



Universiteit  
Leiden  
The Netherlands

## Kummer theory for commutative algebraic groups

Tronto, S.

### Citation

Tronto, S. (2022, September 8). *Kummer theory for commutative algebraic groups*. Retrieved from <https://hdl.handle.net/1887/3455350>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3455350>

**Note:** To cite this publication please use the final published version (if applicable).

# Chapter 3

## Radical entanglement for elliptic curves

*by Sebastiano Tronto [Tro20]*

### 1 Introduction

#### 1.1 Setting

Let  $K$  be a number field and fix an algebraic closure  $\overline{K}$  of  $K$ . If  $G$  is a commutative connected algebraic group over  $K$  and  $A$  is a finitely generated and torsion-free subgroup of  $G(K)$ , for any positive integer  $n$  we may consider the field  $K(n^{-1}A)$ , that is the smallest extension of  $K$  inside  $\overline{K}$  containing the coordinates of all points  $P \in G(\overline{K})$  such that  $nP \in A$ . This is a Galois extension of  $K$  containing the  $n$ -th torsion field  $K(G[n])$  of  $G$ .

If  $G = \mathbb{G}_m$  is the multiplicative group, such extensions are studied by classical Kummer theory. The more general case of an extension of an abelian variety by a torus is treated in Ribet's foundational paper [Rib79]. Under certain assumptions, for example if  $G$  is the product of an abelian variety and a torus and  $A$  has rank 1, it is known that the ratio

$$\frac{n^s}{[K(n^{-1}A) : K(G[n])]} \tag{1.1}$$

where  $s$  is the unique positive integer such that  $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$  for all  $n \geq 1$ , is bounded independently of  $n$  (see also [Ber88, Théorème 5.2] and [Hin88, Lemme 14]).

In [Chapter 1] Lombardo and the author were able to give an effective bound for the ratio (1.1) if  $G = E$  is an elliptic curve with  $\text{End}_K(E) = \mathbb{Z}$  and  $A = \langle \alpha \rangle$  has rank 1. Moreover, a uniform bound in the case  $K = \mathbb{Q}$ , under some necessary assumptions on the divisibility of  $\alpha$  in  $E(K)/E(K)_{\text{tors}}$ , was given.

The bounds given in [Chapter 1] essentially depend on three properties of  $E$  and  $\alpha$ :

- (1) The finiteness of the divisibility of  $\alpha$  in  $E(K)/E(K)_{\text{tors}}$ ;
- (2) Properties of the  $\ell$ -adic Galois representations associated with  $E$ , for every prime  $\ell$ ;
- (3) The finiteness of the exponent of  $H^1(\text{Gal}(K(E(\overline{K})_{\text{tors}}) | K), E(\overline{K})_{\text{tors}})$ .

The goal of the present paper is twofold: firstly, we use the properties of  $r$ -extensions of abelian groups introduced by Palenstijn in [Pal04] and [Pal14] to generalize the methods of [Chapter 1] to groups  $A$  of arbitrary finite rank and any commutative connected algebraic group  $G$  that satisfies the same properties mentioned above. The result we obtain is the following (see Theorem 5.9):

**Theorem 1.1.** *Let  $G$  be a commutative connected algebraic group over a number field  $K$  and let  $A \subseteq G(K)$  be a finitely generated and torsion-free subgroup of rank  $r$ . Let  $s$  be the unique non-negative integer such that  $G[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$  for all  $n \geq 1$ . Let  $H$  denote, after a choice of basis, the image of the adelic Galois representation associated with  $G$  over  $K$*

$$\text{Gal}(\overline{K} | K) \rightarrow \text{GL}_s(\widehat{\mathbb{Z}}).$$

*For every prime  $\ell$ , let  $H_\ell$  denote the image of  $H$  under the projection  $\text{GL}_s(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_s(\mathbb{Z}_\ell)$  and denote by  $\mathbb{Z}_\ell[H_\ell]$  the closed  $\mathbb{Z}_\ell$ -subalgebra of  $\text{Mat}_{s \times s}(\mathbb{Z}_\ell)$  generated by  $H_\ell$ . Assume that*

- (1) *There is an integer  $d_A \geq 1$  such that*

$$d_A \cdot \{P \in G(K) \mid \exists n \in \mathbb{N}_{\geq 1} : nP \in A\} \subseteq A + G(K)_{\text{tors}}.$$

- (2) *There is an integer  $N \geq 1$  such that  $\mathbb{Z}_\ell[H_\ell] \supseteq N \text{Mat}_{s \times s}(\mathbb{Z}_\ell)$  for every prime  $\ell$ .*
- (3) *There is an integer  $M \geq 1$  such that the exponent of the cohomology group  $H^1(\text{Gal}(K_\infty | K), G(\overline{K})_{\text{tors}})$  divides  $M$ , where  $K_\infty = K(G(\overline{K})_{\text{tors}})$ .*

Then for every  $n \geq 1$  the ratio

$$\frac{n^{rs}}{[K(n^{-1}A) : K(G[n])]}$$

divides  $(d_A NM)^{rs}$ .

The first condition of Theorem 1.1 is always satisfied if  $G$  is an abelian variety or  $G = \mathbb{G}_m$  (see Example 5.2). We call such an integer  $d_A$  a *divisibility parameter* for  $A$  in  $G(K)$ . One has  $d_A = 1$  if, for example, the group  $G(K)$  is finitely generated and torsion-free and  $A = G(K)$ .

Notice that if a set of generators for  $A$  is known, modulo the torsion subgroup of  $G(K)$ , in terms of a  $\mathbb{Z}$ -basis of  $G(K)/G(K)_{\text{tors}}$ , one can compute a divisibility parameter  $d_A$ . See section 6.1.

Our second goal is to apply Theorem 1.1 to some specific cases. In particular, we generalize the results of [Chapter 1] to the case of arbitrary rank. Theorems 1.2 and 1.3 below follow from Theorems 6.14, 6.16 and 6.17 and Lemma 5.7.

**Theorem 1.2.** *Let  $E$  be an elliptic curve over a number field  $K$  such that  $\text{End}_K(E) = \mathbb{Z}$ . Let  $A$  be a finitely generated and torsion-free subgroup of  $E(K)$  of rank  $r$ . There is an effectively computable integer  $N > 1$ , depending only on  $E$  and  $K$ , such that for every  $n \geq 1$*

$$\frac{n^{2r}}{[K(n^{-1}A) : K(E[n])]} \quad \text{divides} \quad (d_A N)^{2r}$$

where  $d_A$  is a divisibility parameter for  $A$  in  $E(K)$ .

**Theorem 1.3.** *There is a universal constant  $C \geq 1$  such that for every elliptic curve  $E$  over  $\mathbb{Q}$ , for every torsion-free subgroup  $A$  of  $E(\mathbb{Q})$  and for every  $n \geq 1$*

$$\frac{n^{2\text{rk}(A)}}{[\mathbb{Q}(n^{-1}A) : \mathbb{Q}(E[n])]} \quad \text{divides} \quad (d_A C)^{2\text{rk}(A)}$$

where  $d_A$  is a divisibility parameter for  $A$  in  $E(\mathbb{Q})$ .

## 1.2 Notation

If  $A$  is an abelian group and  $n$  is a positive integer we denote by  $A[n]$  the subgroup of the elements of  $A$  of order dividing  $n$ . We denote by  $A_{\text{tors}}$  the subgroup consisting of all elements of  $A$  of finite order. We denote by  $\text{rk}(A)$  the *rank* of  $A$ , that is the dimension of  $A \otimes_{\mathbb{Z}} \mathbb{Q}$  as a  $\mathbb{Q}$ -vector space.

If  $R$  is a commutative ring, then we denote by  $\text{Mat}_{n \times m}(R)$  the  $R$ -module of  $n \times m$  matrices with entries in  $R$ , which we regard as an  $R$ -algebra if  $n = m$ . If

at least one between  $n$  and  $m$  is zero then  $\text{Mat}_{n \times m}(R)$  is the  $R$ -module ring (or trivial  $R$ -algebra if  $n = m = 0$ ). For  $n > 0$  we denote by  $\text{GL}_n(R)$  the group of invertible  $n \times n$  matrices with entries in  $R$ .

For any prime number  $\ell$  and any non-zero integer  $n$  we denote by  $v_\ell(n)$  the  $\ell$ -adic valuation of  $n$ . We denote by  $\mathbb{Z}_\ell$  the ring of  $\ell$ -adic integers and by  $\hat{\mathbb{Z}}$  the ring of profinite integers, which we identify with the product  $\prod_\ell \mathbb{Z}_\ell$ .

If  $K$  is a number field and  $\bar{K}$  is a fixed algebraic closure of  $K$ , we denote by  $\zeta_n$  a primitive  $n$ -th root of unity in  $\bar{K}$ , for any positive integer  $n$ . If  $G$  is any algebraic group over  $K$  and  $L$  is any field extension of  $K$ , we denote by  $G(L)$  the group of  $L$ -points of  $G$ . If  $S$  is a subset of  $G(\bar{K})$ , we denote by  $K(S)$  the subfield of  $\bar{K}$  whose elements are fixed by

$$H = \{g \in \text{Gal}(\bar{K} \mid K) \mid g(P) = P \quad \forall P \in S\}.$$

If  $G$  is embedded in an affine or projective space (notice that, as a consequence of Chevalley's structure theorem, any algebraic group over a field is quasi-projective) then  $K(S)$  coincides with the field generated by  $K$  and any choice of affine coordinates of all points  $P \in S$ .

### 1.3 Structure of the paper

After some necessary group-theoretic preliminaries in Section 2, we investigate in Section 3 the theory of  $s$ -extensions of abelian groups introduced by Palenstijn. Much of the content of that section can be found, with few differences, in [Pal04].

We then move on to prove some  $\hat{\mathbb{Z}}$ -linear algebra results in Section 4, and finally develop our theory of entanglement for commutative algebraic groups in Section 5. In Section 6 we apply this theory to the case of elliptic curves without complex multiplication.

### 1.4 Acknowledgements

I am grateful to my advisors Antonella Perucca and Peter Bruin for their constant support during the preparation of this paper. I am also very grateful to Hendrik Lenstra and Peter Stevenhagen for giving me some of the main ideas for this work.

## 2 Group-theoretic preliminaries

We collect here some basic group-theoretic results that we will need throughout this paper.

## 2.1 Pontryagin duality

Let  $G$  be a locally compact Hausdorff topological abelian group. Let  $S^1 = \mathbb{R}/\mathbb{Z}$  with the usual topology. The group  $\text{Hom}(G, S^1)$  of continuous homomorphisms from  $G$  to  $S^1$  endowed with the compact-open topology is itself a locally compact abelian group, and it is called the *group of characters* or the (*Pontryagin*) *dual* of  $G$  (see [Pon66, Chapter 6]). We will denote it by  $G^\wedge$ .

**Example 2.1.** Consider  $\mathbb{Q}/\mathbb{Z}$  as a topological group with the discrete topology. We have  $(\mathbb{Q}/\mathbb{Z})^\wedge \cong \widehat{\mathbb{Z}}$ . To see this, notice first that for every positive integer  $n$  there is a natural isomorphism

$$\text{Hom}\left(\frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}\right) \cong \mathbb{Z}/n\mathbb{Z}$$

given by sending a homomorphism  $\varphi : \frac{1}{n}\mathbb{Z}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$  to the unique  $d \in \mathbb{Z}/n\mathbb{Z}$  such that  $\varphi\left(\frac{1}{n}\right) = \frac{d}{n}$ . Now we have

$$\begin{aligned} \text{Hom}(\mathbb{Q}/\mathbb{Z}, S^1) &= \text{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \\ &\cong \text{Hom}\left(\varinjlim_n \frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}\right) \cong \\ &\cong \varprojlim_n \text{Hom}\left(\frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}\right) \cong \\ &\cong \varprojlim_n \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

The maps forming this last projective system are just the natural projections, since for  $n \mid m$  the restriction of

$$\begin{aligned} \varphi : \mathbb{Z}/m\mathbb{Z} &\rightarrow \mathbb{Q}/\mathbb{Z} \\ \frac{1}{m} &\mapsto \frac{d}{m} \end{aligned}$$

to  $\mathbb{Z}/n\mathbb{Z}$  maps  $\frac{1}{n}$  to  $\frac{d}{n}$ . So we get  $\text{Hom}(\mathbb{Q}/\mathbb{Z}, S^1) \cong \widehat{\mathbb{Z}}$ .

**Remark 2.2.** In Section 4 we will need a higher-dimensional analogue of Example 2.1. By the previous example we easily deduce that, for  $r, s \geq 1$ , the group  $\text{Hom}((\mathbb{Q}/\mathbb{Z})^r, (\mathbb{Q}/\mathbb{Z})^s)$  can be identified with  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$ . This can be seen

directly on the finite level as follows: let

$$\begin{aligned} \varphi : \quad \left( \frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}} \right)^r &\rightarrow \left( \frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}} \right)^s \\ \left( \frac{1}{n}, 0, \dots, 0 \right) &\mapsto \left( \frac{d_{11}}{n}, \frac{d_{21}}{n}, \dots, \frac{d_{s1}}{n} \right) \\ \left( 0, \frac{1}{n}, \dots, 0 \right) &\mapsto \left( \frac{d_{12}}{n}, \frac{d_{22}}{n}, \dots, \frac{d_{s2}}{n} \right) \\ &\vdots \\ \left( 0, 0, \dots, \frac{1}{n} \right) &\mapsto \left( \frac{d_{1r}}{n}, \frac{d_{2r}}{n}, \dots, \frac{d_{sr}}{n} \right) \end{aligned}$$

be a group homomorphism. The matrix  $D_\varphi = (d_{ij}) \in \text{Mat}_{s \times r}(\mathbb{Z}/n\mathbb{Z})$  completely describes the homomorphism  $\varphi$ , and the map  $\varphi \mapsto D_\varphi$  is easily checked to be a group isomorphism between  $\text{Hom}((\frac{1}{n}\mathbb{Z}/\mathbb{Z})^r, (\frac{1}{n}\mathbb{Z}/\mathbb{Z})^s)$  and  $\text{Mat}_{s \times r}(\mathbb{Z}/n\mathbb{Z})$ . Passing to the limit in  $n$  we obtain a description of the natural isomorphism  $\text{Hom}((\mathbb{Q}/\mathbb{Z})^r, (\mathbb{Q}/\mathbb{Z})^s) \cong \text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$ .

Furthermore, if  $r = s$  the map  $\varphi \mapsto D_\varphi$  is a ring homomorphism from  $\text{End}((\mathbb{Q}/\mathbb{Z})^s)$  to  $\text{Mat}_{s \times s}(\widehat{\mathbb{Z}})$ . This allows us to identify  $\text{Aut}((\mathbb{Q}/\mathbb{Z})^s) = \text{End}((\mathbb{Q}/\mathbb{Z})^s)^\times$  with  $\text{GL}_s(\widehat{\mathbb{Z}})$ .

**Theorem 2.3** (Pontryagin duality, see [Pon66, Theorems 39 and 40]). *The hom-functor  $\text{Hom}(-, S^1)$  that maps  $G$  to its dual  $G^\wedge$  is an anti-equivalence of the category of locally compact Hausdorff topological abelian groups with itself. Moreover  $(G^\wedge)^\wedge$  is naturally isomorphic to  $G$ .*

*This anti-equivalence induces an inclusion-reversing bijection between the closed subgroups of any locally compact topological abelian group  $G$  and those of  $G^\wedge$ , given by*

$$\begin{aligned} \{\text{closed subgroups of } G\} &\leftrightarrow \{\text{closed subgroups of } G^\wedge\} \\ U &\mapsto \text{Ann } U = \{f \in G^\wedge \mid f(u) = 0 \forall u \in U\} \\ \{g \in G \mid f(g) = 0 \forall f \in V\} = \text{Ann } V &\leftarrow V \end{aligned}$$

*Moreover,  $G$  is discrete if and only if  $G^\wedge$  is compact, and  $G$  is discrete and torsion if and only if  $G^\wedge$  is profinite.*

## 2.2 Relative automorphism groups

In this section we establish some basic results on relative automorphism groups of abelian groups, that is the groups containing those automorphisms that restrict to the identity on a given subgroup.

If  $A$  is an abelian group and  $B, C$  are abelian groups containing  $A$  as a subgroup, then we denote by  $\text{Hom}_A(B, C)$  the set of homomorphisms  $B \rightarrow C$  that restrict to the identity on  $A$ . Similarly we define the ring of endomorphisms  $\text{End}_A(B)$ . We also denote by  $\text{Aut}_A(B)$  the group of all automorphisms of  $B$  that restrict to the identity on  $A$ , that is the group of invertible elements in the ring  $\text{End}_A(B)$ . We call any element of  $\text{Aut}_A(B)$  an  $A$ -automorphism of  $B$ .

**Lemma 2.4.** *Let  $M$  and  $N$  be abelian groups and let  $A$  and  $B$  be subgroups of  $M$ . If  $f : A \rightarrow N$  and  $g : B \rightarrow N$  are group homomorphisms such that  $f|_{A \cap B} = g|_{A \cap B}$ , then there exists a unique map  $\varphi : A + B \rightarrow N$  such that  $\varphi|_A = f$  and  $\varphi|_B = g$ .*

*Proof.* This is just a rephrasing of the universal property of  $A + B$  as the pushout of  $A \cap B \hookrightarrow A$  and  $A \cap B \hookrightarrow B$ .  $\square$

**Definition 2.5.** Let  $A \subseteq B \subseteq M$  be abelian groups. We say that  $B$  is  $A$ -normal in  $M$  if the restriction to  $B$  of every element of  $\text{Aut}_A(M)$  is an automorphism of  $B$ .

If  $B' \subseteq M$  is a subgroup not necessarily containing  $A$ , then we say that  $B'$  is  $A$ -normal in  $M$  if the following two conditions hold:

- (1) The group  $B'$  is  $(A \cap B')$ -normal in  $A + B'$  and
- (2) The group  $A + B'$  is  $A$ -normal in  $M$ .

**Remark 2.6.** The choice of the word *normal* in the above definition is in analogy with the case of field extensions in Galois theory.

**Remark 2.7.** Let  $A \subseteq B \subseteq C \subseteq M$  be abelian groups. If  $C$  is  $A$ -normal in  $M$ , then  $C$  is also  $B$ -normal in  $M$ . If  $B$  is  $A$ -normal in  $C$  and  $C$  is  $A$ -normal in  $M$ , then  $B$  is  $A$ -normal in  $M$ .

If  $A \subseteq B \subseteq M$  are abelian groups, then  $B$  is  $A$ -normal in  $M$  if and only if the restriction map  $\text{Aut}_A(M) \rightarrow \text{Hom}_A(B, M)$  factors via  $\text{Aut}_A(B)$ . In this situation we call this map  $\text{Aut}_A(M) \rightarrow \text{Aut}_A(B)$  the *natural restriction map*.

**Lemma 2.8.** *Let  $M$  be an abelian group and let  $A, B \subseteq M$  be subgroups of  $M$ . Assume that  $B$  is  $A$ -normal in  $A + B$ . Then the natural restriction map  $\text{Aut}_{A \cap B}(A + B) \rightarrow \text{Aut}_{A \cap B}(B)$  induces an isomorphism*

$$\text{Aut}_A(A + B) \cong \text{Aut}_{A \cap B}(B).$$

*Proof.* The inclusion  $\text{Aut}_A(A + B) \hookrightarrow \text{Aut}_{A \cap B}(A + B)$  composed with the natural restriction yields a group homomorphism  $\rho : \text{Aut}_A(A + B) \rightarrow \text{Aut}_{A \cap B}(B)$ , which is injective because  $\ker \rho = \text{Aut}_{A+B}(A + B) = 1$ .



Let  $\sigma \in \text{Aut}_{A \cap B}(B)$  and let  $\tilde{\sigma} : A + B \rightarrow A + B$  be the homomorphism obtained by applying Lemma 2.4 to  $\sigma$  and  $\text{id}_A$ . This map is clearly surjective, since every element of  $A$  and every element of  $B$  are in its image. If  $\tilde{\sigma}(a + b) = 0$  for some  $a \in A$  and some  $b \in B$ , then  $\sigma(b) = -a \in A \cap B$ , which implies that  $b \in A \cap B$  and thus  $a + b = 0$ . So  $\tilde{\sigma}$  is injective, thus an automorphism. We conclude that  $\rho$  is an isomorphism.  $\square$

## 2.3 Projective limits of exact sequences

**Remark 2.9.** Let

$$1 \rightarrow A \rightarrow G \rightarrow H \rightarrow 1$$

be an exact sequence of groups, and assume that  $A$  is abelian. Then there is a natural left action of  $H$  on  $A$ , defined as follows.

Let  $h \in H$  and consider any lift  $\tilde{h} \in G$  of  $h$ . Then the action of  $h$  on  $a \in A$  is defined as

$$\tilde{h}a\tilde{h}^{-1}$$

where we see  $a$  as an element of  $G$  via the inclusion map. This definition does not depend on the choice of the lift  $\tilde{h}$ , because if  $\hat{h}$  is a different lift of  $h$  then  $\hat{h} = \tilde{h}b$  for some  $b \in A$ , and we have  $\hat{h}a\hat{h}^{-1} = \tilde{h}bab^{-1}\tilde{h}^{-1} = \tilde{h}a\tilde{h}^{-1}$ . Moreover  $\tilde{h}a\tilde{h}^{-1}$  is mapped to 1 in  $H$ , so this clearly defines an action of  $H$  on  $A$ .

**Lemma 2.10.** *Let  $I$  be a partially ordered set. For every  $i \in I$  let  $\mathcal{A}_i$  denote an exact sequence of topological groups*

$$1 \rightarrow A'_i \rightarrow A_i \rightarrow A''_i \rightarrow 1$$

*such that  $A'_i$  and  $A''_i$  have the subspace and quotient topology with respect to  $A_i$ , respectively. For every  $i \leq j$  let  $\rho_{ij} : \mathcal{A}_j \rightarrow \mathcal{A}_i$  be a map of exact sequences such that  $\{(\mathcal{A})_{i \in I}, (\rho_{ij})_{i, j \in I}\}$  is a projective system. Let  $\{\mathcal{A}, (\pi_i)_{i \in I}\}$  be the limit of this projective system, where  $\mathcal{A}$  is*

$$1 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 1.$$

*Then the subspace topology on  $A'$  and the quotient topology on  $A''$  coincide with their respective limit topology.*

*Proof.* The limit topologies on  $A$  and  $A'$  are the subspace topologies with respect to the products  $\prod_{i \in I} A_i$  and  $\prod_{i \in I} A'_i$ , respectively. Since each  $A'_i$  has the subspace topology with respect to  $A_i$ , it follows that  $\prod_{i \in I} A'_i$  has the subspace topology with respect to  $\prod_{i \in I} A_i$ , so  $A'$  has the subspace topology with respect to  $A$ .

In order to show that the limit topology on  $A''$  is the quotient topology, we need to show that every  $U \subseteq A''$  is open for the limit topology if and only if its preimage in  $A$  is open. If  $U \subseteq A''$  is open for the limit topology, there is  $V \subseteq \prod_{i \in I} A_i''$  open such that  $V \cap A'' = U$ . Its preimage  $W \subseteq \prod_{i \in I} A_i$  is open and such that  $W \cap A$ , which coincides with the preimage of  $U$  in  $A$ , is open. On the other hand, if the preimage  $V' \subseteq A$  of  $U$  is open, there must be  $W \subseteq \prod_{i \in I} A_i$  open and such that  $W \cap A = V'$ . But then, since a quotient map between topological groups is open and the product of surjective open maps is open, the projection  $V$  of  $W$  in  $\prod_{i \in I} A_i''$  is open, and so is  $V \cap A''$ , which coincides with  $U$ .  $\square$

### 3 The $s$ -extensions of abelian groups

In this section we are going to revisit the theory of certain kinds of extensions of abelian groups that were first introduced by Palenstijn in his master thesis [Pal04]. These extensions arise naturally when considering the so-called *division points* of a certain subgroup  $A$  of the rational points of a commutative algebraic group. In particular, the automorphism groups of these extension provide a framework to study the Galois groups of field extensions generated by division points.

#### 3.1 General definitions and first results

Fix a positive integer  $s$ .

**Definition 3.1.** Let  $A$  be a finitely generated abelian group. An  $s$ -extension of  $A$  is an abelian group  $B$  containing  $A$  such that:

- (1)  $B/A$  is torsion;
- (2) the torsion subgroup of  $B$  is isomorphic to a subgroup of  $(\mathbb{Q}/\mathbb{Z})^s$ .

**Remark 3.2.** A necessary (and sufficient) condition for a finitely generated abelian group  $A$  to admit an  $s$ -extension is that the torsion subgroup  $A_{\text{tors}}$  of  $A$  can be embedded in  $(\mathbb{Q}/\mathbb{Z})^s$ .

**Definition 3.3.** Let  $A$  be a finitely generated abelian group. For every  $s$ -extension  $B$  of  $A$ , every  $a \in A$  and every positive integer  $n$  we call any  $b \in B$  such that  $nb = a$  an  $n$ -division point of  $a$  (in  $B$ ). We denote by

$$n_B^{-1}a := \{b \in B \mid nb = a\}$$

the set of  $n$ -division points of  $a$ . We omit the subscript  $B$  from  $n_B^{-1}$  if this is clear from the context. We also denote by

$$B_n := \{b \in B \mid nb \in A\} = \bigcup_{a \in A} n_B^{-1}a$$

the set of all  $n$ -division points of elements of  $A$ , which is again an  $s$ -extension of  $A$ . Notice that for  $n \mid m$  we have  $B_n \subseteq B_m$  and that  $B = \bigcup_{n \geq 1} B_n$ .

**Remark 3.4.** Assume that  $n_B^{-1}a$  is not empty. Then for any fixed  $b_0 \in n_B^{-1}a$ , the map

$$\begin{aligned} n_B^{-1}a &\rightarrow B[n] \\ b &\mapsto b - b_0 \end{aligned}$$

is a bijection.

The following lemmas will be used in what follows, in particular in Section 3.2.

**Lemma 3.5.** *Let  $B$  and  $C$  be two  $s$ -extensions of a finitely generated abelian group  $A$  and let  $\varphi : B \rightarrow C$  be a group homomorphism that is the identity on  $A$ . For every  $a \in A$  and every  $b \in n_B^{-1}a$  we have  $\varphi(b) \in n_C^{-1}a$ . In particular, we have  $\varphi(B_n) \subseteq C_n$ .*

*Proof.* It is enough to notice that  $n\varphi(b) = \varphi(nb) = \varphi(a) = a$ . □

**Lemma 3.6.** *Let  $B$  and  $C$  be two  $s$ -extensions of a finitely generated abelian group  $A$  and let  $\varphi : B \rightarrow C$  be a group homomorphism that is the identity on  $A$ . The kernel of  $\varphi$  is contained in  $B_{\text{tors}}$ . Moreover, if for every prime  $\ell$  the restriction of  $\varphi$  to  $B[\ell]$  is injective, then  $\varphi$  is injective.*

*Proof.* Let  $b \in \ker \varphi$  and let  $n$  be a positive integer such that  $nb = a \in A$ . By Lemma 3.5 we have  $0 \in n_C^{-1}a$ , which implies that  $a = 0$ . In particular,  $b$  is torsion. For the second assertion, assume that  $b \neq 0$  and let  $\ell$  be a prime dividing the order of  $b$ . But then  $b$  has a multiple of order  $\ell$  which is in  $\ker \varphi$ , a contradiction. □

**Lemma 3.7.** *Let  $B$  be an  $s$ -extension of a finitely generated abelian group  $A$  and let  $\varphi : B \rightarrow B$  be an endomorphism that is the identity on  $A$ . If  $\varphi$  is injective, then it is an automorphism.*

*Proof.* Assume first that  $\varphi$  is injective and let  $b \in B$ . Let  $n$  be a positive integer such that  $nb = a \in A$ . By Lemma 3.5 we have  $\varphi(n^{-1}a) \subseteq n^{-1}a$ . Since  $n^{-1}a$  is finite there must be some  $b' \in n^{-1}a$  such that  $\varphi(b') = b$ , hence  $\varphi$  is surjective. □

The following proposition gives a criterion to verify if an  $s$ -extension is normal in the sense of Definition 2.5.

**Proposition 3.8.** *Let  $B$  be an  $s$ -extension of a finitely generated abelian group  $A$  and let  $C \subseteq B$  be a subgroup. If  $\text{Hom}_{A \cap C}(C, B) \subseteq \text{Hom}_{A \cap C}(C, C)$ , then  $C$  is  $A$ -normal in  $B$ .*

*Moreover, under the same assumptions, for every  $A \subseteq A' \subseteq C \subseteq B' \subseteq B$  we have that  $C$  is  $A'$ -normal in  $B'$ .*

*Proof.* First of all, notice that  $C$  is an  $s$ -extension of  $A \cap C$  and that  $A + C$  is an  $s$ -extension of  $A$ . Let now  $\sigma \in \text{Aut}_{A \cap C}(A + C)$  and consider its restriction  $\sigma_C : C \rightarrow A + C$ . We then have

$$\sigma_C \in \text{Hom}_{A \cap C}(C, A + C) \subseteq \text{Hom}_{A \cap C}(C, B) \subseteq \text{Hom}_{A \cap C}(C, C).$$

Moreover  $\sigma_C$  is injective, thus an automorphism by Lemma 3.7. This shows that  $C$  is  $(A \cap C)$ -normal in  $A + C$ .

To see that  $A + C$  is  $A$ -normal in  $B$ , let  $\tau \in \text{Aut}_A(B)$  and consider its restriction  $\tau_{A+C} : A + C \rightarrow B$ . Since  $\tau$  is the identity on  $A$  and the image of its restriction to  $C$  is contained in  $C$  by assumption, we have that the image of  $\tau_{A+C}$  is contained in  $A + C$ . Since  $\tau$  is injective, by applying Lemma 3.7 we see that  $\tau_{A+C}$  is an  $A$ -automorphism of  $A + C$ , so we conclude that  $A + C$  is  $A$ -normal in  $B$ . Thus  $C$  is  $A$ -normal in  $B$ .

The second assertion follows from the first by noticing that  $\text{Hom}_{A' \cap C}(C, B')$  is contained in  $\text{Hom}_{A \cap C}(C, B)$ .  $\square$

**Example 3.9.** Let  $B$  be an  $s$ -extension of a finitely generated abelian group  $A$ . Proposition 3.8 can be applied in the following cases:

- (1) Let  $C$  be either  $B_{\text{tors}}$  or  $B[n]$  for some positive integer  $n$ . Then the image of every group homomorphism from  $C$  to  $B$  is contained in  $C$ , so in particular  $\text{Hom}_{A \cap C}(C, B) \subseteq \text{Hom}_{A \cap C}(C, C)$ .
- (2) If  $C = B_n$  for some positive integer  $n$ , then by Lemma 3.5 we have  $\text{Hom}_A(B_n, B) \subseteq \text{Hom}_A(B_n, B_n)$  and hence

$$\text{Hom}_{A \cap B_n}(B_n, B) \subseteq \text{Hom}_{A \cap B_n}(B_n, B_n).$$

### 3.2 Automorphisms of $s$ -extensions

We now study the automorphisms of an  $s$ -extension that are the identity on the base group. Recall that if  $B$  is an abelian group and  $A \subseteq B$  is a subgroup we denote by  $\text{Aut}_A(B)$  the group of all automorphisms of  $B$  that restrict to the identity on  $A$ .

Fix for the remainder of this section a finitely generated abelian group  $A$ .

The following result is a generalization of [Pal14, Lemma 1.8], and the proof is essentially the same. We include it here for the sake of completeness.

**Proposition 3.10.** *Let  $B$  be an  $s$ -extension of  $A$  and let  $C \subseteq B$  be a subgroup. If  $C$  is  $A$ -normal in  $B$ , the image of the restriction map  $\text{Aut}_A(B) \rightarrow \text{Hom}_{A \cap C}(C, B)$  is  $\text{Aut}_{A \cap C}(C)$ .*

*Proof.* By Lemma 2.8 we have  $\text{Aut}_A(A + C) \cong \text{Aut}_{A \cap C}(C)$  via the restriction map, so it is enough to show that the restriction  $\text{Aut}_A(B) \rightarrow \text{Aut}_A(A + C)$ , which exists because  $A + C$  is  $A$ -normal in  $B$ , is surjective. Thus we may assume that  $A \subseteq C$ .

In view of Lemma 3.7 it is enough to prove that every  $\varphi \in \text{Aut}(C)$  can be extended to an injective homomorphism  $B \rightarrow B$ . Consider the set of pairs  $(M, \phi)$ , where  $M$  is a subgroup of  $B$  containing  $C$  and  $\phi : M \rightarrow B$  is an injective homomorphism extending  $\varphi$ , ordered by inclusion

$$(M, \phi) \subseteq (M', \phi') \iff M \subseteq M' \text{ and } \phi'|_M = \phi.$$

By Zorn's Lemma this ordered set admits a maximal element  $(\tilde{B}, \tilde{\varphi})$  and we need to show that  $\tilde{B} = B$ . We prove this by contradiction, assuming that there exists  $x \in B \setminus \tilde{B}$  and proving that we can then extend  $\tilde{\varphi}$  to an injective map  $\langle \tilde{B}, x \rangle \rightarrow B$ .

Assume first that the order of  $x$  is a prime number  $\ell$ . An element of  $\tilde{B}$  mapping to  $B[\ell]$  must be in  $\tilde{B}[\ell]$  because  $\tilde{\varphi}$  is injective. Since  $x \in B[\ell] \setminus \tilde{B}[\ell]$  we have  $\#B[\ell] < \#\tilde{B}[\ell]$ , so there must be  $y \in B[\ell] \setminus \{0\}$  that is not in the image of  $\tilde{\varphi}$ . Using Lemma 2.4 we can then extend  $\tilde{\varphi}$  to  $\langle \tilde{B}, x \rangle$  by letting  $\tilde{\varphi}(x) := y$ . The map we obtain is still injective, so we may assume that  $\tilde{B}$  contains all elements of prime order of  $B$ .

Let now  $k$  be the smallest positive integer such that  $kx \in \tilde{B}$ . Up to replacing  $x$  with a suitable multiple, we may assume that  $k = \ell$  is a prime number. Let  $b = \ell x \in \tilde{B}$ . The fact that  $B[\ell] \subseteq \tilde{B}$  implies that  $\ell_B^{-1}b \subseteq B \setminus \tilde{B}$ .

Consider now  $\tilde{\varphi}(b) \in B$  and let  $y \in \ell_B^{-1}\tilde{\varphi}(b)$ . If  $y \in \text{Im}(\tilde{\varphi})$ , then there is  $z \in \tilde{B}$  such that  $\tilde{\varphi}(z) = y$ , thus  $\tilde{\varphi}(\ell z) = \ell y = \tilde{\varphi}(b)$  and so  $\ell z = b$ , a contradiction. Since  $\tilde{B} \cap \langle x \rangle = \langle \ell x \rangle$  and  $\tilde{\varphi}(\ell x) = \ell y$ , using again Lemma 2.4 we can extend  $\tilde{\varphi}$  to  $\langle \tilde{B}, x \rangle$  by letting  $\tilde{\varphi}(x) := y$ . By Lemma 3.6, the homomorphism  $\langle \tilde{B}, x \rangle \rightarrow B$  that we obtain is still injective.

We conclude that  $\tilde{B} = B$ , thus the restriction map  $\text{Aut}_A(B) \rightarrow \text{Aut}_A(C)$  is surjective.  $\square$

**Proposition 3.11.** *Let  $B$  be an  $s$ -extension of  $A$ . There is a canonical isomorphism*

$$\varphi : \text{Aut}_{A+B_{\text{tors}}}(B) \cong \text{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}})$$

which sends any  $\sigma \in \text{Aut}_{A+B_{\text{tors}}}(B)$  to the group homomorphism  $[b] \mapsto \sigma(b) - b$ .

*Proof.* Let  $\sigma \in \text{Aut}_{A+B_{\text{tors}}}(B)$ . By Lemma 3.5 we can define a map

$$\begin{aligned} \varphi_\sigma : B/(A + B_{\text{tors}}) &\rightarrow B_{\text{tors}} \\ [b] &\mapsto \sigma(b) - b \end{aligned}$$

which is clearly a group homomorphism. We claim that the map

$$\begin{aligned} \varphi : \text{Aut}_{A+B_{\text{tors}}}(B) &\rightarrow \text{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}}) \\ \sigma &\mapsto \varphi_\sigma \end{aligned}$$

is also a group homomorphism. To see this, let  $\sigma, \tau \in \text{Aut}_{A+B_{\text{tors}}}(B)$ . Notice that, since  $\tau(b) - b \in B_{\text{tors}}$  for every  $b \in B$ , we have  $\sigma(\tau(b) - b) = \tau(b) - b$ . Then we have

$$\begin{aligned} \varphi_{\sigma\tau}([b]) &= \sigma(\tau(b)) - b = \\ &= \sigma(\tau(b)) - b + \tau(b) - b - \sigma(\tau(b) - b) = \\ &= \tau(b) - b + \sigma(b) - b = \\ &= \varphi_\sigma([b]) + \varphi_\tau([b]) \end{aligned}$$

which proves our claim.

The homomorphism  $\varphi$  is injective, because if  $\varphi_\sigma = 0$  then  $\sigma(b) = b$  for all  $b \in B$ . To see that  $\varphi$  is surjective, for any  $\psi \in \text{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}})$  let

$$\begin{aligned} \sigma_\psi : B &\longrightarrow B \\ b &\longmapsto b + \psi([b]) \end{aligned}$$

which is clearly a group homomorphism that is the identity on  $A + B_{\text{tors}}$ . It is also injective, because if  $b + \psi([b]) = 0$  then  $b = -\psi([b])$  must be a torsion point, hence  $-b = \psi([b]) = \psi(0) = 0$ . By Lemma 3.7, we have  $\sigma_\psi \in \text{Aut}_{A+B_{\text{tors}}}(B)$  and clearly  $\varphi_{\sigma_\psi} = \psi$ , so  $\varphi$  is surjective. We conclude that  $\varphi$  is an isomorphism.  $\square$

Combining the previous results, we obtain a fundamental exact sequence that provides our framework for the study of Kummer extensions.

**Proposition 3.12** ([Pal04, Corollary 3.12 and Corollary 3.18]). *Let  $B$  be an  $s$ -extension of  $A$ . There is an exact sequence*

$$0 \rightarrow \text{Hom}\left(\frac{B}{A + B_{\text{tors}}}, B_{\text{tors}}\right) \rightarrow \text{Aut}_A(B) \rightarrow \text{Aut}_{A_{\text{tors}}}(B_{\text{tors}}) \rightarrow 1.$$

*Moreover, the group  $\text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  acts on  $\text{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}})$  by composition.*

*Proof.* Notice that  $B_{\text{tors}}$  is  $A$ -normal in  $B$  by Example 3.9, so the restriction  $\text{Aut}_A(B) \rightarrow \text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  is surjective by Proposition 3.10, and its kernel is  $\text{Aut}_{A+B_{\text{tors}}}(B)$ . By Proposition 3.11 we have

$$\text{Aut}_{A+B_{\text{tors}}}(B) \cong \text{Hom}(B/(A+B_{\text{tors}}), B_{\text{tors}})$$

so we get the desired exact sequence.

It follows from the existence of the exact sequence above and by Remark 2.9 that the group  $\text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  acts naturally on  $\text{Hom}(B/(A+B_{\text{tors}}), B_{\text{tors}})$ . Let now  $\psi \in \text{Hom}(B/(A+B_{\text{tors}}), B_{\text{tors}})$  correspond to the automorphism  $\sigma_\psi : b \rightarrow b + \psi([b])$  via the isomorphism of Proposition 3.11, and let  $\tau \in \text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$ . Let moreover  $\tilde{\tau}$  be any lift of  $\tau$  to  $\text{Aut}_A(B)$ . Then for every  $b \in B$  we have

$$\begin{aligned} (\tilde{\tau} \circ \sigma_\psi \circ \tilde{\tau}^{-1})(b) &= \tilde{\tau}(\tilde{\tau}^{-1}(b) + \psi([\tilde{\tau}^{-1}(b)])) = \\ &= b + \tilde{\tau}(\psi([\tilde{\tau}^{-1}(b)])) \end{aligned}$$

and since  $\tilde{\tau}^{-1}$  fixes  $A$ , as in the proof of Proposition 3.11 we have that  $\tilde{\tau}^{-1}(b) - b \in B_{\text{tors}}$ . It follows that  $\psi([\tilde{\tau}^{-1}(b)]) = \psi([b])$ , so

$$(\tilde{\tau} \circ \sigma_\psi \circ \tilde{\tau}^{-1})(b) = b + \tilde{\tau}(\psi([b])) = b + (\tau \circ \psi)([b]),$$

where the last equality follows from the fact that  $\psi([b]) \in B_{\text{tors}}$ . We conclude that the natural action of  $\text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  on  $\text{Hom}(B/(A+B_{\text{tors}}), B_{\text{tors}})$  is given by composition.  $\square$

### 3.3 Profinite structure of automorphism groups

Fix for the remainder of this section a finitely generated abelian group  $A$ . For any  $s$ -extension  $B$  of  $A$  and for any positive integer  $n$  we can consider the group  $B_n$  and its automorphism group  $\text{Aut}_A(B_n)$  which, according to the following proposition, is finite.

**Proposition 3.13.** *Let  $B$  be an  $s$ -extension of  $A$  and assume that  $B/A$  has finite exponent. Then the automorphism group  $\text{Aut}_A(B)$  is finite.*

*Proof.* In view of Proposition 3.12 it is enough to prove that  $\text{Hom}(B/(A+B_{\text{tors}}), B_{\text{tors}})$  and  $\text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  are finite. But this follows from the fact that both  $B_{\text{tors}}$  and  $B/(A+B_{\text{tors}})$  are finite, since  $A$  is finitely generated,  $B/A$  has finite exponent and  $B_{\text{tors}}$  embeds in  $(\mathbb{Q}/\mathbb{Z})^s$ .  $\square$

Let  $B$  be an  $s$ -extension of  $A$ . By Proposition 3.12 for every positive  $n$  we have an exact sequence

$$0 \rightarrow \text{Hom}\left(\frac{B_n}{A+B_{n,\text{tors}}}, B_{n,\text{tors}}\right) \rightarrow \text{Aut}_A(B_n) \rightarrow \text{Aut}_{A_{\text{tors}}}(B_{n,\text{tors}}) \rightarrow 1$$

and for every  $n \mid m$  the restriction maps make the following diagram commute:

$$\begin{array}{ccccccc}
 0 \longrightarrow \operatorname{Hom}\left(\frac{B_m}{A+B_{m,\text{tors}}}, B_{m,\text{tors}}\right) & \longrightarrow & \operatorname{Aut}_A(B_m) & \longrightarrow & \operatorname{Aut}_{A_{\text{tors}}}(B_{m,\text{tors}}) & \longrightarrow & 1 \\
 & \downarrow & \downarrow & & \downarrow & & \\
 0 \longrightarrow \operatorname{Hom}\left(\frac{B_n}{A+B_{n,\text{tors}}}, B_{n,\text{tors}}\right) & \longrightarrow & \operatorname{Aut}_A(B_n) & \longrightarrow & \operatorname{Aut}_{A_{\text{tors}}}(B_{n,\text{tors}}) & \longrightarrow & 1
 \end{array}$$

Notice that the rows of this diagram are exact and that every vertical map is surjective by Proposition 3.10. In fact, we have

- The map on the left is, once we apply Proposition 3.11, the restriction map

$$\operatorname{Aut}_{A+B_{m,\text{tors}}}(B_m) \rightarrow \operatorname{Aut}_{A+B_{n,\text{tors}}}(B_n)$$

and  $A+B_{n,\text{tors}}$  is  $A$ -normal in  $A+B_{m,\text{tors}}$  by Proposition 3.8 (notice that the image of any  $A$ -homomorphism from  $A+B_{n,\text{tors}}$  to  $A+B_{m,\text{tors}}$  is contained in  $A+B_{n,\text{tors}}$ ).

- The group  $B_n$  is  $A$ -normal in  $B_m$  by Example 3.9(2) and Proposition 3.8.
- The groups  $B_{n,\text{tors}}$  and  $B_{m,\text{tors}}$  are  $s$ -extensions of  $A_{\text{tors}}$ , and  $B_{n,\text{tors}}$  is  $A_{\text{tors}}$ -normal in  $B_{m,\text{tors}}$  by Example 3.9(1) and Proposition 3.8.

**Proposition 3.14.** *Let  $B$  be an  $s$ -extension of  $A$ . The groups  $\operatorname{Aut}_A(B_n)$  together with the natural restriction maps  $\rho_{nm} : \operatorname{Aut}_A(B_m) \rightarrow \operatorname{Aut}_A(B_n)$  for  $n \mid m$  form a projective system. The group  $\operatorname{Aut}_A(B)$  together with the natural restriction maps  $\rho_n : \operatorname{Aut}_A(B) \rightarrow \operatorname{Aut}_A(B_n)$  is the limit of this projective system.*

*Proof.* By Proposition 3.10 the restriction map  $\rho_m : \operatorname{Aut}_A(B) \rightarrow \operatorname{Aut}_A(B_m)$  is surjective for every  $m$ . Since for every  $n \mid m$  we have  $\rho_n = \rho_{nm} \circ \rho_m$ , the map  $\rho_{nm}$  is surjective as well. These maps are clearly compatible, so they form a projective system.

Let  $G$  be any group with a compatible system of maps  $\varphi_n : G \rightarrow \operatorname{Aut}_A(B_n)$ . Then we can define a map  $\varphi : G \rightarrow \operatorname{Aut}_A(B)$  by letting for every  $g \in G$  and every  $b \in B$

$$\varphi(g)(b) := \varphi_n(g)(b)$$

where  $n$  is such that  $b \in B_n$ . It is easy to check that this map is well-defined and that it is the unique map  $G \rightarrow \operatorname{Aut}_A(B)$  compatible with the projections.  $\square$



From the above proposition it follows that the projective limit of these exact sequences is the same exact sequence of Proposition 3.12:

$$0 \rightarrow \operatorname{Hom}\left(\frac{B}{A + B_{\text{tors}}}, B_{\text{tors}}\right) \rightarrow \operatorname{Aut}_A(B) \rightarrow \operatorname{Aut}_{A_{\text{tors}}}(B_{\text{tors}}) \rightarrow 1.$$

Since this sequence is a projective limit we can endow the groups involved with the natural profinite topology by giving each finite group the discrete topology. The maps appearing in the exact sequence above are then continuous and, in particular,  $\operatorname{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}})$  and  $\operatorname{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  have the subspace and quotient topology, respectively (see Lemma 2.10). Notice also that  $\operatorname{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}})$ , being the kernel of a continuous homomorphism, is a closed normal subgroup of  $\operatorname{Aut}_A(B)$ .

We have obtained the following refinement of Proposition 3.12.

**Proposition 3.15.** *Let  $B$  be an  $s$ -extension of  $A$ . The group  $\operatorname{Aut}_A(B)$  together with the natural restriction maps is the projective limit of the finite groups  $\operatorname{Aut}_A(B_n)$ , thus it is a profinite group. In particular,  $\operatorname{Aut}_A(B)$  is a compact Hausdorff topological group.*

*There is an exact sequence of profinite groups*

$$0 \rightarrow \operatorname{Hom}\left(\frac{B}{A + B_{\text{tors}}}, B_{\text{tors}}\right) \rightarrow \operatorname{Aut}_A(B) \rightarrow \operatorname{Aut}_{A_{\text{tors}}}(B_{\text{tors}}) \rightarrow 1.$$

*Moreover, the group  $\operatorname{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$  acts on  $\operatorname{Hom}(B/(A + B_{\text{tors}}), B_{\text{tors}})$  by composition, and the action is continuous.*

### 3.4 Full $s$ -extensions

In this section we give a characterization of the *maximal  $s$ -extensions* of [Pal04, Section 2.2]. We will not prove here the maximality of these extensions in the sense of [Pal04, Theorem 2.6], hence the change of name to *full  $s$ -extensions*. Our motivation for the study of these kind of extensions is that they provide a useful abstraction for the set of points of a commutative algebraic group that have a multiple in a fixed subgroup of rational points, in other words it is “full” of all division points. However, the equivalence of the two definitions follows immediately from Proposition 3.19.

**Definition 3.16.** Let  $A$  be a finitely generated abelian group. An  $s$ -extension  $\Gamma$  of  $A$  is called *full* if  $\Gamma$  is a divisible abelian group and  $\Gamma_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z})^s$ .

**Remark 3.17.** Recall from Remark 3.2 that a necessary condition for  $A$  to admit any  $s$ -extension is that  $A_{\text{tors}}$  can be embedded in  $(\mathbb{Q}/\mathbb{Z})^s$ . This condition is also sufficient for  $A$  to admit a full  $s$ -extension. To see this, fix an isomorphism

$A \cong \mathbb{Z}^{\text{rk}(A)} \oplus T$ , where  $T$  is a finite subgroup of  $(\mathbb{Q}/\mathbb{Z})^s$ . Then the natural inclusion  $\mathbb{Z}^{\text{rk}(A)} \oplus T \hookrightarrow \mathbb{Q}^{\text{rk}(A)} \oplus (\mathbb{Q}/\mathbb{Z})^s$  realizes  $\mathbb{Q}^{\text{rk}(A)} \oplus (\mathbb{Q}/\mathbb{Z})^s$  as a full  $s$ -extension of  $A$ .

**Remark 3.18.** Let  $\Gamma$  be a full  $s$ -extension of a finitely generated abelian group  $A$ . Then  $\Gamma_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z})^s$  is a divisible abelian group. It follows that the exact sequence

$$0 \rightarrow \Gamma_{\text{tors}} \rightarrow \Gamma \rightarrow \Gamma/\Gamma_{\text{tors}} \rightarrow 0$$

splits (non-canonically), so that  $\Gamma \cong (\Gamma/\Gamma_{\text{tors}}) \oplus \Gamma_{\text{tors}} \cong (\Gamma/\Gamma_{\text{tors}}) \oplus (\mathbb{Q}/\mathbb{Z})^s$ .

The following proposition shows in particular that a finitely generated abelian group  $A$  can have at most one full  $s$ -extension, up to (a not necessarily unique) isomorphism.

**Proposition 3.19.** *Let  $A$  be a finitely generated abelian group of rank  $r$  which admits a full  $s$ -extension  $\Gamma$ . There is a canonical isomorphism*

$$\Gamma/\Gamma_{\text{tors}} \xrightarrow{\sim} A \otimes_{\mathbb{Z}} \mathbb{Q} \quad (3.1)$$

that sends the subgroup  $A/A_{\text{tors}}$  of  $\Gamma/\Gamma_{\text{tors}}$  to  $\overline{A} := \{a \otimes 1 \mid a \in A\}$ .

Moreover, there is an isomorphism

$$\Gamma \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s \quad (3.2)$$

that sends  $A$  to  $\mathbb{Z}^r \subseteq \mathbb{Q}^r$ .

*Proof.* Since  $\Gamma/A$  is torsion, for every  $b \in \Gamma$  there is an integer  $n \geq 1$  such that  $nb \in A$ . Let  $n_b := \min\{n \in \mathbb{N}_{\geq 1} \mid nb \in A\}$ . We define a map

$$\begin{aligned} \psi : \Gamma &\longrightarrow A \otimes_{\mathbb{Z}} \mathbb{Q} \\ b &\longmapsto (n_b b) \otimes \frac{1}{n_b}. \end{aligned}$$

The map  $\psi$  is a group homomorphism. To see this, notice first that for every  $b \in \Gamma$  and every  $n \in \mathbb{N}_{\geq 1}$  such that  $nb \in A$  we have  $(nb) \otimes \frac{1}{n} = (n_b b) \otimes \frac{1}{n_b}$ . Then for every  $b, c \in \Gamma$  we have

$$\begin{aligned} \psi(b+c) &= n_{b+c}(b+c) \otimes \frac{1}{n_{b+c}} = n_b n_c (b+c) \otimes \frac{1}{n_b n_c} = \\ &= (n_b n_c b) \otimes \frac{1}{n_b n_c} + (n_b n_c c) \otimes \frac{1}{n_b n_c} = \\ &= (n_b b) \otimes \frac{1}{n_b} + (n_c c) \otimes \frac{1}{n_c} = \\ &= \psi(b) + \psi(c). \end{aligned}$$

The map  $\psi$  is also surjective: in fact, let  $a \in A$  and  $n \in \mathbb{N}_{\geq 1}$ . Since  $\Gamma$  is divisible, there must be an element  $b \in \Gamma$  such that  $nb = a$ , and thus  $\psi(b) = a \otimes \frac{1}{n}$ .

Now we show that the  $\ker \psi = \Gamma_{\text{tors}}$ . If  $b \in \Gamma$  has order  $n \geq 1$ , then  $\psi(b) = (nb) \otimes \frac{1}{n} = 0$ , showing that  $b \in \ker \psi$ . On the other hand, if  $\psi(b) = (n_b b) \otimes \frac{1}{n_b} = 0$ , then necessarily  $n_b b = 0$ , so that  $b \in \Gamma_{\text{tors}}$ . So we get an isomorphism which sends  $A/A_{\text{tors}}$  to  $\bar{A}$ .

For the second part, since  $A$  has rank  $r$  we have  $A \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r$ . It follows from the first part that there is an isomorphism  $\Gamma/\Gamma_{\text{tors}} \xrightarrow{\sim} \mathbb{Q}^r$  that sends  $A/A_{\text{tors}}$  to  $\mathbb{Z}^r \subseteq \mathbb{Q}^r$ . The conclusion follows by combining this with any isomorphism  $\Gamma \xrightarrow{\sim} (\Gamma/\Gamma_{\text{tors}}) \oplus (\mathbb{Q}/\mathbb{Z})^s$  (see Remark 3.18).  $\square$

**Remark 3.20.** In Proposition 3.19 the isomorphism (3.1) is canonical, while the isomorphism (3.2) depends on the choice of three isomorphisms: an isomorphism between  $A \otimes_{\mathbb{Z}} \mathbb{Q}$  and  $\mathbb{Q}^r$  (or, equivalently, a choice of a  $\mathbb{Z}$ -basis of  $A/A_{\text{tors}}$ ), a splitting isomorphism  $\Gamma \cong (\Gamma/\Gamma_{\text{tors}}) \oplus \Gamma_{\text{tors}}$  (see Remark 3.18) and an isomorphism  $\Gamma_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z})^s$ .

### 3.5 Automorphisms of full $s$ -extensions

For this section, let  $A$  be a finitely generated and torsion-free abelian group of rank  $r$  and let  $\Gamma$  be a full  $s$ -extension of  $A$ . Notice that, since  $A_{\text{tors}} = 0$ , we have  $\text{Aut}_{A_{\text{tors}}}(\Gamma_{\text{tors}}) = \text{Aut}(\Gamma_{\text{tors}})$  and  $\Gamma_{n,\text{tors}} = \Gamma[n]$  for every  $n > 0$ . By Proposition 3.19 we can fix an isomorphism

$$\Phi : \Gamma \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s$$

that maps  $A$  onto  $\mathbb{Z}^r \subseteq \mathbb{Q}^r$ . This induces isomorphisms

$$\begin{aligned} \Phi_{\text{kumm}} : \quad & \frac{\Gamma}{A + \Gamma_{\text{tors}}} \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})^r, \\ \Phi_{\text{tors}} : \quad & \Gamma_{\text{tors}} \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})^s. \end{aligned}$$

Recall from Remark 2.2 that we have canonical isomorphisms

$$\begin{aligned} \text{Aut}((\mathbb{Q}/\mathbb{Z})^s) &\cong \text{GL}_s(\widehat{\mathbb{Z}}), \\ \text{Hom}((\mathbb{Q}/\mathbb{Z})^r, (\mathbb{Q}/\mathbb{Z})^s) &\cong \text{Mat}_{s \times r}(\widehat{\mathbb{Z}}) \end{aligned}$$

under which the action of  $\text{Aut}((\mathbb{Q}/\mathbb{Z})^s)$  on  $\text{Hom}((\mathbb{Q}/\mathbb{Z})^r, (\mathbb{Q}/\mathbb{Z})^s)$  given by composition becomes matrix multiplication on the left. So we get isomorphisms

$$\begin{aligned} \Phi_{\text{kumm}}^* : \quad & \text{Hom}\left(\frac{\Gamma}{A + \Gamma_{\text{tors}}}, \Gamma_{\text{tors}}\right) \xrightarrow{\sim} \text{Mat}_{s \times r}(\widehat{\mathbb{Z}}), \\ \Phi_{\text{tors}}^* : \quad & \text{Aut}(\Gamma_{\text{tors}}) \xrightarrow{\sim} \text{GL}_s(\widehat{\mathbb{Z}}). \end{aligned}$$

On the finite level, these isomorphisms induce, for every  $n > 0$ , isomorphisms

$$\begin{aligned} \psi_n : \operatorname{Hom}\left(\frac{\Gamma_n}{A + \Gamma[n]}, \Gamma[n]\right) &\xrightarrow{\sim} \operatorname{Mat}_{s \times r}(\mathbb{Z}/n\mathbb{Z}) \\ \varphi_n : \operatorname{Aut}(\Gamma[n]) &\xrightarrow{\sim} \operatorname{GL}_s(\mathbb{Z}/n\mathbb{Z}) \end{aligned}$$

which are compatible with the natural projections, in the sense that for every  $n \mid m$  the diagrams

$$\begin{array}{ccc} \operatorname{Hom}\left(\frac{\Gamma_m}{A + \Gamma[m]}, \Gamma[m]\right) & \xrightarrow{\psi_m} & \operatorname{Mat}_{s \times r}(\mathbb{Z}/m\mathbb{Z}) \\ \downarrow & & \downarrow \\ \operatorname{Hom}\left(\frac{\Gamma_n}{A + \Gamma[n]}, \Gamma[n]\right) & \xrightarrow{\psi_n} & \operatorname{Mat}_{s \times r}(\mathbb{Z}/n\mathbb{Z}) \end{array}$$

and

$$\begin{array}{ccc} \operatorname{Aut}(\Gamma[m]) & \xrightarrow{\varphi_m} & \operatorname{GL}_s(\mathbb{Z}/m\mathbb{Z}) \\ \downarrow & & \downarrow \\ \operatorname{Aut}(\Gamma[n]) & \xrightarrow{\varphi_n} & \operatorname{GL}_s(\mathbb{Z}/n\mathbb{Z}) \end{array}$$

commute. This shows that the topology with which we endowed our automorphism groups coincides with the natural topology of the  $\widehat{\mathbb{Z}}$ -matrix rings, as stated in the following proposition.

**Proposition 3.21.** *Let  $A$  be a finitely generated and torsion-free abelian group of rank  $r$  and let  $\Gamma$  be a full  $s$ -extension of  $A$ . Consider the group  $\operatorname{Aut}_A(\Gamma)$  with the profinite topology described in Section 3.3 and the groups  $\operatorname{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  and  $\operatorname{GL}_s(\widehat{\mathbb{Z}})$  with the topology induced by the profinite topology of  $\widehat{\mathbb{Z}}$ .*

*Then every isomorphism of abelian groups*

$$\Phi : \Gamma \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s$$

*that maps  $A$  onto  $\mathbb{Z}^r \subseteq \mathbb{Q}^r$  induces isomorphisms of topological groups*

$$\begin{aligned} \Phi_{\text{kumm}}^* : \operatorname{Hom}\left(\frac{\Gamma}{A + \Gamma_{\text{tors}}}, \Gamma_{\text{tors}}\right) &\xrightarrow{\sim} \operatorname{Mat}_{s \times r}(\widehat{\mathbb{Z}}), \\ \Phi_{\text{tors}}^* : \operatorname{Aut}(\Gamma_{\text{tors}}) &\xrightarrow{\sim} \operatorname{GL}_s(\widehat{\mathbb{Z}}). \end{aligned}$$

*Moreover, the action of  $\operatorname{Aut}(\Gamma_{\text{tors}})$  on  $\operatorname{Hom}(\Gamma/(A + \Gamma_{\text{tors}}), \Gamma_{\text{tors}})$  given by composition is identified under these isomorphisms with matrix multiplication on the left.*

## 4 Some linear algebra

Motivated by the results of the previous sections we will now establish some results of linear algebra over the ring  $\widehat{\mathbb{Z}}$ . In particular, we are interested in certain properties of  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  as a left  $\text{Mat}_{s \times s}(\widehat{\mathbb{Z}})$ -module.

Fix for this section two non-negative integers  $s$  and  $r$ .

**Proposition 4.1.** *Let  $R := \text{Mat}_{s \times s}(\widehat{\mathbb{Z}})$  and view  $M := \text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  as a left  $R$ -module. Let  $V \subseteq M$  be a left  $R$ -submodule. Assume that there is a positive integer  $n$  such that, viewing the elements of  $V$  as maps  $(\mathbb{Q}/\mathbb{Z})^r \rightarrow (\mathbb{Q}/\mathbb{Z})^s$ , we have*

$$\bigcap_{f \in V} \ker f \subseteq (\mathbb{Q}/\mathbb{Z})^r [n]. \quad (4.1)$$

Then  $V \supseteq nM$ .

*Proof.* Let  $L$  denote the right  $R$ -module  $\widehat{\mathbb{Z}}^s$  of row vectors and let  $N$  denote the left  $R$ -module  $\widehat{\mathbb{Z}}^s$  of column vectors. Notice that there is a natural  $R$ -module isomorphism, obtained by applying  $\otimes_R M$  to the natural isomorphism  $N \otimes_{\widehat{\mathbb{Z}}} L \rightarrow R$ :

$$\begin{aligned} N \otimes_{\widehat{\mathbb{Z}}} L \otimes_R M &\rightarrow M \\ x \otimes y \otimes m &\mapsto x \cdot y \cdot m \end{aligned}$$

whose inverse is

$$\begin{aligned} \psi: M &\rightarrow N \otimes_{\widehat{\mathbb{Z}}} L \otimes_R M \\ m &\mapsto \sum_{i=1}^s e_i \otimes f_i \otimes m \end{aligned}$$

where  $\{e_i\}$  and  $\{f_i\}$  are the canonical bases for  $N$  and  $L$  respectively.

Consider now the abelian group  $M_L := L \otimes_R M$ , which is isomorphic to  $\widehat{\mathbb{Z}}^r$  via

$$\begin{aligned} L \otimes_R M &\rightarrow \widehat{\mathbb{Z}}^r \\ y \otimes v &\mapsto y \cdot v \end{aligned}$$

and its subgroup

$$V_L = \langle y \otimes v \mid y \in L, v \in V \rangle.$$

Condition (4.1) implies that, seeing the elements of  $V_L$  as maps  $(\mathbb{Q}/\mathbb{Z})^r \rightarrow \mathbb{Q}/\mathbb{Z}$ , we have  $\bigcap_{f \in V_L} \ker f \subseteq (\mathbb{Q}/\mathbb{Z})^r [n]$ . Then by Pontryagin duality (Theorem 2.3) we have  $V_L \supseteq nM_L$ .

The image of  $V$  in  $N \otimes_{\widehat{\mathbb{Z}}} L \otimes_R M$  under the isomorphism  $\psi$  is

$$\psi(V) = \langle x \otimes y \otimes v \mid x \in N, y \in L, v \in V \rangle = \langle x \otimes v_L \mid x \in N, v_L \in V_L \rangle$$

and since

$$\begin{aligned} n(N \otimes_{\widehat{\mathbb{Z}}} L \otimes_R M) &= \langle n(x \otimes y \otimes v) \mid x \in N, y \in L, v \in M \rangle = \\ &= \langle x \otimes n(y \otimes v) \mid x \in N, y \in L, v \in M \rangle = \\ &= \langle x \otimes w \mid x \in N, w \in nM_L \rangle \end{aligned}$$

we have

$$\psi(V) \supseteq n(N \otimes_{\widehat{\mathbb{Z}}} L \otimes_R M)$$

which is equivalent to  $V \supseteq nM$ .  $\square$

**Lemma 4.2.** *Let  $R$  be a compact topological ring and let  $M$  be a compact topological  $R$ -module. Let  $T \subseteq R$  be a subring of  $R$  and let  $S$  denote the smallest closed subring of  $R$  containing  $T$ . If  $V \subseteq M$  is a closed  $T$ -submodule, then  $V$  is also an  $S$ -module.*

*Proof.* Let  $v \in V$  and consider the continuous map

$$\begin{aligned} f_v : R &\rightarrow M \\ x &\mapsto xv \end{aligned}$$

Since  $S$  is the closure of  $T$  in  $R$ , we have

$$\begin{aligned} f_v(S) &= f_v \left( \bigcap \{C \mid C \text{ closed}, T \subseteq C \subseteq R\} \right) \\ &\subseteq \bigcap \{f_v(C) \mid C \text{ closed}, T \subseteq C \subseteq R\}. \end{aligned}$$

For any closed subset  $D$  of  $M$  containing  $f(T)$  we have that  $f^{-1}(D)$  is closed and contains  $T$  and  $f(f^{-1}(D)) \subseteq D$ , so  $f_v(S)$  is contained in the closure of  $f(T)$ .

Since  $V$  is a  $T$ -module, we have  $f_v(T) \subseteq V$ , and since  $V$  is closed we have  $f_v(S) \subseteq V$  by what we have just said. Since this holds for any  $v \in V$ , we conclude that  $V$  is an  $S$ -module.  $\square$

The following proposition is essentially a generalization of [Chapter 1, Proposition 4.12(1)].

**Proposition 4.3.** *Let  $R := \text{Mat}_{s \times s}(\mathbb{Z}_\ell)$  and view  $M := \text{Mat}_{s \times r}(\mathbb{Z}_\ell)$  as a left  $R$ -module. Let  $H$  be a closed subgroup of  $\text{GL}_s(\mathbb{Z}_\ell)$  and  $V \subseteq M$  a closed left  $H$ -submodule. Let  $W = R \cdot V$  and let  $S$  denote the closed  $\mathbb{Z}_\ell$ -subalgebra of  $R$  generated by  $H$ . Suppose that there are non-negative integers  $n$  and  $m$  such that*

(1)  $W \supseteq \ell^n M$  and

(2)  $S \supseteq \ell^m R$ .

Then we have  $V \supseteq \ell^{n+m} M$ .

*Proof.* Let  $T$  denote the (not necessarily closed)  $\mathbb{Z}_\ell$ -subalgebra of  $R$  generated by  $H$ , so that  $S$  is the closure of  $T$ . It is clear that  $V$ , being both a  $\mathbb{Z}_\ell$ -module and an  $H$ -module, is a  $T$ -module. Since it is closed,  $V$  is also an  $S$ -module by Lemma 4.2 above.

Then we have  $V \supseteq S \cdot V \supseteq \ell^m R \cdot V = \ell^m W \supseteq \ell^m \cdot \ell^n M$ .  $\square$

The following result is an adelic version of Proposition 4.3.

**Proposition 4.4.** *Let  $R := \text{Mat}_{s \times s}(\widehat{\mathbb{Z}})$  and view  $M := \text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  as a left  $R$ -module. Let  $H$  be a closed subgroup of  $\text{GL}_s(\widehat{\mathbb{Z}})$  and let  $V \subseteq M$  be a closed left  $H$ -submodule. Let  $W = R \cdot V$  and, for every prime  $\ell$ , let  $H_\ell$  denote the image of  $H$  under the projection  $\text{GL}_s(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_s(\mathbb{Z}_\ell)$  and let  $\mathbb{Z}_\ell[H_\ell]$  denote the closed sub- $\mathbb{Z}_\ell$ -algebra of  $\text{Mat}_{s \times s}(\mathbb{Z}_\ell)$  generated by  $H_\ell$ . Suppose that there are positive integers  $n$  and  $m$  such that*

(1)  $W \supseteq nM$ ;

(2) For every prime  $\ell$  we have  $\mathbb{Z}_\ell[H_\ell] \supseteq m \text{Mat}_{s \times s}(\mathbb{Z}_\ell)$ .

Then we have  $V \supseteq nmM$ .

*Proof.* Let  $R_\ell := \text{Mat}_{s \times s}(\mathbb{Z}_\ell)$  and  $M_\ell := \text{Mat}_{s \times r}(\mathbb{Z}_\ell)$ , so that

$$R = \prod_{\ell} R_\ell \quad \text{and} \quad M = \prod_{\ell} M_\ell.$$

Let moreover  $V_\ell$  and  $W_\ell$  denote the images of  $V$  and  $W$  in  $M_\ell$ , respectively. Notice that  $V_\ell$  is an  $H_\ell$ -submodule of  $M_\ell$  and that  $W_\ell$  is the  $R_\ell$ -submodule of  $M_\ell$  generated by  $V_\ell$ .

By (1) we have that  $W_\ell$  contains the image of  $nM$  in  $M_\ell$ , which is  $nM_\ell$ . By (2) we have  $\mathbb{Z}_\ell[H_\ell] \supseteq m \text{Mat}_{s \times s}(\mathbb{Z}_\ell)$ , so we can apply Proposition 4.3 and deduce that  $V_\ell \supseteq nmM_\ell$ .

We claim that  $V = \prod_{\ell} V_\ell$ , seen as a subgroup of  $\prod_{\ell} M_\ell$ . Clearly  $V \subseteq \prod_{\ell} V_\ell$ , since every  $v \in V$  is equal to the tuple  $(e_\ell v)_\ell$ , where  $e_\ell \in \widehat{\mathbb{Z}} = \prod \mathbb{Z}_p$  is the element whose  $\ell$ -component is 1 and whose  $p$ -component is 0 for all  $p \neq \ell$ . For the other inclusion, let  $(w_\ell)_\ell \in \prod_{\ell} V_\ell$ . Since  $V_\ell$  is the image of  $V$  under the natural projection, for every  $\ell$  there must be  $\tilde{w}_\ell \in V$  whose  $\ell$ -component is  $w_\ell$ . Then the infinite sum

$$\sum_{\ell} e_\ell \tilde{w}_\ell$$

converges to  $(w_\ell)_\ell$  in  $M$ : consider the sequence of partial sums

$$\{x_k\}_{k \in \mathbb{N}} = \left\{ \sum_{\ell \leq k} e_\ell \tilde{w}_\ell \right\}_{k \in \mathbb{N}}$$

and let  $U \subseteq M$  be an open neighbourhood of  $(w_\ell)_\ell$ , which must be of the form

$$\prod_{\ell \leq N} U_\ell \times \prod_{\ell > N} M_\ell$$

for some integer  $N$  and some open neighbourhoods  $U_\ell$  of  $w_\ell$  in  $M_\ell$ ; then clearly  $x_k \in U$  for all  $k \geq N$ .

Since  $V$  is closed in  $M$ , we must then have  $(w_\ell)_\ell \in V$ , which shows that  $V = \prod_\ell V_\ell$ .

Since for every prime  $\ell$  the multiplication-by- $\ell$  endomorphism on a  $\widehat{\mathbb{Z}}$ -module is invertible on all prime-to- $\ell$  components, we have  $\prod_\ell nmM_\ell = \prod_\ell \ell^{v_\ell(nm)} M_\ell = nmM$ , so

$$V = \prod_\ell V_\ell \supseteq \prod_\ell nmM_\ell = nmM$$

and we conclude.  $\square$

## 5 General entanglement theory

### 5.1 Initial remarks and definitions

Fix a number field  $K$  and an algebraic closure  $\overline{K}$  of  $K$ . Let  $G$  be a commutative connected algebraic group over  $K$ . It is well-known that there is a non-negative integer  $s$ , depending only on  $G$ , such that  $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$  for all integers  $n > 1$ . For example, if  $G$  is an abelian variety of dimension  $g$ , we have  $s = 2g$ .

Let  $A \subseteq G(K)$  be a finitely generated and torsion-free subgroup of rank  $r$  and consider the *divisible hull* of  $A$  in  $G(\overline{K})$

$$\Gamma := \{P \in G(\overline{K}) \mid \exists n \in \mathbb{N}_{\geq 1} : nP \in A\} \quad (5.1)$$

which is a subgroup of  $G(\overline{K})$  and a full  $s$ -extension of  $A$ .

We have  $\Gamma_{\text{tors}} = G(\overline{K})_{\text{tors}}$ , which we will also denote by  $G_{\text{tors}}$ . We also have

$$A + G(K)_{\text{tors}} \subseteq \Gamma \cap G(K).$$

The quotient group  $(\Gamma \cap G(K))/(A + G(K)_{\text{tors}})$ , being a quotient of a subgroup of  $\Gamma/A$ , is always a torsion group.



**Definition 5.1.** We call any integer  $d_A > 1$  such that  $d_A(\Gamma \cap G(K)) \subseteq A + G(K)_{\text{tors}}$  a *divisibility parameter* for  $A$  in  $G(K)$ . If such an integer exists, we say that  $A$  has *finite divisibility* in  $G(K)$ .

**Example 5.2.** (1) If  $G(K)$  is finitely generated, every torsion-free subgroup  $A \subseteq G(K)$  has finite divisibility in  $G(K)$ : in fact, the abelian group  $(\Gamma \cap G(K))/(A + G(K)_{\text{tors}})$  is torsion and finitely generated, so it is finite.

(2) Let  $G = \mathbb{G}_m$  be the multiplicative group, so that  $s = 1$ . In this case  $G(K) = K^\times$  is not finitely generated, but it still holds that every finitely generated  $A \subseteq G(K)$  has finite divisibility. In order to prove this it is enough to show that for every prime number  $\ell$  there is a non-negative integer  $m_\ell$  such that the  $\ell$ -power torsion of  $(\Gamma \cap G(K))/(A + G(K)_{\text{tors}})$  is contained in

$$\frac{\Gamma \cap G(K)}{A + G(K)_{\text{tors}}}[\ell^{m_\ell}]$$

and that we can take  $m_\ell = 0$  for all but finitely many primes  $\ell$ . The first part is just [DP16, Lemma 12]. As for the second part, assume that  $A$  admits a strongly  $\ell$ -independent basis  $a_1, \dots, a_r$  as in [PS19, Definition 2.1], which is true for all but finitely many  $\ell$  by [PS19, Theorem 2.7]. Let  $b \in \Gamma \cap K^\times$  be such that  $b^{\ell^m} \in A \cdot \mu(K)$  for some  $m \geq 1$ . Then

$$b^{\ell^m} = \zeta \cdot \prod_{i=1}^r a_i^{x_i}$$

for some  $x_1, \dots, x_r \in \mathbb{Z}$  and some root of unity  $\zeta \in K$  of order a power of  $\ell$ . Since the  $a_i$  are strongly  $\ell$ -independent, every  $x_i$  is divisible by  $\ell^m$ . This means that  $b \in A \cdot \mu(K) = A + G(K)_{\text{tors}}$ , so we can take  $m_\ell = 0$ .

Notice that the cited results are fully explicit, so a divisibility parameter for  $A$  is effectively computable.

(3) Let  $G = \mathbb{G}_a$  be the additive group, so that  $s = 0$ . In this case no non-trivial subgroup  $A \subseteq G(K)$  has finite divisibility. In fact we have

$$\Gamma = \{b \in \overline{K} \mid \exists n \in \mathbb{N}_{\geq 1} \text{ such that } nb \in A\} \subseteq K.$$

Then  $(\Gamma \cap G(K))/A = \Gamma/A$  contains elements of unbounded order. Since  $\Gamma \subseteq G(K)$ , *Kummer theory for the additive group is trivial*.

## 5.2 Torsion and Kummer representations and the entanglement group

Fix for the rest of the section a finitely generated subgroup  $A \subseteq G(K)$ . For simplicity, we will denote  $K(G_{\text{tors}})$  by  $K_\infty$ . We are interested in studying the

tower of extensions  $K(\Gamma) \mid K_\infty \mid K$ . Notice that  $K(\Gamma)$  is a Galois extension of  $K$ : in fact it is the union of its finite subextensions of the form  $K(\Gamma_n)$ , where  $\Gamma_n = \{P \in G(\overline{K}) \mid nP \in A\}$ , which are Galois. Similarly,  $K_\infty \mid K$  is Galois, since it is the union of the finite Galois extensions  $K_n := K(G[n])$  of  $K$ .

The action of  $\text{Gal}(\overline{K} \mid K)$  on  $G(\overline{K})$  gives rise, for every  $n \geq 1$ , to injective homomorphisms

$$\text{Gal}(K(\Gamma_n) \mid K_n) \hookrightarrow \text{Aut}_{A+G[n]}(\Gamma_n) \cong \text{Hom}\left(\frac{\Gamma_n}{A+G[n]}, G[n]\right),$$

$$\text{Gal}(K(\Gamma_n) \mid K) \hookrightarrow \text{Aut}_A(\Gamma_n),$$

$$\text{Gal}(K_n \mid K) \hookrightarrow \text{Aut}(G[n])$$

which by Proposition 3.15 fit into the commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Gal}(K(\Gamma_n) \mid K_n) & \longrightarrow & \text{Gal}(K(\Gamma_n) \mid K) & \longrightarrow & \text{Gal}(K_n \mid K) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Hom}\left(\frac{\Gamma_n}{A+G[n]}, G[n]\right) & \longrightarrow & \text{Aut}_A(\Gamma_n) & \longrightarrow & \text{Aut}(G[n]) \longrightarrow 1 \end{array}$$

Taking the projective limit we obtain the following commutative diagram of topological groups with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Gal}(K(\Gamma) \mid K_\infty) & \longrightarrow & \text{Gal}(K(\Gamma) \mid K) & \longrightarrow & \text{Gal}(K_\infty \mid K) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Hom}\left(\frac{\Gamma}{A+G_{\text{tors}}}, G_{\text{tors}}\right) & \longrightarrow & \text{Aut}_A(\Gamma) & \longrightarrow & \text{Aut}(G_{\text{tors}}) \longrightarrow 1 \end{array}$$

and the Krull topology on the Galois groups coincides with the subspace topology with respect to the automorphism groups.

**Definition 5.3.** We call the cokernel of the above defined map

$$\text{Gal}(K(\Gamma) \mid K_\infty) \hookrightarrow \text{Hom}\left(\frac{\Gamma}{A+G_{\text{tors}}}, G_{\text{tors}}\right)$$

the **entanglement group** of  $A$ , and we denote it by  $\text{Ent}(A)$ .

Fixing an isomorphism as in Proposition 3.19

$$\Phi : \Gamma \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s$$

that maps  $A$  to  $\mathbb{Z}^r \subseteq \mathbb{Q}^r$ , we get by Proposition 3.21 isomorphisms of topological groups

$$\begin{aligned} \Phi_{\text{kumm}}^* : \quad & \text{Hom}\left(\frac{\Gamma}{A + \Gamma_{\text{tors}}}, \Gamma_{\text{tors}}\right) \xrightarrow{\sim} \text{Mat}_{s \times r}(\widehat{\mathbb{Z}}), \\ \Phi_{\text{tors}}^* : \quad & \text{Aut}(\Gamma_{\text{tors}}) \xrightarrow{\sim} \text{GL}_s(\widehat{\mathbb{Z}}). \end{aligned}$$

Then we get a diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Gal}(K(\Gamma) \mid K_\infty) & \longrightarrow & \text{Gal}(K(\Gamma) \mid K) & \longrightarrow & \text{Gal}(K_\infty \mid K) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Mat}_{s \times r}(\widehat{\mathbb{Z}}) & \longrightarrow & \text{Aut}_{\mathbb{Z}^r}(\mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s) & \longrightarrow & \text{GL}_s(\widehat{\mathbb{Z}}) \longrightarrow 1 \end{array}$$

which we will refer to as the **torsion-Kummer representation** related to  $A$ . We will also call the map

$$\text{Gal}(K(\Gamma) \mid K_\infty) \hookrightarrow \text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$$

the **Kummer representation**, and the map

$$\text{Gal}(K_\infty \mid K) \hookrightarrow \text{GL}_s(\widehat{\mathbb{Z}})$$

the **torsion representation**.

**Definition 5.4.** We will denote by  $H(G)$  the image of  $\text{Gal}(K_\infty \mid K)$  in  $\text{GL}_s(\widehat{\mathbb{Z}})$  and by  $V(A)$  the image of  $\text{Gal}(K(\Gamma) \mid K_\infty)$  in  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$ .

Since all groups appearing in the diagram above are profinite and all the maps are continuous, it follows that  $V(A)$  and  $H(G)$  are closed subgroups of  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  and  $\text{GL}_s(\widehat{\mathbb{Z}})$ , respectively. One of our goals is proving that, under certain conditions,  $V(A)$  is also open. More precisely, we want to bound the order of  $\text{Ent}(A) \cong \text{Mat}_{s \times r}(\widehat{\mathbb{Z}})/V(A)$ .

**Remark 5.5.** It follows from the existence of the Kummer representation that for any  $n \geq 1$  the degree  $[K(n^{-1}A) : K(G[n])]$  divides  $n^{rs}$ .

**Remark 5.6.** The definition of entanglement group given here is different from that of [Pal14], where the entanglement group for  $G = \mathbb{G}_m$  is defined as the quotient of  $\text{Aut}_A(\Gamma)$  by the image of  $\text{Gal}(K(\Gamma) \mid K)$ , which in the cases considered there is a normal subgroup (see [Pal14, Theorem 1.6]). In fact, the entanglement group defined here is a subgroup of that of [Pal14].

We conclude this section by remarking the following fact.

**Lemma 5.7.** *Let  $G$  be a commutative connected algebraic group over a number field  $K$  and let  $A \subseteq G(K)$  be a finitely generated, torsion-free subgroup of  $G(K)$  of rank  $r$ . If  $\text{Ent}(A)$  is finite, then for every  $n \geq 1$*

$$\frac{n^{rs}}{[K(n^{-1}A) : K(G[n])]} \quad \text{divides} \quad \#\text{Ent}(A).$$

*Proof.* The image of  $V(A)$  under the natural quotient map  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}}) \rightarrow \text{Mat}_{s \times r}(\mathbb{Z}/n\mathbb{Z})$  is  $\text{Gal}(K_\infty(n^{-1}A) \mid K_\infty)$ , so the ratio

$$\frac{n^{rs}}{[K_\infty(n^{-1}A) : K_\infty]}$$

divides  $\#\text{Ent}(A)$ . In order to conclude it suffices to notice that

$$\begin{aligned} [K(n^{-1}A) : K(G[n])] &= \\ &= [K(n^{-1}A) : K_\infty \cap K(n^{-1}A)] \cdot [K_\infty \cap K(n^{-1}A) : K(G[n])] = \\ &= [K_\infty(n^{-1}A) : K_\infty] \cdot [K_\infty \cap K(n^{-1}A) : K(G[n])]. \end{aligned}$$

□

### 5.3 Bounding the entanglement group

We now give some sufficient conditions for the finiteness of the entanglement group  $\text{Ent}(A)$ . In particular, we want to explicitly bound its cardinality in terms of some known quantities. This will be accomplished by applying the results of Section 4.

Assume for the rest of this section that  $A$  has finite divisibility and that  $d_A$  is a divisibility parameter for  $A$  in  $G(K)$ . Consider the joint kernel of the elements of  $V(A)$ , that is

$$S(A) := \bigcap_{f \in V(A)} \ker f \subseteq (\mathbb{Q}/\mathbb{Z})^r.$$

where we consider elements of  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  as maps  $(\mathbb{Q}/\mathbb{Z})^r \rightarrow (\mathbb{Q}/\mathbb{Z})^s$ . The image of any  $[b] \in \Gamma/(A + G_{\text{tors}})$  in  $(\mathbb{Q}/\mathbb{Z})^r$  is in the kernel of every  $f \in V(A)$  if and only if  $b$  is fixed by every automorphism  $\sigma \in \text{Gal}(K(\Gamma) \mid K_\infty)$ , that is if and only if  $b \in G(K_\infty)$ . So we have

$$S(A) = \overline{\Phi \left( \frac{\Gamma \cap G(K_\infty)}{A + G_{\text{tors}}} \right)}.$$

where we have denoted by  $\bar{\Phi}$  the isomorphism  $\Gamma/(A + \Gamma_{\text{tors}}) \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})^r$  induced by  $\Phi$ . Let

$$\varphi : \Gamma \cap G(K_{\infty}) \longrightarrow H^1(\text{Gal}(K_{\infty} | K), G_{\text{tors}})$$

be the group homomorphism that maps an element  $b \in \Gamma \cap G(K_{\infty})$  to the class of the cocycle  $\varphi_b : \sigma \mapsto \sigma(b) - b$ . Notice that  $A + G_{\text{tors}} \subseteq \ker \varphi$ , because  $\text{Gal}(K_{\infty} | K)$  acts trivially on  $A$  and  $\varphi_t$  is a coboundary for every  $t \in G_{\text{tors}}$ . So  $\varphi$  gives rise to a map

$$S(A) \longrightarrow H^1(\text{Gal}(K_{\infty} | K), G_{\text{tors}})$$

which we also denote by  $\varphi$ .

**Proposition 5.8.** *The kernel of  $\varphi : S(A) \rightarrow H^1(\text{Gal}(K_{\infty} | K), G_{\text{tors}})$  is contained in  $S(A)[d_A]$ . In particular, if  $H^1(\text{Gal}(K_{\infty} | K), G_{\text{tors}})$  has finite exponent  $n$ , then the exponent of  $S(A)$  divides  $nd_A$ .*

*Proof.* Let  $b \in \Gamma \cap G(K_{\infty})$  and assume that  $\varphi_b$  is a coboundary. We want to show that  $d_A b \in A + G_{\text{tors}}$ . Since  $\varphi_b$  is a coboundary, there is  $t_0 \in G_{\text{tors}}$  such that for all  $\sigma \in \text{Gal}(K_{\infty} | K)$  we have  $\sigma(b) - b = \sigma(t_0) - t_0$ , hence  $\sigma(b - t_0) = b - t_0$ . This means that  $b - t_0 \in \Gamma \cap G(K)$ , hence  $d_A b = d_A(b - t_0) + d_A t_0 \in d_A(\Gamma \cap G(K)) + G_{\text{tors}}$ . Since  $d_A$  is a divisibility parameter for  $A$  we have

$$A + G(K)_{\text{tors}} \supseteq d_A(\Gamma \cap G(K))$$

so that

$$A + G_{\text{tors}} \supseteq d_A(\Gamma \cap G(K)) + G_{\text{tors}}$$

and it follows that  $d_A b \in A + G_{\text{tors}}$ , so we conclude.  $\square$

We can finally prove the main theorem of this section. Recall that  $s$  is a non-negative integer such that  $G[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$  for every  $n \geq 1$  and that  $H(G)$  denotes the image of  $\text{Gal}(K_{\infty} | K)$  in  $\text{GL}_s(\widehat{\mathbb{Z}})$ .

**Theorem 5.9.** *Let  $G$  be a commutative connected algebraic group over a number field  $K$  and let  $A \subseteq G(K)$  be a finitely generated and torsion-free subgroup of rank  $r$ . For every prime  $\ell$ , let  $H_{\ell}(G)$  denote the image of  $H(G)$  under the projection  $\text{GL}_s(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_s(\mathbb{Z}_{\ell})$  and denote by  $\mathbb{Z}_{\ell}[H_{\ell}(G)]$  the closed sub- $\mathbb{Z}_{\ell}$ -algebra of  $\text{Mat}_{s \times s}(\mathbb{Z}_{\ell})$  generated by  $H_{\ell}(G)$ . Assume that*

- (1) *The group  $A$  admits a divisibility parameter  $d_A$  in  $G(K)$ .*
- (2) *There is an integer  $n \geq 1$  such that  $\mathbb{Z}_{\ell}[H_{\ell}(G)] \supseteq n \text{Mat}_{s \times s}(\mathbb{Z}_{\ell})$  for every prime  $\ell$ .*

- (3) There is an integer  $m \geq 1$  such that the exponent of  $H^1(\text{Gal}(K_\infty | K), G_{\text{tors}})$  divides  $m$ .

Then  $V(A)$  is open in  $\text{Mat}_{r \times s}(\widehat{\mathbb{Z}})$ . More precisely, the order of  $\text{Ent}(A)$  divides  $(d_A n m)^{rs}$ .

*Proof.* Let  $\Gamma := \{P \in G(\overline{K}) \mid \exists n \in \mathbb{N}_{\geq 1} : nP \in A\}$  and fix an isomorphism  $\Gamma \xrightarrow{\sim} \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s$  that sends  $A$  to  $\mathbb{Z}^r$  as in Proposition 3.19, so that we get a torsion-Kummer representation as in the previous subsection. We can then identify  $H(G)$  with a subgroup of  $\text{GL}_s(\widehat{\mathbb{Z}})$  and  $V(A)$  with a subgroup of  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$ , and the natural action of  $H(G)$  on  $V(A)$  is identified with the usual matrix multiplication on the left (see Proposition 3.21).

Thanks to conditions (1) and (3) we can apply Proposition 5.8 and deduce that

$$S(A) = \bigcap_{f \in V(A)} \ker f \subseteq (\mathbb{Q}/\mathbb{Z})^r [d_A m],$$

so that by Proposition 4.1 we have that the  $\text{GL}_s(\widehat{\mathbb{Z}})$ -submodule of  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  generated by  $V(A)$  contains  $d_A m \text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$ . This property and (2) allow us to apply Proposition 4.4 and deduce that the index of  $V(A)$  in  $\text{Mat}_{s \times r}(\widehat{\mathbb{Z}})$  divides  $(d_A n m)^{rs}$ .  $\square$

**Remark 5.10.** Let  $G = \mathbb{G}_m$  and let  $A$  be a finitely generated and torsion-free subgroup of  $G(K)$  of rank  $r$ . Theorem 5.9 gives us another way of proving [PS19, Theorem 1.1], which states that there exists an integer  $C \geq 1$  such that for every  $n \geq 1$  the ratio

$$\frac{n^r}{\left[ K \left( \zeta_n, \sqrt[n]{A} \right) : K(\zeta_n) \right]} \quad (5.2)$$

divides  $C$ . Indeed, the ratio (5.2) always divides  $\# \text{Ent}(A)$  (Lemma 5.7), and we have:

- (1) The group  $A$  has finite divisibility (see Example 5.2).
- (2) The torsion representation  $\tau : \text{Gal}(K_\infty | K) \rightarrow \text{GL}_1(\widehat{\mathbb{Z}}) = \widehat{\mathbb{Z}}^\times$  coincides with the adelic cyclotomic character, whose image is open in  $\widehat{\mathbb{Z}}^\times$ ; more precisely, the index of  $H(\mathbb{G}_m)$  in  $\widehat{\mathbb{Z}}^\times$  divides  $[K : \mathbb{Q}]$ , so that  $\mathbb{Z}_\ell[H_\ell(\mathbb{G}_m)]$  contains  $[K : \mathbb{Q}] \text{Mat}_{s \times s}(\mathbb{Z}_\ell)$  for every prime  $\ell$ .
- (3) By (2) above  $H(\mathbb{G}_m)$  contains every element of  $\mathbb{Z}^\times$  that is congruent to the identity modulo  $[K : \mathbb{Q}]$ ; an application of Sah's Lemma (see also the proof of Proposition 6.3) tells us that

$$[K : \mathbb{Q}] H^1(\text{Gal}(K_\infty | K), \mathbb{G}_{m, \text{tors}}) = 0.$$

So by Theorem 5.9 we may take  $C = (d_A \cdot [K : \mathbb{Q}]^2)^r$ .

It is worth noting that the methods of [PS19] provide a more precise bound.

## 6 Elliptic curves

For this section we fix a number field  $K$  with algebraic closure  $\overline{K}$  and an elliptic curve  $E$  over  $K$  with  $\text{End}_K(E) = \mathbb{Z}$ . Moreover, we let  $A$  be a torsion-free subgroup of  $E(K)$  of rank  $r$  and let  $\Gamma \subseteq E(\overline{K})$  be the subgroup defined in (5.1), which is a full 2-extension of  $A$ .

Our goal is to apply Theorem 5.9 to get an explicit bound on the cardinality of  $\text{Ent}(A)$ . In order to do so, we need to study the divisibility parameter  $d_A$  and the torsion representations associated with  $E/K$ .

### 6.1 The divisibility parameter

If a set of generators for  $A$ , modulo torsion in  $E(K)$ , is known in terms of a  $\mathbb{Z}$ -basis for  $E(K)/E(K)_{\text{tors}}$ , then we can compute  $d_A$  effectively. In fact, let  $\overline{E(K)} = E(K)/E(K)_{\text{tors}}$  and let  $\overline{A}$  be the image of  $A$  in  $\overline{E(K)}$ . Let  $\mathbf{e}_1, \dots, \mathbf{e}_\rho$  be a basis for  $\overline{E(K)}$  as a free  $\mathbb{Z}$ -module and let  $\mathbf{a}_1, \dots, \mathbf{a}_t$  be a set of generators for  $\overline{A}$ . Write

$$\mathbf{a}_i = \sum_{j=1}^{\rho} m_{ij} \mathbf{e}_j$$

for some integers  $m_{ij}$ , and let  $M$  be the  $\rho \times t$  matrix  $(m_{ji})$  whose columns are the coordinate vectors representing the  $\mathbf{a}_i$ .

We can then reduce  $M$  to its *Smith Normal Form* (see [Jac12, Chapter 3]), that is, we can find matrices  $P \in \text{GL}_\rho(\mathbb{Z})$  and  $Q \in \text{GL}_t(\mathbb{Z})$  such that

$$PMQ = \begin{pmatrix} d_1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & d_2 & & & & & \vdots \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & d_r & & & \vdots \\ \vdots & & & & 0 & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

where  $d_1, \dots, d_r$  are integers such that  $d_1 \mid d_2 \mid \dots \mid d_r$  and  $r$  is the rank of  $A$ . The integers  $d_i$  are uniquely determined up to sign, and they are easily computable from the minors of  $M$  (see [Jac12, Theorem 3.9]).

It follows that there is a  $\mathbb{Z}$ -basis  $\{\mathbf{f}_1, \dots, \mathbf{f}_\rho\}$  of  $\overline{E(K)}$  such that  $\{d_1 \mathbf{f}_1, \dots, d_r \mathbf{f}_r\}$  is a  $\mathbb{Z}$ -basis for  $A$ . Moreover, if  $\Gamma$  is defined as in (5.1), we have that  $(\Gamma \cap E(K))/E(K)_{\text{tors}}$  is generated by  $\{\mathbf{f}_1, \dots, \mathbf{f}_r\}$ . We then have that  $d_r(\Gamma \cap E(K)) \subseteq A + E(K)_{\text{tors}}$ , so we can take  $d_A = d_r$ .

## 6.2 The torsion representation

The torsion representation is nothing but the usual Galois representation attached to the torsion of  $E$ . After a choice of basis, we will denote it by

$$\tau_\infty : \text{Gal}(K_\infty \mid K) \rightarrow \text{GL}_2(\widehat{\mathbb{Z}})$$

and we will denote its image by  $H(E)$ . If  $\ell$  is a prime we will denote by  $\tau_\ell$  the composition of  $\tau_\infty$  with the natural projection  $\text{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_2(\mathbb{Z}_\ell)$  and by  $H_\ell(E)$  the image of  $\tau_\ell$ .

### The non-CM case

**Definition 6.1.** We call *adelic bound* for the torsion representation a positive even integer  $m_E$  such that  $H(E)$  contains all the elements of  $\text{GL}_2(\widehat{\mathbb{Z}})$  congruent to the identity modulo  $m_E$ . If  $\ell$  is a prime, we call an integer  $n_\ell \geq 1$  such that  $H_\ell(E) \supseteq I + \ell^{n_\ell} \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell)$  a *parameter of maximal growth* for the  $\ell$ -adic torsion representation. If  $\ell = 2$  we require  $n_\ell \geq 2$ .

If  $E$  does not have complex multiplication over  $\overline{K}$ , by Serre's Open Image Theorem (see [Ser72]) we know that an adelic bound exists.

**Remark 6.2.** Notice that, if an explicit bound for  $m_E$  is known, one can easily give a bound for each  $n_\ell$  by just letting  $n_\ell = \max(1, v_\ell(m_E))$ . However, it is possible to give an effective bound for each  $n_\ell$  (see [LP21, Theorem 14 and Remark 15] and [Chapter 1, Remark 3.7]), so we will keep these constants separate.

**Proposition 6.3.** *If  $m_E$  is an adelic bound for the torsion representation of  $E$  over  $K$ , then  $m_E H^1(\text{Gal}(K_\infty \mid K), E_{\text{tors}}) = 0$ .*

*Proof.* Let  $G = \text{Gal}(K_\infty \mid K)$  and let  $z = (z_\ell)_\ell \in \widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$  be defined as

$$z_\ell = \begin{cases} 1 + \ell^{v_\ell(m_E)} & \text{if } \ell \mid m_E, \\ 2 & \text{if } \ell \nmid m_E. \end{cases}$$



Since by definition  $2 \mid m_E$  we have  $z \in \widehat{\mathbb{Z}}^\times$ . Moreover  $z - 1 = um_E$  for some  $u \in \widehat{\mathbb{Z}}^\times$ .

Consider now the element  $g = zI \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ : it is congruent to the identity matrix modulo  $m_E$ , so it lies in  $G$ ; moreover it is a scalar matrix, so it lies in the center of  $G$ . By Sah's Lemma (see [BR03, Lemma A.2]) the endomorphism of  $H^1(G, E_{\mathrm{tors}})$  defined by  $f \mapsto (g - I)f$  kills  $H^1(G, E_{\mathrm{tors}})$ . Since  $g - I = um_E I$  for  $u \in \widehat{\mathbb{Z}}^\times$ , we have that  $m_E H^1(G, E_{\mathrm{tors}}) = 0$ , as required.  $\square$

**Definition 6.4.** Let  $K$  be a number field with absolute discriminant  $\Delta_K$  and let  $E$  be an elliptic curve over  $K$  without CM over  $\overline{K}$ . We denote by  $S(E)$  the finite set of primes  $\ell$  that satisfy at least one of the following conditions:

- (1)  $\ell \mid 2 \cdot 3 \cdot 5 \cdot \Delta_K$ ;
- (2) the Galois group  $\mathrm{Gal}(K_\ell \mid K)$  is not isomorphic to  $\mathrm{GL}_2(\mathbb{F}_\ell)$ .
- (3)  $E$  has bad reduction at some prime of  $K$  of characteristic  $\ell$ .

**Remark 6.5.** The set  $S(E)$  is effectively computable (see [Chapter 1, Remark 5.2]).

An explicit value for the adelic bound  $m_E$  is provided by the following result by F. Campagna and P. Stevenhagen:

**Theorem 6.6** ([CS19, Theorem 3.4]). *Let  $E$  be an elliptic curve over  $K$  without CM over  $\overline{K}$ . Write  $K_{\ell^\infty}$  for the compositum of all  $\ell$ -power division fields of  $E$  over  $K$ , and  $K_{S(E)}$  for the compositum of the fields  $K_{\ell^\infty}$  with  $\ell \in S(E)$ . Then the family consisting of  $K_{S(E)}$  and  $\{K_{\ell^\infty}\}_{\ell \notin S(E)}$  is linearly disjoint over  $K$ , that is, the natural map*

$$\mathrm{Gal}(K_\infty \mid K) \rightarrow \mathrm{Gal}(K_{S(E)} \mid K) \times \prod_{\ell \notin S(E)} \mathrm{Gal}(K_{\ell^\infty} \mid K)$$

*is an isomorphism.*

**Remark 6.7.** For every prime  $\ell \notin S(E)$ , the  $\ell$ -adic representation associated with  $E$  is surjective. This follows from the fact that the mod  $\ell$  torsion representation associated with  $E$  and the  $\ell$ -adic cyclotomic character of  $K$  are both surjective (since  $\ell \nmid \Delta_K$ ): in fact in this case we have  $(H(E) \bmod \ell) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$  and  $\det(H_\ell(E)) = \mathbb{Z}_\ell^\times$ , which implies (see [Ser97, IV-23]) that  $H_\ell(E) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ .

**Corollary 6.8.** *For every prime  $\ell \in S(E)$  let  $n_\ell$  be a parameter of maximal growth for the  $\ell$ -adic torsion representation. Let moreover  $R := \prod_{\ell \in S(E)} \ell$  and  $m_\ell = v_\ell([K_R : K])$ . Then an adelic bound for the torsion representation is given by*

$$m_E = \prod_{\ell \in S(E)} \ell^{n_\ell + m_\ell}.$$

*Proof.* We have to show that the image of  $\text{Gal}(K_\infty | K)$  in  $\text{GL}_2(\widehat{\mathbb{Z}})$  contains

$$\prod_{\ell \in S(E)} (I + \ell^{m_\ell + n_\ell} \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell)) \times \prod_{\ell \notin S(E)} \text{GL}_2(\mathbb{Z}_\ell).$$

We will do so by considering the subgroup  $\text{Gal}(K_\infty | K_R)$  of  $\text{Gal}(K_\infty | K)$ .

Notice that, since for every prime  $\ell$  and every  $n \geq 1$  the degree of  $K_{\ell^n}$  over  $K_\ell$  is a power of  $\ell$ , the family  $\{K_{\ell^\infty R}\}_{\ell \in S(E)}$  is linearly disjoint over  $K_R$ . Then we have

$$\begin{aligned} \text{Gal}(K_\infty | K_R) &= \text{Gal}(K_{S(E)} | K_R) \times \prod_{\ell \notin S(E)} \text{Gal}(K_{\ell^\infty} | K) = \\ &= \prod_{\ell \in S(E)} \text{Gal}(K_{\ell^\infty R} | K_R) \times \prod_{\ell \notin S(E)} \text{Gal}(K_{\ell^\infty} | K). \end{aligned}$$

For every  $\ell \in S(E)$  we have  $\tau_\ell(\text{Gal}(K_{\ell^\infty R} | K_R)) \supseteq I + \ell^{r_\ell} \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell)$ , where  $r_\ell$  is a parameter of maximal growth for the  $\ell$ -adic torsion representation attached to  $E$  over  $K_R$ . By [Chapter 1, Lemma 3.10] we can take  $r_\ell \leq n + m_\ell$ , so  $\rho_\infty(\text{Gal}(K_\infty | K_R))$  contains

$$\prod_{\ell \in S(E)} (I + \ell^{n_\ell + m_\ell} \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell)) \times \prod_{\ell \notin S(E)} \text{GL}_2(\mathbb{Z}_\ell)$$

so it contains all elements that are congruent to  $I$  modulo  $m_E$ , as required.  $\square$

**Remark 6.9.** We can give an explicit bound for the integers  $m_\ell$  of the above corollary:

$$m_\ell = v_\ell([K_R : K]) \leq v_\ell(\# \text{GL}_2(\mathbb{Z}/R\mathbb{Z})) = \sum_{p \in S(E)} v_\ell((p^2 - 1)(p^2 - p)).$$

### The CM case

The torsion representations associated with elliptic curves with complex multiplication have been studied for example in [Deu53] and [Deu58]. They are deeply related to the endomorphism ring  $\mathcal{O}_E = \text{End}_{\overline{K}}(E)$  of  $E$ , which is an order in an imaginary quadratic number field  $F$ .

For every prime  $\ell$ , the group

$$\mathcal{C}_\ell(E) := (\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^\times$$

can be identified with a subgroup of  $\text{GL}_2(\mathbb{Z}_\ell)$  via the action of  $\mathcal{O}_E$  on the  $\ell$ -power torsion of  $E$ , and is called the *Cartan subgroup* of  $\text{GL}_2(\mathbb{Z}_\ell)$  associated with  $E$ .

We also let

$$\mathcal{C}(E) := \left( \mathcal{O}_E \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \right)^{\times} = \prod_{\ell \text{ prime}} \mathcal{C}_{\ell}(E)$$

which can be identified with a subgroup of  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ , and we denote by  $\mathcal{N}_{\ell}(E)$  and  $\mathcal{N}(E)$  the normalizers of  $\mathcal{C}_{\ell}(E)$  in  $\mathrm{GL}_2(\mathbb{Z}_{\ell})$  and of  $\mathcal{C}(E)$  in  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ , respectively.

The group  $\mathcal{C}_{\ell}(E)$  is always conjugate to a subgroup of  $\mathrm{GL}_2(\mathbb{Z}_{\ell})$  of the form

$$\left\{ \begin{pmatrix} x & \delta y \\ y & x + \gamma y \end{pmatrix} : x, y \in \mathbb{Z}_{\ell}, v_{\ell}(x(x + \gamma y) - \delta y^2) = 0 \right\}$$

for some integers  $\gamma$  and  $\delta$ , which are called *parameters* for  $\mathcal{C}_{\ell}(E)$  (see [LP17, §2.3]).

The image of the torsion representation associated with  $E$  is contained in  $\mathcal{N}(E)$ , and can be described as follows.

**Proposition 6.10** ([Lom17, Theorem 1.5]). *Let  $E$  be an elliptic curve over  $K$  with CM over  $\overline{K}$ , and let  $F$  be the CM field of  $E$ . Let  $\mathcal{S}$  denote the set of primes  $\ell$  that either ramify in  $K \cdot F$  or are such that  $E$  has bad reduction at some prime of  $K$  of characteristic  $\ell$ . Then:*

1. *if  $F \subseteq K$ , then  $H(E) \subseteq \mathcal{C}(E)$  and  $[\mathcal{C}(E) : H(E)]$  divides  $6[K : \mathbb{Q}]$ . Moreover,  $H_{\ell}(E) = \mathcal{C}_{\ell}(E)$  for every  $\ell \notin \mathcal{S}$ ;*
2. *if  $F \not\subseteq K$ , then  $H(E) \subseteq \mathcal{N}(E)$ , but  $H(E) \not\subseteq \mathcal{C}(E)$ , and  $[\mathcal{C}(E) : \mathcal{C}(E) \cap H(E)]$  divides  $12[K : \mathbb{Q}]$ . Moreover,  $H_{\ell}(E) = \mathcal{N}_{\ell}(E)$  for every  $\ell \notin \mathcal{S}$ .*

**Remark 6.11.** The result mentioned above [Lom17, Theorem 1.5] states that  $[\mathcal{C}(E) : H(E)] \leq 3[K : \mathbb{Q}]$  if  $F \subseteq K$  and  $[\mathcal{C}(E) : \mathcal{C}(E) \cap H(E)] \leq 6[K : \mathbb{Q}]$  if  $F \not\subseteq K$ . However, one can check that its proof also yields Proposition 6.10 as stated here.

**Proposition 6.12.** *Let  $E$  be a CM elliptic curve over  $K$  and let  $e_K = 12[K : \mathbb{Q}]$ . Let moreover*

$$m_K := 4^{e_K} \cdot \prod_{\ell} \ell^{e_K},$$

*where the product runs over all odd primes  $\ell$  such that  $(\ell - 1)$  divides  $e_K$ . Then we have  $m_K H^1(\mathrm{Gal}(K_{\infty} | K), E_{\mathrm{tors}}) = 0$ .*

*Proof.* Let  $k_2 = 3$  and, for any odd prime  $\ell$ , let  $k_{\ell}$  be an integer whose class modulo  $\ell$  is a generator of  $(\mathbb{Z}/\ell\mathbb{Z})^{\times}$  and  $1 < k_{\ell} < \ell$ . Let then  $z = (k_{\ell}^{e_K})_{\ell} \in \widehat{\mathbb{Z}}$ ,

and let  $g = zI \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ . By Proposition 6.10 we have  $(\mathcal{C}(E))^{e_K} \subseteq H(E)$ , so in particular  $g \in H(E)$ . Applying Sah's Lemma as in Proposition 6.3 we see that  $g - I$  kills  $H^1(\mathrm{Gal}(K_\infty | K), E_{\mathrm{tors}})$ . Since

$$\begin{aligned} v_2(3^{e_K} - 1) &\leq 2e_K, \\ v_\ell(k_\ell^{e_K} - 1) &\leq e_K \quad \text{for all } \ell > 2, \\ v_\ell(k_\ell^{e_K} - 1) &= 0 \quad \text{for all } \ell \text{ such that } (\ell - 1) \nmid e_K, \end{aligned}$$

we have that  $z - 1 = um$  for some  $u \in \widehat{\mathbb{Z}}^\times$  and some  $m$  which divides  $m_K$ . As in Proposition 6.3 we conclude that the exponent of  $H^1(\mathrm{Gal}(K_\infty | K), E_{\mathrm{tors}}) = 0$  divides  $m_K$ .  $\square$

It follows from classical results (see also [LP21, Section 2]) that for every prime  $\ell$  there is a positive integer  $n_\ell$  such that

$$\#(H(E) \bmod \ell^{n+1}) / \#(H(E) \bmod \ell^n) = \ell^2 \quad \text{for all } n \geq n_\ell. \quad (6.1)$$

**Definition 6.13.** We call a positive integer  $n_\ell$  satisfying (6.1) a *parameter of maximal growth* for the  $\ell$ -adic torsion representation. If  $\ell = 2$  we require  $n_\ell \geq 2$ .

### 6.3 Main theorems

We can finally prove our main results, which are higher-rank generalizations of [Chapter 1, Theorems 1.1 and 1.2].

**Theorem 6.14.** *Let  $E$  be an elliptic curve over a number field  $K$  without complex multiplication over  $\bar{K}$ . Let  $A$  be a finitely generated and torsion-free subgroup of  $E(K)$  of rank  $r$ .*

*Let  $d_A$  be a divisibility parameter for  $A$ . Let  $S(E)$  be the finite set of primes of Definition 6.4 and for every  $\ell \in S(E)$  let  $n_\ell$  be a parameter of maximal growth for the  $\ell$ -adic torsion representation of  $E/K$  and*

$$m_\ell := \sum_{p \in S(E)} v_\ell((p^2 - 1)(p^2 - p)).$$

*Then  $V(A)$  is open in  $\mathrm{Mat}_{r \times 2}(\widehat{\mathbb{Z}})$ . More precisely, the order of  $\mathrm{Ent}(A)$  divides*

$$\left( d_A \cdot \prod_{\ell \in S(E)} \ell^{2n_\ell + m_\ell} \right)^{2r}.$$

*Proof.* By Remark 6.7, the integer  $n := \prod_{\ell \in S(E)} \ell^{n_\ell}$  is such that  $\mathbb{Z}_\ell[H_\ell(E)]$  contains  $n \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell)$  for every prime number  $\ell$ . By Corollary 6.8 and Remark 6.9 the integer  $m := \prod_{\ell \in S(E)} \ell^{n_\ell + m_\ell}$  is an adelic bound for the torsion representation associated with  $E$ , so by Proposition 6.3 the exponent of the group  $H^1(\text{Gal}(K_\infty | K), E_{\text{tors}})$  divides  $m$ .

Then by Theorem 5.9 we have that the order of  $\text{Ent}(A)$  divides  $(d_A n m)^{2r}$ .  $\square$

**Definition 6.15.** Let  $E$  be an elliptic curve over a number field  $K$  with CM over  $\bar{K}$ . Let  $\mathcal{O}_E = \text{End}_{\bar{K}}(E)$  and let  $F = \text{Frac}(\mathcal{O}_E)$ . We denote by  $S(E)$  the finite set of primes such that at least one of the following conditions is satisfied:

1.  $\ell$  divides the conductor of  $\mathcal{O}_E$ ;
2.  $\ell$  ramifies in  $K$ ;
3.  $E$  has bad reduction at some prime of  $K$  of characteristic  $\ell$ .

**Theorem 6.16.** Let  $E$  be an elliptic curve over a number field  $K$ , with CM over  $\bar{K}$  but not over  $K$ . Let  $A$  be a finitely generated and torsion-free subgroup of  $E(K)$  of rank  $r$ .

Let  $d_A$  be a divisibility parameter for  $A$ . For every prime  $\ell$  let  $n_\ell$  be a parameter of maximal growth for the  $\ell$ -adic torsion representation of  $E/K$  and let  $(\gamma_\ell, \delta_\ell)$  be parameters for  $\mathcal{C}_\ell(E)$ . Let  $m_K$  be the integer defined in Proposition 6.12. Let moreover  $S(E)$  be the finite set of primes of Definition 6.15.

Then  $V(A)$  is open in  $\text{Mat}_{r \times 2}(\hat{\mathbb{Z}})$ . More precisely, the order of  $\text{Ent}(A)$  divides

$$\left( d_A m_K \cdot \prod_{\ell \in S(E)} \ell^{n_\ell + v_\ell(4\delta_\ell)} \right)^{2r},$$

where we let  $v_\ell(0) = 0$  for every prime  $\ell$ .

*Proof.* In order to apply Theorem 5.9 we only need to prove that:

1. for every prime  $\ell \notin S(E)$  we have

$$\mathbb{Z}_\ell[H_\ell(E)] = \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell);$$

2. for every prime  $\ell \in S(E)$  we have

$$\mathbb{Z}_\ell[H_\ell(E)] \supseteq \ell^{n_\ell + v_\ell(4\delta_\ell)} \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell).$$

Both parts follow from from [Chapter 1, Proposition 4.12, proof of (3)], noticing that for every  $\ell \notin S(E)$  one may take  $d = 0$  by [LP17, Proposition 10].  $\square$

**Theorem 6.17.** *There is a universal constant  $C \geq 1$  such that, for every elliptic curve  $E/\mathbb{Q}$  and every torsion-free subgroup  $A$  of  $E(\mathbb{Q})$ , the order of  $\text{Ent}(A)$  divides  $(d_A C)^{2\text{rk}(A)}$ .*

*Proof.* By [Chapter 1, Corollary 3.13] (which relies on [Ara08, Theorem 1.2] for the non-CM case) the parameters of maximal growth for the  $\ell$ -adic torsion representation associated with an elliptic curve over  $\mathbb{Q}$  can be bounded independently of  $E$ . By [Chapter 1, Theorem 1.3] there is a constant  $C_1$  such that the exponent of  $H^1(\text{Gal}(\mathbb{Q}_\infty | \mathbb{Q}), E_{\text{tors}})$  divides  $C_1$ . The conclusion then follows from Theorem 5.9.  $\square$

**Remark 6.18.** Theorem 6.16 does not hold if  $\mathcal{O}_E = \text{End}_K(E) \neq \mathbb{Z}$ . In fact in this case one may find a subgroup  $A \subseteq E(K)$  such that  $\text{Ent}(A)$  is infinite.

To see this, let  $P \in E(K)$  be a point of infinite order and let  $A = \mathcal{O}_E P$  and  $A' = \mathbb{Z}P$ . Since  $A$  is a free  $\mathcal{O}_E$ -module of rank 1, it has rank 2 as an abelian group.

Let  $Q \in n^{-1}P$ . For every  $n > 1$  and every  $\sigma \in \mathcal{O}_E$  we have  $n^{-1}\sigma(P) = \sigma(Q) + E[n]$ , so

$$n^{-1}A = \mathcal{O}_E Q + E[n].$$

Since  $Q \in n^{-1}A'$  and  $\mathcal{O}_E$  is defined over  $K$  we have that  $\mathcal{O}_E Q$  is defined over  $K(n^{-1}A')$ . Since moreover  $E[n] \subseteq n^{-1}A'$  we deduce that  $K(n^{-1}A) \subseteq K(n^{-1}A')$ . In fact, since  $A \supseteq A'$ , the two fields coincide. So in particular

$$[K(n^{-1}A) : K(E[n])] = [K(n^{-1}A') : K(E[n])] .$$

Then for every  $n > 1$  we have by Remark 5.5

$$\frac{n^4}{[K(n^{-1}A) : K(E[n])]} = \frac{n^4}{[K(n^{-1}A') : K(E[n])]} \geq n^2$$

which, by Lemma 5.7, implies that  $\text{Ent}(A)$  is infinite.

Notice that two generators of  $A$  as a free  $\mathbb{Z}$ -module cannot be linearly independent over  $\mathcal{O}$ . In fact, the condition that the points are linearly independent over the endomorphism ring of the curve can also be found in [Rib79, Theorem 1.2].

