Division points in arithmetic

Javan Peykar, A.

CHAPTER 1

Radical Galois groups and cohomology

1. Introduction

Let K be a field of characteristic 0, and let $\overline{K}$ be an algebraic closure of K. Let μ be the subgroup of $\overline{K}^*$ consisting of all roots of unity. The maximal cyclotomic extension $K(\mu)$ is Galois over K, and we canonically identify its Galois group with a closed subgroup Γ_K of the group of units $\widehat{\mathbf{Z}}^*$ of the profinite completion $\widehat{\mathbf{Z}}$ of $\mathbf{Z}$.

Let, in general, Γ be a closed subgroup of $\widehat{\mathbf{Z}}^*$, and let A be a profinite abelian group. Then the natural $\widehat{\mathbf{Z}}$-module structure on A canonically induces an action of Γ on A, which we call the *natural action* of Γ on A. A short exact sequence

$$0 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} \Gamma \longrightarrow 1$$

in the category of profinite groups is called a *natural extension of* Γ *by* A or simply a *natural extension of* Γ if for all $x \in A$ and $\sigma \in G$ we have $\sigma f(x)\sigma^{-1} = f(g(\sigma) \cdot x)$, where $\cdot$ is the natural action of Γ on A.

Let W be a finitely generated subgroup of K^*. We call $\dim_{\mathbf{Q}}(W \otimes_{\mathbf{Z}} \mathbf{Q})$ the *rank* of W.

Let

$$W^{1/\infty} = \{x \in \overline{K}^* : x^m \in W \text{ for some } m \in \mathbf{Z}_{\geq 1}\}$$

be the group of all radicals of W, and note that $K(W^{1/\infty})$ is a Galois extension of K. In this chapter we study the structure of the Galois group of $K(W^{1/\infty})$ over K, and prove the following main theorem.

Theorem 1 (Main theorem)**.** *Let $n \in \mathbf{Z}_{\geq 0}$ and let F be a free $\widehat{\mathbf{Z}}$-module of rank n. Let G be a profinite group, and let K be a finite field extension of $\mathbf{Q}$. Then the following are equivalent.*

(a) *There exists a finitely generated subgroup W of K^* of rank n such that*

$$G \cong \mathrm{Gal}(K(W^{1/\infty})/K)$$

as profinite groups.

(b) *There is a natural extension of Γ_K*

$$0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1$$

such that if $K = \mathbf{Q}$, the image of F in G equals the algebraic commutator subgroup $[G, G]$ of G.

The case $n = 1$ over $K = \mathbf{Q}$ was the subject of the author's master's thesis, see [Jav13]. The special condition for $K = \mathbf{Q}$ was encountered already there. It is a condition entirely due to the theorem of Kronecker–Weber (see [Hil96]), which shows how number theory is involved in determining these Galois groups.

The (a) to (b) implication is a fairly easy consequence of Kummer theory and Schinzel's lemma, which we show in the next section.

The main tool in our proof of the inverse implication is the algebraic cohomology of topological groups acting continuously on topological modules, which one calls *continuous*

cochain cohomology. Given a topological group Γ and a topological Γ-module A, the *continuous cochain cohomology of* Γ *with coefficients in* A is the cohomology obtained from the complex

$$0 \longrightarrow A \xrightarrow{d_0} \mathrm{C}^1(\Gamma, A) \xrightarrow{d_1} \mathrm{C}^2(\Gamma, A) \xrightarrow{d_2} \mathrm{C}^3(\Gamma, A) \xrightarrow{d_3} \mathrm{C}^4(\Gamma, A) \xrightarrow{d_4} \dots$$

where for $n \in \mathbf{Z}_{\geq 1}$ the group $\mathrm{C}^n(\Gamma, A)$ consists of all continuous maps of

$$\Gamma^{\times n} = \underbrace{\Gamma \times \cdots \times \Gamma}_{n \text{ times}}$$

to A, and d_n is the standard coboundary map one also has in non-continuous group cohomology. For $n \in \mathbf{Z}_{\geq 0}$, we denote the cohomology groups of this complex by $\mathrm{H}^n(\Gamma, A)$. See section 1.3 for more details.

Now, let $n \in \mathbf{Z}_{\geq 0}$, let Γ be a closed subgroup of $\widehat{\mathbf{Z}}^*$, and let F be a free $\widehat{\mathbf{Z}}$-module of rank n. We define an equivalence relation on the collection of natural extensions of Γ by F (see 1.19), and find as in non-continuous group cohomology that the set of equivalence classes under this equivalence relation may be identified with $\mathrm{H}^2(\Gamma, F)$ (see 1.20). However, natural extensions of Γ by F that have isomorphic profinite groups in the middle, do not need to define the same element of $\mathrm{H}^2(\Gamma, F)$. To work around this, we consider the $\mathrm{Aut}(F)$-orbit of the equivalence class of a natural extension $0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma \longrightarrow 0$, which may be identified with the isomorphism class of G. The next theorem shows that the set of these orbits is in bijection with the set of subgroups of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$ that can be generated by n elements.

Theorem 2. *Let $n \in \mathbf{Z}_{\geq 0}$, let Γ be an open subgroup of $\widehat{\mathbf{Z}}^*$, and let F be a free $\widehat{\mathbf{Z}}$-module of rank n. Let S be the set of isomorphism classes of profinite groups G for which there exists a natural extension of Γ*

$$0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma \longrightarrow 1.$$

Let T be the set of subgroups of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$ that can be generated by n elements. Then there is a well-defined bijection of S with T that sends a class $[G] \in S$ to the image of the group morphism

$$\mathrm{CHom}(F, \widehat{\mathbf{Z}}) \longrightarrow \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}), \qquad f \mapsto \mathrm{H}^2(\Gamma, f)(E)$$

where $\mathrm{CHom}(F, \widehat{\mathbf{Z}})$ is the set of all continuous group morphisms from F to $\widehat{\mathbf{Z}}$, and $E \in \mathrm{H}^2(\Gamma, F)$ is the extension class of any natural extension $0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$.

For more details and the proof, see section 1.7 and section 1.8.

Our next step is to describe $\mathrm{H}^2(\Gamma_K, \widehat{\mathbf{Z}})$ in terms of the field K. An important auxiliary result is the following theorem, which has already been used in the rank 1 case over $\mathbf{Q}$ in [Jav13].

Theorem 3. *Let K be a number field, and let w be the number of roots of unity in K. Let A be a profinite abelian group. Then for any $m \in \mathbf{Z}_{\geq 0}$ we have*

$$w \cdot \mathrm{H}^m(\Gamma_K, A) = 0,$$

where Γ_K acts on A in the natural way.

See section 1.6 for more details.

Theorem 4. *Let K be a number field, let w be the number of roots of unity in K, and let μ_w denote the subgroup of K^* consisting of all roots of unity. Then the group $\mathrm{H}^2(\Gamma_K, \widehat{\mathbf{Z}})$ is isomorphic to*

$$\frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}}.$$

A more precise version of this theorem including a description of the isomorphism between the two groups is given in Theorem 1.34.

Using Theorems 2 and 4, we see that an extension of Γ_K as in part (b) of Theorem 1 corresponds to a subgroup H of $\frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}}$ that can be generated by n elements. The last step

in the proof of the (b) to (a) implication of Theorem 1 is to lift this subgroup to a subgroup W of K^*. Putting $M = K^*/\mu_w K^{*w}$ and $\Lambda = \frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}}$, the following theorem enables us to construct W in the case that K is unequal to $\mathbf{Q}$.

Theorem 5. *Let $w \in \mathbf{Z}_{>1}$, and let M be a free module over $\mathbf{Z}/w\mathbf{Z}$. Let Λ be a submodule of M, let $n \in \mathbf{Z}_{\geq 1}$, and let $H \subset \Lambda$ be a finite subgroup generated by at most n elements. Assume that the quotient group $M[p]/\Lambda[p]$ of the p-torsion parts of M and Λ is infinite for every prime p dividing w. Then there is a submodule I of M that is free over $\mathbf{Z}/w\mathbf{Z}$ of rank n such that $I \cap \Lambda = H$.*

For the proof see Theorem 1.39 in section 1.10. Note that we have

$$\frac{\mathbf{Q}(\mu)^{*2} \cap \mathbf{Q}^*}{\pm \mathbf{Q}^{*2}} = \mathbf{Q}^* / \pm \mathbf{Q}^{*2},$$

that is, we have $\Lambda = M$ for $K = \mathbf{Q}$. The restriction this puts on constructing W, in the case of $K = \mathbf{Q}$, translates into the extra condition in Theorem 1.

The present chapter is organized as follows.

In section 1.2 we prove the (a) to (b) implication of Theorem 1. In sections 1.3 and 1.4 we copy the definitions and theorems of continuous cochain cohomology and topological group extensions from [Jav13]. The proofs, which are omitted in this section, are found in [Jav13, Chapter 1]. In section 1.5 we prove a lemma in profinite group theory on natural extensions. In section 1.6 we elaborate on Theorem 3 above. Section 1.7 is concentrated on proving Theorem 2 above. Section 1.8 concerns the extended version of Theorem 4 above. In section 1.9 we study the image of $\mathrm{Gal}(K(W^{1/\infty})/K)$ under the bijection of Theorem 2. In section 1.10 we prove the lifting theorems, such as Theorem 5 above. The last section contains the proof of the main theorem.

2. Maximal radical extensions of number fields

Theorem 1.1 (Schinzel)**.** *Let K be a field, let $a \in K$, and let $n \in \mathbf{Z}_{>0}$ be not divisible by* $\mathrm{char}\, K$*. Let d be the number of n-th roots of unity in K. Then the splitting field of $X^n - a$ is abelian over K if and only if there exists $b \in K$ with $a^d = b^n$.*

Proof. See [Sch77, Theorem 2], [Len07] . ∎

Definition 1.2. For an abelian group W we write $\mathrm{rk}(W)$ for the *rank* $\dim_{\mathbf{Q}}(W \otimes_{\mathbf{Z}} \mathbf{Q})$ of W.

Let K be a field of characteristic 0, let $\overline{K}$ be an algebraic closure of K, and let W be a subgroup of K^*. Let

$$W^{1/\infty} = \{x \in \overline{K}^* : x^m \in W \text{ for some } m \in \mathbf{Z}_{\geq 1}\}$$

be the group of all radicals of W. The field $K(W^{1/\infty})$ is the union over all positive integers m of the Galois extensions $K(W^{1/m})$ of K where

$$W^{1/m} = \{x \in \overline{K}^* : x^m \in W\}.$$

Therefore, the field $K(W^{1/\infty})$ is Galois over K.

For a field L we write $\mu(L)$ for the subgroup of L^* consisting of the roots of unity of L^*. For simplicity we write μ for the subgroup $\mu(\overline{L})$ of $\overline{L}^*$ consisting of all roots of unity. For an integer $d \in \mathbf{Z}_{\geq 1}$ we write μ_d for the subgroup of μ consisting of the dth roots of unity.

The maximal cyclotomic extension $K(\mu)$ is Galois over K, and there is a canonical injection

$$\mathrm{Gal}(K(\mu)/K) \longrightarrow \mathrm{Aut}(\mu)$$

of profinite groups. Observe that $\mathrm{Aut}(\mu)$ is canonically isomorphic to $\widehat{\mathbf{Z}}^*$ as a profinite group. As $\mathrm{Gal}(K(\mu)/K)$ is compact and $\widehat{\mathbf{Z}}^*$ is Hausdorff, we may identify $\mathrm{Gal}(K(\mu)/K)$ with a

closed subgroup of $\widehat{\mathbf{Z}}^*$, which we denote by Γ_K. As $K(\mu)$ is clearly a subfield of $K(W^{1/\infty})$, we see that Γ_K is a quotient of $\mathrm{Gal}(K(W^{1/\infty})/K)$.

We write

$$\mathrm{Sat}(W) = W^{1/\infty} \cap K^*$$

and

$$\mathrm{Cyc}(W) = W^{1/\infty} \cap K(\mu)^*.$$

Proposition 1.3. *Let K be a number field, and let $\overline{K}$ be an algebraic closure of K. Let $w = \#\mu(K)$. Let K^{ab} be the maximal abelian extension of K inside $\overline{K}$.*

(a) *Then we have*

$$K^{*1/\infty} \cap K^{\mathrm{ab}\,*} = \mu \cdot K^{*1/w}.$$

(b) *Let W be a subgroup of K^*. Then*

$$\mathrm{Cyc}(W) = \mu \cdot (\mathrm{Sat}(W)^{1/w} \cap K(\mu)^*).$$

Proof. To prove (a), note that the right-to-left inclusion follows immediately from Kummer theory and the fact that cyclotomic extensions are abelian. For the left-to-right inclusion, let $\alpha \in K^{*1/\infty} \cap K^{\mathrm{ab}\,*}$. Then there is $n \in \mathbf{Z}_{\geq 1}$ such that $\alpha^n = a \in K^*$. As $X^n - a$ is abelian over K, by Theorem 1.1 there exists $b \in K^*$ such that $a^d = b^n$, where d is the number of n-th roots of unity in K. Then we have $\alpha = \zeta_{nd} b^{1/d}$, where ζ_{nd} is some nd-th root of unity. It follows that $\alpha \in \mu \cdot K^{*1/w}$, which shows the left-to-right inclusion.

For (b), intersect $K^{*1/\infty} \cap K^{\mathrm{ab}\,*} = \mu \cdot K^{*1/w}$ on both sides with $\mathrm{Cyc}(W)$ to obtain

$$\mathrm{Cyc}(W) = \left(\mu \cdot K^{*1/w}\right) \cap \mathrm{Cyc}(W).$$

As $\mu \subset \mathrm{Cyc}(W)$, it follows that

$$\mathrm{Cyc}(W) = \mu \cdot (\mathrm{Sat}(W)^{1/w} \cap K(\mu)^*)$$

as desired. ∎

Lemma 1.4. *Let K be a number field, and let W be a finitely generated subgroup of K^*. Let $n = \mathrm{rk}(W)$. Then the following statements hold.*

(a) *The group $\mathrm{Sat}(W)$ is finitely generated of rank n.*

(b) *The quotient $\mathrm{Cyc}(W)/\mu$ is free of rank n.*

Proof. Note that $\mathrm{Sat}(W)/W$ is equal to the torsion subgroup of K^*/W. By Lemma 3 in [Iwa53], there is a countably infinite index set I such that $K^* \cong \mu(K) \times \mathbf{Z}^{(I)}$. Moreover, there is a finite subset J of I such that W is contained in $\mu(K) \times \mathbf{Z}^{(J)}$. Then

$$K^* \cong \mu(K) \times \mathbf{Z}^{(J)} \oplus \mathbf{Z}^{(I \setminus J)}.$$

Hence, the torsion part of K^*/W is a finitely generated abelian group, which is therefore finite. As $\mathrm{Sat}(W)/W$ is finite, the group $\mathrm{Sat}(W)$ is finitely generated of rank n, which proves (a).

By Proposition 1.3 we have $\mathrm{Cyc}(W) = \mu \cdot (\mathrm{Sat}(W)^{1/w} \cap K(\mu)^*)$. Observe that $\mathrm{Sat}(W)^{1/w}$ is finitely generated, so

$$\mathrm{Sat}(W)^{1/w} \cap K(\mu)^* = \mathrm{Cyc}(W)/\mu$$

is also finitely generated. As the quotient $\mathrm{Cyc}(W)/(\mu \cdot \mathrm{Sat}(W))$ is finitely generated and annihilated by w, it follows that $\mathrm{Cyc}(W)/(\mu \cdot \mathrm{Sat}(W))$ is a finitely generated torsion group. Hence

$$\mathrm{Cyc}(W)/(\mu \cdot \mathrm{Sat}(W))$$

is finite, which implies that $\mathrm{Cyc}(W)/\mu$ is free of rank n. ∎

Recall that a topological module M over a topological ring R is an R-module M that is a topological group such that $R \times M \longrightarrow M$ is continuous, where $R \times M$ has the product topology. Similarly, a topological module M over a topological group Γ is a Γ-module M

that is a topological group such that $\Gamma \times M \longrightarrow M$ is continuous, where $\Gamma \times M$ has the product topology.

Let A be a profinite abelian group. Then by [Jav13, Lemma 2.3] A has a unique $\widehat{\mathbf{Z}}$-module structure, and it makes A into a topological $\widehat{\mathbf{Z}}$-module. We call this the *natural $\widehat{\mathbf{Z}}$-module structure* of A. By restriction, A has a topological Γ-action, for every closed subgroup Γ of $\widehat{\mathbf{Z}}^*$. For any such Γ, we call this the *natural action* of Γ on A.

Moreover, a short exact sequence $0 \longrightarrow A \xrightarrow{f} E \xrightarrow{g} \Gamma \longrightarrow 1$ of profinite groups where A is abelian and for all $\sigma \in E$ and $x \in A$ we have

$$\sigma f(x)\sigma^{-1} = f(g(\sigma) \cdot x)$$

with $\cdot$ the natural action, is called a *natural extension of Γ by A* or simply a *natural extension of Γ*.

Let K be a field, and $\overline{K}$ an algebraic closure of K. For every $k \in \mathbf{Z}_{\geq 1}$ let μ_k denote the group of all kth roots of unity in $\overline{K}^*$. Let $m \in \mathbf{Z}_{\geq 1}$, and note that for every multiple k of m, there is a group morphism $\mu_k \longrightarrow \mu_m$ sending $\zeta \in \mu_k$ to $\zeta^{k/m}$. This defines a projective system, of which the projective limit $\widehat{\mu}$ is called the *Tate module of the multiplicative group*. It is a profinite module over $\widehat{\mathbf{Z}}$ that is free of rank 1. For $\alpha \in \widehat{\mu}$ we let α_m denote its image in μ_m under the canonical projection $\widehat{\mu} \longrightarrow \mu_m$.

Theorem 1.5. *Let K be a field of characteristic 0, and let W be a finitely generated subgroup of K^*. Let $G = \mathrm{Gal}(K(W^{1/\infty})/K)$. Then there is a natural extension of Γ_K*

$$0 \longrightarrow \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) \xrightarrow{\iota} G \longrightarrow \Gamma_K \longrightarrow 1$$

such that for all $f \in \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})$, $x \in W^{1/\infty}$ and $m \in \mathbf{Z}_{\geq 1}$ with $x^m \in \mathrm{Cyc}(W)$ the Galois automorphism $\iota(f)$ satisfies

$$\iota(f)(x) = f(x^m)_m \cdot x.$$

Proof. By Galois theory, there is a natural extension of Γ_K

$$0 \longrightarrow \mathrm{Gal}(K(W^{1/\infty})/K(\mu)) \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1.$$

By Kummer theory, there is an isomorphism

$$\mathrm{Gal}(K(W^{1/\infty})/K(\mu)) \longrightarrow \mathrm{Aut}_{\mathrm{Cyc}(W)}(\mathrm{Cyc}(W)^{1/\infty})$$

of profinite groups that sends each σ to its restriction to $W^{1/\infty} = \mathrm{Cyc}(W)^{1/\infty}$. Moreover, there is an isomorphism

$$\mathrm{Aut}_{\mathrm{Cyc}(W)}(\mathrm{Cyc}(W)^{1/\infty}) \longrightarrow \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})$$

of profinite Γ_K-modules given by sending σ to the group morphism $\mathrm{Cyc}(W) \longrightarrow \widehat{\mu}$ that sends $x \in \mathrm{Cyc}(W)$ to $(\sigma(y_m)/y_m)_{m\geq 1}$ where $y_m \in \overline{K}^*$ are such that $y_m^m = x$ for every $m \in \mathbf{Z}_{\geq 0}$. As these isomorphisms are Γ_K-linear, composing their inverses gives the desired natural extension of Γ_K. ∎

Remark 1.6. Let K, W and n be as in Lemma 1.4. Then by Lemma 1.4 there are $t_1, \ldots, t_n \in K(\mu)^*$ such that $\mathrm{Cyc}(W) = \mu \cdot \langle t_1, \ldots, t_n \rangle$.

Proposition 1.7. *Let K be a number field, and let W be a finitely generated subgroup of K^*. Let $n = \mathrm{rk}(W)$. Let $t_1, \ldots, t_n \in K(\mu)^*$ be such that $\mathrm{Cyc}(W) = \mu \cdot \langle t_1, \ldots, t_n \rangle$. Then there is an isomorphism*

$$\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) \longrightarrow \widehat{\mu}^{\oplus n}$$

of topological $\widehat{\mathbf{Z}}$-modules sending $f \in \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})$ to $(f(t_i))_{i=1}^n$.

Proof. As $\widehat{\mu}$ has no torsion, we have $\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) = \mathrm{Hom}(\mathrm{Cyc}(W)/\mu, \widehat{\mu})$. Let

$$\varphi \colon \mathbf{Z}^n \longrightarrow \mathrm{Cyc}(W)/\mu$$

be the group isomorphism sending the standard basis element $e_i \in \mathbf{Z}^n$ to $t_i \cdot \mu$ for $i = 1, \ldots, n$. Then φ induces the isomorphisms

$$\mathrm{Hom}(\mathrm{Cyc}(W)/\mu, \widehat{\mu}) \cong \mathrm{Hom}(\mathbf{Z}^n, \widehat{\mu}) \cong \widehat{\mu}^{\oplus n}$$

of profinite groups, where the last isomorphism sends $f \in \mathrm{Hom}(\mathbf{Z}^n, \widehat{\mu})$ to $(f(e_i))_{i=1}^n$. By [Jav13, Lemma 2.3] these are in fact $\widehat{\mathbf{Z}}$-linear morphisms. ∎

Lemma 1.8. *Let Γ be an open subgroup of $\widehat{\mathbf{Z}}^*$, and let F be a free module over $\widehat{\mathbf{Z}}$ of finite rank. Let*

$$0 \longrightarrow F \xrightarrow{\iota} G \longrightarrow \Gamma \longrightarrow 1$$

be a natural extension of Γ by F. Let $[G, G]$ be the algebraic commutator subgroup of G. Then the following hold.

(a) *There exists $m \in \mathbf{Z}_{\geq 0}$ such that $\iota(mF) \subset [G, G]$.*

(b) *$[G, G]$ is closed in G.*

Proof. Since the kernels $\ker(\widehat{\mathbf{Z}}^* \longrightarrow (\mathbf{Z}/m\mathbf{Z})^*)$ form a fundamental system of neighbourhoods of $1 \in \widehat{\mathbf{Z}}^*$, there is $m \in \mathbf{Z}_{>0}$ such that $\ker(\widehat{\mathbf{Z}}^* \longrightarrow (\mathbf{Z}/m\mathbf{Z})^*)$ is contained in Γ. Choose such m even, which we may do without loss of generality. Let

$$u = (1 + m, 2) \in \prod_{p \mid m} \mathbf{Z}_p \times \prod_{p \nmid m} \mathbf{Z}_p = \widehat{\mathbf{Z}}$$

and note that $u \in \widehat{\mathbf{Z}}^*$. Since $u \equiv 1 \pmod{m}$, we have $u \in \Gamma$. Moreover, by construction we have $(u - 1)\widehat{\mathbf{Z}} = m\widehat{\mathbf{Z}}$.

Now, let $x \in F$, and let $v \in G$ such that $\pi(v) = u$. Observe that

$$(u - 1) \cdot x = \iota^{-1}(v\iota(x)v^{-1}\iota(x)^{-1}),$$

which is an element of $\iota^{-1}([G,G])$. It follows that

$$(u-1)F = mF \subset \iota^{-1}([G,G]).$$

As mF is open in F, it follows that $\iota^{-1}([G,G])$ is open in F, so in particular it is closed in F. Since ι is a closed map, $[G,G]$ is closed in G, as desired. ∎

Now, we are able to prove the (a) to (b) implication of the main theorem of this chapter (see Theorem 1 of the Introduction).

Proof of (a) implies (b) of the main theorem. By Theorem 1.5, there is a natural extension of Γ_K

$$0 \longrightarrow \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) \xrightarrow{\iota} G \longrightarrow \Gamma_K \longrightarrow 1,$$

where $\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})$ is free of rank n over $\widehat{\mathbf{Z}}$ by Proposition 1.7. Moreover, if $K = \mathbf{Q}$, then by the theorem of Kronecker–Weber (see [Hil96]) the image of $\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})$ is necessarily the closure $\overline{[G,G]}$ of the algebraic commutator subgroup of G. By 1.8(b) this is equal to the algebraic commutator subgroup $[G,G]$. ∎

3. Continuous cochain cohomology

Let Γ be a topological group. We denote the category of topological Γ-modules by Γ**-TMod**, and note that it is an additive category. The morphism sets in this category are denoted by $\mathrm{CHom}_\Gamma(-,-)$, $\mathrm{CEnd}_\Gamma(-)$ and $\mathrm{CAut}_\Gamma(-)$. When it is clear that every group morphism between two topological Γ-modules is continuous, we drop the 'C' from the notation; e.g. when the domain is discrete. Similarly, we drop the subscript Γ when it is clear that every group morphism between two Γ-modules is Γ-linear; e.g. when Γ is trivial or when Γ is a closed subgroup of $\widehat{\mathbf{Z}}^*$ and the action is natural (see [Jav13, Lemma 2.3]).

Let A be a topological Γ-module. For $n \in \mathbf{Z}_{\geq 0}$, endow $\Gamma^{\times n}$ with the product topology, and let $\mathrm{C}^n(\Gamma, A)$ denote the group $\mathrm{C}(\Gamma^{\times n}, A)$ of continuous functions from $\Gamma^{\times n}$ to A. The elements of $\mathrm{C}^n(\Gamma, A)$ are called *continuous n-cochains*.

For $n \in \mathbf{Z}_{\geq 0}$ define the *boundary map* $d_n \colon \mathrm{C}^n(\Gamma, A) \longrightarrow \mathrm{C}^{n+1}(\Gamma, A)$ by

$$(d_n\varphi)(\gamma_1, \ldots, \gamma_{n+1}) = \gamma_1 \cdot \varphi(\gamma_2, \ldots, \gamma_{n+1}) +$$

$$+ \textstyle\sum_{i=1}^{n} (-1)^i \varphi(\gamma_1, \ldots, \gamma_i\gamma_{i+1}, \ldots, \gamma_{n+1}) + (-1)^{n+1}\varphi(\gamma_1, \ldots, \gamma_n),$$

whose kernel is the group of *continuous n-cocycles*, and is denoted by $\mathrm{Z}^n(\Gamma, A)$. For all $n \in \mathbf{Z}_{\geq 0}$ we have $d_{n+1} \circ d_n = 0$. Hence, for $n \in \mathbf{Z}_{\geq 1}$ the image of d_{n-1}, denoted by $\mathrm{B}^n(\Gamma, A)$, is contained in $\mathrm{Z}^n(\Gamma, A)$; its elements are called the *continuous n-coboundaries*. Moreover, the group of continuous 0-coboundaries $\mathrm{B}^0(\Gamma, A)$ is defined as the trivial subgroup of $\mathrm{C}^0(\Gamma, A)$. For $n \in \mathbf{Z}_{\geq 0}$, we define the *$n$-th continuous cochain cohomology group of Γ with coefficients in A* as the quotient $\mathrm{Z}^n(\Gamma, A)/\,\mathrm{B}^n(\Gamma, A)$, denoted by $\mathrm{H}^n(\Gamma, A)$.

We will almost always omit 'continuous' in the above defined objects. Note that if Γ is a discrete topological group, the notions above coincide with the usual group cohomology notions.

The cohomology group $\mathrm{H}^0(\Gamma, A)$ will often be identified with the subgroup A^Γ of Γ-invariants of A via the group isomorphism $\varphi \mapsto \varphi(1)$. Moreover, if Γ acts trivially on A, then $\mathrm{H}^1(\Gamma, A)$ is equal to the group of continuous group morphisms $\mathrm{CHom}(\Gamma, A)$ of Γ to A.

Let Δ and Γ be topological groups, and let $\varphi \colon \Delta \longrightarrow \Gamma$ and $\psi \colon A \longrightarrow B$ be continuous group morphisms, where A and B are topological modules over Γ and Δ, respectively. The pair (φ, ψ) is called *compatible* if for all $\delta \in \Delta$ and $a \in A$ we have $\psi(\varphi(\delta)a) = \delta(\psi(a))$.

Lemma 1.9. *Let $\varphi \colon \Delta \longrightarrow \Gamma$ and $\psi \colon A \longrightarrow B$ be a compatible pair. Then the following statements hold.*

(a) *For each* $n \in \mathbf{Z}_{\geq 0}$ *there is an induced group morphism*

$$\mathrm{C}^n(\varphi, \psi)\colon\ \mathrm{C}^n(\Gamma, A) \longrightarrow \mathrm{C}^n(\Delta, B)$$

given by

$$\mathrm{C}^n(\varphi, \psi)(f) = \psi \circ f \circ \varphi^{\times n},$$

where $\varphi^{\times n}\colon \Delta^{\times n} \longrightarrow \Gamma^{\times n}$ *sends* $(\delta_1, \ldots, \delta_n) \in \Delta^{\times n}$ *to* $(\varphi(\delta_1), \ldots, \varphi(\delta_n))$.

(b) *For each* $n \in \mathbf{Z}_{\geq 0}$ *the diagram*

$$\begin{array}{ccc} \mathrm{C}^n(\Gamma, A) & \xrightarrow{d_n} & \mathrm{C}^{n+1}(\Gamma, A) \\ {\scriptstyle \mathrm{C}^n(\varphi,\psi)}\downarrow & & \downarrow{\scriptstyle \mathrm{C}^{n+1}(\varphi,\psi)} \\ \mathrm{C}^n(\Delta, B) & \xrightarrow[d_n]{} & \mathrm{C}^{n+1}(\Delta, B) \end{array}$$

is commutative.

(c) *For each* $n \in \mathbf{Z}_{\geq 0}$ *there is an induced group morphism*

$$\mathrm{H}^n(\varphi, \psi)\colon\ \mathrm{H}^n(\Gamma, A) \longrightarrow \mathrm{H}^n(\Delta, B)$$

defined by sending $[f] \in \mathrm{H}^n(\Gamma, A)$ *to* $[\mathrm{C}^n(\varphi, \psi)(f)]$.

Proof. See [Wil98, Lemma 9.2.1]. ∎

Let $\mathcal{C}$ be the category defined as follows. Let the objects of $\mathcal{C}$ be all pairs (Γ, A) where Γ is a topological group and A is a topological Γ-module. A morphism between (Γ, A) and (Δ, B) is given by a compatible pair (φ, ψ) where $\varphi\colon \Delta \longrightarrow \Gamma$ and $\psi\colon A \longrightarrow B$. Composition of two morphisms $(\varphi\colon \Delta \longrightarrow \Gamma, \psi\colon A \longrightarrow B)$ and $(\varphi'\colon I \longrightarrow \Delta, \psi'\colon B \longrightarrow C)$ is given by

$$(\varphi', \psi') \circ (\varphi, \psi) = (\varphi \circ \varphi', \psi' \circ \psi).$$

Proposition 1.10. *Let $n \in \mathbf{Z}_{\geq 0}$. Then*

$$\mathrm{C}^n(\cdot,\cdot)\colon \mathcal{C} \longrightarrow \mathbf{Ab} \text{ and } \mathrm{H}^n(\cdot,\cdot)\colon \mathcal{C} \longrightarrow \mathbf{Ab}$$

are covariant functors from $\mathcal{C}$ to the category **Ab** *of abelian groups.*

Proof. See [Jav13, Proposition 1.3]. ∎

Throughout the rest of this section, let Γ be a topological group. The subcategory $\mathcal{C}_\Gamma$ of $\mathcal{C}$ consisting of the pairs (Γ, A) with A a topological Γ-module, and with morphisms all compatible pairs $(\mathrm{id}_\Gamma, \psi)$ where ψ is a continuous Γ-module morphism, can be canonically identified with the category Γ**-TMod** of topological Γ-modules. For a morphism ψ of topological Γ-modules, let $\mathrm{C}^n(\Gamma, \psi) = \mathrm{C}^n(\mathrm{id}_\Gamma, \psi)$ and $\mathrm{H}^n(\Gamma, \psi) = \mathrm{H}^n(\mathrm{id}_\Gamma, \psi)$.

Proposition 1.11. *Let $n \in \mathbf{Z}_{\geq 0}$. Then*

$$\mathrm{C}^n(\Gamma,\cdot)\colon \Gamma\text{-}\mathbf{TMod} \longrightarrow \mathbf{Ab} \text{ and } \mathrm{H}^n(\Gamma,\cdot)\colon \Gamma\text{-}\mathbf{TMod} \longrightarrow \mathbf{Ab}$$

are additive covariant functors.

Proof. See [Jav13, Proposition 1.4]. ∎

Proposition 1.12. *The functors $\mathrm{C}^n(\Gamma,\cdot)$ and $\mathrm{H}^n(\Gamma,\cdot)$ commute with arbitrary products.*

Proof. See [Jav13, Proposition 1.6]. ∎

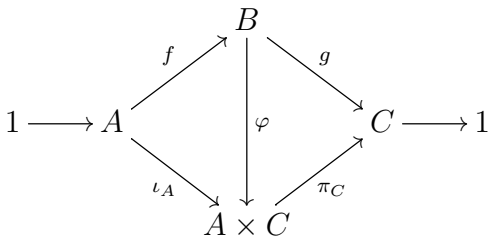
Proposition 1.13. *Let*

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

be a short exact sequence of not necessarily abelian topological groups. Then the following are equivalent.

(a) *The map f induces a homeomorphism from A to its image, and g admits a continuous set-theoretic section.*

(b) *There is a homeomorphism* $\varphi\colon B \longrightarrow A \times C$*, where* $A \times C$ *has the product topology, such that the diagram*



commutes, where ι_A *sends* $a \in A$ *to* $(a, 1)$ *and* π_C *sends* $(a, c) \in A \times C$ *to* c*.*

Proof. See [Jav13, Proposition 1.7]. ∎

Definition 1.14. A short exact sequence

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

of not necessarily abelian topological groups is called *well-adjusted* if it satisfies either one of the equivalent conditions 1.13(a) and 1.13(b) above.

All short exact sequences of discrete groups are well-adjusted, as are all short exact sequences of profinite groups, see [Wil98, Lemma 0.1.2].

Proposition 1.15. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a well-adjusted short exact sequence of topological Γ*-modules. Then for each* $n \in \mathbf{Z}_{\geq 0}$ *there is a unique group morphism*

$$\delta_n\colon \mathrm{H}^n(\Gamma, C) \longrightarrow \mathrm{H}^{n+1}(\Gamma, A)$$

such that for every $c \in \mathrm{Z}^n(\Gamma, C)$ *and for every* $a \in \mathrm{C}^{n+1}(\Gamma, A)$ *and* $b \in \mathrm{C}^n(\Gamma, B)$ *satisfying* $\mathrm{C}^n(\Gamma, g)(b) = c$ *and* $\mathrm{C}^{n+1}(\Gamma, f)(a) = d_n(b)$*, we have* $a \in \mathrm{Z}^{n+1}(\Gamma, A)$ *and* $\delta_n([c]) = [a]$*.*

Proof. See [Jav13, Proposition 1.13]. ∎

Theorem 1.16. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a well-adjusted short exact sequence of topological Γ*-modules. Then the sequence*

$$0 \longrightarrow \mathrm{H}^0(\Gamma, A) \xrightarrow{\mathrm{H}^0(f)} \mathrm{H}^0(\Gamma, B) \xrightarrow{\mathrm{H}^0(g)} \mathrm{H}^0(\Gamma, C) \xrightarrow{\delta_0} \mathrm{H}^1(\Gamma, A) \xrightarrow{\mathrm{H}^1(f)} \dots$$

$$\dots \xrightarrow{\delta_{n-1}} \mathrm{H}^n(\Gamma, A) \xrightarrow{\mathrm{H}^n(f)} \mathrm{H}^n(\Gamma, B) \xrightarrow{\mathrm{H}^n(g)} \mathrm{H}^n(\Gamma, C) \xrightarrow{\delta_n} \mathrm{H}^{n+1}(\Gamma, A) \xrightarrow{\mathrm{H}^{n+1}(f)} \dots$$

is exact.

Proof. See [Jav13, Theorem 1.15]. ∎

4. Topological group extensions

Throughout this section, let Γ be a topological group, and let A be a topological Γ-module.

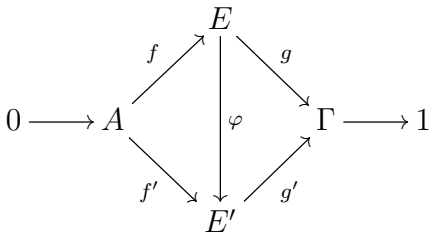
Definition 1.17. A *topological group extension of* Γ *by* A is a triple (E, f, g) consisting of a topological group E together with a well-adjusted short exact sequence

$$0 \longrightarrow A \xrightarrow{f} E \xrightarrow{g} \Gamma \longrightarrow 1$$

of topological groups, such that for all $a \in A$ and $x \in E$ we have $xf(a)x^{-1} = f(g(x) \cdot a)$.

Notation 1.18. We will often denote the extension (E, f, g) by the well-adjusted short exact sequence that is associated with it, or just by E when the maps f and g are understood.

Definition 1.19. Let (E, f, g) and (E', f', g') be two topological extensions of Γ by A. Then (E, f, g) and (E', f', g') are said to be *equivalent* if there exists an isomorphism $\varphi\colon E \longrightarrow E'$ of topological groups such that the diagram



commutes.

The above defines an equivalence relation on the class of all topological extensions of Γ by A. For convenience, let X denote the set of all equivalence classes of topological extensions of Γ by A.

Let (E, f, g) be a topological extension of Γ by A, and let s be a continuous section of g. Then associating to (E, f, g) the map $\Gamma^{\times 2} \longrightarrow A$ given by

$$(\gamma_1, \gamma_2) \mapsto f^{-1}(s(\gamma_1)s(\gamma_2)s(\gamma_1\gamma_2)^{-1}), \qquad (*)$$

induces a well-defined map $\varphi\colon X \longrightarrow \mathrm{H}^2(\Gamma, A)$, see [Hu52].

Theorem 1.20. *The map φ above is a bijection of sets.*

Proof. See [Hu52]. ∎

The theorem above enables us to identify elements of $\mathrm{H}^2(\Gamma, A)$ with equivalence classes of topological extensions of Γ by A, and vice versa.

Let B be a topological Γ-module, and let $\psi\colon A \longrightarrow B$ be a morphism of topological Γ-modules. Let (E, f, g) be a topological extension of Γ by A. Compose

$$E \longrightarrow \Gamma \longrightarrow \mathrm{Aut}(B)$$

to obtain a canonical action of E on B. Then the *pushout* $\psi_*(E)$ *of* E *along* ψ is

$$\psi_*(E) = (B \rtimes E)/\{(\psi(a), -f(a)) : a \in A\},$$

where the semi-direct product has the product topology and the quotient has the quotient topology. One easily checks that $(\psi_*(E), \iota_B, \pi)$ defines an element of $\mathrm{H}^2(\Gamma, B)$, where ι_B is the inclusion of B in $\psi_*(E)$ and π is the canonical surjection of $\psi_*(E)$ to Γ.

Proposition 1.21. *We have* $\mathrm{H}^2(\Gamma, \psi)([E]) = [(\psi_*(E), \iota_B, \pi)]$.

Proof. Clear from $(*)$. ∎

5. On profinite groups

Lemma 1.22. *Let* F *be a free* $\widehat{\mathbf{Z}}$*-module of finite rank, and let* H *be a profinite group. Then every group morphism* $F \longrightarrow H$ *is continuous.*

Proof. Note that every finite index subgroup of F is open, because multiplication on F by every element of $\mathbf{Z}$ is a continuous morphism. By [Wil98, Proposition 1.1.6(d)] the map $F \longrightarrow H$ is continuous if and only if for every open normal subgroup N of H the composition $f_N \colon F \longrightarrow H/N$ is continuous. As H/N is finite, it follows that $\ker f_N$ is open in F.

By [Wil98, Lemma 1.2.6], a map from a profinite group to a discrete space is continuous if and only if there is an open normal subgroup N of G such that f factors through G/N. It follows that $F \longrightarrow H$ is continuous. ∎

Lemma 1.23. *Let* F *be a free* $\widehat{\mathbf{Z}}$*-module of finite nonzero rank, and let* Γ *be an open subgroup of* $\widehat{\mathbf{Z}}^*$*. Let*

$$0 \longrightarrow F \xrightarrow{\iota} G \longrightarrow \Gamma \longrightarrow 0$$

be a natural extension. Then the image of ι is equal to the centralizer

$$\mathrm{C}_G([G,G]) = \{g \in G : gx = xg \text{ for all } x \in [G,G]\}$$

of $[G,G]$ in G.

Proof. First, note that $[G,G] \subset \iota(F)$, because Γ is abelian. As $\iota(F)$ is abelian, it centralises every subgroup. Hence $\iota(F) \subset \mathrm{C}_G([G,G])$.

Conversely, note that by Lemma 1.8(a) there is $m \in \mathbf{Z}_{>0}$ such that $\iota(mF) \subset [G,G]$. Let $\sigma \in \mathrm{C}_G([G,G])$, and let $x \in F$. As $\iota(mx) \in [G,G]$, we have

$$\sigma \cdot \iota(mx) = \sigma\iota(mx)\sigma^{-1} = \iota(mx).$$

Since F is torsion-free, it follows that σ acts as the identity on F. Equivalently σ maps to the identity in Γ, because F is a free $\widehat{\mathbf{Z}}$-module of finite nonzero rank. Hence $\sigma \in \iota(F)$, which proves that $\mathrm{C}_G([G,G]) \subset \iota(F)$. ∎

6. Roots of unity and cohomology

Let Γ be a closed subgroup of $\widehat{\mathbf{Z}}^*$. Define

$$I_\Gamma = \sum_{\gamma \in \Gamma} \widehat{\mathbf{Z}}(\gamma - 1)$$

to be the $\widehat{\mathbf{Z}}$-ideal generated by $\Gamma - 1 = \{\gamma - 1 : \gamma \in \Gamma\}$, and let $J_\Gamma = \overline{I_\Gamma}$ be its topological closure in $\widehat{\mathbf{Z}}$. For example, one has $I_{\widehat{\mathbf{Z}}^*} = J_{\widehat{\mathbf{Z}}^*} = 2\widehat{\mathbf{Z}}$.

Let M be a profinite abelian group. As M is a $\widehat{\mathbf{Z}}$-module, there is an induced module structure of $\widehat{\mathbf{Z}}$ on $\mathrm{H}^n(\Gamma, M)$ for each $n \in \mathbf{Z}_{\geq 0}$.

Theorem 1.24. *Let Γ be a closed subgroup of $\widehat{\mathbf{Z}}^*$. Let M be a profinite abelian group, and let Γ act naturally on M. Then for all $n \in \mathbf{Z}_{\geq 0}$ we have $J_\Gamma \cdot \mathrm{H}^n(\Gamma, M) = 0$.*

Proof. See [Jav13, Theorem 2.16]. ∎

Recall that for a field K of characteristic 0, we identify the maximal cyclotomic Galois group $\mathrm{Gal}(K(\mu)/K)$ of K canonically with a closed subgroup of $\widehat{\mathbf{Z}}^*$, which we denote by Γ_K.

Theorem 1.25. *Let K be a field of characteristic 0, and let Γ_K be its maximal cyclotomic Galois group. Then $J_{\Gamma_K} = \mathrm{Ann}_{\widehat{\mathbf{Z}}}(\mu(K))$.*

Proof. See [Jav13, Theorem 2.17]. ∎

Corollary 1.26. *Let Γ_K be as in* Theorem 1.25*, and let M be a profinite abelian group with the natural Γ_K-action. Then for all $n \in \mathbf{Z}_{\geq 0}$ we have $\mathrm{Ann}_{\widehat{\mathbf{Z}}}(\mu(K)) \cdot \mathrm{H}^n(\Gamma_K, M) = 0$.*

Proof. This follows immediately from Theorem 1.24 and Theorem 1.25. ∎

Example 1.27. Let K be a field of characteristic 0 with only finitely many roots of unity, say $w = \#\mu(K)$. Then $\mathrm{Ann}_{\widehat{\mathbf{Z}}}(\mu(K)) = w\widehat{\mathbf{Z}} = J_\Gamma$. Hence $w \cdot \mathrm{H}^n(\Gamma_K, M) = 0$ for every profinite abelian group M.

7. Orbits of natural extensions

Throughout this section, let $n \in \mathbf{Z}_{\geq 0}$, let M be a free $\widehat{\mathbf{Z}}$-module of rank 1, let F be a free $\widehat{\mathbf{Z}}$-module of rank n, and let Γ be an open subgroup of $\widehat{\mathbf{Z}}^*$. Let S be the set of isomorphism classes of profinite groups G such that there exists a natural extension

$$0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma \longrightarrow 1.$$

Such an extension has a class $[0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma \longrightarrow 1]$ that belongs to $\mathrm{H}^2(\Gamma, F)$; for $f \in \mathrm{Hom}(F, M)$, the map $\mathrm{H}^2(\Gamma, f)$ sends this class to an element of $\mathrm{H}^2(\Gamma, M)$.

Let T be the set of subgroups of $\mathrm{H}^2(\Gamma, M)$ that can be generated by n elements. In this section we prove the following theorem.

Theorem 1.28. *The map $\rho\colon S \longrightarrow T$ given by*

$$[G] \mapsto \left\{\mathrm{H}^2(\Gamma, f)([0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma \longrightarrow 1]) : f \in \mathrm{Hom}(F, M)\right\}$$

is well-defined and bijective.

We briefly give an outline of the proof. First, note that the theorem is trivial for $n = 0$. Assume $n > 0$ and for simplicity take $F = \widehat{\mathbf{Z}}^{\oplus n}$ and $M = \widehat{\mathbf{Z}}$. We define $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-actions on $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$ and $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$ and give an isomorphism

$$\omega\colon\ \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \longrightarrow \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$$

of $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-modules. We give S and T the trivial $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-action, and construct $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-equivariant maps

$$\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \longrightarrow S$$

and

$$\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n} \longrightarrow T$$

that both have the property that two elements in the domain map to the same element in the codomain if and only if they are in the same $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-orbit in the domain. We show that the latter maps make the diagram

$$\begin{array}{ccc} \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) & \xrightarrow{\omega} & \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n} \\ \downarrow & & \downarrow \\ S & \xrightarrow[\rho]{} & T \end{array}$$

commutative in the category of $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-sets. Then ρ is the map induced by ω on the orbit spaces. As ω is an isomorphism, the map ρ is a bijection, as desired.

Assume that $n \geq 1$. By additivity of $\mathrm{H}^2(\Gamma, \cdot)$ there is a ring morphism

$$\mathrm{CEnd}_\Gamma(\widehat{\mathbf{Z}}^{\oplus n}) \longrightarrow \mathrm{End}(\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}))$$

given by $f \mapsto \mathrm{H}^2(\Gamma, f)$. By Lemma 1.22 and the fact that any continuous group morphism of profinite abelian groups is $\widehat{\mathbf{Z}}$-linear (see [Jav13, Lemma 2.3]), we may drop the 'C' and subscript Γ, so that we have an $\mathrm{End}(\widehat{\mathbf{Z}}^{\oplus n})$-module structure on $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$. For simplicity we write $\mathrm{M}_n(\widehat{\mathbf{Z}})$ for $\mathrm{End}(\widehat{\mathbf{Z}}^{\oplus n})$ and $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ for $\mathrm{Aut}(\widehat{\mathbf{Z}}^{\oplus n})$.

By additivity of $\mathrm{H}^2(\Gamma, \cdot)$ the map

$$\omega\colon\ \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \longrightarrow \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$$

given by $x \mapsto \big(\mathrm{H}^2(\Gamma, \pi_i)(x)\big)_{i=1}^n$, where π_i is the i-th projection of $\widehat{\mathbf{Z}}^{\oplus n}$ onto $\widehat{\mathbf{Z}}$, is an isomorphism of groups. Then

$$\mathrm{End}(\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})) \longrightarrow \mathrm{End}(\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n})$$

given by $f \mapsto \omega \circ f \circ \omega^{-1}$ is an isomorphism defining the $\mathrm{M}_n(\widehat{\mathbf{Z}})$-module structure on $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$. The map ω then becomes an isomorphism of $\mathrm{M}_n(\widehat{\mathbf{Z}})$-modules. Moreover, for $f \in \mathrm{M}_n(\widehat{\mathbf{Z}})$ and $(x_1, \ldots, x_n) \in \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$ we explicitly have

$$f \cdot (x_1, \ldots, x_n) = \left(\sum_{j=1}^{n} \mathrm{H}^2(\Gamma, \pi_i \circ f \circ \iota_j)(x_j) \right)_{i=1}^{n}.$$

We summarize the above in the following lemma.

Lemma 1.29. *Assume that $n \geq 1$. For $i = 1, \ldots, n$ let π_i be the i-th projection of $\widehat{\mathbf{Z}}^{\oplus n}$ onto $\widehat{\mathbf{Z}}$, and ι_i the i-th injection of $\widehat{\mathbf{Z}}$ into $\widehat{\mathbf{Z}}^{\oplus n}$. Then the map*

$$\omega\colon\ \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \longrightarrow \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$$

defined by $x \mapsto (\mathrm{H}^2(\Gamma, \pi_i)(x))_{i=1}^n$ is an isomorphism of $\mathrm{M}_n(\widehat{\mathbf{Z}})$-modules, where for $f \in \mathrm{M}_n(\widehat{\mathbf{Z}})$ and $x \in \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$ and $(x_1, \ldots, x_n) \in \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$ we have

$$f \cdot x = \mathrm{H}^2(\Gamma, f)(x)$$

and

$$f \cdot (x_1, \ldots, x_n) = \left(\sum_{j=1}^{n} \mathrm{H}^2(\Gamma, \pi_i \circ f \circ \iota_j)(x_j) \right)_{i=1}^{n}.$$

Lemma 1.30. *Assume that $n \geq 1$. Let $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ act on $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$ by restricting the $\mathrm{M}_n(\widehat{\mathbf{Z}})$-action, and let $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ act trivially on S. Then the map $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \longrightarrow S$ given by*

$$[0 \longrightarrow \widehat{\mathbf{Z}}^{\oplus n} \longrightarrow G \longrightarrow \Gamma \longrightarrow 1] \mapsto [G]$$

is a well-defined $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-map with the property that two elements in $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$ map to the same element in S if and only if they are in the same $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-orbit.

Proof. The map is clearly well-defined. Equivariance under $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ follows from the second statement of the lemma, which we prove now.

Let

$$[(G_1, f_1, g_1)] = [G_1], [(G_2, f_2, g_2)] = [G_2] \in \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$$

and suppose that they map to the same element in S. Let $\alpha \colon G_1 \longrightarrow G_2$ be an isomorphism of topological groups, which exists since G_1 and G_2 map to the same element in S. As

$$\alpha(\mathrm{C}_{G_1}([G_1, G_1])) = \mathrm{C}_{G_2}([G_2, G_2]),$$

Lemma 1.23 implies that the map α induces an isomorphism $\alpha' \colon \widehat{\mathbf{Z}}^{\oplus n} \longrightarrow \widehat{\mathbf{Z}}^{\oplus n}$ such that the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{\mathbf{Z}}^{\oplus n} & \xrightarrow{f_1} & G_1 & \xrightarrow{g_1} & \Gamma & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \\
0 & \longrightarrow & \widehat{\mathbf{Z}}^{\oplus n} & \xrightarrow[f_2]{} & G_2 & \xrightarrow[g_2]{} & \Gamma & \longrightarrow & 1
\end{array}$$

commutes. The vertical map $\Gamma \longrightarrow \Gamma$ is induced by the universal property of cokernels. Since the action of Γ on $\widehat{\mathbf{Z}}^{\oplus n}$ is the same as the actions of G_1 and G_2 on $\widehat{\mathbf{Z}}^{\oplus n}$, it follows that

the vertical map $\Gamma \longrightarrow \Gamma$ is the identity. Moreover, as G_2 is the pushout of G_1 along α', Proposition 1.21 implies that $\mathrm{H}^2(\Gamma, \alpha')([G_1]) = [G_2]$.

Conversely, suppose that there is $f \in \mathrm{GL}_n(\widehat{\mathbf{Z}})$ with $\mathrm{H}^2(\Gamma, f)([G_1]) = [G_2]$. By Proposition 1.21, the latter equality implies that G_2 is isomorphic to the pushout $f_*(G_1)$ of G_1 along f. As f is an isomorphism, it follows that G_1 is isomorphic to $f_*(G_1)$. Hence, we have $G_1 \cong G_2$ as profinite groups. ∎

Let R be a not necessarily commutative ring. Recall that the *Jacobson radical* $\mathrm{Jac}(R)$ of R is the intersection of all maximal left ideals of R. Moreover, recall that a left R-module M is called *simple* if it has exactly two R-submodules, and that M is called *semisimple* if it is the direct sum of simple R-modules. The ring R is called *semisimple* if it is semisimple as a module over itself. The ring R is called *semi-local* if $R/\operatorname{Jac}(R)$ is semisimple.

Lemma 1.31. *Let R be a (not necessarily commutative) semi-local ring. Let A be a finitely generated R-module, and let P be a finitely generated projective R-module. Assume that we have two surjective R-module morphisms $f, g\colon P \longrightarrow A$. Then there is an isomorphism $h\colon P \longrightarrow P$ of R-modules such that $g \circ h = f$.*

Proof. First, assume that R is semisimple. Then A is projective, so we have R-module isomorphisms

$$p_1\colon P \longrightarrow A \oplus \ker f$$

and

$$p_2\colon P \longrightarrow A \oplus \ker g$$

such that $f = \pi_A \circ p_1$ and $g = \pi_A \circ p_2$, where

$$\pi_A\colon A \oplus \ker f \longrightarrow A$$

and

$$\pi'_A\colon A \oplus \ker g \longrightarrow A$$

are the canonical projection maps. As P is both noetherian and artinian as R-module, the theorem of Krull-Remak-Schmidt (see [Lan02, Chapter X, Theorem 7.5]) implies that $\ker f$ and $\ker g$ are isomorphic as R-modules. Choose any R-module isomorphism

$$p\colon \ker f \longrightarrow \ker g.$$

It follows that

$$h = p_2^{-1} \circ (\mathrm{id}_A \oplus p) \circ p_1\colon P \longrightarrow P$$

is an R-module isomorphism that satisfies $g \circ h = f$. Indeed, we have

$$g \circ h = \pi'_A \circ p_2 \circ h = \pi'_A \circ (\mathrm{id}_A \oplus p) \circ p_1 = \pi_A \circ p_1 = f,$$

which proves the statement for R semisimple.

Now drop the assumption that R is semisimple. By definition of a semi-local ring, the ring $R/\operatorname{Jac}(R)$ is semisimple. For simplicity write $J = \operatorname{Jac}(R)$. Then f and g induce surjective R-module morphisms

$$\overline{f}, \overline{g}\colon P/JP \longrightarrow A/JA.$$

As R/J is semisimple, the R/J-module $P/JP = (R/J) \otimes_R P$ is projective. Hence, there is an R-module isomorphism

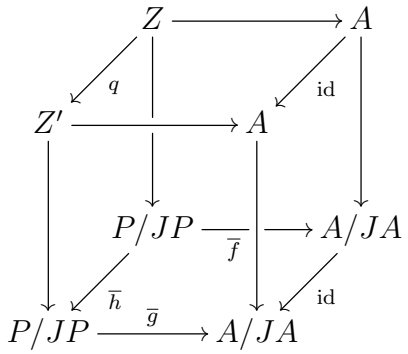
$$\overline{h}\colon P/JP \longrightarrow P/JP$$

such that $\overline{g} \circ \overline{h} = \overline{f}$. Let Z be the pullback of the canonical projection $A \longrightarrow A/JA$ and $\overline{f}\colon P/JP \longrightarrow A/JA$. Let Z' be the pullback of the same diagram with $\overline{f}$ replaced by $\overline{g}$.

As the pullback diagrams of Z and Z' are isomorphic, there is an isomorphism

$$q\colon Z \longrightarrow Z'$$

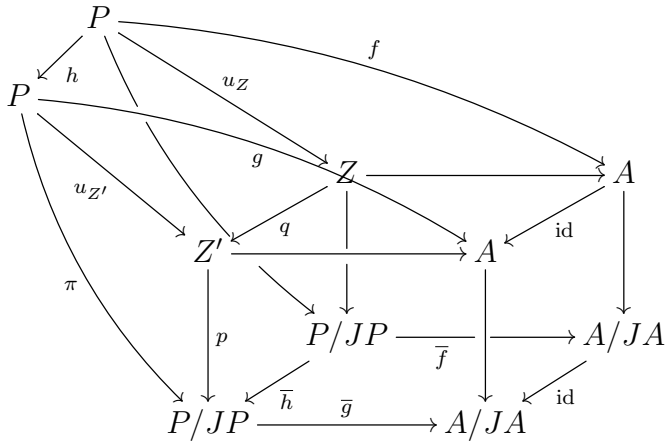
such that the cube



commutes. By the universal property of Z, the canonical projection $P \longrightarrow P/JP$ and f induce an R-module morphism $u_Z \colon P \longrightarrow Z$. By a diagram chasing argument, one easily sees that this map is surjective. Analogously, we have a surjective morphism

$$u_{Z'} \colon P \longrightarrow Z'.$$

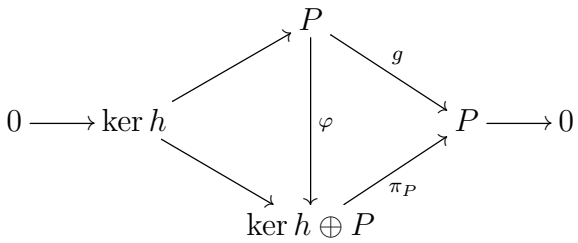
By projectivity of P, there is a morphism $h \colon P \longrightarrow P$ such that $u_{Z'} \circ h = q \circ u_Z$. Now, the three-dimensional diagram



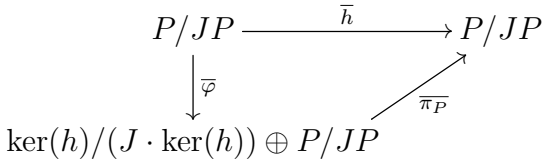
commutes. Note that we have $g \circ h = f$. Therefore, it remains to show that h is an isomorphism of R-modules. To show surjectivity, note that u_Z, q and p are surjective. Therefore, the map $p \circ u_{Z'} \circ h = \pi \circ h$ is surjective. Thus, we have $P = h(P) + JP$. Since P is finitely

generated, the quotient $P/h(P)$ is so too. Moreover, we have $J(P/h(P)) = P/h(P)$. Hence, by Nakayama's lemma (see [Lam91, Theorem 4.22]) we have $P/h(P) = 0$. It follows that h is surjective.

By projectivity of P the sequence $0 \longrightarrow \ker h \longrightarrow P \longrightarrow P \longrightarrow 0$ splits, that is, there is an R-module isomorphism $\varphi\colon P \longrightarrow \ker h \oplus P$ such that



commutes, where π_P is the projection to P. As P is finitely generated and the sequence splits, $\ker h$ is also finitely generated. Applying the functor $(R/J) \otimes_R -$ to $h = \pi_P \circ \varphi$ shows that



commutes. As $\overline{h}$ and $\overline{\varphi}$ are isomorphisms, it follows that $\overline{\pi_P}$ is an isomorphism. Hence, we have

$$\ker(h)/(J \cdot \ker(h)) = 0.$$

Then Nakayama's lemma (see [Lam91, Theorem 4.22]) implies that $\ker h = 0$, so that h is injective. This shows that h is an isomorphism of R-modules, which finishes the proof. ∎

Lemma 1.32. *Assume that $n \geq 1$, and that $M = \widehat{\mathbf{Z}}$. Let $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ act on $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$ by restricting the $\mathrm{M}_n(\widehat{\mathbf{Z}})$-action, and let $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ act trivially on the set T from* Theorem 1.28. *Then the map*

$$\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n} \longrightarrow T$$

given by

$$(x_1, \ldots, x_n) \mapsto \langle x_1, \ldots, x_n \rangle$$

is a $\mathrm{GL}_n(\widehat{\mathbf{Z}})$*-map with the property that two elements in* $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$ *map to the same element in* T *if and only if they are in the same* $\mathrm{GL}_n(\widehat{\mathbf{Z}})$*-orbit.*

Proof. Equivariance under $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ follows from the second statement of the lemma, which we prove now.

Let $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ be elements of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$. Suppose that $\langle x_1, \ldots, x_n \rangle$ and $\langle y_1, \ldots, y_n \rangle$ are the same subgroup of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$, say N. By Theorem 1.24, the ideal J_Γ annihilates the group $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$. As Γ is open, it is equal to Γ_K for some number field K. Hence, by Example 1.27 there is $w \in \mathbf{Z}_{\geq 2}$ such that $w\widehat{\mathbf{Z}} = J_\Gamma$. Now $J_\Gamma \cdot \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}) = 0$ implies that $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$ is torsion. It follows that N is a finite group. Now, we replace $\widehat{\mathbf{Z}}$ with the ring $\widehat{\mathbf{Z}}_N = \prod_{p \mid \#N} \mathbf{Z}_p$, because the action of $\widehat{\mathbf{Z}}$ on N factors via $\widehat{\mathbf{Z}}_N$. As $\widehat{\mathbf{Z}}_N$ is a finite product of local rings, it is semi-local; in particular, the quotient $\widehat{\mathbf{Z}}_N / \operatorname{Jac}(\widehat{\mathbf{Z}}_N)$ is semisimple.

Each set of generators of N defines a surjective morphism

$$\widehat{\mathbf{Z}}_N^{\oplus n} \longrightarrow N$$

of $\widehat{\mathbf{Z}}_N$-modules by sending the standard basis to the set of generators. Let f be the morphism corresponding to $(x_1, \ldots, x_n)$, and let g be the morphism corresponding to $(y_1, \ldots, y_n)$. Then by Lemma 1.31 it follows that there is an isomorphism

$$h \colon \widehat{\mathbf{Z}}_N^{\oplus n} \longrightarrow \widehat{\mathbf{Z}}_N^{\oplus n}$$

of $\widehat{\mathbf{Z}}_N$-modules such that $g \circ h = f$. Extend h to an automorphism of $\widehat{\mathbf{Z}}^{\oplus n}$ by the identity on $\prod_{p \nmid \#N} \mathbf{Z}_p$.

Let A be the matrix in $\mathrm{GL}_n(\widehat{\mathbf{Z}})$ corresponding to h. Then

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

This action of A on $(x_1, \ldots, x_n)$ is the same as the action of h on $(x_1, \ldots, x_n)$. It follows that $h \cdot (x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ as desired.

Conversely, suppose there is $f \in \mathrm{GL}_n(\widehat{\mathbf{Z}})$ such that $f \cdot (x_1, \ldots, x_n) = (y_1, \ldots, y_n)$. Then y_i is a $\widehat{\mathbf{Z}}$-linear combination of $x_1, \ldots, x_n$ for every $i = 1, \ldots, n$. Hence, we have

$$\langle y_1, \ldots, y_n \rangle \subset \langle x_1, \ldots, x_n \rangle.$$

The other inclusion follows from the identity $f^{-1} \cdot (y_1, \ldots, y_n) = (x_1, \ldots, x_n)$. ∎

Remark 1.33. One easily sees that the above lemma is true if we replace $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$ by an abelian torsion group A that is an $\mathrm{M}_n(\widehat{\mathbf{Z}})$-module, and replace T by the corresponding set of subgroups of A that can be generated by n elements of A.

Proof of Theorem 1.28. Observe that the theorem is trivial for $n = 0$. Assume $n > 0$. It is clear that we may take $F = \widehat{\mathbf{Z}}^{\oplus n}$ and $M = \widehat{\mathbf{Z}}$, which we do for simplicity. To show that ρ is well-defined, note that

$$\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \times \mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}}) \longrightarrow \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$$

given by $(x, f) \mapsto \mathrm{H}^2(\Gamma, f)(x)$ is a bilinear mapping. Hence, for fixed $x \in \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$ the image $\mathrm{H}^2(\Gamma, \mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}}))(x)$ is indeed a subgroup of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$. Moreover, the group $\mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}})$ is generated as a $\widehat{\mathbf{Z}}$-module by the n projection morphisms $\pi_1, \ldots, \pi_n$. Then by additivity of $\mathrm{H}^2(\Gamma, \cdot)$ it follows that $\mathrm{H}^2(\Gamma, \mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}}))(x)$ is indeed a subgroup of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})$ that can be generated by n elements.

To show that for $[G] \in S$ the image $\rho([G])$ does not depend on the equivalence class $[0 \longrightarrow \widehat{\mathbf{Z}}^{\oplus n} \longrightarrow G \longrightarrow \Gamma \longrightarrow 1]$ in $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$, suppose $[(G, f_1, g_1)]$ and $[(G, f_2, g_2)]$ are two elements of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$. Let $\alpha \colon G \longrightarrow G$ be an automorphism of G. By Lemma 1.23,

there exists an isomorphism α' of $\widehat{\mathbf{Z}}^{\oplus n}$ such that

$$\begin{array}{ccc} \widehat{\mathbf{Z}}^{\oplus n} & \xrightarrow{f_1} & G \\ {\scriptstyle \alpha'}\downarrow & & \downarrow{\scriptstyle \alpha} \\ \widehat{\mathbf{Z}}^{\oplus n} & \xrightarrow[g_2]{} & G \end{array}$$

commutes. Then clearly G is the pushout of G along α', so that we have

$$\mathrm{H}^2(\Gamma, f)([(G, f_2, g_2)]) = \mathrm{H}^2(\Gamma, f \circ \alpha')([(G, f_1, g_1)]).$$

As composition with α' induces an automorphism of $\mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}})$, it follows that

$$\mathrm{H}^2(\Gamma, \mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}}))([(G, f_1, g_1)]) = \mathrm{H}^2(\Gamma, \mathrm{Hom}(\widehat{\mathbf{Z}}^{\oplus n}, \widehat{\mathbf{Z}}))([(G, f_2, g_2)]).$$

Hence, the map ρ is well-defined.

Now, one easily checks that we have a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) & \xrightarrow{\omega} & \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n} \\ {\scriptstyle 1.30}\downarrow & & \downarrow{\scriptstyle 1.32} \\ S & \xrightarrow[\rho]{} & T \end{array}$$

of $\mathrm{GL}_n(\widehat{\mathbf{Z}})$-equivariant maps, where ω is defined in Lemma 1.29. By Lemma 1.30 and 1.32, the sets S and T are in bijection with the orbit spaces of $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n})$ and $\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n}$ under the action of $\mathrm{GL}_n(\widehat{\mathbf{Z}})$, respectively. By commutativity of the diagram ρ is a bijection. ∎

8. Cohomology of the Tate module

Throughout this section, let K be a number field, $\overline{K}$ an algebraic closure of K, and $w = \#\mu(K)$. For every $m \in \mathbf{Z}_{\geq 1}$ we put $K_m = \overline{K}^*$. For every positive integer m' dividing m we have a surjective map $K_m \longrightarrow K_{m'}$ given by exponentiation by m/m'. This forms a

projective system and its limit is denoted by $\widehat{K^*}$. The elements $x = (x_m)_{m\geq 1}$ of $\widehat{K^*}$ are, in particular, systems of compatible roots of x_1, that is, for every $m, d \in \mathbf{Z}_{\geq 1}$ we have $x_m^m = x_1$ and $x_{md}^d = x_m$.

Theorem 1.34. *There is a unique isomorphism*

$$\varphi\colon \frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}} \longrightarrow \mathrm{H}^2(\Gamma_K, \widehat{\mu})$$

such that for every $x \in K(\mu)^{*w} \cap K^*$, every $(x_m)_{m\geq 1} \in \widehat{K^*}$ with $x_1 = x$ and every continuous set-theoretic section $s\colon \Gamma_K \longrightarrow \mathrm{Gal}(\overline{K}/K)$ we have

$$\varphi(x \cdot \mu_w K^{*w}) = \left[(\sigma, \tau) \mapsto \left(\frac{s(\sigma)s(\tau)x_{mw}}{s(\sigma\tau)x_{mw}}\right)_{m\geq 1}\right].$$

Proof. Exponentiation by w is a continuous Γ_K-module endomorphism of $\widehat{\mu}$, giving the well-adjusted sequence (see 1.14)

$$0 \longrightarrow \widehat{\mu} \xrightarrow{\cdot w} \widehat{\mu} \xrightarrow{\pi} \mu_w \longrightarrow 0$$

of topological Γ_K-modules. By Theorem 1.16 the following long sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^0(\Gamma_K, \widehat{\mu}) &\xrightarrow{\mathrm{H}^0(\cdot w)} \mathrm{H}^0(\Gamma_K, \widehat{\mu}) \xrightarrow{\mathrm{H}^0(\pi)} \mathrm{H}^0(\Gamma_K, \mu_w) \\ &\xrightarrow{\delta_0} \mathrm{H}^1(\Gamma_K, \widehat{\mu}) \xrightarrow{\mathrm{H}^1(\cdot w)} \mathrm{H}^1(\Gamma_K, \widehat{\mu}) \xrightarrow{\mathrm{H}^1(\pi)} \mathrm{H}^1(\Gamma_K, \mu_w) \\ &\xrightarrow{\delta_1} \mathrm{H}^2(\Gamma_K, \widehat{\mu}) \xrightarrow{\mathrm{H}^2(\cdot w)} \mathrm{H}^2(\Gamma_K, \widehat{\mu}) \xrightarrow{\mathrm{H}^2(\pi)} \cdots \end{aligned}$$

of continuous cohomology groups is exact. By Corollary 1.26 we have

$$\mathrm{Ann}_{\widehat{\mathbf{Z}}}(\mu(K)) \cdot \mathrm{H}^0(\Gamma_K, \widehat{\mu}) = 0.$$

As $\widehat{\mu}$ has no non-trivial w-torsion, it follows that

$$\mathrm{H}^0(\Gamma_K, \widehat{\mu}) = \widehat{\mu}^{\Gamma_K} = 0.$$

As $\mathrm{Ann}_{\widehat{\mathbf{Z}}}(\mu(K)) = w\widehat{\mathbf{Z}}$ (see Example 1.27) and $\mathrm{H}^m(\Gamma_K, \cdot)$ is an additive functor for every $m \in \mathbf{Z}_{\geq 0}$ (see Proposition 1.11), the group morphism $\mathrm{H}^m(\Gamma_K, \cdot w)$ is the zero map. Thus, the map $\delta_0 \colon \mu_w \longrightarrow \mathrm{H}^1(\Gamma_K, \widehat{\mu})$ is an isomorphism of groups.

Moreover, the long exact sequence above gives the exact sequence

$$0 \longrightarrow \mathrm{H}^1(\Gamma_K, \widehat{\mu}) \xrightarrow{\mathrm{H}^1(\pi)} \mathrm{H}^1(\Gamma_K, \mu_w) \xrightarrow{\delta_1} \mathrm{H}^2(\Gamma_K, \widehat{\mu}) \longrightarrow 0.$$

As Γ_K acts trivially on μ_w, we have $\mathrm{H}^1(\Gamma_K, \mu_w) = \mathrm{CHom}(\Gamma_K, \mu_w)$. By Kummer theory the map

$$\kappa \colon \frac{K(\mu)^{*w} \cap K^*}{K^{*w}} \longrightarrow \mathrm{CHom}(\Gamma_K, \mu_w)$$

defined by

$$uK^{*w} \mapsto \left(\sigma \mapsto \frac{\sigma(t)}{t}\right)$$

where $t \in \overline{K}^*$ is such that $t^w = x$, is an isomorphism of groups. Using Proposition 1.15, one easily checks that

$$\begin{array}{ccc} \mathrm{H}^1(\Gamma_K, \widehat{\mu}) & \xrightarrow{\mathrm{H}^1(\pi)} & \mathrm{CHom}(\Gamma_K, \mu_w) \\ {\scriptstyle \delta_0}\uparrow{\scriptstyle \wr} & & {\scriptstyle \wr}\uparrow{\scriptstyle \kappa} \\ \mu_w & \longrightarrow & \dfrac{K(\mu)^{*w} \cap K^*}{K^{*w}} \end{array}$$

is a commutative diagram, where the lower horizontal map is the natural inclusion. Hence, the map $\delta_1 \circ \kappa$ induces an isomorphism

$$\frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}} \longrightarrow \mathrm{H}^2(\Gamma_K, \widehat{\mu})$$

of groups, which we will call φ.

Let $x \in K(\mu)^{*w} \cap K^*$, $(x_m)_{m \geq 1} \in \widehat{K^*}$ with $x_1 = x$ and $s \colon \Gamma_K \longrightarrow \mathrm{Gal}(\overline{K}/K)$ a continuous set-theoretic section. We will show that the image of $x \cdot \mu_w K^{*w}$ under φ is

$$\left[(\sigma, \tau) \mapsto \left(\frac{s(\sigma)s(\tau)x_{mw}}{s(\sigma\tau)x_{mw}}\right)_{m \geq 1}\right].$$

Then we have $\kappa(x \cdot K^{*w}) = \left[\sigma \mapsto \frac{\sigma(x_w)}{x_w}\right]$. For brevity we will denote $\kappa(x \cdot K^{*w})$ by γ_x. Now, for the image of γ_x under δ_1 we are going to apply Proposition 1.15.

Define $\beta_x \colon \Gamma_K \longrightarrow \widehat{\mu}$ by $\sigma \mapsto \left(\frac{s(\sigma)(x_m)}{x_m}\right)_{m\geq 1}$ and note that it is an element of $\mathrm{C}^1(\Gamma_K, \widehat{\mu})$ that maps to γ_x under $\mathrm{C}^1(\Gamma_K, \pi)$. Moreover, writing out the formula for d_1 (see beginning of Section 1.3) we obtain

$$\begin{aligned} d_1(\beta_x)(\sigma,\tau) &= \left(\sigma\left(\frac{s(\tau)(x_m)}{x_m}\right)\cdot\frac{x_m}{s(\sigma\tau)(x_m)}\cdot\frac{s(\sigma)(x_m)}{x_m}\right)_{m\geq 1} \\ &= \left(s(\sigma)\left(\frac{s(\tau)(x_m)}{x_m}\right)\cdot\frac{x_m}{s(\sigma\tau)(x_m)}\cdot\frac{s(\sigma)(x_m)}{x_m}\right)_{m\geq 1} \\ &= \left(\frac{s(\sigma)s(\tau)(x_m)}{s(\sigma)(x_m)}\cdot\frac{x_m}{s(\sigma\tau)(x_m)}\cdot\frac{s(\sigma)(x_m)}{x_m}\right)_{m\geq 1} \\ &= \left(\frac{s(\sigma)s(\tau)(x_m)}{s(\sigma\tau)(x_m)}\right)_{m\geq 1}. \end{aligned}$$

On the other hand, define

$$\alpha_x \colon \Gamma_K \times \Gamma_K \longrightarrow \widehat{\mu}$$

by $(\sigma,\tau) \mapsto \left(\frac{s(\sigma)s(\tau)x_{mw}}{s(\sigma\tau)x_{mw}}\right)_{m\geq 1}$. Since $x \in K(\mu)^{*w}$, for all $m \in \mathbf{Z}_{\geq 1}$ we have

$$\frac{s(\sigma)s(\tau)x_{mw}}{s(\sigma\tau)x_{mw}} \in \mu_m.$$

The formula for $d_1(\beta_x)$ given above shows that the map α_x maps to $d_1(\beta_x)$ under $\mathrm{C}^2(\Gamma_K, \cdot w)$. Hence, by Proposition 1.15 the identity $\delta_1([\gamma_x]) = [\alpha_x]$ holds.

It follows that the image of $x \cdot \mu_w K^{*w}$ under φ is $[\alpha_x]$, as desired. ∎

9. Galois groups of maximal radical extensions

Throughout this section, let K be a number field, let $\overline{K}$ an algebraic closure of K, let $w = \#\mu(K)$, and let

$$\Lambda(K) = \frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}}.$$

Let $n \in \mathbf{Z}_{\geq 0}$, and let F be a free $\widehat{\mathbf{Z}}$-module of rank n. Let S be the set of isomorphism classes of profinite groups G such that there exists a natural extension of Γ_K

$$0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1,$$

and let T be the set of subgroups of $\mathrm{H}^2(\Gamma_K, \widehat{\mu})$ that can be generated by n elements. Then by Theorem 1.28 the map $\rho\colon S \longrightarrow T$ given by

$$[G] \mapsto \{\mathrm{H}^2(\Gamma_K, f)([0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1]) : f \in \mathrm{Hom}(F, \widehat{\mu})\}$$

is a bijection. Let T' be the set of subgroups of $\Lambda(K)$ that can be generated by n elements. The isomorphism φ of Theorem 1.34 induces a bijection

$$\Phi\colon T' \longrightarrow T$$

given by $H \mapsto \varphi(H)$, and its inverse $\Phi^{-1}\colon T \longrightarrow T'$ is given by $H \mapsto \varphi^{-1}(H)$. Thus, the map

$$\chi = \Phi^{-1} \circ \rho$$

is a bijection of S with T' given by

$$\chi([G]) = \varphi^{-1}(\{\mathrm{H}^2(\Gamma_K, f)([0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1]) : f \in \mathrm{Hom}(F, \widehat{\mu})\}).$$

Observe that for any finitely generated subgroup W of K^* of rank n, the Galois group

$$\mathrm{Gal}(K(W^{1/\infty})/K)$$

defines an element of S by Theorem 1.5 and Proposition 1.7. In this section we prove the following theorem.

Theorem 1.35. *Let W be a finitely generated subgroup of K^* of rank n, and let*

$$\mathrm{Cyc}(W) = W^{1/\infty} \cap K(\mu)^*.$$

Then the image of the isomorphism class of $\mathrm{Gal}(K(W^{1/\infty})/K)$ *in* S *under the bijection* χ *is*

$$\frac{(\mathrm{Cyc}(W)^w \cap K^*)K^{*w}}{\mu_w K^{*w}} \subset \Lambda(K).$$

Let A be a discrete abelian group. Then $\mathrm{Hom}(A, \widehat{\mu})$ is a topological Γ_K-module, where Γ_K acts via the second argument. For any $x \in A$ we have a continuous Γ_K-linear morphism $\mathrm{ev}_x \colon \mathrm{Hom}(A, \widehat{\mu}) \longrightarrow \widehat{\mu}$ given by $f \mapsto f(x)$. This induces a group morphism

$$\mathrm{H}^2(\Gamma_K, \mathrm{ev}_x) \colon \mathrm{H}^2(\Gamma_K, \mathrm{Hom}(A, \widehat{\mu})) \longrightarrow \mathrm{H}^2(\Gamma_K, \widehat{\mu}).$$

As $\mathrm{H}^2(\Gamma_K, \cdot)$ is an additive functor (see 1.11) and for any $x, y \in A$ we have $\mathrm{ev}_{x+y} = \mathrm{ev}_x + \mathrm{ev}_y$, there is a group morphism

$$\psi_A \colon \mathrm{H}^2(\Gamma_K, \mathrm{Hom}(A, \widehat{\mu})) \longrightarrow \mathrm{Hom}(A, \mathrm{H}^2(\Gamma_K, \widehat{\mu}))$$

given by $[c] \mapsto (x \mapsto \mathrm{H}^2(\mathrm{ev}_x)(c))$. This defines a morphism of additive functors in A.

Lemma 1.36. *Let* W *be a finitely generated subgroup of* K^* *of rank* n*, and let*

$$\mathrm{Cyc}(W) = W^{1/\infty} \cap K(\mu)^*.$$

Let ψ *be the group morphism* $\psi_{\mathrm{Cyc}(W)}$ *defined above, and let* $\widehat{K^*}$ *be as defined in the beginning of section* 1.8*. Then*

$$\psi \colon \mathrm{H}^2(\Gamma_K, \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})) \longrightarrow \mathrm{Hom}(\mathrm{Cyc}(W), \mathrm{H}^2(\Gamma_K, \widehat{\mu}))$$

is a group isomorphism such that for every $x \in \mathrm{Cyc}(W)$*, for every* $(x_m)_{m\geq 1} \in \widehat{K^*}$ *with* $x_1 = x$ *and for every continuous set-theoretic section* $s \colon \Gamma_K \longrightarrow \mathrm{Gal}(\overline{K}/K)$*, the image of the equivalence class of the natural extension of* Γ_K

$$e \colon 0 \longrightarrow \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) \longrightarrow \mathrm{Gal}(K(W^{1/\infty})/K) \longrightarrow \Gamma_K \longrightarrow 1$$

of Theorem 1.5 *is defined by*

$$x \mapsto \left[(\sigma, \tau) \mapsto \left(\frac{s(\sigma)s(\tau)x_m}{s(\sigma\tau)x_m} \right)_{m \geq 1} \right].$$

Proof. We first show that $\psi_{\mathbf{Z}}$ is an isomorphism. To this end, observe that

$$\chi_{\widehat{\mu}} \colon \operatorname{Hom}(\mathbf{Z}, \widehat{\mu}) \longrightarrow \widehat{\mu}$$

defined by $f \mapsto f(1)$ is an isomorphism of Γ_K-modules. Hence

$$\mathrm{H}^2(\Gamma_K, \chi_{\widehat{\mu}}) \colon \mathrm{H}^2(\Gamma_K, \operatorname{Hom}(\mathbf{Z}, \widehat{\mu})) \longrightarrow \mathrm{H}^2(\Gamma_K, \widehat{\mu})$$

is an isomorphism of groups. Moreover

$$\chi_{\mathrm{H}^2(\Gamma_K, \widehat{\mu})} \colon \operatorname{Hom}(\mathbf{Z}, \mathrm{H}^2(\Gamma_K, \widehat{\mu})) \longrightarrow \mathrm{H}^2(\Gamma_K, \widehat{\mu})$$

is an isomorphism of groups. Since $\chi_{\mathrm{H}^2(\Gamma_K, \widehat{\mu})} \circ \psi_{\mathbf{Z}} = \mathrm{H}^2(\Gamma_K, \chi_{\widehat{\mu}})$, the map $\psi_{\mathbf{Z}}$ is an isomorphism.

Now, note that $\operatorname{Hom}(\operatorname{Cyc}(W), \widehat{\mu}) = \operatorname{Hom}(\operatorname{Cyc}(W)/\mu, \widehat{\mu})$ and that $\operatorname{Cyc}(W)/\mu \cong \mathbf{Z}^n$ for some $n \in \mathbf{Z}_{\geq 1}$ (see Lemma 1.4). Moreover, since μ is divisible and $\mathrm{H}^2(\Gamma_K, \widehat{\mu})$ has exponent w (see Theorem 1.34), we have

$$\operatorname{Hom}(\operatorname{Cyc}(W), \mathrm{H}^2(\Gamma_K, \widehat{\mu})) = \operatorname{Hom}(\operatorname{Cyc}(W)/\mu, \mathrm{H}^2(\Gamma_K, \widehat{\mu})).$$

Then by additivity of $\mathrm{H}^2(\Gamma_K, \operatorname{Hom}(\cdot, \widehat{\mu}))$ and $\operatorname{Hom}(\cdot, \mathrm{H}^2(\Gamma_K, \widehat{\mu}))$, the map $\psi_{\operatorname{Cyc}(W)}$ is an isomorphism of groups.

For the second part of the lemma, let $x \in \operatorname{Cyc}(W)$, $(x_m)_{m \geq 1} \in \widehat{K^*}$ with $x_1 = x$ and $s \colon \Gamma_K \longrightarrow \operatorname{Gal}(\overline{K}/K)$ a continuous set-theoretic section. Let

$$e \colon 0 \longrightarrow \operatorname{Hom}(\operatorname{Cyc}(W), \widehat{\mu}) \longrightarrow \operatorname{Gal}(K(W^{1/\infty})/K) \longrightarrow \Gamma_K \longrightarrow 0$$

be as in Theorem 1.5. Then e corresponds to the element $[(\sigma,\tau)\mapsto s(\sigma)s(\tau)s(\sigma\tau)^{-1}]$ of the cohomology group $\mathrm{H}^2(\Gamma_K,\mathrm{Hom}(\mathrm{Cyc}(W),\widehat{\mu}))$ (see Theorem 1.20).

Recall that the isomorphism $\alpha\colon\ \mathrm{Gal}(K(W^{1/\infty})/K(\mu))\longrightarrow\mathrm{Hom}(\mathrm{Cyc}(W),\widehat{\mu})$ is defined by $\sigma\mapsto\left(y\mapsto\left(\frac{\sigma(y_m)}{y_m}\right)_{m\geq 1}\right)$ (see Theorem 1.5). Then we deduce

$$\begin{aligned}\psi_{\mathrm{Cyc}(W)}(e)(x) &= \left[(\sigma,\tau)\mapsto\alpha(s(\sigma)s(\tau)s(\sigma\tau)^{-1})(x)\right]\\ &= \left[(\sigma,\tau)\mapsto\left(\frac{s(\sigma)s(\tau)s(\sigma\tau)^{-1}(x_m)}{x_m}\right)_{m\geq 1}\right].\end{aligned}$$

Observe that for any $\sigma,\tau\in\Gamma_K$ and $m\in\mathbf{Z}_{\geq 1}$ the identity

$$\frac{s(\sigma)s(\tau)\left(\frac{s(\sigma\tau)^{-1}x_m}{x_m}\right)}{s(\sigma\tau)\left(\frac{s(\sigma\tau)^{-1}x_m}{x_m}\right)}=1$$

holds. Thus, for any $\sigma,\tau\in\Gamma_K$ and $m\in\mathbf{Z}_{\geq 1}$ we have

$$\frac{s(\sigma)s(\tau)s(\sigma\tau)^{-1}x_m}{x_m}=\frac{s(\sigma)s(\tau)x_m}{s(\sigma\tau)x_m}\cdot\frac{s(\sigma)s(\tau)\left(\frac{s(\sigma\tau)^{-1}x_m}{x_m}\right)}{s(\sigma\tau)\left(\frac{s(\sigma\tau)^{-1}x_m}{x_m}\right)}=\frac{s(\sigma)s(\tau)x_m}{s(\sigma\tau)x_m}.$$

This shows that

$$\psi_{\mathrm{Cyc}(W)}(e)(x)=\left[(\sigma,\tau)\mapsto\left(\frac{s(\sigma)s(\tau)x_m}{s(\sigma\tau)x_m}\right)_{m\geq 1}\right].$$

■

Let W be a finitely generated subgroup of K^* of rank n, and let $\mathrm{Sat}(W)=W^{1/\infty}\cap K^*$ and $\mathrm{Cyc}(W)=W^{1/\infty}\cap K(\mu)^*$. By Proposition 1.3 we have

$$\mathrm{Cyc}(W)=\mu\cdot(\mathrm{Sat}(W)^{1/w}\cap K(\mu)^*).$$

Moreover, as μ is divisible and $\Lambda(K)$ has exponent w, the map

$$\nu_W\colon\ \mathrm{Cyc}(W)\longrightarrow\Lambda(K)$$

defined by $x\mapsto y\cdot\mu_w K^{*w}$, where $x^w=\zeta\cdot y$ for some $\zeta\in\mu$ and $y\in K^*$, is a well-defined group morphism.

Lemma 1.37. *Let W be a finitely generated subgroup of K^* of rank n, and let*

$$\mathrm{Cyc}(W) = W^{1/\infty} \cap K(\mu)^*.$$

Then for every $x \in \mathrm{Cyc}(W)$, for every $(x_m)_{m\geq 1} \in \widehat{K^*}$ with $x_1 = x$ and for every continuous set-theoretic section $s\colon \Gamma_K \longrightarrow \mathrm{Gal}(\overline{K}/K)$ we have

$$(\varphi \circ \nu_W)(x) = \left[(\sigma,\tau) \mapsto \left(\frac{s(\sigma)s(\tau)x_m}{s(\sigma\tau)x_m}\right)_{m\geq 1}\right]$$

where φ is defined in Theorem 1.34.

Proof. Let $x \in \mathrm{Cyc}(W)$, $(x_m)_{m\geq 1} \in \widehat{K^*}$ with $x_1 = x$ and $s\colon \Gamma_K \longrightarrow \mathrm{Gal}(\overline{K}/K)$ a continuous set-theoretic section. Let $\zeta \in \mu$ and $y \in K^*$ be such that $x^w = y\zeta$. Then $(x_m)^w_{m\geq 1} = (y_m)(\zeta_m)_{m\geq 1}$ for some $(y_m)_{m\geq 1} \in \widehat{K^*}$ with $y_1 = y$ and $(\zeta_m)_{m\geq 1} \in \widehat{K^*}$ with $\zeta_1 = \zeta$. Then by Theorem 1.34 we have

$$\begin{aligned}
(\varphi \circ \nu_W)(x) &= \left[(\sigma,\tau) \mapsto \left(\frac{s(\sigma)s(\tau)y_{mw}}{s(\sigma\tau)y_{mw}}\right)_{m\geq 1}\right] \\
&= \left[(\sigma,\tau) \mapsto \left(\frac{s(\sigma)s(\tau)(x_m\zeta_{mw}^{-1})}{s(\sigma\tau)(x_m\zeta_{mw}^{-1})}\right)_{m\geq 1}\right] \\
&= \left[(\sigma,\tau) \mapsto \left(\frac{s(\sigma)s(\tau)x_m}{s(\sigma\tau)x_m}\right)_{m\geq 1}\right]
\end{aligned}$$

where we used that for every $\gamma \in \Gamma_K$ and $m \geq 1$ we have $s(\gamma)\zeta_m = \gamma\zeta_m$. ∎

Lemma 1.38. *Let W be a finitely generated subgroup of K^* of rank n, let*

$$\mathrm{Sat}(W) = W^{1/\infty} \cap K^*,$$

and let

$$\mathrm{Cyc}(W) = W^{1/\infty} \cap K(\mu)^*.$$

Then the kernel of ν_W is $\mathrm{Sat}(W) \cdot \mu$ and its image is

$$\nu_W(\mathrm{Cyc}(W)) = \frac{(\mathrm{Cyc}(W)^w \cap K^*) \cdot K^{*w}}{\mu_w K^{*w}}.$$

Proof. This is clear since modulo μ the map ν_W is given by exponentiation by w, and because by Proposition 1.3 we have $\mathrm{Cyc}(W) = \mu \cdot (\mathrm{Sat}(W)^{1/w} \cap K(\mu)^*)$. ∎

Proof of Theorem 1.35. Let $G_W = \mathrm{Gal}(K(W^{1/\infty})/K)$, and let $\nu = \nu_W$. Recall the definitions of ρ and Φ^{-1} from the beginning of this section. We will first show that

$$\rho([G_W]) = \Phi(\nu(\mathrm{Cyc}(W))),$$

where Φ is the inverse of Φ^{-1}. To this end, let

$$E_W \colon 0 \longrightarrow \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) \longrightarrow G_W \longrightarrow \Gamma_K \longrightarrow 1$$

be the natural extension of Γ_K of Theorem 1.5. Note that

$$\rho([G_W]) = \{\mathrm{H}^2(\Gamma_K, f)([0 \longrightarrow F \longrightarrow G_W \longrightarrow \Gamma_K \longrightarrow 1]) : f \in \mathrm{Hom}(F, \widehat{\mu})\},$$

where it does not matter which equivalence class of natural extensions of Γ_K by F we take (see Theorem 1.28). As $\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu})$ is isomorphic to F as topological $\widehat{\mathbf{Z}}$-module, we have

$$\rho([G_W]) = \{\mathrm{H}^2(\Gamma_K, g)([E_W]) : g \in \mathrm{Hom}(\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}), \widehat{\mu})\},$$

where again we are free to choose which equivalence class of natural extensions of Γ_K we use.

On the other hand, note that $\nu(\mathrm{Cyc}(W))$ is indeed an element of T', since $\mathrm{Cyc}(W)/\mu$ is free of rank n (see Lemma 1.4) and $\mu \subset \ker(\nu)$. Hence

$$\Phi(\nu(\mathrm{Cyc}(W))) = (\varphi \circ \nu)(\mathrm{Cyc}(W))$$

is an element of T. By Lemma 1.36 and Lemma 1.37 we have

$$(\varphi \circ \nu)(\mathrm{Cyc}(W)) = \psi([E_W])(\mathrm{Cyc}(W))$$

where $[E_W]$ is the equivalence class of E_W in $\mathrm{H}^2(\Gamma_K, \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}))$, and ψ is defined in Lemma 1.36. Recall that

$$\psi([E_W])\colon\ \mathrm{Cyc}(W) \longrightarrow \mathrm{H}^2(\Gamma_K, \widehat{\mu})$$

is given by $x \mapsto \mathrm{H}^2(\Gamma_K, \mathrm{ev}_x)([E_W])$, where $\mathrm{ev}_x\colon\ \mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}) \longrightarrow \widehat{\mu}$ is evaluation at x. Hence

$$\psi([E_W])(\mathrm{Cyc}(W)) = \{\mathrm{H}^2(\Gamma_K, \mathrm{ev}_x)([E_W]) : x \in \mathrm{Cyc}(W)\},$$

which we want to be equal to

$$\{\mathrm{H}^2(\Gamma_K, g)([E_W]) : g \in \mathrm{Hom}(\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}), \widehat{\mu})\}.$$

To see this, note that the canonical group morphism

$$\mathrm{Cyc}(W) \longrightarrow \mathrm{Hom}(\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}), \widehat{\mu})$$

given by $x \mapsto \mathrm{ev}_x$ has kernel μ. It induces an injective $\widehat{\mathbf{Z}}$-module morphism

$$(\mathrm{Cyc}(W)/\mu) \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}} \longrightarrow \mathrm{Hom}(\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}), \widehat{\mu}) = \mathrm{Hom}(\mathrm{Hom}(\mathrm{Cyc}(W)/\mu, \widehat{\mu}), \widehat{\mu}). \quad (*)$$

Note that $(*)$ is an isomorphism when $\mathrm{Cyc}(W)/\mu$ is replaced by $\mathbf{Z}^n$. As

$$\mathrm{Cyc}(W)/\mu \cong \mathbf{Z}^n$$

as groups, the map $(*)$ is an isomorphism (cf. the proof of Lemma 1.36). Hence, we have

$$\begin{aligned}
\Phi(\nu(\mathrm{Cyc}(W))) &= (\varphi \circ \nu)(\mathrm{Cyc}(W)) \\
&= \psi([E_W])(\mathrm{Cyc}(W)) \\
&= \{\mathrm{H}^2(\Gamma_K, \mathrm{ev}_x)([E_W]) : x \in \mathrm{Cyc}(W)\} \\
&= \{\mathrm{H}^2(\Gamma_K, g)([E_W]) : g \in \mathrm{Hom}(\mathrm{Hom}(\mathrm{Cyc}(W), \widehat{\mu}), \widehat{\mu})\} \\
&= \rho([G_W]),
\end{aligned}$$

as we wanted to show.

Now, applying Φ^{-1} we obtain $\chi([G_W]) = \nu(\mathrm{Cyc}(W))$. Hence, by Lemma 1.38 we have

$$\chi([G_W]) = \nu(\mathrm{Cyc}(W)) = \frac{(\mathrm{Cyc}(W)^w \cap K^*) \cdot K^{*w}}{\mu_w K^{*w}}.$$

■

10. Lifting

In this section we prove the following two theorems.

Theorem 1.39. *Let $w \in \mathbf{Z}_{>1}$, and let M be a free module over $\mathbf{Z}/w\mathbf{Z}$. Let Λ be a submodule of M, let $n \in \mathbf{Z}_{\geq 1}$, and let $H \subset \Lambda$ be a finite subgroup generated by at most n elements. Assume that $M[l]/\Lambda[l]$ is infinite for every prime l dividing w. Then there is a submodule I of M that is free over $\mathbf{Z}/w\mathbf{Z}$ of rank n such that $I \cap \Lambda = H$.*

Theorem 1.40. *Let K be a number field unequal to $\mathbf{Q}$, and let $w = \#\mu(K)$. Let $M = K^*/\mu_w K^{*w}$ and $\Lambda = \frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}}$. Then for every prime l dividing w the quotient $M[l]/\Lambda[l]$ is infinite.*

We remark that Theorem 1.40 does not hold for $\mathbf{Q}$, since

$$\frac{\mathbf{Q}(\mu)^{*2} \cap \mathbf{Q}^*}{\pm \mathbf{Q}^{*2}} = \mathbf{Q}^*/\pm \mathbf{Q}^{*2}$$

holds as a corollary of the Kronecker-Weber theorem.

Proof of 1.39. As $\mathbf{Z}/w\mathbf{Z}$ is a Gorenstein ring, projective modules are injective. Therefore M is injective over $\mathbf{Z}/w\mathbf{Z}$. Let I be a free $\mathbf{Z}/w\mathbf{Z}$-module of rank n and choose an injection

$H \longrightarrow I$. Let $H \longrightarrow \Lambda \longrightarrow M$ be the composition of injections. Then by injectivity of M there is a group morphism $f\colon I \longrightarrow M$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & I & \xrightarrow{\pi} & I/H & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \overline{f}} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & M & \xrightarrow[\pi']{} & M/\Lambda & \longrightarrow & 0 \end{array}$$

commutative, where π and π' are the canonical quotient maps, and $\overline{f}$ is the induced map on the quotients.

We will construct a group morphism $g\colon I/H \longrightarrow M$ such that the map

$$\overline{f + g\pi} = \overline{f} + \pi' g\colon I/H \longrightarrow M/\Lambda$$

induced by $f + g\pi$ is injective. Given such a g, the Snake Lemma implies that the map $f + g\pi\colon I \longrightarrow M$ is injective. Then we have injective morphisms $I \longrightarrow M$ and $I/H \longrightarrow M/\Lambda$ making the above diagram commute, which finishes the proof, for I can be identified with a free $\mathbf{Z}/w\mathbf{Z}$-submodule of M of rank n whose intersection with Λ is H.

To construct g, we first assume $w = l^k$ where l is prime and $k \in \mathbf{Z}_{\geq 1}$. Let

$$(-)[l]\colon \mathbf{Ab} \longrightarrow \mathbf{Ab}$$

be the functor of the category of abelian groups to the category of abelian groups sending objects A to their l-torsion subgroup $A[l] \cong \mathrm{Hom}(\mathbf{Z}/l\mathbf{Z}, A)$, and morphisms $\phi\colon A \longrightarrow B$ to their restriction $\phi[l]\colon A[l] \longrightarrow B[l]$ to the l-torsion subgroup of the domain.

As $(-)[l]$ is left exact, we obtain the exact sequence

$$0 \longrightarrow \Lambda[l] \longrightarrow M[l] \xrightarrow{\pi'[l]} (M/\Lambda)[l].$$

This induces the injection $M[l]/\Lambda[l] \longrightarrow (M/\Lambda)[l]$, which we also denote by $\pi'[l]$ by abuse of notation. Let $c\colon (M/\Lambda)[l] \longrightarrow N$ be the cokernel of $\overline{f}[l]$, and let N_0 be the image of

$c \circ \pi'[l]$. As $(I/H)[l]$ is finite, it follows that N and N_0 are both infinite. We have the following commutative diagram

$$\begin{array}{ccccccc} (I/H)[l] & \xrightarrow{\overline{f}[l]} & (M/\Lambda)[l] & \xrightarrow{c} & N & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \pi'[l]} & & \uparrow{\scriptstyle \iota} & & \\ & & M[l]/\Lambda[l] & \xrightarrow{c\circ\pi'[l]} & N_0 & \longrightarrow & 0 \end{array}$$

with exact rows. Observe that all groups in this diagram are $\mathbf{F}_l$-vector spaces, hence they are injective and projective over $\mathbf{F}_l$. Since $(I/H)[l]$ is finite dimensional over $\mathbf{F}_l$ and N_0 is infinite dimensional over $\mathbf{F}_l$, we can embed the former in the latter. Choose such an embedding and call it $\overline{j}$. Using projectivity of $(I/H)[l]$, lift $\overline{j}$ to a morphism $j\colon (I/H)[l] \longrightarrow M[l]$ via the surjective composition

$$M[l] \longrightarrow M[l]/\Lambda[l] \longrightarrow N_0.$$

Composing with the canonical embedding $M[l] \longrightarrow M$, we obtain a morphism

$$(I/H)[l] \longrightarrow M.$$

Using injectivity of M, we lift this map to a map $g\colon I/H \longrightarrow M$ via the embedding $(I/H)[l] \longrightarrow I/H$.

Now we show that $\overline{f + g\pi} = \overline{f} + \pi' g$ is injective. As $w = l^k$, it suffices to show that $(\overline{f} + \pi' g)[l]$ is injective. Note that

$$(\overline{f} + \pi' g)[l] = f[l] + \pi'[l] \circ q \circ g[l],$$

where q is the surjection $M[l] \longrightarrow M[l]/\Lambda[l]$. Composing with c gives

$$c \circ (\overline{f} + \pi' g)[l] = c \circ f[l] + c \circ \pi'[l] \circ q \circ g[l] = 0 + \iota \circ \overline{j}.$$

As $\overline{j}$ and ι are both injective, the composition $c \circ (\overline{f} + \pi' g)[l]$ is injective. It follows that $(\overline{f} + \pi' g)[l]$ is injective. Thus, we have constructed g such that $\overline{f + g\pi}$ is injective, proving the theorem for w a prime power.

Now, suppose $w \in \mathbf{Z}_{>1}$. Let l be a prime divisor of w. Restrict f to the l-part of I and do the above for the l-part of H, I, Λ and M. This gives a morphism g_l for every l dividing w. The direct sum of all the g_l defines a map $g\colon I/H \longrightarrow M$ such that $\overline{f+g\pi}$ is injective, which finishes the proof. ∎

Lemma 1.41. *Let K be a number field, let L be a finite extension of K, and let F be a (not necessarily finite) abelian extension of K. Let $M = F \cdot L$. Let p be a prime of K that does not ramify in L, and let $\mathfrak{p}$ and $\mathfrak{q}$ be primes of L lying above p. Then the inertia groups $\mathrm{I}_{\mathfrak{p}}(M/L)$ and $\mathrm{I}_{\mathfrak{q}}(M/L)$ are equal.*

Proof. Let $\mathrm{I}_p = \mathrm{I}_p(F/K)$, $\mathrm{I}_{\mathfrak{p}} = \mathrm{I}_{\mathfrak{p}}(M/L)$ and $\mathrm{I}_{\mathfrak{q}} = \mathrm{I}_{\mathfrak{q}}(M/L)$. As p does not ramify in L, we have

$$L \cap F \subset F^{\mathrm{I}_p} = E.$$

Recall that there is a canonical isomorphism between the Galois groups $\mathrm{Gal}(F/L \cap F)$ and $\mathrm{Gal}(M/L)$. Hence I_p corresponds to a unique subgroup of $\mathrm{Gal}(M/L)$, which we again denote by I_p.

Observe that $E \cdot L = M^{\mathrm{I}_p}$. We claim that $E \cdot L$ is contained in $M^{\mathrm{I}_{\mathfrak{p}}}$. Indeed, let $\mathfrak{s}$ be a prime of $E \cdot L$ dividing $\mathfrak{p}$. Then $\mathfrak{s} \cap E$ is unramified over p, since E is the inertia subfield of p in F. Moreover, as M is the compositum of F with L, and $\mathfrak{s} \cap E$ is unramified over $\mathfrak{s} \cap (F \cap L)$, it follows that $\mathfrak{s}$ is unramified over $\mathfrak{p}$. Hence $M^{\mathrm{I}_p} \subset M^{\mathrm{I}_{\mathfrak{p}}}$, which gives $\mathrm{I}_{\mathfrak{p}} \subset \mathrm{I}_p$ and proves the claim.

Consider $\mathrm{I}_{\mathfrak{p}}$ as a subgroup of $\mathrm{Gal}(F/F \cap L)$, and note that $\mathrm{I}_{\mathfrak{p}} \subset \mathrm{I}_p$ implies $E \subset F^{\mathrm{I}_{\mathfrak{p}}}$. Let $\mathfrak{r}$ be a prime of $M^{\mathrm{I}_{\mathfrak{p}}}$ dividing $\mathfrak{p}$. Then $\mathfrak{r}$ is unramified over $E \cdot L$, as $E \cdot L$ is contained in the inertia subfield of $\mathfrak{r} \cap L = \mathfrak{p}$ in M. Moreover, $\mathfrak{r} \cap (E \cdot L)$ is unramified over E, since $\mathfrak{p}$ is unramified over $\mathfrak{p} \cap (L \cap F)$.

On the other hand, $\mathfrak{r} \cap F^{\mathrm{I}_{\mathfrak{p}}}$ is totally ramified over E, since E is the inertia subfield of p in F. This implies that $\mathfrak{r} \cap F^{\mathrm{I}_{\mathfrak{p}}}$ is totally ramified and unramified over E, hence $F^{\mathrm{I}_{\mathfrak{p}}} = E$.

It follows that $\mathrm{I}_{\mathfrak{p}} = \mathrm{I}_p$.

Analogously, we find $\mathrm{I}_p = \mathrm{I}_{\mathfrak{q}}$, so that $\mathrm{I}_{\mathfrak{p}} = \mathrm{I}_{\mathfrak{q}}$, as desired. ∎

Proof of Theorem 1.40. Let l be a prime divisor of w. Let $\tilde{K} = K(K^{*1/w})$, let M_l be the maximal exponent l extension of $K(\mu_{w^2})$ contained inside of $\tilde{K}$, and let Λ_l be the maximal exponent l extension of $K(\mu_{w^2})$ contained inside of $K(\mu) \cap \tilde{K}$. One easily checks that under Kummer and Galois dualities with $K(\mu_{w^2})$ as basefield, the quotient $M[l]$ corresponds to M_l, and $\Lambda[l]$ corresponds to Λ_l. To show that $M[l]/\Lambda[l]$ is infinite is then equivalent to showing that M_l/Λ_l is an infinite extension.

Suppose by contradiction that M_l/Λ_l is finite. Then there is a finite extension L of $K(\mu_{w^2})$ such that $M_l = L \cdot \Lambda_l$. Let $F = \mathbf{Q}(\mu) \cap \Lambda_l$, and note that $F \cdot K(\mu_{w^2}) = \Lambda_l$, so that $F \cdot L = M_l$.

Now, let p be a prime number different from l that splits completely in L. As $K \neq \mathbf{Q}$, there are two distinct primes $\mathfrak{p}$ and $\mathfrak{q}$ of K above p. Let $\mathfrak{p}'$ and $\mathfrak{q}'$ be primes of L above $\mathfrak{p}$ and $\mathfrak{q}$, respectively. Since F is abelian over $\mathbf{Q}$, and p is unramified in L, Lemma 1.41 with $\mathbf{Q}$ in the role of K implies that $\mathrm{I}_{\mathfrak{p}'}(M_l/L) = \mathrm{I}_{\mathfrak{q}'}(M_l/L)$. Moreover L is unramified at p over K, so we have

$$\mathrm{I}_{\mathfrak{p}}(M_l/K) = \mathrm{I}_{\mathfrak{p}'}(M_l/L) = \mathrm{I}_{\mathfrak{q}'}(M_l/L) = \mathrm{I}_{\mathfrak{q}}(M_l/K).$$

Let $\alpha \in K^*$ such that α does not have a l-th root in L, $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$, and $\alpha \notin \mathfrak{q}$. Then $X^l - \alpha \in K[X]$ is Eisenstein at $\mathfrak{p}$, so that $K' = K(\alpha^{1/l})$ is totally ramified at $\mathfrak{p}$. Therefore the inertia group $\mathrm{I}_{\mathfrak{p}}(K'/K)$ is nontrivial. However, the prime $\mathfrak{q}$ does not contain l nor α, which implies that $\mathfrak{q}$ does not ramify in K'. Note that K' is contained in $\tilde{K}$, and moreover, as it has exponent l over K, it is contained in M_l. Thus, it follows that $\mathrm{I}_{\mathfrak{p}}(M_l/K) \neq \mathrm{I}_{\mathfrak{q}}(M_l/K)$, which is a contradiction. We conclude that M_l has infinite degree over Λ_l, as desired. ∎

11. The main theorem

In this section we prove the main theorem of this chapter.

Theorem 1.42 (Main theorem)**.** *Let $n \in \mathbf{Z}_{\geq 0}$, and let F be a free $\widehat{\mathbf{Z}}$-module of rank n. Let G be a profinite group, and let K be a number field. Then the following are equivalent.*

(a) *There exists a finitely generated subgroup $W \subset K^*$ of rank n such that*

$$G \cong \mathrm{Gal}(K(W^{1/\infty})/K)$$

as profinite groups.

(b) *There is a natural extension of Γ_K*

$$0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1$$

such that if $K = \mathbf{Q}$, the image of F in G equals the algebraic commutator subgroup $[G, G]$ of G.

Proof of main theorem. As the implication (a) to (b) was already proven in Section 1.2, it remains to show the implication (b) to (a).

First, suppose K is unequal to $\mathbf{Q}$, and let us be given a natural Γ_K-extension

$$0 \longrightarrow F \longrightarrow G \longrightarrow \Gamma_K \longrightarrow 1.$$

Then we want to show that there is $W \subset K^*$ of rank n such that $G \cong \mathrm{Gal}(K(W^{1/\infty})/K)$ as profinite groups.

Let S be the set of isomorphism classes of profinite groups that are natural Γ_K-extensions by F. Let T' be the set of subgroups of

$$\Lambda = \frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}}$$

that can be generated by at most n elements. As described in the beginning of Section 1.9, there is by Theorems 1.28 and 1.34 a bijection χ of S with T'. Under this bijection the class of G in S corresponds to a unique element, say H, of T'.

By [Iwa53, Lemma 3] we know that K^*/μ_w is free over $\mathbf{Z}$. It follows that

$$M = K^*/\mu_w K^{*w}$$

is free over $\mathbf{Z}/w\mathbf{Z}$. Then by Theorem 1.40 and Theorem 1.39, there exists $I \subset M$ such that I is free over $\mathbf{Z}/w\mathbf{Z}$ of rank n and $I \cap \Lambda = H$. Let $x_1, \ldots, x_n$ be a $\mathbf{Z}/w\mathbf{Z}$-basis of I, and lift them to K^*, to say $y_1, \ldots, y_n$. Let W be the group generated by $y_1, \ldots, y_n$.

Let

$$\mathrm{Sat}(W) = W^{1/\infty} \cap K^*$$

and

$$\mathrm{Cyc}(W) = W^{1/\infty} \cap K(\mu)^*.$$

By Lemma 1.4 the group $\mathrm{Sat}(W)$ is finitely generated of rank n. As $\mathrm{Sat}(W)$ contains W, and the image of W under the canonical map

$$K^* \longrightarrow K^*/\mu_w K^{*w}$$

is equal to the free module I of rank n over $\mathbf{Z}/w\mathbf{Z}$, the image of $\mathrm{Sat}(W)$ is also equal to I. Hence, the identity

$$I = \frac{\mathrm{Sat}(W)K^{*w}}{\mu_w K^{*w}}$$

holds. Let $G_W = \mathrm{Gal}(K(W^{1/\infty})/K)$. Then Theorem 1.35 implies that

$$\chi([G_W]) = \frac{(\mathrm{Cyc}(W)^w \cap K^*)K^{*w}}{\mu_w K^{*w}}.$$

Moreover, recall that

$$\mathrm{Cyc}(W) = \mu \cdot (\mathrm{Sat}(W)^{1/w} \cap K(\mu)^*)$$

by Proposition 1.3. Hence, we have

$$\begin{aligned} H = I \cap \Lambda &= \frac{\mathrm{Sat}(W)K^{*w}}{\mu_w K^{*w}} \bigcap \frac{K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}} \\ &= \frac{\mathrm{Sat}(W)K^{*w} \cap K(\mu)^{*w} \cap K^*}{\mu_w K^{*w}} \\ &= \frac{(\mathrm{Sat}(W) \cap K(\mu)^{*w} \cap K^*)K^{*w}}{\mu_w K^{*w}} \\ &= \frac{(\mathrm{Cyc}(W)^w \cap K^*)K^{*w}}{\mu_w K^{*w}} \\ &= \chi([G_W]), \end{aligned}$$

we see that H is the image of $[G_W]$. As χ is a bijection, it follows that $G \in [G_W]$, that is, we have $G \cong G_W$.

Now, suppose K is equal to $\mathbf{Q}$, and note that $\Gamma_K = \widehat{\mathbf{Z}}^*$. Let

$$E\colon 0 \longrightarrow F \longrightarrow G \longrightarrow \widehat{\mathbf{Z}}^* \longrightarrow 1$$

be a natural extension of $\widehat{\mathbf{Z}}^*$ with $F = [G, G]$. Suppose that $n = 1$. Since the semi-direct product has commutator subgroup $2\widehat{\mathbf{Z}}$ and $[G, G] = \widehat{\mathbf{Z}}$, it follows that G is not the trivial extension. Then [Jav13, Theorem 1, page v] states that any natural extension of $\widehat{\mathbf{Z}}^*$ by $\widehat{\mathbf{Z}}$ that is not the trivial extension $\widehat{\mathbf{Z}} \rtimes \widehat{\mathbf{Z}}^*$, is isomorphic to a Galois group $\mathrm{Gal}(\mathbf{Q}(\langle r \rangle^{1/\infty})/\mathbf{Q})$ for some $r \in \mathbf{Q}^*$. This proves the theorem for $n = 1$.

Now suppose $n \in \mathbf{Z}_{\geq 2}$, and let $f_1, \ldots, f_n$ be generators of $\mathrm{Hom}(F, \widehat{\mathbf{Z}})$. Then

$$(\mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_i))_{i=1}^n\colon\ \mathrm{H}^2(\widehat{\mathbf{Z}}^*, F) \longrightarrow \mathrm{H}^2(\widehat{\mathbf{Z}}^*, \widehat{\mathbf{Z}})^{\oplus n}$$

is an isomorphism of groups that sends $[E]$ to $(\mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_i)([E]))_{i=1}^n$. As $2 \cdot \mathrm{H}^2(\widehat{\mathbf{Z}}^*, \widehat{\mathbf{Z}}) = 0$ by Theorem 1.24, the group $\mathrm{H}^2(\widehat{\mathbf{Z}}^*, \widehat{\mathbf{Z}})$ is an $\mathbf{F}_2$-vector space. Moreover, the subgroup

$$\langle \mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_i)([E]) : i = 1, \ldots, n \rangle$$

is an $\mathbf{F}_2$-subvector space of $\mathrm{H}^2(\widehat{\mathbf{Z}}^*, \widehat{\mathbf{Z}})$. We show that this subspace is in fact n-dimensional, that is, we show that $\mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_1)([E]), \ldots, \mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_n)([E])$ are linearly independent over $\mathbf{F}_2$.

To this end, let N be any nonempty subset of $\{1, \ldots, n\}$ and consider $f = \sum_{i \in N} f_i$. Then by Proposition 1.21 we have

$$\mathrm{H}^2(\widehat{\mathbf{Z}}^*, f)([E]) = [0 \longrightarrow \widehat{\mathbf{Z}} \longrightarrow f_*(G) \longrightarrow \widehat{\mathbf{Z}}^* \longrightarrow 1].$$

As f is surjective, the map $G \longrightarrow f_*(G)$ is surjective. Therefore, we have

$$[f_*(G), f_*(G)] = f([G, G]) = \widehat{\mathbf{Z}}.$$

Since $f_*(G)$ has commutator subgroup $\widehat{\mathbf{Z}}$, it is not the trivial extension $\widehat{\mathbf{Z}} \rtimes \widehat{\mathbf{Z}}^*$, that is, the element $\mathrm{H}^2(\widehat{\mathbf{Z}}^*, f)([E])$ is different from 0. As N was any nonempty subset of $\{1, \ldots, n\}$, the elements

$$\mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_1)([E]), \ldots, \mathrm{H}^2(\widehat{\mathbf{Z}}^*, f_n)([E])$$

are linearly independent over $\mathbf{F}_2$.

Define S, T' and χ similarly as above for $K = \mathbf{Q}$ and

$$\Lambda = \frac{\mathbf{Q}(\mu)^{*2} \cap \mathbf{Q}^*}{\pm \mathbf{Q}^{*2}} = \mathbf{Q}^* / \pm \mathbf{Q}^{*2}.$$

Under χ the isomorphism class $[G]$ maps to a subgroup H of Λ that is free of rank n over $\mathbf{Z}/2\mathbf{Z}$. We define W to be the subgroup of $\mathbf{Q}^*$ generated by the liftings of the n generators of H. Let $\mathrm{Sat}(W)$, $\mathrm{Cyc}(W)$ and G_W be similar as above for $K = \mathbf{Q}$. Then Theorem 1.35 implies that

$$\chi([G_W]) = \frac{(\mathrm{Cyc}(W)^2 \cap \mathbf{Q}^*)\, \mathbf{Q}^{*2}}{\pm \mathbf{Q}^{*2}}.$$

Moreover, similarly as above we have

$$\chi([G]) = \frac{\mathrm{Sat}(W)\mathbf{Q}^{*2}}{\pm \mathbf{Q}^{*2}}.$$

Using $\mathbf{Q}(\mu)^{*2} \cap \mathbf{Q}^* = \mathbf{Q}^*$ one checks similarly as above that $\chi([G]) = \chi([G_W])$, from which it follows that $G \cong G_W$, as desired. ∎