Division points in arithmetic

Javan Peykar, A.

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 $\mathcal{O} = \mathrm{End}_K(E)$, 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

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

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 $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ a Dedekind domain, let $W \subset E(K)$ be an $\mathcal{O}$-submodule, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Then $K(W : \mathfrak{a})$ is abelian over K if and only if*

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

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

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

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

Now, 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.

Theorem 12. *Let K be a number field, and 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 Steinitz ideal of $\mathcal{O}$. Then the map*

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

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

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

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

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

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 $a_1, \ldots, a_n \in \mathcal{O}$, 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 $x \mapsto (a_1 \cdot x + W, \ldots, a_n \cdot x + W)$. 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

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

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

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

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

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

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 $\mathcal{O}_{\mathfrak{p}}^{*} \longrightarrow (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})})^{*}$ 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

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

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

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

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 $\mathcal{O} = \mathrm{End}_K(E) \neq \mathbf{Z}$ 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 $K(W \colon \mathfrak{a})$ is abelian over K. To this end, let $Q \in W \colon \mathfrak{a}$, 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 $K(E_{\mathrm{tor}})$ 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 $K(W \colon \mathfrak{a})$ is abelian over K.

Now, we prove the 'only if' part. Suppose that $K(W \colon \mathfrak{a})$ 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 $(\mathcal{O} \cdot P) \colon \mathfrak{a}$. As $P \colon a \subset W \colon a$ and $K(W \colon a)$ 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 $(E(K)\colon (\mathfrak{w}+\mathfrak{a})) + E[\mathfrak{w}\mathfrak{a}]$ is contained in $E(K)\colon \mathfrak{a}$ and in $(E(K)\colon \mathfrak{w}) + E_{\text{tor}}$. Therefore, we have

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

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

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

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* $\prod_{\mathfrak{p}\in\mathcal{P}} \mathrm{Aut}_{\mathcal{O},E[\mathfrak{p}^{i_{\mathfrak{p}}}]}(E[\mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})}])$ *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 $\mathrm{N}_{\mathrm{I}_{L'}/\mathrm{I}_L} : \mathrm{I}_{L'} \longrightarrow \mathrm{I}_L$ 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

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

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

$$U \subset U : \mathfrak{a} \subset \operatorname{Sat}_{\mathfrak{a}}(U, K'),$$

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 $\mathfrak{w} = \operatorname{Ann}_{\widehat{\mathcal{O}}}(E(K)_{\mathrm{tor}})$. As K is a number field, the module $E(K)_{\mathrm{tor}}$ is finite, so that $\mathfrak{w} = \operatorname{Ann}_{\mathcal{O}}(E(K)_{\mathrm{tor}})$. Observe that

$$\operatorname{Cyc}_{\mathfrak{a}}(E(K)) \subset (E(K) : \mathfrak{a}) \cap E(K^{\mathrm{ab}}).$$

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 $\operatorname{Cyc}_{\mathfrak{a}}(E(K))/E[\mathfrak{a}]$ 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 $\mathfrak{w} + \mathfrak{a} = \operatorname{Ann}_{\mathcal{O}}(E(K)[\mathfrak{a}])$ 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 $\operatorname{Cyc}_{\mathfrak{a}}(E(K))/E[\mathfrak{a}]$ is finitely generated over $\mathcal{O}$.

Now, as

$$U \subset \operatorname{Cyc}_{\mathfrak{a}}(U) \subset U : \mathfrak{a}$$

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

$$\frac{U:\mathfrak{b}}{(U:\mathfrak{b})\cap \mathrm{Cyc}_{\mathfrak{a}}(U)},$$

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 $\mathrm{Hom}_{\mathcal{O}}\Big(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\Big)$ may be identified with the projective limit of the finite groups

$$H_{\mathfrak{b}} = \mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{b}}{(U:\mathfrak{b})\cap \mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{b}]\right),$$

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 $U:\mathfrak{b}$ is a finitely generated $\mathcal{O}$-module of rank n whose torsion submodule is cyclic and contains $E[\mathfrak{b}]$, we have

$$U:\mathfrak{b} \cong_{\mathcal{O}} M \oplus (\mathcal{O}/\mathfrak{c})$$

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

$$\frac{U:\mathfrak{b}}{\mathfrak{b}\cdot(U:\mathfrak{b})} \cong_{\mathcal{O}/\mathfrak{b}} (M/\mathfrak{b}M) \oplus (\mathcal{O}/\mathfrak{b}),$$

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 $G = \mathrm{Gal}(K(U:\mathfrak{a})/K(E[\mathfrak{a}]))$, 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

$$\frac{(U:\mathfrak{a})^{\langle\sigma\rangle}}{\mathrm{Cyc}_{\mathfrak{a}}(U)},$$

where $(U:\mathfrak{a})^{\langle\sigma\rangle}$ is the group of fixed points of $U:\mathfrak{a}$ under the subgroup $\langle\sigma\rangle$ of G generated by σ. Hence, we have

$$\bigcap_{f\in\kappa(G)} \ker f = \frac{(U:\mathfrak{a})^{G}}{\mathrm{Cyc}_{\mathfrak{a}}(U)} = \frac{\mathrm{Cyc}_{\mathfrak{a}}(U)}{\mathrm{Cyc}_{\mathfrak{a}}(U)} = 0,$$

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 $\tau_x \in \mathrm{Gal}(K(U\colon\mathfrak{a})/K)$ 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 $Q \in U\colon\mathfrak{a}$. Recall that

$$U\colon\mathfrak{a} = \bigcup_{\mathfrak{b}} U\colon\mathfrak{b},$$

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 $Q \in U\colon\mathfrak{b}$. 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 $Q \in U : \mathfrak{a}$, 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 $\mathrm{Hom}_{\mathcal{O}}\left(\frac{U:\mathfrak{a}}{\mathrm{Cyc}_{\mathfrak{a}}(U)}, E[\mathfrak{a}]\right)$.

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 $\mathcal{O} = \operatorname{End}_K(E) \neq \mathbf{Z}$ 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 $\operatorname{Gal}(K(U:\mathfrak{a})/K)$ is an open subgroup of $\operatorname{Aut}_{\mathcal{O},U}(U:\mathfrak{a})$.*

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

$$0 \longrightarrow \operatorname{Aut}_{\mathcal{O},U+E[\mathfrak{a}]}(U:\mathfrak{a}) \longrightarrow \operatorname{Aut}_{\mathcal{O},U}(U:\mathfrak{a}) \longrightarrow \operatorname{Aut}_{\mathcal{O},U[\mathfrak{a}]}(E[\mathfrak{a}]) \longrightarrow 0. \qquad (*)$$

Moreover, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Gal}(K(U:\mathfrak{a})/K(E[\mathfrak{a}])) \arrow[r] \arrow[d] & \operatorname{Gal}(K(U:\mathfrak{a})/K) \arrow[r] \arrow[d] & \operatorname{Gal}(K(E[\mathfrak{a}])/K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Aut}_{\mathcal{O},U+E[\mathfrak{a}]}(U:\mathfrak{a}) \arrow[r] & \operatorname{Aut}_{\mathcal{O},U}(U:\mathfrak{a}) \arrow[r] & \operatorname{Aut}_{\mathcal{O},U[\mathfrak{a}]}(E[\mathfrak{a}]) \arrow[r] & 0
\end{tikzcd}$$

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 $\mathcal{O} = \operatorname{End}_K(E) \neq \mathbf{Z}$ 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).

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*

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

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 $G = \mathrm{Gal}(M/L)$ decomposes as a product over $\mathfrak{p} \in \mathcal{P}$ of the Galois groups $G_{\mathfrak{p}} = \mathrm{Gal}(L(U : \mathfrak{p}^\infty)/L)$, 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

$$G_{\mathfrak{p},i} = \mathrm{Gal}(M/L(U : \mathfrak{p}^i)),$$

let

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

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*

$$\Big[\tfrac{1}{[L:K]}\cdot\prod_{\mathfrak{p}\in\mathcal{P}}\tfrac{\mathrm{N}(\mathfrak{p})-1}{\mathrm{N}(\mathfrak{p})^{n(j_{\mathfrak{p}}-1)+j_{\mathfrak{p}}}(\mathrm{N}(\mathfrak{p})^{n+1}-1)},\prod_{\mathfrak{p}\in\mathcal{P}}\Big(1-\tfrac{\mathrm{N}(\mathfrak{p})^{n}-1}{\mathrm{N}(\mathfrak{p})^{(n+1)j_{\mathfrak{p}}}\cdot(\mathrm{N}(\mathfrak{p})^{n+1}-1)}\Big)\Big]$$

whose denominator divides

$$[L:K]\prod_{\mathfrak{p}\in\mathcal{P}}\bigg(\mathrm{N}(\mathfrak{p})^{(n+1)j_{\mathfrak{p}}}\cdot\frac{\mathrm{N}(\mathfrak{p})^{n+1}-1}{\mathrm{N}(\mathfrak{p})-1}\bigg).$$

(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

$$\tfrac{1}{[L:K]}\prod_{\mathfrak{p}\in\mathcal{P}}\Big[\tfrac{1}{[L(U:\mathfrak{p}^{j_{\mathfrak{p}}}):L]}\cdot\tfrac{\mathrm{N}(\mathfrak{p})^{n}(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1}+\sum_{i=0}^{j_{\mathfrak{p}}-1}\Big(\tfrac{1}{[L(U:\mathfrak{p}^{i}):L]}-\tfrac{1}{[L(U:\mathfrak{p}^{i},W:\mathfrak{p}^{i+1}):L]}\Big)\Big],$$

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

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

Hence $[L(U\,{:}\,\mathfrak{p}^i, W\,{:}\,\mathfrak{p}^{i+1}) : L(U\,{:}\,\mathfrak{p}^i)] = 1$ implies $T_i = 0$. Using Lemma 3.27 we obtain for $\mathfrak{p} \in \mathcal{P}$ that

$$\frac{1}{[L(U\,{:}\,\mathfrak{p}^{j_\mathfrak{p}}) : L]} \cdot \frac{\mathrm{N}(\mathfrak{p})^n(\mathrm{N}(\mathfrak{p})-1)}{\mathrm{N}(\mathfrak{p})^{n+1}-1} + \sum_{i=0}^{j_\mathfrak{p}-1} T_i$$

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 $i \in \mathbf{Z}_{\geq 0}$

$$L(U\,{:}\,\mathfrak{p}^i, W\,{:}\,\mathfrak{p}^{i+1}) \subset L(U\,{:}\,\mathfrak{p}^{i+1}),$$

so that

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

Then for $\mathfrak{p} \in \mathcal{P}$, write $d_\mathfrak{p} = [L(U\,{:}\,\mathfrak{p}^{j_\mathfrak{p}}) : L]$ 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 $d_\mathfrak{p} = [L(U\,{:}\,\mathfrak{p}^{j_\mathfrak{p}}) : L] \leq \mathrm{N}(\mathfrak{p})^{(n+1)j_\mathfrak{p}}$ (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 $i \in \{0, \ldots, j_{\mathfrak{p}} - 1\}$ 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). ■