)_p \circ h^{-1} : &\qquad \mu_2 \times \widehat{\mathbb{Z}}^* \to \bigwedge^2 \widehat{\mathbb{Z}}^*. \end{aligned}$$

For example, for $\bigwedge^2 \kappa$ this follows because for each odd prime p the composition

$$\mathbb{Z}_p^* \xrightarrow{h_p^{-1}} \bigwedge^2 \mathbb{Q}_p^* \xrightarrow{\bigwedge^2 \kappa_p} \bigwedge^2 \prod_q \mathbb{Z}_q^* \xrightarrow{\text{quotient map}} \bigwedge^2 \prod_q (\mathbb{Z}_q^*/N_q)$$

is trivial if $N_p = \mathbb{Z}_p^*$, where $N_q \subset \mathbb{Z}_q^*$ is an open subgroup for each q. The pushout $P := \bigwedge^2 \widehat{\mathbb{Z}}^* \sqcup_{\mu_2 \times \widehat{\mathbb{Z}}^*} J'$ of t and $\bigwedge^2 \kappa$ gives a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \times \widehat{\mathbb{Z}}^* \arrow[r, "t"] \arrow[d, "\bigwedge^2 \kappa"] & J' \arrow[r, "u"] \arrow[d] & \widehat{\mathbb{Z}}^* \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & \bigwedge^2 \widehat{\mathbb{Z}}^* \arrow[r] & P \arrow[r] & \widehat{\mathbb{Z}}^* \arrow[r] & 1
\end{tikzcd}$$

and we consider the bottom extension class $[P] \in \mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$.

Theorem 7.33. *In* $\mathrm{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ *we have* $\mathrm{ret}[\Gamma] = [P]$.

Proof. Recall that for any prime p we have $\mathrm{ret}[I_p] = [J'_p]$. By Lemma 7.32 it thus suffices to show that for all primes p we have $\mathrm{Ext}^1(\kappa_p \iota_p, \mathrm{id})[P] = \mathrm{Ext}^1(\mathrm{id}, \bigwedge^2 \kappa_p)[J'_p]$. Let p be a prime number. We denote by j_p the composition $\bigwedge^2 \widehat{\mathbb{Q}_p^*} \overset{h_p}{\to} \mathrm{im}(h_p) \hookrightarrow \mu_2 \times \widehat{\mathbb{Z}}^*$. The extension class $\mathrm{Ext}^1(\kappa_p \iota_p, \mathrm{id})[P]$ is induced by the pullback $Q := \mathbb{Z}_p^* \times_{\widehat{\mathbb{Z}}^*} P$ of $\kappa_p \iota_p$ and $P \to \widehat{\mathbb{Z}}^*$: it is the class of the bottom row of the following commutative diagram.

$$\begin{tikzcd}
1 \arrow[r] & \bigwedge^2 \widehat{\mathbb{Q}_p^*} \arrow[r, "t_p"] \arrow[d, "j_p"] & J'_p \arrow[r, "u_p"] \arrow[d, hook] & \mathbb{Z}_p^* \arrow[r] \arrow[d, "\kappa_p \iota_p"] & 1 \\
1 \arrow[r] & \mu_2 \times \widehat{\mathbb{Z}}^* \arrow[r, "t"] \arrow[d, "\bigwedge^2 \kappa"] & J' \arrow[r, "u"] \arrow[d] & \widehat{\mathbb{Z}}^* \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & \bigwedge^2 \widehat{\mathbb{Z}}^* \arrow[r] & P \arrow[r] & \widehat{\mathbb{Z}}^* \arrow[r] & 1 \\
1 \arrow[r] & \bigwedge^2 \widehat{\mathbb{Z}}^* \arrow[r] \arrow[u, "\mathrm{id}"] & Q \arrow[r] \arrow[u] & \mathbb{Z}_p^* \arrow[r] \arrow[u, "\kappa_p \iota_p"'] & 1
\end{tikzcd}$$

Applying Proposition 3.13 to this diagram yields the relations

$$\mathrm{Ext}^1(\mathrm{id}, j_p)[J'_p] = \mathrm{Ext}^1(\kappa_p \iota_p, \mathrm{id})[J'], \quad \mathrm{Ext}^1(\mathrm{id}, \bigwedge^2 \kappa)[J'] = [P], \quad \mathrm{Ext}^1(\kappa_p \iota_p, \mathrm{id})[P] = [Q].$$

Using $\bigwedge^2 \kappa_p = (\bigwedge^2 \kappa) j_p$, we now conclude that

$$\mathrm{Ext}^1(\mathrm{id}, \bigwedge \kappa_p)[J'_p] = \mathrm{Ext}^1(\kappa_p \iota_p, \bigwedge^2 \kappa)[J'] = \mathrm{Ext}^1(\kappa_p \iota_p, \mathrm{id})[P] = [Q]. \qquad \square$$

We can now fully describe Γ.

Theorem 7.34. $[\Gamma] \in \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ *is the Baer sum of* $[P]$ *and* $[\Gamma_0]$.

Proof. This follows from Lemma 7.31 and Theorem 7.33. □

7.6 Decomposition groups in global class-2 group

In this section we will use the same notation and conventions as in section 7.5. As in section 7.5, we denote for any prime p by r_p the map $\Gamma_p \to \Gamma$ that restricts automorphisms in Γ_p to $\mathbb{Q}^{\mathrm{cl2}} \subset \mathbb{Q}_p^{\mathrm{cl2}}$. The goal of this section is to prove the following theorem, which states that the decomposition group Γ_p of every prime p is mapped injectively to Γ by r_p. Notice that for any prime p the map r_p is injective if and only if $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cl2}}/\mathbb{Q}^{\mathrm{cl2}}\mathbb{Q}_p)$ is trivial, i.e., if and only if $\mathbb{Q}^{\mathrm{cl2}}\mathbb{Q}_p = \mathbb{Q}_p^{\mathrm{cl2}}$.

Theorem 7.35. *For every prime p, the map $r_p : \Gamma_p \to \Gamma$ is injective.*

Let p be a prime. We remark that $r_p^{\mathrm{ab}} : \Gamma_p^{\mathrm{ab}} \to \Gamma^{\mathrm{ab}}$ from section 7.5 is injective by class field theory. From Figure 4 in section 7.5 it follows that r_p is injective if and only if $r_p^{(2)} : \Gamma_p^{(2)} \to \Gamma^{(2)}$ is injective. Hence, the decomposition group Γ_p is mapped injectively to Γ by r_p if and only if $\bigwedge^2 \kappa_p : \bigwedge^2 \widehat{\mathbb{Q}_p^*} \to \bigwedge^2 \widehat{\mathbb{Z}}^*$ is injective, where $\kappa_p : \widehat{\mathbb{Q}_p^*} \to \widehat{\mathbb{Z}}^*$ is the morphism as defined in section 7.5.

Lemma 7.36. *Let p be a prime number. Then r_p is injective if and only if for each non-trivial $x \in \mathbb{Z}_p^*$ there exists a prime $q \neq p$ such that $x \otimes p \in \mathbb{Z}_p^* \otimes \mathbb{Z}_q^*$ is non-zero.*

Proof. As noticed before this lemma, r_p is injective if and only if $\bigwedge^2 \kappa_p : \bigwedge^2 \widehat{\mathbb{Q}_p^*} \to \bigwedge^2 \widehat{\mathbb{Z}}^*$ is injective. By writing $\widehat{\mathbb{Z}}^* \cong \prod_q \mathbb{Z}_q^*$, Lemma 4.12 yields an isomorphism

$$\psi_1 : \bigwedge^2 \widehat{\mathbb{Z}}^* \xrightarrow{\sim} \Big(\bigwedge^2 \mathbb{Z}_2^*\Big) \times \prod_{2 \le q_1 < q_2} \mathbb{Z}_{q_1}^* \otimes \mathbb{Z}_{q_2}^*.$$

We also consider the morphism of profinite groups

$$\psi_2 : \mathbb{Z}_p^* \to \bigwedge^2 \widehat{\mathbb{Q}_p^*}, \quad x \mapsto p \wedge x,$$

which is an isomorphism if p is odd by Example 4.16. It can be easily verified that $\bigwedge^2 \kappa_p$ is injective if and only if $\psi := \psi_1(\bigwedge^2 \kappa_p)\psi_2$ is injective. Notice that ψ is given by

$$x \longmapsto (0, (a_{q_1,q_2})_{2 \le q_1 < q_2}), \quad \text{where} \quad a_{q_1,q_2} = \begin{cases} p^{-1} \otimes x & \text{if } q_1 \neq p \text{ and } q_2 = p, \\ x \otimes p & \text{if } q_1 = p \text{ and } q_2 \neq p, \\ 0 & \text{else.} \end{cases}$$

The result follows. □

For any prime q we write

$$q_* := \begin{cases} q & \text{if } q > 2, \\ 4 & \text{if } q = 2. \end{cases}$$

Denote by $\phi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ Euler's totient function. For any prime q and any non-zero integer x we denote by $\mathrm{ord}_q(x)$ the largest $n \in \mathbb{Z}_{\geq 0}$ such that q^n divides x.

Lemma 7.37. *Let p be a prime number. For any odd prime $q \neq p$ we denote by d_q the order of $p \bmod q_*$ in $(\mathbb{Z}/q_*\mathbb{Z})^*$. Suppose that the following two statements are true:*

(i) *for any integer $N > 0$ there exists a prime $q \neq p$ such that $\mathrm{ord}_p(d_q) > N$,*

(ii) *for any prime divisor r of $\phi(p_*)$ there exists a prime $q \neq p$ such that*

$$\mathrm{ord}_r(d_q) = \mathrm{ord}_r(\phi(q_*)) \geq \mathrm{ord}_r(\phi(p_*)).$$

Then the map $r_p : \Gamma_p \to \Gamma$ is injective.

Proof. For every q we have $\mathbb{Z}_q^* = (1 + q_*\mathbb{Z}_q) \times (\mathbb{Z}/q_*\mathbb{Z})^*$. Let $x \in \mathbb{Z}_p^*$. The result follows straightforwardly from Lemma 7.36 by examining for every prime $q \neq p$ the projection of $x \otimes p \in \mathbb{Z}_p^* \otimes \mathbb{Z}_q^*$ to $(1 + p_*\mathbb{Z}_p) \otimes (\mathbb{Z}/q_*\mathbb{Z})^*$ and to $(\mathbb{Z}/p_*\mathbb{Z})^* \otimes (\mathbb{Z}/q_*\mathbb{Z})^*$. □

Now we will prove Theorem 7.35 by using Chebotarev's density theorem, see [10, Ch. 8.4, Thm. 10].

Proof Theorem 7.35. Let p be a prime. We will prove (i) and (ii) of Lemma 7.37.

(i) Let $N > 0$ be an integer. Let $L \geq 3$ and $M > L + N$ be integers. Let $q > 2$ be a prime that does not divide the discriminant $\Delta(X^{p^L} - p)$ and note that $q \neq p$. Then $\mathrm{ord}_p(d_q) > N$ holds if $p^M \mid q - 1$ and $p^L \nmid (\mathbb{F}_q^* : \langle p \mod q \rangle)$, i.e., if q splits completely in $\mathbb{Q}(\zeta_{p^M})$ yet does not split completely in $\mathbb{Q}(\sqrt[p^L]{p})$, where ζ_{p^M} is a primitive root of $X^{p^M} - 1$ in $\mathbb{Q}^{\mathrm{alg}}$ and $\sqrt[p^L]{p}$ is a root of $X^{p^L} - p$ in $\mathbb{Q}^{\mathrm{alg}}$. By Schinzel's Theorem [13, Thm. 2], for a field K, an integer $n > 0$ that is not divisible by the characteristic of K, and any $a \in K$, the Galois group of $X^n - a$ over K is abelian if and only if there exists $b \in K$ such that $a^w = b^n$, where w is the number of n^{th} roots of unity in K. Since $L \geq 3$, it follows that the normal closure of $\mathbb{Q}(\sqrt[p^L]{p})/\mathbb{Q}$ is a non-abelian Galois extension of $\mathbb{Q}$. Therefore, the field $\mathbb{Q}(\zeta_{p^M}, \sqrt[p^L]{p})$ is strictly larger than $\mathbb{Q}(\zeta_{p^M})$.

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{p^M}, \sqrt[p^L]{p}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[p^L]{p}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{p^M}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

By a special case of the Chebotarev's density theorem [10, Ch. 8.4] the natural density of the primes q that split completely in a finite Galois extension $K/\mathbb{Q}$ equals $1/[K : \mathbb{Q}]$. It follows that there exist infinitely many primes q that are completely split in $\mathbb{Q}(\zeta_{p^M})$ yet not completely split in $\mathbb{Q}(\zeta_{p^M}, \sqrt[p^L]{p})$, and each such q is not completely split in $\mathbb{Q}(\sqrt[p^L]{p})$. This proves (i).

(ii) Let r be a prime divisor of $\phi(p_*)$. We translate the conditions of (ii) to splitting behaviour of primes in algebraic number fields. Let $q > 2$ be a prime that does not divide the discriminant $\Delta(X^r - p)$ and note that $q \neq p$. Write $k := \mathrm{ord}_r(\phi(p_*))$, and let $\sqrt[r]{p}$ and ζ_{r^k} be roots of $X^r - p$ and $X^{r^k} - 1$ in $\mathbb{Q}^{\mathrm{alg}}$ respectively with ζ_{r^k} primitive. Then we have $\mathrm{ord}_r(d_q) = \mathrm{ord}_r(q - 1)$ if and only if $p \mod q$ is not an r^{th} power in $\mathbb{F}_q^*$, i.e., if and only if q is not completely split in $\mathbb{Q}(\sqrt[r]{p})$. We also have $\mathrm{ord}_r(q-1) \geq \mathrm{ord}_r(\phi(p_*))$ if and only if q splits completely in $\mathbb{Q}(\zeta_{r^k})$. Since p ramifies in $\mathbb{Q}(\sqrt[r]{p})$ and does not ramify in $\mathbb{Q}(\zeta_{r^k})$, it follows that we have $\mathbb{Q}(\zeta_{r^k}) \subsetneq \mathbb{Q}(\zeta_{r^k}, \sqrt[r]{p})$. Hence, by Chebotarev's density theorem, there exist infinitely many primes q that are completely split in $\mathbb{Q}(\zeta_{r^k})$ yet not completely split in $\mathbb{Q}(\zeta_{r^k}, \sqrt[r]{p})$, and each such q is not completely split in $\mathbb{Q}(\sqrt[r]{p})$.

We now conclude that r_p is injective by Lemma 7.37. □

7.7 Descriptions Ext-part with cocycles

With the theory from section 3.4 and the previous sections of chapter 7, we can express the maximal class-2 extension of $\mathbb{Q}$ and $\mathbb{Q}_p$ also in terms of cocycle classes. This description depends on the choice of generators of $\mathbb{F}_p^*$ for each odd prime p. We will use the same notation as in all of section 7.5.

For every prime $p > 2$, let α_p be a generator of $\mathbb{F}_p^*$, and let $\alpha_2 \in (1 + 4\mathbb{Z}_2)\backslash(1 + 8\mathbb{Z}_2)$. Naturally, we can view α_p as an element of $\mathbb{Z}_p^*$ for all primes p since $\mathbb{F}_p^* \subset \mathbb{Z}_p^*$. For every prime $p > 2$, we consider the map

$$\begin{aligned} \nu_p : \widehat{\mathbb{Q}_p^*} &\to \{0, \ldots, p-2\} \\ p^{\widehat{\mathbb{Z}}} \times (1 + p\mathbb{Z}_p) \times \mathbb{F}_p^* \ni (p^m, x, \alpha_p^n) &\mapsto n, \quad \text{where } n \in \{0, \ldots, p-2\} \end{aligned}$$

which depends on the choice of α_p. Moreover, for $p = 2$ we consider the map

$$\begin{aligned} \nu_2 : \mathbb{Q}_2^* &\to \{0, 1\} \\ 2^{\widehat{\mathbb{Z}}} \times (1 + 4\mathbb{Z}_2) \times \{\pm 1\} \ni (m, x, (-1)^n) &\mapsto n, \quad \text{where } n \in \{0, 1\}. \end{aligned}$$

As in section 7.5, we view $[I_p]$, $[\Gamma_p]$ and $[\Gamma]$ as elements of $\mathrm{H}^2(\mathbb{Z}_p^*, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$, $\mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$, $\mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ respectively. We consider the same isomorphisms $h_p : \bigwedge^2 \mathbb{Q}_p^* \to \mathbb{Z}_p^*$ for all odd primes p and isomorphism $h_2 : \bigwedge^2 \mathbb{Q}_2^* \to \{\pm 1\} \times \mathbb{Z}_2^*$ as in section 7.5. For any prime $p > 2$ we write $p_* := p$ and we write $2_* := 4$. Denote by $\phi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ Euler's totient function.

Theorem 7.38. *Let p be a prime. Then*

$$\begin{aligned} \omega_p : \widehat{\mathbb{Q}_p^*} \times \widehat{\mathbb{Q}_p^*} &\to \bigwedge^2 \widehat{\mathbb{Q}_p^*} \\ (x, y) &\mapsto \begin{cases} p \wedge \alpha_p & \text{if } \nu_p(x) + \nu_p(y) \geq \phi(p_*), \\ 1 & \text{if } \nu_p(x) + \nu_p(y) < \phi(p_*) \end{cases} \end{aligned}$$

is a continuous cocycle, and $\mathrm{ret}[\Gamma_p] \in \mathrm{Ext}^1(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$ *corresponds via Proposition 3.10 to the cocycle class* $[\omega_p]$.

Proof. We only prove the theorem for p odd. For $p = 2$ this follows similarly from Theorem 7.20. Consider $I_p' = (1 + p\mathbb{Z}_p) \times \mu_{(p-1)^2} \times (1 + p\mathbb{Z}_p)$ and $\Gamma_p'' = I_p' \times \widehat{\mathbb{Z}}$. Let ψ be the isomorphism $\mathbb{Z}_p^* \times \widehat{\mathbb{Z}} \to \widehat{\mathbb{Q}_p^*}$, $(a, n) \mapsto ap^n$. Using Theorem 7.18 it can be routinely verified that $\mathrm{Ext}^1(\psi, h_p)\,\mathrm{ret}[\Gamma_p]$ is the class of the extension

$$1 \to \mathbb{Z}_p^* \to \Gamma_p'' \to \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} \to 1$$

where the maps are given by

$$(1 + p\mathbb{Z}_p) \times \mathbb{F}_p^* \to \Gamma_p'', \quad (x, \zeta) \mapsto (x, \zeta, 1, 0)$$

and

$$\Gamma_p'' \to (1+p\mathbb{Z}_p) \times \mathbb{F}_p^* \times \widehat{\mathbb{Z}}, \quad (x, \zeta, y, m) \mapsto (\zeta, y, m).$$

Let $\beta_p \in \mu_{(p-1)^2}$ be such that $\beta_p^{p-1} = \alpha_p$. Then the map

$$\begin{gathered} s_p : \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} \to \Gamma_p'' \\ ((1+p\mathbb{Z}_p) \times \mathbb{F}_p^*) \times \widehat{\mathbb{Z}} \ni ((x, \alpha_p^n), m) \mapsto (1, \beta_p^n, x, m), \quad \text{where } n \in \{0, \dots, p-2\} \end{gathered}$$

is a continuous section of $\Gamma_p'' \to \mathbb{Z}_p^* \times \widehat{\mathbb{Z}}$, and we have $h_p \omega_p(\psi x, \psi y) = s_p(x) s_p(y) s_p(xy)^{-1}$ for all $x, y \in \widehat{\mathbb{Q}_p^*}$. □

We will now construct a cocycle class $[\omega]$ corresponding to $\operatorname{ret}[\Gamma] \in \operatorname{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ via Proposition 3.10. For every prime p, let $\omega_p : \widehat{\mathbb{Q}_p^*} \times \widehat{\mathbb{Q}_p^*} \to \bigwedge^2 \widehat{\mathbb{Q}_p^*}$ be the cocycle from Theorem 7.38, and let $\kappa_p : \mathbb{Q}_p^* \to \widehat{\mathbb{Z}}^*$ and $\iota_p : \mathbb{Z}_p^* \hookrightarrow \mathbb{Q}_p^*$ be as in section 7.5. For every prime p we write

$$\widetilde{\alpha_p} := (\bigwedge^2 \kappa_p)(p \wedge \alpha_p) = (x_q)_q \wedge (y_q)_q \in \bigwedge^2 \prod_q \mathbb{Z}_q^*, \quad \text{where}$$

$$x_q = \begin{cases} 1 & \text{if } q = p, \\ p^{-1} & \text{if } q \neq p, \end{cases} \quad \text{and} \quad y_q = \begin{cases} \alpha_p & \text{if } q = p, \\ 1 & \text{if } q \neq p. \end{cases}$$

Then for every prime p we have that $\omega_p' := \mathrm{Z}^2(\iota_p, \bigwedge^2 \kappa_p)(\omega_p)$ is the map

$$\omega_p' : \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \bigwedge^2 \widehat{\mathbb{Z}}^*, \quad (x, y) \mapsto \begin{cases} \widetilde{\alpha_p} & \text{if } \nu_p(x) + \nu_p(y) \geq p, \\ 1 & \text{if } \nu_p(x) + \nu_p(y) < p. \end{cases}$$

Theorem 7.39. *The map*

$$\begin{gathered} \omega : \widehat{\mathbb{Z}}^* \times \widehat{\mathbb{Z}}^* \to \bigwedge^2 \widehat{\mathbb{Z}}^* \\ \Big(\prod_p \mathbb{Z}_p^*\Big) \times \Big(\prod_p \mathbb{Z}_p^*\Big) \ni ((x_p)_p, (y_p)_p) \mapsto \prod_p \omega_p'(x_p, y_p) \end{gathered}$$

is a well-defined continuous cocycle, and $\operatorname{ret}[\Gamma] \in \operatorname{Ext}^1(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ *corresponds via Proposition 3.10 to the cocycle class* $[\omega]$.

Proof. From Lemma 4.1 it follows that ω is a well-defined continuous cocycle. It is clear that for every prime p we have $\operatorname{Ext}^1(\mathrm{id}, \kappa_p \iota_p)[\omega] = \operatorname{Ext}^1(\iota_p, \bigwedge^2 \kappa_p)[\omega_p]$. Since $\operatorname{ret}[I_p]$ corresponds to $\operatorname{Ext}^1(\iota_p, \mathrm{id})[\omega_p]$ by Theorem 7.38, we now conclude by Lemma 7.32 that $\operatorname{ret}[\Gamma]$ corresponds to $[\omega]$. □

The descriptions of the cocycle classes corresponding to $\operatorname{ret}[\Gamma_p]$ and $\operatorname{ret}[\Gamma]$ yield descriptions of the extension classes $[\Gamma_p] \in \mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$ and $[\Gamma] \in \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$, as we will state in the next theorem. By Proposition 5.9 the factorizations

$$\widehat{\mathbb{Q}_2^*} = \mu_2 \times (1 + 4\mathbb{Z}_2) \times 2^{\widehat{\mathbb{Z}}}, \quad \widehat{\mathbb{Q}_p^*} = \mathbb{Z}_p^* \times p^{\widehat{\mathbb{Z}}} \text{ for } p > 2, \quad \widehat{\mathbb{Z}}^* = \mu_2 \times (1 + 4\mathbb{Z}_2) \times \prod_{p>2} \mathbb{Z}_p^*,$$

yield cocycles

$$\theta_2 : \widehat{\mathbb{Q}_2^*} \times \widehat{\mathbb{Q}_2^*} \to \bigwedge^2 \widehat{\mathbb{Q}_2^*}, \qquad \theta_p : \widehat{\mathbb{Q}_p^*} \times \widehat{\mathbb{Q}_p^*} \to \bigwedge^2 \widehat{\mathbb{Q}_p^*} \quad \text{for } p > 2, \qquad \theta : \widehat{\mathbb{Z}}^* \times \widehat{\mathbb{Z}}^* \to \bigwedge^2 \widehat{\mathbb{Z}}^*$$

respectively, and they are such that applying the isomorphisms $(\operatorname{ret}, \operatorname{cp})$ to any of the corresponding cocycle classes yields $(0, \mathrm{id})$ as in Proposition 5.9. For any prime p we consider the cocycle ω_p as in Theorem 7.38, and we also consider the cocycle ω as in Theorem 7.39.

Theorem 7.40. *We have the following correspondences between extension classes and cocycle classes via Proposition 3.10.*

(i) *For any prime p the extension class $[\Gamma_p] \in \mathrm{H}^2(\widehat{\mathbb{Q}_p^*}, \bigwedge^2 \widehat{\mathbb{Q}_p^*})$ corresponds to the cocycle class $[\omega_p + \theta_p]$.*

(ii) *The extension class $[\Gamma] \in \mathrm{H}^2(\widehat{\mathbb{Z}}^*, \bigwedge^2 \widehat{\mathbb{Z}}^*)$ corresponds to the cocycle class $[\omega + \theta]$.*

References

[1] G.W. Anderson. Kronecker-Weber plus epsilon. *Duke Mathematical Journal*, 114(3):439–475, 2002.

[2] N. Bourbaki. *Éléments de mathématique: Algèbre commutative.* Springer, 2006.

[3] K.S. Brown. *Cohomology of groups*, volume 87. Springer Science & Business Media, 2012.

[4] H. Cartan and S. Eilenberg. *Homological algebra*, volume 41. Princeton University Press, 1999.

[5] J.W.S. Cassels and A. Fröhlich. *Algebraic number theory: proceedings of an instructional conference.* Academic Press, 1967.

[6] A. Fröhlich. *Central extensions, Galois groups, and ideal class groups of number fields*, volume 24. American Mathematical Society Providence, RI, 1983.

[7] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 165. Cambridge University Press, 2017.

[8] A. Javanpeykar. Radical Galois groups and cohomology. Master's thesis, Master's thesis. Universiteit Leiden, `https://www.math.leidenuniv.nl/scripties/1MasterJavanpeykar.pdf`, 2013.

[9] T. Jech. *Set theory.* Springer Science & Business Media, 2013.

[10] S. Lang. *Algebraic number theory*, volume 110. Springer Science & Business Media, 2013.

[11] L. Ribes and P. Zalesskii. Profinite groups. In *Profinite Groups*, pages 19–77. Springer, 2000.

[12] J.J. Rotman. *An introduction to homological algebra.* Springer Science & Business Media, 2008.

[13] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arithmetica*, 32(3):245–274, 1977.

[14] J.-P. Serre. Modular forms of weight one and Galois representations, algebraic number fields: L-functions and Galois properties (proc. sympos., univ. durham, durham, 1975), 1977.

[15] J.-P. Serre. *Cohomologie galoisienne*, volume 5. Springer Science & Business Media, 1994.

[16] J.-P. Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.

[17] C.A. Weibel. *An introduction to homological algebra*. Number 38 in Cambridge studies in advanced mathematics. Cambridge University Press, 1995.

[18] J.S. Wilson. *Profinite groups*, volume 19. Clarendon Press, 1998.