Division points in arithmetic

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 5 januari 2021
klokke 11:15 uur

door

Abtien Javan Peykar
geboren te Apeldoorn
in 1989

Promotor: Prof. dr. P. Stevenhagen

Copromotor: Prof. dr. H. W. Lenstra

Promotiecommissie:

Prof. dr. B. de Smit	
Prof. dr. R. van Luijk	
Prof. dr. S. J. Edixhoven	
Dr. A. Perucca	Université du Luxembourg
Dr. P. Moree	Max Planck Institute for Mathematics

Contents

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* $\operatorname{char} K$. *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 $\operatorname{rk}(W)$ 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

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

of profinite groups. Observe that $\operatorname{Aut}(\mu)$ is canonically isomorphic to $\widehat{\mathbf{Z}}^*$ as a profinite group. As $\operatorname{Gal}(K(\mu)/K)$ is compact and $\widehat{\mathbf{Z}}^*$ is Hausdorff, we may identify $\operatorname{Gal}(K(\mu)/K)$ 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 $n = \operatorname{rk}(W)$. Then the following statements hold.*

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

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

Proof. Note that $\operatorname{Sat}(W)/W$ 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 $\operatorname{Sat}(W)/W$ is finite, the group $\operatorname{Sat}(W)$ is finitely generated of rank n, which proves (a).

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

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

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

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

is finite, which implies that $\operatorname{Cyc}(W)/\mu$ 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 $G = \operatorname{Gal}(K(W^{1/\infty})/K)$. Then there is a natural extension of Γ_K*

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

such that for all $f \in \operatorname{Hom}(\operatorname{Cyc}(W), \widehat{\mu})$, $x \in W^{1/\infty}$ and $m \in \mathbf{Z}_{\geq 1}$ with $x^m \in \operatorname{Cyc}(W)$ 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 $i = 1, \dots, n$. 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*

$$\begin{tikzcd}
\mathrm{C}^n(\Gamma, A) \arrow[r, "d_n"] \arrow[d, "\mathrm{C}^n(\varphi,\psi)"'] & \mathrm{C}^{n+1}(\Gamma, A) \arrow[d, "\mathrm{C}^{n+1}(\varphi,\psi)"] \\
\mathrm{C}^n(\Delta, B) \arrow[r, "d_n"'] & \mathrm{C}^{n+1}(\Delta, B)
\end{tikzcd}$$

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*

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

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*

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

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*

$$\begin{tikzcd}
 & & B \arrow[dd, "\varphi"] \arrow[dr, "g"] & & \\
1 \arrow[r] & A \arrow[ur, "f"] \arrow[dr, "\iota_A"'] & & C \arrow[r] & 1 \\
 & & A \times C \arrow[ur, "\pi_C"'] & &
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & & E \arrow[dd, "\varphi"] \arrow[dr, "g"] & & \\
0 \arrow[r] & A \arrow[ur, "f"] \arrow[dr, "f'"'] & & \Gamma \arrow[r] & 1 \\
 & & E' \arrow[ur, "g'"'] & &
\end{tikzcd}$$

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

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

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

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

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

$$\begin{tikzcd}
\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \arrow[r, "\omega"] \arrow[d] & \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n} \arrow[d] \\
S \arrow[r, "\rho"'] & T
\end{tikzcd}$$

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

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

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

$$\begin{tikzcd}
0 \arrow[r] & \widehat{\mathbf{Z}}^{\oplus n} \arrow[r, "f_1"] \arrow[d, "\alpha'"'] & G_1 \arrow[r, "g_1"] \arrow[d, "\alpha"'] & \Gamma \arrow[r] \arrow[d] & 1 \\
0 \arrow[r] & \widehat{\mathbf{Z}}^{\oplus n} \arrow[r, "f_2"'] & G_2 \arrow[r, "g_2"'] & \Gamma \arrow[r] & 1
\end{tikzcd}$$

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

$$\begin{tikzcd}
& Z \arrow[rr] \arrow[dl, "q"] \arrow[dd] & & A \arrow[dl, "\mathrm{id}"] \arrow[dd] \\
Z' \arrow[rr] \arrow[dd] & & A \arrow[dd] & \\
& P/JP \arrow[rr, "\overline{f}"'] \arrow[dl, "\overline{h}"] & & A/JA \arrow[dl, "\mathrm{id}"] \\
P/JP \arrow[rr, "\overline{g}"] & & A/JA &
\end{tikzcd}$$

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

$$\begin{tikzcd}
& P \arrow[dl, "h"] \arrow[ddrr, "u_Z"] \arrow[ddrrrr, bend left, "f"] \arrow[dddr, bend right] & & & & \\
P \arrow[ddrr, "u_{Z'}"'] \arrow[ddrrrr, bend left, "g"] \arrow[ddddrr, bend right, "\pi"'] & & & & & \\
& & & Z \arrow[rr] \arrow[dl, "q"] \arrow[dd] & & A \arrow[dl, "\mathrm{id}"] \arrow[dd] \\
& & Z' \arrow[rr] \arrow[dd, "p"] \arrow[dr] & & A \arrow[dd] & \\
& & & P/JP \arrow[rr, "\overline{f}"'] \arrow[dl, "\overline{h}"] & & A/JA \arrow[dl, "\mathrm{id}"] \\
& & P/JP \arrow[rr, "\overline{g}"] & & A/JA &
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & & P \arrow[dd, "\varphi"] \arrow[dr, "g"] & & \\
0 \arrow[r] & \ker h \arrow[ur] \arrow[dr] & & P \arrow[r] & 0 \\
 & & \ker h \oplus P \arrow[ur, "\pi_P"'] & &
\end{tikzcd}$$

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

$$\begin{tikzcd}
P/JP \arrow[rr, "\overline{h}"] \arrow[d, "\overline{\varphi}"] & & P/JP \\
\ker(h)/(J \cdot \ker(h)) \oplus P/JP \arrow[urr, "\overline{\pi_P}"'] & &
\end{tikzcd}$$

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

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

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

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

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 $\pi_1, \dots, \pi_n$. 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

$$\begin{tikzcd}
\widehat{\mathbf{Z}}^{\oplus n} \arrow[r, "f_1"] \arrow[d, "\alpha'"'] & G \arrow[d, "\alpha"] \\
\widehat{\mathbf{Z}}^{\oplus n} \arrow[r, "g_2"'] & G
\end{tikzcd}$$

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

$$\begin{tikzcd}
\mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}}^{\oplus n}) \arrow[r, "\omega"] \arrow[d, "1.30"'] & \mathrm{H}^2(\Gamma, \widehat{\mathbf{Z}})^{\oplus n} \arrow[d, "1.32"] \\
S \arrow[r, "\rho"'] & T
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^0(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^0(\cdot w)"] & \mathrm{H}^0(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^0(\pi)"] & \mathrm{H}^0(\Gamma_K, \mu_w) \arrow[dll, "\delta_0"] \\
& \mathrm{H}^1(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^1(\cdot w)"] & \mathrm{H}^1(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^1(\pi)"] & \mathrm{H}^1(\Gamma_K, \mu_w) \arrow[dll, "\delta_1"] \\
& \mathrm{H}^2(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^2(\cdot w)"] & \mathrm{H}^2(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^2(\pi)"] & \cdots
\end{tikzcd}$$

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 $\operatorname{Ann}_{\widehat{\mathbf{Z}}}(\mu(K)) = w\widehat{\mathbf{Z}}$ (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

$$\begin{tikzcd} \mathrm{H}^1(\Gamma_K, \widehat{\mu}) \arrow[r, "\mathrm{H}^1(\pi)"] & \mathrm{CHom}(\Gamma_K, \mu_w) \\ \mu_w \arrow[u, "\delta_0", "\wr"'] \arrow[r] & \frac{K(\mu)^{*w} \cap K^*}{K^{*w}} \arrow[u, "\kappa"', "\wr"] \end{tikzcd}$$

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 $\operatorname{Gal}(K(W^{1/\infty})/K)$ *in* S *under the bijection* χ *is*

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

Let A be a discrete abelian group. Then $\operatorname{Hom}(A, \widehat{\mu})$ 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 $\operatorname{ev}_x \colon \operatorname{Hom}(A, \widehat{\mu}) \longrightarrow \widehat{\mu}$ given by $f \mapsto f(x)$. This induces a group morphism

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

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

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

given by $[c] \mapsto (x \mapsto \mathrm{H}^2(\operatorname{ev}_x)(c))$. 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*

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

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

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

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

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

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

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

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

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

is an isomorphism of groups. Moreover

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

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

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

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

For the second part of the lemma, 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

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

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

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

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*

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

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

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

and let

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

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

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

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

$$\begin{tikzcd}
0 \arrow[r] & H \arrow[r] \arrow[d] & I \arrow[r, "\pi"] \arrow[d, "f"'] & I/H \arrow[r] \arrow[d, "\overline{f}"] & 0 \\
0 \arrow[r] & \Lambda \arrow[r] & M \arrow[r, "\pi'"'] & M/\Lambda \arrow[r] & 0
\end{tikzcd}$$

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 $A[l] \cong \operatorname{Hom}(\mathbf{Z}/l\mathbf{Z}, A)$, 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

$$\begin{tikzcd}
(I/H)[l] \arrow[r, "\overline{f}{[l]}"] & (M/\Lambda)[l] \arrow[r, "c"] & N \arrow[r] & 0 \\
 & M[l]/\Lambda[l] \arrow[u, hook, "\pi'{[l]}"] \arrow[r, "c\circ\pi'{[l]}"] & N_0 \arrow[u, hook, "\iota"] \arrow[r] & 0
\end{tikzcd}$$

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. ■

CHAPTER 2

Reductions of multiplicative subgroups of number fields

1. Introduction

Let K be a number field, and let W be a finitely generated subgroup of K^*. Let $\mathcal{O}_K$ be the ring of integers of K. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $\mathrm{v}_\mathfrak{p}\colon K \longrightarrow \mathbf{Z} \cup \{\infty\}$ be the $\mathfrak{p}$-adic valuation function, let $\mathcal{O}_{K,\mathfrak{p}}$ be the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, and let $\kappa(\mathfrak{p})$ be the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$. Let Ω_K be the set of maximal ideals of $\mathcal{O}_K$, let

$$S = \{\mathfrak{p} \in \Omega_K : \text{ there is } w \in W \text{ such that } \mathrm{v}_\mathfrak{p}(w) \neq 0\},$$

and note that S is finite. Then for $\mathfrak{p} \in \Omega_K \setminus S$ we have $W \subset \mathcal{O}_{K,\mathfrak{p}}^*$. Thus, the canonical ring morphism $\mathcal{O}_{K,\mathfrak{p}} \longrightarrow \kappa(\mathfrak{p})$ induces a group morphism $\pi_\mathfrak{p}\colon W \longrightarrow \kappa(\mathfrak{p})^*$.

Let V be a subgroup of W such that W/V is finite cyclic. Note that for any $\mathfrak{p} \in \Omega_K \setminus S$ the kernel of $\pi_\mathfrak{p}$ is such a subgroup of W. Let

$$A(W,V) = \{\mathfrak{p} \in \Omega_K \setminus S : \ker(\pi_\mathfrak{p}) \subset V\}.$$

For any subset N of Ω_K we write $\mathrm{d}(N)$ for its natural density, if it exists. In this chapter we show that the set $A(W,V)$ has a natural density $\mathrm{d}(A(W,V))$ in Ω_K, and prove properties of this density of both qualitative and quantitative nature.

Theorem 6 (Main theorem)**.**

(a) *The set $A(W,V)$ has a natural density $\mathrm{d}(A(W,V))$ in Ω_K.*

(b) *The density $\mathrm{d}(A(W,V))$ is rational.*

(c) *As a function of K, W and V, the density $\mathrm{d}(A(W,V))$ is computable.*

(d) *Let V' be a subgroup of W containing V, and suppose that W is infinite. Then $\mathrm{d}(A(W,V)) = \mathrm{d}(A(W,V'))$ if and only if $V = V'$.*

(e) *The density $\mathrm{d}(A(W,V))$ is positive.*

(f) *We have $\mathrm{d}(A(W,V)) = 1$ if and only if $V = W$ or W is finite.*

See Theorem 2.24 and Theorem 2.25 in Section 2.7 for the proof.

Suppose x and y are positive integers with the property that for all positive integers n the set of prime numbers dividing $x^n - 1$ is equal to the set of prime numbers dividing $y^n - 1$. Pál Erdös asked, at the 1988 number theory conference in Banff, whether it follows that x is equal to y. This question was labeled the *support problem*, and was answered affirmatively by C. Corrales-Rodrigáñez and R. Schoof in [CRS97], who, in the same paper, formulated and proved an elliptic analogue of the support problem. One can find many generalisations and variations of the support problem in the literature, see [Kha03, Proposition 3], [BGK05], [Lar02], [Wes03], [Bar10], [Per09], [Per12]. As an application of Theorem 6(e), we give an alternative solution to the following two generalisations of the support problem.

Throughout this chapter, we use the phrase *almost all* as a substitute for *all but finitely many*.

Theorem 7. *Let K be a number field, and let X and Y be finitely generated subgroups of K^*.*

(a) *Let $S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X \cup Y : \mathrm{v}_{\mathfrak{p}}(x) \neq 0\}$. Then $Y \subset X$ if and only if for almost all $\mathfrak{p} \in \Omega_K \setminus S'$ we have $Y \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}}$.*

(b) *Suppose that $Y \subset X$. Let l be a prime number. Let*

$$S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X : \mathrm{v}_{\mathfrak{p}}(x) \neq 0\}.$$

Then

$$(X : Y) < \infty \text{ and } l \nmid (X : Y)$$

$$\text{if and only if}$$

$$\text{for almost all } \mathfrak{p} \in \Omega_K \setminus S' \text{ we have } l \nmid (X \pmod{\mathfrak{p}} : Y \pmod{\mathfrak{p}}).$$

See Theorem 2.27 and Theorem 2.28 in Section 2.8 for the proof.

Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a subgroup of W such that W/V is finite cyclic. The existence of the natural density of $A(W, V)$ is obtained by a version of Chebotarev's density theorem for infinite algebraic extensions of a number field. Using this theorem, we also obtain a formula for $\mathrm{d}(A(W, V))$ that is, however, a finite product of infinite sums. In order to obtain a closed-form formula for $\mathrm{d}(A(W, V))$ we investigate the radical extensions of K occurring in this formula. We refer to Section 2.3 for the infinite version of Chebotarev's density theorem and to Section 2.4 for the proof of the existence and formula of $\mathrm{d}(A(W, V))$.

Let s be a Steinitz number, that is, let $s = \prod_p p^{e(p)}$, where p runs over all prime numbers and $e(p) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$. Let $\overline{K}$ be an algebraic closure of K and define

$$W^{1/s} = \{x \in \overline{K}^* : \exists d \in \mathbf{Z}_{\geq 1} : d | s \text{ and } x^d \in W\}.$$

The field $K(W^{1/s})$ is Galois over K and any field automorphism of $K(W^{1/s})$ over K is determined by its action on $W^{1/s}$, that is, we can identify $\mathrm{Gal}(K(W^{1/s})/K)$ with a subgroup of the group $\mathrm{Aut}_W(W^{1/s})$ of automorphisms of $W^{1/s}$ that are the identity on W. By abuse of notation we denote this subgroup also by $\mathrm{Gal}(K(W^{1/s})/K)$. We remark that $\mathrm{Aut}_W(W^{1/s})$ is the profinite group

$$\varprojlim_{d} \mathrm{Aut}_W(W^{1/d})$$

where d runs over all positive integers dividing s. As $\mathrm{Gal}(K(W^{1/s})/K)$ is compact and $\mathrm{Aut}_W(W^{1/s})$ is Hausdorff, the subgroup $\mathrm{Gal}(K(W^{1/s})/K)$ of $\mathrm{Aut}_W(W^{1/s})$ is closed.

For a prime p let v_p be the p-adic valuation function. Moreover, for a group G write $\exp(G)$ for its exponent.

Theorem 8. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let s be a Steinitz number.*

(a) *Then $\mathrm{Gal}(K(W^{1/s})/K)$ is an open subgroup of $\mathrm{Aut}_W(W^{1/s})$.*

(b) *Suppose that $s = p^\infty$, where p is prime. Let*

$$F = \begin{cases} K(\mu_4) & \textit{if } p = 2, \\ K(\mu_p) & \textit{otherwise}. \end{cases}$$

Then $\exp((W^{1/s} \cap F^*)/W)$ is an integer, and moreover, for

$$j = \mathrm{v}_p(\exp((W^{1/s} \cap F^*)/W))$$

and for all $i \in \mathbf{Z}_{\geq j}$ we have

$$\mathrm{Aut}_{W^{1/p^i}}(W^{1/s}) \subset \mathrm{Gal}(K(W^{1/s})/K).$$

See Section 2.5 for the proof of this theorem.

By using elementary group theory, we are able to calculate the order of an automorphism group of the form $\mathrm{Aut}_{W^{1/x'}}(W^{1/x})$, where W is as in the theorem above, $x', x \in \mathbf{Z}_{\geq 1}$ and x' divides x. As a result, we obtain the following closed-form expression for the density $\mathrm{d}(A(W, V))$.

Theorem 9. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a subgroup of W such that W/V is finite cyclic. Let $m = (W : V)$, let $U = V^{1/m}$, and let $L = K(U)$. Let $n = \mathrm{rk}(W)$ (see* Definition 1.2*), and let $\mathcal{P}$ be the set of prime divisors of m. Let $(j_p)_{p\in\mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $p \in \mathcal{P}$*

$$\mathrm{Aut}_{U^{1/p^{j_p}}}(U^{1/p^\infty}) \subset \mathrm{Gal}(L(U^{1/p^\infty})/L).$$

Then $\mathrm{d}(A(W, V))$ equals

$$\tfrac{1}{[L:K]} \prod_{p\in\mathcal{P}} \Big[\tfrac{1}{[L(U^{1/p^{j_p}}):L]} \cdot \tfrac{p^n(p-1)}{p^{n+1}-1} + \textstyle\sum_{i=0}^{j_p-1} \Big(\tfrac{1}{[L(U^{1/p^i}):L]} - \tfrac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}):L]} \Big) \Big].$$

For the sake of showcasing, we remark that in certain cases the above lengthy formula breaks down to a rather simple formula, presented by the following corollary.

Corollary. *Suppose that for every $p \in \mathcal{P}$ we have*

$$\mathrm{Gal}(L(U^{1/p^\infty})/L) = \mathrm{Aut}_U(U^{1/p^\infty}).$$

Then

$$\mathrm{d}(A(W, V)) = \frac{1}{[L : K]} \prod_{p\in\mathcal{P}} \frac{p^n(p-1)}{p^{n+1}-1}.$$

In addition, suppose that $[L : K] = \phi(m)m^{n-1}$, where ϕ is Euler's totient function. Then we have

$$\mathrm{d}(A(W, V)) = \frac{1}{m^n} \cdot \prod_{p\in\mathcal{P}} \frac{p^{n+1}}{p^{n+1}-1}.$$

See Section 2.6 for the proof of Theorem 9 and its corollary.

At last, using the closed-form formula given in Theorem 9, we are able to make the following quantitative observations about $\mathrm{d}(A(W,V))$.

Theorem 10. *Let K, W, V, m, U, L, n, $\mathcal{P}$, and $(j_p)_{p\in\mathcal{P}}$ be as in* Theorem 9. *Then the density $\mathrm{d}(A(W,V))$ exists and equals a positive rational number in the interval*

$$\left[\frac{1}{m^n}\cdot\prod_{p\in\mathcal{P}}\frac{1}{p^{(j_p-1)(n+1)}\cdot(p^{n+1}-1)},\prod_{p\in\mathcal{P}}\left(1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)}\right)\right]$$

whose denominator divides $m^n\cdot\prod_{p\in\mathcal{P}}\bigl(p^{(n+1)j_p-1}\cdot(p^{n+1}-1)\bigr)$.

See Section 2.7 for the proof of this theorem.

The present chapter is organised as follows.

In Section 2.2 we recall the necessary definitions and lemmas of measure theory. In Section 2.3 we state the infinite version of Chebotarev's density theorem. In Section 2.4 we prove the existence of the density of Theorem 6 and give a formula for it. In Section 2.5 we prove Theorem 8, and in Section 2.6 we prove Theorem 9. In Section 2.7 we prove Theorem 10 and the remaining parts of Theorem 6. At last, Section 2.8 contains the proof of Theorem 7.

2. Haar measure on profinite groups

In this section we briefly recall the theory of Haar measures on profinite groups. For a more elaborate treatment of the subject see [HR79], [FJ08] or [RV99].

Definition 2.1. Let X be a set, and let Σ be a σ-algebra over X. A *measure* on Σ is a function $\lambda\colon\Sigma\longrightarrow\mathbf{R}\cup\{\infty\}$ that satisfies:

(a) For all $E \in \Sigma$ we have $\lambda(E) \geq 0$;

(b) We have $\lambda(\emptyset) = 0$;

(c) For all countable collections $\{E_i\}_{i \in I}$ of pairwise disjoint sets in Σ we have

$$\lambda\left(\coprod_{i \in I} E_i\right) = \sum_{i \in I} \lambda(E_i).$$

Proposition 2.2. *Let X be a set, let Σ be a σ-algebra on X, and let λ be a measure on Σ. Then the following statements hold.*

(a) *For $E_1, E_2 \in \Sigma$ with $E_1 \subset E_2$, we have $\lambda(E_1) \leq \lambda(E_2)$.*

(b) *For $E_1, E_2 \in \Sigma$ with $E_2 \subset E_1$ and $\lambda(E_2) < \infty$, we have $\lambda(E_1 \setminus E_2) = \lambda(E_1) - \lambda(E_2)$.*

(c) *For any countable collection $\{E_i\}_{i \in I}$ of sets in Σ we have*

$$\lambda\left(\bigcup_{i \in I} E_i\right) \leq \sum_{i \in I} \lambda(E_i).$$

Proof. See [Bau01, §1.3]. ■

Let G be a profinite group. The σ-algebra $\mathcal{B}(G)$ generated by all open sets of G is called the *Borel algebra* of G. An element of $\mathcal{B}(G)$ is called a *Borel set* of G.

Theorem 2.3. *Let G be a profinite group. Then there is a unique measure λ on $\mathcal{B}(G)$ satisfying:*

(a) *For every $g \in G$ and $E \in \mathcal{B}(G)$ we have $\lambda(gE) = \lambda(E)$;*

(b) $\lambda(G) = 1$.

Proof. See [FJ08, Theorem 18.2.1]. ■

Definition 2.4. Let G be a profinite group. We call the unique measure on $\mathcal{B}(G)$ of Theorem 2.3 the *Haar measure* on G and denote it by λ_G, or just λ when the group G is understood. Elements of $\mathcal{B}(G)$ are called *measurable under the Haar measure* or *Haar measurable*.

Lemma 2.5. *Let G be a profinite group. Then the following statements hold.*

(a) *Let $H \subset G$ be a Haar measurable subgroup of finite index. Then*

$$\lambda(H) = 1/[G : H].$$

(b) *Let $H \subset G$ be a Haar measurable subgroup that is not of finite index in G. Then $\lambda(H) = 0$.*

Proof. See [FJ08, §18.1]. ■

Lemma 2.6. *Let $\pi \colon G \longrightarrow H$ be a surjective morphism of profinite groups. Then for each $E \in \mathcal{B}(H)$ we have $\pi^{-1}(E) \in \mathcal{B}(G)$ and $\lambda_H(E) = \lambda_G(\pi^{-1}(E))$.*

Proof. See [FJ08, Proposition 18.2.2]. ■

Lemma 2.7. *Let $n \in \mathbf{Z}_{\geq 1}$. Let $G_1, \ldots, G_n$ be profinite groups with Haar measures $\lambda_1, \ldots, \lambda_n$, respectively. Let $G = \prod_{i=1}^n G_i$. For $i = 1, \ldots, n$ let $E_i \in \mathcal{B}(G_i)$. Then $\lambda_G(E_1 \times \cdots \times E_n) = \lambda_1(E_1) \cdots \lambda_n(E_n)$.*

Proof. See [FJ08, Proposition 18.4.2]. ■

3. Chebotarev density theorem for infinite extensions

In this section we briefly recall the theory of infinite Galois extensions of number fields to state the Chebotarev density theorem for an infinite Galois extension of a number field. For details and proofs we refer to [Ser89] or [Neu99].

Let K be an algebraic extension of $\mathbf{Q}$. We denote the set of maximal ideals of $\mathcal{O}_K$ by Ω_K. For $\mathfrak{p} \in \Omega_K$ we denote the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$ by $\kappa(\mathfrak{p})$. Now, suppose K is a number field, and let L be an infinite Galois extension of K with Galois group G. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ a maximal ideal of $\mathcal{O}_L$ extending $\mathfrak{p}$, that is, $\mathfrak{q} \cap K = \mathfrak{p}$. Then the *decomposition group*

$$\mathrm{D}(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

of $\mathfrak{q}$ over $\mathfrak{p}$ is a closed subgroup of G. There is a canonical morphism of topological groups

$$r\colon\ \mathrm{D}(\mathfrak{q}/\mathfrak{p}) \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})),$$

which is surjective. The kernel of r, called the *inertia group* $\mathrm{I}(\mathfrak{q}/\mathfrak{p})$ of $\mathfrak{q}$ over $\mathfrak{p}$, is trivial if and only if $\mathfrak{p}$ is unramified in L.

Suppose that $\mathfrak{p}$ is unramified. Then r is an isomorphism of topological groups. Note that $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ is topologically generated by the Frobenius morphism

$$\mathrm{Frob}_{\mathfrak{p}}\colon \kappa(\mathfrak{q}) \longrightarrow \kappa(\mathfrak{q})$$

sending $x \in \kappa(\mathfrak{q})$ to $x^{\#\kappa(\mathfrak{p})}$. We denote the inverse image of $\mathrm{Frob}_{\mathfrak{p}}$ under r by $\mathrm{Frob}(\mathfrak{q}/\mathfrak{p})$ and call it the *Frobenius element* of $\mathfrak{q}$ over $\mathfrak{p}$ in G. The Frobenius elements of the different maximal ideals extending $\mathfrak{p}$ form a conjugacy class in G. We write $(\mathfrak{p}, L/K)$ for the conjugacy class consisting of the Frobenius elements $\mathrm{Frob}(\mathfrak{q}/\mathfrak{p})$ where $\mathfrak{q}$ runs over all primes of L extending $\mathfrak{p}$.

Let C be a subset of G. Let $\overline{C}$ be the closure of C in G, and let C^{o} be the interior of C in G. Then the boundary ∂C of C is equal to $\overline{C} \setminus C^{\mathrm{o}}$. Equivalently, we have $\partial C = \overline{C} \cap \overline{G \setminus C}$.

Let P be a subset of Ω_K. Recall that the natural density $\mathrm{d}(P)$ of P in Ω_K is equal to

$$\lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in P : \#\kappa(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \Omega_K : \#\kappa(\mathfrak{p}) \leq x\}}.$$

We have the following version of the Chebotarev density theorem that can also handle infinite Galois extensions of number fields.

Theorem 2.8. *Let K be a number field, and let L be a Galois extension of K that is unramified outside a finite set of primes S of K. Let C be a Haar measurable subset of* $\mathrm{Gal}(L/K)$ *that is closed under conjugation. Assume that the boundary ∂C has Haar measure 0. Then the set*

$$\{\mathfrak{p} \in \Omega_K \setminus S : (\mathfrak{p}, L/K) \subset C\}$$

has a natural density in Ω_K that is equal to $\lambda(C)$.

Proof. See [Ser89, Corollary 2, page I-9]. ■

4. Existence of the density

Definition 2.9. Let W be a group, and let V be a subgroup of W. Then V is called *cofinite* if V is of finite index in W. Moreover V is called *cocyclic* if W/V is a cyclic group.

Let K be a field, and let $\overline{K}$ be an algebraic closure of K. Let W be a subgroup of K^*, and let s be a Steinitz number not divisible by $\mathrm{char}\, K$. Define

$$W^{1/s} = \{x \in \overline{K}^* : \exists n \in \mathbf{Z}_{\geq 1} : n \mid s \text{ and } x^n \in W\}.$$

Observe that $W^{1/s} = \bigcup_n W^{1/n}$, where n runs over all positive integers dividing s. As usual, we write μ_s for the group of s-th roots of unity $\{1\}^{1/s}$.

Now, let K be a number field, and for $\mathfrak{p} \in \Omega_K$ let $\mathrm{v}_\mathfrak{p}$ be the $\mathfrak{p}$-adic valuation function. Let W be a finitely generated subgroup of K^*, and let

$$S = \{\mathfrak{p} \in \Omega_K : \exists w \in W : \mathrm{v}_\mathfrak{p}(w) \neq 0\},$$

and remark that S is finite. For every $\mathfrak{p} \in \Omega_K \setminus S$ the canonical projection $\mathcal{O}_K \longrightarrow \kappa(\mathfrak{p})$ induces a group morphism $\pi_\mathfrak{p} \colon W \longrightarrow \kappa(\mathfrak{p})^*$.

Let V be a cocyclic cofinite subgroup of W of index m, and write $\mathcal{P}(m)$ for the set of prime divisors of m. Moreover, let

$$A(W,V) = \{\mathfrak{p} \in \Omega_K \setminus S : \ker(\pi_{\mathfrak{p}}) \subset V\}.$$

To ease notation we will write $\mathcal{P}$ for $\mathcal{P}(m)$ and A for $A(W,V)$ throughout this section.

In this section we prove the following theorem.

Theorem 2.10. *Let $m = (W : V)$, let $U = V^{1/m}$, and let $L = K(U)$. Then A has a natural density, which equals*

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{p \in \mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right).$$

Lemma 2.11. *Let W be a group, and let V be a cofinite subgroup of W. Let*

$$\pi \colon W \longrightarrow W'$$

be a group morphism. Then $\ker \pi \subset V$ if and only if $(W : V) = (\pi(W) : \pi(V))$.

Proof. Let $N = \ker \pi$. Observe that $\pi(V) = \pi(VN)$, so that

$$\pi(W)/\pi(V) \cong (W/N)/(VN/N) \cong W/VN$$

as sets. Hence, we have $(\pi(W) : \pi(V)) = (W : VN)$. It follows that

$$(\pi(W) : \pi(V)) = (W : V)$$

if and only if $V = VN$. This is equivalent to V containing N. ■

Throughout the rest of this section let K, W, V, A, m, $\mathcal{P}$, U, and L be as in Theorem 2.10.

Let $\varphi \colon \Omega_L \longrightarrow \Omega_K$ be given by $\mathfrak{q} \mapsto \mathfrak{q} \cap K$, and let

$$S' = \varphi^{-1}(S) \cup \{\mathfrak{q} \in \Omega_L : m \in \mathfrak{q}\}.$$

Then for every $\mathfrak{q} \in \Omega_L \setminus S'$ we have the reduction map $\pi_\mathfrak{q}\colon U \longrightarrow \kappa(\mathfrak{q})^*$, where $\kappa(\mathfrak{q})$ is the residue field of L at $\mathfrak{q}$. Then we let $A' = A'(W, V) = \{\mathfrak{q} \in \Omega_L \setminus S' : \ker(\pi_\mathfrak{q}|_W) \subset V\}$.

Lemma 2.12. *Suppose that* $\mathrm{d}(A')$ *exists. Then* $\mathrm{d}(A)$ *exists and we have*

$$\mathrm{d}(A) = \frac{1}{[L : K]}\,\mathrm{d}(A').$$

Proof. First, note that for all $\mathfrak{q} \in \Omega_L \setminus S'$ we have $\pi_\mathfrak{q}(W) = \pi_{\varphi(\mathfrak{q})}(W)$, so that

$$\ker(\pi_\mathfrak{q}|_W) = \ker(\pi_{\varphi(\mathfrak{q})}|_W).$$

On the other hand, for $\mathfrak{p} \in A$ and $\mathfrak{q} \in \Omega_L \setminus S'$ dividing $\mathfrak{p}$, we have $\mathfrak{q} \in A'$. It follows that for all $\mathfrak{p} \in \Omega_K \setminus S$ and $\mathfrak{q} \in \Omega_L \setminus S'$ dividing $\mathfrak{p}$, we have $\mathfrak{p} \in A$ if and only if $\mathfrak{q} \in A'$.

Now, let $\mathfrak{p} \in A$, and let $\mathfrak{q} \in \Omega_L \setminus S'$ be a prime dividing $\mathfrak{p}$. Then by Lemma 2.11 we have $(\pi_\mathfrak{p}(W) : \pi_\mathfrak{p}(V)) = m$, which implies that m divides $\#\kappa(\mathfrak{p})^*$ and

$$\pi_\mathfrak{p}(V) \subset \kappa(\mathfrak{p})^{*m}.$$

It follows that $\mathfrak{p}$ splits completely in $K(V^{1/m}) = L$. Thus, for $x \in \mathbf{R}_{\geq 1}$ we have

$$\#\{\mathfrak{q} \in \Omega_L : \mathfrak{q} \in A' \wedge \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\} = [L : K]\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \wedge \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}.$$

Hence we have

$$\begin{aligned}
\mathrm{d}(A') &= \lim_{x\to\infty} \frac{\#\{\mathfrak{q} \in \Omega_L : \mathfrak{q} \in A' \text{ and } \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}} \\
&= \lim_{x\to\infty} \frac{[L : K]\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}} \\
&= [L : K] \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}}.
\end{aligned}$$

As

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{q} \in \Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\}}{\#\{\mathfrak{p} \in \Omega_K : \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}} = 1,$$

we have

$$\begin{aligned}
\mathrm{d}(A') &= [L:K]\lim_{x\to\infty}\frac{\#\{\mathfrak{p}\in\Omega_K : \mathfrak{p}\in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\leq x\}}{\#\{\mathfrak{q}\in\Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\leq x\}}\\
&= [L:K]\lim_{x\to\infty}\frac{\#\{\mathfrak{p}\in\Omega_K : \mathfrak{p}\in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\leq x\}}{\#\{\mathfrak{p}\in\Omega_K : \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\leq x\}}\\
&= [L:K]\,\mathrm{d}(A).
\end{aligned}$$

It follows that $\mathrm{d}(A)$ exists and that $\mathrm{d}(A)=\frac{1}{[L:K]}\,\mathrm{d}(A')$. ■

Lemma 2.13. *We have* $A'=\{\mathfrak{q}\in\Omega_L\setminus S' : \pi_\mathfrak{q}(W)=\pi_\mathfrak{q}(U)\}$.

Proof. Let $\mathfrak{q}\in\Omega_L\setminus S'$. Observe that $V=U^m$, and that $(\pi_\mathfrak{q}(U):\pi_\mathfrak{q}(U^m))$ divides m, since $\kappa(\mathfrak{q})^*$ is cyclic. Moreover, as $U=V^{1/m}$ contains a primitive mth root of unity, it follows that m divides $\#\pi_\mathfrak{q}(U)$ and $(\pi_\mathfrak{q}(U):\pi_\mathfrak{q}(V))=m$. It follows that $\pi_\mathfrak{q}(U)=\pi_\mathfrak{q}(W)$ if and only if $(\pi_\mathfrak{q}(W):\pi_\mathfrak{q}(V))=m$. On the other hand, we have by Lemma 2.11 that $(\pi_\mathfrak{q}(W):\pi_\mathfrak{q}(V))=m$ if and only if $\ker(\pi_\mathfrak{q}|_W)\subset V$. ■

Let $m^\infty=\prod_{p\in\mathcal{P}}p^\infty$. Let $\overline{L}$ be an algebraic closure of L, and write G for its Galois group over L. Since $W\subset U$, we have for every $p\in\mathcal{P}$ the following tower

$$\begin{aligned}
&L\subset L(W^{1/p})\subset L(U^{1/p})\subset L(U^{1/p},W^{1/p^2})\subset\cdots\\
&\qquad\cdots\subset L(U^{1/p^i})\subset L(U^{1/p^i},W^{1/p^{i+1}})\subset L(U^{1/p^{i+1}})\subset L(U^{1/p^{i+1}},W^{1/p^{i+2}})\subset\cdots\\
&\qquad\qquad\cdots\subset L(U^{1/p^\infty})\subset L(U^{1/m^\infty})\subset\overline{L}
\end{aligned}$$

of Galois extensions of L.

For all $p\in\mathcal{P}$ and $i\in\mathbf{Z}_{\geq 0}\cup\{\infty\}$ let

$$G_{p,i}=\mathrm{Gal}(\overline{L}/L(U^{1/p^i})),$$

and for $i\in\mathbf{Z}_{\geq 0}$, let

$$H_{p,i}=\mathrm{Gal}(\overline{L}/L(U^{1/p^i},W^{1/p^{i+1}}))\subset G_{p,i}.$$

Note that for all $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$ we have

$$G_{p,\infty} \subset \cdots \subset G_{p,i+1} \subset H_{p,i} \subset G_{p,i} \subset \cdots \subset G_{p,0}$$

by the above. Moreover, define

$$C_{p,i} = G_{p,i} \setminus H_{p,i},$$

and

$$C_p = \bigcup_{i=0}^{\infty} C_{p,i}.$$

One easily sees that C_p is a disjoint union of sets $C_{p,i}$. At last, we define $C = \bigcap_{p \in \mathcal{P}} C_p$.

Lemma 2.14. *The subset C of G is closed under conjugation and open in G.*

Proof. As for all $p \in \mathcal{P}$ and for all $i \in \mathbf{Z}_{\geq 0}$, the sets $G_{p,i}$ and $H_{p,i}$ are normal subgroups of G of finite index, it follows that $C_{p,i} = G_{p,i} \setminus H_{p,i}$ is closed under conjugation and open in G. Thus $C = \bigcap_{p \in \mathcal{P}} C_p$ is closed under conjugation and open in G. ■

Lemma 2.15. *The boundary ∂C of C in G satisfies $\lambda(\partial C) = 0$, where λ is the Haar measure on G (see 2.4).*

Proof. For $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$ let

$$D_{p,i} = H_{p,i} \setminus G_{p,i+1}.$$

Then observe that $G \setminus C$ contains the open set

$$D = \bigcup_{p,i} D_{p,i}$$

of G, where p runs over $\mathcal{P}$ and i runs over $\mathbf{Z}_{\geq 0}$. Hence $\partial C \subset G \setminus (C \cup D)$.

Now, for $\sigma \in G$ let N_σ be the Steinitz number $\prod_{p \in \mathcal{P}} p^{\sigma_p}$ with $\sigma_p \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$ the largest element such that $\sigma \in G_{p,i}$, where we order $\mathbf{Z}_{\geq 0} \cup \{\infty\}$ in the natural way, that is $\sigma_p = \sup\{i : \sigma \in G_{p,i}\}$.

Let $\sigma \in G$ and suppose that N_σ is an integer. This implies that for every $p \in \mathcal{P}$ there exists $i \in \mathbf{Z}_{\geq 0}$ such that $\sigma \in G_{p,i} \setminus G_{p,i+1}$. Then one easily sees that either $\sigma \in C$ or $\sigma \in D$. Thus $\sigma \in \partial C$ implies that N_σ is an infinite Steinitz number. As there are only finitely many primes dividing m, it follows that $\partial C \subset \bigcup_{p \in \mathcal{P}} \mathrm{Gal}(\overline{L}/L(U^{1/p^\infty}))$. Since the field $L(U^{1/p^\infty})$ contains the infinite extension $L(\mu_{p^\infty})$ of L, the former is also infinite over L. Therefore, the group $\mathrm{Gal}(\overline{L}/L(U^{1/p^\infty}))$ is of infinite index in G. Then by Lemma 2.5(b) the Haar measure of $\mathrm{Gal}(\overline{L}/L(U^{1/p^\infty}))$ is 0. Thus, by Proposition 2.2 the Haar measure of ∂C is 0. ■

Lemma 2.16. *We have* $\mathrm{d}(A') = \lambda_G(C)$ *(see text above* Lemma 2.12 *for the definition of* A'*).*

Proof. Let $\mathfrak{q} \in \Omega_L \setminus S'$. As $\zeta_m \in U$, we have $(\pi_\mathfrak{q}(U) : \pi_\mathfrak{q}(U^m)) = m$. Moreover

$$U^m \subset W \subset U,$$

so that $(\pi_\mathfrak{q}(U) : \pi_\mathfrak{q}(W))$ divides m. It follows that $\pi_\mathfrak{q}(U) = \pi_\mathfrak{q}(W)$ if and only if for all $p \in \mathcal{P}$ there is $i \in \mathbf{Z}_{\geq 0}$ such that p^i divides $(\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(U))$ and p^{i+1} does not divide $(\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(W))$.

Let $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$, and note that $\mathfrak{q}$ splits completely in $L(U^{1/p^i})$ if and only if

$$p^i \mid (\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(U)).$$

Similarly $\mathfrak{q}$ does not split completely in $L(W^{1/p^{i+1}})$ if and only if

$$p^{i+1} \nmid (\kappa(\mathfrak{q})^* : \pi_\mathfrak{q}(W)).$$

Now, let $M = L(U^{1/m^\infty})$, let $G' = \mathrm{Gal}(M/L)$, and let C' be the image of C under the canonical surjective map $G \longrightarrow G'$. Observe that there are only finitely many primes ramifying in M. We will show that $\mathrm{d}(A') = \lambda_{G'}(C')$. Then by Lemma 2.6 we have $\mathrm{d}(A') = \lambda_G(C)$, which finishes the proof.

To this end, recall that $\mathfrak{q}$ splits completely in an intermediate extension F of M/L if and only if for any prime ideal Q of M dividing $\mathfrak{q}$ we have $\mathrm{Frob}(Q/\mathfrak{q})|_F = \mathrm{id}$ if and only if

$$(\mathfrak{q}, M/L)|_F = \{\sigma|_F : \sigma \in (\mathfrak{q}, M/L)\} = \{\mathrm{id}\}.$$

Thus, we have $\pi_{\mathfrak{q}}(U) = \pi_{\mathfrak{q}}(W)$ if and only if for all $p \in \mathcal{P}$ there is $i \in \mathbf{Z}_{\geq 0}$ such that

$$(\mathfrak{q}, M/L)|_{L(U^{1/p^i})} = \{\mathrm{id}\} \text{ and } (\mathfrak{q}, M/L)|_{L(U^{1/p^i}, W^{1/p^{i+1}})} \neq \{\mathrm{id}\}.$$

By Lemma 2.13 we have $A' = \{\mathfrak{q} \in \Omega_L \setminus S' : \pi_{\mathfrak{q}}(U) = \pi_{\mathfrak{q}}(W)\}$. Hence, by the equivalences that we just saw we have

$$A' = \{\mathfrak{q} \in \Omega_L \setminus S' : (\mathfrak{q}, M/L) \subset C'\}.$$

Then by Theorem 2.8 and Lemma 2.15 we have $\mathrm{d}(A') = \lambda_{G'}(C')$. ∎

Proof of Theorem 2.10. For $p \in \mathcal{P}$ let $G_p = \mathrm{Gal}(L(U^{1/p^\infty})/L)$, and for $i \in \mathbf{Z}_{\geq 0}$ let

$$G_p(i) = \mathrm{Gal}(L(U^{1/p^\infty})/L(U^{1/p^i})),$$

$$H_p(i) = \mathrm{Gal}(L(U^{1/p^\infty})/L(U^{1/p^i}, W^{1/p^{i+1}}))$$

and $C_p(i) = G_p(i) \setminus H_p(i)$.

Let $p \in \mathcal{P}$ and note that L contains the pth roots of unity. Hence, for every $i \in \mathbf{Z}_{\geq 0}$ the field $L(U^{1/p^i})$ is of p-power degree over L. It follows that the fields $L(U^{1/p^\infty})$ for $p \in \mathcal{P}$ are linearly disjoint over L, so that the canonical morphism

$$\varphi\colon G \longrightarrow \prod_{p \in \mathcal{P}} G_p$$

of profinite groups is surjective. One easily sees that

$$\varphi(C) = \prod_{p \in \mathcal{P}} \prod_{i=0}^{\infty} C_p(i),$$

so that by Lemma 2.7 and Lemma 2.6 we have

$$\lambda_G(C) = \prod_{p\in\mathcal{P}} \lambda_{G_p}\left(\coprod_{i=0}^{\infty} C_p(i)\right).$$

Using Definition 2.1, Proposition 2.2 and Lemma 2.5, we find

$$\begin{aligned}
\mathrm{d}(A') = \lambda_G(C) &= \prod_{p\in\mathcal{P}}\sum_{i=0}^{\infty}\big(\lambda_{G_p}(G_p(i)) - \lambda_{G_p}(H_p(i))\big)\\
&= \prod_{p\in\mathcal{P}}\sum_{i=0}^{\infty}\left(\frac{1}{\big[L(U^{1/p^i}) : L\big]} - \frac{1}{\big[L(U^{1/p^i}, W^{1/p^{i+1}}) : L\big]}\right)\\
&= \prod_{p\in\mathcal{P}}\sum_{i=0}^{\infty}\frac{1}{\big[L(U^{1/p^i}) : L\big]}\left(1 - \frac{1}{\big[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})\big]}\right).
\end{aligned}$$

The desired formula for $\mathrm{d}(A)$ now follows by applying Lemma 2.12. ■

5. Galois representations on radical groups

For G a group and H a subgroup of G, we write $\mathrm{Aut}_H(G)$ for the set of group automorphisms of G that are the identity on H.

Let L be a field, let U be a subgroup of L^*, and let s be a Steinitz number that is not divisible by $\mathrm{char}\, L$. The field $L(U^{1/s})$ over L is Galois and any field automorphism of $L(U^{1/s})$ is determined by its action on $U^{1/s}$, that is, we can identify $\mathrm{Gal}(L(U^{1/s})/L)$ with a subgroup of $\mathrm{Aut}_U(U^{1/s})$. By abuse of notation we denote this subgroup also by $\mathrm{Gal}(L(U^{1/s})/L)$. If U is finitely generated, the group $\mathrm{Aut}_U(U^{1/s})$ is the profinite group

$$\varprojlim_{d} \mathrm{Aut}_U(U^{1/d}),$$

where d runs over all positive integers dividing s. As $\mathrm{Gal}(L(U^{1/s})/L)$ is compact and $\mathrm{Aut}_U(U^{1/s})$ is Hausdorff, the subgroup $\mathrm{Gal}(L(U^{1/s})/L)$ of $\mathrm{Aut}_U(U^{1/s})$ is closed.

For L a number field, U a subgroup of L^*, and s a Steinitz number, we define

$$\mathrm{Sat}_s(U) = U^{1/s} \cap L^*$$

and

$$\mathrm{Cyc}_s(U) = U^{1/s} \cap L(\mu_s)^*.$$

In some cases, we expand our notation to $\mathrm{Sat}_s(U, L)$ and $\mathrm{Cyc}_s(U, L)$ for these groups, to clarify the base field L in which we view U as a subset. When s is $\infty = \prod_p p^\infty$ where p runs over all prime numbers, we leave out the subscript s from the notation, which is consistent with the notation of the previous chapter (see Section 1.2).

For a group G we write $\exp(G)$ for its exponent. Moreover, recall that for a prime number p we write v_p for the p-adic valuation function.

In this section we prove the following theorem.

Theorem 2.17. *Let L be a number field, let U be a finitely generated subgroup of L^*, and let s be a Steinitz number.*

(a) *Then there is $d \in \mathbf{Z}_{\geq 1}$ such that for every $d' \in \mathbf{Z}_{\geq 1}$ with $d|d'|s$ we have*

$$\mathrm{Aut}_{U^{1/d'}}(U^{1/s}) \subset \mathrm{Gal}(L(U^{1/s})/L).$$

(b) *Suppose that $s = p^\infty$, where p is prime. Let*

$$F = \begin{cases} L(\mu_4) & \text{if } p = 2, \\ L(\mu_p) & \text{otherwise.} \end{cases}$$

Then $\exp(\mathrm{Sat}_s(U, F)/U)$ is finite, and there is $j \in \mathbf{Z}_{\geq 0}$ with

$$j \leq \mathrm{v}_p(\exp(\mathrm{Sat}_s(U, F)/U))$$

such that for all $i \in \mathbf{Z}_{\geq j}$ we have

$$\mathrm{Aut}_{U^{1/p^i}}(U^{1/s}) \subset \mathrm{Gal}(L(U^{1/s})/L).$$

Lemma 2.18. *Let $s = p^\infty$, where p is a prime. Let F be a number field with $\mu_p \subset F^*$, and if $p = 2$, with $\mu_4 \subset F^*$. Let $U \subset F^*$ be a subgroup such that* $\mathrm{Sat}_s(U) = U$. *Then* $\mathrm{Cyc}_s(U) = \mu_s \cdot U$.

Proof. The inclusion $\supset$ clearly holds. Moreover, the quotient

$$\mathrm{Cyc}_s(U)/(U \cdot \mu_s)$$

is p-primary, so it suffices to show that this quotient has no element of order p. To this end, let $x \in F(\mu_s)^*$ such that $x^p \in U \cdot \mu_s$. We will show that $x \in U \cdot \mu_s$. Note that there are $u \in U$ and $\zeta \in \mu_s$ such that $x^p = u \cdot \zeta$. Let ξ be a pth root of ζ, and let $y = x/\xi \in F(\mu_s)^*$. Then we will show that $y \in U$, which implies that $x \in U \cdot \mu_s$, as desired. Suppose that $y \in F^*$. As $U = \mathrm{Sat}_s(U)$ and $y^p \in U$, it follows that $y \in U$, as desired.

Suppose that $y \notin F^*$. Since F^* contains μ_p, and also μ_4 if $p = 2$, we have

$$\mathrm{Gal}(F(\mu_s)/F) \cong \mathbf{Z}_p$$

as profinite groups. Moreover, as $y^p \in U \subset F^*$, it follows that $F(y)$ is the unique subextension of $F(\mu_s)/F$ of degree p over F. Then by Kummer theory we have that

$$F(y) = F(\epsilon^{1/p}),$$

where ϵ is a generator of $\mu_s(F)$, and moreover, there are $i \in \{1, \ldots, p-1\}$ and $a \in F^*$ such that

$$y^p = \epsilon^i \cdot a^p.$$

Now, as $\mathrm{Sat}_s(U) = U$, we have $\epsilon \in U$. Furthermore, since $a^p \in U$, we have $a \in U$. It follows that $y = \eta \cdot a$ for some $\eta \in \mu_s$, that is, we have $y \in \mu_s \cdot U$, as desired. ■

Throughout the rest of this section, let L be a number field, let U be a finitely generated subgroup of L^*, let $n = \mathrm{rk}(U)$ (see Definition 1.2), let s be a Steinitz number, let $\Gamma_s = \mathrm{Gal}(L(\mu_s)/L)$, let $A_s = \mathrm{Aut}_{\mu_s \cap U}(\mu_s)$, let $G = \mathrm{Gal}(L(U^{1/s})/L)$, and let $A = \mathrm{Aut}_U(U^{1/s})$.

Lemma 2.19. *The groups* $\mathrm{Sat}_s(U)$ *and* $\mathrm{Cyc}_s(U)/\mu_s$ *are finitely generated of rank* n.

Proof. By Lemma 1.4, the groups U and $\mathrm{Sat}(U)$ are finitely generated of rank n, and $\mathrm{Cyc}(U)/\mu$ is free of rank n. Since $U \subset \mathrm{Sat}_s(U) \subset \mathrm{Sat}(U)$, we have that $\mathrm{Sat}_s(U)$ is finitely generated of rank n.

Let $(\mathrm{Cyc}_s(U))_{\mathrm{tor}}$ be the torsion subgroup of $\mathrm{Cyc}_s(U)$. Note that the quotient

$$\mathrm{Cyc}_s(U)/(\mathrm{Cyc}_s(U))_{\mathrm{tor}}$$

maps injectively to $\mathrm{Cyc}(U)/\mu$. As the latter is a free abelian group of rank n, it follows that $\mathrm{Cyc}_s(U)/(\mathrm{Cyc}_s(U))_{\mathrm{tor}}$ is free of rank n.

Let $w = \mu(L)$, and observe that

$$\mu_s \subseteq (\mathrm{Cyc}_s(U))_{\mathrm{tor}} \subseteq U_{\mathrm{tor}}^{1/s} \subseteq \mu_{ws}.$$

As μ_{ws}/μ_s is finite, it follows that $\mathrm{Cyc}_s(U)/\mu_s$ is finitely generated. ■

Lemma 2.20. (a) *The Galois group* Γ_s *is open in* A_s.

(b) *Suppose that* $s = p^\infty$*, where* p *is prime. Let* $\mu_s \cap L^* = \mu_{p^e}$*. Suppose that* $e \in \mathbf{Z}_{\geq 1}$*. If* $p = 2$*, suppose that* $e \in \mathbf{Z}_{\geq 2}$*. Then*

$$\Gamma_s = \mathrm{Aut}_{\mu_{p^e}}(\mu_s)$$

inside A_s.

Proof. By the irreducibility of the cyclotomic polynomials over $\mathbf{Q}$, we may identify the Galois group $\mathrm{Gal}(\mathbf{Q}(\mu_s)/\mathbf{Q})$ with $\mathrm{Aut}(\mu_s)$. Moreover

$$\Gamma_s \cong \mathrm{Gal}(\mathbf{Q}(\mu_s)/(L \cap \mathbf{Q}(\mu_s))),$$

as profinite groups. As $L \cap \mathbf{Q}(\mu_s)$ is a finite extension of $\mathbf{Q}$, it follows that Γ_s is a closed subgroup of finite index in $\mathrm{Aut}(\mu_s)$. It follows that Γ_s is open in A_s, as desired.

Suppose s, p, and e are as in (b). There is a canonical isomorphism

$$\varphi\colon \operatorname{Aut}(\mu_s) \longrightarrow \mathbf{Z}_p^*$$

of profinite groups, so $\varphi(\Gamma_s)$ is an open subgroup of $\mathbf{Z}_p^*$.

As every element of Γ_s is the identity on μ_{p^e}, the image $\varphi(\Gamma_s)$ is contained in the subgroup $1 + p^e\mathbf{Z}_p$ of $\mathbf{Z}_p^*$. Moreover, since $\mu_{p^{e+1}} \not\subset L$, the image $\varphi(\Gamma_s)$ is not contained in $1 + p^{e+1}\mathbf{Z}_p$.

Now, because $e \geq 2$ for $p = 2$, we have $1 + p^e\mathbf{Z}_p \cong \mathbf{Z}_p$ as profinite groups. The latter implies that $1+p^e\mathbf{Z}_p$ is topologically generated by any element not in $1+p^{e+1}\mathbf{Z}_p$. Thus $\varphi(\Gamma_s)$ is equal to $1 + p^e\mathbf{Z}_p$. We conclude that the image of Γ_s inside A_s is equal to $\operatorname{Aut}_{\mu_{p^e}}(\mu_s)$. This proves (b). ■

Proof of Theorem 2.17. As μ_s is a direct summand of $U^{1/s}$, the natural map

$$r\colon A \longrightarrow A_s$$

sending f to $f|_{\mu_s}$ is surjective. Moreover, one easily checks that the kernel $\operatorname{Aut}_{\mu_s\cdot U}(U^{1/s})$ of r is canonically isomorphic to $\operatorname{Hom}(U^{1/s}/(\mu_s \cdot U), \mu_s)$ as a profinite group.

On the other hand, by Kummer theory the kernel of the restriction morphism $G \longrightarrow \Gamma_s$ is canonically isomorphic to $\operatorname{Hom}(U^{1/s}/\operatorname{Cyc}_s(U), \mu_s)$ as a profinite group. The surjective morphism $U^{1/s}/(\mu_s \cdot U) \longrightarrow U^{1/s}/\operatorname{Cyc}_s(U)$ of discrete groups gives rise to a canonical injective morphism

$$\operatorname{Hom}(U^{1/s}/\operatorname{Cyc}_s(U), \mu_s) \longrightarrow \operatorname{Hom}(U^{1/s}/(\mu_s \cdot U), \mu_s)$$

of profinite groups that makes the following diagram of profinite groups

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}\big(U^{1/s}/\operatorname{Cyc}_s(U), \mu_s\big) \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & \Gamma_s \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Hom}\big(U^{1/s}/(\mu_s \cdot U), \mu_s\big) \arrow[r] & A \arrow[r] & A_s \arrow[r] & 0
\end{tikzcd} \tag{$*$}$$

commutative, where all other maps are defined above.

The kernel of $U^{1/s}/(\mu_s{\cdot}U) \longrightarrow U^{1/s}/\operatorname{Cyc}_s(U)$ is equal to $\operatorname{Cyc}_s(U)/(\mu_s{\cdot}U)$. Therefore the cokernel of the left vertical map is contained in $\operatorname{Hom}(\operatorname{Cyc}_s(U)/(\mu_s \cdot U), \mu_s)$. As by Lemma 2.19 the quotient $\operatorname{Cyc}_s(U)/(\mu_s \cdot U)$ is finite, it follows that the cokernel of the left vertical map is finite.

On the other hand, by Lemma 2.20 the profinite group Γ_s is open in A_s, implying that the cokernel $\operatorname{coker}(\Gamma_s \longrightarrow A_s)$ is finite. Hence $\operatorname{coker}(G \longrightarrow A)$ is finite. As G is closed in A (see beginning of this section), it follows that G is open in A. Equivalently, there is $d \in \mathbf{Z}_{\geq 1}$ such that

$$\operatorname{Aut}_{U^{1/d}}(U^{1/s}) \subset \operatorname{Gal}(L(U^{1/s})/L).$$

Moreover, for every $d' \in \mathbf{Z}_{\geq 1}$ with $d|d'|s$ we have

$$\operatorname{Aut}_{U^{1/d'}}(U^{1/s}) \subset \operatorname{Aut}_{U^{1/d}}(U^{1/s}),$$

which finishes the proof of (a).

Suppose that $s = p^\infty$, where p is prime. By (a) we know that there is $j \in \mathbf{Z}_{\geq 0}$ such that for every $i \in \mathbf{Z}_{\geq j}$

$$\operatorname{Aut}_{U^{1/p^i}}(U^{1/s}) = \operatorname{Gal}(L(U^{1/s})/L(U^{1/p^i})).$$

Let

$$F = \begin{cases} L(\mu_4) & \text{if } p = 2, \\ L(\mu_p) & \text{otherwise.} \end{cases}$$

and let $U' = \operatorname{Sat}_s(U, F)$. Then Lemma 2.19 implies that $\exp(U'/U)$ is finite. Let

$$e = \mathrm{v}_p(\exp(U'/U)).$$

We will show that j can be taken equal to e, which finishes the proof. To this end, we will prove that $\operatorname{Aut}_{U'}(U'^{1/s}) \subset G$.

First, note that $\mu_s \cap F^* = \mu_s \cap U'$. Then Lemma 2.20(b) implies that

$$\mathrm{Gal}(F(\mu_s)/F) = \mathrm{Aut}_{U' \cap \mu_s}(\mu_s).$$

Since $F(\mu_s) = L(\mu_s)$, it follows that

$$\mathrm{Aut}_{U' \cap \mu_s}(\mu_s) = \mathrm{Gal}(L(\mu_s)/F).$$

On the other hand, by Lemma 2.18 we have

$$\mathrm{Cyc}_s(U, F) = \mu_s \cdot U'.$$

Moreover, since $U'^{1/s} = U^{1/s}$, we have

$$\mathrm{Hom}(U^{1/s}/\,\mathrm{Cyc}_s(U', F), \mu_s) = \mathrm{Hom}(U^{1/s}/(\mu_s \cdot U'), \mu_s).$$

Replacing L by F and U by U' in $(*)$, we obtain

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}\big(U^{1/s}/\,\mathrm{Cyc}_s(U', F), \mu_s\big) \arrow[r] \arrow[d] & \mathrm{Gal}(L(U^{1/s})/F) \arrow[r] \arrow[d] & \mathrm{Gal}(L(\mu_s)/F) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Hom}\big(U^{1/s}/(\mu_s \cdot U'), \mu_s\big) \arrow[r] & \mathrm{Aut}_{U'}(U^{1/s}) \arrow[r] & \mathrm{Aut}_{U' \cap \mu_s}(\mu_s) \arrow[r] & 0
\end{tikzcd}$$

where, by the above, the left and right vertical maps are isomorphisms. It follows that

$$\mathrm{Gal}(L(U^{1/s})/F) = \mathrm{Aut}_{U'}(U^{1/s}),$$

so that $\mathrm{Aut}_{U'}(U^{1/s}) \subset G$. At last, as $U' \subset U^{1/p^e}$, we have

$$\mathrm{Aut}_{U^{1/p^e}}(U^{1/s}) \subset \mathrm{Aut}_{U'}(U^{1/s}) \subset G,$$

which finishes the proof. ■

6. Rationality of the density

Throughout this section, let K be a number field, let W be a finitely generated subgroup of K^*, and let V be cocyclic cofinite subgroup of W. Let $m = (W : V)$, let $\mathcal{P}$ be the set of prime divisors of m, let $n = \mathrm{rk}(W)$ (see Definition 1.2), let $U = V^{1/m}$, and let $L = K(U)$. We remark that $W/V \cong \mathbf{Z}/m\mathbf{Z}$ implies that $W \subset U$.

In this section, we prove a closed-form expression of the density $\mathrm{d}(A(W,V))$ using the formula given in Theorem 2.10 and Theorem 2.17.

Theorem 2.21. *Let $(j_p)_{p\in\mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $p \in \mathcal{P}$*

$$\mathrm{Aut}_{U^{1/p^{j_p}}}(U^{1/p^\infty}) \subset \mathrm{Gal}(L(U^{1/p^\infty})/L).$$

Then the density $\mathrm{d}(A(W,V))$ equals

$$\tfrac{1}{[L:K]} \textstyle\prod_{p\in\mathcal{P}} \left[\tfrac{1}{[L(U^{1/p^{j_p}}):L]} \cdot \tfrac{p^n(p-1)}{p^{n+1}-1} + \sum_{i=0}^{j_p-1} \left(\tfrac{1}{[L(U^{1/p^i}):L]} - \tfrac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}):L]} \right) \right].$$

We remark that one can find suitable $(j_p)_{p\in\mathcal{P}}$, as in the theorem above, in Theorem 2.17.

Corollary 2.22. *Suppose that for every $p \in \mathcal{P}$ we have*

$$\mathrm{Gal}(L(U^{1/p^\infty})/L) = \mathrm{Aut}_U(U^{1/p^\infty}).$$

Then

$$\mathrm{d}(A(W,V)) = \frac{1}{[L:K]} \prod_{p\in\mathcal{P}} \frac{p^n(p-1)}{p^{n+1}-1}.$$

In addition, suppose that $[L : K] = \phi(m)m^{n-1}$, where ϕ is Euler's totient function. Then we have

$$\mathrm{d}(A(W,V)) = \frac{1}{m^n} \cdot \prod_{p\in\mathcal{P}} \frac{p^{n+1}}{p^{n+1}-1}.$$

Proof. The proof follows directly from Theorem 2.21 by putting $j_p = 0$ for all $p \in \mathcal{P}$. ■

Lemma 2.23. *Let $p \in \mathcal{P}$, and let $i \in \mathbf{Z}_{\geq 0}$. Then the following hold.*

(a) *The degree $[L(U^{1/p^{i+1}}) : L(U^{1/p^i})]$ divides p^{n+1}, and if $i \geq j_p$, it is equal to p^{n+1}.*

(b) *The degree $[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]$ divides p, and if $i \geq j_p$, it is equal to p.*

Proof. Let $s = p^\infty$. As U is a finitely generated abelian group of rank n and $\mu_m \subset U$, we have $U \cong \frac{1}{u}\mathbf{Z}/\mathbf{Z} \oplus \mathbf{Z}^n$, where $u \in \mathbf{Z}_{\geq 1}$ is divisible by m. Then we have

$$U^{1/p^i} \cong \frac{1}{up^i}\mathbf{Z}/\mathbf{Z} \oplus \left(\frac{1}{p^i}\mathbf{Z}\right)^n,$$

so that

$$\begin{aligned} \operatorname{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) &\cong \operatorname{Hom}\left(\frac{U^{1/p^{i+1}}}{U^{1/p^i}}, U^{1/p^{i+1}}\right) \\ &\cong \operatorname{Hom}\left(\left(\frac{1}{p}\mathbf{Z}/\mathbf{Z}\right)^{n+1}, \frac{1}{up^{i+1}}\mathbf{Z}/\mathbf{Z} \oplus \left(\frac{1}{p^{i+1}}\mathbf{Z}\right)^n\right). \end{aligned}$$

Since

$$\# \operatorname{Hom}\left((\mathbf{Z}/p\mathbf{Z})^{n+1}, \mathbf{Z}/up^{i+1}\mathbf{Z} \oplus \left(\frac{1}{p^{i+1}}\mathbf{Z}\right)^n\right) = p^{n+1},$$

we have that

$$\# \operatorname{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) = p^{n+1}.$$

Now, note that

$$\operatorname{Gal}(L(U^{1/p^{i+1}})/L(U^{1/p^i})) \subset \operatorname{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}),$$

which implies that $[L(U^{1/p^{i+1}}) : L(U^{1/p^i})]$ divides p^{n+1}.

Now, suppose that $i \in \mathbf{Z}_{\geq j_p}$. Then by Theorem 2.17

$$\operatorname{Gal}(L(U^{1/s})/L(U^{1/p^i})) = \operatorname{Aut}_{U^{1/p^i}}(U^{1/s}).$$

Moreover, by [Pal14, Theorem 2.12] the sequence

$$0 \longrightarrow \operatorname{Aut}_{U^{1/p^{i+1}}}(U^{1/s}) \longrightarrow \operatorname{Aut}_{U^{1/p^i}}(U^{1/s}) \longrightarrow \operatorname{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) \longrightarrow 0$$

of profinite groups is exact. Then by Galois theory

$$p^{n+1} = \# \operatorname{Aut}_{U^{1/p^i}}(U^{1/p^{i+1}}) = [L(U^{1/p^{i+1}}) : L(U^{1/p^i})].$$

This proves (a).

For (b), note that $W^{1/p^i} \subset L(U^{1/p^i})^*$. Hence, by Kummer theory

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] = (W^{1/p^i} : L(U^{1/p^i})^{*p} \cap W^{1/p^i}).$$

Recall that $U^m = V \subset W$, so that $(U^m)^{1/p^i} \subset W^{1/p^i}$. One easily checks that

$$W^{1/p^{i-1}} \cdot (U^m)^{1/p^i} \subset W^{1/p^i} \cap L(U^{1/p^i})^{*p}.$$

As $W^{1/p^{i-1}} \cdot (U^m)^{1/p^i}$ maps to the unique subgroup of index p of the cyclic group

$$W^{1/p^i}/(U^m)^{1/p^i}$$

of order m, it follows that $(W^{1/p^i} : W^{1/p^i} \cap L(U^{1/p^i})^{*p})$ divides p. Hence

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] \mid p.$$

On the other hand, the degree $[L(U^{1/p^{i+1}}) : L(U^{1/p^i}, W^{1/p^{i+1}})]$ divides p^n, as the p^{i+1}th roots of unity are already contained in $L(U^{1/p^i}, W^{1/p^{i+1}})$. Hence for $i \geq j_p$ we have

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] = p,$$

as desired. ■

Proof of Theorem 2.21. Write $A = A(W, V)$. Then by Theorem 2.10 we have

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{p \in \mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right).$$

By Lemma 2.23, we have for all $p \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq j_p}$

$$[L(U^{1/p^{i+1}}) : L(U^{1/p^i})] = p^{n+1}$$

and

$$[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})] = p.$$

Hence

$$\sum_{i=j_p}^{\infty} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right)$$

is equal to

$$\frac{1}{[L(U^{1/p^{j_p}}) : L]} \sum_{i=0}^{\infty} \frac{1}{p^{(n+1)i}} \left(1 - \frac{1}{p}\right) = \frac{1}{[L(U^{1/p^{j_p}}) : L]} \cdot \frac{p^n(p-1)}{p^{n+1}-1}.$$

Using this in the expression for $\mathrm{d}(A)$, we find

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{p \in \mathcal{P}} \Bigg[\frac{1}{[L(U^{1/p^{j_p}}) : L]} \cdot \frac{p^n(p-1)}{p^{n+1}-1} + \sum_{i=0}^{j_p - 1} \frac{1}{[L(U^{1/p^i}) : L]} \left(1 - \frac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}) : L(U^{1/p^i})]}\right) \Bigg],$$

which is the desired formula. ■

7. Main theorem

In this section we

Theorem 2.24. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a cocyclic cofinite subgroup of W. Let $m = (W : V)$, let $U = V^{1/m}$, and let $L = K(U)$. Let $n = \mathrm{rk}(W)$ (see* Definition 1.2*), and let $\mathcal{P}$ be the set of primes dividing m. Let $(j_p)_{p \in \mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $p \in \mathcal{P}$*

$$\mathrm{Aut}_{U^{1/p^{j_p}}}(U^{1/p^\infty}) \subset \mathrm{Gal}(L(U^{1/p^\infty})/L).$$

Then the following statements hold.

(a) *The density* $\mathrm{d}(A(W,V))$ *exists and equals a positive rational number in the interval*

$$\left[\frac{1}{m^n}\cdot\prod_{p\in\mathcal{P}}\frac{1}{p^{(j_p-1)(n+1)}\cdot(p^{n+1}-1)},\prod_{p\in\mathcal{P}}\left(1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)}\right)\right]$$

whose denominator divides $m^n\cdot\prod_{p\in\mathcal{P}}\big(p^{(n+1)j_p-1}\cdot(p^{n+1}-1)\big)$.

(b) $\mathrm{d}(A(W,V))=1$ *if and only if* $V=W$ *or* W *is finite.*

(c) $\mathrm{d}(A(W,V))$ *is computable as a function of* K, W *and* V.

Proof. By Theorem 2.21 we have that $\mathrm{d}(A(W,V))$ exists and is equal to

$$\tfrac{1}{[L:K]}\prod_{p\in\mathcal{P}}\left[\tfrac{1}{[L(U^{1/p^{j_p}}):L]}\cdot\tfrac{p^n(p-1)}{p^{n+1}-1}+\sum_{i=0}^{j_p-1}\left(\tfrac{1}{[L(U^{1/p^i}):L]}-\tfrac{1}{[L(U^{1/p^i},W^{1/p^{i+1}}):L]}\right)\right],$$

which is rational. We first note that $[L:K]$ divides $\phi(m)m^{n-1}$, where ϕ is Euler's totient function.

Now, let $p\in\mathcal{P}$. By Lemma 2.23 we have for all $i\in\mathbf{Z}_{\geq 0}$ that

$$[L(U^{1/p^{i+1}}):L(U^{1/p^i})]\mid p^{n+1}$$

and

$$[L(U^{1/p^i},W^{1/p^{i+1}}):L(U^{1/p^i})]\mid p.$$

To ease the notation, for $i\in\mathbf{Z}_{\geq 0}$ write

$$T_i=\frac{1}{[L(U^{1/p^i}):L]}-\frac{1}{[L(U^{1/p^i},W^{1/p^{i+1}}):L]},$$

and note that

$$T_i=\frac{1}{[L(U^{1/p^i}):L]}\left(1-\frac{1}{[L(U^{1/p^i},W^{1/p^{i+1}}):L(U^{1/p^i})]}\right).$$

Hence $[L(U^{1/p^i},W^{1/p^{i+1}}):L(U^{1/p^i})]=1$ implies $T_i=0$. Using Lemma 2.23 we obtain for $p\in\mathcal{P}$

$$\frac{1}{[L(U^{1/p^{j_p}}):L]}\cdot\frac{p^n(p-1)}{p^{n+1}-1}+\sum_{i=0}^{j_p-1}T_i\geq\frac{1}{p^{(n+1)j_p}}\cdot\frac{p^{n+1}-p^n}{p^{n+1}-1}=\frac{p-1}{p^{n(j_p-1)+j_p}(p^{n+1}-1)},$$

so that

$$\begin{aligned}\mathrm{d}(A(W,V)) &\geq \frac{1}{[L:K]}\prod_{p\in\mathcal{P}}\frac{p-1}{p^{n(j_p-1)+j_p}(p^{n+1}-1)}\\ &\geq \frac{1}{\phi(m)m^{n-1}}\prod_{p\in\mathcal{P}}\frac{p-1}{p^{n(j_p-1)+j_p}(p^{n+1}-1)}.\end{aligned}$$

Then using the identity $\phi(m) = m\cdot\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p}\right)$ in the latter, we obtain the lower bound

$$\frac{1}{m^n}\cdot\prod_{p\in\mathcal{P}}\frac{1}{p^{(j_p-1)(n+1)}\cdot(p^{n+1}-1)}$$

for $\mathrm{d}(A(W,V))$. For the upper bound, note that

$$\sum_{i=0}^{j_p-1}T_i \leq 1-\frac{1}{[L(U^{1/p^{j_p}}):L]}.$$

Then for $p\in\mathcal{P}$ write $d_p = [L(U^{1/p^{j_p}}):L]$, so that we have

$$\begin{aligned}\frac{1}{d_p}\cdot\frac{p^n(p-1)}{p^{n+1}-1}+\sum_{i=0}^{j_p-1}T_i &\leq \frac{1}{d_p}\cdot\frac{p^n(p-1)}{p^{n+1}-1}+1-\frac{1}{d_p}\\ &\leq 1-\frac{1}{p^{(n+1)j_p}}\left(1-\frac{p^n(p-1)}{p^{n+1}-1}\right)\\ &= 1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)},\end{aligned}$$

where we use that $d_p \leq p^{(n+1)j_p}$ (see Lemma 2.23). Thus, as $[L:K]\geq 1$, an upper bound for $\mathrm{d}(A(W,V))$ is

$$\prod_{p\in\mathcal{P}}\left(1-\frac{p^n-1}{p^{(n+1)j_p}\cdot(p^{n+1}-1)}\right).$$

Now, we want to find $x\in\mathbf{Z}_{\geq 1}$ such that $x\cdot\mathrm{d}(A(W,V))\in\mathbf{Z}$. To this end, note that

$$\phi(m)m^{n-1}\cdot[L:K]^{-1}\in\mathbf{Z}.$$

Moreover, by Lemma 2.23 we have

$$p^{(n+1)j_p}\cdot[L(U^{1/p^{j_p}}):L]^{-1}\in\mathbf{Z}.$$

As for $i \in \{0, \dots, j_p-1\}$ the fields $L(U^{1/p^i})$ and $L(U^{1/p^i}, W^{1/p^{i+1}})$ are contained in $L(U^{1/p^{j_p}})$, we have

$$p^{(n+1)j_p} \cdot \sum_{i=0}^{j_p-1} T_i \in \mathbf{Z}.$$

It follows that the denominator of $\mathrm{d}(A(W,V))$ divides

$$\phi(m)m^{n-1} \prod_{p\in\mathcal{P}} \left(p^{(n+1)j_p} \cdot \frac{p^{n+1}-1}{p-1} \right),$$

which by using $\phi(m) = m \cdot \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p}\right)$ is equal to

$$m^n \cdot \prod_{p\in\mathcal{P}} \left(p^{(n+1)j_p-1} \cdot \left(p^{n+1}-1\right)\right),$$

as desired.

From the lower bound, we see that $\mathrm{d}(A(W,V))$ is nonzero. From the upper bound, we see that $\mathrm{d}(A(W,V)) = 1$ only if $m = 1$ or $n = 0$, that is, only if $V = W$ or W is finite. On the other hand, if $V = W$ or W is finite, we easily see that $\mathrm{d}(A(W,V)) = 1$. This proves (a) and (b).

To prove (c), we will show that there exists an algorithm that terminates after finitely many steps, whose input is K, W, and V, and whose output is the density $\mathrm{d}(A(W,V))$. Let K, W, V, n, $\mathcal{P}$, U, and L be as in the theorem. By Theorem 2.21 we have that $\mathrm{d}(A(W,V))$ equals

$$\tfrac{1}{[L:K]} \prod_{p\in\mathcal{P}} \left[\tfrac{1}{[L(U^{1/p^{j_p}}):L]} \cdot \tfrac{p^n(p-1)}{p^{n+1}-1} + \sum_{i=0}^{j_p-1} \left(\tfrac{1}{[L(U^{1/p^i}):L]} - \tfrac{1}{[L(U^{1/p^i}, W^{1/p^{i+1}}):L]} \right) \right],$$

so it suffices to show that there exist three algorithms for calculating (1) $\mathcal{P}$, (2) $(j_p)_{p\in\mathcal{P}}$, and (3) the degrees of the field extensions $[L(U^{1/p^i}) : L]$ and $[L(U^{1/p^i}, W^{1/p^{i+1}}) : L]$ for $i \in \{0, \dots, j_p\}$. The algorithms for (1) and (3) are well-known from elementary computational algebraic number theory for which we refer to [Coh96]. It remains to show that for each $p \in \mathcal{P}$ we can compute j_p.

To this end, let $p \in \mathcal{P}$, and let $s = p^\infty$. Let

$$F = \begin{cases} L(\mu_4) & \text{if } p = 2 \\ L & \text{otherwise.} \end{cases}$$

Compute and write

$$U = \coprod_{i=1}^{k} u_i \cdot U^p,$$

and compute

$$S_0 = \langle x \in F : x^p \in \{u_1, \ldots, u_k\} \rangle.$$

If $S_0 \subset U$, we have $\exp(\mathrm{Sat}_s(U, F)/U) = 1$ and put $j_p = 0$ (see Theorem 2.17). Otherwise, let $U_1 = U \cdot S_0$, and write

$$U_1 = \coprod_{i=1}^{k_1} u_{i,1} \cdot U_1^p.$$

Then compute

$$S_1 = \langle x \in F : x^p \in \{u_{1,1}, \ldots, u_{k_1,1}\} \rangle.$$

If $S_1 \subset U_1$, then we have $\exp(\mathrm{Sat}_s(U, F)/U) = p$ and put $j_p = 1$. Otherwise, repeat the above process to define U_2 and find S_2, and so on. By Lemma 2.19 the quotient $\mathrm{Sat}_s(U, F)/U$ is finite, so there is $i \in \mathbf{Z}$ such that $S_i \subset U_i$. Continue the above process until $S_i \subset U_i$, and put $j_p = i$. Then observe that $\exp(\mathrm{Sat}_s(U, F)/U) = p^{j_p}$. This shows that there is an algorithm to compute $(j_p)_{p \in \mathcal{P}}$, which finishes the proof of (c). ■

Theorem 2.25. *Let K be a number field, and let W be a finitely generated subgroup of K^* of positive rank, and let V be a cocyclic cofinite subgroup of W. Let V' be a subgroup of W containing V. Then $\mathrm{d}(A(W, V)) = \mathrm{d}(A(W, V'))$ if and only if $V = V'$.*

Proof. First, note that $V = V'$ clearly implies $\mathrm{d}(A(W, V)) = \mathrm{d}(A(W, V'))$. To prove the reverse implication, let V' be a subgroup of W containing V, and assume $V' \neq V$. We will show that $\mathrm{d}(A(W,V)) < \mathrm{d}(A(W,V'))$, which finishes the proof. As for V'' such that $V \subset V'' \subset V'$ we have

$$\mathrm{d}(A(W,V)) \leq \mathrm{d}(A(W,V'')) \leq \mathrm{d}(A(W,V')),$$

we may assume that V is of prime index, say q, in V'.

Now, let $m = (W : V)$, let $U = V^{1/m}$, let $L = K(U)$, let $A'(W,V)$ as defined above Lemma 2.12, and let $\overline{L}$ be an algebraic closure of L (and of K). For p dividing m and $i \in \mathbf{Z}_{\geq 0}$, let $G_{p,i}$, $H_{p,i}$, $C_{p,i}$, C_p and C be as defined above Lemma 2.14. Then by Lemma 2.16 and Lemma 2.12 we have

$$\mathrm{d}(A(W,V)) = \frac{1}{[L:K]} \cdot \lambda_{\mathrm{Gal}(\overline{L}/L)}(C).$$

Observe that $\mathrm{Gal}(\overline{L}/L)$ is a subgroup of $G = \mathrm{Gal}(\overline{L}/K)$ of index $[L : K]$. By abuse of notation we write C for the image of C in G, that is, henceforth we have

$$C = \{\sigma \in \mathrm{Gal}(\overline{L}/K) : \sigma|_U = \mathrm{id}_U,\ \forall p|m : \exists i \in \mathbf{Z}_{\geq 0} : \sigma|_{U^{1/p^i}} = \mathrm{id} \wedge \sigma|_{W^{1/p^{i+1}}} \neq \mathrm{id}\}.$$

Then we have

$$\mathrm{d}(A(W,V)) = \lambda_G(C).$$

Now, let $m/q = m' = (W : V')$, let $U' = V'^{1/m'}$, let $L' = K(U')$, and note that $V' \subset V^{1/q}$ implies that $U' \subset U$ and $L' \subset L$. For p dividing m' and $i \in \mathbf{Z}_{\geq 0}$ let $G'_{p,i}$, $H'_{p,i}$, $C'_{p,i}$, C'_p and C' be defined as above with L replaced by L' and U by U'. Moreover, by abuse of notation write C' for the image of C' in G, so that

$$C' = \{\sigma \in \mathrm{Gal}(\overline{L}/K) : \sigma|_{U'} = \mathrm{id}_{U'},\ \forall p|m' : \exists i \in \mathbf{Z}_{\geq 0} : \sigma|_{U'^{1/p^i}} = \mathrm{id} \wedge \sigma|_{W^{1/p^{i+1}}} \neq \mathrm{id}\}.$$

Then we have

$$\mathrm{d}(A(W,V')) = \lambda_G(C').$$

Moreover, for every prime p and $i \in \mathbf{Z}_{\geq 0}$ we have $U'^{1/p^i} \subset U^{1/p^i}$, so $C \subset C' \subset G$. We will show that there is a non-empty open subset of C' that is disjoint from C, which by the above and the fact that non-empty open subsets have positive density, proves that

$$\mathrm{d}(A(W, V)) < \mathrm{d}(A(W, V')),$$

as desired. Let $j \in \mathbf{Z}_{\geq 0}$ be such that $\mathrm{Aut}_{U^{1/q^j}}(U^{1/q^\infty}) \subset \mathrm{Gal}(L(U^{1/q^\infty})/L)$ (see Theorem 2.17).

Suppose first that q does not divide m'. For primes p dividing m', let

$$X_p = C_p = \bigcup_{i=0}^{\infty} G_{p,i} \setminus H_{p,i}$$

and

$$X_q = H_{q,j} \setminus G_{q,j+1}.$$

Note that $X_q \cap C_q = \emptyset$. We claim that the set

$$X = \bigcap_{p|m} X_p$$

has the desired properties of being a non-empty open subset of C' that is disjoint from C. That X is open is proved in the same way as Lemma 2.14. That each X_p, including X_q, is non-empty follows from Lemma 2.23 (at this point it is used that W is infinite, so that n in Lemma 2.23(a) is positive). Since for primes p dividing m the degrees of the fields $L(U^{1/p^\infty})$ over L are p-powers, they are all linearly disjoint over L, so X is non-empty as well. As q does not divide m', we have $X \subset C'$. From $X_q \cap C_q = \emptyset$ it follows that we have $X \cap C = \emptyset$. This finishes the proof of this case.

Now, suppose that q divides m'. We claim that for every $i \in \mathbf{Z}_{\geq 0}$ we have

$$U'^{1/q^i} = V^{1/(m'q^i)} \cdot W^{1/q^i}.$$

It suffices to prove the claim for $i = 0$. To this end, observe that

$$V^{1/m'} \cdot W \neq V^{1/m'},$$

because W/V is cyclic of order $m'q$. Moreover, as $W \subset U'$, it follows that

$$V^{1/m'} \cdot W \subset U'.$$

As V'/V has order q, also $U'/V^{1/m'}$ has order q. It follows that $U' = V^{1/m'} \cdot W$, which finishes the proof of the claim. We remark that for $i \in \mathbf{Z}_{\geq 1}$ we have

$$V^{1/(m'q^i)} = V^{1/(mq^{i-1})} = U^{1/q^{i-1}},$$

so that the claim states that

$$U'^{1/q^i} = U^{1/q^{i-1}} \cdot W^{1/q^i}.$$

As $U^q = V^{1/m'}$ is contained in $V'^{1/m'} = U'$, we have $U \subset U'^{1/q}$, so that

$$L' \subset L \subset L'(U'^{1/q}).$$

Then the claim implies that for every $i \in \mathbf{Z}_{\geq 0}$ we have

$$L'(U'^{1/q^{i+1}}) = L(U^{1/q^i}, W^{1/q^{i+1}}),$$

and moreover, since $W \subset U$, we have the following diagram

$$\begin{tikzcd}
 & L'(U'^{1/q^{i+2}}) = L(U^{1/q^{i+1}}, W^{1/q^{i+2}}) \arrow[dl, dash] \arrow[dr, dash] & \\
L'(U'^{1/q^{i+1}}, W^{1/q^{i+2}}) \arrow[dr, dash] & & L(U^{1/q^{i+1}}) \arrow[dl, dash] \\
 & L'(U'^{1/q^{i+1}}) = L(U^{1/q^i}, W^{1/q^{i+1}}) &
\end{tikzcd}$$

of fields, where the upper field is the composite of the fields on the left and right. The corresponding diagram of Galois groups looks as follows:

$$\begin{tikzcd}
 & G'_{q,i+2} = H_{q,i+1} = H'_{q,i+1} \cap G_{q,i+1} \arrow[dl, hook] \arrow[dr, hook] & \\
H'_{q,i+1} \arrow[dr, hook] & & G_{q,i+1} \arrow[dl, hook] \\
 & G'_{q,i+1} = H_{q,i} &
\end{tikzcd}$$

where the arrows in the diagram depict inclusions.

Now, for the prime divisors p of m' that are not equal to q, let

$$Y_p = C'_p = \bigcup_{i=0}^{\infty} G'_{p,i} \setminus H'_{p,i},$$

and let

$$Y_q = G'_{q,j+1} \setminus \big(H'_{q,j+1} \cup G_{q,j+1}\big).$$

Note that one has $Y_q \subset H_{q,j} \setminus G_{q,j+1}$, so that we have $Y_q \cap C_q = \emptyset$. We claim that the set $Y = \bigcap_{p|m} Y_p$ has the desired property of being a non-empty open subset of C' that is disjoint from C. That Y is open is proved in the same way as Lemma 2.14. We next prove that each Y_p is non-empty. For $p \neq q$ this follows directly from Lemma 2.23. For $q = p$, our choice of j and Lemma 2.23 imply first that $G_{q,j+1}$ has index q^n in $H_{q,j}$, and next that $H_{q,j+1}$ has index q in $G_{q,j+1}$, which by $H_{q,j+1} = H'_{q,j+1} \cap G_{q,j+1}$ implies that $G_{q,j+1}$ is not contained in $H'_{q,j+1}$, so that $H'_{q,j+1} \neq H_{q,j}$. Thus, since $n \in \mathbf{Z}_{>1}$, each of $G_{q,j+1}$ and $H'_{q,j+1}$ is a proper subgroup of $G'_{q,j+1} = H_{q,j}$, which implies that Y_q is non-empty. By linear disjointness, the set Y is non-empty as well. From $Y_q \cap C_q = \emptyset$ it follows that we have $Y \cap C = \emptyset$, while from

$$Y_q \subset G'_{q,j+1} \setminus H'_{q,j+1} \subset C'_q$$

we obtain $Y \subset C'$. This finishes the proof. ■

Corollary 2.26. *Let K be a number field, let W be a finitely generated subgroup of K^*, and let V be a cofinite cocyclic subgroup of W. Let*

$$S = \{\mathfrak{p} \in \Omega_K : \text{ there is } w \in W \text{ such that } \mathrm{v}_{\mathfrak{p}}(w) \neq 0\}.$$

For $\mathfrak{p} \in \Omega_K \setminus S$ let $W_{\mathfrak{p}}$ denote the kernel of the restriction map $\pi_{\mathfrak{p}} \colon W \longrightarrow \kappa(\mathfrak{p})^*$. Let S' be a finite subset of $\Omega_K \setminus S$. Then there are $t \in \mathbf{Z}_{\geq 1}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t \in \Omega_K \setminus S'$ such that

$$V = \langle W_{\mathfrak{p}_i} : i \in \{1, \ldots, t\}\rangle.$$

Proof. Let $T = \langle W_{\mathfrak{p}} : \mathfrak{p} \notin S', W_{\mathfrak{p}} \subset V\rangle$. Then T is cofinite and contained in V, and moreover, $\mathrm{d}(A(W, V)) > 0$ implies that T is cocyclic in W. Since T is finitely generated, there are $t \in \mathbf{Z}_{\geq 0}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t \in \Omega_K \setminus S'$ such that $T = \langle W_{\mathfrak{p}_i} : i \in \{1, \ldots, t\}\rangle$. Now, one easily sees that $\mathrm{d}(A(W, T)) = \mathrm{d}(A(W, V))$. Hence Theorem 2.25 implies that $T = V$, as desired. ■

8. Applications

Theorem 2.27. *Let K be a number field, and let X and Y be finitely generated subgroups of K^*. Let*

$$S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X \cup Y : \mathrm{v}_{\mathfrak{p}}(x) \neq 0\}.$$

Suppose that for all primes $\mathfrak{p}$ in a subset of $\Omega_K \setminus S'$ of density one, we have

$$Y \ (\mathrm{mod}\ \mathfrak{p}) \subset X \ (\mathrm{mod}\ \mathfrak{p}).$$

Then $Y \subset X$.

Proof. Suppose that $Y \not\subset X$, let $W = Y \cdot X$, and note that $X \subsetneq W$. As W is a finitely generated abelian group, there exist a prime number p and a surjective morphism

$$f \colon W \longrightarrow \mathbf{Z}/p\mathbf{Z}$$

of groups with kernel containing X. Let $V = \ker f$, and note that $X \subset V$. As W/V is finite cyclic, Theorem 2.24 implies that

$$\mathrm{d}(\{\mathfrak{p} \in \Omega_K : W_\mathfrak{p} \subset V\}) > 0,$$

where $W_\mathfrak{p}$ is the kernel of the reduction map $\pi_\mathfrak{p} \colon W \longrightarrow \kappa(\mathfrak{p})^*$.

Observe that for $\mathfrak{p} \in \Omega_K \setminus S'$ the condition $Y \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}}$ is equivalent to $X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}}$, so that

$$\mathrm{d}(\{\mathfrak{p} \in \Omega_K : X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}}\}) = 1.$$

Let $\mathfrak{p}$ be a prime of K such that $W_\mathfrak{p} \subset V$ and $X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}}$. As $X \subset V$ and $W_\mathfrak{p} \subset V$, we have

$$\pi_\mathfrak{p}(X) = (X \cdot W_\mathfrak{p})/W_\mathfrak{p} \subset V/W_\mathfrak{p}.$$

Moreover, since f is surjective, we have

$$W_\mathfrak{p} \subset V \subsetneq W.$$

Hence $V/W_\mathfrak{p} \subsetneq W/W_\mathfrak{p}$. However

$$X \pmod{\mathfrak{p}} = W \pmod{\mathfrak{p}} \cong W/W_\mathfrak{p},$$

which is a contradiction. It follows that $Y \subset X$. ■

Theorem 2.28. *Let K be a number field, let X be a finitely generated subgroup of K^*, let Y be a subgroup of X, and let l be a prime number. Let*

$$S' = \{\mathfrak{p} \in \Omega_K : \exists x \in X : \mathrm{v}_\mathfrak{p}(x) \neq 0\}.$$

Suppose that for almost all $\mathfrak{p} \in \Omega_K \setminus S'$ we have

$$l \nmid (X \pmod{\mathfrak{p}} : Y \pmod{\mathfrak{p}}).$$

Then $(X : Y) < \infty$ and $l \nmid (X : Y)$.

Proof. Let $V = X^l \cdot Y$, and note that $Y \subset V \subset X$. For almost all $\mathfrak{p} \in \Omega_K$ we have $l \nmid (X \pmod{\mathfrak{p}} : Y \pmod{\mathfrak{p}})$. As $X \pmod{\mathfrak{p}}/V \pmod{\mathfrak{p}}$ is annihilated by l and for almost all $\mathfrak{p}$ we have

$$Y \pmod{\mathfrak{p}} \subset V \pmod{\mathfrak{p}} \subset X \pmod{\mathfrak{p}},$$

it follows that for almost all $\mathfrak{p}$ we have $X \pmod{\mathfrak{p}} = V \pmod{\mathfrak{p}}$. Then Theorem 2.27 implies that $X = V = X^l \cdot Y$, so that $(X/Y)^l = X/Y$. As X/Y is a finitely generated abelian group with the property that $(X/Y)^l = X/Y$, it follows that X/Y is finite of order coprime to l. ■

CHAPTER 3

Reductions of the Mordell-Weil group over number fields

1. Introduction

In this chapter we carry out for elliptic curves with complex multiplication the analogue of Chapter 2 for the multiplicative group. In the previous chapter, say in the *multiplicative case*, all modules involved are over $\mathbf{Z}$, whereas in this chapter, say in the *elliptic case*, the modules are over the endomorphism ring of an elliptic curve with complex multiplication. Moving from the principal ideal domain $\mathbf{Z}$ to an order in a quadratic number field, which is not necessarily a principal ideal domain, is where the complications are met in this chapter. For simplicity, we do assume that the order is maximal, in the sense that it is a Dedekind domain, but we remark that with some minor alterations the theorems in this chapter remain valid without the maximality restriction.

For our first theorem, recall Theorem 1.1 from Chapter 1, also known as *Schinzel's theorem*. We state and prove an analogue of this theorem for elliptic curves with complex multiplication.

For a field K of characteristic 0, an algebraic closure $\overline{K}$ of K, an elliptic curve E over K with endomorphism ring $\mathcal{O} = \operatorname{End}_K(E)$, and an ideal $\mathfrak{a}$ of $\mathcal{O}$ we write

$$E(K)[\mathfrak{a}] = \{P \in E(K) : \mathfrak{a} \cdot P = 0\}$$

for the $\mathcal{O}$-module of $\mathfrak{a}$-*torsion points* of E over K, and we write

$$E[\mathfrak{a}] = \{P \in E(\overline{K}) : \mathfrak{a} \cdot P = 0\}$$

for the $\mathcal{O}$-module of all $\mathfrak{a}$-torsion points. Then for elliptic curves the analogue of the nth radicals of an algebraic number is obtained by *dividing* points of the elliptic curve by an ideal $\mathfrak{a}$ of $\mathcal{O}$. More precisely, for an $\mathcal{O}$-submodule W of $E(\overline{K})$ and a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$ we write

$$W : \mathfrak{a} = \{P \in E(\overline{K}) : \mathfrak{a} \cdot P \subset W\}$$

for the $\mathcal{O}$-module of $\mathfrak{a}$-*division points* of W. Field extensions of K obtained by adjoining division points are called *division fields* over K.

Moreover, for a module M over a ring R we write

$$\operatorname{Ann}_R(M) = \{r \in R : rM = 0\}$$

for the two-sided *annihilator ideal* of M. Then the analogue of Schinzel's theorem, mentioned above, is as follows.

Theorem 11. *Let K be a field of characteristic 0, let E be an elliptic curve over K with $\mathcal{O} = \operatorname{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, let $W \subset E(K)$ be an $\mathcal{O}$-submodule, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Then $K(W : \mathfrak{a})$ is abelian over K if and only if*

$$\operatorname{Ann}_{\mathcal{O}}(E(K)[\mathfrak{a}]) \cdot W \subset \mathfrak{a} \cdot E(K).$$

See Section 3.4 for the proof of this theorem.

Our second main theorem is an analogue of Theorem 2.17(a) for elliptic curves with complex multiplication. Let K be a number field, and let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain. Let

$$\widehat{\mathcal{O}} = \varprojlim_{\mathfrak{b}} \mathcal{O}/\mathfrak{b},$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$, be the profinite completion of $\mathcal{O}$ as a ring. A *Steinitz ideal* $\mathfrak{a}$ of $\mathcal{O}$ is a closed ideal of $\widehat{\mathcal{O}}$. See Definition 3.5 for more details.

Let W be an $\mathcal{O}$-submodule of $E(K)$, and let $\mathfrak{a}$ be a Steinitz ideal. Then we define

$$\begin{aligned} E(K)[\mathfrak{a}] &= \bigcup_{\mathfrak{b}} E(K)[\mathfrak{b}], \\ E[\mathfrak{a}] &= \bigcup_{\mathfrak{b}} E[\mathfrak{b}], \\ W\colon\mathfrak{a} &= \bigcup_{\mathfrak{b}} W\colon\mathfrak{b}, \end{aligned}$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$.

Now, the field $K(W\colon\mathfrak{a})$ is Galois over K, and any field automorphism of $K(W\colon\mathfrak{a})$ over K is determined by its action on $W\colon\mathfrak{a}$. Moreover, the action of $\mathcal{O}$ on $W\colon\mathfrak{a}$ commutes with the action of Galois. Hence, we may identify $\mathrm{Gal}(K(W\colon\mathfrak{a})/K)$ with a subgroup of the group of $\mathcal{O}$-automorphisms $\mathrm{Aut}_{\mathcal{O},W}(W\colon\mathfrak{a})$ of $W\colon\mathfrak{a}$ that are the identity on W. Note that $\mathrm{Aut}_{\mathcal{O},W}(W\colon\mathfrak{a})$ is the profinite group

$$\varprojlim_{\mathfrak{b}} \mathrm{Aut}_{\mathcal{O},W}(W\colon\mathfrak{b}),$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. As $\mathrm{Gal}(K(W\colon\mathfrak{a})/K)$ is compact and $\mathrm{Aut}_{\mathcal{O},W}(W\colon\mathfrak{a})$ is Hausdorff, the subgroup $\mathrm{Gal}(K(W\colon\mathfrak{a})/K)$ of $\mathrm{Aut}_{\mathcal{O},W}(W\colon\mathfrak{a})$ is closed.

Theorem 12. *Let K be a number field, and let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain. Let $W \subset E(K)$ be an $\mathcal{O}$-submodule, and let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then the map*

$$\iota\colon\ \mathrm{Gal}(K(W\!:\mathfrak{a})/K) \longrightarrow \mathrm{Aut}_{\mathcal{O},W}(W\!:\mathfrak{a})$$

is open.

See Section 3.7 for the proof.

We prove this theorem in two steps. As in the case of the multiplicative group, we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(K(W\!:\mathfrak{a})/K(E[\mathfrak{a}])) \arrow[r] \arrow[d] & \mathrm{Gal}(K(W\!:\mathfrak{a})/K) \arrow[r] \arrow[d, "\iota"'] & \mathrm{Gal}(K(E[\mathfrak{a}])/K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Aut}_{\mathcal{O},W+E[\mathfrak{a}]}(W\!:\mathfrak{a}) \arrow[r] & \mathrm{Aut}_{\mathcal{O},W}(W\!:\mathfrak{a}) \arrow[r] & \mathrm{Aut}_{\mathcal{O},W[\mathfrak{a}]}(E[\mathfrak{a}]) \arrow[r] & 0.
\end{tikzcd}$$

In Section 3.5 we prove that the right vertical map is open, and do so effectively. The latter means that we give an explicit nonzero ideal $\mathfrak{b}$ of $\mathcal{O}$ dividing $\mathfrak{a}$ such that

$$\mathrm{Aut}_{\mathcal{O},E[\mathfrak{b}]}(E[\mathfrak{a}]) \subset \mathrm{Gal}(K(E[\mathfrak{a}])/K).$$

In Section 3.6 we prove that the left vertical map is open. By combining these two results, we prove that the middle vertical map is open, as desired.

As an application of the above theorems, we state and prove an analogue of Theorem 6 of Chapter 2, see Theorem 13 below.

Let W be an $\mathcal{O}$-submodule of $E(K)$, let V be an $\mathcal{O}$-submodule of W such that

$$W/V \cong \mathcal{O}/I$$

as $\mathcal{O}$-modules, for some nonzero ideal I of $\mathcal{O}$.

Throughout this chapter, we use the phrase *almost all* as a substitute for *all but finitely many*. Let Ω_K be the set of maximal ideals of $\mathcal{O}_K$. Choosing a model of E over a finitely generated subring of K, we may talk about the reduction of E modulo $\mathfrak{p}$ for almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$, and denote it by $E_\mathfrak{p}$. For the definition of *good*, *bad*, *ordinary*, and *supersingular reduction* we refer to [Sil94].

As all elements of $\mathcal{O}$ are defined over K, the action of $\mathcal{O}$ on the tangent space at the origin induces an injective ring morphism $\mathcal{O} \longrightarrow K$, which extends to an injective map $F \longrightarrow K$ (see [Sil94, Chapter 2]). Throughout this chapter, we identify $\mathcal{O}$ and F with their images in K, so that we have $\mathcal{O} \subset \mathcal{O}_K$ and $F \subset K$.

Let S be the subset of Ω_K consisting of the primes where $E_\mathfrak{p}$ is not defined, the primes of bad reduction for E, the primes of supersingular reduction for E (see [Sil94]), and the primes dividing $I \cdot \mathcal{O}_K$. By [Lan87, Theorem 12, §13.4] the set of supersingular primes has density zero. As there are only finitely many primes for which $E_\mathfrak{p}$ is not defined, finitely many primes of bad reduction for E, and finitely many primes dividing $I \cdot \mathcal{O}_K$, the set S has density zero too.

Now, for every $\mathfrak{p} \in \Omega_K \setminus S$ we have a reduction map

$$\pi_\mathfrak{p} \colon W \longrightarrow E_\mathfrak{p}(\kappa(\mathfrak{p}))$$

of $\mathcal{O}$-modules, where $\kappa(\mathfrak{p})$ is the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$. We define

$$A(W, V) = \{\mathfrak{p} \in \Omega_K \setminus S : \ker(\pi_\mathfrak{p}) \subset V\},$$

for which we often simply write A.

Then we prove the following theorem about the density $\mathrm{d}(A(W, V))$.

Theorem 13. *Suppose that I is not divisible by any prime number that splits completely in $\mathcal{O}$. Then the following statements hold.*

(a) *The set* $A(W,V)$ *has a natural density* $\mathrm{d}(A(W,V))$ *in* Ω_K.

(b) *The density* $\mathrm{d}(A(W,V))$ *is rational.*

(c) *The density* $\mathrm{d}(A(W,V))$ *is positive.*

(d) *We have* $\mathrm{d}(A(W,V)) = 1$ *if and only if* $V = W$ *or* W *is finite.*

The proof of this theorem has a similar structure to that of Theorem 6 in Section 2.1. Note that computability of $\mathrm{d}(A(W,V))$ is missing in this theorem. There is little doubt that detailed scrutiny of our proofs will lead to a proof that $\mathrm{d}(A(W,V))$ is indeed computable, and that likewise the assumption on the ideal I can be omitted at the cost of some additional complications. We leave these issues to the diligence of the interested reader.

The present chapter is organised as follows.

In Section 3.2 we define division in modules over a commutative ring. In Section 3.3 we apply this theory to elliptic curves, and define Steinitz ideals and treat their properties. Section 3.4 contains the proof of Theorem 11 above. In Section 3.5 we prove the openness of the right vertical map in the commutative diagram above, and in Section 3.6 we prove that the left vertical map is open. Section 3.7 contains the proof of Theorem 12. In Section 3.8 we prove part (a) of Theorem 13, and in Section 3.9 we prove part (b) of the same theorem. The last Section 3.10 consists of the proofs of the last two parts (c) and (d) of Theorem 13.

2. Division in modules

Let $\mathcal{O}$ be a commutative ring, and let M be an $\mathcal{O}$-module. Let W be an $\mathcal{O}$-submodule of M, and let $\mathfrak{a} \subset \mathcal{O}$ be an ideal. Then we define the *module of* $\mathfrak{a}$*-division points of* W *in* M as

$$W :_M \mathfrak{a} = \{x \in M : \mathfrak{a} \cdot x \subset W\}.$$

If $\mathfrak{a} = (a)$ is principal, we simply write $W :_M a$. Moreover, if $W = \mathcal{O} \cdot x$, we simply write $W :_M \mathfrak{a} = x :_M \mathfrak{a}$. When the module M is understood, we leave it out of the notation.

We define *the module of* $\mathfrak{a}$*-torsion points* $M[\mathfrak{a}]$ as $0 \colon \mathfrak{a}$. Note that $M[\mathfrak{a}] \subset W \colon \mathfrak{a}$ and $(W \colon \mathfrak{a})/W = (M/W)[\mathfrak{a}]$.

Lemma 3.1. *Suppose that* $\mathfrak{a}$ *is finitely generated, and let* S *be a multiplicatively closed subset of* $\mathcal{O}$*. Then* $S^{-1}(W :_M \mathfrak{a}) = S^{-1}W :_{S^{-1}M} S^{-1}\mathfrak{a}$*.*

Proof. Suppose $\mathfrak{a}$ is generated by $a_1, \dots, a_n \in \mathcal{O}$, where $n \in \mathbf{Z}_{\geq 1}$. Then $W \colon \mathfrak{a}$ is the kernel of the morphism

$$f \colon M \longrightarrow \bigoplus_{i=1}^{n} M/W$$

of $\mathcal{O}$-modules defined by $x \mapsto (a_1 \cdot x + W, \dots, a_n \cdot x + W)$. By exactness of $S^{-1}(-)$, we then have that $S^{-1}(W \colon \mathfrak{a})$ is the kernel of

$$S^{-1}(f) \colon S^{-1}M \longrightarrow \bigoplus_{i=1}^{n} S^{-1}M/S^{-1}W.$$

Observe that the kernel of $S^{-1}(f)$ is exactly equal to $S^{-1}W :_{S^{-1}M} S^{-1}\mathfrak{a}$, which proves the lemma. ■

Proposition 3.2. *Let* W *and* V *be* $\mathcal{O}$*-submodules of* M*, and let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be ideals of* $\mathcal{O}$ *that are coprime. Then* $W \colon \mathfrak{a}\mathfrak{b} = W \colon \mathfrak{a} + W \colon \mathfrak{b}$*.*

Proof. First, observe that the right to left inclusion is straightforward. To prove the other inclusion, let $x \in W \colon \mathfrak{a}\mathfrak{b}$. As $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. Note that $\mathfrak{b} \cdot ax \subset W$ and $\mathfrak{a} \cdot bx \subset W$, so that $ax \in W \colon \mathfrak{b}$ and $bx \in W \colon \mathfrak{a}$. It follows that $x = (a + b)x = ax + bx \in W \colon \mathfrak{a} + W \colon \mathfrak{b}$. ■

We say an ideal $\mathfrak{a}$ of $\mathcal{O}$ is *invertible* if it is projective of rank 1. Moreover, throughout the rest of this section, and only in this section, we denote the localisation of an $\mathcal{O}$-module N at a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ by $N_{\mathfrak{p}}$.

Proposition 3.3. *Let W be an $\mathcal{O}$-submodule of M, and let $\mathfrak{a} \subset \mathcal{O}$ be an invertible ideal.*

(a) *Then* $\mathfrak{a}W : \mathfrak{a} = W + M[\mathfrak{a}]$.

(b) *Suppose that* $\mathfrak{a}M = M$. *Then* $W = \mathfrak{a}(W : \mathfrak{a})$.

Proof. First, observe that the right to left inclusions of (a) and (b) are straightforward. To prove the left to right inclusions of (a) and (b), we first prove them in the case that $\mathfrak{a}$ is principal. To this end, suppose that $\mathfrak{a} = (a)$, and let $x \in aW : a$. Then $ax = aw$ for some $w \in W$, so that $x - w \in M[a]$. It follows that $x \in W + M[a]$. This proves (a) for principal ideals $\mathfrak{a}$.

Let $x \in W$. As $aM = M$, there is $y \in M$ such that $ay = x$, and hence $y \in W : a$. It follows that $x \in \mathfrak{a}(W : \mathfrak{a})$, which proves (b) for principal ideals $\mathfrak{a}$.

Now, suppose $\mathfrak{a}$ is any invertible ideal. As $\mathfrak{a}$ is projective of rank 1, it is finitely generated and its localisation at every prime $\mathfrak{p}$ of $\mathcal{O}$ is principal in $\mathcal{O}_{\mathfrak{p}}$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}$. Then $(\mathfrak{a}W)_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}W_{\mathfrak{p}}$. By Lemma 3.1 we have

$$(\mathfrak{a} \cdot W : \mathfrak{a})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}W_{\mathfrak{p}} :_{M_{\mathfrak{p}}} \mathfrak{a}_{\mathfrak{p}}.$$

On the other hand, by exactness of localisation we have

$$(W + M[\mathfrak{a}])_{\mathfrak{p}} = W_{\mathfrak{p}} + M[\mathfrak{a}]_{\mathfrak{p}},$$

where $M[\mathfrak{a}]_{\mathfrak{p}} = M_{\mathfrak{p}}[\mathfrak{a}_{\mathfrak{p}}]$ by Lemma 3.1.

Since we proved the principal case, and $\mathfrak{a}_{\mathfrak{p}}$ is principal, we have

$$\mathfrak{a}_{\mathfrak{p}}W_{\mathfrak{p}} :_{M_{\mathfrak{p}}} \mathfrak{a}_{\mathfrak{p}} = W_{\mathfrak{p}} + M_{\mathfrak{p}}[\mathfrak{a}_{\mathfrak{p}}].$$

It follows that for every prime $\mathfrak{p}$ of $\mathcal{O}$ we have

$$(\mathfrak{a} \cdot W : \mathfrak{a})_{\mathfrak{p}} = (W + M[\mathfrak{a}])_{\mathfrak{p}}.$$

Hence $\mathfrak{a}W : \mathfrak{a} = W + M[\mathfrak{a}]$, which proves (a).

For (b), let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$, and observe that $(\mathfrak{a}(W : \mathfrak{a}))_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}(W_{\mathfrak{p}} : \mathfrak{a}_{\mathfrak{p}})$. As $\mathfrak{a}_{\mathfrak{p}}$ is principal, it follows that $\mathfrak{a}_{\mathfrak{p}}(W_{\mathfrak{p}} : \mathfrak{a}_{\mathfrak{p}}) = W_{\mathfrak{p}}$. As this holds for every prime $\mathfrak{p}$ of $\mathcal{O}$, we conclude that $\mathfrak{a}(W : \mathfrak{a}) = W$. ■

Proposition 3.4. *Let $\mathfrak{a} \subset \mathcal{O}$ be an invertible ideal, and suppose that the module M satisfies $M = \mathfrak{a}M$. Let W and V be $\mathcal{O}$-submodules of M. Then*

$$(W + V) : \mathfrak{a} = (W : \mathfrak{a}) + (V : \mathfrak{a}).$$

Proof. First, let $x \in W : \mathfrak{a}$ and $y \in V : \mathfrak{a}$ and note that

$$\mathfrak{a}(x + y) \subset \mathfrak{a}x + \mathfrak{a}y \subset W + V,$$

so that

$$x + y \in (W + V) : \mathfrak{a}.$$

This proves the right to left inclusion. To show the reverse inclusion, we first suppose that $\mathfrak{a} = (a)$ is principal.

Let $x \in (W + V) : a$. Then $ax = y + z$ for some $y \in W$ and $z \in V$. As $M = aM$ we have $y = au$ for some $u \in M$. Since $au = y \in W$, we have $u \in W : a$. On the other hand, the identity

$$ax = y + z = au + z$$

implies that

$$a(x - u) = z.$$

As $z \in V$, it follows that $x - u \in V : a$. Then

$$x = u + (x - u) \in (W : a) + (V : a),$$

which proves the statement for principal ideals $\mathfrak{a}$.

Now, suppose $\mathfrak{a}$ is any invertible ideal, and let $\mathfrak{p}$ be a prime of $\mathcal{O}$. By Lemma 3.1 we have

$$((W+V)\colon\mathfrak{a})_{\mathfrak{p}} = (W+V)_{\mathfrak{p}}\colon\mathfrak{a}_{\mathfrak{p}}.$$

By exactness of localisation, we have $(W+V)_{\mathfrak{p}} = W_{\mathfrak{p}} + V_{\mathfrak{p}}$. As $\mathfrak{a}_{\mathfrak{p}}$ is principal, we have

$$(W_{\mathfrak{p}}+V_{\mathfrak{p}})\colon\mathfrak{a}_{\mathfrak{p}} \subset (W_{\mathfrak{p}}\colon\mathfrak{a}_{\mathfrak{p}}) + (V_{\mathfrak{p}}\colon\mathfrak{a}_{\mathfrak{p}}) = (W\colon\mathfrak{a})_{\mathfrak{p}} + (V\colon\mathfrak{a})_{\mathfrak{p}} = ((W\colon\mathfrak{a}) + (V\colon\mathfrak{a}))_{\mathfrak{p}}.$$

Hence $(W+V)\colon\mathfrak{a} \subset (W\colon\mathfrak{a}) + (V\colon\mathfrak{a})$, which proves the proposition. ■

3. Dividing points on elliptic curves

Throughout this section, let K be a field of characteristic 0, let $\overline{K}$ be an algebraic closure of K, let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, and let F be the fraction field of $\mathcal{O}$. In this chapter, for an ideal $\mathfrak{a}$ of $\mathcal{O}$ and W an $\mathcal{O}$-submodule of $E(\overline{K})$, the module of $\mathfrak{a}$-division points $W\colon\mathfrak{a}$ of W, defined in the previous section, is taken inside $M = E(\overline{K})$. For any field extension L of K and nonzero ideal $\mathfrak{a} \subset \mathcal{O}$, we write $E(L)[\mathfrak{a}]$ for the module of $\mathfrak{a}$-torsion points of the $\mathcal{O}$-module $E(L)$, and $E(L)_{\mathrm{tor}}$ for the $\mathcal{O}$-module of all torsion points of E over L. For simplicity, we write $E[\mathfrak{a}]$ for $E(\overline{K})[\mathfrak{a}]$, and E_{tor} for $E(\overline{K})_{\mathrm{tor}}$.

Definition 3.5. Let $\widehat{\mathcal{O}} = \varprojlim_{\mathfrak{b}} \mathcal{O}/\mathfrak{b}$, where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$, be the profinite completion of $\mathcal{O}$ as a ring. A *Steinitz ideal* $\mathfrak{a}$ of $\mathcal{O}$ is a closed ideal of $\widehat{\mathcal{O}}$. One easily checks that the set of open ideals of $\widehat{\mathcal{O}}$ is in bijection with the set of nonzero ideals of $\mathcal{O}$. Therefore, we often identify an open Steinitz ideal with the ideal it corresponds to in $\mathcal{O}$.

Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. For an $\mathcal{O}$-submodule W of $E(\overline{K})$, we define

$$W\colon\mathfrak{a} = \bigcup_{\mathfrak{b}} (W\colon\mathfrak{b}),$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. Consistently with our notation for ideals of $\mathcal{O}$, we write $E[\mathfrak{a}]$ for the $\mathfrak{a}$-torsion $0 \colon \mathfrak{a} = \bigcup_{\mathfrak{b}} E[\mathfrak{b}]$, where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. Note that both $W \colon \mathfrak{a}$ and $E[\mathfrak{a}]$ are $\mathcal{O}$-modules. In fact, the canonical module structure of $\mathcal{O}$ on E_{tor} extends naturally to a module structure of $\widehat{\mathcal{O}}$ on E_{tor}. Then the $\widehat{\mathcal{O}}$-module $E[\mathfrak{a}]$ is canonically an $\widehat{\mathcal{O}}/\mathfrak{a}$-module.

Remark 3.6. For a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$, there is a unique factorization of $\mathfrak{a}$ into prime ideals of $\mathcal{O}$. The same can be done for Steinitz ideals. Indeed, an ideal of a product $\prod_{i \in I} R_i$ of topological Hausdorff rings R_i is closed if and only if it is of the form $\prod_{i \in I} J_i$, where J_i is a closed ideal of R_i for each $i \in I$. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, let

$$\mathrm{v}_{\mathfrak{p}} \colon F \longrightarrow \mathbf{Z} \cup \{\infty\}$$

be the $\mathfrak{p}$-adic valuation, and let $\mathcal{O}_{\mathfrak{p}}$ be the completion of $\mathcal{O}$ at $\mathfrak{p}$. The nonzero ideals of $\mathcal{O}_{\mathfrak{p}}$ are powers of the maximal ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ and closed. Now, observe that

$$\widehat{\mathcal{O}} = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$$

as profinite rings. Hence, putting $\mathfrak{p}^{\infty}\mathcal{O}_{\mathfrak{p}} = \{0\}\mathcal{O}_{\mathfrak{p}}$, we may represent a Steinitz ideal $\mathfrak{a}$ uniquely as

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})} \mathcal{O}_{\mathfrak{p}}.$$

For simplicity, we often leave out $\mathcal{O}_{\mathfrak{p}}$ from the notation.

For a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$, we write $\mathfrak{a}^{\infty}$ for the ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\infty}\mathcal{O}_{\mathfrak{p}} \times \prod_{\mathfrak{p}'} \mathcal{O}_{\mathfrak{p}'} \subset \widehat{\mathcal{O}} = \prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}},$$

where $\mathfrak{p}$ runs over the maximal ideals of $\mathcal{O}$ dividing $\mathfrak{a}$, and $\mathfrak{p}'$ runs over the other maximal ideals of $\mathcal{O}$, and $\mathfrak{q}$ runs over all maximal ideals of $\mathcal{O}$.

Note that for any $\mathcal{O}$-submodule $W \subset E(\overline{K})$ and Steinitz ideal $\mathfrak{a}$ of $\mathcal{O}$, the module $E[\mathfrak{a}]$ is contained in $W : \mathfrak{a}$, and $K(W : \mathfrak{a})$ is Galois over $K(W)$.

Let W be a finitely generated $\mathcal{O}$-submodule of $E(K)$ and let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. The field $K(W : \mathfrak{a})$ is Galois over K, and any field automorphism of $K(W : \mathfrak{a})$ over K is determined by its action on $W : \mathfrak{a}$. Moreover, the action of $\mathcal{O}$ on $W : \mathfrak{a}$ commutes with the action of Galois. Hence, we may identify $\mathrm{Gal}(K(W : \mathfrak{a})/K)$ with a subgroup of the group of $\mathcal{O}$-automorphisms $\mathrm{Aut}_{\mathcal{O},W}(W : \mathfrak{a})$ of $W : \mathfrak{a}$ that are the identity on W. Note that $\mathrm{Aut}_{\mathcal{O},W}(W : \mathfrak{a})$ is the profinite group

$$\varprojlim_{\mathfrak{b}} \mathrm{Aut}_{\mathcal{O},W}(W : \mathfrak{b}),$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. As $\mathrm{Gal}(K(W : \mathfrak{a})/K)$ is compact and $\mathrm{Aut}_{\mathcal{O},W}(W : \mathfrak{a})$ is Hausdorff, the subgroup $\mathrm{Gal}(K(W : \mathfrak{a})/K)$ of $\mathrm{Aut}_{\mathcal{O},W}(W : \mathfrak{a})$ is closed.

Endow $F/\mathcal{O}$ with the canonical $\mathcal{O}$-module structure, and note that this structure naturally extends to an $\widehat{\mathcal{O}}$-module structure.

Proposition 3.7. *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then the following statements hold.*

(a) $E[\mathfrak{a}] \cong_{\mathcal{O}} (F/\mathcal{O})[\mathfrak{a}] = \{x \in F/\mathcal{O} : \mathfrak{a}x = 0\}$ *and* $E_{\mathrm{tor}} \cong_{\mathcal{O}} F/\mathcal{O}$.

(b) $\mathrm{End}_{\mathcal{O}}(E[\mathfrak{a}]) \cong_{\mathcal{O}} \widehat{\mathcal{O}}/\mathfrak{a}$ *as $\mathcal{O}$-algebras, and for a Steinitz ideal $\mathfrak{a}'$ of $\mathcal{O}$ divisible by $\mathfrak{a}$ the restriction map* $\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}']) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}])$ *is surjective.*

(c) *The field $K(E[\mathfrak{a}])$ is abelian over K.*

Proof. The second statement of (a) follows from Theorem 3 in [Len96]. The first statement follows directly from the second one, since $\mathcal{O}$-module isomorphisms respect the $\mathcal{O}$-torsion. This finishes the proof of (a).

For the first statement of (b), let $\mathfrak{b}$ a nonzero ideal of $\mathcal{O}$ dividing $\mathfrak{a}$. One easily sees that $(F/\mathcal{O})[\mathfrak{b}] \cong_{\mathcal{O}} \mathcal{O}/\mathfrak{b}$ as $\mathcal{O}$-modules, and $\mathrm{End}_{\mathcal{O}}(\mathcal{O}/\mathfrak{b}) \cong_{\mathcal{O}} \mathcal{O}/\mathfrak{b}$ as $\mathcal{O}$-algebras. Then (a) implies

$$\mathrm{End}_{\mathcal{O}}(E[\mathfrak{b}]) \cong_{\mathcal{O}} \mathrm{End}_{\mathcal{O}}((F/\mathcal{O})[\mathfrak{b}]) \cong_{\mathcal{O}} \mathrm{End}_{\mathcal{O}}(\mathcal{O}/\mathfrak{b}) \cong_{\mathcal{O}} \mathcal{O}/\mathfrak{b}$$

as $\mathcal{O}$-algebras. Using $E[\mathfrak{a}] = \varinjlim_{\mathfrak{b}} E[\mathfrak{b}]$, where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$, we obtain

$$\mathrm{End}_{\mathcal{O}}(E[\mathfrak{a}]) = \mathrm{End}_{\mathcal{O}}(\varinjlim_{\mathfrak{b}} E[\mathfrak{b}]) \cong_{\mathcal{O}} \varprojlim_{\mathfrak{b}} \mathrm{End}_{\mathcal{O}}(E[\mathfrak{b}]) \cong_{\mathcal{O}} \varprojlim_{\mathfrak{b}} \mathcal{O}/\mathfrak{b} \cong_{\mathcal{O}} \widehat{\mathcal{O}}/\mathfrak{a},$$

as $\mathcal{O}$-algebras. This proves the first statement of (b).

For the second part, we first prove the statement for $\mathfrak{a}' = \prod_{\mathfrak{p}} \mathfrak{p}^{\infty}$ where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$. Then we have $E[\mathfrak{a}'] = E_{\mathrm{tor}}$ and $\widehat{\mathcal{O}}/\mathfrak{a}' = \widehat{\mathcal{O}}$. The above implies that there are canonical isomorphisms

$$\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}}) \longrightarrow \widehat{\mathcal{O}}^*$$

and

$$\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}]) \longrightarrow (\widehat{\mathcal{O}}/\mathfrak{a})^*$$

which make the diagram

$$\begin{tikzcd}
\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}}) \arrow[r] \arrow[d] & \widehat{\mathcal{O}}^* \arrow[d] \\
\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}]) \arrow[r] & (\widehat{\mathcal{O}}/\mathfrak{a})^*
\end{tikzcd} \tag{$*$}$$

commutative, where the vertical arrows are the restriction maps. Moreover, using the identity $\widehat{\mathcal{O}} \cong \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$, one easily checks that the diagram

$$\begin{tikzcd}
\widehat{\mathcal{O}}^* \arrow[r, "\cong"] \arrow[d] & \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^* \arrow[d] \\
(\widehat{\mathcal{O}}/\mathfrak{a})^* \arrow[r, "\cong"'] & \prod_{\mathfrak{p}} (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})})^*
\end{tikzcd} \tag{$**$}$$

is commutative, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$, and $\mathfrak{p}^{\infty}$ equals the zero ideal of $\mathcal{O}_{\mathfrak{p}}$. Since $\mathcal{O}_{\mathfrak{p}}$ is a local ring, the map $\mathcal{O}_{\mathfrak{p}}^* \longrightarrow (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})})^*$ is surjective. By commutativity of $(**)$, we have that $\widehat{\mathcal{O}}^* \longrightarrow (\widehat{\mathcal{O}}/\mathfrak{a})^*$ is surjective. Then commutativity of $(*)$ implies that $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}}) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}])$ is surjective, as desired.

Now, the case for general $\mathfrak{a}'$ follows directly from the fact that $\widehat{\mathcal{O}}^* \longrightarrow (\widehat{\mathcal{O}}/\mathfrak{a})^*$ factors via $\widehat{\mathcal{O}}^* \longrightarrow (\widehat{\mathcal{O}}/\mathfrak{a}')^*$.

For (c), note that $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$ is a subgroup of $\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}])$. By (b) we have

$$\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}]) = \mathrm{End}_{\mathcal{O}}(E[\mathfrak{a}])^* \cong (\widehat{\mathcal{O}}/\mathfrak{a})^*.$$

As the last group is clearly abelian, the subgroup $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$ is abelian also, so that $K(E[\mathfrak{a}])$ is abelian over K. ■

For a module N over a ring R, we write $\mathrm{Ann}_R(N) = \{r \in R : \forall x \in N : rx = 0\}$ for the annihilator ideal of N.

Proposition 3.8. (a) *There is an inclusion-reversing bijection*

$$\psi\colon \{\text{Steinitz ideals of } \mathcal{O}\} \longrightarrow \{\mathcal{O}\text{-submodules of } E_{\mathrm{tor}}\}$$

of sets, given by sending a Steinitz ideal $\mathfrak{a}$ to $E[\mathfrak{a}]$. Moreover, its inverse is also inclusion-reversing, sending an $\mathcal{O}$-submodule M of E_{tor} to the $\widehat{\mathcal{O}}$-annihilator

$$\mathrm{Ann}_{\widehat{\mathcal{O}}}(M) = \{r \in \widehat{\mathcal{O}} : r \cdot M = 0\}$$

of M.

(b) *Let $\mathfrak{a}$ and $\mathfrak{a}'$ be Steinitz ideals of $\mathcal{O}$. Then $\mathfrak{a} = \mathrm{Ann}_{\widehat{\mathcal{O}}}(E(K)[\mathfrak{a}'])$ if and only if $E[\mathfrak{a}] = E(K)[\mathfrak{a}']$.*

Proof. For (a), define the map

$$\varphi\colon \{\text{Steinitz ideals of } \mathcal{O}\} \longrightarrow \{\mathcal{O}\text{-submodules of } F/\mathcal{O}\},$$

by sending the Steinitz ideal $\mathfrak{a}$ to $(F/\mathcal{O})[\mathfrak{a}] = \{x \in F/\mathcal{O} : \mathfrak{a} \cdot x = 0\}$. We will show that φ is a bijection.

For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ we write $\mathfrak{a}^{-1}$ for its *ideal inverse*

$$\mathcal{O} :_F \mathfrak{a} = \{x \in F : \mathfrak{a} \cdot x \subset \mathcal{O}\}.$$

As $\mathcal{O}$ is Dedekind, there is a bijection of the set of nonzero ideals of $\mathcal{O}$ with the set of fractional ideals of $\mathcal{O}$ containing $\mathcal{O}$ given by the ideal inverse. Moreover, one easily checks that the map from the set of finite $\mathcal{O}$-submodules of $F/\mathcal{O}$ to the set of fractional ideals of $\mathcal{O}$ containing $\mathcal{O}$ defined by sending $M \subset F/\mathcal{O}$ to the fractional ideal $\operatorname{Ann}_{\mathcal{O}}(M)^{-1}$ is a bijection, and its inverse sends a fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ containing $\mathcal{O}$ to $\mathfrak{a}/\mathcal{O}$. Composing the above two bijections, we obtain another bijection, which is in fact the restriction of φ to the subset of open Steinitz ideals of $\mathcal{O}$. Thus φ restricts to a bijection of the subset of open Steinitz ideals of $\mathcal{O}$ with the subset of finite $\mathcal{O}$-submodules of $F/\mathcal{O}$.

Now, let $\mathfrak{a}$ be a Steinitz ideal, and note that

$$(F/\mathcal{O})[\mathfrak{a}] = \bigcup_{\mathfrak{b}} (F/\mathcal{O})[\mathfrak{b}] = \bigcup_{\mathfrak{b}} \mathfrak{b}^{-1}/\mathcal{O},$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. Then

$$\operatorname{Ann}_{\widehat{\mathcal{O}}}((F/\mathcal{O})[\mathfrak{a}]) = \operatorname{Ann}_{\widehat{\mathcal{O}}}\left(\bigcup_{\mathfrak{b}} \mathfrak{b}^{-1}/\mathcal{O}\right) = \bigcap_{\mathfrak{b}} \operatorname{Ann}_{\widehat{\mathcal{O}}}(\mathfrak{b}^{-1}/\mathcal{O}) = \bigcap_{\mathfrak{b}} \mathfrak{b}\widehat{\mathcal{O}} = \mathfrak{a}.$$

Conversely, let M be an $\mathcal{O}$-submodule of $F/\mathcal{O}$. One easily checks that

$$M = \sum_{\mathfrak{p}} \mathfrak{p}^{-e(\mathfrak{p})}/\mathcal{O},$$

where $\mathfrak{p}$ runs over the maximal ideals of $\mathcal{O}$, and $e(\mathfrak{p}) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$, and $\mathfrak{p}^{-\infty} = \bigcup_{i \geq 0} \mathfrak{p}^{-i}$. Hence, we have

$$\operatorname{Ann}_{\widehat{\mathcal{O}}}(M) = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}\mathcal{O}_{\mathfrak{p}},$$

where $\mathfrak{p}$ runs over the maximal ideals of $\mathcal{O}$. Then one easily sees that

$$(F/\mathcal{O})\big[\operatorname{Ann}_{\widehat{\mathcal{O}}}(M)\big] = \sum_{\mathfrak{p}} \mathfrak{p}^{-e(\mathfrak{p})}/\mathcal{O},$$

where $\mathfrak{p}$ runs over the maximal ideals of $\mathcal{O}$, which shows that φ is a bijection.

By Proposition 3.7(a) there is an isomorphism $f\colon E_{\mathrm{tor}} \longrightarrow F/\mathcal{O}$ of $\mathcal{O}$-modules. This induces a bijection

$$\{\mathcal{O}\text{-submodules of } F/\mathcal{O}\} \longrightarrow \{\mathcal{O}\text{-submodules of } E_{\mathrm{tor}}\},$$

which composed with φ gives us ψ, independent of the choice of the isomorphism f. As φ is a bijection, it follows that ψ is a bijection. One easily checks that ψ and its inverse are inclusion-reversing, which finishes the proof of (a).

For (b), let $\mathfrak{a}$ and $\mathfrak{a}'$ be Steinitz ideals of $\mathcal{O}$. Observe that for an $\mathcal{O}$-submodule M of E_{tor}, part (a) implies that

$$\mathfrak{a} = \psi^{-1}(M) \Leftrightarrow \psi(\mathfrak{a}) = M.$$

Hence

$$\mathfrak{a} = \operatorname{Ann}_{\widehat{\mathcal{O}}}(E(K)[\mathfrak{a}']) = \psi^{-1}(E(K)[\mathfrak{a}']) \Leftrightarrow E[\mathfrak{a}] = \psi(\mathfrak{a}) = E(K)[\mathfrak{a}'],$$

as desired. ∎

4. Abelian division fields

Throughout this section let K be a field of characteristic 0, let $\overline{K}$ be an algebraic closure of K, let K^{ab} be the maximal abelian extension of K contained in $\overline{K}$, let E be an elliptic curve over K with $\mathcal{O} = \operatorname{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, let F be the fraction field of $\mathcal{O}$, let $\widehat{\mathcal{O}}$ be as in Definition 3.5, and let $W \subset E(K)$ be an $\mathcal{O}$-submodule.

In this section we prove the following theorem.

Theorem 3.9. *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$, and let $\mathfrak{w} = \operatorname{Ann}_{\widehat{\mathcal{O}}}(E(K)_{\mathrm{tor}})$. Then*

$$(E(K)\colon \mathfrak{a})^{\operatorname{Gal}(\overline{K}/K^{\mathrm{ab}})} = (E(K)\colon (\mathfrak{w} + \mathfrak{a})) + E[\mathfrak{w}\mathfrak{a}].$$

To prove this theorem, we first prove the following analogue of Schinzel's theorem (see Theorem 1.1) for elliptic curves with complex multiplication.

Theorem 3.10. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Then $K(W\colon \mathfrak{a})$ is abelian over K if and only if $\operatorname{Ann}_{\mathcal{O}}(E(K)[\mathfrak{a}]) \cdot W \subset \mathfrak{a} \cdot E(K)$.*

Remark 3.11. In the rest of this section, we write $\mathfrak{w} = \operatorname{Ann}_{\widehat{\mathcal{O}}}(E(K)_{\mathrm{tor}})$, and for a Steinitz ideal $\mathfrak{a}$ we write $w_{\mathfrak{a}} = \mathfrak{w} + \mathfrak{a}$. By Proposition 3.8(a) we have for a Steinitz ideal $\mathfrak{a}$ and an $\mathcal{O}$-submodule M of E_{tor} the equivalence

$$\mathfrak{a} = \operatorname{Ann}_{\widehat{\mathcal{O}}}(M) \Leftrightarrow E[\mathfrak{a}] = M.$$

Therefore, we have $E[\mathfrak{w}] = E(K)_{\mathrm{tor}}$. Moreover, we have

$$E[w_{\mathfrak{a}}] = E[\mathfrak{w} + \mathfrak{a}] = E[\mathfrak{w}][\mathfrak{a}] = E(K)_{\mathrm{tor}}[\mathfrak{a}] = E(K)[\mathfrak{a}],$$

so Proposition 3.8(b) implies

$$w_{\mathfrak{a}} = \operatorname{Ann}_{\widehat{\mathcal{O}}}(E(K)[\mathfrak{a}]).$$

Proposition 3.12. *The field $K(E(K)\colon \mathfrak{w})$ is abelian over K.*

Proof. By Remark 3.11 we have $E[\mathfrak{w}] = E(K)_{\mathrm{tor}}$.

Now, let

$$\varphi\colon\ \operatorname{Gal}(K(E(K)\colon \mathfrak{w})/K) \longrightarrow \operatorname{Hom}((E(K)\colon \mathfrak{w})/E(K), E[\mathfrak{w}])$$

be the map defined by

$$\sigma \mapsto [Q + E(K) \mapsto \sigma(Q) - Q].$$

As $E[\mathfrak{w}] \subset E(K)$, the map φ is a group morphism. A field automorphism of $K(E(K)\colon\mathfrak{w})$ over K is determined by its action on $E(K)\colon\mathfrak{w}$. Hence φ is injective. As the codomain is clearly abelian, it follows that $\mathrm{Gal}(K(E(K)\colon\mathfrak{w})/K)$ is abelian. ■

Proof of Theorem 3.10. We first prove the 'if' part. To this end, recall by Remark 3.11 that $w_{\mathfrak{a}} = \mathfrak{w} + \mathfrak{a} = \mathrm{Ann}_{\widehat{\mathcal{O}}}(E(K)[\mathfrak{a}])$. Suppose that $w_{\mathfrak{a}} \cdot W \subset \mathfrak{a} \cdot E(K)$. We will prove that $K(W : \mathfrak{a})$ is abelian over K. To this end, let $Q \in W : \mathfrak{a}$, and note that

$$\mathfrak{a} w_{\mathfrak{a}} Q \subset \mathfrak{a} E(K).$$

Then Proposition 3.3(a) implies $w_{\mathfrak{a}} Q \subset E(K) + E[\mathfrak{a}]$. Since $\mathfrak{a}$ is an ideal of $\mathcal{O}$, the ideal $w_{\mathfrak{a}}$ is open and we may consider it as an ideal of $\mathcal{O}$. Then Proposition 3.4 implies

$$Q \in (E(K)\colon w_{\mathfrak{a}}) + E[\mathfrak{a}]\colon w_{\mathfrak{a}},$$

where $E[\mathfrak{a}]\colon w_{\mathfrak{a}} = E[\mathfrak{a} w_{\mathfrak{a}}]$. By Proposition 3.7(c) we know that $K(E_{\text{tor}})$ is abelian over K, so in particular $K(E[\mathfrak{a} w_{\mathfrak{a}}])$ is abelian over K. On the other hand, by Proposition 3.12 we know that $K(E(K)\colon w_{\mathfrak{a}})$ is abelian over K. It follows that $K((E(K)\colon w_{\mathfrak{a}}) + E[\mathfrak{a} w_{\mathfrak{a}}])$ is abelian over K, so that $K(Q)$ is abelian over K. We conclude that $K(W : \mathfrak{a})$ is abelian over K.

Now, we prove the 'only if' part. Suppose that $K(W : \mathfrak{a})$ is abelian over K. We will show that $w_{\mathfrak{a}} \cdot W \subset \mathfrak{a} \cdot E(K)$. To this end, suppose first that $\mathfrak{a} = (a)$ is principal. Let $P \in W$, and recall that we write $P\colon a$ instead of $(\mathcal{O} \cdot P) : \mathfrak{a}$. As $P\colon a \subset W : a$ and $K(W : a)$ is abelian over K, the field $K(P\colon a)$ is abelian over K. Write G for its Galois group $\mathrm{Gal}(K(P\colon a)/K)$, and let $Q \in P\colon a$ be such that $aQ = P$.

The natural $\mathcal{O}$-module structure and G-module structure on $E[a]$ are compatible with each other, so $E[a]$ is an $\mathcal{O}[G]$-module. By Proposition 3.7(b) we have

$$\mathrm{End}_{\mathcal{O}}(E[a]) \cong \mathcal{O}/a\mathcal{O}.$$

It follows that for every $\sigma \in G$ we can choose $\mathrm{c}(\sigma) \in \mathcal{O}$ such that σ acts on $E[a]$ by multiplication with $\mathrm{c}(\sigma)$. We fix such $\mathrm{c}(\sigma) \in \mathcal{O}$. Now, for every $\sigma \in G$ we have

$$a\sigma(Q) = \sigma(P) = P = aQ.$$

Therefore, for every $\sigma \in G$ there is $T_\sigma \in E[a]$ such that $\sigma(Q) = Q + T_\sigma$. Let $\sigma, \tau \in G$, and observe that

$$\tau\sigma(Q) - \sigma(Q) = \sigma\tau(Q) - \sigma(Q) = \sigma(Q) + \sigma(T_\tau) - \sigma(Q) = \mathrm{c}(\sigma)T_\tau.$$

Moreover, we have

$$\mathrm{c}(\sigma)T_\tau = \mathrm{c}(\sigma)Q + \mathrm{c}(\sigma)T_\tau - \mathrm{c}(\sigma)Q = \mathrm{c}(\sigma)\tau(Q) - \mathrm{c}(\sigma)Q = \tau(\mathrm{c}(\sigma)Q) - \mathrm{c}(\sigma)Q.$$

Thus, we have $\tau\sigma(Q) - \sigma(Q) = \tau(\mathrm{c}(\sigma)Q) - \mathrm{c}(\sigma)Q$, which is equivalent to

$$\tau(\mathrm{c}(\sigma)Q - \sigma(Q)) = \mathrm{c}(\sigma)Q - \sigma(Q).$$

As the latter holds for all $\sigma, \tau \in G$, we conclude that

$$\mathrm{c}(\sigma)Q - \sigma(Q) \in E(K)$$

for all $\sigma \in G$. Multiplying by a on both sides, we obtain

$$(\mathrm{c}(\sigma) - 1) \cdot P \in aE(K),$$

for all $\sigma \in G$. Let

$$\mathfrak{d} = (a) + \sum_{\sigma \in G} (\mathrm{c}(\sigma) - 1)\mathcal{O},$$

and note that

$$\mathfrak{d} \cdot P \subset (a) \cdot E(K).$$

We will now show that $\mathfrak{d} = \mathrm{Ann}_{\mathcal{O}}(E(K)[a])$. To this end, observe that Proposition 3.8 implies that $\mathfrak{d} = \mathrm{Ann}_{\mathcal{O}}(E(K)[a])$ if and only if $E[\mathfrak{d}] = E(K)[a]$. Note that $a \in \mathfrak{d}$, so $E[\mathfrak{d}] \subset E[a]$. Let $T \in E[a]$, and observe that

$$T \in E(K)[a] \Leftrightarrow \forall \sigma \in G : \sigma(T) = T \Leftrightarrow \forall \sigma \in G : (\mathrm{c}(\sigma) - 1)T = 0 \Leftrightarrow T \in E[\mathfrak{d}],$$

that is, we have $E[\mathfrak{d}] = E(K)[a]$. Hence $\mathfrak{d} = \mathrm{Ann}_{\mathcal{O}}(E(K)[a])$.

Now, we have shown that for every $P \in W$ we have

$$\mathrm{Ann}_{\mathcal{O}}(E(K)[a]) \cdot P \subset (a) \cdot E(K),$$

which implies that

$$\mathrm{Ann}_{\mathcal{O}}(E(K)[a]) \cdot W \subset (a) \cdot E(K).$$

This proves the statement for principal ideals $\mathfrak{a}$.

Now, suppose $\mathfrak{a}$ is any nonzero ideal. We will show that $w_{\mathfrak{a}} W \subset \mathfrak{a}E(K)$. Since $\mathcal{O}$ is Dedekind, there is an ideal $\mathfrak{b}$ of $\mathcal{O}$ such that $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$ and $\mathfrak{a}\mathfrak{b}$ is principal. Moreover, by Proposition 3.2 we have

$$\mathfrak{b}W : \mathfrak{a}\mathfrak{b} = \mathfrak{b}W : \mathfrak{a} + \mathfrak{b}W : \mathfrak{b},$$

and

$$\mathfrak{b}W : \mathfrak{b} = W + E[\mathfrak{b}]$$

by Proposition 3.3(a). As $E[\mathfrak{b}]$ is abelian over K, and by assumption, the field $K(W : \mathfrak{a})$ is abelian over K, the field $K(\mathfrak{b}W : \mathfrak{a}\mathfrak{b}) = K((\mathfrak{b}W : \mathfrak{a}) + E[\mathfrak{b}])$ contained in $K((W : \mathfrak{a}) + E[\mathfrak{b}])$ is abelian over K. Then, because $\mathfrak{a}\mathfrak{b}$ is principal, the above proof for principal ideals shows that $w_{\mathfrak{a}\mathfrak{b}} \cdot \mathfrak{b}W \subset \mathfrak{a}\mathfrak{b}E(K)$.

By Remark 3.11 we have $E[w_{\mathfrak{a}}] = E(K)[\mathfrak{a}]$ and $E[w_{\mathfrak{a}\mathfrak{b}}] = E(K)[\mathfrak{a}\mathfrak{b}]$. Moreover, we have

$$E[w_{\mathfrak{a}\mathfrak{b}} + \mathfrak{a}] = E[w_{\mathfrak{a}\mathfrak{b}}] \cap E[\mathfrak{a}] = E(K)[\mathfrak{a}\mathfrak{b}] \cap E[\mathfrak{a}] = E(K)[\mathfrak{a}] = E[w_{\mathfrak{a}}].$$

Thus $w_{\mathfrak{ab}} + \mathfrak{a} = w_{\mathfrak{a}}$ by Proposition 3.8.

Recall from the above that $w_{\mathfrak{ab}}\mathfrak{b}W \subset \mathfrak{ab}E(K)$, so that

$$w_{\mathfrak{a}} \cdot \mathfrak{b}W = (w_{\mathfrak{ab}} + \mathfrak{a}) \cdot \mathfrak{b}W = w_{\mathfrak{ab}}\mathfrak{b}W + \mathfrak{ab}W \subset \mathfrak{ab}E(K),$$

where we used that $\mathfrak{ab}W \subset \mathfrak{ab}E(K)$. As $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$, we have

$$w_{\mathfrak{a}}W = w_{\mathfrak{a}}(\mathfrak{a} + \mathfrak{b})W = w_{\mathfrak{a}}\mathfrak{a}W + w_{\mathfrak{a}}\mathfrak{b}W.$$

Moreover $w_{\mathfrak{a}}\mathfrak{a}W \subset w_{\mathfrak{a}}\mathfrak{a}E(K) \subset \mathfrak{a}E(K)$, and $w_{\mathfrak{a}}\mathfrak{b}W \subset \mathfrak{ab}E(K) \subset \mathfrak{a}E(K)$. Hence, we have

$$w_{\mathfrak{a}}W = w_{\mathfrak{a}}\mathfrak{a}W + w_{\mathfrak{a}}\mathfrak{b}W \subset \mathfrak{a}E(K) + \mathfrak{a}E(K) \subset \mathfrak{a}E(K),$$

as desired. ■

Proof of Theorem 3.9. We first prove the right to left inclusion. By Proposition 3.12 and Proposition 3.7(c), we have

$$(E(K)\colon \mathfrak{w}) + E_{\text{tor}} \subset E(K^{\text{ab}}).$$

By Remark 3.11 we have

$$E[\mathfrak{w}] = E(K)_{\text{tor}} \subset E(K),$$

so that $(E(K)\colon (\mathfrak{w}+\mathfrak{a})) + E[\mathfrak{wa}]$ is contained in $E(K)\colon \mathfrak{a}$ and in $(E(K)\colon \mathfrak{w}) + E_{\text{tor}}$. Therefore, we have

$$(E(K)\colon (\mathfrak{w} + \mathfrak{a})) + E[\mathfrak{wa}] \subset (E(K)\colon \mathfrak{a}) \cap E(K^{\text{ab}}) = (E(K)\colon \mathfrak{a})^{\text{Gal}(\overline{K}/K^{\text{ab}})},$$

which proves the right to left inclusion.

We prove the other inclusion in two steps. First, we prove the inclusion for $\mathfrak{a}$ a nonzero ideal of $\mathcal{O}$. To this end, let

$$X = (E(K)\colon \mathfrak{a})^{\text{Gal}(\overline{K}/K^{\text{ab}})}.$$

As $E[\mathfrak{a}] \subset X$, Proposition 3.3(a) implies that

$$\mathfrak{a}X : \mathfrak{a} = X + E[\mathfrak{a}] = X.$$

Moreover, it is clear that $\mathfrak{a}X \subset E(K)$ is an $\mathcal{O}$-submodule. Now, as $K(\mathfrak{a}X : \mathfrak{a}) = K(X)$ is abelian over K, Theorem 3.10 implies that

$$w_{\mathfrak{a}} \cdot (\mathfrak{a}X) \subset \mathfrak{a}E(K),$$

where $w_{\mathfrak{a}} = \mathfrak{w} + \mathfrak{a}$ (see Remark 3.11). It follows that

$$w_{\mathfrak{a}} \cdot X \subset \mathfrak{a}E(K) : \mathfrak{a} = E(K) + E[\mathfrak{a}],$$

where the equality follows from Proposition 3.3(a). Thus

$$X \subset (E(K) + E[\mathfrak{a}]) : w_{\mathfrak{a}} = (E(K) : w_{\mathfrak{a}}) + (E[\mathfrak{a}] : w_{\mathfrak{a}}),$$

where the equality follows from Proposition 3.4. Observe that

$$E[\mathfrak{a}] : w_{\mathfrak{a}} = E[\mathfrak{a}w_{\mathfrak{a}}] \subset E[\mathfrak{a}\mathfrak{w}].$$

Hence, we have

$$X \subset (E(K) : (\mathfrak{w} + \mathfrak{a})) + E[\mathfrak{a}\mathfrak{w}],$$

as desired.

Now, suppose $\mathfrak{a}$ is any Steinitz ideal, and note that

$$\begin{aligned} (E(K) : \mathfrak{a})^{\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})} &= \bigcup_{\mathfrak{b}} (E(K) : \mathfrak{b})^{\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})} \\ &\subset \bigcup_{\mathfrak{b}} ((E(K) : (\mathfrak{w} + \mathfrak{b})) + E[\mathfrak{b}\mathfrak{w}]) \\ &= \bigcup_{\mathfrak{b}} (E(K) : (\mathfrak{w} + \mathfrak{b})) + \bigcup_{\mathfrak{b}} E[\mathfrak{b}\mathfrak{w}], \end{aligned}$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. At last,

$$\bigcup_{\mathfrak{b}}(E(K)\colon(\mathfrak{w}+\mathfrak{b}))\subset E(K)\colon(\mathfrak{w}+\mathfrak{a})$$

and $\bigcup_{\mathfrak{b}} E[\mathfrak{b}\mathfrak{w}] \subset E[\mathfrak{a}\mathfrak{w}]$, so that

$$(E(K)\colon\mathfrak{a})^{\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})}\subset E(K)\colon(\mathfrak{w}+\mathfrak{a})+E[\mathfrak{a}\mathfrak{w}],$$

as desired. ■

5. Galois representation on torsion points

Throughout this section, let K be a number field, let E be an elliptic curve over K with $\mathcal{O}=\mathrm{End}_K(E)\neq\mathbf{Z}$ a Dedekind domain, let F be the fraction field of $\mathcal{O}$, let $\mathcal{O}_K$ be the ring of integers of K, and let $\mathfrak{c}$ be the conductor of E over K (see [Sil94, §IV.10]). Remark that $\mathfrak{c}$ is a nonzero $\mathcal{O}_K$-ideal. For an extension of prime ideals $\mathfrak{q}/\mathfrak{p}$ in an extension of rings we write $\mathrm{e}(\mathfrak{q}/\mathfrak{p})$ for the *ramification index* of $\mathfrak{q}$ over $\mathfrak{p}$, if it exists.

As all elements of $\mathcal{O}$ are defined over K, the action of $\mathcal{O}$ on the tangent space at the origin induces an injective ring morphism $\mathcal{O}\longrightarrow K$, which extends to an injective map $F\longrightarrow K$ (see [Sil94, Chapter 2]). Throughout this chapter, we identify $\mathcal{O}$ and F with their images in K, so that we have $\mathcal{O}\subset\mathcal{O}_K$ and $F\subset K$.

For $\mathfrak{p}$ a maximal ideal of $\mathcal{O}$, define $i_{\mathfrak{p}}\in\mathbf{Z}_{\geq 0}$ as follows. For primes $\mathfrak{q}$ of $\mathcal{O}_K$ dividing $\mathfrak{p}$, let $i_{\mathfrak{q}}\in\mathbf{Z}_{\geq 0}$ be such that

$$i_{\mathfrak{q}}=\begin{cases}1 & \text{if } \mathrm{v}_{\mathfrak{q}}(\mathfrak{c})=0 \text{ and } \mathrm{e}(\mathfrak{q}/\mathfrak{p})\neq 1,\\ \frac{\mathrm{v}_{\mathfrak{q}}(\mathfrak{c})}{2} & \text{if } \mathrm{v}_{\mathfrak{q}}(\mathfrak{c})>0 \text{ or } \mathrm{e}(\mathfrak{q}/\mathfrak{p})=1,\end{cases}$$

where $\mathrm{v}_{\mathfrak{q}}$ is the $\mathfrak{q}$-adic valuation (cf. Remark 3.6), and observe that

$$i_{\mathfrak{q}}=0\Leftrightarrow[\mathrm{e}(\mathfrak{q}/\mathfrak{p})=1\text{ and }\mathfrak{q}\nmid\mathfrak{c}].$$

By Theorem 6 in [ST68] we have for all primes $\mathfrak{q}$ of $\mathcal{O}_K$ that $\mathrm{v}_\mathfrak{q}(\mathfrak{c})$ is divisible by 2. Hence $i_\mathfrak{q}$ is an integer. Let p be the characteristic of $\mathcal{O}/\mathfrak{p}$, let

$$m_\mathfrak{q} = \max\left\{ \left\lceil \frac{i_\mathfrak{q}}{\mathrm{e}(\mathfrak{q}/\mathfrak{p})} \right\rceil, \left\lfloor \frac{\mathrm{e}(\mathfrak{p}/p)}{p-1} \right\rfloor + 1 \right\},$$

and let

$$i_{\mathfrak{p},\mathfrak{q}} = \begin{cases} \left\lceil \frac{i_\mathfrak{q}}{\mathrm{e}(\mathfrak{q}/\mathfrak{p})} \right\rceil & \text{if } p \nmid \mathrm{e}(\mathfrak{q}/\mathfrak{p}), \\ m_\mathfrak{q} + \mathrm{e}(\mathfrak{p}/p) \cdot \mathrm{v}_p(\mathrm{e}(\mathfrak{q}/\mathfrak{p})) & \text{if } p \mid \mathrm{e}(\mathfrak{q}/\mathfrak{p}). \end{cases}$$

Then put $i_\mathfrak{p} = \min_\mathfrak{q} i_{\mathfrak{p},\mathfrak{q}}$, where $\mathfrak{q}$ runs over the primes of $\mathcal{O}_K$ dividing $\mathfrak{p}$. Now, observe that for maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ not dividing $\mathfrak{c} \cdot \Delta_{K/F}$, where $\Delta_{K/F}$ is the discriminant of K over F, we have $i_\mathfrak{p} = 0$. Thus, for almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ we have $i_\mathfrak{p} = 0$.

For an $\mathcal{O}$-module N and $\mathcal{O}$-submodule N' of N we write $\mathrm{Aut}_{\mathcal{O},N'}(N)$ for the group of $\mathcal{O}$-automorphisms of N that are the identity on N'. Moreover, observe that for a Steinitz ideal $\mathfrak{a}$ of $\mathcal{O}$ the group $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$ may be identified with a subgroup of $\mathrm{Aut}_{\mathcal{O},E(K)[\mathfrak{a}]}(E[\mathfrak{a}])$ (see also the text before Proposition 3.7).

In this section, we prove the following theorem.

Theorem 3.13. *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$.*

(a) *Then $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$ is open in $\mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}])$.*

(b) *Let $\mathcal{P}$ be the set of maximal ideals of $\mathcal{O}$ dividing $\mathfrak{a}$ that satisfy $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) \geq i_\mathfrak{p}$. Then the subgroup $\prod_{\mathfrak{p}\in\mathcal{P}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_\mathfrak{p}}]}\big(E[\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}]\big)$ of $\mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}])$ is open, and moreover, we have*

$$\prod_{\mathfrak{p}\in\mathcal{P}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_\mathfrak{p}}]}\big(E[\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}]\big) \subset \mathrm{Gal}(K(E[\mathfrak{a}])/K)$$

as subgroups of $\mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}])$.

General notation. Let L be a number field, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_L$. Then we write $\mathcal{O}_{L,\mathfrak{a}}$ for the $\mathfrak{a}$-adic completion of $\mathcal{O}_L$, and $L_\mathfrak{a} = L \otimes_{\mathcal{O}_L} \mathcal{O}_{L,\mathfrak{a}}$. If $\mathfrak{a} = (a)$ is principal, we simply write $\mathcal{O}_{L,a}$ instead of $\mathcal{O}_{L,\mathfrak{a}}$, and L_a instead of $L_\mathfrak{a}$. Note that $\mathcal{O}_{L,\mathfrak{a}} = \prod_\mathfrak{p} \mathcal{O}_{L,\mathfrak{p}}$ and $L_\mathfrak{a} = \prod_\mathfrak{p} L_\mathfrak{p}$ where $\mathfrak{p}$ runs over all primes of $\mathcal{O}_L$ dividing $\mathfrak{a}$.

Suppose that $\mathfrak{a} = \mathfrak{p}$ is a prime ideal. Then by abuse of notation we also write $\mathfrak{p}$ for the maximal ideal of the ring of integers of the local field $L_\mathfrak{p}$. For $i \in \mathbf{Z}_{\geq 0}$ we write $\mathrm{U}_{\mathfrak{p},i}$ or $\mathrm{U}_{L_\mathfrak{p},i}$ for the *ith unit group* of $L_\mathfrak{p}$, that is,

$$\mathrm{U}_{\mathfrak{p},0} = (\mathcal{O}_{L,\mathfrak{p}})^*$$

and for $i \geq 1$

$$\mathrm{U}_{\mathfrak{p},i} = 1 + \mathfrak{p}^i \mathcal{O}_{L,\mathfrak{p}}.$$

We write I_L for the idèle group of L.

Let L'/L be an extension of number fields, and let $\mathfrak{q}$ be a prime of $\mathcal{O}_{L'}$ dividing $\mathfrak{p}$. For the extension $L'_\mathfrak{q}/L_\mathfrak{p}$ of local fields, we sometimes write $\mathrm{e}(L'_\mathfrak{q}/L_\mathfrak{p})$ for $\mathrm{e}(\mathfrak{q}/\mathfrak{p})$. We write $\mathrm{N}_{\mathrm{I}_{L'}/\mathrm{I}_L} \colon \mathrm{I}_{L'} \longrightarrow \mathrm{I}_L$ for the idèle norm. Let p be the characteristic of $\mathfrak{p}$, and embed L'^*_p in $\mathrm{I}_{L'}$ by putting 1's at the primes not over p. Then we write

$$\mathrm{N}_{L'_p/L_p} = \prod_\mathfrak{p} \prod_\mathfrak{q} \mathrm{N}_{L'_\mathfrak{q}/L_\mathfrak{p}} \colon L'^*_p \longrightarrow L^*_p$$

for the restriction of the idèle norm to L'^*_p, where $\mathfrak{p}$ runs over the primes of $\mathcal{O}_L$ dividing p, and $\mathfrak{q}$ runs over the primes of $\mathcal{O}_{L'}$ dividing $\mathfrak{p}$.

Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. By Proposition 3.7 we have

$$E[\mathfrak{a}] \cong_\mathcal{O} (F/\mathcal{O})[\mathfrak{a}] = \mathfrak{a}^{-1}/\mathcal{O} \cong \mathcal{O}/\mathfrak{a},$$

so that $\mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}]) \cong (\mathcal{O}/\mathfrak{a})^*$. Moreover, the latter isomorphism is compatible with the restriction maps $\mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}]) \longrightarrow \mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}'])$ and canonical maps $(\mathcal{O}/\mathfrak{a})^* \longrightarrow (\mathcal{O}/\mathfrak{a}')^*$ for $\mathfrak{a}'$ an ideal of $\mathcal{O}$ dividing $\mathfrak{a}$. Hence, we have

$$\mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}^\infty]) = \varprojlim_i \mathrm{Aut}_\mathcal{O}(E[\mathfrak{a}^i]) \cong \mathcal{O}^*_\mathfrak{a},$$

where for simplicity we write $\mathcal{O}_{\mathfrak{a}}$ for $\mathcal{O}_{F,\mathfrak{a}}$. We define the map $\varphi_{\mathfrak{a}}$ as the following composition of canonical maps

$$\mathrm{Gal}(K(E[\mathfrak{a}^\infty])/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}^\infty]) \xrightarrow{\sim} \mathcal{O}_{\mathfrak{a}}^*,$$

and note that $\varphi_{\mathfrak{a}}$ is injective. As $K(E[\mathfrak{a}^\infty])$ is contained in the maximal abelian extension K^{ab} of K (see Proposition 3.7(c)), the global reciprocity law induces a surjective morphism $\psi_{\mathfrak{a}}\colon \mathrm{I}_K \longrightarrow \mathrm{Gal}(K(E[\mathfrak{a}^\infty])/K)$ of topological groups. We define $\rho_{\mathfrak{a}}$ as the composition

$$\rho_{\mathfrak{a}} = \varphi_{\mathfrak{a}} \circ \psi_{\mathfrak{a}}\colon \mathrm{I}_K \longrightarrow \mathcal{O}_{\mathfrak{a}}^*.$$

Now, let $\mathfrak{a} = (0)$, and define $\varphi_{\mathfrak{a}}$, $\psi_{\mathfrak{a}}$ and $\rho_{\mathfrak{a}}$ by doing exactly the above while replacing $\mathcal{O}_{\mathfrak{a}}$ with $\widehat{\mathcal{O}}$. If $\mathfrak{a} = (a)$ is principal, we simply write a subscript a instead of a subscript $\mathfrak{a}$ in the above notation, and if $\mathfrak{a} = (0)$, we simply write no subscript.

As we remarked earlier, for a prime $\mathfrak{q}$ of $\mathcal{O}_K$ dividing the conductor $\mathfrak{c}$, Theorem 6 in [ST68] implies that $\mathrm{v}_{\mathfrak{q}}(\mathfrak{c})$ is divisible by 2. We write

$$1 + \sqrt{\mathfrak{c}} = \prod_{\mathfrak{q}} \mathrm{U}_{\mathfrak{q},\frac{\mathrm{v}_{\mathfrak{q}}(\mathfrak{c})}{2}} \subset (\mathcal{O}_{K,\mathfrak{c}})^*,$$

where $\mathfrak{q}$ runs over all primes of $\mathcal{O}_K$ dividing $\mathfrak{c}$.

As F is a quadratic imaginary field contained in K, the field K is totally complex.

Proposition 3.14. *Let F^* be endowed with the discrete topology. Then there is a unique continuous group morphism $\epsilon\colon \mathrm{I}_K \longrightarrow F^*$ such that $\epsilon(x) = \mathrm{N}_{K/F}(x)$ for all $x \in K^*$, and such that for each prime number p and each $a \in \mathrm{I}_K$*

$$\rho_p(a) = \epsilon(a)\,\mathrm{N}_{K_p/F_p}((a_p)^{-1}) \in \mathcal{O}_p^*,$$

where $a_p = (a_{\mathfrak{q}})_{\mathfrak{q}} \in \prod_{\mathfrak{q}} K_{\mathfrak{q}}^*$ and $\mathfrak{q}$ runs over the maximal ideals of $\mathcal{O}_K$ dividing p. Moreover, the kernel of ϵ contains

$$(1 + \sqrt{\mathfrak{c}}) \times \prod_{\mathfrak{q}} \mathrm{U}_{\mathfrak{q},0} \times \prod_{\mathfrak{r}} K_{\mathfrak{r}}^*,$$

where $\mathfrak{q}$ *runs over all finite primes of* $\mathcal{O}_K$ *not dividing* $\mathfrak{c}$*, and* $\mathfrak{r}$ *runs over all infinite primes of* K.

Proof. For the first part of the theorem see [Ser72, Theorem 5] or [ST68, §7]. For the second part see [ST68, Theorem 6 and Theorem 11]. ■

Lemma 3.15. *Let* p *be a prime number, let* L *be a finite extension of* $\mathbf{Q}_p$*, let* L' *be a finite extension of* L*, and let* $\mathrm{e}_L = \mathrm{e}(L/\mathbf{Q}_p)$.

(a) *Suppose that* $\mathrm{e}(L'/L) = 1$. *Then for all* $i \in \mathbf{Z}_{\geq 0}$ *we have*

$$\mathrm{U}_{L,i} = \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}),$$

where $\mathrm{N}_{L'/L}\colon L'^{*} \longrightarrow L^{*}$ *is the norm function.*

(b) *Let* $i \in \mathbf{Z}_{\geq 1}$*, and let* $m = \max\left\{\left\lceil \frac{i}{\mathrm{e}(L'/L)} \right\rceil, \left\lfloor \frac{\mathrm{e}_L}{p-1} \right\rfloor + 1\right\}$. *Put*

$$i_0 = \begin{cases} \lceil i/\,\mathrm{e}(L'/L) \rceil & \text{if } p \nmid \mathrm{e}(L'/L), \\ m + \mathrm{e}_L \cdot \mathrm{v}_p(\mathrm{e}(L'/L)) & \text{otherwise}. \end{cases}$$

Then

$$\mathrm{U}_{L,i_0} \subset \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}),$$

where $\mathrm{N}_{L'/L}\colon L'^{*} \longrightarrow L^{*}$ *is the norm function.*

Proof. If $\mathrm{e}(L'/L) = 1$, then [Ser79, Chapter V, §2] implies that for every $i \in \mathbf{Z}_{\geq 0}$

$$\mathrm{U}_{L,i} = \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}),$$

which proves statement (a) and also statement (b) in the case that $\mathrm{e}(L'/L) = 1$.

Now, suppose that $i > 0$. By transitivity of the norm and the above case, we may assume that L'/L is totally ramified. Let L_{t} be the maximal tamely ramified extension of L

inside L', let $\mathrm{e}(L'/L)_{\mathrm{t}} = [L_{\mathrm{t}} : L]$ be the tame part of $\mathrm{e}(L'/L)$, and let $\mathrm{e}(L'/L)_p = [L' : L_{\mathrm{t}}]$ be the wild part of $\mathrm{e}(L'/L)$.

Note that for $x \in L$ we have

$$\mathrm{N}_{L'/L}(x) = x^{[L':L]} = x^{\mathrm{e}(L'/L)}.$$

Let $\mathfrak{p}$ be the maximal ideal of the ring of integers $\mathcal{O}_L$ of L and let $\mathfrak{q}$ be the maximal ideal of $\mathcal{O}_{L'}$. Then $\mathfrak{p} \subset \mathfrak{q}^{\mathrm{e}(L'/L)}$ implies that

$$\left(\mathrm{U}_{L,\lceil \frac{i}{\mathrm{e}(L'/L)} \rceil}\right)^{\mathrm{e}(L'/L)} \subset \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}).$$

As for $l \in \mathbf{Z}_{\geq 1}$ the groups $\mathrm{U}_{L,l}$ are pro-p-groups, we have

$$\left(\mathrm{U}_{L,\lceil \frac{i}{\mathrm{e}(L'/L)} \rceil}\right)^{\mathrm{e}(L'/L)_p} = \left(\mathrm{U}_{L,\lceil \frac{i}{\mathrm{e}(L'/L)} \rceil}\right)^{\mathrm{e}(L'/L)} \subset \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}).$$

Suppose that p does not divide $\mathrm{e}(L'/L)$. Then $\mathrm{e}(L'/L)_p = 1$, so

$$\mathrm{U}_{L,\lceil \frac{i}{\mathrm{e}(L'/L)} \rceil} = \left(\mathrm{U}_{L,\lceil \frac{i}{\mathrm{e}(L'/L)} \rceil}\right)^{\mathrm{e}(L'/L)_p} \subset \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}),$$

which proves the lemma in the case that $p \nmid \mathrm{e}(L'/L)$.

Now, suppose that $\mathrm{e}(L'/L)_p \neq 1$. Since $m \geq \frac{i}{\mathrm{e}(L'/L)}$, we have

$$(\mathrm{U}_{L,m})^{\mathrm{e}(L'/L)_p} \subset \left(\mathrm{U}_{L,\lceil \frac{i}{\mathrm{e}(L'/L)} \rceil}\right)^{\mathrm{e}(L'/L)_p} \subset \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}).$$

Moreover, by [Ser79, Chapter XIV, Proposition 9] we have for every integer $l > \frac{\mathrm{e}_L}{p-1}$ that

$$(\mathrm{U}_{L,l})^p = \mathrm{U}_{L,l+\mathrm{e}_L}.$$

Hence, since $m > \frac{\mathrm{e}_L}{p-1}$, we have

$$\mathrm{U}_{L,i_0} = \mathrm{U}_{L,m+\mathrm{e}_L \cdot \mathrm{v}_p(\mathrm{e}(L'/L))} = (\mathrm{U}_{L,m})^{\mathrm{e}(L'/L)_p} \subset \mathrm{N}_{L'/L}(\mathrm{U}_{L',i}),$$

which proves the lemma in the final case that $p \mid \mathrm{e}(L'/L)$. ■

Proof of Theorem 3.13. We first prove (b) for the Steinitz ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\infty}$, that is, we first show that

$$\prod_{\mathfrak{p}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_{\mathfrak{p}}}]}(E[\mathfrak{p}^{\infty}]) \subset \mathrm{Gal}(K(E_{\mathrm{tor}})/K),$$

as subgroups of $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}})$, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$. To this end, let

$$U = (1+\sqrt{\mathfrak{c}}) \times \prod_{\mathfrak{q}} \mathrm{U}_{\mathfrak{q},0} \times \prod_{\mathfrak{r}} K_{\mathfrak{r}}^{*},$$

where $1+\sqrt{\mathfrak{c}}$ is defined above Proposition 3.14, where $\mathfrak{q}$ runs over all finite primes of $\mathcal{O}_K$ not dividing $\mathfrak{c}$, and $\mathfrak{r}$ runs over all infinite primes of K.

For an ideal $\mathfrak{b}$ of $\mathcal{O}$, let $\psi_{\mathfrak{b}}$, $\varphi_{\mathfrak{b}}$ and $\rho_{\mathfrak{b}}$ be as defined above Proposition 3.14. Recall that if (b) is principal, we simply write ψ_b, φ_b and ρ_b for these maps, and if $\mathfrak{b} = (0)$ we have $(0)^{\infty} = \mathfrak{a}$ and simply write ψ, φ and ρ.

We claim that $\rho = \prod_{\mathfrak{p}} \rho_{\mathfrak{p}}$ where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$.

Indeed, we have $\widehat{\mathcal{O}} = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ as profinite rings, so that $\widehat{\mathcal{O}}^{*} = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{*}$ as profinite groups. Moreover, for a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ we have the following commutative diagram

$$\begin{tikzcd}
\mathrm{I}_K \arrow[r, "\psi"] \arrow[d, "\mathrm{id}"'] \arrow[rr, bend left, "\rho"] & \mathrm{Gal}(K(E_{\mathrm{tor}})/K) \arrow[r, "\varphi"] \arrow[d] & \widehat{\mathcal{O}}^{*} \arrow[d] \\
\mathrm{I}_K \arrow[r, "\psi_{\mathfrak{p}}"'] \arrow[rr, bend right, "\rho_{\mathfrak{p}}"'] & \mathrm{Gal}(K(E[\mathfrak{p}^{\infty}])/K) \arrow[r, "\varphi_{\mathfrak{p}}"'] & \mathcal{O}_{\mathfrak{p}}^{*}
\end{tikzcd}$$

where the two right vertical maps are the canonical maps. The claim now follows from the universal property of products.

Now, by Proposition 3.14 we have for all prime numbers p that $\rho_p(U) = \mathrm{N}_{K_p/F_p}(U_p)$, where U_p is the pth component of U. Then for a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ one easily sees that

$$\rho_{\mathfrak{p}}(U) = \prod_{\mathfrak{q}} \mathrm{N}_{K_{\mathfrak{q}}/F_{\mathfrak{p}}}(U_{\mathfrak{q}}),$$

where $\mathfrak{q}$ runs over all primes of $\mathcal{O}_K$ dividing $\mathfrak{p}$, and $U_\mathfrak{q}$ is the $\mathfrak{q}$th component of U.

Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$, and let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_K$ dividing $\mathfrak{p}$. If $\mathrm{v}_\mathfrak{q}(\mathfrak{c}) = 0$, we have $U_\mathfrak{q} = U_{\mathfrak{q},0}$ by definition of U, so $i_\mathfrak{q} \geq 0$ implies that

$$U_\mathfrak{q} \supset \mathrm{U}_{K_\mathfrak{q}, i_\mathfrak{q}}\,.$$

On the other hand, if $\mathrm{v}_\mathfrak{q}(\mathfrak{c}) > 0$, we have

$$U_\mathfrak{q} = U_{\mathfrak{q}, \frac{\mathrm{v}_\mathfrak{q}(\mathfrak{c})}{2}} = U_{\mathfrak{q}, i_\mathfrak{q}}$$

by definition of U and $i_\mathfrak{q}$. Thus, in both cases the inclusion $U_{K_\mathfrak{q}, i_\mathfrak{q}} \subset U_\mathfrak{q}$ holds. Moreover, the equivalence

$$i_\mathfrak{q} = 0 \Leftrightarrow [\mathrm{e}(\mathfrak{q}/\mathfrak{p}) = 1 \text{ and } \mathfrak{q} \nmid \mathfrak{c}]$$

holds. Then Lemma 3.15, where $L' = K_\mathfrak{q}$, $L = F_\mathfrak{p}$, and $i = i_\mathfrak{q}$, implies that

$$\mathrm{U}_{F_\mathfrak{p}, i_{\mathfrak{p},\mathfrak{q}}} \subset \mathrm{N}_{K_\mathfrak{q}/F_\mathfrak{p}}(U_\mathfrak{q}).$$

Thus, for all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ and $\mathfrak{q}$ of $\mathcal{O}_K$ dividing $\mathfrak{p}$, we have by definition of $i_\mathfrak{p}$ that

$$\mathrm{U}_{F_\mathfrak{p}, i_\mathfrak{p}} \subset \prod_\mathfrak{q} \mathrm{N}_{K_\mathfrak{q}/F_\mathfrak{p}}(U_\mathfrak{q}),$$

which implies that the image of $\rho_\mathfrak{p}$, and also of $\varphi_\mathfrak{p}$, in $\mathcal{O}_\mathfrak{p}^*$ contains $\mathrm{U}_{F_\mathfrak{p}, i_\mathfrak{p}}$.

Since $\rho(U) = \prod_\mathfrak{p} \rho_\mathfrak{p}(U)$ and the image of φ contains $\rho(U)$, the inclusions

$$\mathrm{im}(\varphi) \supset \rho(U) \supset \prod_\mathfrak{p} U_{F_\mathfrak{p}, i_\mathfrak{p}}$$

hold, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$.

Now, under the isomorphism $\widehat{\mathcal{O}}^* \longrightarrow \mathrm{Aut}_\mathcal{O}(E_{\mathrm{tor}})$ the subgroup $\prod_\mathfrak{p} \mathrm{U}_{F_\mathfrak{p}, i_\mathfrak{p}}$ corresponds to the subgroup

$$\prod_\mathfrak{p} \mathrm{Aut}_{\mathcal{O}, E[\mathfrak{p}^{i_\mathfrak{p}}]}(E[\mathfrak{p}^\infty])$$

of $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}})$, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$. Thus, we have

$$\prod_{\mathfrak{p}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_{\mathfrak{p}}}]}(E[\mathfrak{p}^{\infty}]) \subset \mathrm{Gal}(K(E_{\mathrm{tor}})/K),$$

where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$.

At last, observe that for a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ the subgroup

$$\mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_{\mathfrak{p}}}]}(E[\mathfrak{p}^{\infty}])$$

is open in $\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{p}^{\infty}])$. Simultaneously, we have $i_{\mathfrak{p}} = 0$ for almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$. Therefore, the subgroup

$$\prod_{\mathfrak{p}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_{\mathfrak{p}}}]}(E[\mathfrak{p}^{\infty}])$$

is open in

$$\prod_{\mathfrak{p}} \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{p}^{\infty}]) = \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}}),$$

where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$. Consequently, the group $\mathrm{Gal}(K(E_{\mathrm{tor}})/K)$ is open in $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}})$. This proves (a) and (b) for the Steinitz ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\infty}$, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$.

Let $\mathfrak{a}$ be a Steinitz ideal. Then the diagram

$$\begin{tikzcd}
\mathrm{Gal}(K(E_{\mathrm{tor}})/K) \arrow[r] \arrow[d] & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tor}}) \arrow[d] \\
\mathrm{Gal}(K(E[\mathfrak{a}])/K) \arrow[r] & \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}])
\end{tikzcd}$$

is commutative, where the vertical maps are the surjective restriction maps (see Proposition 3.7(b)). As the vertical maps are open, commutativity of the diagram implies that the composition

$$\mathrm{Gal}(K(E_{\mathrm{tor}})/K) \longrightarrow \mathrm{Gal}(K(E[\mathfrak{a}])/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}])$$

is open. Hence $\mathrm{Gal}(K(E[\mathfrak{a}])/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}])$ is open, which proves (a).

Let $\mathcal{P}$ be the set of maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ dividing $\mathfrak{a}$ with multiplicity at least $i_{\mathfrak{p}}$, that is, let

$$\mathcal{P} = \{\mathfrak{p} \subset \mathcal{O} : \mathfrak{p} \text{ maximal}, \mathfrak{p}|\mathfrak{a}, \mathrm{v}_{\mathfrak{p}}(\mathfrak{a}) \geq i_{\mathfrak{p}}\}.$$

Using Proposition 3.7(b) we see that the image of the subgroup $\prod_{\mathfrak{p}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_{\mathfrak{p}}}]}(E[\mathfrak{p}^{\infty}])$, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$, under the restriction map

$$\mathrm{Gal}(K(E_{\mathrm{tor}})/K) \longrightarrow \mathrm{Gal}(K(E[\mathfrak{a}])/K)$$

is equal to

$$\prod_{\mathfrak{q} \in \mathcal{P}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{q}^{i_{\mathfrak{q}}}]}(E[\mathfrak{q}^{\mathrm{v}_{\mathfrak{q}}(\mathfrak{a})}]),$$

which proves (b). ■

6. Kummer theory

Throughout this section, let K be a number field, let $\overline{K}$ be an algebraic closure of K, let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, let F be the fraction field of $\mathcal{O}$, and let $U \subset E(K)$ be an $\mathcal{O}$-submodule.

In this section we prove the following theorem (see the text before Theorem 3.13 for the definition of the automorphism groups mentioned).

Theorem 3.16. *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then the canonical map*

$$\mathrm{Gal}(K(U\!:\mathfrak{a})/K(E[\mathfrak{a}])) \longrightarrow \mathrm{Aut}_{\mathcal{O},U+E[\mathfrak{a}]}(U\!:\mathfrak{a})$$

is injective and open.

Notation. Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then we write

$$\mathrm{Sat}_{\mathfrak{a}}(U) = (U\!:\mathfrak{a}) \cap E(K) = (U\!:\mathfrak{a})^{\mathrm{Gal}(\overline{K}/K)},$$

and

$$\mathrm{Cyc}_{\mathfrak{a}}(U) = (U : \mathfrak{a}) \cap E(K(E[\mathfrak{a}])) = (U : \mathfrak{a})^{\mathrm{Gal}(\overline{K}/K(E[\mathfrak{a}]))}.$$

In some cases, we expand our notation to $\mathrm{Sat}_{\mathfrak{a}}(U, K)$ and $\mathrm{Cyc}_{\mathfrak{a}}(U, K)$ to clarify the base field K. When $\mathfrak{a} = \infty_{\mathcal{O}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\infty}$, where $\mathfrak{p}$ runs over all maximal ideals of $\mathcal{O}$, we leave out the subscript $\mathfrak{a}$ from the notation.

Definition 3.17. For an $\mathcal{O}$-module M we write $\mathrm{rk}_{\mathcal{O}}(M)$ for the *$\mathcal{O}$-rank* $\dim_F(M \otimes_{\mathcal{O}} F)$ of M, where F is the fraction field of $\mathcal{O}$.

Observe that $\mathrm{rk}_{\mathcal{O}}(U)$ is finite.

Proposition 3.18. *Let $n = \mathrm{rk}_{\mathcal{O}}(U)$.*

(a) *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Then $U : \mathfrak{a}$ is finitely generated over $\mathcal{O}$ of $\mathcal{O}$-rank n.*

(b) *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then for any finite extension K'/K the $\mathcal{O}$-module $\mathrm{Sat}_{\mathfrak{a}}(U, K')$ is finitely generated over $\mathcal{O}$ of $\mathcal{O}$-rank n.*

(c) *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then $\mathrm{Cyc}_{\mathfrak{a}}(U)/E[\mathfrak{a}]$ is finitely generated over $\mathcal{O}$ of $\mathcal{O}$-rank n.*

Proof. Let $\mathfrak{a}$ and K' be as in (b). By the Mordell-Weil theorem (see [Sil09]) we know that $E(K')$ is finitely generated over **Z**, and, consequently, over $\mathcal{O}$. As $\mathrm{Sat}_{\mathfrak{a}}(U, K')$ is contained in $E(K')$, we have that $\mathrm{Sat}_{\mathfrak{a}}(U, K')$ is finitely generated over $\mathcal{O}$. Then the quotient $Q = \mathrm{Sat}_{\mathfrak{a}}(U, K')/U$ is finitely generated over $\mathcal{O}$. Moreover, by definition of $\mathrm{Sat}_{\mathfrak{a}}(U, K')$ the quotient Q is torsion over $\mathcal{O}$. It follows that $\mathrm{Sat}_{\mathfrak{a}}(U, K')$ has the same $\mathcal{O}$-rank as U, which proves (b).

Now, let $\mathfrak{a}$ be as in (a). As U is finitely generated over $\mathcal{O}$, the module $U : \mathfrak{a}$ is finitely generated too. Then the field $K' = K(U : \mathfrak{a})$ is finite over K. By (b) the module $\mathrm{Sat}_{\mathfrak{a}}(U, K')$

is finitely generated of $\mathcal{O}$-rank n. As

$$U \subset U : \mathfrak{a} \subset \mathrm{Sat}_{\mathfrak{a}}(U, K'),$$

it follows that $U : \mathfrak{a}$ has $\mathcal{O}$-rank n. This proves (a).

Let $\mathfrak{a}$ be as in (c). Let K^{ab} be the maximal abelian extension of K contained in $\overline{K}$. Let $\widehat{\mathcal{O}}$ be the profinite completion of $\mathcal{O}$, and let $\mathfrak{w} = \mathrm{Ann}_{\widehat{\mathcal{O}}}(E(K)_{\mathrm{tor}})$. As K is a number field, the module $E(K)_{\mathrm{tor}}$ is finite, so that $\mathfrak{w} = \mathrm{Ann}_{\mathcal{O}}(E(K)_{\mathrm{tor}})$. Observe that

$$\mathrm{Cyc}_{\mathfrak{a}}(E(K)) \subset (E(K) : \mathfrak{a}) \cap E(K^{\mathrm{ab}}).$$

By Theorem 3.9 we have

$$(E(K) : \mathfrak{a}) \cap E(K^{\mathrm{ab}}) = (E(K) : (\mathfrak{w} + \mathfrak{a})) + E[\mathfrak{w}\mathfrak{a}].$$

First, we will show that $\mathrm{Cyc}_{\mathfrak{a}}(E(K))/E[\mathfrak{a}]$ is finitely generated over $\mathcal{O}$. By the above, it suffices to show that $(E(K) : (\mathfrak{w} + \mathfrak{a}))$ and $E[\mathfrak{w}\mathfrak{a}]/E[\mathfrak{a}]$ are finitely generated over $\mathcal{O}$.

To this end, observe that $\mathfrak{w} + \mathfrak{a} = \mathrm{Ann}_{\mathcal{O}}(E(K)[\mathfrak{a}])$ is an ideal of $\mathcal{O}$ and $E(K)$ is finitely generated over $\mathcal{O}$, so $E(K) : (\mathfrak{w} + \mathfrak{a})$ is finitely generated over $\mathcal{O}$.

Moreover, the $\mathcal{O}$-module $E[\mathfrak{w}\mathfrak{a}]$ decomposes as $\bigoplus_{\mathfrak{p}} E[\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{w}) + \mathrm{v}_{\mathfrak{p}}(\mathfrak{a})}]$, where $\mathfrak{p}$ runs over all primes of $\mathcal{O}$ dividing $\mathfrak{w}\mathfrak{a}$. Then one easily sees that

$$E[\mathfrak{w}\mathfrak{a}]/E[\mathfrak{a}] \cong \bigoplus_{\mathfrak{p}} \left(E\left[\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{w}) + \mathrm{v}_{\mathfrak{p}}(\mathfrak{a})}\right] / E\left[\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})}\right] \right),$$

where $\mathfrak{p}$ runs over all primes of $\mathcal{O}$ dividing $\mathfrak{w}\mathfrak{a}$ such that $\mathrm{v}_{\mathfrak{p}}(\mathfrak{a}) < \infty$ and $\mathrm{v}_{\mathfrak{p}}(\mathfrak{w}) > 0$. As there are only finitely many such $\mathfrak{p}$, and $\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})$ and $\mathrm{v}_{\mathfrak{p}}(\mathfrak{w})$ are finite, the decomposition is a finite direct sum of finitely generated modules over $\mathcal{O}$. It follows that $E[\mathfrak{w}\mathfrak{a}]/E[\mathfrak{a}]$ is finitely generated over $\mathcal{O}$, so that $\mathrm{Cyc}_{\mathfrak{a}}(E(K))/E[\mathfrak{a}]$ is finitely generated over $\mathcal{O}$.

Now, as

$$U \subset \mathrm{Cyc}_{\mathfrak{a}}(U) \subset U : \mathfrak{a}$$

and $\frac{U:\mathfrak{a}}{U}$ is torsion over $\mathcal{O}$ (annihilated by $\mathfrak{a}$), we have that $\mathrm{rk}_{\mathcal{O}}(\mathrm{Cyc}_{\mathfrak{a}}(U)) = \mathrm{rk}_{\mathcal{O}}(U)$. It follows that $\mathrm{Cyc}_{\mathfrak{a}}(U)/E[\mathfrak{a}]$ is finitely generated over $\mathcal{O}$ of the same $\mathcal{O}$-rank as U, which proves (c). ∎

In the rest of this section, we use two $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$-modules extensively, which we define as follows.

Let $\mathfrak{a}$ be a Steinitz ideal. Recall from Theorem 3.13 and Proposition 3.7(b) that we may consider $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$ as a subgroup of $(\widehat{\mathcal{O}}/\mathfrak{a})^*$. The short exact sequence

$$0 \longrightarrow \mathrm{Gal}(K(U:\mathfrak{a})/K(E[\mathfrak{a}])) \longrightarrow \mathrm{Gal}(K(U:\mathfrak{a})/K) \longrightarrow \mathrm{Gal}(K(E[\mathfrak{a}])/K) \longrightarrow 0$$

induces a $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$-module structure on $\mathrm{Gal}(K(U:\mathfrak{a})/K(E[\mathfrak{a}]))$, because the latter is abelian by Proposition 3.12.

On the other hand, define

$$\kappa_{\mathfrak{a}}\colon\ \mathrm{Gal}(K(U:\mathfrak{a})/K(E[\mathfrak{a}])) \longrightarrow \mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$$

as the canonical map given by $\sigma \mapsto [Q + \mathrm{Cyc}_{\mathfrak{a}}(U) \mapsto \sigma(Q) - Q]$, and note that $\kappa_{\mathfrak{a}}$ is an injective group morphism. The multiplication action of $\widehat{\mathcal{O}}/\mathfrak{a}$ on $E[\mathfrak{a}]$ induces an $\widehat{\mathcal{O}}/\mathfrak{a}$-module structure on $\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$. In particular, there is a $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$-module structure on $\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$, where we consider $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$ as a subgroup of $(\widehat{\mathcal{O}}/\mathfrak{a})^*$.

Lemma 3.19. *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then the following statements hold.*

(a) *The group* $\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$ *is profinite.*

(b) *Let $G \subset \mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$ be a closed subgroup. Then G is a finitely generated profinite group.*

Proof. The $\mathcal{O}$-module

$$\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}$$

is the union of the submodules

$$\frac{U\colon\mathfrak{b}}{(U\colon\mathfrak{b})\cap\mathrm{Cyc}_{\mathfrak{a}}(U)},$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. For each such $\mathfrak{b}$, the corresponding module is finite and annihilated by $\mathfrak{b}$. It follows that the group $\mathrm{Hom}_{\mathcal{O}}\Big(\frac{U\colon\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\Big)$ may be identified with the projective limit of the finite groups

$$H_{\mathfrak{b}} = \mathrm{Hom}_{\mathcal{O}}\left(\frac{U\colon\mathfrak{b}}{(U\colon\mathfrak{b})\cap\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{b}]\right),$$

and is therefore profinite. This proves (a).

Now, let G be as in (b). Since G is closed, we have

$$G = \varprojlim_{\mathfrak{b}} G_{\mathfrak{b}},$$

where $G_{\mathfrak{b}}$ is the image of G in $H_{\mathfrak{b}}$. We will show that there is $c \in \mathbf{Z}_{\geq 1}$ such that for every $m \in \mathbf{Z}_{\geq 1}$ we have $\#(G/mG) \leq m^c$, which implies that G is finitely generated (see [RZ09, Lemma 2.5.3]), as desired.

To this end, let $m \in \mathbf{Z}_{\geq 1}$, and let n be the $\mathcal{O}$-rank of U. We will show that for every nonzero ideal $\mathfrak{b}$ of $\mathcal{O}$ dividing $\mathfrak{a}$ we have

$$\#(G_{\mathfrak{b}}/mG_{\mathfrak{b}}) \leq m^{2n+2}.$$

Let $\mathfrak{b}$ be a nonzero ideal of $\mathcal{O}$ dividing $\mathfrak{a}$, and note that $E[\mathfrak{b}] \cong_{\mathcal{O}} \mathcal{O}/\mathfrak{b}$ (see Proposition 3.7(a)). As $U\colon\mathfrak{b}$ is a finitely generated $\mathcal{O}$-module of rank n whose torsion submodule is cyclic and contains $E[\mathfrak{b}]$, we have

$$U\colon\mathfrak{b} \cong_{\mathcal{O}} M \oplus (\mathcal{O}/\mathfrak{c})$$

where M is a finitely generated projective $\mathcal{O}$-module of rank n and $\mathfrak{c}$ is a nonzero ideal of $\mathcal{O}$ divisible by $\mathfrak{b}$. Then

$$\frac{U\colon\mathfrak{b}}{\mathfrak{b}\cdot(U\colon\mathfrak{b})} \cong_{\mathcal{O}/\mathfrak{b}} (M/\mathfrak{b}M) \oplus (\mathcal{O}/\mathfrak{b}),$$

which is $\mathcal{O}/\mathfrak{b}$-projective of rank $n+1$. As projective modules of constant rank over finite commutative rings are free, we have

$$\frac{U:\mathfrak{b}}{\mathfrak{b}\cdot(U:\mathfrak{b})} \cong_{\mathcal{O}} (\mathcal{O}/\mathfrak{b})^{n+1}. \tag{$*$}$$

Now, since every $f \in H_{\mathfrak{b}}$ is annihilated by $\mathfrak{b}$, we may identify $H_{\mathfrak{b}}$ with a subgroup of

$$\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{b}}{\mathfrak{b}\cdot(U:\mathfrak{b})}, E[\mathfrak{b}]\right),$$

so that $(*)$ and the identity $E[\mathfrak{b}] \cong_{\mathcal{O}} \mathcal{O}/\mathfrak{b}$ imply that $H_{\mathfrak{b}}$ may be identified with a subgroup of $(\mathcal{O}/\mathfrak{b})^{n+1}$. As $G_{\mathfrak{b}}$ is a subgroup of $H_{\mathfrak{b}}$, we see that $G_{\mathfrak{b}}$ may be identified with a subgroup of $(\mathcal{O}/\mathfrak{b})^{n+1}$. Then using that $\mathcal{O}$ is quadratic over $\mathbf{Z}$, we obtain

$$G_{\mathfrak{b}}/(m\cdot G_{\mathfrak{b}}) \cong_{\mathcal{O}} G_{\mathfrak{b}}[m] \subset ((\mathcal{O}/\mathfrak{b})[m])^{n+1},$$

so that $G_{\mathfrak{b}}/(m\cdot G_{\mathfrak{b}})$ has order dividing m^{2n+2}.

We conclude that for every nonzero ideal $\mathfrak{b}$ of $\mathcal{O}$ dividing $\mathfrak{a}$ and for every $m \in \mathbf{Z}_{\geq 1}$ we have $\#G_{\mathfrak{b}}/m\,\mathrm{G}_{b} \leq m^{2n+2}$. At last, one easily checks that

$$\#\left(\varprojlim_{\mathfrak{b}} G_{\mathfrak{b}}/mG_{\mathfrak{b}}\right) \leq m^{2n+2},$$

and that

$$\varprojlim_{\mathfrak{b}} G_{\mathfrak{b}}/mG_{\mathfrak{b}} \cong_{\mathcal{O}} G/mG,$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. Hence we have

$$\#(G/mG) \leq m^{2n+2},$$

as desired. ■

Proposition 3.20. *Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then the following statements hold.*

(a) *The map $\kappa_{\mathfrak{a}}$, defined above* Lemma 3.19, *is* $\mathrm{Gal}(K(E[\mathfrak{a}])/K)$*-linear, and its image generates* $\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$ *as an* $\widehat{\mathcal{O}}/\mathfrak{a}$*-module.*

(b) *The image of* $\kappa_{\mathfrak{a}}$ *is open in* $\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$.

Proof. Let $\mathfrak{a}$ be a Steinitz ideal, and for simplicity, write $G = \mathrm{Gal}(K(U\colon\mathfrak{a})/K(E[\mathfrak{a}]))$, and $H = \mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$. Moreover, we write κ for $\kappa_{\mathfrak{a}}$. Let G' be the $\widehat{\mathcal{O}}/\mathfrak{a}$-module generated by $\kappa(G)$ inside H. We first prove the second statement of (a), namely that $G' = H$.

First, as G is compact, the subset $\kappa(G)$ is compact in H. As $\widehat{\mathcal{O}}$ is of rank 2 over $\widehat{\mathbf{Z}}$ as a module, we have $\widehat{\mathcal{O}} = \widehat{\mathbf{Z}} \cdot 1 + \widehat{\mathbf{Z}} \cdot \alpha$ for some $\alpha \in \widehat{\mathcal{O}}$. Moreover, since $\kappa(G)$ is a $\widehat{\mathbf{Z}}$-module, we have

$$G' = \kappa(G) + \kappa(G) \cdot \alpha$$

as a $\widehat{\mathbf{Z}}$-module. Then, as $\kappa(G)$ is compact and H is Hausdorff, the submodule G' of H is closed.

For $\sigma \in G$, the kernel $\ker(\kappa(\sigma))$ is equal to

$$\frac{(U\colon\mathfrak{a})^{\langle\sigma\rangle}}{\mathrm{Cyc}_{\mathfrak{a}}(U)},$$

where $(U\colon\mathfrak{a})^{\langle\sigma\rangle}$ is the group of fixed points of $U\colon\mathfrak{a}$ under the subgroup $\langle\sigma\rangle$ of G generated by σ. Hence, we have

$$\bigcap_{f\in\kappa(G)} \ker f = \frac{(U\colon\mathfrak{a})^{G}}{\mathrm{Cyc}_{\mathfrak{a}}(U)} = \frac{\mathrm{Cyc}_{\mathfrak{a}}(U)}{\mathrm{Cyc}_{\mathfrak{a}}(U)} = 0,$$

so that a fortiori

$$\bigcap_{f\in G'} \ker f = 0.$$

We will show that G' maps surjectively to $\mathrm{Hom}_{\mathcal{O}}(M, E[\mathfrak{a}])$ for all finite $\mathcal{O}$-submodules M of $\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}$.

To this end, let M be a finite $\mathcal{O}$-submodule of $\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}$. Let

$$\varphi\colon G' \longrightarrow \mathrm{Hom}_{\mathcal{O}}(M, E[\mathfrak{a}])$$

be the canonical $\mathcal{O}$-module morphism given by $f \mapsto f|_M$. As $\bigcap_{f\in G'} \ker f = 0$ (see above), one easily sees that

$$\bigcap_{f\in I} \ker f = 0,$$

where $I = \varphi(G')$. Now, let

$$\psi\colon M \longrightarrow \mathrm{Hom}_{\mathcal{O}}(I, E[\mathfrak{a}])$$

be given by $x \mapsto [f \mapsto f(x)]$. For $x \in \ker\psi$, we have

$$x \in \bigcap_{f\in I} \ker f = 0,$$

which implies that ψ is injective. Since finite modules over a Dedekind ring are direct sums of cyclic modules and the $\mathcal{O}$-module $E[\mathfrak{a}]$ is isomorphic to $(F/\mathcal{O})[\mathfrak{a}]$ (see Proposition 3.7(a)), one easily sees that for finite $\mathcal{O}$-modules X that are annihilated by $\mathfrak{a}$ we have

$$\#X = \#\,\mathrm{Hom}_{\mathcal{O}}(X, E[\mathfrak{a}]).$$

Therefore, we have

$$\#M \leq \#\,\mathrm{Hom}_{\mathcal{O}}(I, E[\mathfrak{a}]) = \#I \leq \#\,\mathrm{Hom}_{\mathcal{O}}(M, E[\mathfrak{a}]) = \#M,$$

that is, we have $I = \mathrm{Hom}_{\mathcal{O}}(M, E[\mathfrak{a}])$. Therefore, the map φ is surjective.

Now, observe that

$$H = \varprojlim_{M} \mathrm{Hom}_{\mathcal{O}}(M, E[\mathfrak{a}]),$$

where M runs over all finite $\mathcal{O}$-submodules of $\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}$, so that surjectivity of φ implies that G' is dense in the profinite group H. Then the closedness of G' in H implies that $G' = H$, which finishes the proof of the second statement of (a).

For the first statement of (a), write $\Gamma = \mathrm{Gal}(K(E[\mathfrak{a}])/K)$ and consider it as a subgroup of $(\widehat{\mathcal{O}}/\mathfrak{a})^*$. Let $x \in \Gamma$, $\sigma \in G$, and $\tau_x \in \mathrm{Gal}(K(U : \mathfrak{a})/K)$ a lift of x. Then the action of Γ on G is given by

$$x \cdot \sigma = \tau_x \sigma \tau_x^{-1}.$$

Now, let $Q \in U : \mathfrak{a}$. Recall that

$$U : \mathfrak{a} = \bigcup_{\mathfrak{b}} U : \mathfrak{b},$$

where $\mathfrak{b}$ runs over all nonzero ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. Let $\mathfrak{b}$ be a nonzero ideal of $\mathcal{O}$ dividing $\mathfrak{a}$ such that $Q \in U : \mathfrak{b}$. Then for $b \in \mathfrak{b}$ we have

$$bQ \in U \subset E(K),$$

so

$$bQ = \tau_x^{-1}(bQ) = b\tau_x^{-1}(Q).$$

Hence

$$Q - \tau_x^{-1}(Q) \in E[\mathfrak{b}] \subset E[\mathfrak{a}],$$

so that

$$\sigma(Q - \tau_x^{-1}(Q)) = Q - \tau_x^{-1}(Q).$$

It follows that

$$\sigma(Q) - Q = \sigma\tau_x^{-1}(Q) - \tau_x^{-1}(Q).$$

Thus

$$\begin{aligned}
\kappa(x \cdot \sigma)(Q + \mathrm{Cyc}_{\mathfrak{a}}(U)) &= \kappa(\tau_x \sigma \tau_x^{-1})(Q + \mathrm{Cyc}_{\mathfrak{a}}(U)) \\
&= \tau_x \sigma \tau_x^{-1}(Q) - Q \\
&= \tau_x(\sigma\tau_x^{-1}(Q) - \tau_x^{-1}(Q)) \\
&= \tau_x(\sigma(Q) - Q) \\
&= x \cdot \kappa(\sigma)(Q + \mathrm{Cyc}_{\mathfrak{a}}(U)),
\end{aligned}$$

where the latter $\cdot$ is the natural action of $\widehat{\mathcal{O}}/\mathfrak{a}$ on H. As the above holds for all $Q \in U\colon \mathfrak{a}$, we have

$$\kappa(x \cdot \sigma) = x \cdot \kappa(\sigma).$$

Hence κ is Γ-linear, as desired.

Now we prove (b). By (a) we have

$$(\widehat{\mathcal{O}}/\mathfrak{a}) \cdot \kappa(G) = H.$$

Let R be the subring of $\widehat{\mathcal{O}}/\mathfrak{a}$ generated by Γ. As κ is Γ-linear (see (a)), we have

$$R \cdot \kappa(G) = \kappa(G).$$

Then, since R is a subring of $\widehat{\mathcal{O}}/\mathfrak{a}$, the image $\kappa(G)$ is in fact an R-submodule of H. We will first show that R is open in $\widehat{\mathcal{O}}/\mathfrak{a}$, so that $(\widehat{\mathcal{O}}/\mathfrak{a})/R$ is finite.

For $\mathfrak{p}$ a maximal ideal of $\mathcal{O}$ let $i_\mathfrak{p}$ be as defined before Theorem 3.13. Then let

$$i'_\mathfrak{p} = \begin{cases} i_\mathfrak{p} + 1 & \text{if } \mathrm{N}_{F/\mathbf{Q}}(\mathfrak{p}) = 2 \text{ and } i_\mathfrak{p} = 0, \\ i_\mathfrak{p} & \text{otherwise.} \end{cases}$$

As for almost all $\mathfrak{p}$ of $\mathcal{O}$ we have $i_\mathfrak{p} = 0$ (see definition of $i_\mathfrak{p}$), we have for almost all $\mathfrak{p}$ of $\mathcal{O}$ that $i'_\mathfrak{p} = 0$. Now, for ease of notation, let $\mathcal{P}$ be the set of maximal ideals of $\mathcal{O}$ dividing $\mathfrak{a}$. Then using Theorem 3.13(b) one easily sees that the group

$$\Gamma' = \prod_{i'_\mathfrak{p}=0} \left(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}\right)^* \times \prod_{\substack{\mathrm{v}_\mathfrak{p}(\mathfrak{a}) \geq i'_\mathfrak{p} \\ i'_\mathfrak{p} > 0}} \left(1 + \mathfrak{p}^{i'_\mathfrak{p}}\left(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}\right)\right) \times \prod_{\mathrm{v}_\mathfrak{p}(\mathfrak{a}) < i'_\mathfrak{p}} \{1\}$$

is a subgroup of Γ, where each product runs over $\mathfrak{p} \in \mathcal{P}$, and where we identified the automorphism groups in Theorem 3.13(b) with their image in $(\widehat{\mathcal{O}}/\mathfrak{a})^*$.

Observe that

$$\widehat{\mathcal{O}}/\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}) \times \prod_{\substack{\mathfrak{p} \text{ maximal} \\ \mathfrak{p} \nmid \mathfrak{a}}} \{0\},$$

where $\mathfrak{p}^\infty = \{0\}$, and consider the canonical morphism

$$\varphi\colon \widehat{\mathcal{O}}/\mathfrak{a} \longrightarrow \prod_{\substack{\mathrm{v}_\mathfrak{p}(\mathfrak{a}) \geq i'_\mathfrak{p} \\ i'_\mathfrak{p} > 0}} \left(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{i'_\mathfrak{p}}\right) \times \prod_{\mathrm{v}_\mathfrak{p}(\mathfrak{a}) < i'_\mathfrak{p}} \mathcal{O}_\mathfrak{p}/\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}$$

of profinite rings, where each product runs over $\mathfrak{p} \in \mathcal{P}$, and observe that it is surjective. Observe that $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) < i'_\mathfrak{p}$ implies that $i'_\mathfrak{p} > 0$. Now, as there are only finitely many $\mathfrak{p}$ with $i'_\mathfrak{p} > 0$, the codomain of φ is finite, and therefore discrete. Hence $\ker(\varphi) = \varphi^{-1}(\{0\})$ is an open ideal of $\widehat{\mathcal{O}}/\mathfrak{a}$. We will show that

$$\ker(\varphi) \subset \Gamma' - \Gamma' = \{\gamma - \gamma' : \gamma, \gamma' \in \Gamma'\}.$$

Then, as R is a ring containing Γ', we have $\ker(\varphi) \subset R$. Therefore $\ker(\varphi)$ being open in $\widehat{\mathcal{O}}/\mathfrak{a}$ implies that R is open in $\widehat{\mathcal{O}}/\mathfrak{a}$, as desired.

Let $a = (a_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}} \in \ker(\varphi)$. We will show that for every $\mathfrak{p} \in \mathcal{P}$ there are $\gamma_\mathfrak{p}$ and $\gamma'_\mathfrak{p}$ in the $\mathfrak{p}$-th component of Γ', such that

$$a_\mathfrak{p} = \gamma_\mathfrak{p} - \gamma'_\mathfrak{p}. \tag{$*$}$$

If we restrict φ to a component where $\mathfrak{p} \in \mathcal{P}$ and $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) < i'_\mathfrak{p}$, then we have the identity map. Thus, for $\mathfrak{p} \in \mathcal{P}$ with $\mathrm{v}_\mathfrak{p}(a) < i'_\mathfrak{p}$ we have $a_\mathfrak{p} = 0$. Hence $\gamma_\mathfrak{p} = \gamma'_\mathfrak{p} = 1$ proves $(*)$ in this case.

Let $\mathfrak{p} \in \mathcal{P}$ with $i'_\mathfrak{p} > 0$ and $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) \geq i'_\mathfrak{p}$. Then we have

$$1 + a_\mathfrak{p} \in 1 + \mathfrak{p}^{i'_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}),$$

so taking $\gamma_\mathfrak{p} = 1 + a_\mathfrak{p}$ and $\gamma'_\mathfrak{p} = 1$ proves $(*)$ in this case.

At last, let $\mathfrak{p} \in \mathcal{P}$ with $i'_\mathfrak{p} = 0$. By the definition of $i'_\mathfrak{p}$ we have at least three residue classes modulo $\mathfrak{p}$. Therefore, we may choose $u_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}$ such that $u_\mathfrak{p} \not\equiv 0 \pmod{\mathfrak{p}}$ and $u_\mathfrak{p} \not\equiv a_\mathfrak{p} \pmod{\mathfrak{p}}$. Then putting $\gamma_\mathfrak{p} = u_\mathfrak{p}$ and $\gamma'_\mathfrak{p} = u_\mathfrak{p} - a_\mathfrak{p}$ proves $(*)$ in this last case as well. Hence, we have $\ker(\varphi) \subset \Gamma' - \Gamma'$, so R is open in $\widehat{\mathcal{O}}/\mathfrak{a}$, as desired.

Now, the image $\kappa(G)$ is a closed subgroup of H, so Lemma 3.19(b) states that $\kappa(G)$ is finitely generated. Thus, there is a finite subset $X \subset \kappa(G)$ such that $\overline{\langle X\rangle} = \kappa(G)$. Note that we also have $\overline{R \cdot X} = \kappa(G)$. As R is open in $\widehat{\mathcal{O}}/\mathfrak{a}$, it is also closed. Hence, by compactness of $\widehat{\mathcal{O}}/\mathfrak{a}$, the ring R is compact, so that $R \cdot X$ is compact. The latter implies that $R \cdot X$ is closed, thus $\overline{R \cdot X} = R \cdot X = \kappa(G)$. It follows that $\kappa(G)$ is finitely generated as an R-module.

Then by finiteness of $(\widehat{\mathcal{O}}/\mathfrak{a})/R$ the quotient

$$\frac{(\widehat{\mathcal{O}}/\mathfrak{a}) \cdot \kappa(G)}{R \cdot \kappa(G)} \tag{$**$}$$

is finite. By (a) we have $(\widehat{\mathcal{O}}/\mathfrak{a}) \cdot \kappa(G) = H$ and $R \cdot \kappa(G) = \kappa(G)$. Thus, the finite quotient $(**)$ is equal to $H/\kappa(G)$, which shows that $\kappa(G)$ is open in H, as desired. ■

Proof of Theorem 3.16. Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. By Proposition 3.20(b) we have that $\kappa_{\mathfrak{a}}(\mathrm{Gal}(K(U : \mathfrak{a})/K(E[\mathfrak{a}])))$ is open in $\mathrm{Hom}_{\mathcal{O}}\Big(\frac{U : \mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\Big)$.

Observe that for any $\mathcal{O}$-submodule V of $U : \mathfrak{a}$ containing $E[\mathfrak{a}]$ the map

$$\mathrm{Hom}_{\mathcal{O}}\left(\frac{U : \mathfrak{a}}{V}, E[\mathfrak{a}]\right) \longrightarrow \mathrm{Aut}_{\mathcal{O},V}(U : \mathfrak{a})$$

given by $f \mapsto [Q \mapsto Q + f(Q)]$ is an isomorphism of topological groups. Hence, we have the identification

$$\mathrm{Aut}_{\mathcal{O},U+E[\mathfrak{a}]}(U : \mathfrak{a}) = \mathrm{Hom}_{\mathcal{O}}\left(\frac{U : \mathfrak{a}}{U + E[\mathfrak{a}]}, E[\mathfrak{a}]\right).$$

Moreover, we have the inclusion

$$H_{\mathfrak{a}} = \mathrm{Hom}_{\mathcal{O}}\left(\frac{U : \mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right) \subset H'_{\mathfrak{a}} = \mathrm{Hom}_{\mathcal{O}}\left(\frac{U : \mathfrak{a}}{U + E[\mathfrak{a}]}, E[\mathfrak{a}]\right).$$

Now, by Proposition 3.18(c) the $\mathcal{O}$-module $\mathrm{Cyc}_{\mathfrak{a}}(U)/E[\mathfrak{a}]$ is finitely generated of the same $\mathcal{O}$-rank as U. Therefore, the quotient $H'_{\mathfrak{a}}/H_{\mathfrak{a}}$ is finite, so that $H_{\mathfrak{a}}$ is open in $H'_{\mathfrak{a}}$. As $\mathrm{im}(\kappa_{\mathfrak{a}})$ is open in $H_{\mathfrak{a}}$, and $H_{\mathfrak{a}}$ is open in $H'_{\mathfrak{a}}$, it follows that $\mathrm{im}(\kappa_{\mathfrak{a}})$ is open in $H'_{\mathfrak{a}}$, which proves the theorem. ■

7. Galois representations on division points

Throughout this section, let K be a number field, let $\overline{K}$ be an algebraic closure of K, let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, and let $U \subset E(K)$ be an $\mathcal{O}$-submodule.

In this section we combine Theorem 3.13 and Theorem 3.16 from the previous two sections to prove the following theorem.

Theorem 3.21. *Let K be a number field, and let E, $\mathcal{O}$, and U be as above. Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. Then $\mathrm{Gal}(K(U : \mathfrak{a})/K)$ is an open subgroup of $\mathrm{Aut}_{\mathcal{O},U}(U : \mathfrak{a})$.*

Proof. Let $\mathfrak{a}$ be a Steinitz ideal of $\mathcal{O}$. By elementary module theory over $\mathcal{O}$, we have the following short exact sequence

$$0 \longrightarrow \mathrm{Aut}_{\mathcal{O},U+E[\mathfrak{a}]}(U : \mathfrak{a}) \longrightarrow \mathrm{Aut}_{\mathcal{O},U}(U : \mathfrak{a}) \longrightarrow \mathrm{Aut}_{\mathcal{O},U[\mathfrak{a}]}(E[\mathfrak{a}]) \longrightarrow 0. \qquad (*)$$

Moreover, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(K(U : \mathfrak{a})/K(E[\mathfrak{a}])) \arrow[r] \arrow[d] & \mathrm{Gal}(K(U : \mathfrak{a})/K) \arrow[r] \arrow[d] & \mathrm{Gal}(K(E[\mathfrak{a}])/K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Aut}_{\mathcal{O},U+E[\mathfrak{a}]}(U : \mathfrak{a}) \arrow[r] & \mathrm{Aut}_{\mathcal{O},U}(U : \mathfrak{a}) \arrow[r] & \mathrm{Aut}_{\mathcal{O},U[\mathfrak{a}]}(E[\mathfrak{a}]) \arrow[r] & 0
\end{tikzcd}$$

of profinite groups, where the vertical maps are the canonical injective maps. By Theorem 3.16 the left vertical map is open, and by Theorem 3.13(a) the right vertical map is open. It follows that the middle map is open, which proves the theorem. ■

8. Existence of the density

Throughout this section, let K be a number field, let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, let W be an $\mathcal{O}$-submodule of $E(K)$, and let V be an $\mathcal{O}$-submodule of W such that $W/V \cong \mathcal{O}/I$, where I is a nonzero ideal of $\mathcal{O}$. Let $\mathcal{P}$ be the set of prime ideals of $\mathcal{O}$ dividing I, let $U = V\colon I$, and let $L = K(U)$. Let F be the fraction field of $\mathcal{O}$, and let $n = \mathrm{rk}_{\mathcal{O}}(U)$ (see Definition 3.17).

Let Ω_K be the set of maximal ideals of $\mathcal{O}_K$. Choosing a model of E over a finitely generated subring of K, we may talk about the reduction of E modulo $\mathfrak{p}$ for almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$, and denote it by $E_{\mathfrak{p}}$. For the definition of *good*, *bad*, *ordinary*, and *supersingular reduction* we refer to [Sil94].

Let S be the subset of Ω_K consisting of the primes where $E_{\mathfrak{p}}$ is not defined, the primes of bad reduction for E, the primes of supersingular reduction for E (see [Sil94]), and the primes dividing I. By [Lan87, Theorem 12, §13.4] the set of supersingular primes has density zero. As there are only finitely many primes for which $E_{\mathfrak{p}}$ is not defined, finitely many primes of bad reduction for E, and finitely many primes dividing I, the set S has density zero too.

Now, for every $\mathfrak{p} \in \Omega_K \setminus S$ we have a reduction map

$$\pi_{\mathfrak{p}}\colon W \longrightarrow E_{\mathfrak{p}}(\kappa(\mathfrak{p}))$$

of $\mathcal{O}$-modules, where $\kappa(\mathfrak{p})$ is the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$. We define

$$A(W, V) = \{\mathfrak{p} \in \Omega_K \setminus S : \ker(\pi_{\mathfrak{p}}) \subset V\},$$

for which we often simply write A.

In this section we prove the following theorem.

Theorem 3.22. *Suppose that I is not divisible by any prime number p that splits completely in $\mathcal{O}$. Then the set A has a natural density equal to*

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{\mathfrak{p}\in\mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{[L(U\colon\mathfrak{p}^i):L]} \left(1 - \frac{1}{[L((U\colon\mathfrak{p}^i),(W\colon\mathfrak{p}^{i+1})):L(U\colon\mathfrak{p}^i)]}\right).$$

The proof of this theorem, given at the end of this section, follows the same lines as the proof of Theorem 2.10.

Lemma 3.23. *Let R be a commutative ring, and let $\varphi\colon N \longrightarrow N'$ be a morphism of R-modules. Let X be an R-submodule of N such that $N/X \cong_R R/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of R. Then $\ker(\varphi) \subset X$ if and only if $\varphi(N)/\varphi(X) \cong_R R/\mathfrak{a}$.*

Proof. 'Only if': note that there is a canonical isomorphism

$$N/(X + \ker(\varphi)) \longrightarrow \varphi(N)/\varphi(X)$$

induced by φ and the projection map $\varphi(N) \longrightarrow \varphi(N)/\varphi(X)$. Hence, if $\ker(\varphi) \subset X$, then

$$\varphi(N)/\varphi(X) \cong_R N/X \cong_R R/\mathfrak{a}.$$

'If': on the other hand, suppose that $\varphi(N)/\varphi(X) \cong_R R/\mathfrak{a}$. As R is commutative, any surjective map $R/\mathfrak{a} \longrightarrow R/\mathfrak{a}$ of R-modules is an isomorphism. It follows that the canonical map

$$f\colon N/X \longrightarrow \varphi(N)/\varphi(X)$$

induced by φ and the projection map $\varphi(N) \longrightarrow \varphi(N)/\varphi(X)$ is an isomorphism. Now, the kernel of f, which is trivial, contains $(\ker(\varphi) + X)/X$, so that $\ker(\varphi) + X = X$. Hence, we have $\ker(\varphi) \subset X$, as desired. ■

Let $\varphi\colon \Omega_L \longrightarrow \Omega_K$ be given by $\mathfrak{q} \mapsto \mathfrak{q} \cap K$, and let $S' = \varphi^{-1}(S)$. Then for every $\mathfrak{q} \in \Omega_L \setminus S'$ we have the reduction map $\pi_{\mathfrak{q}}\colon U \longrightarrow E_{\mathfrak{q}}(\kappa(\mathfrak{q}))$, where $\kappa(\mathfrak{q})$ is the residue field of L at $\mathfrak{q}$. Now, since $W/V \cong_{\mathcal{O}} \mathcal{O}/I$, we have $IW \subset V$, so that $W \subset U$. Hence, we may define

$$A' = \{\mathfrak{q} \in \Omega_L \setminus S' : \ker(\pi_{\mathfrak{q}}|_W) \subset V\}.$$

Similarly to the case of S, also S' has density zero.

Lemma 3.24. *Suppose that $\mathrm{d}(A')$ exists. Then $\mathrm{d}(A)$ exists and we have*

$$\mathrm{d}(A) = \frac{1}{[L:K]}\,\mathrm{d}(A').$$

Proof. First, note that for all $\mathfrak{p} \in \Omega_K \setminus S$ and $\mathfrak{q} \in \Omega_L \setminus S'$ dividing $\mathfrak{p}$, we have $\mathfrak{p} \in A$ if and only if $\mathfrak{q} \in A'$.

Now, let $\mathfrak{p} \in A$, and let $\mathfrak{q} \in \Omega_L \setminus S'$ be a prime dividing $\mathfrak{p}$. We will show that $\mathfrak{p}$ splits completely in L.

As $\mathfrak{p}$ is of ordinary reduction, the reduction $E_\mathfrak{p}$ of E modulo $\mathfrak{p}$ has endomorphism ring $\mathcal{O}$. Moreover, by [Len96, Theorem 1] we have

$$N = E_\mathfrak{p}(\kappa(\mathfrak{p})) \cong_\mathcal{O} \mathcal{O}/(\pi - 1),$$

where π is the Frobenius endomorphism of $E_\mathfrak{p}$. As $\mathcal{O}$ is Dedekind, every submodule of the cyclic module N is again cyclic. Therefore $\pi_\mathfrak{p}(W)$ and $\pi_\mathfrak{p}(V)$ are cyclic. Now, since $\mathfrak{p} \in A$, we have $\ker(\pi_\mathfrak{p}) \subset V$, so Lemma 3.23 implies that

$$\pi_\mathfrak{p}(W)/\pi_\mathfrak{p}(V) \cong_\mathcal{O} \mathcal{O}/I.$$

Hence, by cyclicity $\pi_\mathfrak{p}(V) = I\pi_\mathfrak{p}(W)$, so that $\pi_\mathfrak{p}(V) \subset IN$. Let $M = E_\mathfrak{p}(\overline{\kappa(\mathfrak{p})})$ where $\overline{\kappa(\mathfrak{p})}$ is an algebraic closure of the residue field $\kappa(\mathfrak{p})$. By Proposition 3.3(a) we have

$$\pi_\mathfrak{p}(V) :_M I \subset N + M[I].$$

Moreover, since $N \cong_\mathcal{O} \mathcal{O}/(\pi - 1)$, we have $(\pi - 1) \subset I$. Then $\mathcal{O}/(\mathfrak{p} - 1)$ maps surjectively to $\mathcal{O}/I$, so that $M[I] \subset N$. It follows that $\pi_\mathfrak{p}(V) :_M I \subset N$. We conclude that $\mathfrak{p}$ splits completely in L.

Thus, for $x \in \mathbf{R}_{\geq 1}$ we have

$$\#\{\mathfrak{q} \in \Omega_L : \mathfrak{q} \in A' \wedge \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q}) \leq x\} = [L : K] \cdot \#\{\mathfrak{p} \in \Omega_K : \mathfrak{p} \in A \wedge \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}.$$

Hence, we have

$$\begin{aligned}
\mathrm{d}(A') &= \lim_{x\to\infty} \frac{\#\{\mathfrak{q}\in\Omega_L : \mathfrak{q}\in A' \text{ and } \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\le x\}}{\#\{\mathfrak{q}\in\Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\le x\}}\\
&= \lim_{x\to\infty} \frac{[L:K]\#\{\mathfrak{p}\in\Omega_K : \mathfrak{p}\in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\le x\}}{\#\{\mathfrak{q}\in\Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\le x\}}\\
&= [L:K]\lim_{x\to\infty} \frac{\#\{\mathfrak{p}\in\Omega_K : \mathfrak{p}\in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\le x\}}{\#\{\mathfrak{q}\in\Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\le x\}}.
\end{aligned}$$

As

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{q}\in\Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\le x\}}{\#\{\mathfrak{p}\in\Omega_K : \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\le x\}} = 1,$$

we have

$$\begin{aligned}
\mathrm{d}(A') &= [L:K]\lim_{x\to\infty} \frac{\#\{\mathfrak{p}\in\Omega_K : \mathfrak{p}\in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\le x\}}{\#\{\mathfrak{q}\in\Omega_L : \mathrm{N}_{L/\mathbf{Q}}(\mathfrak{q})\le x\}}\\
&= [L:K]\lim_{x\to\infty} \frac{\#\{\mathfrak{p}\in\Omega_K : \mathfrak{p}\in A \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\le x\}}{\#\{\mathfrak{p}\in\Omega_K : \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{p})\le x\}}\\
&= [L:K]\,\mathrm{d}(A).
\end{aligned}$$

It follows that $\mathrm{d}(A)$ exists and that $\mathrm{d}(A) = \frac{1}{[L:K]}\,\mathrm{d}(A')$. ■

Lemma 3.25. *We have* $A' = \{\mathfrak{q}\in\Omega_L\setminus S' : \pi_{\mathfrak{q}}(W) = \pi_{\mathfrak{q}}(U)\}$.

Proof. Let $\mathfrak{q}\in\Omega_L\setminus S'$, and recall that S' has density zero. As $\mathfrak{q}$ is of ordinary reduction, the reduction $E_{\mathfrak{q}}$ of E modulo $\mathfrak{q}$ has endomorphism ring $\mathcal{O}$. Moreover, by [Len96, Theorem 1] we have

$$N = E_{\mathfrak{q}}(\kappa(\mathfrak{q})) \cong_{\mathcal{O}} \mathcal{O}/(\pi-1),$$

where π is the Frobenius endomorphism of $E_{\mathfrak{q}}$. Since $\mathcal{O}$ is Dedekind, every submodule of the cyclic module N is again cyclic.

By Proposition 3.3(b) we have $I\cdot U = V$, and by $\mathcal{O}$-linearity of $\pi_{\mathfrak{q}}$ we have

$$\pi_{\mathfrak{q}}(I\cdot U) = I\cdot\pi_{\mathfrak{q}}(U).$$

Therefore

$$\pi_{\mathfrak{q}}(U)/\pi_{\mathfrak{q}}(V) = \pi_{\mathfrak{q}}(U)/(I\pi_{\mathfrak{q}}(U)).$$

On the other hand $E[I] \subset U$ and $E_{\mathfrak{q}}[I] \subset \pi_{\mathfrak{q}}(U) \subset N$, so that the cyclicity of N implies that

$$\pi_{\mathfrak{q}}(U)/\pi_{\mathfrak{q}}(V) \cong_{\mathcal{O}} \mathcal{O}/I.$$

It follows that $\pi_{\mathfrak{q}}(W) = \pi_{\mathfrak{q}}(U)$ if and only if $\pi_{\mathfrak{q}}(W)/\pi_{\mathfrak{q}}(V) \cong_{\mathcal{O}} \mathcal{O}/I$. By Lemma 3.23, the latter holds if and only if $\ker(W \longrightarrow E(\kappa(\mathfrak{q}))) \subset V$. ■

Proof of Theorem 3.22. As $W \subset U$, we have for every $\mathfrak{p} \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$ that

$$W\!:\mathfrak{p}^i \subset U\!:\mathfrak{p}^i.$$

Let $M = L(V\!:I^\infty) = L(W\!:I^\infty) = L(U\!:I^\infty)$ and note that

$$M = L(U\!:\mathfrak{p}^\infty : \mathfrak{p} \in \mathcal{P}).$$

For $\mathfrak{p} \in \mathcal{P}$ with residue characteristic p, the finite subfields of $L(U\!:\mathfrak{p}^\infty)$ have p-power degree over L. Hence, since I is not divisible by two distinct primes having the same residue characteristic, we have for distinct $\mathfrak{p}$ and $\mathfrak{q}$ in $\mathcal{P}$ that

$$L(U\!:\mathfrak{p}^\infty) \cap L(U\!:\mathfrak{q}^\infty) = L.$$

It follows that $G = \operatorname{Gal}(M/L)$ decomposes as a product over $\mathfrak{p} \in \mathcal{P}$ of the Galois groups $G_{\mathfrak{p}} = \operatorname{Gal}(L(U\!:\mathfrak{p}^\infty)/L)$, that is, we have $G = \prod_{\mathfrak{p}\in\mathcal{P}} G_{\mathfrak{p}}$. Now, for all $\mathfrak{p} \in \mathcal{P}$ and $i \in \mathbf{Z}_{\geq 0}$ let

$$G_{\mathfrak{p},i} = \operatorname{Gal}(M/L(U\!:\mathfrak{p}^i)),$$

let

$$H_{\mathfrak{p},i} = \operatorname{Gal}(M/L((U\!:\mathfrak{p}^i),(W\!:\mathfrak{p}^{i+1}))) \subset G_{\mathfrak{p},i},$$

and note that we have

$$\cdots \subset G_{\mathfrak{p},i+1} \subset H_{\mathfrak{p},i} \subset G_{\mathfrak{p},i} \subset \cdots$$

by the above. Define

$$C_{\mathfrak{p},i} = G_{\mathfrak{p},i} \setminus H_{\mathfrak{p},i},$$

and

$$C_{\mathfrak{p}} = \bigcup_{i=0}^{\infty} C_{\mathfrak{p},i}.$$

One easily sees that $C_{\mathfrak{p}}$ is a disjoint union of sets $C_{\mathfrak{p},i}$. At last, define

$$C = \bigcap_{\mathfrak{p}\in\mathcal{P}} C_{\mathfrak{p}}.$$

To prove that C is closed under conjugation in G, open in G, and that $\lambda(\partial C) = 0$, where λ is the Haar measure on G, one easily imitates the Galois theoretic proofs of lemma's 2.14, and 2.15.

The rest of the proof is an imitation of the proof of Theorem 2.10. One uses Lemma 3.25 to show that $\mathrm{d}(A') = \lambda(C)$. Then by Lemma 3.24 and the decomposition

$$G = \prod_{\mathfrak{p}\in\mathcal{P}} \mathrm{Gal}(L(U : \mathfrak{p}^{\infty})/L),$$

one finds

$$\mathrm{d}(A) = \frac{1}{[L:K]} \prod_{\mathfrak{p}\in\mathcal{P}} \sum_{i=0}^{\infty} \frac{1}{[L(U : \mathfrak{p}^{i}) : L]} \left(1 - \frac{1}{[L((U : \mathfrak{p}^{i}), (W : \mathfrak{p}^{i+1})) : L(U : \mathfrak{p}^{i})]}\right),$$

as desired. ■

9. Rationality of the density

Throughout this section, let K be a number field, and let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain. Let W be an $\mathcal{O}$-submodule of $E(K)$, and let V be an $\mathcal{O}$-submodule of W such that $W/V \cong \mathcal{O}/I$ where I is a nonzero ideal of $\mathcal{O}$. Let $\mathcal{P}$ be the set of prime ideals of $\mathcal{O}$ dividing I, let $U = V : I$, and let $L = K(U)$. Let F be the fraction field of $\mathcal{O}$, and let $n = \mathrm{rk}_{\mathcal{O}}(U)$ (see Definition 3.17). Write N for the field norm $\mathrm{N}_{F/\mathbf{Q}}$.

In this section we prove the following theorem.

Theorem 3.26. *Suppose that I is not divisible by any prime number p that splits completely in $\mathcal{O}$. Let $(j_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $\mathfrak{p} \in \mathcal{P}$*

$$\mathrm{Aut}_{\mathcal{O},U:\mathfrak{p}^{j_{\mathfrak{p}}}}(U:\mathfrak{p}^{\infty}) \subset \mathrm{Gal}(L(U:\mathfrak{p}^{\infty})/L).$$

Then the density $\mathrm{d}(A(W,V))$ equals

$$\tfrac{1}{[L:K]} \textstyle\prod_{\mathfrak{p}\in\mathcal{P}} \Big[\tfrac{1}{[L(U:\mathfrak{p}^{j_{\mathfrak{p}}}):L]} \cdot \tfrac{\mathrm{N}(\mathfrak{p})^n(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1} + \textstyle\sum_{i=0}^{j_{\mathfrak{p}}-1} \Big(\tfrac{1}{[L(U:\mathfrak{p}^i):L]} - \tfrac{1}{[L(U:\mathfrak{p}^i, W:\mathfrak{p}^{i+1}):L]} \Big) \Big].$$

We remark that $(j_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{P}}$, as in the theorem above, exist by Theorem 3.21.

Lemma 3.27. *Let $\mathfrak{p} \in \mathcal{P}$, and let $i \in \mathbf{Z}_{\geq 0}$. Then the following hold.*

(a) *The degree $[L(U:\mathfrak{p}^{i+1}) : L(U:\mathfrak{p}^i)]$ divides $\mathrm{N}(\mathfrak{p})^{n+1}$, and if $i \geq j_{\mathfrak{p}}$, it is equal to $\mathrm{N}(\mathfrak{p})^{n+1}$.*

(b) *The degree $[L(U:\mathfrak{p}^i, W:\mathfrak{p}^{i+1}) : L(U:\mathfrak{p}^i)]$ divides $\mathrm{N}(\mathfrak{p})$, and if $i \geq j_{\mathfrak{p}}$, it is equal to $\mathrm{N}(\mathfrak{p})$.*

Proof. Write $X = U:\mathfrak{p}^{i+1}$. By Proposition 3.3(b) we have $\mathfrak{p}X = U:\mathfrak{p}^i$. Then the inclusions $E[\mathfrak{p}] \subset U \subset \mathfrak{p}X$ imply that the morphism

$$f\colon\ \mathrm{Aut}_{\mathcal{O},\mathfrak{p}X}(X) \longrightarrow \mathrm{Hom}_{\mathcal{O}}(X/\mathfrak{p}X, E[\mathfrak{p}])$$

of groups given by $\sigma \mapsto [x+\mathfrak{p}X \mapsto \sigma(x)-x]$ is an isomorphism. As X is a finitely generated $\mathcal{O}$-module of rank n whose torsion submodule is cyclic and contains $E[\mathfrak{p}]$, we have

$$X \cong_{\mathcal{O}} M \oplus (\mathcal{O}/\mathfrak{b}),$$

where $\mathfrak{b}$ is an ideal of $\mathcal{O}$ divisible by $\mathfrak{p}$ and M is a finitely generated projective $\mathcal{O}$-module of rank n. It follows that

$$X/\mathfrak{p}X \cong_{\mathcal{O}} (\mathcal{O}/\mathfrak{p})^{n+1}.$$

Since $E[\mathfrak{p}] \cong_{\mathcal{O}} \mathcal{O}/\mathfrak{p}$ and $\#(\mathcal{O}/\mathfrak{p}) = \mathrm{N}(\mathfrak{p})$, the group $\mathrm{Aut}_{\mathcal{O},\mathfrak{p}X}(X)$ has order $\mathrm{N}(\mathfrak{p})^{n+1}$.

Now, recall that we have an injective morphism

$$\varphi\colon\ \mathrm{Gal}(L(X)/L(\mathfrak{p}X)) \longrightarrow \mathrm{Aut}_{\mathcal{O},\mathfrak{p}X}(X)$$

of groups, implying that $[L(X) : L(\mathfrak{p}X)]$ divides $\mathrm{N}(\mathfrak{p})^{n+1}$. Moreover, if $i \in \mathbf{Z}_{\geq j_{\mathfrak{p}}}$, then one easily checks that φ is an isomorphism. The latter shows that

$$[L(X) : L(\mathfrak{p}X)] = \mathrm{N}(\mathfrak{p})^{n+1},$$

which proves (a).

To prove (b), write

$$Y = W : \mathfrak{p}^{i+1},$$

and observe that $\mathrm{Gal}(L(\mathfrak{p}X, Y)/L(\mathfrak{p}X))$ maps injectively to $\mathrm{Aut}_{\mathcal{O},\mathfrak{p}X}(Y + \mathfrak{p}X)$. One easily checks that

$$\mathrm{Aut}_{\mathcal{O},\mathfrak{p}X}(Y + \mathfrak{p}X) \longrightarrow \mathrm{Hom}_{\mathcal{O}}\left(\frac{Y + \mathfrak{p}X}{\mathfrak{p}X}, E[\mathfrak{p}]\right)$$

sending $\sigma \mapsto [x + \mathfrak{p}X \mapsto \sigma(x) - x]$ is an isomorphism, and that

$$\frac{Y + \mathfrak{p}X}{\mathfrak{p}X} \cong_{\mathcal{O}} \frac{Y}{Y \cap \mathfrak{p}X}$$

holds. Therefore, for the first statement of (b) it suffices to show $\mathrm{Hom}_{\mathcal{O}}\left(\frac{Y+\mathfrak{p}X}{\mathfrak{p}X}, E[\mathfrak{p}]\right)$ has order dividing $\mathrm{N}(\mathfrak{p})$. We will show that the order of $Y/(Y \cap \mathfrak{p}X)$ equals $\mathrm{N}(\mathfrak{p})$, which finishes the proof of the first statement of (b).

To this end, recall that $U = V : I$, so that $I \cdot U = V$. We claim that

$$Y/(V : \mathfrak{p}^{i+1}) \cong_{\mathcal{O}} \mathcal{O}/I, \tag{$*$}$$

and prove it as follows.

As Y is a finitely generated $\mathcal{O}$-module of rank n whose torsion submodule is cyclic and contains $E[\mathfrak{p}^{i+1}]$, we have

$$Y \cong_{\mathcal{O}} N \oplus (\mathcal{O}/\mathfrak{c}),$$

where $\mathfrak{c}$ is an ideal of $\mathcal{O}$ divisible by $\mathfrak{p}^{i+1}$ and N is a finitely generated projective $\mathcal{O}$-module of rank n. It follows that

$$\frac{Y}{\mathfrak{p}^{i+1}Y} \cong_{\mathcal{O}} (\mathcal{O}/\mathfrak{p}^{i+1})^{n+1}.$$

By Proposition 3.3(b) we have $\mathfrak{p}^{i+1}Y = W$, so that the index $(Y : W)$ of W in Y equals $\mathrm{N}(\mathfrak{p}^{i+1})^{n+1}$. Similarly, one shows that

$$\big((V : \mathfrak{p}^{i+1}) : V\big) = \mathrm{N}(\mathfrak{p}^{i+1})^{n+1}.$$

Now, observe that

$$(Y : V) = (Y : W) \cdot (W : V)$$

and

$$(Y : V) = \big(Y : (V : \mathfrak{p}^{i+1})\big) \cdot \big((V : \mathfrak{p}^{i+1}) : V\big),$$

from which it follows that

$$(Y : (V : \mathfrak{p}^{i+1})) = (W : V) = \mathrm{N}(I).$$

Moreover, the annihilator of $Y/(V : \mathfrak{p}^{i+1})$ is equal to I. Indeed, from $I \cdot W \subset V$ we see $I \cdot Y \subset V : \mathfrak{p}^{i+1}$. Conversely, for $x \in \mathcal{O}$ with

$$x \cdot \left(\frac{Y}{V : \mathfrak{p}^{i+1}}\right) = 0,$$

we have

$$x \cdot Y \subset V : \mathfrak{p}^{i+1}.$$

Multiplying the latter by $\mathfrak{p}^{i+1}$ and using Proposition 3.3(b) we see that $x \cdot W \subset V$, which implies that $x \in I$.

Thus, we have that $Y/(V : \mathfrak{p}^{i+1})$ has order $\mathrm{N}(I)$ and its $\mathcal{O}$-annihilator equals I. As up to isomorphism there is only one $\mathcal{O}$-module of order $\mathrm{N}(I)$ and with $\mathcal{O}$-annihilator I, namely $\mathcal{O}/I$, this finishes the proof of the claim $(*)$.

Observe that we have the following inclusions

$$V : \mathfrak{p}^{i+1} \subset \mathfrak{p}Y + \big(V : \mathfrak{p}^{i+1}\big) \subset Y \cap \mathfrak{p}X \subset Y.$$

Then by $(*)$ we have that $Y/(Y \cap \mathfrak{p}X)$ is cyclic. Moreover, as $\frac{Y}{\mathfrak{p}Y + (V : \mathfrak{p}^{i+1})}$ is annihilated by $\mathfrak{p}$, it follows that $Y/(Y \cap \mathfrak{p}X)$ is also annihilated by $\mathfrak{p}$. Therefore $Y/(Y \cap \mathfrak{p}X)$ is a vector space of dimension 0 or 1 over $\mathcal{O}/\mathfrak{p}$, so that $Y/(Y \cap \mathfrak{p}X)$ has order 1 or $\mathrm{N}(\mathfrak{p})$.

Suppose that $Y/(Y \cap \mathfrak{p}X)$ has order 1. Then by definition of Y and X we have

$$W : \mathfrak{p}^{i+1} \subset \mathfrak{p}(U : \mathfrak{p}^{i+1}).$$

Multiplying by $\mathfrak{p}^{i+1}$ and using Proposition 3.3(b) we find

$$W \subset \mathfrak{p}U = \mathfrak{p}(V : I).$$

Writing $I = J\mathfrak{p}$ for some ideal J of $\mathcal{O}$, we obtain

$$W \subset \mathfrak{p}((V : J) : \mathfrak{p}) = V : J,$$

so that $JW \subset V$. However, the latter means $J \cdot (W/V) = 0$, which is a contradiction, since W/V has annihilator I and J strictly contains I. It follows that $Y/(Y \cap \mathfrak{p}X)$ has order $\mathrm{N}(\mathfrak{p})$, as desired. We conclude that

$$[L(\mathfrak{p}X, Y) : L(\mathfrak{p}X)] \mid \mathrm{N}(\mathfrak{p}).$$

Now, note that we have the equality

$$\#(X/\mathfrak{p}X) = \#\left(\frac{Y + \mathfrak{p}X}{\mathfrak{p}X}\right) \cdot \#\left(\frac{X}{Y + \mathfrak{p}X}\right),$$

where by the above we have

$$\#(X/\mathfrak{p}X) = \mathrm{N}(\mathfrak{p})^{n+1} \quad \text{and} \quad \#\left(\frac{Y+\mathfrak{p}X}{\mathfrak{p}X}\right) = \mathrm{N}(\mathfrak{p}),$$

so that

$$\#\left(\frac{X}{Y+\mathfrak{p}X}\right) = \mathrm{N}(\mathfrak{p})^{n}.$$

Then

$$[L(X) : L(\mathfrak{p}X, Y)] \mid \mathrm{N}(\mathfrak{p})^{n}.$$

Suppose that $i \in \mathbf{Z}_{\geq j_{\mathfrak{p}}}$. Then by (a) we have $[L(X) : L(\mathfrak{p}X)] = \mathrm{N}(\mathfrak{p})^{n+1}$. As $[L(X) : L(\mathfrak{p}X, Y)]$ divides $\mathrm{N}(\mathfrak{p})^{n}$ and $[L(\mathfrak{p}X, Y) : L(\mathfrak{p}X)]$ divides $\mathrm{N}(\mathfrak{p})$, it follows that $[L(X) : L(\mathfrak{p}X, Y)] = \mathrm{N}(\mathfrak{p})^{n}$ and $[L(\mathfrak{p}X, Y) : L(\mathfrak{p}X)] = \mathrm{N}(\mathfrak{p})$. ■

Proof of Theorem 3.26. This is completely analogous to the proof of Theorem 2.21, using Theorem 3.22 instead of Theorem 2.10 and Lemma 3.27 instead of Lemma 2.23. ■

10. Main theorem

Let K be a number field, and let E be an elliptic curve over K with $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain. Let $W \subset E(K)$ be an $\mathcal{O}$-submodule, and let $V \subset W$ be an $\mathcal{O}$-submodule such that $W/V \cong_{\mathcal{O}} \mathcal{O}/I$ where I is a nonzero ideal of $\mathcal{O}$. Let $U = V : I$, and let $L = K(U)$. Let $n = \mathrm{rk}_{\mathcal{O}}(W)$ (see Definition 3.17), and let $\mathcal{P}$ be the set of prime ideals of $\mathcal{O}$ dividing I.

Let $(j_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{P}} \in (\mathbf{Z}_{\geq 0})^{\mathcal{P}}$ such that for every $\mathfrak{p} \in \mathcal{P}$ we have

$$\mathrm{Aut}_{\mathcal{O}, U : \mathfrak{p}^{j_{\mathfrak{p}}}}(U : \mathfrak{p}^{\infty}) \subset \mathrm{Gal}(L(U : \mathfrak{p}^{\infty})/L).$$

We remark that such $j_{\mathfrak{p}}$ exist by Theorem 3.21.

Theorem 3.28. *Suppose that I is not divisible by any prime number p that splits completely in $\mathcal{O}$. Let $A(W, V)$ be defined as above* Theorem 3.22*. Then the following statements hold.*

(a) *The density* $\mathrm{d}(A(W,V))$ *exists and equals a positive rational number in the interval*

$$\left[\tfrac{1}{[L:K]}\cdot\prod_{\mathfrak{p}\in\mathcal{P}}\tfrac{\mathrm{N}(\mathfrak{p})-1}{\mathrm{N}(\mathfrak{p})^{n(j_\mathfrak{p}-1)+j_\mathfrak{p}}(\mathrm{N}(\mathfrak{p})^{n+1}-1)},\prod_{\mathfrak{p}\in\mathcal{P}}\left(1-\tfrac{\mathrm{N}(\mathfrak{p})^{n}-1}{\mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}}\cdot(\mathrm{N}(\mathfrak{p})^{n+1}-1)}\right)\right]$$

whose denominator divides

$$[L:K]\prod_{\mathfrak{p}\in\mathcal{P}}\left(\mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}}\cdot\frac{\mathrm{N}(\mathfrak{p})^{n+1}-1}{\mathrm{N}(\mathfrak{p})-1}\right).$$

(b) $\mathrm{d}(A(W,V))=1$ *if and only if* $V=W$ *or* W *is finite.*

Observe that Theorem 13 in Section 3.1 follows from the above theorem.

Proof. By Theorem 3.26 we have that $\mathrm{d}(A(W,V))$ exists and is equal to

$$\tfrac{1}{[L:K]}\prod_{\mathfrak{p}\in\mathcal{P}}\left[\tfrac{1}{[L(U:\mathfrak{p}^{j_\mathfrak{p}}):L]}\cdot\tfrac{\mathrm{N}(\mathfrak{p})^{n}(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1}+\sum_{i=0}^{j_\mathfrak{p}-1}\left(\tfrac{1}{[L(U:\mathfrak{p}^{i}):L]}-\tfrac{1}{[L(U:\mathfrak{p}^{i},W:\mathfrak{p}^{i+1}):L]}\right)\right],$$

which is rational.

Now, let $\mathfrak{p}\in\mathcal{P}$. By Lemma 3.27 we have for all $i\in\mathbf{Z}_{\geq 0}$ that

$$[L(U:\mathfrak{p}^{i+1}):L(U:\mathfrak{p}^{i})]\mid\mathrm{N}(\mathfrak{p})^{n+1}$$

and

$$[L(U:\mathfrak{p}^{i},W:\mathfrak{p}^{i+1}):L(U:\mathfrak{p}^{i})]\mid\mathrm{N}(\mathfrak{p}).$$

To ease the notation, for $i\in\mathbf{Z}_{\geq 0}$ write

$$T_i=\frac{1}{[L(U:\mathfrak{p}^{i}):L]}-\frac{1}{[L(U:\mathfrak{p}^{i},W:\mathfrak{p}^{i+1}):L]},$$

and note that

$$T_i=\frac{1}{[L(U:\mathfrak{p}^{i}):L]}\left(1-\frac{1}{[L(U:\mathfrak{p}^{i},W:\mathfrak{p}^{i+1}):L(U:\mathfrak{p}^{i})]}\right).$$

Hence $[L(U\colon\mathfrak{p}^i, W\colon\mathfrak{p}^{i+1}) : L(U\colon\mathfrak{p}^i)] = 1$ implies $T_i = 0$. Using Lemma 3.27 we obtain for $\mathfrak{p} \in \mathcal{P}$ that

$$\frac{1}{[L(U\colon\mathfrak{p}^{j_\mathfrak{p}}) : L]} \cdot \frac{\mathrm{N}(\mathfrak{p})^n(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1} + \sum_{i=0}^{j_\mathfrak{p}-1} T_i$$

is greater than or equal to

$$\frac{1}{\mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}}} \cdot \frac{\mathrm{N}(\mathfrak{p})^{n+1}-\mathrm{N}(\mathfrak{p})^n}{\mathrm{N}(\mathfrak{p})^{n+1}-1} = \frac{\mathrm{N}(\mathfrak{p})-1}{\mathrm{N}(\mathfrak{p})^{n(j_\mathfrak{p}-1)+j_\mathfrak{p}}(\mathrm{N}(\mathfrak{p})^{n+1}-1)}.$$

Thus, we have the lower bound

$$\mathrm{d}(A(W,V)) \geq \frac{1}{[L:K]} \cdot \prod_{\mathfrak{p}\in\mathcal{P}} \frac{\mathrm{N}(\mathfrak{p})-1}{\mathrm{N}(\mathfrak{p})^{n(j_\mathfrak{p}-1)+j_\mathfrak{p}}(\mathrm{N}(\mathfrak{p})^{n+1}-1)}.$$

For the upper bound, we have for $i \in \mathbf{Z}_{\geq 0}$

$$L(U\colon\mathfrak{p}^i, W\colon\mathfrak{p}^{i+1}) \subset L(U\colon\mathfrak{p}^{i+1}),$$

so that

$$\sum_{i=0}^{j_\mathfrak{p}-1} T_i \leq 1 - \frac{1}{[L(U\colon\mathfrak{p}^{j_\mathfrak{p}}) : L]}.$$

Then for $\mathfrak{p} \in \mathcal{P}$, write $d_\mathfrak{p} = [L(U\colon\mathfrak{p}^{j_\mathfrak{p}}) : L]$ and note that we have

$$\begin{aligned} \frac{1}{d_\mathfrak{p}} \cdot \frac{\mathrm{N}(\mathfrak{p})^n(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1} + \sum_{i=0}^{j_\mathfrak{p}-1} T_i &\leq \frac{1}{d_\mathfrak{p}} \cdot \frac{\mathrm{N}(\mathfrak{p})^n(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1} + 1 - \frac{1}{d_\mathfrak{p}} \\ &\leq 1 - \frac{1}{\mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}}}\left(1 - \frac{\mathrm{N}(\mathfrak{p})^n(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1}\right) \\ &= 1 - \frac{\mathrm{N}(\mathfrak{p})^n - 1}{\mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}} \cdot (\mathrm{N}(\mathfrak{p})^{n+1}-1)}, \end{aligned}$$

where we use that $d_\mathfrak{p} = [L(U\colon\mathfrak{p}^{j_\mathfrak{p}}) : L] \leq \mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}}$ (see Lemma 3.27). Thus, as $[L:K] \geq 1$, an upper bound for $\mathrm{d}(A(W,V))$ is

$$\prod_{\mathfrak{p}\in\mathcal{P}}\left(1 - \frac{\mathrm{N}(\mathfrak{p})^n - 1}{\mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}} \cdot (\mathrm{N}(\mathfrak{p})^{n+1}-1)}\right).$$

Now, we want to find $x \in \mathbf{Z}_{\geq 1}$ such that $x \cdot \mathrm{d}(A(W,V)) \in \mathbf{Z}$. By Lemma 3.27 we have

$$\mathrm{N}(\mathfrak{p})^{(n+1)j_{\mathfrak{p}}} \cdot [L(U : \mathfrak{p}^{j_{\mathfrak{p}}}) : L]^{-1} \in \mathbf{Z}.$$

As for $i \in \{0, \dots, j_{\mathfrak{p}} - 1\}$ the fields $L(U : \mathfrak{p}^{i})$ and $L(U : \mathfrak{p}^{i}, W : \mathfrak{p}^{i+1})$ are contained in $L(U : \mathfrak{p}^{j_{\mathfrak{p}}})$, we have

$$\mathrm{N}(\mathfrak{p})^{(n+1)j_{\mathfrak{p}}} \cdot \sum_{i=0}^{j_{\mathfrak{p}}-1} T_i \in \mathbf{Z}.$$

It follows that the denominator of $\mathrm{d}(A(W,V))$ divides

$$[L : K] \prod_{\mathfrak{p} \in \mathcal{P}} \left(\mathrm{N}(\mathfrak{p})^{(n+1)j_{\mathfrak{p}}} \cdot \frac{\mathrm{N}(\mathfrak{p})^{n+1} - 1}{\mathrm{N}(\mathfrak{p}) - 1} \right),$$

which finishes the proof of (a).

From the lower bound, we see that $\mathrm{d}(A(W,V))$ is nonzero. From the upper bound, we see that $\mathrm{d}(A(W,V)) = 1$ only if $I = \mathcal{O}$ or $n = 0$, that is, only if $V = W$ or W is finite. On the other hand, if $V = W$ or W is finite, we easily see that $\mathrm{d}(A(W,V)) = 1$, which finishes the proof of (b). ■

Bibliography

[Bar10] S. Barańczuk, *On a generalization of the support problem of Erdös and its analogues for abelian varieties and K-theory*, Journal of Pure and Applied Algebra **214** (2010), 380–384.

[Bau01] H. Bauer, *Measure and integration theory*, Walter de Gruyter, 2001.

[BGK05] G. Banaszak, W. Gajda, and P. Krason, *Detecting linear dependence by reduction maps*, Journal of Number Theory **115** (2005), 322–342.

[Coh96] H. Cohen, *A course in computational algebraic number theory*, third ed., Springer, 1996.

[CRS97] C. Corrales-Rodrigáñez and R. Schoof, *The support problem and its elliptic analogue*, Journal of Number Theory **64** (1997), 276–290.

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

[Hil96] D. Hilbert, *Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1896), 29–39.

[HR79] E. Hewitt and K.A. Ross, *Abstract harmonic analysis, vol. I*, second ed., Springer-Verlag, 1979.

[Hu52] S. Hu, *Cohomology theory in topological groups*, Michigan Mathematical Journal **1** (1952), 11–59.

[Iwa53] K. Iwasawa, *A note on Kummer extensions*, Journal of the Mathematical Society of Japan **5** (1953), 253–262.

[Jav13] A. Javanpeykar, *Radical Galois groups and cohomology*, Master's thesis, 2013, `http://www.math.leidenuniv.nl/scripties/1MasterJavanpeykar.pdf`.

[Kha03] C. Khare, *Compatible systems of mod p Galois representations and Hecke characters*, Mathematical Research Letters **10** (2003), 71–83.

[Lam91] T.Y. Lam, *A first course in noncommutative rings*, Springer-Verlag, 1991.

[Lan87] S. Lang, *Elliptic functions*, second ed., Springer-Verlag, 1987.

[Lan02] ______, *Algebra*, revised third ed., Springer-Verlag, 2002.

[Lar02] M. Larsen, *The support problem for abelian varieties*, Journal of Number Theory **101** (2002), 398–403.

[Len96] H.W. Lenstra, *Complex multiplication structure of elliptic curves*, Journal of Number Theory **56** (1996), 227–241.

[Len07] H. W. Lenstra, *Commentary on H: Divisibility and congruences*, Andrzej Schinzel Selecta Vol. II, European Mathematical Society, 2007, pp. 901–902.

[Neu99] J. Neukirch, *Algebraic number theory*, Springer-Verlag, 1999.

[Pal14] W. J. Palenstijn, *Radicals in arithmetic*, PhD thesis, 2014, `https://openaccess.leidenuniv.nl//handle/1887/25833`.

[Per09] A. Perucca, *Two variants of the support problem for products of abelian varieties and tori*, Journal of Number Theory **129** (2009), 1883–1892.

[Per12] ______, *The multilinear support problem for products of abelian varieties and tori*, International Journal of Number Theory **8** (2012), 255–264.

[RV99] D. Ramakrishnan and R. Valenza, *Fourier analysis on number fields*, Springer-Verlag, 1999.

[RZ09] L. Ribes and P. Zalesskii, *Profinite groups*, Springer-Verlag, 2009.

[Sch77] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arithmetica **32** (1977), 245–274.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae **15** (1972), 259–331.

[Ser79] ______, *Local fields*, Springer-Verlag, 1979.

[Ser89] ______, *Abelian l-adic representations and elliptic curves*, second ed., Addison-Wesley, 1989.

[Sil94] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, 1994.

[Sil09] ______, *The arithmetic of elliptic curves*, Springer, 2009.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics **88** (1968), 492–517.

[Wes03] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups*, Acta Arithmetica **110** (2003), 77–88.

[Wil98] J. S. Wilson, *Profinite groups*, Clarendon Press, 1998.

Samenvatting

De Nederlandse vertaling van de titel van dit proefschrift is *Delingspunten in de getaltheorie*. Het proefschrift bestaat uit drie hoofdstukken, waarvan de eerste twee hoofdstukken delingspunten van elementen van de multiplicatieve groep van een getallenlichaam betreffen. Het derde hoofdstuk betreft delingspunten van punten op een elliptische kromme met complexe vermenigvuldiging over een getallenlichaam.

In hoofdstuk één kijken we naar lichaamsuitbreidingen van getallenlichamen verkregen door het adjungeren van alle radicalen van eindig voortgebrachte multiplicatieve ondergroepen, zogeheten *maximale radicale uitbreidingen*. We bewijzen stellingen over de structuur van de pro-eindige groepen die optreden als Galoisgroep van een maximale radicale uitbreiding van een getallenlichaam.

In hoofdstuk twee bestuderen we de Galoisgroepen van alle radicale uitbreidingen van getallenlichamen en bewijzen wij hiermee stellingen over de natuurlijke dichtheid van bepaalde verzamelingen van priemen van getallenlichamen.

In hoofdstuk drie voeren we het analogon uit van hoofdstuk twee voor elliptische krommen met complexe vermenigvuldiging over een getallenlichaam. We bestuderen de Galoisgroepen van lichaamsuitbreidingen van getallenlichamen verkregen door het adjungeren van delingspunten van een elliptische kromme met complexe vermenigvuldiging over een getallenlichaam. Hiermee bewijzen we het analogon van de dichtheidsstelling van hoofdstuk twee

voor het geval van elliptische krommen.

In alle genoemde gevallen hebben de genoemde Galoisgroepen een open beeld binnen een geschikt gedefiniëerde groep van moduulautomorfismen.

Dankwoord

Allereerst wil ik mijn begeleider en copromotor Hendrik Lenstra bedanken voor zijn zeer uitgebreide en zorgvuldige begeleiding. Het is mij een groot genoegen geweest om zijn wiskundig meesterschap van dichtbij ervaren te hebben.

Ook wil ik graag Bas Edixhoven, Ronald van Luijk, Bart de Smit en Peter Stevenhagen bedanken, wier deuren altijd voor mij open stonden, voor zowel wiskundige vragen als alles daarbuiten.

Verder dank ik de rest van de promotiecommissie, Antonella Perucca en Pieter Moree, voor het lezen van dit proefschrift, en voor de verbeteringen die het resultaat van hun suggesties waren.

Curriculum vitae

Abtien Javan Peykar is geboren op 15 augustus 1989 te Apeldoorn. Hij behaalde in 2008 zijn vwo-diploma aan het Alfrink College te Zoetermeer, en in 2011 zijn bachelorgraad in de wiskunde aan de Universiteit Leiden. Hij deed de internationale wiskunde master *ALGANT* (Algebra, Geometry and Number Theory), waarvoor hij in zijn eerste jaar studeerde aan de Università degli Studi di Padova te Padova, Italië, en waarvoor hij in zijn tweede jaar studeerde aan de Universiteit Leiden. In augustus 2013 verdedigde hij zijn masterscriptie getiteld *Radical Galois groups and cohomology*, geschreven onder begeleiding van prof. dr. Hendrik Lenstra, en studeerde hij *cum laude* af. De daarop volgende maand begon hij aan zijn promotietraject aan de Universiteit Leiden onder begeleiding van prof. dr. Hendrik Lenstra. Sinds 2018 is hij actief op het gebied van de kunstmatige intelligentie, waar hij onder andere bedrijven helpt met innoveren.