Kummer theory for commutative algebraic groups

Tronto, S.

Kummer theory for commutative algebraic groups

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op donderdag 8 september 2022
klokke 11:15 uur

door

Sebastiano Tronto
geboren te Feltre, Italië
in 1994

Promotor:
Prof.dr. P. Stevenhagen

Co-promotores:
Dr. P.J. Bruin
Dr. A. Perucca (University of Luxembourg)

Promotiecommissie:
Prof.dr. M. Fiocco
Prof.dr. R.M. van Luijk
Prof.dr. J. Voight (Dartmouth College)
Prof.dr. G. Wiese (University of Luxembourg)
Dr. C. Salgado Guimarães da Silva (Rijksuniversiteit Groningen)

Introduction

This thesis consists of four research articles that treat different aspects of *Kummer theory for commutative algebraic groups*, with particular emphasis on explicit and effective results. To understand the motivation behind the study of this topic and what we are trying to achieve, we have to take a step back and see which aspects of classical Kummer theory we are trying to generalize to algebraic groups.

Kummer theory

If n is a positive integer and K is a field of characteristic coprime to n we may consider, for any non-zero $\alpha \in K$, the *set* $\sqrt[n]{\alpha}$ of all elements β in a fixed algebraic closure $\overline{K}$ of K such that $\beta^n = \alpha$. In other words, $\sqrt[n]{\alpha}$ is the set of all n-th roots of α. Given any n-th root β_0 of α, all the others are of the form $\zeta\beta_0$ for some n-th root of unity $\zeta \in \overline{K}$, that is an element such that $\zeta^n = 1$. The field generated over K by all n-th roots of α is a Galois extension of K which contains the n-th *cyclotomic field*, that is the field generated over K by all n-th roots of unity. This remains true if we replace α by a finitely generated subgroup A of the multiplicative group $K^\times$, and we consider the set $\sqrt[n]{A} = \{\beta \in \overline{K} \mid \beta^n \in A\}$. Roughly speaking, classical Kummer theory is the study of this kind of field extensions.

The most classical result in Kummer theory is the classification of the abelian extensions of exponent dividing n of a field K which contains all n-th roots of unity and whose characteristic does not divide n. Indeed, a bijection between the set of such extensions, contained in a fixed algebraic closure $\overline{K}$, and the set of subgroups of $K^\times$ that contain $(K^\times)^n$ is obtained by mapping L to $K^\times \cap (L^\times)^n$, see for example [Lan02, Theorem VI.8.2].

Kummer theory has interesting applications in studying certain *density problems*: if α is a non-zero element of a number field K, then the density of primes $\mathfrak{p}$ of K such that the multiplicative order of α modulo $\mathfrak{p}$ is coprime to some fixed prime ℓ, or has a prescribed ℓ-adic valuation, can be expressed in terms of the degrees of the cyclotomic-Kummer extensions $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha})$ for all $n > 0$, where ζ_{ℓ^n}

is a root of unity of order ℓ^n. See [Per15] for the case we have just described and [DP16, PS19] for a generalization to finite rank sugroups of $K^\times$. These problems are closely related to Artin's primitive root conjecture, as explained for example in [Mor12].

Computing the degrees of infinitely many field extensions might seem an arduous task. However, the following is known (for a direct proof, see [PS19, Theorem 1.1]): if A is a subgroup of $K^\times$ of finite rank r, then there is a constant $C > 0$ such that for every positive integer n the ratio between n^r and the degree $[K(\sqrt[n]{A}) : K(\zeta_n)]$ divides C. This result can be made effective, see [PST20a, Theorem 1.2], and the results of [PST20b] provide, for the case $K = \mathbb{Q}$, an algorithm whose output is a finite formula for these degrees. This algorithm has been implemented in SageMath, see [Tro19].

Algebraic groups

So far we have only discussed Kummer theory in the classical sense, but these concepts can be generalized as follows. Let K be a field, say for simplicity of characteristic zero, fix an algebraic closure $\overline{K}$ of K and let G be a commutative algebraic group over K. If S is a subset of $G(\overline{K})$, the *field extension of K generated by S* is the subfield of $\overline{K}$ obtained by adjoining to K the coordinates of the points of S. More precisely, identifying every x in S with a morphism of schemes $\operatorname{spec} \overline{K} \to \operatorname{spec} K(x)$, we have a collection of morphisms $K(x) \to \overline{K}$ as x varies in S, and the compositum of the images of these morphisms is by definition $K(S)$.

Let now $A \subseteq G(K)$ be a finitely generated subgroup. For any positive integer n we may consider the subset $n^{-1}A = \{P \in G(\overline{K}) \mid nP \in A\}$. Extensions of K of the form $K(n^{-1}A)$ are the object of study of *Kummer theory for commutative algebraic groups*. As one can see by taking $G = \mathbb{G}_m$, the multiplicative group over K, this theory is a direct generalization of classical Kummer theory. Even in this generality, Kummer extensions have many of the interesting properties of their classical counterparts. For example $K(n^{-1}A)$ is a Galois extension of K that contains the *n-torsion field* of G, that is the field extension of K generated by all n-torsion points of $G(\overline{K})$, and it is Galois and abelian over this field. Torsion fields are the direct generalization of cyclotomic fields, and many results on Kummer extensions can be deduced from properties of these fields.

If K is a number field, the density problem mentioned above can be stated *mutatis mutandis* in this more general context, and it is still related to the degrees of Kummer extensions. See [Pin04] for a discussion in the case of abelian varieties and [Per08, Per11] for the product of an abelian variety and a torus. This motivates the study of the degrees of Kummer extensions in the general context. In his foundational paper [Rib79], Ribet proved the following result: if

G is the product of an abelian variety and a torus and $A \subseteq G(K)$ is a free $\mathbb{Z}$-module of rank r with a basis over $\mathbb{Z}$ of points linearly independent over $\mathrm{End}_K(G)$, there exists a positive integer C such that the ratio between n^{rs} and the degree $[K(n^{-1}A) : K(G[n])]$ divides C for every positive integer n. Here s is the unique positive integer such that $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$ for every $n > 1$. See also [Ber88, Théorème 5.2] and [Hin88, Lemme 14]. The papers collected in this thesis are devoted to making this result more effective, trying to express the constant C in terms of known quantities related to the torsion fields of G.

Effective results for elliptic curves

The first two papers, written in collaboration with Lombardo, focus on the case of elliptic curves. Assume that G is an elliptic curve over a number field K and fix an algebraic closure $\overline{K}$ of K. Fix moreover a point $\alpha \in G(K)$. In [JR10] Jones and Rouse proved that for every prime ℓ, under some assumption on α and with a small exception for the prime 2, the surjectivity of the ℓ-adic Galois representation associated with G implies the maximality of the Kummer extensions $K(n^{-1}\alpha)$ over $K(G[n])$ if n is a power of ℓ. See [JR10, Theorem 5.2] for the non-CM case and [JR10, Theorem 5.8] for the CM case. Two questions, suggested by Perucca, arose: If the Galois representation is not surjective, can we describe, or at least bound, the failure of maximality of the Kummer extensions in terms of the failure of maximality of the Galois representations? Can these results be generalized to the case where n is any positive integer?

The first paper presented here [Chapter 1] aims at answering these questions. The main theorem [Chapter 1, Theorem 1.1] provides a positive answer, but only under the assumption that $\mathrm{End}_K(G) = \mathbb{Z}$. This theorem is an effective version of the classical result by Ribet in the case of a group G generated by a single point α, and it shows that the constant C mentioned above can be taken to depend only on properties of the *ℓ-adic* representations, for all the different primes ℓ, and other effectively computable quantities associated with G. Examples that demonstrate the inapplicability of these methods to the CM case are provided in [Chapter 1, Section 6]. The second main theorem [Chapter 1, Theorem 1.2] shows that over the field $\mathbb{Q}$ there exists a uniform version of this result under the assumption that the point α is not divisible in $G(\mathbb{Q})/G(\mathbb{Q})_{\mathrm{tors}}$ – that is, that there is no $\beta \in G(\mathbb{Q})$ such that α equals $n\beta + \tau$ for some integer $n > 1$ and some $\tau \in G(\mathbb{Q})_{\mathrm{tors}}$.

The goal of the second paper with Lombardo [Chapter 2] is to make the aforementioned result [Chapter 1, Theorem 1.2] explicit by finding an actual numerical value for the constant C, see [Chapter 2, Theorem 6.5]. These results have been achieved by giving uniform bounds to other interesting quantities related to the Galois representations of G. A notable example of such a quantity are the ex-

ponents of the cohomology groups of $\mathrm{Gal}(\mathbb{Q}(G(\overline{\mathbb{Q}})_{\mathrm{tors}}) \mid \mathbb{Q})$ with coefficients in the torsion subgroups of G, regarded as Galois modules. Bounds for similar quantities have been found independently by Cerchia and Rouse [CR21].

A technical framework for general Kummer theory

Some of the explicit results mentioned above depend on properties of Galois representations that are known in an effective form only for elliptic curves, but the methods used to show that the degrees of Kummer extensions are related to these quantities do not. In the third article reported here [Chapter 3] this is made clear by conceptualizing the theoretical background in a framework that is applicable to any commutative algebraic group over K that satisfies $\mathrm{End}_K(G) = \mathbb{Z}$. The methods used in this work are inspired by results of Palenstijn [Pal04, Pal14] and by discussions with Lenstra and Stevenhagen. As an application, the results of [Chapter 1] and [Chapter 2] are extended to groups A of rank higher than 1.

So far we have not yet successfully tackled the case when the endomorphism ring of G is larger than $\mathbb{Z}$, and it seems that our methods need a substantial refinement to be applied in that case. In his thesis [JP21], Javan Peykar addresses this problem in the case of elliptic curves with complex multiplication by taking $A \subseteq G(K)$ to be an $\mathrm{End}_K(G)$-module, and considering the modules of "division points" by a *Steinitz ideal*. Even if with some technical limitation, this method is very successful.

Motivated by this approach, the last paper in this thesis [Chapter 4] is mostly devoted to the study of purely algebraic properties of division modules over general rings. The Steinitz ideals used by Javan Peykar are replaced by *ideal filters*, and a generalization of the classical notion of injectivity, which to the author's knowledge is new, is provided. A notion of (J, T)-*extension*, where J is a fixed ideal filter and T a suitable R-module, generalizes the modules of division points. The properties of these objects are then studied with a category-theoretical point of view before generalizing some results on their automorphism groups that have appeared in the less general settings of [Pal04], [Pal14] and [JP21].

This long digression in commutative algebra bears in the end its fruits: the theory so constructed, which generalizes that of [Chapter 3], is finally applied to unify and generalize the results of [Chapter 1] and [JP21], showing that the two apparently different approaches are actually just different realizations of a more general theory. The degree of generality used in this paper opens the door to applications to higher-dimensional abelian varieties and other classes of commutative algebraic groups.

Samenvatting

Dit proefschrift bestaat uit vier onderzoeksartikelen die verschillende aspecten van de *Kummertheorie voor commutatieve algebraïsche groepen* behandelen, met bijzondere nadruk op expliciete en effectieve resultaten. Om de motivatie achter de studie van dit onderwerp en onze doelen te begrijpen, moeten we een stap terug doen en kijken welke aspecten van de klassieke Kummertheorie we proberen te generaliseren naar algebraïsche groepen.

Kummertheorie

Als n een positief geheel getal is en K een lichaam van karakteristiek copriem met n, kunnen we voor elke $\alpha \neq 0$ in K de *verzameling* $\sqrt[n]{\alpha}$ beschouwen van alle elementen β in een vast gekozen algebraïsche afsluiting $\overline{K}$ van K zodanig dat $\beta^n = \alpha$. Met andere woorden, $\sqrt[n]{\alpha}$ is de verzameling van alle n-de wortels van α. Zij b_0 een n-de wortel van α, dan hebben alle andere wortels de vorm $\zeta\beta_0$ voor een n-de eenheidswortel $\zeta \in \overline{K}$, dat wil zeggen een element zodanig dat $\zeta^n = 1$. Het lichaam voortgebracht over K door alle n-de wortels van α is een Galoisuitbreiding van K die het n-de *cyclotomische lichaam* bevat, dat wil zeggen het lichaam voortgebracht over K door alle n-de eenheidswortels. Dit blijft waar als we α vervangen door een eindig voortgebrachte ondergroep A van de multiplicatieve groep $K^\times$, en we de verzameling $\sqrt[n]{A} = \{\beta \in \overline{K} \mid \beta^n \in A\}$ beschouwen. De klassieke Kummertheorie is grofweg de studie van dit soort lichaamsuitbreidingen.

Het meest klassieke resultaat in de Kummertheorie is de classificatie van de abelse uitbreidingen met exponent die n deelt van een lichaam K dat alle n-de eenheidswortels bevat en waarvan de karakteristiek n niet deelt. Een bijectie tussen de verzameling van dergelijke uitbreidingen, bevat in een vast gekozen algebraïsche afsluiting $\overline{K}$, en de verzameling ondergroepen van $K^\times$ die $(K^\times)^n$ bevatten, wordt namelijk verkregen door L te associëren met $K^\times \cap (L^\times)^n$, zie bijvoorbeeld [Lan02, Theorem VI.8.2].

De Kummertheorie heeft interessante toepassingen bij het bestuderen van

bepaalde *dichtheidsproblemen*: als $\alpha \neq 0$ een element is van een getallenlichaam K, dan is de dichtheid van priemidealen $\mathfrak{p}$ van K zodanig dat de multiplicatieve orde van α modulo $\mathfrak{p}$ copriem is met een vast priemgetal ℓ, dan wel een voorgeschreven ℓ-adische valuatie heeft, kan worden uitgedrukt in termen van de graden van de cyclotomische-Kummeruitbreidingen $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha})$ voor alle $n > 0$, waarbij ζ_{ℓ^n} een eenheidswortel van orde ℓ^n is. Zie [Per15] voor het zojuist beschreven geval en [DP16, PS19] voor een generalisatie naar ondergroepen van eindige rang in $K^\times$. Deze problemen hangen nauw samen met het vermoeden van Artin over primitieve wortels, zoals bijvoorbeeld uitgelegd in [Mor12].

Het berekenen van de graden van oneindig veel lichaamsuitbreidingen lijkt misschien een zware taak. Het volgende is echter bekend (zie [PS19, Theorem 1.1] voor een direct bewijs): als A een ondergroep van $K^\times$ is van eindige rang r, dan is er een constante $C > 0$ zodanig dat voor elk positief geheel getal n de verhouding tussen n^r en de graad $[K(\sqrt[n]{A}) : K(\zeta_n)]$ een deler is van C. Dit resultaat kan effectief worden gemaakt, zie [PST20a, Theorem 1.2], en voor het geval $K = \mathbb{Q}$ verschaffen de resultaten van [PST20b] een algoritme waarvan de output een eindige formule is voor deze graden. Dit algoritme is geïmplementeerd in SageMath, zie [Tro19].

Algebraïsche groepen

Tot nu toe hebben we Kummertheorie alleen in de klassieke zin besproken, maar deze concepten kunnen als volgt worden veralgemeend. Zijn K een lichaam, zeg voor de eenvoud van karakteristiek nul, $\overline{K}$ een algebraïsche afsluiting van K, en G een commutatieve algebraïsche groep over K. Als S een deelverzameling van $G(\overline{K})$ is, dan is de *lichaamsuitbreiding van K voortgebracht door S* het deellichaam van $\overline{K}$ verkregen door aan K de coördinaten van de punten van S toe te voegen. Om precies te zijn: als we elke x in S identificeren met een morfisme van schema's $\operatorname{spec} \overline{K} \to \operatorname{spec} K(x)$, dan hebben we een verzameling morfismen $K(x) \to \overline{K}$ als x varieert in S, en de samenstelling van de beelden van deze morfismen is dan per definitie $K(S)$.

Zij nu $A \subseteq G(K)$ een eindig voortgebrachte ondergroep. Voor elk positief geheel getal n kunnen we de deelverzameling $n^{-1}A = \{P \in G(\overline{K}) \mid nP \in A\}$ beschouwen. Uitbreidingen van K van de vorm $K(n^{-1}A)$ zijn het onderwerp van de studie van de *Kummertheorie voor commutatieve algebraïsche groepen*. Zoals men kan zien door $G = \mathbb{G}_m$ te nemen, waar $\mathbb{G}_m$ de multiplicatieve groep over K is, is deze theorie een directe generalisatie van de klassieke Kummertheorie. Zelfs in deze algemeenheid hebben Kummeruitbreidingen veel van de interessante eigenschappen van hun klassieke tegenhangers. Bijvoorbeeld is $K(n^{-1}A)$ een Galoisuitbreiding van K die het *n-torsielichaam* van G bevat, dat wil zeggen de lichaamsuitbreiding van K voortgebracht door alle n-torsiepunten van $G(\overline{K})$;

bovendien is het Galois en abels over dit lichaam. Torsielichamen zijn de directe veralgemening van cyclotomische lichamen, en veel resultaten over Kummeruitbreidingen kunnen worden afgeleid uit eigenschappen van deze lichamen.

Als K een getallenlichaam is, dan kan het bovengenoemde dichtheidsprobleem *mutatis mutandis* in deze algemenere context worden geformuleerd, en is het nog steeds gerelateerd aan de graden van Kummeruitbreidingen. Zie [Pin04] voor een bespreking in het geval van abelse variëteiten en [Per08, Per11] voor het product van een abelse variëteit en een torus. Dit motiveert de studie van de graden van Kummeruitbreidingen in een algemene context. In zijn fundamentele artikel [Rib79] bewees Ribet het volgende resultaat: als G het product is van een abelse variëteit en een torus en $A \subseteq G(K)$ een vrij $\mathbb{Z}$-moduul van rang r is, met een basis over $\mathbb{Z}$ van punten lineair onafhankelijk over $\mathrm{End}_K(G)$, dan bestaat er een positief geheel getal C zodanig dat de verhouding tussen n^{rs} en de graad $[K(n^{-1}A) : K(G[n])]$ een deler is van C voor elk positief geheel getal n. Hier is s het unieke positieve gehele getal zodanig dat voor elke $n > 1$ geldt $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$. Zie ook [Ber88, Théorème 5.2] en [Hin88, Lemme 14]. De artikelen die in dit proefschrift zijn verzameld, zijn gewijd aan het effectiever maken van dit resultaat, waarbij wordt geprobeerd de constante C uit te drukken in termen van bekende grootheden gerelateerd aan de torsielichamen van G.

Effectieve resultaten voor elliptische krommen

De eerste twee artikelen, geschreven in samenwerking met Lombardo, richten zich op het geval van elliptische krommen. Zij G een elliptische kromme over een getallenlichaam K, zij $\overline{K}$ een algebraïsche afsluiting van K, en zij $\alpha \in G(K)$. In [JR10] hebben Jones en Rouse bewezen dat voor elk priemgetal ℓ, onder bepaalde aannames over α en met een kleine uitzondering voor het priemgetal 2, de surjectiviteit van de ℓ-adische Galoisrepresentatie geassocieerd met G de maximaliteit van de Kummeruitbreidingen $K(n^{-1}\alpha)$ over $K(G[n])$ impliceert als n een macht is van ℓ. Zie [JR10, stelling 5.2] voor het niet-CM-geval en [JR10, stelling 5.8] voor het CM-geval. In het licht hiervan formuleerde Perucca twee vragen: Als de Galoisrepresentatie niet surjectief is, kunnen we dan het falen van de maximaliteit van de Kummeruitbreidingen beschrijven, of op zijn minst begrenzen, in termen van het falen van de maximaliteit van de Galoisrepresentaties? Kunnen deze resultaten worden gegeneraliseerd naar het geval waarin n een positief geheel getal is?

Het eerste artikel dat hier [Chapter 1] wordt gepresenteerd, is bedoeld om deze vragen te beantwoorden. De hoofdstelling [Chapter 1, Theorem 1.1] geeft een positief antwoord, maar alleen onder de aanname dat $\mathrm{End}_K(G) = \mathbb{Z}$. Deze stelling is een effectieve versie van het klassieke resultaat van Ribet in het geval van een groep G voortgebracht door een enkel punt α, en het laat zien dat de

bovengenoemde constante C alleen afhangt van eigenschappen van de *ℓ-adische* representaties, voor alle priemgetallen ℓ, en andere effectief berekenbare grootheden geassocieerd met G. Voorbeelden die de niet-toepasbaarheid van deze methoden op het CM-geval aantonen, worden gegeven in [Chapter 1, Section 6]. De tweede hoofdstelling [Chapter 1, Theorem 1.2] laat zien dat er over het lichaam $\mathbb{Q}$ een uniforme versie van dit resultaat bestaat onder de aanname dat het punt α niet deelbaar is in $G(\mathbb{Q})/G(\mathbb{Q})_{\mathrm{tors}}$ – dat wil zeggen dat er geen $\beta \in G(\mathbb{Q})$ bestaat zodanig dat α geschreven kan worden als $n\beta + \tau$ voor een geheel getal $n > 1$ en $\tau \in G(\mathbb{Q})_{\mathrm{tors}}$.

Het doel van het tweede artikel met Lombardo [Chapter 2] is om het bovengenoemde resultaat [Chapter 1, Theorem 1.2] expliciet te maken door een werkelijke numerieke waarde te vinden voor de constante C, zie [Chapter 2, Theorem 6.5]. Deze resultaten zijn bereikt door uniforme grenzen te geven aan andere interessante grootheden die verband houden met de Galoisrepresentaties van G. Opmerkelijke voorbeelden van zulke grootheden zijn de exponenten van de cohomologiegroepen van $\mathrm{Gal}(\mathbb{Q}(G(\overline{\mathbb{Q}})_{\mathrm{tors}}) \mid \mathbb{Q})$ met coëfficiënten in de torsieondergroepen van G, beschouwd als Galoismodulen. Grenzen voor vergelijkbare grootheden zijn onafhankelijk gevonden door Cerchia en Rouse [CR21].

Een technisch raamwerk voor de algemene Kummertheorie

Sommige van de bovengenoemde expliciete resultaten zijn afhankelijk van eigenschappen van Galoisrepresentaties die alleen voor elliptische krommen in een effectieve vorm bekend zijn. De methoden die worden gebruikt om aan te tonen dat de graden van Kummeruitbreidingen gerelateerd zijn aan deze grootheden, zijn hier echter onafhankelijk van. In het derde artikel dat in dit proefschrift is opgenomen, wordt dit duidelijk gemaakt door de theoretische achtergrond te conceptualiseren in een raamwerk dat van toepassing is op elke commutatieve algebraïsche groep G over K die voldoet aan $\mathrm{End}_K(G) = \mathbb{Z}$. De methoden die in dit werk worden gebruikt, zijn geïnspireerd op resultaten van Palenstijn [Pal04, Pal14] en op gesprekken met Lenstra en Stevenhagen. Als toepassing worden de resultaten van [Chapter 1] en [Chapter 2] uitgebreid naar groepen A met een rang hoger dan 1.

Tot nu toe hebben we het geval waarin de endomorfismering van G groter is dan $\mathbb{Z}$ nog niet met succes aangepakt, en het lijkt erop dat onze methoden in dat geval een substantiële verfijning nodig hebben. In zijn proefschrift [JP21] gaat Javan Peykar in op dit probleem in het geval van elliptische krommen met complexe vermenigvuldiging door $A \subseteq G(K)$ te nemen als een $\mathrm{End}_K(G)$-moduul, en de modulen van "delingspunten" door een *Steinitzideaal* te beschouwen. Zelfs

met enige technische beperkingen is deze methode zeer succesvol.

Gemotiveerd door deze benadering is het laatste artikel in dit proefschrift [Chapter 4] voornamelijk gewijd aan de studie van puur algebraïsche eigenschappen van delingsmodulen over algemene ringen. De door Javan Peykar gebruikte Steinitzidealen worden vervangen door *ideaalfilters*, en er wordt een veralgemening gegeven van het klassieke begrip injectiviteit, dat voor zover de auteur weet nieuw is. Een notie van (J, T)-*uitbreiding*, waarbij J een vast ideaalfilter is en T een geschikt R-moduul, generaliseert de modulen van delingspunten. De eigenschappen van deze objecten worden vervolgens bestudeerd vanuit een categorietheoretisch oogpunt, waarna enkele resultaten over hun automorfismegroepen worden gegeneraliseerd die zijn verschenen in de minder algemene settings van [Pal04], [Pal14] en [JP21].

Deze lange uitweiding in de commutatieve algebra werpt uiteindelijk zijn vruchten af: de zo geconstrueerde theorie, die die van [Chapter 3] generaliseert, wordt uiteindelijk toegepast om de resultaten van [Chapter 1] en [JP21] te verenigen en te veralgemenen, wat aantoont dat de twee schijnbaar verschillende benaderingen eigenlijk gewoon verschillende realisaties zijn van een algemenere theorie. De mate van algemeenheid die in dit artikel wordt gebruikt, opent de deur naar toepassingen op hogerdimensionale abelse variëteiten en andere klassen van commutatieve algebraïsche groepen.

Chapter 1

Effective Kummer theory for elliptic curves

by Davide Lombardo and Sebastiano Tronto [LT21a]

1 Introduction

1.1 Setting

Let E be an elliptic curve defined over a number field K (for which we fix an algebraic closure $\overline{K}$) and let $\alpha \in E(K)$ be a point of infinite order. The purpose of this paper is to study the extensions of K generated by the division points of α; in order to formally introduce these extensions we need to set some notation.

Given a positive integer M, we denote by $E[M]$ the group of M-torsion points of E, that is, the set $\{P \in E(\overline{K}) : MP = 0\}$ equipped with the group law inherited from E. Moreover, we denote by K_M the *M-th torsion field* $K(E[M])$ of E, namely, the finite extension of K obtained by adjoining the coordinates of all the M-torsion points of E. For each positive integer N dividing M, we let $N^{-1}\alpha := \left\{\beta \in E(\overline{K}) \mid N\beta = \alpha\right\}$ denote the set of N-division points of α and set

$$K_{M,N} := K(E[M], N^{-1}\alpha).$$

The field $K_{M,N}$ is called the (M,N)-*Kummer extension* of K (associated with α), and both K_M and $K_{M,N}$ are finite Galois extensions of K. It is a classical

question to study the degree of $K_{M,N}$ over K_M as M, N vary, see for example [Ber88, Théorème 1], [Hin88, Lemme 14], or Ribet's foundational paper [Rib79]. In particular, it is known that there exists an integer $C = C(E/K, \alpha)$, depending only on E/K and α, such that

$$\frac{N^2}{[K_{M,N} : K_M]} \quad \text{divides} \quad C$$

for every pair of positive integers (M, N) with $N \mid M$. The aim of this paper is to give an explicit version of this result, and to show that it can be made *uniform* when the base field is $K = \mathbb{Q}$. Our first result is that, under the assumption $\mathrm{End}_K(E) = \mathbb{Z}$, the integer C can be bounded (explicitly) in terms of the ℓ-adic Galois representations attached to E and of divisibility properties of the point α, and that this statement becomes false if we remove the hypothesis $\mathrm{End}_K(E) = \mathbb{Z}$. On the other hand, the assumption $\mathrm{End}_K(E) = \mathbb{Z}$ is always satisfied when $K = \mathbb{Q}$, and we show that in this case C can be taken to be independent of E and α, provided that α and all its translates by torsion points are not divisible by any $n > 1$ in the group $E(\mathbb{Q})$. This is a rather surprising statement, especially given that such a strong uniformity result is not known for the closely connected problem of studying the degrees of the torsion fields K_M over K.

1.2 Main results

Our main results are the following.

Theorem 1.1. *Assume that* $\mathrm{End}_K(E) = \mathbb{Z}$. *There is an explicit constant* C, *depending only on* α *and on the* ℓ*-adic torsion representations associated to* E *for all primes* ℓ, *such that*

$$\frac{N^2}{[K_{M,N} : K_M]} \quad \textit{divides} \quad C$$

for all pairs of positive integers (M, N) *with* N *dividing* M.

The proof gives an explicit expression for C that depends on computable parameters associated with E and α. We also show that all these quantities can be bounded effectively in terms of standard invariants of the elliptic curve and of the height of α, see Remark 5.17.

Theorem 1.2. *There is a universal constant* $C > 0$ *with the following property. Let* $E/\mathbb{Q}$ *be an elliptic curve, and let* $\alpha \in E(\mathbb{Q})$ *be a point such that the class of* α *in the free abelian group* $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ *is not divisible by any* $n > 1$. *Then*

$$\frac{N^2}{[\mathbb{Q}_{M,N} : \mathbb{Q}_M]} \quad \textit{divides} \quad C$$

for all pairs of positive integers (M, N) with N dividing M.

The assumption on the divisibility of the point α is necessary: it is enough to replace α with a multiple $\ell\alpha$ to gain an extra factor ℓ^2 in the ratio $\frac{N^2}{[\mathbb{Q}_{M,N}:\mathbb{Q}_M]}$ when N is divisible by a sufficiently high power of ℓ. However, one can remove this assumption and obtain a bound that depends only on the largest integer n such that α is n-divisible in $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, but not on the curve, see Remark 7.2. Also observe that Theorems 1.1 and 1.2 immediately imply lower bounds of the form $[K_{M,N} : K_M] \geqslant \frac{1}{C}N^2$.

We remark that recent work by Cerchia and Rouse [CR21] also investigates similar questions – in particular, the problem of uniformity – but only focuses on a single ℓ-adic representation at a time (equivalently: the case when M, N are both powers of some fixed prime ℓ), while our results cover the more general adelic situation. In fact, the main difficulty in the present work stems from the possible interactions between the ℓ-power torsion fields for different primes ℓ (the so-called *entanglement* phenomenon), and it is to handle this difficulty that we need to introduce some new ideas in Section 7. These ideas allow us to reduce the study of the cohomology of the Galois modules $E[N]$ for general N to the corresponding question for $E[\ell^k]$, where $\ell^k \mid N$; this is nontrivial precisely because there can be interactions between torsion fields related to different primes. Our main cohomological result (Theorem 7.5) can be stated as follows.

Theorem 1.3. *There is a positive integer C_1 such that, for every elliptic curve $E/\mathbb{Q}$, the exponent of $H^1(\mathrm{Gal}(\mathbb{Q}(E(\overline{\mathbb{Q}})_{\mathrm{tors}}) \mid \mathbb{Q}), E(\overline{\mathbb{Q}})_{\mathrm{tors}})$ divides C_1.*

It is not hard to see that this statement would follow from a positive answer to Serre's well-known uniformity question concerning the Galois representations attached to elliptic curves over $\mathbb{Q}$ (see e.g. [Ser72, §4.3]). In order to obtain an unconditional proof we need to combine several ingredients: in addition to some cohomological tools, including the inflation-restriction sequence, our proof of this theorem relies on several deep results on the images of the modulo-ℓ Galois representations attached to elliptic curves, including the uniform boundedness of isogenies for elliptic curves defined over $\mathbb{Q}$ (Theorem 3.14). The fact that similar results are not known for general number fields is the main reason why at present we cannot easily generalise Theorem 1.2 to number fields other than $\mathbb{Q}$.

1.3 Structure of the paper

We start with some necessary general preliminaries in Section 2, leading up to a factorisation of the constant C of Theorem 1.1 as a product of certain contributions which we dub the *ℓ-adic* and *adelic* failures (corresponding to E, α, and a fixed prime ℓ). In the same section we also introduce some of the main actors of this paper, in the form of several Galois representations associated with

the torsion and Kummer extensions. In Section 3 we then recall some important properties of the torsion representations that will be needed in the rest of the paper. In Sections 4 and 5 we study the ℓ-adic and adelic failures respectively. In Section 6 we show that one cannot hope to naïvely generalise some of the results in section 4 to CM curves. Finally, in Section 7 we prove Theorem 1.2 by establishing several auxiliary results about the Galois cohomology of the torsion modules $E[M]$ that might have an independent interest.

2 Preliminaries

2.1 Notation and definitions

The letter K will always denote a number field, E an elliptic curve defined over K, and α a point of infinite order in $E(K)$. For n a positive integer, we denote by ζ_n a primitive root of unity of order n. Given a prime ℓ, we denote by v_ℓ the usual ℓ-adic valuation on $\mathbb{Q}$ and on $\mathbb{Q}_\ell$. If X is a vector in $\mathbb{Z}_\ell^n$ or a matrix in $\mathrm{Mat}_{m\times n}(\mathbb{Z}_\ell)$, we call *valuation* of X, denoted by $v_\ell(X)$, the minimum of the ℓ-adic valuations of its coefficients.

We shall often use divisibility conditions involving the symbols ℓ^∞ (where ℓ is a prime) and ∞. Our convention is that every power of ℓ divides ℓ^∞, every positive integer divides ∞, and ℓ^∞ divides ∞. Recall from the Introduction that we denote by K_M the field $K(E[M])$ generated by the coordinates of the M-torsion points of E, and by $K_{M,N}$ (for $N \mid M$) the field $K(E[M], N^{-1}\alpha)$. We extend this notation by setting $K_{\ell^\infty} = \bigcup_n K_{\ell^n}$, $K_\infty = \bigcup_M K_M$, and more generally, for $M, N \in \mathbb{N}_{>0} \cup \{\ell^\infty, \infty\}$ with $N \mid M$,

$$K_M = \bigcup_{d|M} K_d, \quad K_{M,N} = \bigcup_{d|M} \bigcup_{\substack{e|d \\ e|N}} K_{d,e}$$

If H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we denote by $\mathbb{Z}_\ell[H]$ the sub-$\mathbb{Z}_\ell$-algebra of $\mathrm{Mat}_2(\mathbb{Z}_\ell)$ topologically generated by the elements of H. Let G be a (profinite) group. We write G' for its derived subgroup, namely, the subgroup of G (topologically) generated by commutators, and $G^{\mathrm{ab}} = G/G'$ for its abelianisation, namely, its largest abelian (profinite) quotient. We say that a finite simple group S *occurs* in a profinite group G if there are closed subgroups H_1, H_2 of G, with $H_1 \triangleleft H_2$, such that H_2/H_1 is isomorphic to S. Finally, we denote by $\exp G$ the exponent of a finite group G, namely, the smallest integer $e \geqslant 1$ such that $g^e = 1$ for every $g \in G$.

2.2 The ℓ-adic and adelic failures

We start by observing that it is enough to restrict our attention to the case $N = M$:

Remark 2.1. Suppose that there is a constant $C \geqslant 1$ such that

$$\frac{M^2}{[K_{M,M} : K_M]} \quad \text{divides} \quad C$$

for all positive integers M. Then for any $N \mid M$, since $[K_{M,M} : K_{M,N}]$ divides $(M/N)^2$, we have that

$$\frac{N^2}{[K_{M,N} : K_M]} = \frac{N^2[K_{M,M} : K_{M,N}]}{[K_{M,M} : K_M]} \quad \text{divides} \quad \frac{M^2}{[K_{M,M} : K_M]},$$

which in turn divides C.

We now describe a decomposition of the ratio $\frac{N^2}{[K_{N,N}:K_N]}$ into two arithmetically meaningful parts. Elementary field theory gives

$$\begin{aligned}
\frac{N^2}{[K_{N,N} : K_N]} &= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2n_\ell}}{[K_{N,\ell^{n_\ell}} : K_N]} = \\
&= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2n_\ell}}{[K_{\ell^{n_\ell},\ell^{n_\ell}} : K_{\ell^{n_\ell}}]} \cdot \frac{[K_{\ell^{n_\ell},\ell^{n_\ell}} : K_{\ell^{n_\ell}}]}{[K_{N,\ell^{n_\ell}} : K_N]} = \\
&= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2n_\ell}}{[K_{\ell^{n_\ell},\ell^{n_\ell}} : K_{\ell^{n_\ell}}]} \cdot [K_{\ell^{n_\ell},\ell^{n_\ell}} \cap K_N : K_{\ell^{n_\ell}}]
\end{aligned}$$

where $n_\ell = v_\ell(N)$. To see why the first equality holds, recall that the degree $[K_{N,\ell^{n_\ell}} : K_N]$ is a power of ℓ, so the fields $K_{N,\ell^{n_\ell}}$ are linearly disjoint over K_N, and clearly they generate all of $K_{N,N}$.

Definition 2.2. Let ℓ be a prime and N a positive integer. Let $n := v_\ell(N)$. We call

$$A_\ell(N) := \frac{\ell^{2n}}{[K_{\ell^n,\ell^n} : K_{\ell^n}]}$$

the *ℓ-adic failure* at N and

$$B_\ell(N) := \frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{N,\ell^n} : K_N]} = [K_{\ell^n,\ell^n} \cap K_N : K_{\ell^n}]$$

the *adelic failure* at N (related to ℓ). Notice that both $A_\ell(N)$ and $B_\ell(N)$ are powers of ℓ.

Example 2.3. It is clear that the ℓ-adic failure $A_\ell(N)$ can be nontrivial, that is, different from 1. Suppose for example that $\alpha = \ell\beta$ for some $\beta \in E(K)$: then we have

$$K_{\ell^n,\ell^n} = K_{\ell^n}(\ell^{-n}\alpha) = K_{\ell^n}(\ell^{-n+1}\beta),$$

and the degree of this field over K_{ℓ^n} is at most $\ell^{2(n-1)}$, so $\ell^2 \mid A_\ell(N)$. In Example 4.5 we will show that the ℓ-adic failure can be non-trivial also when α is strongly ℓ-indivisible (see Definition 4.1).

Example 2.4. We now show that the adelic failure $B_\ell(N)$ can be non-trivial as well. Consider the elliptic curve E over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 + x^2 - 44x - 84$$

and with Cremona label 624f2 (see [LMF22, label 624f2]). One can show that $E(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$, so that the curve has full rational 2-torsion, and that a generator of the free part of $E(\mathbb{Q})$ is given by $P = (-5, 6)$. The 2-division points of P are given by $(1 + \sqrt{-3}, -3 + 7\sqrt{-3})$, $(-11 + 3\sqrt{-3}, 27 + 15\sqrt{-3})$, and their Galois conjugates, so they are defined over $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}_3$, and we have $B_2(6) := [\mathbb{Q}_{2,2} \cap \mathbb{Q}_6 : \mathbb{Q}_2] = [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. These computations have been checked with SageMath [The].

2.3 The torsion, Kummer and arboreal representations

In this section we introduce three representations of the absolute Galois group of K that will be our main tool for studying the extensions $K_{M,N}$. For further information about these representations see for example [JR10, Section 3], [BP21], and [LP21].

The torsion representation

Let N be a positive integer. The group $E[N]$ of N-torsion points of E is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. Since the multiplication-by-N map is defined over K, the absolute Galois group of K acts $\mathbb{Z}/N\mathbb{Z}$-linearly on $E[N]$, and we get a homomorphism

$$\tau_N : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{Aut}(E[N]).$$

The field fixed by the kernel of τ_N is exactly the N-th torsion field K_N. Thus, after fixing a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$, the Galois group $\mathrm{Gal}(K_N \mid K)$ is identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which we denote by H_N.

As N varies, and provided that we have made compatible choices of bases, these representations form a compatible projective system. We can therefore pass

to the limit over the powers of a fixed prime number ℓ to obtain the *ℓ-adic torsion representation* $\tau_{\ell^\infty} : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. We can also take the limit over all integers N (ordered by divisibility) to obtain the *adelic torsion representation* $\tau_\infty : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$. We denote by H_{ℓ^∞} (resp. H_∞) the image of τ_{ℓ^∞} (resp. τ_∞). The group H_{ℓ^∞} (resp. H_∞) is isomorphic to $\mathrm{Gal}(K_{\ell^\infty} \mid K)$ (resp. $\mathrm{Gal}(K_\infty \mid K)$).

One can also pass to the limit on the torsion subgroups themselves, obtaining the *ℓ-adic Tate module* $T_\ell E = \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell^2$ and the *adelic Tate module* $TE = \varprojlim_M E[M] \cong \widehat{\mathbb{Z}}^2 \cong \prod_\ell \mathbb{Z}_\ell^2$.

The Kummer representation

Let M and N be positive integers with $N \mid M$. Let $\beta \in E(\overline{K})$ be a point such that $N\beta = \alpha$. For any $\sigma \in \mathrm{Gal}(\overline{K} \mid K_M)$ we have that $\sigma(\beta) - \beta$ is an N-torsion point, so the following map is well-defined:

$$\begin{array}{rccc} \kappa_N : & \mathrm{Gal}(\overline{K} \mid K_M) & \to & E[N] \\ & \sigma & \mapsto & \sigma(\beta) - \beta. \end{array}$$

Since any other N-division point β' of α satisfies $\beta' = \beta + T$ for some $T \in E[N]$, and the coordinates of T belong to $K_N \subseteq K_M$, the map κ_N does not depend on the choice of β. It is also immediate to check that κ_N is a group homomorphism, and that the field fixed by its kernel is exactly the (M, N)-Kummer extension of K. Fixing a basis of $E[N]$ we can identify the Galois group $\mathrm{Gal}(K_{M,N} \mid K_M)$ with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^2$. It is then clear that $K_{M,N}$ is an abelian extension of K_M of degree dividing N^2, and the Galois group of this extension has exponent dividing N. In the special case $M = N$ we denote by V_N the image of $\mathrm{Gal}\,(K_{N,N} \mid K_N)$ in $(\mathbb{Z}/N\mathbb{Z})^2$.

By passing to the limit in the previous constructions we also obtain the following:

(i) There is an ℓ-adic Kummer representation $\kappa_{\ell^\infty} : \mathrm{Gal}(\overline{K} \mid K_{\ell^\infty}) \to T_\ell E$ which factors via a map $\mathrm{Gal}(K_{\ell^\infty,\ell^\infty} \mid K_{\ell^\infty}) \to T_\ell E$ (still denoted by κ_{ℓ^∞}).

(ii) The image V_{ℓ^∞} of κ_{ℓ^∞} is a sub-$\mathbb{Z}_\ell$-module of $T_\ell E \cong \mathbb{Z}_\ell^2$, and it is isomorphic to $\mathrm{Gal}(K_{\ell^\infty,\ell^\infty} \mid K_{\ell^\infty})$ as a profinite group. We therefore identify the Galois group $\mathrm{Gal}(K_{\ell^\infty,\ell^\infty} \mid K_{\ell^\infty})$ with V_{ℓ^∞}.

(iii) We can identify the Galois group $\mathrm{Gal}(K_{\infty,\ell^\infty} \mid K_\infty)$ with a $\mathbb{Z}_\ell$-submodule W_{ℓ^∞} of V_{ℓ^∞} (hence also of $T_\ell E$) via the representation κ_{ℓ^∞}.

(iv) We can identify the Galois group $\mathrm{Gal}(K_{\infty,\infty} \mid K_\infty)$ with a sub-$\widehat{\mathbb{Z}}$-module W_∞ of $TE \cong \widehat{\mathbb{Z}}^2$.

Notice that W_{ℓ^∞} is the projection of W_∞ in $\mathbb{Z}_\ell^2$, and since W_{ℓ^∞} is a pro-ℓ group and there are no nontrivial continuous morphisms from a pro-ℓ group to a pro-ℓ' group for $\ell \neq \ell'$ we have $W_\infty = \prod_\ell W_{\ell^\infty}$.

The arboreal representation

Fix a sequence $\{\beta_i\}_{i\in\mathbb{N}}$ of points in $E(\overline{K})$ such that $\beta_1 = \alpha$ and $N\beta_M = \beta_{M/N}$ for all pairs of positive integers (N, M) with $N \mid M$. For every $N \geqslant 1$ fix furthermore a $\mathbb{Z}/N\mathbb{Z}$-basis $\{T_1^N, T_2^N\}$ of $E[N]$ in such a way that $NT_1^M = T_1^{M/N}$ and $NT_2^M = T_2^{M/N}$ for every pair of positive integers (N, M) with $N \mid M$. For every $N \geqslant 1$, the map

$$\begin{aligned} \omega_N : \mathrm{Gal}(K_{N,N} \mid K) &\to (\mathbb{Z}/N\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \sigma &\mapsto (\sigma(\beta_N) - \beta_N, \tau_N(\sigma)) \end{aligned}$$

is an injective homomorphism (similarly to [JR10, Proposition 3.1]) and thus identifies the group $\mathrm{Gal}(K_{N,N} \mid K)$ with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

It will be important for our applications to notice that V_N comes equipped with an action of H_N coming from the fact that V_N is the (abelian) kernel of the natural map $\mathrm{Gal}(K_{N,N} \mid K) \to H_N$. More precisely, the action of $h \in H_N$ on $v \in V_N$ is given by conjugating the element $(v, \mathrm{Id}) \in (\mathbb{Z}/N\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by $(0, h)$. Explicitly, we have

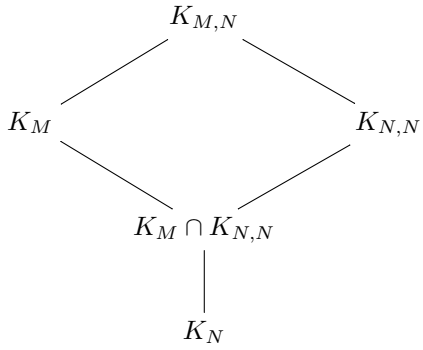
$$(0, h)(v, \mathrm{Id})(0, h)^{-1} = (hv, h)(0, h^{-1}) = (hv, \mathrm{Id}),$$

so that the action of H_N on V_N is induced by the natural action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $(\mathbb{Z}/N\mathbb{Z})^2$. We obtain similar statements by suitably passing to the limit in N:

Lemma 2.5. *For every positive integer N, the group V_N is an H_N-submodule of $(\mathbb{Z}/N\mathbb{Z})^2$ for the natural action of $H_N \leqslant \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $V_N \leqslant (\mathbb{Z}/N\mathbb{Z})^2$. Similarly, both V_{ℓ^∞} and W_{ℓ^∞} are H_{ℓ^∞}-modules.*

Remark 2.6. Let $N \in \mathbb{N} \cup \{\ell^\infty\}$ and $M \in \mathbb{N} \cup \{\ell^\infty, \infty\}$ with $N \mid M$. Then the group $\mathrm{Gal}(K_{M,N} \mid K_M)$ can be identified with a subgroup of V_N: this follows

from inspection of the diagram



which shows that $\mathrm{Gal}(K_{M,N} \mid K_M)$ is isomorphic to $\mathrm{Gal}(K_{N,N} \mid K_M \cap K_{N,N})$, which in turn is clearly a subgroup of $\mathrm{Gal}(K_{N,N} \mid K_N) \cong V_N$.

2.4 Curves with complex multiplication

If $\mathrm{End}_{\overline{K}}(E) \neq \mathbb{Z}$ we say that E *has complex multiplication*, or CM for short. In this case $\mathrm{End}_{\overline{K}}(E)$ is an order in an imaginary quadratic field, called *the CM-field of* E. The torsion representations in the CM case have been studied for example in [Deu53] and [Deu58]. In this case, the image of the torsion representation τ_{ℓ^∞} is closely related to the *Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *corresponding to* $\mathrm{End}_{\overline{K}}(E)$, defined as follows:

Definition 2.7. Let F be a reduced $\mathbb{Q}_\ell$-algebra of degree 2 and let $\mathcal{A}_\ell$ be a $\mathbb{Z}_\ell$-order in F. The *Cartan subgroup* corresponding to $\mathcal{A}_\ell$ is the group of units of $\mathcal{A}_\ell$, which we embed in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ by fixing a $\mathbb{Z}_\ell$-basis of $\mathcal{A}_\ell$ and considering the left multiplication action of $\mathcal{A}_\ell^\times$. If $\mathcal{A}$ is an order in an imaginary quadratic number field, the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$ is defined by taking $\mathcal{A}_\ell = \mathcal{A} \otimes \mathbb{Z}_\ell$ in the above.

More precisely, when E/K is an elliptic curve with CM, the image of the ℓ-adic torsion representation τ_{ℓ^∞} is always contained (up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}_\ell)$) in the normaliser of the Cartan subgroup corresponding to $\mathrm{End}_{\overline{K}}(E)$, and is contained in the Cartan subgroup itself if and only if the complex multiplication is defined over the base field K.

In order to have a practical representation of Cartan subgroups, we recall the following definition from [LP17]:

Definition 2.8. Let C be a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We say that $(\gamma, \delta) \in \mathbb{Z}_\ell^2$ are *parameters for* C if C is conjugated in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to the subgroup

$$\left\{ \begin{pmatrix} x & \delta y \\ y & x + \gamma y \end{pmatrix} : x, y \in \mathbb{Z}_\ell,\ v_\ell(x(x+\gamma y) - \delta y^2) = 0 \right\}. \tag{2.1}$$

Parameters for C always exist, see [LP17, §2.3].

Remark 2.9 ([LP17, Remark 9])**.** One may always assume that γ, δ are integers. Furthermore, one can always take $\gamma \in \{0, 1\}$, and $\gamma = 0$ if $\ell \neq 2$.

We also recall the following explicit description of the normaliser of a Cartan subgroup [LP17, Lemma 14]:

Lemma 2.10. *A Cartan subgroup has index* 2 *in its normaliser. If* C *is as in* (2.1)*, its normaliser* N *in* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *is the disjoint union of* C *and*

$$C' := \begin{pmatrix} 1 & \gamma \\ 0 & -1 \end{pmatrix} \cdot C\,.$$

3 Properties of the torsion representation

Torsion representations are studied extensively in the literature; we have in particular the following fundamental theorem of Serre [Ser72], which applies to all elliptic curves (defined over number fields) without complex multiplication:

Theorem 3.1 (Serre)**.** *If* $\mathrm{End}_{\overline{K}}(E) = \mathbb{Z}$*, then* H_∞ *is open in* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$*. Equivalently, the index of* H_N *in* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *is bounded independently of* N*.*

There is also a CM analogue of Theorem 3.1, which is more easily stated by introducing the following definition:

Definition 3.2. Let E/K be an elliptic curve and ℓ be a prime number. We say that the image of the ℓ-adic representation is *maximal* if one of the following holds:

(i) E does not have CM over $\overline{K}$ and $H_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

(ii) E has CM over K by an order $\mathcal{A}$ in the imaginary quadratic field F, the prime ℓ is unramified in F and does not divide $[\mathcal{O}_F : \mathcal{A}]$, and H_{ℓ^∞} is conjugated to the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$.

(iii) E has CM over $\overline{K}$ (but not over K) by an order $\mathcal{A}$ in the imaginary quadratic field F, the prime ℓ is unramified in F and does not divide $[\mathcal{O}_F : \mathcal{A}]$, and H_{ℓ^∞} is conjugated to the normaliser of the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$.

Theorem 3.3 ([Ser72, Corollaire on p. 302])**.** *Let E/K be an elliptic curve admitting CM over $\overline{K}$. Then the ℓ-adic representation attached to E/K is maximal for all but finitely many primes ℓ.*

In the rest of this section we recall various important properties of the torsion representations: we shall need results that describe both the asymptotic behaviour of the mod ℓ^n torsion representation as $n \to \infty$ (§3.1 and 3.2) and the possible images of the mod ℓ representations attached to elliptic curves defined over the rationals (§3.3).

3.1 Maximal growth

We recall some results on the growth of the torsion extensions from [LP21, §2.3].

Proposition 3.4. *Let ℓ be a prime number. Let $\delta = 2$ if E has complex multiplication and $\delta = 4$ otherwise. There exists a positive integer n_ℓ such that*

$$\#H_{\ell^{n+1}}/\#H_{\ell^n} = \ell^\delta \qquad \text{for every } n \geqslant n_\ell.$$

Proof. This follows from Theorem 3.1 in the non-CM case and from classical results in the CM case. See also [LP21, Lemma 10 and Remark 13] for a more general result. □

Definition 3.5. We call an integer n_ℓ as in Proposition 3.4 a *parameter of maximal growth for the ℓ-adic torsion representation.* We say that it is *minimal* if $n_\ell - 1$ is not a parameter of maximal growth; when $\ell = 2$, we require that the minimal parameter be at least 2.

Remark 3.6. In the non-CM case we can give an equivalent definition of n_ℓ as follows. Consider the fundamental system of open neighbourhoods of Id in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ given by the normal subgroups

$$\cdots \subseteq \mathrm{Id} + \ell^n \operatorname{Mat}_2(\mathbb{Z}_\ell) \subseteq \cdots \subseteq \mathrm{Id} + \ell^2 \operatorname{Mat}_2(\mathbb{Z}_\ell) \subseteq \mathrm{Id} + \ell \operatorname{Mat}_2(\mathbb{Z}_\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

If E does not have CM over $\overline{K}$, Theorem 3.1 implies that H_{ℓ^∞} has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, so it must contain a subgroup of the form $I + \ell^n \operatorname{Mat}_2(\mathbb{Z}_\ell)$. Then it is easy to see that n_ℓ is the minimal such positive integer n. One can also give similar, but more complicated, characterisations of n_ℓ in the CM case using the structure of the Cartan subgroup associated with the ℓ-adic Galois representation attached to E/K.

Remark 3.7. The assumption $n_\ell \geqslant 2$ when $\ell = 2$ is needed to apply [LP21, Theorem 12].

Remark 3.8. Given an explicit elliptic curve E/K and a prime ℓ, the problem of determining the optimal value of n_ℓ can be solved effectively (see [LP21, Remark 13]). However, computing n_ℓ can be challenging in practice, because the naïve algorithm requires the determination of the Galois groups of the splitting fields of several large-degree polynomials. The situation is usually better for smaller primes ℓ, and especially for $\ell = 2$, for which the 2-torsion tower is known essentially explicitly (see [RZB15] for a complete classification result when $K = \mathbb{Q}$, and [Yel15] for a description of the 2-torsion tower of a given elliptic curve over a number field).

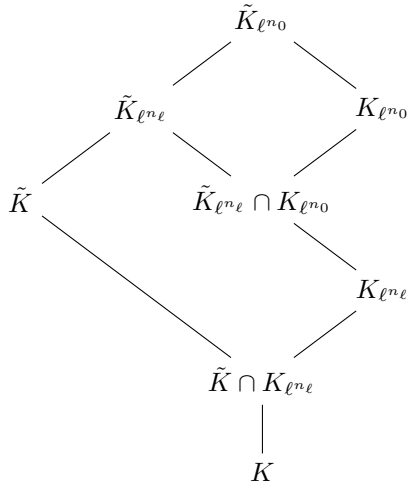
The following lemma, originally due to Serre, is very close in spirit to Proposition 3.4, and gives some control on the growth of the image of the ℓ-adic representation when the residual mod-ℓ representation is surjective:

Lemma 3.9 (Serre, [Ser97, IV-23, Lemma 3])**.** *Let $\ell \geqslant 5$ be a prime and let $G \subseteq \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ be a subgroup. Let $\pi : \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be the reduction homomorphism and suppose that $\pi(G) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$: then $G = \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$.*

In Section 5 we will need to bound the minimal parameter of maximal growth for the ℓ-adic torsion representation defined over certain extensions of the base field. We will do so with the help of the following Lemma:

Lemma 3.10. *Let $\tilde{K}$ be a finite extension of K. Let n_ℓ (resp. $\tilde{n}_\ell$) be the minimal parameter of maximal growth for the ℓ-adic torsion representation attached to E/K (resp. $E/\tilde{K}$). Then $\tilde{n}_\ell \leqslant n_\ell + v_\ell([\tilde{K} : K])$.*

Proof. Let $n_0 := n_\ell + v_\ell([\tilde{K} : K]) + 1$ and consider the following diagram:



Since clearly $[\tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]$ divides $[\tilde{K}_{\ell^{n_\ell}} : K_{\ell^{n_\ell}}]$, which in turn divides $[\tilde{K} : K]$, and since $[\tilde{K}_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}}] = [K_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}}]$, we have

$$\begin{aligned} v_\ell\left([K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]\right) &= v_\ell\left([K_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}}]\right) + v_\ell\left([\tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]\right) \\ &\leqslant v_\ell\left([\tilde{K}_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}}]\right) + v_\ell\left([\tilde{K} : K]\right). \end{aligned}$$

By [LP21, Theorem 12] we have

$$v_\ell\left([K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]\right) = \delta(n_0 - n_\ell) = \delta\left(v_\ell\left([\tilde{K} : K]\right) + 1\right),$$

where δ is as in Proposition 3.4, and we get

$$v_\ell\left([\tilde{K}_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}}]\right) \geqslant \delta + (\delta - 1)v_\ell\left([\tilde{K} : K]\right) > (\delta - 1)(n_0 - n_\ell).$$

Consider now the tower of extensions $\tilde{K}_{\ell^{n_\ell}} \subseteq \tilde{K}_{\ell^{n_\ell+1}} \subseteq \cdots \subseteq \tilde{K}_{\ell^{n_0}}$ and notice that by the pigeonhole principle for at least one $n \in \{n_\ell, n_\ell + 1, \ldots, n_0 - 1\}$ we must have $[\tilde{K}_{\ell^{n+1}} : \tilde{K}_{\ell^n}] \geqslant \delta$. But then by [LP21, Theorem 12] we have maximal growth over $\tilde{K}$ from $n < n_0$. Thus we get $\tilde{n}_\ell \leqslant n_\ell + v_\ell\left([\tilde{K} : K]\right)$ as claimed. □

3.2 Uniform growth of ℓ-adic representations

The results in this subsection and the next will be needed in Section 7. We start by recalling the following result, due to Arai:

Theorem 3.11 ([Ara08, Theorem 1.2])**.** *Let K be a number field and let ℓ be a prime. Then there exists an integer $n \geqslant 0$, depending only on K and ℓ, such that for any elliptic curve E over K with no complex multiplication over $\overline{K}$ we have*

$$\tau_{\ell^\infty}(\mathrm{Gal}(\overline{K} \mid K)) \supseteq \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \mathrm{Id} \pmod{\ell^n}\}.$$

For the next result we shall need a well-known Lemma about twists of elliptic curves:

Lemma 3.12. *Let E_1, E_2 be elliptic curves over K such that $(E_1)_{\overline{\mathbb{Q}}}$ is isomorphic to $(E_2)_{\overline{\mathbb{Q}}}$. There is an extension F of K, of degree dividing 12, such that E_1 and E_2 become isomorphic over F.*

Proof. Fixing a $\overline{\mathbb{Q}}$-isomorphism between E_1 and E_2 allows us to attach to E_2 a class in the cohomology group $H^1\left(\mathrm{Gal}(\overline{K} \mid K), \mathrm{Aut}(E_1)\right)$. Since

$$H^1\left(\mathrm{Gal}(\overline{K} \mid K), \mathrm{Aut}(E_1)\right) \cong K^\times / K^{\times n}$$

for some $n \in \{2, 4, 6\}$ (see [Sil09, Proposition X.5.4]), the class of E_2 corresponds to the class of a certain $[\alpha] \in K^\times/K^{\times n}$. Letting $F = K(\sqrt[n]{\alpha})$, whose degree over K divides 12, it is clear that $[\alpha] \in F^\times/F^{\times n}$ is trivial, so the same is true for $[E_2] \in H^1(\mathrm{Gal}(\overline{F} \mid F), \mathrm{Aut}(E_1))$, which means that E_2 is isomorphic to E_1 over F as desired. □

Corollary 3.13. *Let K be a number field and ℓ be a prime number. There exists an integer n_ℓ with the following property: for every elliptic curve E/K, the minimal parameter of maximal growth for the ℓ-adic representation attached to E is at most n_ℓ.*

Proof. Let n be the integer whose existence is guaranteed by Theorem 3.11. By the general theory of CM elliptic curves, we know that there are finitely many values $j_1, \dots, j_k \in \overline{\mathbb{Q}}$ such that for every CM elliptic curve E/K we have $j(E) \in \{j_1, \dots, j_k\}$. For each such j_i, fix an elliptic curve E_i/K with $j(E_i) = j_i$. To every E_i/K corresponds a minimal parameter of maximal growth for the ℓ-adic representation that we call m_i. Let $n_\ell = \max\{n, m_i + 2 \mid i = 1, \dots, k\}$: we claim that this value of n_ℓ satisfies the conclusion of the Corollary. Indeed, let E/K be any elliptic curve. If E does not have CM, the minimal parameter of maximal growth for its ℓ-adic representation is at most $n \leqslant n_\ell$. If E has CM, then there exists i such that $j(E) = j_i = j(E_i)$, so E is a twist of E_i. By Lemma 3.12 the curves E and E_i become isomorphic over an extension F/K of degree dividing 12, so if m (resp. $\tilde{m}$, resp. $\tilde{m}_i$) denotes the minimal parameter of maximal growth for E/K (resp. for E/F, resp. for E_i/F) we have

$$m \leqslant \tilde{m} = \tilde{m}_i \leqslant m_i + 2 \leqslant n_\ell,$$

where the equality follows from the fact that E and E_i are isomorphic over F, while the inequality $\tilde{m}_i \leqslant m_i + 2$ follows from Lemma 3.10 combined with the fact that we have $v_\ell([F : K]) \leqslant v_\ell(12) \leqslant 2$ for every prime ℓ. □

3.3 Possible images of $\bmod \ell$ representations

We recall several results concerning the images of the $\bmod \ell$ representations attached to elliptic curves over $\mathbb{Q}$. We begin with a famous Theorem of Mazur, to state which we let

$$\mathcal{T}_0 := \{p \text{ prime } \mid p \leqslant 17\} \cup \{37\}.$$

Theorem 3.14 ([MG78, Theorem 1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve and assume that E has a $\mathbb{Q}$-rational subgroup of order p. Then $p \in \mathcal{T}_0 \cup \{19, 43, 67, 163\}$. If E does not have CM over $\overline{\mathbb{Q}}$, then $p \in \mathcal{T}_0$.*

We then recall the following result of Zywina, which builds upon previous work of Serre, Mazur [MG78], Bilu-Parent [BP11], and Bilu-Parent-Rebolledo [BPR13]:

Theorem 3.15 ([Zyw15a, Proposition 1.13])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \notin \mathcal{T}_0$ be a prime. Let $C_{\mathrm{ns}}(p)$ be the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of all matrices of the form $\begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}$ with $(a,b) \in \mathbb{F}_p^2 \setminus \{(0,0)\}$ and ϵ a fixed element of $\mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$. Then H_p is conjugate to one of the following:*

(i) $\mathrm{GL}_2(\mathbb{F}_p)$*;*

(ii) *the normaliser $N_{\mathrm{ns}}(p)$ of $C_{\mathrm{ns}}(p)$;*

(iii) *the index 3 subgroup*

$$D(p) := \left\{a^3 \mid a \in C_{\mathrm{ns}}(p)\right\} \cup \left\{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot a^3 \mid a \in C_{\mathrm{ns}}(p)\right\}$$

of $N_{\mathrm{ns}}(p)$.

Moreover, the last case can only occur if $p \equiv 2 \pmod 3$.

Corollary 3.16. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \notin \mathcal{T}_0$ be a prime. The following hold:*

(1) *The image H_p of the modulo-p representation attached to E contains*

$$\{\lambda \,\mathrm{Id} \mid \lambda \in \mathbb{F}_p^\times\}.$$

(2) *Suppose $H_p \neq \mathrm{GL}_2(\mathbb{F}_p)$ and let $g_p \in \mathrm{GL}_2(\mathbb{F}_p)$ be an element that normalises H_p. Then there is $h \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $h^{-1}g_p h \in N_{\mathrm{ns}}(p)$ and $h^{-1}H_p h \subseteq N_{\mathrm{ns}}(p)$.*

Proof. (1) We apply Theorem 3.15. If H_p is either $\mathrm{GL}_2(\mathbb{F}_p)$ or conjugate to $N_{\mathrm{ns}}(p)$, the conclusion follows trivially, since $C_{\mathrm{ns}}(p)$ contains all scalars. In case (iii) of Theorem 3.15, H_p contains the cubes of the scalars, hence all scalars since $p \equiv 2 \pmod 3$.

(2) We only have to consider cases (ii) and (iii) of Theorem 3.15. Up to conjugation, we may assume that $H_p \subseteq N_{\mathrm{ns}}(p)$ and the claim becomes $g_p \in N_{\mathrm{ns}}(p)$.

In case (ii) it suffices to check that the normaliser of $N_{\mathrm{ns}}(p)$ is $N_{\mathrm{ns}}(p)$ itself. This holds because $C_{\mathrm{ns}}(p)$, being the only cyclic subgroup of index 2 of $N_{\mathrm{ns}}(p)$, is characteristic in $N_{\mathrm{ns}}(p)$; hence any element that normalises $N_{\mathrm{ns}}(p)$ normalises $C_{\mathrm{ns}}(p)$ as well, so it must be in $N_{\mathrm{ns}}(p)$. In case (iii), one similarly sees that $\{a^3 \mid a \in C_{\mathrm{ns}}(p)\}$ is characteristic in $D(p)$ and that its normaliser is $N_{\mathrm{ns}}(p)$, and the conclusion follows as above.

□

Lemma 3.17. *Let ℓ be a prime number and let H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Denote by H_ℓ the reduction of H modulo ℓ and suppose that H_ℓ contains a scalar matrix $\overline{\lambda}\,\mathrm{Id}$. Then H contains a scalar matrix $\lambda\,\mathrm{Id}$ for some $\lambda \in \mathbb{Z}_\ell^\times$ with $\lambda \equiv \overline{\lambda} \pmod{\ell}$.*

Proof. Let $h \in H$ be any element that is congruent modulo ℓ to $\overline{\lambda}\,\mathrm{Id}$. Let $\lambda \in \mathbb{Z}_\ell^\times$ be the Teichmüller lift of $\overline{\lambda}$ (that is, $\lambda^\ell = \lambda$ and $\lambda \equiv \overline{\lambda} \pmod{\ell}$) and write $h = \lambda h_1$, where $h_1 = \mathrm{Id} + \ell A$ for some $A \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$. The sequence $h^{\ell^n} = \lambda^{\ell^n} h_1^{\ell^n} = \lambda h_1^{\ell^n}$ converges to $\lambda\,\mathrm{Id}$, because for every n we have $h_1^{\ell^n} = (\mathrm{Id} + \ell A)^{\ell^n} \equiv \mathrm{Id} \pmod{\ell^n}$. As H is closed, the limit of this sequence, namely $\lambda\,\mathrm{Id}$, also belongs to H as claimed. □

We conclude this section with a group-theoretic lemma. Recall from Section 2 that we say that a finite simple group S occurs in G if S is isomorphic to a quotient of a subgroup of G.

Lemma 3.18 (Serre, [Ser97, IV-25])**.** *Let p be a prime and let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Let S be a non-abelian simple group that occurs in H. Then S is isomorphic either to A_5 or to $\mathrm{PSL}_2(\mathbb{F}_p)$; the latter case is only possible if H contains $\mathrm{SL}_2(\mathbb{F}_p)$.*

4 The ℓ-adic failure

The aim of this section is to study the ℓ-adic failure $A_\ell(N)$ for a fixed prime ℓ. The divisibility properties of α in the group $E(K)$ play a crucial role in the study of this quantity, so we begin with the following definition:

Definition 4.1. Let $\alpha \in E(K)$ and let n be a positive integer. We say that α is *n-indivisible over K* if there is no $\beta \in E(K)$ such that $n\beta = \alpha$; otherwise we say that α is *n-divisible* or *divisible by n over K*. Let ℓ be a prime number. We say that α is *strongly ℓ-indivisible over K* if the point $\alpha + T$ is ℓ-indivisible over K for every torsion point $T \in E(K)$ of ℓ-power order. Finally, we say that α is *strongly indivisible over K* if its image in the free abelian group $E(K)/E(K)_{\mathrm{tors}}$ is not divisible by any $n > 1$, or equivalently if α is strongly ℓ-indivisible over K for every prime ℓ.

Our aim is to give an analogue of the following result, which bounds the index of the image of the Kummer representation, in those cases when the torsion representation is not surjective.

Theorem 4.2 (Jones-Rouse, [JR10, Theorem 5.2])**.** *Assume that the ℓ-adic torsion representation $\tau_{\ell^\infty} : \mathrm{Gal}(K_{\ell^\infty} \mid K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective. Assume that α is ℓ-indivisible in $E(K)$ and, if $\ell = 2$, assume that $K_{2,2} \not\subseteq K_4$. Then the ℓ-adic Kummer representation $\kappa_{\ell^\infty} : \mathrm{Gal}(K_{\ell^\infty, \ell^\infty} \mid K_{\ell^\infty}) \to \mathbb{Z}_\ell^2$ is surjective.*

4.1 An exact sequence

We shall need to understand the divisibility properties of α not only over the base field K, but also over the division fields of E. Thus we turn to studying how the divisibility of the point α by powers of ℓ changes when passing to a field extension. Our main tool will be the following Lemma.

Lemma 4.3. *Let L be a finite Galois extension of K with Galois group G. For every $m \geqslant 1$ there is an exact sequence of abelian groups*

$$0 \to mE(K) \to E(K) \cap mE(L) \to H^1(G, E[m](L)),$$

where the injective map on the left is the natural inclusion.

Proof. Consider the short exact sequence of G-modules

$$0 \to E[m](L) \to E(L) \xrightarrow{[m]} mE(L) \to 0$$

and the beginning of the long exact sequence in cohomology,

$$0 \to (E[m](L))^G \to (E(L))^G \to (mE(L))^G \to H^1(G, E[m](L)).$$

Noticing that

$$(E[m](L))^G = E[m](K), \quad (E(L))^G = E(K), \quad (mE(L))^G = E(K) \cap mE(L)$$

and that

$$E(K)/E[m](K) \cong mE(K)$$

the lemma follows. □

The quotient $(E(K) \cap mE(L))/mE(K)$ gives a measure of "how many" K-points of E are m-divisible in $E(L)$ but not m-divisible in $E(K)$. We shall often use this Lemma in the special case of $m = \ell^n$ being a power of ℓ: in this context, the quotient $(E(K) \cap \ell^n E(L))/\ell^n E(K)$ is a subgroup of $E(K)/\ell^n E(K)$, so its exponent divides ℓ^n. We conclude that if $\ell \nmid \#H^1(G, E[\ell^n](L))$ then no ℓ-indivisible K-point of E can become ℓ-divisible in $E(L)$. This applies in particular when $\ell \nmid \#G$, see [NSW13, Proposition 1.6.2].

4.2 Divisibility in the ℓ-torsion field

As an example, we investigate the situation of Lemma 4.3 with $m = \ell$ and $L = K_\ell$. In this case the exact sequence becomes

$$0 \to \ell E(K) \to E(K) \cap \ell E(K_\ell) \to H^1(H_\ell, E[\ell]).$$

The following Lemma can also be found in [LW15, Section 3].

Lemma 4.4. *The cohomology group $H^1(H_\ell, E[\ell])$ is either trivial or cyclic of order ℓ. When $\ell = 2$ it is always trivial.*

Proof. Since $\ell E[\ell] = 0$, we have $\ell H^1(H_\ell, E[\ell]) = 0$. It follows from [Ser13, Theorem IX.4] that we have an injective map $H^1(H_\ell, E[\ell]) \to H^1(S_\ell, E[\ell])$, where S_ℓ is an ℓ-Sylow subgroup of H_ℓ. This is either trivial, in which case $H^1(H_\ell, E[\ell]) = 0$, or cyclic of order ℓ. In the latter case, up to a change of basis for $E[\ell]$ we can assume that S_ℓ is generated by $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. One can conclude the proof by explicitly computing the cohomology of the cyclic group $\langle\sigma\rangle$ as in [LW15, Lemma 7]. □

In [LW15] the authors classify the cases when $H^1(H_\ell, E[\ell]) \neq 0$ for $K = \mathbb{Q}$ and they give rather complete results in case K is a number field with $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$. In particular, it turns out that, for $K = \mathbb{Q}$, the group $H^1(H_\ell, E[\ell])$ can be non-trivial only when $\ell = 3, 5, 11$, and only when additional conditions are satisfied (see [LW15, Theorem 1]).

The next Example shows that for $K = \mathbb{Q}$ a point in $E(\mathbb{Q})$ that is strongly 3-indivisible may become 3-divisible over the 3-torsion field.

Example 4.5. Consider the elliptic curve E over $\mathbb{Q}$ given by the equation

$$y^2 + y = x^3 - 216x - 1861$$

with Cremona label 17739g1 (see [LMF22, label 17739g1]). We have $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, with a generator of the free part given by $P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right)$, which is therefore a strongly 3-indivisible point. Since the $\mathbb{Q}$-isogeny class of E consists of exactly two curves, by [LW15, Theorem 1] we have $H^1(H_3, E[3]) = \mathbb{Z}/3\mathbb{Z}$. The 3-torsion field is given by $\mathbb{Q}(z)$, where z is any root of $x^6 + 3$. Over this field the point

$$Q = \left(\frac{803}{400}z^4 - \frac{416}{400}z^2 + \frac{507}{400}, \frac{89133}{8000}z^4 - \frac{199071}{8000}z^2 - \frac{95323}{8000}\right) \in E(\mathbb{Q}(z))$$

is such that $3Q = P$.

A computer search performed with the help of the LMFDB [LMF22] and of Pari/GP [The19] shows that there are only 20 elliptic curves with conductor less than 4×10^5 satisfying this property for $\ell = 3$, none of which has conductor less than 17739.

4.3 Divisibility in the ℓ-adic torsion tower

As we have seen in the previous Section, the ℓ-divisibility of a point can increase when we move along the ℓ-adic torsion field tower. We would now like to give a bound on the extent of this phenomenon.

Our purpose in this section is to prove Proposition 4.10 (essentially an application of Sah's lemma, see [Sah68, Proposition 2.7(b)] and [BR03, Lemma A.2]), which will allow us to give such a bound in terms of the image of the torsion representation.

Lemma 4.6. *Let L be a finite Galois extension of K containing K_{ℓ^n} and let $G := \mathrm{Gal}(L|K)$. Assume that $\ell^k H^1(G, E[\ell^n]) = 0$. If $\alpha \in E(K)$ is strongly ℓ-indivisible in $E(K)$, then α is not ℓ^{k+1}-divisible in $E(L)$.*

Proof. Applying Lemma 4.3 with $M = \ell^{k+1}$ we see that the quotient

$$\frac{E(K) \cap \ell^{k+1} E(L)}{\ell^{k+1} E(K)}$$

embeds in $H^1(G, E[\ell^n])$, so it is killed by ℓ^k. It follows that $\ell^k \left(E(K) \cap \ell^{k+1} E(L)\right)$ is contained in $\ell^{k+1} E(K)$. Assuming by contradiction that $\alpha \in \ell^{k+1} E(L)$ we get $\ell^k \alpha = \ell^{k+1} \beta$ for some $\beta \in E(K)$. But then $T = \ell\beta - \alpha \in E[\ell^k](K)$ is such that $\alpha + T \in \ell E(K)$, contradicting our assumption that α is strongly ℓ-indivisible. □

Lemma 4.7. *Assume that for some $n_0 \geqslant 1$ we have $(1+\ell^{n_0})\,\mathrm{Id} \in H_{\ell^n}$ (if $n \leqslant n_0$ the condition is automatically satisfied). Then the exponent of $H^1(H_{\ell^n}, E[\ell^k])$ divides ℓ^{n_0} for every $k \leqslant n$.*

Proof. Let $\lambda = (1 + \ell^{n_0})\,\mathrm{Id}$ and let $\varphi : H_{\ell^n} \to E[\ell^k]$ be a cocycle. Using that λ is central in H_{ℓ^n} and that φ is a cocycle, for any $g \in H_{\ell^n}$ we have

$$g\varphi(\lambda) + \varphi(g) = \varphi(g\lambda) = \varphi(\lambda g) = \lambda\varphi(g) + \varphi(\lambda),$$

so

$$\ell^{n_0}\varphi(g) = (\lambda - 1)\varphi(g) = g\varphi(\lambda) - \varphi(\lambda),$$

that is, $\ell^{n_0}\varphi$ is a coboundary. This proves that $\ell^{n_0} H^1(H_{\ell^n}, E[\ell^k]) = 0$ as claimed. □

Lemma 4.8. *Assume that E does not have complex multiplication and let $n_\ell \geqslant 1$ be a parameter of maximal growth for the ℓ-adic torsion representation. Then for every $n \geqslant n_\ell$ and for every $g \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$ we have that $(\mathrm{Id} + \ell^{n_\ell} g) \bmod \ell^n$ is an element of H_{ℓ^n}.*

Proof. We prove this by induction. For $n = n_\ell$ the statement is trivial, so suppose $(\mathrm{Id} + \ell^{n_\ell} g) \bmod \ell^n$ belongs to H_{ℓ^n} for some $n > n_\ell$. Since the map $H_{\ell^{n+1}} \to H_{\ell^n}$ is surjective we can lift this element to an element of the form $\mathrm{Id} + \ell^{n_\ell} g + \ell^n g' \in H_{\ell^{n+1}}$, where $g' \in \mathrm{Mat}_2(\mathbb{F}_\ell)$. Since

$$\ker(H_{\ell^{n+1}} \to H_{\ell^n}) = \{\mathrm{Id} + \ell^n h \mid h \in \mathrm{Mat}_2(\mathbb{F}_\ell)\}$$

we have that $\mathrm{Id} - \ell^n g'$ is in $H_{\ell^{n+1}}$, hence $H_{\ell^{n+1}}$ contains the product

$$(\mathrm{Id} - \ell^n g')(\mathrm{Id} + \ell^{n_\ell} g + \ell^n g') \equiv (\mathrm{Id} + \ell^{n_\ell} g) \pmod{\ell^{n+1}},$$

where we use the fact that $\ell^{2n}(g')^2 = \ell^{n+n_\ell} g' g = 0$ since we are working modulo ℓ^{n+1}. □

In the special case $g = \mathrm{Id}$, the same result also holds for elliptic curves with complex multiplication:

Lemma 4.9. *Let E be an arbitrary elliptic curve and let $n_\ell \geqslant 1$ be a parameter of maximal growth for E (in particular, $n_\ell \geqslant 2$ if $\ell = 2$). Then for every $n \geqslant n_\ell$ we have $(1 + \ell^{n_\ell})\,\mathrm{Id} \in H_{\ell^n}$.*

Proof. In the light of the previous lemma we may assume that E has complex multiplication, so that the image of the torsion representation is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The equality $\# H_{\ell^{n+1}} = \ell^2 \# H_{\ell^n}$ for $n \geqslant n_\ell$ is equivalent to

$$\ker\left(H_{\ell^{n+1}} \to H_{\ell^n}\right) = \mathrm{Id} + \ell^n \mathbb{T},$$

where both sides are seen as subsets of $\{M \in \mathrm{Mat}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) : M \equiv \mathrm{Id} \pmod{\ell^n}\}$, and $\mathbb{T}$ is the tangent space to the image of the Galois representation as introduced in [LP21, Definition 9] and further studied in [LP17, Definition 18]. We proceed by induction, the base case $n = n_\ell$ being trivial. By surjectivity of $H_{\ell^{n+1}} \to H_{\ell^n}$ and the inductive hypothesis, we know that $H_{\ell^{n+1}}$ contains an element reducing to $(1+\ell^{n_\ell})\,\mathrm{Id}$ modulo ℓ^n, that is, an element of the form $M_{n+1} := (1+\ell^{n_\ell})\,\mathrm{Id} + \ell^n t$. Here t is an element of $\mathbb{T}$: to see this, notice that M_{n+1} is congruent to the identity modulo ℓ^{n_ℓ}, so it cannot lie in the non-trivial coset of the normaliser of a Cartan subgroup ([LP17, Theorem 40]), and therefore belongs to the Cartan subgroup itself. But then M_{n+1} is of the form $\begin{pmatrix} x & \delta y \\ y & x + \gamma y \end{pmatrix}$ for appropriate parameters (γ, δ), hence

$$t = \frac{1}{\ell^n} \begin{pmatrix} x - 1 - \ell^{n_\ell} & \delta y \\ y & (x - 1 - \ell^{n_\ell}) + \gamma y \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{F}_\ell)$$

belongs to $\mathbb{T}$ by the explicit description given in [LP17, Definition 18]. The equality $\ker\left(H_{\ell^{n+1}} \to H_{\ell^n}\right) = \mathrm{Id} + \ell^n \mathbb{T}$ implies that $H_{\ell^{n+1}}$ also contains $\mathrm{Id} - \ell^n t$, so it contains

$$\begin{aligned}((1 + \ell^{n_\ell})\,\mathrm{Id} + \ell^n t)(\mathrm{Id} - \ell^n t) &\equiv \mathrm{Id} - \ell^{2n} t^2 + \ell^{n_\ell}\,\mathrm{Id} - \ell^{n+n_\ell} t \\ &\equiv (1 + \ell^{n_\ell})\,\mathrm{Id} \pmod{\ell^{n+1}}\end{aligned}$$

as claimed. □

Proposition 4.10. *Assume that α is strongly ℓ-indivisible in $E(K)$. Let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation. Then for every n the point α is not $\ell^{n_\ell+1}$-divisible in K_{ℓ^n}; equivalently, α is not $\ell^{n_\ell+1}$-divisible in K_{ℓ^∞}.*

Proof. By Lemma 4.9 the group H_{ℓ^n} contains $(1+\ell^{n_\ell})\,\mathrm{Id}$, so by Lemma 4.7 the exponent of the group $H^1(H_{\ell^n}, E[\ell^n])$ divides ℓ^{n_ℓ}. We conclude by Lemma 4.6. □

4.4 The ℓ-adic failure is bounded

In this section we establish some general results that will form the basis of all subsequent arguments (in particular Lemma 4.11 and Proposition 4.12) and use them to show that the ℓ-adic failure $A_\ell(N)$ can be effectively bounded (Theorem 4.17).

Lemma 4.11. *Assume that for some $d \geqslant 0$ the point $\alpha \in E(K)$ is not ℓ^{d+1}-divisible over K_{ℓ^∞}. Then V_{ℓ^∞} contains a vector of valuation at most d. Similarly, if $\alpha \in E(K)$ is not ℓ^{d+1}-divisible over K_∞ then W_{ℓ^∞} contains a vector of valuation at most d.*

Proof. Assume by contradiction that every element of V_{ℓ^∞} has valuation at least $d+1$. Then the image of V_{ℓ^∞} in $E[\ell^{d+1}] = T_\ell(E)/\ell^{d+1}T_\ell(E)$ is zero. As this image is exactly $\mathrm{Gal}(K_{\ell^\infty,\ell^{d+1}} \mid K_{\ell^\infty})$, we obtain $K_{\ell^\infty,\ell^{d+1}} = K_{\ell^\infty}$, so α is ℓ^{d+1}-divisible in K_{ℓ^∞}, a contradiction.

The second part can be proved in exactly the same way. □

The following group-theoretic Proposition will be applied in this section and in Section 7. In all of our applications the group H will be the image of the ℓ-adic torsion representation associated with some elliptic curve.

Proposition 4.12. *Let ℓ be a prime number, d be a positive integer, H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and $A = \mathbb{Z}_\ell[H]$ be the sub-$\mathbb{Z}_\ell$-algebra of $\mathrm{Mat}_2(\mathbb{Z}_\ell)$ topologically generated by the elements of H. Let $V \subseteq \mathbb{Z}_\ell^2$ be an A-submodule of $\mathbb{Z}_\ell^2$, and suppose that V contains at least one vector of ℓ-adic valuation at most d.*

(1) *Suppose that H contains $\{M \in \mathrm{Mat}_2(\mathbb{Z}_\ell) : M \equiv \mathrm{Id} \pmod{\ell^n}\}$ for some $n \geqslant 1$. Then V contains $\ell^{d+n}\mathbb{Z}_\ell^2$.*

(2) *Suppose that the reduction of H modulo ℓ acts irreducibly on $\mathbb{F}_\ell^2$. Then V contains $\ell^d\mathbb{Z}_\ell^2$.*

(3) *Let C be a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters (γ, δ) and let N be its normaliser. Suppose that H is an open subgroup of N not contained in C, and that H contains $\{M \in C : M \equiv \mathrm{Id} \pmod{\ell^n}\}$ for some $n \geqslant 1$. Then V contains $\ell^{3n+d+v_\ell(4\delta)}\mathbb{Z}_\ell^2$.*

Proof. Both the assumptions and the conclusions of the Proposition are invariant under changes of basis in $\mathbb{Z}_\ell^2$, so we may assume that $v = \ell^d e_1$ is in V, where $e_1 = \begin{pmatrix}1\\0\end{pmatrix}$.

(1) It is clear that A contains $\ell^n \operatorname{Mat}_2(\mathbb{Z}_\ell)$, so we have

$$V \supseteq A \cdot v \supseteq \ell^n \operatorname{Mat}_2(\mathbb{Z}_\ell) \cdot v = \ell^{n+d} \operatorname{Mat}_2(\mathbb{Z}_\ell) \cdot e_1 = \ell^{n+d}\mathbb{Z}_\ell^2.$$

(2) Let H_ℓ denote the reduction of H modulo ℓ. The condition that H_ℓ acts irreducibly on $\mathbb{F}_\ell^2$ implies that there exists $\overline{M} \in \mathbb{F}_\ell[H_\ell]$ such that $\overline{M}e_1 \equiv \begin{pmatrix}0\\1\end{pmatrix}$ (mod ℓ). Fix a lift $M \in A$ of $\overline{M}$, which exists because the natural reduction map $A = \mathbb{Z}_\ell[H] \to \mathbb{F}_\ell[H_\ell]$ is clearly surjective. Then $Mv = \ell^d M e_1$ is a vector whose second coordinate has valuation exactly d and whose first coordinate has valuation strictly larger than d. It is then immediate to see that v and Mv, that are contained in V, generate $\ell^d\mathbb{Z}_\ell^2$.

(3) It is enough to show that A contains $\ell^{3n+v_\ell(4\delta)} \operatorname{Mat}_2(\mathbb{Z}_\ell)$, and the conclusion follows as in (1) above. Suppose first that $\gamma = 0$, and let

$$M_0 = \begin{pmatrix}x_0 & -\delta y_0\\ y_0 & -x_0\end{pmatrix} \in H \setminus C \qquad \text{and} \qquad M_1 = \begin{pmatrix}1+\ell^n x_0 & \delta\ell^n y_0\\ \ell^n y_0 & 1+\ell^n x_0\end{pmatrix} \in H.$$

The existence and the form of such matrices follow from the assumptions and from the description of Cartan subgroups and their normaliser given in Definition 2.8 and Lemma 2.10. Then A contains $M_2 = M_1 - \mathrm{Id} + \ell^n M_0 = 2\ell^n \begin{pmatrix}x_0 & 0\\ y_0 & 0\end{pmatrix}$. Let moreover $M_3 = \ell^n \begin{pmatrix}0 & \delta\\ 1 & 0\end{pmatrix}$, which is in A since it can be written as $\begin{pmatrix}1 & \ell^n\delta\\ \ell^n & 1\end{pmatrix} - \mathrm{Id}$, where both matrices are in H by assumption. Then we have

$$4\ell^{2n}\begin{pmatrix}x_0^2 - \delta y_0^2 & 0\\ 0 & 0\end{pmatrix} = (M_2 - 2y_0 M_3)\cdot M_2 \in A$$

and $x_0^2 - \delta y_0^2 = -\det M_0 \in \mathbb{Z}_\ell^\times$. It follows that A contains $4\ell^{2n}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$, and since $\mathrm{Id} \in A$ we have that all diagonal matrices of valuation at least $2n+v_\ell(4)$ are in A, which therefore also contains

$$\begin{pmatrix}0 & 0\\ \ell^{3n+v_\ell(4)} & 0\end{pmatrix} = M_3\begin{pmatrix}\ell^{2n+v_\ell(4)} & 0\\ 0 & 0\end{pmatrix}$$

and

$$\begin{pmatrix} 0 & \ell^{3n+v_\ell(4)}\delta \\ 0 & 0 \end{pmatrix} = M_3 \begin{pmatrix} 0 & 0 \\ 0 & \ell^{2n+v_\ell(4)} \end{pmatrix}.$$

Together with the diagonal matrices found above, these elements clearly generate the submodule $\ell^{3n+v_\ell(4\delta)}\operatorname{Mat}_2(\mathbb{Z}_\ell)$, and we are done. If $\gamma \neq 0$, by Remark 2.9 we may assume $\gamma = 1$ and $\ell = 2$. In this case let

$$M_0 = \begin{pmatrix} x_0 + y_0 & \delta y_0 + x_0 + y_0 \\ -y_0 & -x_0 - y_0 \end{pmatrix} \in H \setminus C$$

and

$$M_1 = \mathrm{Id} + \ell^n \begin{pmatrix} x_0 & \delta y_0 \\ y_0 & x_0 + y_0 \end{pmatrix} \in H.$$

Then A contains $M_2 = M_1 - \mathrm{Id} + \ell^n M_0 = \ell^n \begin{pmatrix} 2x_0 + y_0 & 2\delta y_0 + x_0 + y_0 \\ 0 & 0 \end{pmatrix}$.

Let moreover $M_3 = \ell^n \begin{pmatrix} -1 & \delta \\ 1 & 0 \end{pmatrix} \in A$. Then we have

$$M_2(\delta M_2 - (2\delta y_0 + x_0 + y_0)M_3) = -\ell^{2n} \det(M_0)(1 + 4\delta) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A,$$

and using the fact that $\det(M_0) \in \mathbb{Z}_\ell^\times$ (since $M_0 \in H \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$) we obtain that A contains all diagonal matrices of valuation at least $2n$. We can then conclude as before.

□

Proposition 4.13. *Assume that α is strongly ℓ-indivisible in $E(K)$ and let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation.*

(1) *Assume that E does not have complex multiplication. Then for every $k \geqslant 1$ we have $E[\ell^k] \subseteq V_{\ell^{k+2n_\ell}}$.*

(2) *Assume that E has complex multiplication by $\mathcal{A} := \mathrm{End}_{\overline{K}}(E)$, and that K does not contain the imaginary quadratic field $\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. Let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$. Then for all $k \geqslant 1$ we have $E[\ell^k] \subseteq V_{\ell^{k+4n_\ell+v_\ell(4\delta)}}$.*

Proof. By Remark 2.6, in order to show (1) it is enough to prove that $\ell^{2n_\ell}T_\ell(E)$ is contained in V_{ℓ^∞}. To see that this holds, notice that by Lemma 4.11 and Proposition 4.10 there is an element of valuation at most n_ℓ in V_{ℓ^∞}. Now we just need to apply Proposition 4.12(1) with $H = H_{\ell^\infty}$, $V = V_{\ell^\infty}$ and $d = n = n_\ell$. Part (2) can be proved in the same way using Proposition 4.12(3). □

Proposition 4.13 is the main ingredient for the proof of Theorem 4.17 below, and in fact it implies it directly in case the point α is strongly indivisible. To finish the proof one also needs to relate the degrees of the Kummer extensions for divisible and indivisible points, which is accomplished in Lemma 4.16.

In §6 we will show that a naïve analogue of Proposition 4.13 does not hold in case E has complex multiplication defined over K.

Remark 4.14. Write $\alpha = \ell^d\beta + T_h$, where $\beta \in E(K)$ is strongly ℓ-indivisible and $T_h \in E[\ell^h](K)$ is a point of order ℓ^h, for some $h, d \geqslant 0$. Notice that it is always possible to do so: first, let $\beta \in E(K)$ and d be such that $\alpha = \ell^d\beta + T$ for some $T \in E(K)$ of order a power of ℓ, with d maximal. Assume then by contradiction that β is not strongly ℓ-indivisible. This means that there are $\gamma, S \in E(K)$ with S of order a power of ℓ such that $\beta = \ell\gamma + S$. But then $\alpha = \ell^d(\ell\gamma + S) + T = \ell^{d+1}\gamma + (\ell^d S + T)$, contradicting the maximality of d.

Remark 4.15. Let $\widehat{h}$ be the canonical (Néron-Tate) height on E, as described in [Sil09, Section VIII.9]. Following [Pet06], it is possible to bound the divisibility parameters d and h in terms of $\widehat{h}(\alpha)$, the degree of K over $\mathbb{Q}$, the discriminant Δ_E of E over K and the Szpiro ratio

$$\sigma = \begin{cases} 1 & \text{if } E \text{ has everywhere good reduction} \\ \frac{\log|N_{K/\mathbb{Q}}(\Delta_E)|}{\log|N_{K/\mathbb{Q}}(N_E)|} & \text{otherwise} \end{cases}$$

where N_E denotes the conductor of E over K. In fact, [Pet06, Theorem 1] gives the bound

$$h \leqslant \log_\ell \left\lfloor c_1[K:\mathbb{Q}]\sigma^2 \log\left(c_2[K:\mathbb{Q}]\sigma^2\right)\right\rfloor$$

where $c_1 = 134861$ and $c_2 = 104613$. Alternatively, one could also use the uniform boundedness of torsion [Mer96, Par96] to give an upper bound on h that only depends on $[K:\mathbb{Q}]$.

For the parameter d we can reason as follows. For $\alpha = \ell^d\beta + T_h$, by [Sil09, Theorem 9.3] we have

$$\widehat{h}(\alpha) = \widehat{h}(\ell^d\beta + T_h) = \widehat{h}(\ell^d\beta) = \ell^{2d}\widehat{h}(\beta)$$

so we get $d \leqslant \dfrac{1}{2\log\ell}\log\left(\dfrac{\widehat{h}(\alpha)}{\widehat{h}(\beta)}\right)$. Now in view of [Pet06, Theorem 2] for any non-torsion point $\beta \in E(K)$ we have

$$\widehat{h}(\beta) \geqslant B := \frac{\log|N_{K/\mathbb{Q}}(\Delta_E)|}{10^{15}[K:\mathbb{Q}]^3\sigma^6\log^2(c_2[K:\mathbb{Q}]\sigma^2)},$$

where again $c_2 = 104613$. We thus obtain the effective bound

$$d \leqslant \frac{1}{2\log \ell} \log\left(\frac{\widehat{h}(\alpha)}{B}\right).$$

Lemma 4.16. *Let $\alpha, \beta \in E(K)$ be points of infinite order such that $\alpha = d\beta + T_h$ for positive integers d, h and some $T_h \in E(K)[h]$. If $N \geqslant 1$ is a multiple of d then*

$$\left[K_{Nh}\left(\left(\frac{N}{d}\right)^{-1}\beta\right) : K_{Nh}\right] \qquad \textit{divides} \qquad \left[K_N\left(N^{-1}\alpha\right) : K_N\right],$$

thus

$$\frac{N^2}{\left[K_N\left(N^{-1}\alpha\right) : K_N\right]} \qquad \textit{divides} \qquad d^2 \cdot \frac{\left(\frac{N}{d}\right)^2}{\left[K_{Nh}\left(\left(\frac{N}{d}\right)^{-1}\beta\right) : K_{Nh}\right]}.$$

Proof. Notice that

$$K_{Nh}\left(\left(\frac{N}{d}\right)^{-1}\beta\right) = K_{Nh}\left(N^{-1}(d\beta)\right) K_{Nh}\left(N^{-1}(d\beta + T_h)\right) = K_{Nh}\left(N^{-1}\alpha\right)$$

and thus

$$\left[K_{Nh}\left(\left(\frac{N}{d}\right)^{-1}\beta\right) : K_{Nh}\right] = \left[K_{Nh}(N^{-1}\alpha) : K_{Nh}\right].$$

It is clear that $\left[K_{Nh}(N^{-1}\alpha) : K_{Nh}\right]$ divides $\left[K_N(N^{-1}\alpha) : K_N\right]$, so we conclude. □

Theorem 4.17. *Let ℓ be a prime and assume that $\mathrm{End}_K(E) = \mathbb{Z}$ (i.e. either E does not have CM, or it has CM but the complex multiplication is not defined over K). There is an effectively computable constant a_ℓ, depending only on α and on the ℓ-adic torsion representation associated to E, such that $A_\ell(N)$ divides ℓ^{a_ℓ} for all positive integers N.*

Moreover, a_ℓ is zero for every odd prime ℓ such that α is ℓ-indivisible and for which the ℓ-adic torsion representation associated with E is maximal (see Definition 3.2). For the finitely many remaining primes ℓ we can take a_ℓ as follows: let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation and let d be as in Remark 4.14. If E has CM over $\overline{K}$, let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathrm{End}_{\overline{K}}(E)$. Then:

(1) *$a_\ell = 4n_\ell + 2d$ if E does not have CM over $\overline{K}$;*

(2) $a_\ell = 8n_\ell + 2v_\ell(4\delta) + 2d$ *if* E *has CM over* $\overline{K}$.

Proof. Let $\alpha = \ell^d\beta + T_h$ as described above. Notice that if α is strongly ℓ-indivisible we have $d = 0$, and the conclusion follows from Proposition 4.13. If the ℓ-adic torsion representation is maximal, the fact that a_ℓ is zero in the cases stated follows from [JR10, Theorem 5.2 and Theorem 5.8].

In the general case, let $n = v_\ell(N)$ and notice that the claim is trivial for $n \leqslant d$, so we may assume $n > d$. By Lemma 4.16, we have that

$$\frac{\ell^{2n}}{[K_{\ell^{n+h}}(\ell^{-n}\alpha) : K_{\ell^{n+h}}]} \quad \text{divides} \quad \ell^{2d}\frac{\ell^{2(n-d)}}{[K_{\ell^{n+h}}(\ell^{-(n-d)}\beta) : K_{\ell^{n+h}}]},$$

so in view of Remark 2.1 we are reduced to proving the statement for β instead of α. Since β is strongly ℓ-indivisible, we can conclude as stated at the beginning of the proof.

The fact that a_ℓ is effective follows from the fact that one can effectively compute a parameter of maximal growth for the ℓ-adic torsion representation (Remark 3.8), an upper bound for the value of d (Remark 4.15), and the ring $\mathrm{End}_{\overline{K}}(E)$ ([Ach05], [CMSV19], [Lom19]). □

Remark 4.18. Recent results by Cerchia and Rouse [CR21], obtained independently from those in the present paper, imply that the better bound $a_\ell = 3n_\ell + 2d$ holds in the non-CM case.

5 The adelic failure

In this section we study the adelic failure $B_\ell(N)$, that is, the degree of the intersection $K_{\ell^n,\ell^n} \cap K_N$ over K_{ℓ^n}. Notice that this intersection is a finite Galois extension of K_{ℓ^n}.

5.1 Intersection of torsion fields in the non-CM case

We first aim to establish certain properties of the intersections of different torsion fields of E, assuming for this subsection that E does not have complex multiplication over $\overline{K}$. Our main tool is the following result, due to Campagna and Stevenhagen [CS19, Theorem 3.4]:

Theorem 5.1 (Campagna-Stevenhagen)**.** *Assume that E does not have complex multiplication. Let S be the set consisting of the primes ℓ satisfying one or more of the following three conditions:*

(i) $\ell \mid 30\,\mathrm{disc}(K \mid \mathbb{Q})$;

(ii) *E has bad reduction at some prime of K above ℓ;*

(iii) *the modulo ℓ torsion representation is not surjective.*

For every $\ell \notin S$ we have $K_{\ell^n} \cap K_M = K$ for all $M, n \geqslant 1$ with $\ell \nmid M$.

Remark 5.2. The finite set S appearing in Theorem 5.1 can be computed explicitly. In fact, it is well known that one can compute the discriminant of K and the set of primes of bad reduction of E. An algorithm to compute the set of primes for which the mod ℓ representation is not surjective is described in [Zyw15b].

An immediate consequence of the Theorem above is the following corollary, which gives a slightly more precise version of [Ser97, §3.4, Lemma 6].

Corollary 5.3. *Assume that E does not have complex multiplication and let S be as in Theorem 5.1. Let M be a positive integer and write $M = M_1 M_2$, where*

$$M_1 = \prod_{p \notin S} p^{e_p} \qquad p \text{ prime, } e_p \geqslant 0,$$
$$M_2 = \prod_{q \in S} q^{e_q} \qquad q \text{ prime, } e_q \geqslant 0.$$

Then we have

$$\mathrm{Gal}(K_M \mid K) \cong \mathrm{GL}_2\left(\mathbb{Z}/M_1\mathbb{Z}\right) \times \mathrm{Gal}\left(K_{M_2} \mid K\right).$$

Remark 5.4. Let $\tilde{K}$ be the compositum of the fields K_p for all $p \in S$, where S is as in Theorem 5.1. In the following section it will be important to notice that S is stable under base change to $\tilde{K}$. More precisely, let $\tilde{S}$ be the set of all primes ℓ that satisfy one of the following:

(i') $\ell \mid 30 \operatorname{disc}(\tilde{K} \mid \mathbb{Q})$;

(ii') E has bad reduction at some prime of $\tilde{K}$ above ℓ;

(iii') the modulo ℓ torsion representation attached to $E/\tilde{K}$ is not surjective.

Then $\tilde{S} = S$.

Indeed, the inclusion $\tilde{S} \supseteq S$ is easy to see: clearly conditions (i) and (iii) imply (i') and (iii') respectively, so we only need to discuss (ii). Let $\mathfrak{p}$ be a prime of K (of characteristic ℓ) at which E has bad reduction, and let $\mathfrak{q}$ be a prime of $\tilde{K}$ lying over $\mathfrak{p}$. We need to show that $\ell \in \tilde{S}$. If E has bad reduction at $\mathfrak{q}$ we have $\ell \in \tilde{S}$ by (ii'), while if E has good reduction at $\mathfrak{q}$ then $\mathfrak{p}$ ramifies in $\tilde{K}$ by [Sil09, Proposition VII.5.4 (a)], so we have $\ell \mid \operatorname{disc}(\tilde{K} \mid \mathbb{Q})$ and ℓ is in $\tilde{S}$ by (i').

Conversely, let $\ell \in \tilde{S}$. If (ii') holds, then clearly also (ii) holds, and ℓ is in S. Suppose that (i') holds. If ℓ divides 30, then it is in S by (1). Otherwise ℓ divides $\mathrm{disc}(\tilde{K} \mid \mathbb{Q})$, which by [Ser13, III.§4, Proposition 8] is equal to $\mathrm{disc}(K \mid \mathbb{Q})^{[\tilde{K}:K]} N_{K/\mathbb{Q}} \mathrm{disc}(\tilde{K} \mid K)$; if ℓ divides $\mathrm{disc}(K \mid \mathbb{Q})$, then it is in S by (1), while if it divides $\mathrm{disc}(\tilde{K} \mid K)$ then we have $\ell \in S$ by [Sil09, Proposition VIII.1.5(b)]. We may therefore assume that (i') and (ii') do not hold. Since ℓ is in $\tilde{S}$, (iii') must hold, that is, the modulo-ℓ torsion representation attached to $E/\tilde{K}$ is not surjective. We claim that the same is true for E/K. Indeed, if ℓ is in S this is true by definition, while if $\ell \notin S$ the previous corollary shows that K_ℓ is linearly disjoint from $\tilde{K}$, so the images of the modulo-ℓ representations over K and over $\tilde{K}$ coincide.

5.2 The adelic failure is bounded

We now go back to the general case of E possibly admitting complex multiplication.

Fix an integer $N > 1$ and a prime number ℓ dividing N. Write $N = \ell^n R$ with $\ell \nmid R$ and recall that the adelic failure $B_\ell(N)$ is defined to be the degree $[K_{\ell^n,\ell^n} \cap K_N : K_{\ell^n}]$. In this section we study this failure for $N = \ell^n R$, starting with a simple Lemma in Galois theory.

Lemma 5.5. *Let L_1, L_2 and L_3 be field extensions of K, with $L_1 \subseteq L_2$ and L_2 Galois over K. Then the compositum $L_1(L_2 \cap L_3)$ is equal to the intersection $L_2 \cap (L_1 L_3)$.*

Proof. Let $G = \mathrm{Gal}(\overline{K} \mid K)$ and, for $i = 1, 2, 3$, let $G_i := \mathrm{Gal}(\overline{K} \mid L_i)$. The claim is equivalent to $G_1 \cap \langle G_2, G_3 \rangle = \langle G_2, G_1 \cap G_3 \rangle$, where the inclusion "$\supseteq$" is obvious. Since $L_2 \mid K$ is Galois, the Galois group G_2 is normal in G, so we have $\langle G_2, G_3 \rangle = G_2 \cdot G_3$ and $\langle G_2, G_1 \cap G_3 \rangle = G_2 \cdot (G_1 \cap G_3)$. Let then $g \in G_1 \cap (G_2 \cdot G_3)$, so that there are $g_1 \in G_1$, $g_2 \in G_2$ and $g_3 \in G_3$ such that $g = g_1 = g_2 g_3$. But then $g_2^{-1} g_1 = g_3 \in G_3$ and, since $G_2 \subseteq G_1$, also $g_2^{-1} g_1 \in G_1$, so that $g = g_2(g_2^{-1} g_1) \in G_2 \cdot (G_1 \cap G_3)$. □

We now establish some properties of certain subfields of $K_{\ell^n R, \ell^n}$.

Lemma 5.6. *Setting $L := K_{\ell^n,\ell^n} \cap K_N$, $F := L \cap K_R = K_{\ell^n,\ell^n} \cap K_R$, and $T := F \cap K_{\ell^n} = K_{\ell^n} \cap K_R$ we have:*

(1) *The compositum $F K_{\ell^n}$ is L.*

(2) $\mathrm{Gal}(F \mid T) \cong \mathrm{Gal}(L \mid K_{\ell^n})$*; in particular,* $\mathrm{Gal}(F \mid T)$ *is an abelian ℓ-group.*

(3) *F is the intersection of the maximal abelian extension of T contained in K_{ℓ^n,ℓ^n} and the maximal abelian extension of T contained in K_R.*

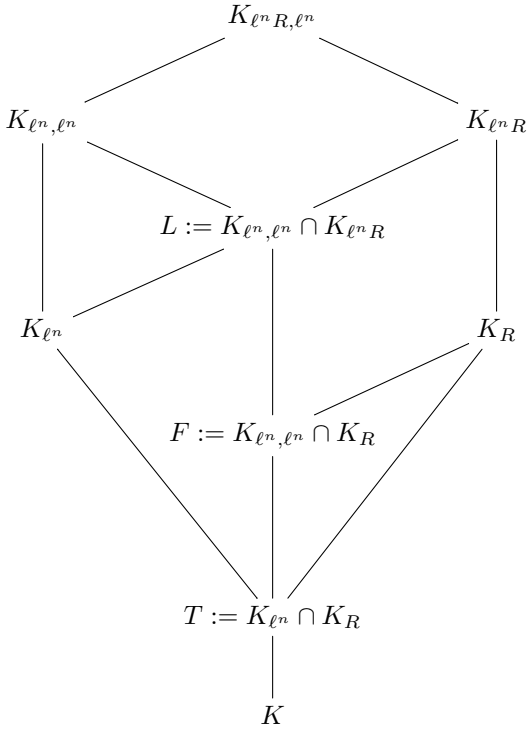


Figure 1.1: The situation described in Lemma 5.6 and Proposition 5.7.

Proof. (1) By Lemma 5.5 we have $FK_{\ell^n} = K_{\ell^n}(K_{\ell^n,\ell^n} \cap K_R) = K_{\ell^n,\ell^n} \cap K_{\ell^n R} = L$. Part (2) follows from (1) and standard Galois theory. For (3), notice that F is abelian over T by (2), so it must be contained in the maximal abelian extension of T contained in K_{ℓ^n,ℓ^n} and in the maximal abelian extension of T contained in K_R. On the other hand, F cannot be smaller than the intersection of these abelian extensions, because by definition it is the intersection of K_{ℓ^n,ℓ^n} and K_R. □

Proposition 5.7. *The adelic failure $B_\ell(N)$ is equal to $[F : T]$, where $F = K_{\ell^n,\ell^n} \cap K_R$ and $T = K_{\ell^n} \cap K_R$.*

Proof. Let as above $L = K_{\ell^n,\ell^n} \cap K_{\ell^n R}$. We have

$$\mathrm{Gal}(K_{\ell^n,\ell^n} \mid L) \cong \mathrm{Gal}(K_{\ell^n R,\ell^n} \mid K_{\ell^n R}),$$

so we get

$$[K_{\ell^n,\ell^n} : K_{\ell^n}] = [K_{\ell^n,\ell^n} : L][L : K_{\ell^n}] = [K_{\ell^n R,\ell^n} : K_{\ell^n R}][L : K_{\ell^n}]$$

and we conclude by Lemma 5.6(b). □

In what follows we will need to work over a certain extension $\tilde{K}$ of K; this extension will depend on the prime ℓ. More precisely, we give the following definition.

Definition 5.8. Let $\tilde{K}$ be the finite extension of K defined as follows:

(i) If E has complex multiplication, we take $\tilde{K}$ to be the compositum of K with the CM field of E. This is an at most quadratic extension of K. Notice that in this case by [LR18, Lemma 2.2] we have $\tilde{K}_n = K_n$ for every $n \geqslant 3$.

(ii) If E does not have CM and ℓ is not one of the primes in the set S of Theorem 5.1, we just let $\tilde{K} = K$. Notice that this happens for all but finitely many primes ℓ.

(iii) If E does not have CM and ℓ is one of the primes in the set S of Theorem 5.1, we let $\tilde{K}$ be the compositum of all the K_p for $p \in S$. Notice that in this case $\tilde{K}_\ell = \tilde{K}$.

We shall use the notation $\tilde{K}_M$ (respectively $\tilde{K}_{M,N}$) for the torsion (respectively Kummer) extensions of $\tilde{K}$. We shall also write

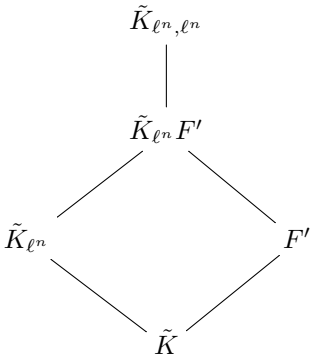
$$\tilde{H}_{\ell^n} := \mathrm{Im}\left(\tau_{\ell^n} : \mathrm{Gal}(\overline{K} \mid \tilde{K}) \to \mathrm{Aut}(E[\ell^n])\right) \cong \mathrm{Gal}\left(\tilde{K}_{\ell^n} \mid \tilde{K}\right),$$
$$\tilde{V}_{\ell^n} := \mathrm{Im}\left(\kappa_{\ell^n} : \mathrm{Gal}(\overline{K} \mid \tilde{K}_{\ell^n}) \to E[\ell^n]\right) \cong \mathrm{Gal}\left(\tilde{K}_{\ell^n,\ell^n} \mid \tilde{K}_{\ell^n}\right)$$

for the images of the ℓ^n-torsion representation and of the (ℓ^n, ℓ^n)-Kummer map attached to $E/\tilde{K}$. Finally, we let $\tilde{n}_\ell$ be the minimal parameter of maximal growth for the ℓ-adic torsion representation over $\tilde{K}$. Notice that, thanks to Lemma 3.10, we have $\tilde{n}_\ell \leqslant n_\ell + v_\ell([\tilde{K} : K])$.

Proposition 5.9. *The extension $F' := \tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_R$ is abelian over $\tilde{K}$.*

Proof. This is well known if E has complex multiplication because then $\tilde{K}_R$ is itself abelian over $\tilde{K}$, see for example [Sil94, Theorem II.2.3]. In case E does not have complex multiplication and ℓ is not in the set S of Theorem 5.1, this follows

easily by considering the diagram



In fact, since $\tilde{K}_{\ell^n} \cap F' = \tilde{K}$ by Theorem 5.1 (notice that in this case $\tilde{K} = K$), we have that $\mathrm{Gal}(F' \mid \tilde{K}) \cong \mathrm{Gal}(\tilde{K}_{\ell^n}F' \mid \tilde{K}_{\ell^n})$ is a quotient of $\tilde{V}_{\ell^n}$, hence abelian. Thus we can assume that E does not have CM and that ℓ is in the set S of Theorem 5.1.

Notice that F' is a Galois extension of $\tilde{K}$ with degree a power of ℓ, since the same is true for $\tilde{K}_{\ell^n,\ell^n} \mid \tilde{K}$ and $F' \subseteq \tilde{K}_{\ell^n,\ell^n}$. Letting r denote the radical of R, the degree of $[F' : F' \cap \tilde{K}_r]$, which is still a power of ℓ, divides $[\tilde{K}_R : \tilde{K}_r]$, which is a product of primes dividing R. So since $\ell \nmid R$ we obtain $[F' : F' \cap \tilde{K}_r] = 1$, that is $\tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_R = \tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_r$, and we may assume that R is squarefree. Write now $R = R_1R_2$, where R_1 is the product of the prime factors of R that are *not* in S and R_2 is the product of the prime factors of R that belong to S. By definition of $\tilde{K}$ we have $\tilde{K}_R = \tilde{K}_{R_1}$, so we may further assume that no prime $p \in S$ divides R. By Corollary 5.3 we then have $\mathrm{Gal}(\tilde{K}_R \mid \tilde{K}) \cong \mathrm{GL}_2(\mathbb{Z}/R\mathbb{Z})$.

Since $F' \subseteq \tilde{K}_R$, there must be a normal subgroup $D = \mathrm{Gal}(\tilde{K}_R \mid F') \trianglelefteq \mathrm{GL}_2(\mathbb{Z}/R\mathbb{Z})$ of index a power of ℓ. In order to conclude we just need to show that D contains the subgroup $\mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z})$, for then $\mathrm{Gal}(F' \mid \tilde{K}) \cong \mathrm{GL}_2(\mathbb{Z}/R\mathbb{Z})/D$ is abelian.

Write $\mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z}) \cong \prod_{p|R} \mathrm{SL}_2(\mathbb{F}_p)$ and consider the intersection $D_p := D \cap \mathrm{SL}_2(\mathbb{F}_p)$, which is a normal subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$. Here we identify $\mathrm{SL}_2(\mathbb{F}_p)$ with the corresponding direct factor of $\mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z})$. The quotient $\mathrm{SL}_2(\mathbb{F}_p)/D_p$ cannot have order a power of ℓ unless it is trivial (recall that in our case $p \geqslant 5$), so we deduce that $D \supseteq \mathrm{SL}_2(\mathbb{F}_p)$. As this is true for every $p \mid R$, we have $D \supseteq \mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z})$, and we are done. □

In what follows, whenever A is an abelian group and Q is a group acting on A, we denote by $[A, Q]$ the subgroup of A generated by elements of the form $gv - v$ for $v \in A$ and $g \in Q$. For example, we will consider the case $A = \tilde{V}_{\ell^n}$ and $Q = \tilde{H}_{\ell^n}$.

Lemma 5.10. *Let*

$$1 \to A \to G \to Q \to 1$$

be a short exact sequence of groups, with A abelian, so that Q acts naturally on A. Let G^{ab} and Q^{ab} be the maximal abelian quotients of G and Q respectively. Then $A/[A,Q]$ surjects onto $\ker(G^{\mathrm{ab}} \to Q^{\mathrm{ab}})$.

Proof. We have an injective map of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A \cap G' & \longrightarrow & G' & \longrightarrow & Q' & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \end{array}$$

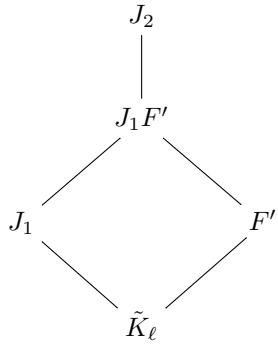
from which we get the exact sequence

$$1 \to \frac{A}{A \cap G'} \to G^{\mathrm{ab}} \to Q^{\mathrm{ab}} \to 1$$

and since $[A,Q] \subseteq A \cap G'$ we conclude that $A/[A,Q]$ surjects onto $A/A \cap G' = \ker(G^{\mathrm{ab}} \to Q^{\mathrm{ab}})$. □

Proposition 5.11. *The adelic failure $B_\ell(N)$ divides* $[\tilde{K} : K] \cdot \#\dfrac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}$.

Proof. Let J_1 and J_2 be the maximal abelian extensions of $\tilde{K}$ contained in $\tilde{K}_{\ell^n}$ and $\tilde{K}_{\ell^n,\ell^n}$ respectively. Then we have $\mathrm{Gal}(J_1 \,|\, \tilde{K}) = \tilde{H}_{\ell^n}^{\mathrm{ab}}$ and $\mathrm{Gal}(J_2 \,|\, \tilde{K}) = \tilde{G}_{\ell^n}^{\mathrm{ab}}$, where $\tilde{G}_{\ell^n} = \mathrm{Gal}(\tilde{K}_{\ell^n,\ell^n} \,|\, \tilde{K})$. Notice that $[J_2 : J_1] = \#W$, where $W = \ker(\tilde{G}_{\ell^n}^{\mathrm{ab}} \to \tilde{H}_{\ell^n}^{\mathrm{ab}})$ is a quotient of $\tilde{V}_{\ell^n}/[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ by Lemma 5.10. Let moreover $F' := \tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_R$ and $T' := \tilde{K}_{\ell^n} \cap \tilde{K}_R$. By Proposition 5.9 we have $F' \subseteq J_2$ and clearly also $T' \subseteq J_1$ (indeed T' is abelian over $\tilde{K}$ since it is a sub-extension of F'). Consider the compositum J_1F' inside J_2.



It is easy to check that $F' \cap J_1 = T'$, so we have that $[F' : T'] = [J_1F' : J_1]$ divides $[J_2 : J_1]$, which in turn divides $\tilde{V}_{\ell^n}/[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$.

Now applying Proposition 5.7 with $\tilde{K}$ in place of K we get that

$$\frac{[\tilde{K}_{\ell^n,\ell^n} : \tilde{K}_{\ell^n}]}{[\tilde{K}_{\ell^n R,\ell^n} : \tilde{K}_{\ell^n R}]} \qquad \text{divides} \qquad [F' : T'],$$

and using that $[\tilde{K}_{\ell^n R,\ell^n} : \tilde{K}_{\ell^n R}]$ divides $[K_{\ell^n R,\ell^n} : K_{\ell^n R}]$ it is easy to see that

$$\frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{\ell^n R,\ell^n} : K_{\ell^n R}]} \qquad \text{divides} \qquad [\tilde{K} : K] \cdot \frac{[\tilde{K}_{\ell^n,\ell^n} : \tilde{K}_{\ell^n}]}{[\tilde{K}_{\ell^n R,\ell^n} : \tilde{K}_{\ell^n R}]}.$$

We conclude that

$$B_\ell(N) = \frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{\ell^n R,\ell^n} : K_{\ell^n R}]} \qquad \text{divides} \qquad [\tilde{K} : K] \cdot \#\frac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}.$$

□

So we are left with giving an upper bound on the ratio $\#\tilde{V}_{\ell^n}/\#[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$: this is achieved in the following Proposition.

Proposition 5.12. *For every n, the order of $\tilde{V}_{\ell^n}/[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ divides $\ell^{2\tilde{n}_\ell}$, where $\tilde{n}_\ell$ is the minimal parameter of maximal growth for the ℓ-adic torsion representation of $E/\tilde{K}$.*

Proof. By Lemma 4.9, the group $\tilde{H}_{\ell^n}$ contains $(1 + \ell^{\tilde{n}_\ell})\,\mathrm{Id}$. This implies that for every $v \in \tilde{V}_{\ell^n}$ the group $[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ contains

$$\left[v, (1 + \ell^{\tilde{n}_\ell})\,\mathrm{Id}\right] = (1 + \ell^{\tilde{n}_\ell})\,\mathrm{Id} \cdot v - v = \ell^{\tilde{n}_\ell} v,$$

that is, $[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ contains $\ell^{\tilde{n}_\ell}\tilde{V}_{\ell^n}$. The claim now follows from the fact that $\tilde{V}_{\ell^n}$ is generated over $\mathbb{Z}/\ell^n\mathbb{Z}$ by at most two elements. □

Lemma 5.13. *Assume that $\ell \geqslant 5$ is unramified in $K \mid \mathbb{Q}$ and that the image of the* mod ℓ *torsion representation is* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *(so in particular E does not have CM over $\overline{K}$). Assume moreover that α is ℓ-indivisible. Then $V_{\ell^n} = [V_{\ell^n}, H_{\ell^n}]$.*

Proof. Since H'_{ℓ^∞} is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose reduction modulo ℓ contains $H'_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)' = \mathrm{SL}_2(\mathbb{F}_\ell)$, by Lemma 3.9 the group H_{ℓ^∞} contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$. The assumption that ℓ is unramified in K implies that $\det(H_{\ell^\infty}) = \mathbb{Z}_\ell^\times$, which together with the inclusion $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq H_{\ell^\infty}$ implies $H_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$, and in

particular $H_{\ell^n} = \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. By [JR10, Theorem 5.2] we have $V_{\ell^n} = (\mathbb{Z}/\ell^n\mathbb{Z})^2$, so it is enough to consider

$$g_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H_{\ell^n}, \quad g_2 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in H_{\ell^n}, \quad v := \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V_{\ell^n}$$

to conclude that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = g_1 v - v \in [V_{\ell^n}, H_{\ell^n}] \quad \text{and} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = g_2 v - v \in [V_{\ell^n}, H_{\ell^n}],$$

so that $V_{\ell^n} \subseteq [V_{\ell^n}, H_{\ell^n}]$. □

Lemma 5.14. *Let E/K be an elliptic curve such that $\mathrm{End}_{\overline{K}}(E)$ is an order $\mathcal{A}$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Let $\ell \geqslant 3$ be a prime unramified both in K and in $\mathbb{Q}(\sqrt{-d})$, and suppose that E has good reduction at all places of K of characteristic ℓ. Then $V_{\ell^n} = [V_{\ell^n}, H_{\ell^n}]$ and $\tilde{V}_{\ell^n} = [\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$.*

Proof. By [Lom17, Theorem 1.5], the image of the ℓ-adic representations attached to both E/K and $E/\tilde{K}$ contains $(\mathcal{A} \otimes \mathbb{Z}_\ell)^\times$, hence in particular it contains an operator that acts as multiplication by 2 on $E[\ell^n]$ for every n. Let λ be such an operator: then $[V_{\ell^n}, H_{\ell^n}]$ contains $[V_{\ell^n}, \lambda] = \{\lambda v - v \mid v \in V_{\ell^n}\} = V_{\ell^n}$ as claimed. The case of $\tilde{V}_{\ell^n}$ is similar. □

Theorem 5.15. *Let ℓ be a prime. There is a constant b_ℓ, depending only on the p-adic torsion representations associated with E for all the primes p, such that $B_\ell(N)$ divides ℓ^{b_ℓ} for all positive integers N. Moreover,*

(1) *Suppose that E does not have complex multiplication over $\overline{\mathbb{Q}}$. Then b_ℓ is zero whenever the following conditions all hold: α is ℓ-indivisible, $\ell > 5$ is unramified in $K \mid \mathbb{Q}$, the $\bmod \ell$ torsion representation is surjective, and E has good reduction at all places of K of characteristic ℓ.*

(2) *Suppose $\mathrm{End}_{\overline{K}}(E)$ is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Then b_ℓ is zero whenever the following conditions all hold: $\ell \geqslant 3$ is a prime unramified both in K and in $\mathbb{Q}(\sqrt{-d})$, and E has good reduction at all places of K of characteristic ℓ.*

Both in the CM and non-CM cases, for the finitely many remaining primes ℓ we can take $b_\ell = 2n_\ell + 3v_\ell\left([\tilde{K} : K]\right)$, where $\tilde{K}$ is as in Definition 5.8 and n_ℓ is a parameter of maximal growth for the ℓ-adic torsion part.

Proof. Let n be the ℓ-adic valuation of N. By Proposition 5.11, the adelic failure $B_\ell(N)$ divides $[\tilde{K} : K] \cdot \#\dfrac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}$.

(1) Suppose that E does not have CM over $\overline{\mathbb{Q}}$, that α is ℓ-indivisible, that $\ell > 5$ is unramified in $K \mid \mathbb{Q}$, that the mod ℓ torsion representation is surjective, and that E has good reduction at all places of K of characteristic ℓ. Under these assumptions, the prime ℓ does not belong to the set S of Theorem 5.1, so we have $\tilde{K} = K$ and $[\tilde{K} : K] \cdot \#\frac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}$ is simply $\#\frac{V_{\ell^n}}{[V_{\ell^n}, H_{\ell^n}]}$. We conclude because this quotient is trivial by Lemma 5.13.

(2) In the CM case, the conclusion follows from Lemma 5.14 since $\ell \nmid [\tilde{K} : K] \leqslant 2$.

For all other primes, combining Proposition 5.11 and Proposition 5.12 we get that $B_\ell(N)$ divides $[\tilde{K} : K] \cdot \ell^{2\tilde{n}_\ell}$ and we conclude using Lemma 3.10. □

Remark 5.16. The proof shows that the inequality

$$v_\ell(B_\ell(N)) \leqslant 2n_\ell + 3v_\ell\left([\tilde{K} : K]\right)$$

holds for every prime ℓ and for every rational point $\alpha \in E(K)$. In other words, for a fixed prime ℓ the adelic failure can be bounded independently of the rational point α.

We can finally prove our first Theorem from the introduction:

Proof of Theorem 1.1. By Remark 2.1, Theorem 1.1 follows from Theorems 4.17 and 5.15 by taking $C := \prod_\ell \ell^{a_\ell + b_\ell}$. □

Remark 5.17. Theorem 1.1 is completely effective, in the following sense: the quantities a_ℓ and b_ℓ can be computed in terms of $[\tilde{K} : K]$, n_ℓ, and the divisibility parameter d. The integer d can be bounded effectively in terms of the height of α and of standard invariants of the elliptic curve, as showed in Remark 4.15. The remaining quantities $[\tilde{K} : K]$ and n_ℓ can be bounded effectively in terms of $[K : \mathbb{Q}]$ and of the height of E, as shown in [Lom15].

6 A counterexample in the CM case

We give an example showing that Proposition 4.13 does not hold in the CM case when ℓ is split in the field of complex multiplication, and that in fact in this case there can be no uniform lower bound on the image of the Kummer representation depending only on the image of the torsion representation, even when α is strongly ℓ-indivisible.

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication over $\overline{\mathbb{Q}}$ by the imaginary quadratic field F. Let $\alpha \in E(\mathbb{Q})$ be such that the ℓ^n-arboreal representation

attached to (E, α) maps onto $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes N_{\ell^n}$ for every $n \geqslant 1$, where N_{ℓ^n} is the normaliser of a Cartan subgroup C_{ℓ^n} of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Suppose furthermore that ℓ is split in F and does not divide the conductor of the order $\mathrm{End}_{\overline{\mathbb{Q}}} E \subseteq \mathcal{O}_F$. Such triples (E, α, ℓ) exist: by [JR10, Example 5.11] we can take $E : y^2 = x^3 + 3x$ (which has CM by $\mathbb{Z}[i]$), $\alpha = (1, -2)$ and $\ell = 5$ (which splits in $\mathbb{Z}[i]$). Notice that for this elliptic curve and this α the same property holds for every $\ell \equiv 1 \pmod 4$: [Lom17, Theorem 1.5 (2)] implies that for all $\ell \geqslant 5$ the image of the Galois representation is the full normaliser of a Cartan subgroup, at which point surjectivity of the Kummer representation follows from [JR10, Theorem 5.8].

Consider now the image of the arboreal representation associated with $(E/F, \alpha, \ell)$. Base-changing E to F has the effect of replacing the normaliser of the Cartan subgroup with Cartan itself: more precisely we have $\omega_{\ell^n}\left(\mathrm{Gal}(F_{\ell^n,\ell^n} \mid F)\right) = (\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n}$ for every $n \geqslant 1$. As ℓ is split in the quadratic ring $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$, so is the Cartan subgroup C_{ℓ^n}, and therefore we can assume – choosing a different basis for $E[\ell^n]$ if necessary – that C_{ℓ^n} is the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Fix now a large n and let

$$B_{\ell^n} = \left\{(t, M) \in (\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n} : t \equiv (*, 0) \pmod{\ell^{n-1}}\right\}.$$

Using the explicit group law on $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n}$ one checks without difficulty that B_{ℓ^n} is a subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n}$: indeed, given two elements $g_1 = (t_1, M_1)$ and $g_2 = (t_2, M_2)$ in B_{ℓ^n}, we have

$$g_1 \cdot g_2 = (t_1, M_1) \cdot (t_2, M_2) = (t_1 + M_1 t_2, M_1 M_2),$$

and (since M_1 is diagonal) the second coordinate of $t_1 + M_1 t_2$ is a linear combination (with $\mathbb{Z}/\ell^n\mathbb{Z}$-coefficients) of the second coordinates of t_1, t_2, hence is zero modulo ℓ^{n-1}. Finally, let $K \subset F_{\ell^n,\ell^n}$ be the field corresponding by Galois theory to the subgroup B_{ℓ^n} of $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n} \cong \mathrm{Gal}(F_{\ell^n,\ell^n} \mid F)$.

We now study the situation of Proposition 4.13 for the elliptic curve E/K and the point α. By construction, the image of the ℓ^{n-1}-torsion representation attached to $(E/K, \ell)$ is $C_{\ell^{n-1}}$, so the parameter of maximal growth can be taken to be $n_\ell = 1$. We claim that $\alpha \in E(K)$ is strongly ℓ-indivisible. The modulo-ℓ torsion representation is surjective onto C_ℓ, so that in particular no ℓ-torsion point of E is defined over K, and strongly ℓ-indivisible is equivalent to ℓ-indivisible. To see that this last condition holds, notice that if α were ℓ-divisible then we would have $K_{\ell,\ell} = K_\ell$. However this is not the case, because by construction $\mathrm{Gal}(K_{\ell,\ell} \mid K_\ell) = \{t \in (\mathbb{Z}/\ell\mathbb{Z})^2 : t \equiv (*, 0) \pmod \ell\}$ has order ℓ. Finally, for $k = n - 3$ we have

$$V_{\ell^{k+2n_\ell}} = V_{\ell^{n-1}} = \{t \in (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 : t \equiv (*, 0) \pmod{\ell^{n-1}}\},$$

which is very far from containing $E[\ell^k]$ – in fact, the index of $V_{\ell^{k+2n_\ell}}$ in $E[\ell^{k+2n_\ell}]$ can be made arbitrarily large by choosing larger and larger values of n. Notice that in any such example the ℓ-adic representation will be surjective onto a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

7 Uniform bounds for the adelic representation

Our aim in this section is to show:

Theorem 7.1. *There is a positive integer C with the following property: for every elliptic curve $E/\mathbb{Q}$ and every strongly indivisible point $\alpha \in E(\mathbb{Q})$, the image W_∞ of the Kummer map associated with $(E/\mathbb{Q}, \alpha)$ has index dividing C in $\prod_\ell T_\ell(E)$.*

This result immediately implies Theorem 1.2:

Proof of Theorem 1.2. By Remark 2.6, for every $N \mid M$ the ratio $\dfrac{N^2}{[\mathbb{Q}_{M,N} : \mathbb{Q}_M]}$ divides

$$\frac{N^2}{[\mathbb{Q}_{\infty,N} : \mathbb{Q}_\infty]} = \left[(\widehat{\mathbb{Z}}/N\widehat{\mathbb{Z}})^2 : W_\infty/NW_\infty\right],$$

which in turn divides $[\widehat{\mathbb{Z}}^2 : W_\infty]$. □

Remark 7.2. The assumption of strong indivisibility of the point α is necessary. In fact, one can take a point α that is divisible in $E(\mathbb{Q})$ by an arbitrarily high power of some prime ℓ, and thus get an index divisible by an arbitrarily large power of ℓ.

However, one can recover a similar result for divisible points allowing the constant C to depend on the largest integer d such that $\alpha = d\beta + T$ for some $\beta \in E(\mathbb{Q})$ and some $T \in E(\mathbb{Q})_{\mathrm{tors}}$. In fact, Lemma 4.16 tells us that in this situation the index of the Kummer representation associated with α divides d^2 times the index of the Kummer representation associated with β.

As in Subsection 3.3, we will denote by $\mathcal{T}_0$ the finite set of primes

$$\mathcal{T}_0 := \{p \text{ prime } \mid p \leqslant 17\} \cup \{37\}.$$

7.1 Bounds on cohomology groups

Let $E/\mathbb{Q}$ be an elliptic curve and N_1, N_2 be positive integers with $N_1 \mid N_2$. The first step in the proof of Theorem 7.1 is to bound the exponent of the cohomology group $H^1(H_{N_2}, E[N_1])$. In the course of the proof we shall need the following technical result, which will be proved in Section 7.2.

Proposition 7.3. *There is a universal constant e satisfying the following property. Let $E/\mathbb{Q}$ be a non-CM elliptic curve, N a positive integer and ℓ a prime factor of N. Let ℓ^k be the largest power of ℓ dividing N and $J = \mathrm{Gal}(\mathbb{Q}_N \mid \mathbb{Q}_{\ell^k}) \triangleleft H_N$. Consider the action of H_N on $\mathrm{Hom}(J, E[\ell^k])$ defined by $(h\psi)(x) = h\psi(h^{-1}xh)$ for all $h \in H_N$, $\psi : J \to E[\ell^k]$ and $x \in J$. Then the exponent of $\mathrm{Hom}\left(J, E[\ell^k]\right)^{H_N}$ divides e.*

Proposition 7.4. *There is a positive integer C_1 with the following property. Let $E/\mathbb{Q}$ be an elliptic curve, N_1 and N_2 be positive integers with $N_1 \mid N_2$. Then the exponent of $H^1(H_{N_2}, E[N_1])$ divides C_1.*

Proof. We can prove the statement separately for CM and non-CM curves, and then conclude by taking the least common multiple of the two constants obtained in the two cases.

Assume first that $E/\mathbb{Q}$ has CM over $\overline{\mathbb{Q}}$. Let F be the CM field of E, let $\mathcal{O}_F$ be the ring of integers of F and $\mathcal{O}_\ell := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. By [Lom17, Theorem 1.5] we have $d := \left[\prod_\ell \mathcal{O}_\ell^\times : H_\infty \cap \prod_\ell \mathcal{O}_\ell^\times\right] \leqslant 6$. In particular all the d-th powers of elements in $\prod_\ell \mathcal{O}_\ell^\times$ are in H_∞, hence we have $\widehat{\mathbb{Z}}^{\times d} \subseteq H_\infty \subseteq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ and H_∞ contains the nontrivial homothety $\lambda = (\lambda_\ell)$, where $\lambda_2 = 3^d$ and $\lambda_\ell = 2^d$ for $\ell \neq 2$. By Sah's Lemma [BR03, Lemma A.2] we have $(\lambda - 1)H^1(H_{N_2}, E[N_1]) = 0$. Notice that the image of $\lambda - 1$ in $\mathbb{Z}_\ell$ is nonzero for all ℓ, and that it is invertible for almost all ℓ. The claim follows from the fact that d is bounded.

Assume now that E does not have complex multiplication over $\overline{\mathbb{Q}}$. As cohomology commutes with finite direct products we have

$$H^1(H_{N_2}, E[N_1]) \cong H^1\left(H_{N_2}, \bigoplus_{\ell^v \mid N_1} E[\ell^v]\right) \cong \bigoplus_{\ell^v \mid N_1} H^1\left(H_{N_2}, E[\ell^v]\right).$$

Fix an ℓ in this sum and let $J = \mathrm{Gal}(\mathbb{Q}_{N_2} \mid \mathbb{Q}_{\ell^k}) \triangleleft H_{N_2}$, where ℓ^k is the largest power of ℓ dividing N_2. By the inflation-restriction sequence we get

$$0 \to H^1(H_{N_2}/J, E[\ell^v]^J) \to H^1(H_{N_2}, E[\ell^v]) \to H^1(J, E[\ell^v])^{H_{N_2}};$$

since by definition J fixes $E[\ell^v]$, this is the same as

$$0 \to H^1(H_{\ell^k}, E[\ell^v]) \to H^1(H_{N_2}, E[\ell^v]) \to \mathrm{Hom}(J, E[\ell^v])^{H_{N_2}}.$$

It is clear that the exponent of $H^1(H_{N_2}, E[N_1])$ is the least common multiple of the exponents of the direct summands $H^1\left(H_{N_2}, E[\ell^v]\right)$ for $\ell \mid N_1$, so we can focus on one such summand at a time. Furthermore, the above inflation-restriction exact sequence shows that the exponent of $H^1(H_{N_2}, E[\ell^v])$ divides the product of the exponents of $H^1(H_{\ell^k}, E[\ell^v])$ and of $\mathrm{Hom}(J, E[\ell^v])^{H_{N_2}}$. It is enough to give a uniform bound for the exponents of these two cohomology groups.

(i) $\boxed{H^1(H_{\ell^k}, E[\ell^v])}$ Assume first that $\ell \notin \mathcal{T}_0$. By Theorem 3.14, H_ℓ is not contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so by [LW15, Lemma 4] it contains a nontrivial homothety. By Lemma 3.17 the image H_{ℓ^∞} of the ℓ-adic representation contains a homothety that is non-trivial modulo ℓ, so by Sah's Lemma [BR03, Lemma A.2] we have $H^1(H_{\ell^k}, E[\ell^v]) = 0$. For $\ell \in \mathcal{T}_0$ let n_ℓ be a universal bound on the parameter of maximal growth of the ℓ-adic representation, as in Corollary 3.13. By Lemma 4.9 we have $(1+\ell^{n_\ell})\,\mathrm{Id} \in H_{\ell^k}$, and from Lemma 4.7 we obtain that the exponent of $H^1(H_{\ell^k}, E[\ell^v])$ divides ℓ^{n_ℓ}.

(ii) $\boxed{\mathrm{Hom}(J, E[\ell^v])^{H_{N_2}}}$ As $v \leqslant k$, this group is contained in $\mathrm{Hom}(J, E[\ell^k])^{H_{N_2}}$, whose exponent is uniformly bounded by Proposition 7.3. Notice that the action of H_{N_2} on $\mathrm{Hom}(J, E[\ell^k])$ is precisely that considered in Proposition 7.3 by well-known properties of the inflation-restriction exact sequence (see e.g. [Ros95, Theorem 4.1.20]).

□

Proposition 7.4 can be restated in terms of $H^1(H_\infty, E(\overline{\mathbb{Q}})_{\mathrm{tors}})$.

Theorem 7.5. *There is a positive integer C_1 such that, for any elliptic curve $E/\mathbb{Q}$, the exponent of $H^1(H_\infty, E(\overline{\mathbb{Q}})_{\mathrm{tors}})$ divides C_1.*

Proof. By [NSW13, Proposition 1.2.6] we have

$$H^1(H_\infty, E(\overline{\mathbb{Q}})_{\mathrm{tors}}) \cong \varinjlim_N H^1(H_N, E[N]),$$

so the result follows from Proposition 7.4. □

Remark 7.6. Let $m := [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : H_\infty]$. By basic group theory, there is a normal subgroup B of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ contained in H_∞ and having index dividing $m!$. It follows that the $m!$-th power of any element of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is in B, hence in H_∞, and in particular H_∞ contains $\widehat{\mathbb{Z}}^{\times m!} \cdot \mathrm{Id}$. An application of Sah's lemma then shows that the exponent of $H^1(H_\infty, E(\overline{\mathbb{Q}})_{\mathrm{tors}})$ can be upper-bounded purely in terms of m. A positive answer to Serre's uniformity question for elliptic curves over $\mathbb{Q}$ would imply that there are only finitely many possibilities for the index m (see for example [Zyw15c]), so Theorem 7.5 would immediately follow.

Corollary 7.7. *Let C_1 be as in Proposition 7.4. Let $E/\mathbb{Q}$ be an elliptic curve and let $\alpha \in E(\mathbb{Q})$ be a strongly indivisible point. If α is divisible by $n \geqslant 1$ over $\mathbb{Q}_\infty$, then $n \mid C_1$.*

Proof. Without loss of generality we can assume that $n = \ell^e$ is a power of a prime ℓ. Since $\mathbb{Q}_\infty$ is the union of the torsion fields $\mathbb{Q}_N$, there exists N such that α is divisible by ℓ^e over $\mathbb{Q}_N$, and we may assume that ℓ^e divides N. The claim then follows from Lemma 4.6, since by Proposition 7.4 the exponent of $H^1(\mathrm{Gal}(\mathbb{Q}_N \mid \mathbb{Q}), E[\ell^e])$ is a power of ℓ that divides C_1. □

Lemma 7.8. *Let C_1 be as in Proposition 7.4. The following hold for every prime ℓ:*

(1) *The $\mathbb{Z}_\ell$-module W_{ℓ^∞}, considered as a submodule of $\mathbb{Z}_\ell^2$, contains a vector of valuation at most $v_\ell(C_1)$.*

(2) *Suppose that E does not have CM over $\overline{\mathbb{Q}}$ and let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation. Then W_{ℓ^∞} contains $\ell^{n_\ell + v_\ell(C_1)} T_\ell(E)$.*

(3) *If $E[\ell]$ is an irreducible H_ℓ-module, then W_{ℓ^∞} contains $\ell^{v_\ell(C_1)} T_\ell(E)$.*

(4) *Suppose that E has CM over $\overline{\mathbb{Q}}$ and let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$. If n_ℓ is a parameter of maximal growth for the ℓ-adic torsion representation, then W_{ℓ^∞} contains $\ell^{3n_\ell + v_\ell(4\delta C_1)} T_\ell(E)$.*

Proof. Part (1) follows from Lemma 4.11, since by Corollary 7.7 the point α is not divisible by $\ell^{v_\ell(C_1)+1}$ over $\mathbb{Q}_\infty$. Parts (2), (3) and (4) then follow from Proposition 4.12 (for part (4) observe that no elliptic curve over $\mathbb{Q}$ has CM defined over $\mathbb{Q}$). □

We can now prove the main Theorem of this section.

Proof of Theorem 7.1. As already explained, we have $W_\infty = \prod_\ell W_{\ell^\infty}$, so we obtain

$$\left[\prod_\ell T_\ell(E) : W_\infty\right] = \prod_\ell [T_\ell(E) : W_{\ell^\infty}].$$

Let

$$\mathcal{T}_1 = \mathcal{T}_0 \cup \{\ell \text{ prime} \mid \ell \text{ divides } C_1\} \cup \{19, 43, 67, 163\}.$$

Notice that by Theorem 3.14 for $\ell \notin \mathcal{T}_1$ there is no elliptic curve over $\mathbb{Q}$ with a rational subgroup of order ℓ. By Lemma 7.8 (3), for $\ell \notin \mathcal{T}_1$ we have $W_{\ell^\infty} = T_\ell(E)$, so

$$\left[\prod_\ell T_\ell(E) : W_\infty\right] = \prod_{\ell \in \mathcal{T}_1} [T_\ell(E) : W_{\ell^\infty}]. \tag{7.1}$$

Now it is enough to prove the Theorem separately in the CM and in the non-CM case, and then take the least common multiple of the two constants obtained.

Suppose first that E does not have CM over $\overline{\mathbb{Q}}$. Applying Lemma 7.8(2) we see that $[T_\ell(E) : W_{\ell^\infty}]$ divides $\ell^{2(n_\ell + v_\ell(C_1))}$, where n_ℓ is a parameter of maximal growth for the ℓ-adic torsion for E. By Theorem 3.11 this can be bounded uniformly in E. Since C_1 does not depend on E, each factor of the right hand side of (7.1) is uniformly bounded.

Assume now that E has complex multiplication over $\overline{\mathbb{Q}}$ and let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$. Applying Lemma 7.8(4), we see that $[T_\ell(E) : W_{\ell^\infty}]$ divides $\ell^{2(3n_\ell + v_\ell(4\delta C_1))}$, where n_ℓ is a parameter of maximal growth for the ℓ-adic torsion representation for E, which is uniformly bounded by Corollary 3.13. It remains to show that $v_\ell(\delta)$ can be bounded uniformly as well. This follows from the fact that δ only depends on the $\overline{\mathbb{Q}}$-isomorphism class of E, and that there are only finitely many rational j-invariants corresponding to CM elliptic curves. □

7.2 Proof of Proposition 7.3

Recall the setting of Proposition 7.3: $E/\mathbb{Q}$ is a non-CM elliptic curve, N is a positive integer, and ℓ is a prime factor of N. Let ℓ^k be the largest power of ℓ dividing N and $J = \mathrm{Gal}(\mathbb{Q}_N \mid \mathbb{Q}_{\ell^k}) \triangleleft H_N$. The question is to study the exponent of the group $\mathrm{Hom}\left(J, E[\ell^k]\right)^{H_N}$. In order to do this, we shall study the conjugation action of $g \in H_N$ on the abelianisation of J. More generally, we shall also consider the conjugation action of elements in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that normalise J.

It will be useful to work with a certain subgroup $J(2)$ of J. More generally, we introduce the following notation.

Definition 7.9. Let G be a group and M a positive integer. We denote by $G(M)$ the subgroup of G generated by $\left\{g^M \mid g \in G\right\}$.

Lemma 7.10. *The subgroup $J(2)$ is normal in J, the quotient group $J/J(2)$ has exponent at most 2, $J(2)$ is stable under the conjugation action of H_N, and*

$$\exp \mathrm{Hom}\left(J, E[\ell^k]\right)^{H_N} \mid 2 \exp \mathrm{Hom}\left(J(2), E[\ell^k]\right)^{H_N}.$$

Proof. Clearly $J(2)$ is a characteristic subgroup of J, so it is normal in J and stable under the conjugation action of H_N on J. Given a coset $hJ(2) \in J/J(2)$ we have $(hJ(2))^2 = h^2 J(2) = J(2)$ since $h^2 \in J(2)$ by definition, so the quotient $J/J(2)$ is killed by 2. Finally, take a homomorphism $\psi : J \to E[\ell^k]$ stable under the conjugation action of H_N and denote by d the exponent of the

abelian group $\mathrm{Hom}\big(J(2), E[\ell^k]\big)^{H_N}$. The restriction of ψ to $J(2)$ is an element of $\mathrm{Hom}\big(J(2), E[\ell^k]\big)^{H_N}$, so it satisfies $d\psi|_{J(2)} = 0$, and thus given any $h \in J$ we have $d\psi|_{J(2)}(h^2) = 0$. This implies that for every $h \in J$ we have $2d\psi(h) = 0$, hence ψ is killed by $2d$. Since this is true for all ψ, the claim follows. □

We will also need the following two simple lemmas:

Lemma 7.11. *Let $E/\mathbb{Q}$ be an elliptic curve and let $M \geqslant 37$ be an integer. If $\ell > M+1$ is a prime number, then $H_{\ell^\infty}(M)$ contains a homothety $\lambda\,\mathrm{Id}$ with $\lambda \not\equiv 1 \pmod{\ell}$.*

Proof. By Corollary 3.16, since $\ell > M+1 > 37$, the image of the modulo-ℓ representation contains all the homotheties. In particular, if $\overline{\mu} \in \mathbb{F}_\ell^\times$ is a generator of the multiplicative group $\mathbb{F}_\ell^\times$, then H_ℓ contains $\overline{\mu}\,\mathrm{Id}$, so by Lemma 3.17 H_{ℓ^∞} contains $\mu\,\mathrm{Id}$, where $\mu \in \mathbb{Z}_\ell^\times$ is congruent to $\overline{\mu}$ modulo ℓ. So $H_{\ell^\infty}(M)$ contains $\mu^M\,\mathrm{Id}$, which is nontrivial modulo ℓ since $\overline{\mu}$ has order $\ell - 1 > M$. □

Lemma 7.12. *Let p be a prime and let n be a positive integer (with $n \geqslant 2$ if $p = 2$). For every positive integer k let $U_k = \big\{x \in \mathbb{Z}_p \mid x \equiv 1 \pmod{p^k}\big\}$. Let M be a positive integer. Then $\big\{x^M \mid x \in U_n\big\} \supseteq U_{n+v_p(M)}$.*

Proof. Let $y \in U_{n+v_p(M)}$ and let $a = y - 1$. By [Coh07, Corollary 4.2.17 and Corollary 4.2.18(1)], the p-adic integer $x = \exp(M^{-1}\log y)$ is well defined and satisfies the inequality $v_p(x-1) \geqslant v_p(M^{-1}a) \geqslant n$. Therefore $x \in U_n$ and clearly $x^M = y$. □

We will derive Proposition 7.3 from the following statement:

Proposition 7.13. *There is a universal constant M with the following property. For every elliptic curve $E/\mathbb{Q}$, every positive integer N, every prime power ℓ^k dividing N, and every $g \in H_N$, the conjugation action of g^M on the abelianisation of $J(2)$ is trivial.*

Proof of Proposition 7.13 $\implies$ Proposition 7.3. By Lemma 7.10 it is enough to prove Proposition 7.3 with J replaced by $J(2)$. Let $\psi \in \mathrm{Hom}\big(J(2), E[\ell^k]\big)$: then as $E[\ell^k]$ is abelian ψ factors through $J(2)^{\mathrm{ab}}$.

For every $g \in H_N$, every $\psi \in \mathrm{Hom}\big(J(2), E[\ell^k]\big)^{H_N}$ and every $h \in J(2)$ we have

$$\psi(h) = g^M \cdot \psi(g^{-M} h g^M) = g^M \cdot \psi(h),$$

where the first equality holds because ψ is H_N-invariant and the second because the automorphism induced by g^M on $J(2)^{\mathrm{ab}}$ is trivial by Proposition 7.13. This means that the image of ψ is contained in $E[\ell^k]^{H_N(M)}$. Since the action of H_N on $E[\ell^k]$ factors via the canonical projection $H_N \to \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$, this is the

same as saying that the image of ψ is contained in the subgroup of $E[\ell^k]$ fixed under $H_{\ell^k}(M)$. It remains to show that the exponent of $E[\ell^k]^{H_{\ell^k}(M)}$ is uniformly bounded, and trivial for ℓ sufficiently large.

To see this, recall that by Theorem 3.11 there exists an integer $n \geqslant 1$, independent of E, such that H_{ℓ^k} contains $\mathrm{Id} + \ell^n \mathrm{Mat}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ (and we have $n \geqslant 2$ if $\ell = 2$). By Lemma 7.12, for every $E/\mathbb{Q}$ the group $H_{\ell^k}(M)$ contains all scalar matrices in $\mathrm{Mat}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ that are congruent to the identity modulo $\ell^{n+v_\ell(M)}$. We claim that the exponent of $E[\ell^k]^{H_{\ell^k}(M)}$ divides $\ell^{n+v_\ell(M)}$. In fact, by what we have seen $H_{\ell^k}(M)$ contains $(1 + \ell^{n+v_\ell(M)})\,\mathrm{Id}$, so $E[\ell^k]^{H_{\ell^k}(M)}$ is in particular fixed by $(1 + \ell^{n+v_\ell(M)})\,\mathrm{Id}$, hence it is contained $E[\ell^{n+v_\ell(M)}]$.

Finally, we show that $\mathrm{Hom}(J, E[\ell^k])^{H_N}$ is trivial for $\ell > M+1$. Since $\ell > 2$, by Lemma 7.10 it is enough to show that $\mathrm{Hom}(J(2), E[\ell^k])^{H_N}$ is trivial. As above, the image of any H_N-stable homomorphism from $J(2)$ to $E[\ell^k]$ is contained in the $H_{\ell^k}(M)$-fixed points of $E[\ell^k]$. By Lemma 7.11, $H_{\ell^k}(M)$ contains a homothety which is nontrivial modulo ℓ, so we are done since the only fixed point of this homothety is 0. □

We now turn to the proof of Proposition 7.13. We start by showing that we may assume N to be of the form $\ell^k \cdot \prod_{p|N, p\neq\ell} p$. To see this, let $N = \ell^k \prod_{p|N,p\neq\ell} p^{e_p}$ be arbitrary and let $N' := \ell^k \prod_{p|N,p\neq\ell} p$. There is an obvious reduction map $J \to \mathrm{Gal}(\mathbb{Q}_{N'} \mid \mathbb{Q}_{\ell^k})$. The kernel $\mathcal{K}$ of this map is a subgroup of J whose order is divisible only by primes $p \mid N, p \neq \ell$. Recall that we will be considering $\mathrm{Hom}(J, E[\ell^k])^{H_N}$. Let $\psi : J \to E[\ell^k]$ be a homomorphism: we claim that ψ factors via the quotient $\mathrm{Gal}(\mathbb{Q}_{N'} \mid \mathbb{Q}_{\ell^k})$. Indeed, all the elements in $\mathcal{K}$ have order prime to ℓ, hence they must go to zero in $E[\ell^k]$. Therefore we may assume $N = N'$, that is, $N = \ell^k \cdot \prod_{p|N,p\neq\ell} p$.

We identify H_N with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) \times \prod_{p|N,p\neq\ell} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and J with the subgroup of H_N consisting of elements having trivial first coordinate, and for $g \in H_N$ we write $g = (g_\ell, g_{p_1}, \ldots, g_{p_r})$ with $g_\ell \in \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ and $g_{p_i} \in \mathrm{GL}_2(\mathbb{Z}/p_i\mathbb{Z})$. Finally, for $p \mid N$, $p \neq \ell$ we denote by $\pi_{p_i} : H_N \to \mathrm{GL}_2(\mathbb{Z}/p_i\mathbb{Z})$ the projection on the factor corresponding to p_i, and we denote by $\pi_\ell : H_N \to \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ the projection on the factor corresponding to ℓ.

Lemma 7.14. *Let p be a prime factor of N with $p \geqslant 7$, $p \neq \ell$. Suppose that the modulo-p representation attached to $E/\mathbb{Q}$ is surjective. Then $J(2)$ contains $\{1\} \times \cdots \times \{1\} \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \times \{1\} \times \cdots \times \{1\}$.*

Proof. Clearly $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs in H_N. Hence it must occur either in J or in H_N/J, but the latter is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ with $\ell \neq p$, so it must occur in J. Consider the kernel of the projection $J \to \prod_{q|N,q\neq p} \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$: then $\mathrm{PSL}_2(\mathbb{F}_p)$ must occur either in this kernel or in $\prod_{q|N,q\neq p} \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, but the latter case is impossible. Using Lemma 3.18, it follows immediately that J

contains $\{1\} \times \cdots \times \{1\} \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \times \{1\} \times \cdots \times \{1\}$. We conclude by noting that $\mathrm{SL}_2(\mathbb{F}_p)$ is generated by its squares. □

Lemma 7.15. *Let $g \in H_N$ and $h \in J(2)$. Then $gh \in H_N$, and the automorphisms of $J(2)^{\mathrm{ab}}$ induced by g and by gh coincide.*

Proof. As $J(2)$ is a subgroup of H_N, the fact that $gh \in H_N$ is obvious. For the second statement, notice that for every $x \in J(2)$ the element $(gh)^{-1}x(gh)$ differs from $g^{-1}xg$ by multiplication by

$$h^{-1}(g^{-1}x^{-1}g)^{-1}h(g^{-1}x^{-1}g),$$

which is a commutator in $J(2)$. Hence the classes of $(gh)^{-1}x(gh)$ and $g^{-1}xg$ are equal in $J(2)^{\mathrm{ab}}$. □

Lemma 7.16. *For each $p \mid N, p \neq \ell$, the component g_p of g along $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ normalises $\pi_p(J(2))$ in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof. Since H_N normalises $J(2)$ by Lemma 7.10, we have $\pi_p(g^{-1}J(2)g) = \pi_p(J(2))$. On the other hand, $\pi_p(g^{-1}J(2)g) = \pi_p(g)^{-1}\pi_p(J(2))\pi_p(g)$, so that as desired we obtain $g_p^{-1}\pi_p(J(2))g_p = \pi_p(J(2))$. □

Corollary 7.17. *Let $p_1, \ldots, p_s \geqslant 7$ be primes all different from ℓ and such that the mod-p_i representation attached to $E/\mathbb{Q}$ is surjective for each p_i. Let $g \in H_N$ and let $\widehat{g}$ be the element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by replacing every p_i-component (for $i = 1, \ldots, s$) of g by* Id. *Then $\widehat{g}^2$ normalises $J(2)$, and it induces on $J(2)^{\mathrm{ab}}$ the same conjugation action as g^2.*

Proof. By Lemma 7.15, if we multiply g^2 by any element of $J(2)$ the conjugation action on $J(2)^{\mathrm{ab}}$ does not change. By construction, the determinant of $\pi_{p_i}(g^2) = g_{p_i}^2$ is a square in $\mathbb{F}_{p_i}^{\times}$, say λ_i^2. It follows that the determinant of $g_{p_i}^2/\lambda_i$ is 1, so $g_{p_i}^2/\lambda_i \in \mathrm{SL}_2(\mathbb{Z}/p_i\mathbb{Z})$. By Lemma 7.14 we have that $J(2)$ contains $h_i = (1, 1, \ldots, 1, g_{p_i}^2/\lambda_i, 1, \ldots, 1)$. Letting $h = h_1 \cdots h_s$, we obtain that the action of g^2h^{-1} is the same as that of g^2. But the element

$$\mu = (1, \ldots, 1, \lambda_1, 1, \ldots, 1) \cdots (1, \ldots, 1, \lambda_s, 1, \ldots, 1)$$

is central in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, so $\widehat{g}^2 = g^2h^{-1}\mu^{-1}$ normalises $J(2)$ and it induces the same action as g^2 on $J(2)^{\mathrm{ab}}$. □

Let $M = \mathrm{lcm}\{\exp \mathrm{PGL}_2(\mathbb{F}_p) : p \in \mathcal{T}_0\}$, where $\exp \mathrm{PGL}_2(\mathbb{F}_p)$ denotes the exponent of the group $\mathrm{PGL}_2(\mathbb{F}_p)$.

Remark 7.18. Notice that M is even. Moreover, for any $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and any $p \in \mathcal{T}_0$ with $p \mid N$ and $p \neq \ell$ we have that $\pi_p(g^M)$ is a scalar in $\mathrm{GL}_2(\mathbb{F}_p)$, since it is trivial in $\mathrm{PGL}_2(\mathbb{F}_p)$.

We now prove Proposition 7.13, using the constant M just introduced.

Proof of Proposition 7.13. Write as before $g = (g_p)$. We divide the prime factors of N different from ℓ into three sets as follows:

$$\mathcal{P}_0 = \{p \mid N \text{ such that } p \in \mathcal{T}_0,\, p \neq \ell\},$$
$$\mathcal{P}_1 = \{p \mid N \text{ such that } H_p = \mathrm{GL}_2(\mathbb{F}_p),\, p \neq \ell\},$$
$$\mathcal{P}_2 = \{p \mid N \text{ such that } H_p \text{ is conjugate to a subgroup of } N_{\mathrm{ns}}(p),\, p \neq \ell\}.$$

Notice that by Theorem 3.15 each prime factor of N different from ℓ belongs to one of these three sets.

We now apply Corollary 7.17 with $\{p_1, \dots, p_s\} = \mathcal{P}_1$ to obtain an element $\widehat{g} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\pi_p(\widehat{g}) = \mathrm{Id}$ for every $p \in \mathcal{P}_1$ and such that $\widehat{g}^2$ induces on $J(2)^{\mathrm{ab}}$ the same conjugation action as g^2. In particular, $\widehat{g}^M$ induces on $J(2)^{\mathrm{ab}}$ the same conjugation as g^M (recall that M is even).

We now prove that this conjugation action is trivial by showing that $\widehat{g}^M$ commutes with every element of $J(2)$. It suffices to show that for each $p \mid N$ the projection $\pi_p(\widehat{g}^M)$ commutes with every element of $\pi_p(J(2))$.

(i) *Case $p \in \mathcal{P}_0$:* by Remark 7.18, $\pi_p(\widehat{g}^M)$ is a scalar, thus it commutes with all of $\mathrm{GL}_2(\mathbb{F}_p)$.

(ii) *Case $p \in \mathcal{P}_1$:* by construction $\pi_p(\widehat{g}^M)$ is trivial.

(iii) *Case $p \in \mathcal{P}_2$:* by Corollary 3.16 applied to $\pi_p(\widehat{g})$, there is $h \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $\pi_p(\widehat{g}) \in hN_{\mathrm{ns}}(p)h^{-1}$ and $H_p \subseteq hN_{\mathrm{ns}}(p)h^{-1}$. Since M is even and $C_{\mathrm{ns}}(p)$ has index 2 in $N_{\mathrm{ns}}(p)$, $\pi_p(\widehat{g}^M) \in hC_{\mathrm{ns}}(p)h^{-1}$ and $\pi_p(J(2)) \subseteq \langle\, a^2 \mid a \in H_p \rangle \subseteq hC_{\mathrm{ns}}(p)h^{-1}$. Since $C_{\mathrm{ns}}(p)$ is abelian, $\pi_p(\widehat{g}^M)$ commutes with every element of $\pi_p(J(2))$.

(iv) *Case $p = \ell$:* by construction $\pi_p(J(2))$ is trivial.

□

Acknoledgments. It is a pleasure to thank Antonella Perucca for suggesting the problem that led to this paper, for her constant support, and for her useful comments. We are grateful to Peter Bruin for many interesting discussions, and to Peter Stevenhagen and Francesco Campagna for useful correspondence about the results of section 5.1.

Chapter 2

Some uniform bounds for elliptic curves over $\mathbb{Q}$

by Davide Lombardo and Sebastiano Tronto [LT21b]

1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Our purpose in this paper is to provide universal bounds on several arithmetically relevant quantities attached to E, and more precisely to its Galois representations. For each prime ℓ we denote by G_{ℓ^∞} the image of the ℓ-adic Galois representation attached to $E/\mathbb{Q}$, and by G_∞ the image of the adelic representation (see Section 2.4 for details). We provide in particular:

1. a uniform upper bound for the index $[\mathbb{Z}_\ell^\times : \mathbb{Z}_\ell^\times \cap G_{\ell^\infty}]$ (Theorem 3.16), that is, we show that for every prime ℓ the subgroup of scalars in the ℓ-adic image of Galois contains a fixed subgroup of $\mathbb{Z}_\ell^\times$ for all elliptic curves $E/\mathbb{Q}$;

2. a uniform upper bound on the exponent of the cohomology groups $H^1(G_\infty, E[N])$, for all positive integers N (Theorem 4.8);

3. a uniform lower bound for the closed $\mathbb{Z}_\ell$-subalgebra $\mathbb{Z}_\ell[G_{\ell^\infty}]$ of $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ generated by $G_{\ell^\infty} \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$: for each prime ℓ we compute an optimal exponent m_ℓ such that $\mathbb{Z}_\ell[G_{\ell^\infty}]$ contains $\ell^{m_\ell}\,\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ (Theorem 5.8);

4. a uniform lower bound on the degrees of the relative 'Kummer extensions' (Section 6), that is, the extensions $\mathbb{Q}(\frac{1}{N}\alpha, E[N])/\mathbb{Q}(E[N])$ obtained by adjoining all N-torsion points of E and all N-division points of a fixed rational point $\alpha \in E(\mathbb{Q})$ (Theorem 6.5), provided that α and all its translates by torsion points are not divisible by any $d > 1$ in the group $E(\mathbb{Q})$.

We now elaborate on each of these four topics. It is well-known that, for a fixed prime ℓ and number field K, the images of the ℓ-adic Galois representations attached to non-CM elliptic curves over K admit a uniform upper bound for the index $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G_{\ell^\infty}]$ (see for example [Ara08]). Since the CM case is easy to handle, this implies the existence of a bound as in (1). However, the result of [Ara08] is not effective, and a great deal of work has gone into classifying the possible ℓ-adic images of Galois even just for elliptic curves over $\mathbb{Q}$ (the so-called 'Program B' of Mazur), see for example [Maz77, RZB15, Zyw15a, BP11, LFL21, GRSS14, Gre12]. Our results on (1), which rely heavily on many of these previous developments, give a complete answer for all primes $\ell \neq 3$, and a rather sharp bound also for the remaining case $\ell = 3$. With the exception of the case $\ell = 2$, that was already treated in [RZB15], we prove our estimates by group-theoretic means (see in particular the criteria given by Corollary 3.7 and Proposition 2.A.1). The advantage of such an approach is that our methods can easily be extended to number fields other than $\mathbb{Q}$. The price to pay is that we don't get the sharpest possible result for $\ell = 3$, a direction we have decided not to pursue further also due to the very recent work of Rouse, Sutherland and Zureick-Brown [RSZB21] on the complete classification of 3-adic images of Galois for elliptic curves over $\mathbb{Q}$ with a rational 3-isogeny (see also Remark 3.15).

Concerning (2), there is already a significant past literature on controlling the cohomology groups $H^1(G_{\ell^\infty}, E[\ell^k])$, see for example [LW15], [Coa70, Lemma 10] and [Cre97, Section 3]. Kolyvagin's celebrated work on the Birch–Swinnerton-Dyer conjecture also needs to rely on vanishing statements for the Galois H^1 of the ℓ-torsion of elliptic curves [Gro91, Proposition 9.1]. In this paper we go beyond the known results in two different ways. On the one hand, we extend the statements in [LW15] by giving a uniform upper bound on the exponents of all the cohomology groups $H^1(G_{\ell^\infty}, E[\ell^k])$, where [LW15] mostly gave vanishing conditions and did not extensively treat the cases when the cohomology does not vanish. As we show in Section 7, these results for a fixed prime ℓ are rather sharp. Secondly, and more importantly for our application (4), we also treat the Galois action on the N-torsion of elliptic curves when N is not necessarily a prime power. While the case $N = \ell^k$ follows easily from the existence of non-trivial scalars in the image of Galois, the general case introduces a number of additional complications, connected with the possible 'entanglement' of torsion fields at different primes. Since not even the classification of possible ℓ-adic images is complete, the problem of describing all possible entanglements between torsion fields seems to

be out of reach for the moment (but see [Mor19], [CS19, §3], [CP20] and [DLM21] for some positive results), so the computation of $H^1(G_\infty, E[N])$ cannot be approached directly. We are still able to obtain useful information on this group (in particular, prove Theorem 4.8) by using the inflation-restriction exact sequence and controlling the amount of entanglement by using our results on scalars and the uniform bound on the degrees of prime-degree isogenies (Mazur's theorem). As in the case of (1), the intermediate technical results on the way to the proof of Theorem 4.8 should hopefully apply in more general situations (see in particular Proposition 4.5). Our numerical estimate on the exponent of $H^1(G_\infty, E[N])$ is nowhere near as sharp as the corresponding bounds for the special case $N = \ell^k$, but notice that (unlike in that case) it is not a priori clear that a uniform bound should even exist. We had in fact already shown the existence of such a bound in [Chapter 1], but the result was not effective.

We remark that we have chosen to formulate our bounds in terms of divisibility: we prove that multiplication by a suitable universal constant e kills the abelian group $H^1(G_\infty, E[N])$, and therefore the exponent of this group divides e. The numerical constant would be much smaller if we instead formulated the result as an inequality (that is, if we were content with knowing that the exponent of $H^1(G_\infty, E[N])$ does not exceed a certain constant e'), but we feel that our version will be more useful in applications. In particular, we would like to stress that – even ignoring the non-effective parts of the argument – the ideas of [Chapter 1] would lead to a (divisibility) bound for $H^1(G_\infty, E[N])$ involving primes up to several millions, while the value of e that we find with the new, more streamlined proof given in the present paper is only divisible by the primes up to 11 (which, as we show in Section 7, all need to appear as factors of e). In other words, while our constant e is probably not optimal, it is at least supported on the correct set of primes.

The algebra $\mathbb{Z}_\ell[G_{\ell^\infty}]$ considered in (3) is also a classical object in the field of Galois representations, and its analogues in arbitrary dimension most famously play an important role in Faltings's proof of his finiteness theorems for abelian varieties. While in many applications one needs control over the actual image of Galois G_{ℓ^∞}, in several cases it is enough to get a handle on the sub-algebra of $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ generated by it. In the hope that it will be useful in such cases, we give explicit values m_ℓ with the property that $\ell^{m_\ell}\,\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ is contained in $\mathbb{Z}_\ell[G_{\ell^\infty}]$ for all elliptic curves $E/\mathbb{Q}$, and we show that these values are optimal.

Finally, (4) was our original motivation for the work done in this paper: we had already shown a similar result in [Chapter 1], but (lacking all the previous information (1), (2), (3)) we could not make it explicit, or in fact even effective. With all the preliminary work done in [Chapter 1] and in the other sections of this paper, the desired result on Kummer extensions is now easy to prove. Notice that the assumption on the (in)divisibility of the point α is necessary: if $\alpha = N\beta$ for

some rational point β then $\mathbb{Q}(\frac{1}{N}\alpha, E[N])$ coincides with the torsion field $\mathbb{Q}(E[N])$, and clearly no non-trivial lower bound for $[\mathbb{Q}(\frac{1}{N}\alpha, E[N]) : \mathbb{Q}(E[N])]$ exists in this case. On the other hand, it is possible to relax this assumption if one is willing to accept a bound that depends on the largest integer d such that α is d-divisible in $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, but not on the curve E, see [Chapter 1, Remark 7.2].

We make two final comments. In order to get completely uniform results, we also need to treat the case of CM elliptic curves: while the proofs are generally easier than their non-CM counterparts, they are genuinely different and require some additional observations. In several cases we also prove sharper results in this context (see in particular Theorem 4.9 for a bound on the cohomology groups attached to CM elliptic curves over number fields). For this reason, while it is clear that one can obtain uniform statements that do not distinguish between CM and non-CM curves (essentially, by taking the maximum of the bounds in the two cases), we have chosen to formulate most of our results with a clear distinction between the two situations.

Finally, we would like to point out that much of what we do in this paper can be extended to number fields K having at least one real place, at least if one is ready to believe the Generalised Riemann Hypothesis. Indeed, under GRH, the uniform boundedness of isogenies of elliptic curves over K holds by [LV14, Corollary 6.5]. Concerning the four topics above, we have already pointed out that (1) is known to be true for all number fields, and the group-theoretic criteria of Propositions 3.4 and 2.A.1 can in most cases make this explicit (in terms of a bound on the possible degrees of cyclic isogenies). As for (2), the proof of Theorem 4.8 can be repeated almost verbatim once one knows that the subgroup of scalars in G_{ℓ^∞} is uniformly lower-bounded for all ℓ and that the degrees of cyclic isogenies are also bounded. A bound as in (3) follows from Proposition 5.1, Proposition 5.3 and Corollary 5.5. Finally, by the results of [Chapter 1] a bound as in (4) can be obtained as a consequence of all the above. We do not pursue this observation further since the result would in any case be conditional on GRH, but we hope to have convinced the reader that the techniques in this paper have wider applicability than just the case of rational numbers.

1.1 Structure of the paper

In Section 2 we recall some basic properties of ℓ-adic numbers and of subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for ℓ a prime number. We also introduce our notation for the Galois representations attached to elliptic curves. In Section 3 we prove our first main results, Theorems 3.16 and Proposition 3.18, which give a uniform lower bound for the subgroup of scalars in the image of Galois representations attached to elliptic curves over $\mathbb{Q}$ (in the non-CM and CM case respectively). In Section 4 we deduce from this an estimate on the exponent of the first cohomology group for the action

of Galois on the torsion points of an elliptic curve $E/\mathbb{Q}$, see Theorem 4.8 and Theorem 4.9 (which covers the CM case for elliptic curves over arbitrary number fields). In Section 5 we describe the $\mathbb{Z}_\ell$-subalgebra of $\mathrm{End}(\mathbb{Z}_\ell^2)$ generated by the image of an ℓ-adic Galois representation attached to an elliptic curve over $\mathbb{Q}$. Finally, in Section 6 we combine the previous results to study the Kummer theory of elliptic curves over $\mathbb{Q}$, leading to a uniform estimate on the degrees of Kummer extensions (Theorem 6.5). Section 7 gives some explicit examples showing that at least some of our estimates are not too far from optimal. The group-theoretic Appendix 2.A contains the proof of an auxiliary result needed in Section 3 to study the case of 3-adic Galois representations.

1.2 Acknowledgements

We thank Peter Bruin for providing us with a reference for Lemma 5.4, and Andrea Maffei for a useful discussion on reductive groups. We also thank Jeremy Rouse and Michael Cerchia for fruitful discussions, for informing us of their work in progress, and for suggesting some improvements to our results.

2 Preliminaries

2.1 The ℓ-adic numbers

For every prime ℓ we denote by $\mathbb{Z}_\ell$ the ring of ℓ-adic integers, which we regard as a profinite (topological) ring, and by v_ℓ the ℓ-adic valuation on $\mathbb{Z}_\ell$. We denote by $\mathbb{Z}_\ell^+$ the underlying abelian group of $\mathbb{Z}_\ell$, which is topologically generated by any element of ℓ-adic valuation 0, and by $\mathbb{Z}_\ell^\times$ its group of units. For $n \geqslant 1$ we let $1 + \ell^n\mathbb{Z}_\ell = \{x \in \mathbb{Z}_\ell \mid v_\ell(x-1) \geqslant n\}$. Since the subgroup $\ell^n\mathbb{Z}_\ell$ of $\mathbb{Z}_\ell^+$ is topologically generated by any element of valuation n, from [Coh07, Proposition 4.3.12] one obtains:

Lemma 2.1. *Let n be a positive integer and let $\ell > 2$ be a prime. Let G be a closed subgroup of $\mathbb{Z}_\ell^\times$. If there is $\lambda \in G$ such that $v_\ell(\lambda - 1) = n$, then G contains $1 + \ell^n\mathbb{Z}_\ell$.*

There is group homomorphism $\mathbb{F}_\ell^\times \to \mathbb{Z}_\ell^\times$, the *Teichmüller lift*, that sends every $\lambda \in \mathbb{F}_\ell^\times$ to the unique $\tilde{\lambda} \in \mathbb{Z}_\ell^\times$ such that $\tilde{\lambda}^\ell = \tilde{\lambda}$ and $\tilde{\lambda} \equiv \lambda \pmod{\ell}$ (such a $\tilde{\lambda}$ exists by Hensel's lemma). The following well-known lemma (see e.g. [Gou97, Corollary 4.5.10]) shows that $\mathbb{Z}_\ell^\times$ is generated by $1 + \ell\mathbb{Z}_\ell$ and by the Teichmüller lifts of all elements of $\mathbb{F}_\ell^\times$, a fact that will be used in Section 3.

Lemma 2.2. *The short exact sequence*

$$1 \to 1 + \ell\mathbb{Z}_\ell \to \mathbb{Z}_\ell^\times \to \mathbb{F}_\ell^\times \to 1$$

is split by the Teichmüller lift.

If m and n are positive integers we extend v_ℓ to the additive group of $m \times n$ matrices with coefficients in $\mathbb{Z}_\ell$ as follows: if $A = (a_{ij})_{1 \leqslant i \leqslant m,\, 1 \leqslant j \leqslant n} \in \mathrm{Mat}_{m \times n}(\mathbb{Z}_\ell)$ we let $v_\ell(A) := \min\{v_\ell(a_{ij}) \mid 1 \leqslant i \leqslant m,\, 1 \leqslant j \leqslant n\}$. The following is proven by an immediate induction on $v_\ell(n)$:

Lemma 2.3. *Let s be a positive integer and let $h \in \mathrm{GL}_s(\mathbb{Z}_\ell)$. If $v_\ell(h - \mathrm{Id}) > 0$, then $v_\ell(h^n - \mathrm{Id}) > v_\ell(n)$ for all positive integers n.*

2.2 Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

We recall the definition and basic properties of Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ when ℓ is an odd prime.

Definition 2.4. Let $\ell > 2$ be a prime and let $\delta \in \mathbb{F}_\ell^\times$. We call

$$C_\ell(\delta) := \left\{ \begin{pmatrix} x & \delta y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{F}_\ell,\, x^2 - \delta y^2 \neq 0 \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$$

the *Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *with parameter* δ. We call $C_\ell(\delta)$ *split* if δ is a square in $\mathbb{F}_\ell$, and *nonsplit* otherwise. We also denote by $N_\ell(\delta)$ the normalizer of $C_\ell(\delta)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Remark 2.5. Let $\lambda \in \mathbb{F}_\ell^\times$. Conjugating $C_\ell(\delta)$ by $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ gives $C_\ell(\delta\lambda^2)$, so that a Cartan subgroup is determined (up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$) by the class of $\delta \in \mathbb{F}_\ell^\times / \mathbb{F}_\ell^{\times 2}$, that is, only by whether or not δ is a square in $\mathbb{F}_\ell^\times$.

Lemma 2.6 ([LP17, Lemma 14])**.** *Let $\ell > 2$ be a prime and let $\delta \in \mathbb{F}_\ell^\times$. The Cartan subgroup $C_\ell(\delta)$ has index 2 in $N_\ell(\delta)$. More precisely, we have*

$$N_\ell(\delta) = C_\ell(\delta) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot C_\ell(\delta)\,.$$

Remark 2.7. Let $\ell > 2$ be a prime and let $\delta \in \mathbb{F}_\ell^\times$. Considering the matrix $g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, whose inverse is $\frac{1}{2}g$, one sees that $C_\ell(1)$ is conjugate to the subgroup

$$C_\ell^*(1) := gC_\ell(1)g^{-1} = \left\{ \begin{pmatrix} t & 0 \\ 0 & w \end{pmatrix} \mid t, w \in \mathbb{F}_\ell^\times \right\}$$

of $\mathrm{GL}_2(\mathbb{F}_\ell)$, whereas for $\delta \neq 1$ it is conjugate to

$$C_\ell^*(\varepsilon) := gC_\ell(\delta)g^{-1} = \left\{ \begin{pmatrix} x + \varepsilon w & -w \\ w & x - \varepsilon w \end{pmatrix} \mid x, w \in \mathbb{F}_\ell,\, x^2 + (1 - \varepsilon^2)w^2 \neq 0 \right\}$$

where $\varepsilon = \frac{\delta+1}{\delta-1}$. Similarly, $N_\ell(\delta)$ is conjugate to

$$N_\ell^*(\varepsilon) = C_\ell^*(\varepsilon) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot C_\ell^*(\varepsilon)\,,$$

which is the normalizer of $C_\ell^*(\varepsilon)$.

2.3 Subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$

Since we will need to rely on it several times throughout the paper, we remind the reader of the well-known classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, traditionally attributed to Dickson. For $\ell = 2$ the group $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to S_3, so its subgroup structure is well-known. Assume now that $\ell > 2$. Recall that a subgroup G of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is said to be *Borel* if it is conjugate to the subgroup of upper-triangular matrices, and is said to be *exceptional* if its image in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is isomorphic to A_4, S_4 or A_5. Also recall the definition of Cartan subgroups from the previous section.

Theorem 2.8 (Dickson's classification, cf. [Ser72, §2])**.** *Let $\ell > 2$ be a prime number and G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

- *If ℓ divides the order of G, then G either contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ or is contained in a Borel subgroup.*
- *If ℓ does not divide the order of G, then G is contained in the normaliser of a (split or nonsplit) Cartan subgroup or in an exceptional group.*

To handle the profinite groups that arise as Galois representations attached to elliptic curves we will find it useful to employ a notion first introduced by Serre [Ser97, IV-25]. We say that a non-abelian finite simple group Σ *occurs* in the profinite group Y if there exist a closed subgroup Y_1 of Y and an open normal subgroup Y_2 of Y_1 such that $\Sigma \cong Y_1/Y_2$. We notice in particular that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ occurs in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We will also need the following fact: for every exact sequence of profinite groups $1 \to N \to G \to G/N \to 1$ and every non-abelian finite simple group Σ, if Σ occurs in G then it occurs in at least one of N and G/N (and conversely), see again [Ser97, IV-25].

2.4 Galois representations and torsion fields of elliptic curves

Let K be a number field and E/K be a fixed elliptic curve. We will say that E is *non-CM* if $\mathrm{End}_{\overline{K}}(E)$ is $\mathbb{Z}$, or equivalently, if E does not have CM over $\overline{K}$. We will denote by E_{tors} the group of all torsion points in $E(\overline{K})$. Consider, for each positive integer N, the natural Galois representation

$$\rho_N : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{Aut}(E[N])$$

afforded by the N-torsion points of $E(\overline{K})$. We will often assume that a basis of the free $\mathbb{Z}/N\mathbb{Z}$-module $E[N]$ has been fixed, and therefore regard the image G_N of ρ_N as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

We denote by K_N the field fixed by the kernel of ρ_N, or equivalently the Galois extension of K generated by the coordinates of all N-torsion points of E. When $N = \ell^n$ is a prime power, by passing to the limit in n we also obtain the group $G_{\ell^\infty} = \mathrm{Gal}\left(K(E[\ell^\infty]) \mid K\right)$, which we consider as a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and the corresponding fixed field $K_{\ell^\infty} = \bigcup_{n\geqslant 1} K_{\ell^n}$. Finally, we also denote by K_∞ the field generated by the various K_{ℓ^∞} as ℓ varies. One can also define the adelic Tate module $TE := \varprojlim_N E[N]$, isomorphic to $\widehat{\mathbb{Z}}^2$, and the adelic Galois representation $\rho_\infty : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{Aut}(TE)$. The Galois group $\mathrm{Gal}(K_\infty \mid K)$ is then isomorphic to the image G_∞ of ρ_∞ (hence to the inverse limit $\varprojlim_N \mathrm{Im}\,\rho_N$), and may be considered – up to the choice of an isomorphism $TE \cong \widehat{\mathbb{Z}}^2$ – as a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Finally we remark that, since all the representations ρ_N are continuous and $\mathrm{Gal}(\overline{K} \mid K)$ is a compact Hausdorff topological group, all the groups just introduced are compact, and therefore closed in their respective ambient spaces.

2.5 Modulo ℓ Galois representations of elliptic curves over $\mathbb{Q}$

Our focus will be on elliptic curves defined over the field of rational numbers. The Galois representations attached to such curves have been studied extensively, and a number of powerful results on their possible images have been proven. We will in particular need to rely on a famous theorem of Mazur concerning the degrees of cyclic isogenies of elliptic curves defined over $\mathbb{Q}$. To state it, let

$$\mathcal{T}_0 := \{p \text{ prime } \mid p \leqslant 17\} \cup \{37\}.$$

Theorem 2.9 ([MG78, Theorem 1])**.** *Let p be a prime number and $E/\mathbb{Q}$ be an elliptic curve, and assume that E has a $\mathbb{Q}$-rational subgroup of order p. Then $p \in \mathcal{T}_0 \cup \{19, 43, 67, 163\}$. If E does not have CM over $\overline{\mathbb{Q}}$, then $p \in \mathcal{T}_0$.*

3 Scalars in the image of Galois representations

Let E be an elliptic curve over a number field K and let ℓ be a prime number. Our purpose in this section is to study the intersection $G_{\ell^\infty} \cap \mathbb{Z}_\ell^\times \cdot \mathrm{Id}$, that is, the subgroup of scalar matrices in the image of the ℓ-adic Galois representation attached to E/K. We will focus mostly, but not exclusively, on the case $K = \mathbb{Q}$. The main result is Theorem 3.16, which – for each prime ℓ – describes a subgroup of $\mathbb{Z}_\ell^\times \cdot \mathrm{Id}$ that is guaranteed to be contained in G_{ℓ^∞} for all non-CM elliptic curves over $\mathbb{Q}$ (see also Proposition 3.18 for the CM case). To simplify the notation,

we will often identify $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ (resp. $\mathbb{Z}_\ell^\times$) with the subgroup $(\mathbb{Z}/\ell^n\mathbb{Z})^\times \cdot \mathrm{Id}$ (resp. $\mathbb{Z}_\ell^\times \cdot \mathrm{Id}$) of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z}_\ell)$).

Since it helps understanding the relevance of the criteria in the next subsection, we briefly contextualise the group-theoretic properties we are going to consider in terms of the Galois representations attached to elliptic curves over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve and let G_{ℓ^∞} (respectively G_ℓ) be the image of the corresponding ℓ-adic (respectively mod ℓ) Galois representation. To begin with, one has $\det(G_{\ell^\infty}) = \mathbb{Z}_\ell^\times$, because for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ the determinant of $\rho_{\ell^\infty}(\sigma)$ is simply $\chi_{\ell^\infty}(\sigma)$, and it is well-known that the ℓ-adic cyclotomic character χ_{ℓ^∞} is surjective. Moreover, when E is non-CM and $\ell \notin \mathcal{T}_0$, by Theorem 2.9 we know that G_ℓ acts irreducibly on $E[\ell]$; in particular, this holds for all $\ell > 37$. We prove in Lemma 3.6 below that if G_ℓ acts irreducibly on $E[\ell]$ and $\ell \mid \#G_\ell$ then $G_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$, so the most interesting case (for ℓ large) is $\ell \nmid \#G_\ell$. In this case [Zyw15a, Proposition 1.13] (or equivalently [LFL21, Appendix B]) shows that (up to conjugacy) there are only two possibilities for G_ℓ, namely a non-split Cartan subgroup or the unique index-3 subgroup thereof. These are therefore the most interesting situations, and are explored in Corollary 3.7. Finally, notice that the image of a complex conjugation in G_{ℓ^∞} is a matrix of order 2 with determinant -1, so – up to conjugation – when $\ell > 2$ we may assume that it is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This explains the relevance of this specific matrix for the statement of Proposition 3.4.

3.1 Group-theoretic criteria

In this section we establish several criteria that guarantee that a closed subgroup G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ contains an (explicit) open subgroup of $\mathbb{Z}_\ell^\times$. A further result of the same kind, whose proof is however more involved, is stated and proved in Appendix 2.A. The criteria in this section will be expressed in terms of G_ℓ, the image of G under reduction modulo ℓ. More generally, we will employ the following notation:

Notation. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We denote by G_{ℓ^n} the image of G under the reduction map $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Lemma 3.1. *Let ℓ be a prime and let $g \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ be such that $g \equiv \lambda\,\mathrm{Id} \pmod{\ell}$ for some $\lambda \in \mathbb{F}_\ell^\times$. Let moreover $\tilde{\lambda} \in \mathbb{Z}_\ell^\times$ be the Teichmüller lift of λ. Then the sequence $\{g^{\ell^n}\}_{n\geqslant 1}$ converges to $\tilde{\lambda}\,\mathrm{Id} \in \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Proof. By Lemma 2.2 we can write $g = \tilde{\lambda}h$, where $h = \mathrm{Id} + \ell h_1 \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ is congruent to the identity modulo ℓ. Then for any $n \geqslant 1$ we have $g^{\ell^n} = \tilde{\lambda}^{\ell^n} h^{\ell^n} = \tilde{\lambda} h^{\ell^n}$. By Lemma 2.3 we have that $v_\ell((\mathrm{Id} + \ell h_1)^{\ell^n} - \mathrm{Id}) > n$ for every $n \geqslant 0$. This

means that the sequence $\{h^{\ell^n}\}_{n\geqslant 1}$ converges to Id, hence $\left\{g^{\ell^n}\right\}_{n\geqslant 1}$ converges to $\tilde{\lambda}\,\mathrm{Id}$. □

Corollary 3.2. *Let ℓ be a prime and let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Suppose that the image of G in $\mathrm{GL}_2(\mathbb{F}_\ell)$ contains $\lambda\,\mathrm{Id}$ for some $\lambda \in \mathbb{F}_\ell^\times$. Then G contains $\tilde{\lambda}\,\mathrm{Id}$.*

Proof. Let $g \in G$ reduce to $\lambda\,\mathrm{Id}$ modulo ℓ. By the previous lemma the sequence $\{g^{\ell^n}\}$ converges to $\tilde{\lambda}\,\mathrm{Id}$, so this is an element of G since by assumption G is closed. □

The following result can be found in [Zyw11, Lemma 2.5], but we include the proof here for ease of reference.

Lemma 3.3. *Let n be a positive integer, let $\ell > 2$ be a prime and let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let*

$$H_n := \{g \in G \mid g \equiv \mathrm{Id} \pmod{\ell^n}\}.$$

If $\det(G) = \mathbb{Z}_\ell^\times$ and $\ell \nmid \#G_\ell$, then $\det(H_n) = 1 + \ell^n\mathbb{Z}_\ell$.

Proof. Clearly $\det(H_n) \subseteq 1 + \ell^n\mathbb{Z}_\ell$, so we only need to prove the other inclusion. Since $\det(G) = \mathbb{Z}_\ell^\times$ there is $g \in G$ such that $\det(g) = 1 + \ell$. Then by Lemma 2.3 the element $h := g^{\ell^{n-1}\cdot \#G_\ell}$ satisfies $h \equiv \mathrm{Id} \pmod{\ell^n}$, so it belongs to H_n. Moreover

$$\det(h) = (1+\ell)^{\ell^{n-1}\cdot \#G_\ell} \equiv 1 + \#G_\ell \ell^n \pmod{\ell^{n+1}}$$

and since $\ell \nmid \#G_\ell$ we have $v_\ell(\det(h) - 1) = n$. By Lemma 2.1 we conclude that $\det(H)$ contains $1 + \ell^n\mathbb{Z}_\ell$. □

We now come to our criterion for the existence of scalars in G when $\ell \nmid \#G_\ell$.

Proposition 3.4. *Let $\ell > 2$ be a prime and G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ such that $\det G = \mathbb{Z}_\ell^\times$. Assume that G_ℓ contains $\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and that $\ell \nmid \#G_\ell$.*

1. *Suppose that G_ℓ contains an element u for which one of the following holds:*
   (a) *u anti-commutes with τ, that is, $u\tau = -\tau u$;*
   (b) *there exists $\varepsilon \in \mathbb{F}_\ell^\times \setminus \{1\}$ such that for all antidiagonal matrices $A = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ we have $uAu^{-1} = \begin{pmatrix} 0 & \varepsilon x \\ \varepsilon^{-1} y & 0 \end{pmatrix}$.*

   Then G contains $1 + \ell\mathbb{Z}_\ell$.

2. *Suppose that one of the assumptions of (1) holds, and that moreover G_ℓ contains $\mathbb{F}_\ell^\times$. Then G contains $\mathbb{Z}_\ell^\times$.*

Remark 3.5. It is immediate to check that the following elements of $\mathrm{GL}_2(\mathbb{F}_\ell)$ have the property required to apply part (1):

(1a) $u = \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}$, where $a, b \in \mathbb{F}_\ell$ are such that $\det(u) = b^2 - a^2 \neq 0$.

(1b) $u = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a, b \in \mathbb{F}_\ell^\times$, $a \neq b$.

Proof. By Lemma 2.1 the element $1 + \ell$ generates $1 + \ell\mathbb{Z}_\ell$, so it suffices to prove that $(1 + \ell)\,\mathrm{Id}$ is in G. For this it suffices to show that $(1 + \ell)\,\mathrm{Id}$ is in G_{ℓ^n} for every $n \geqslant 1$. We prove this by induction. For $n = 1$ the statement holds trivially, so assume that $(1 + \ell)\,\mathrm{Id}$ belongs to G_{ℓ^n} and let $C = (1 + \ell)\,\mathrm{Id} + \ell^n B$ be a lift of this element to $G_{\ell^{n+1}}$, which exists because the map $G_{\ell^{n+1}} \to G_{\ell^n}$ is surjective. Notice that we may consider B as an element of $\mathrm{Mat}_{2\times 2}(\mathbb{F}_\ell)$. In addition, if $n = 1$, thanks to Lemma 3.3 we may assume that $\det(C) \not\equiv 1 \pmod{\ell^2}$, and consequently that $\mathrm{tr}(B) \not\equiv -2 \pmod{\ell}$. If $\tilde{\tau}$ is any lift of τ to $G_{\ell^{n+1}}$, the element

$$\begin{aligned} C' := C\tilde{\tau}C\tilde{\tau}^{-1} &= \left((1 + \ell)\,\mathrm{Id} + \ell^n B\right)\left((1 + \ell)\,\mathrm{Id} + \ell^n \tilde{\tau}B\tilde{\tau}^{-1}\right) \\ &= (1 + \ell)^2\,\mathrm{Id} + (1 + \ell)\ell^n(B + \tilde{\tau}B\tilde{\tau}^{-1}) + \ell^{2n}B\tilde{\tau}B\tilde{\tau}^{-1} \\ &\equiv (1 + \ell)^2\,\mathrm{Id} + \ell^n(B + \tilde{\tau}B\tilde{\tau}^{-1}) \pmod{\ell^{n+1}} \end{aligned}$$

is in $G_{\ell^{n+1}}$. Notice that $D := B + \tau B\tau^{-1}$ is congruent to $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ modulo ℓ, where $a = \mathrm{tr}(B)$ and $b \in \mathbb{F}_\ell$.

- Suppose that G_ℓ contains an element u as in part (1a). Then

$$uDu^{-1} \equiv \begin{pmatrix} a & -b \\ -b & a \end{pmatrix} \pmod{\ell}.$$

If $\tilde{u} \in G_{\ell^{n+1}}$ is a lift of u, the group $G_{\ell^{n+1}}$ contains

$$\begin{aligned} C'\tilde{u}C'\tilde{u}^{-1} &\equiv \left((1 + \ell)^2\,\mathrm{Id} + \ell^n D\right)\left((1 + \ell)^2\,\mathrm{Id} + \ell^n \tilde{u}D\tilde{u}^{-1}\right) \\ &\equiv \left((1 + \ell)^2\,\mathrm{Id} + \ell^n \begin{pmatrix} a & b \\ b & a \end{pmatrix}\right)\left((1 + \ell)^2\,\mathrm{Id} + \ell^n \begin{pmatrix} a & -b \\ -b & a \end{pmatrix}\right) \\ &\equiv (1 + \ell)^4\,\mathrm{Id} + 2a\ell^n\,\mathrm{Id} \pmod{\ell^{n+1}} \end{aligned}$$

which is a scalar matrix congruent to $1 + 4\ell$ modulo ℓ^2 if $n > 1$ or to $1 + 2\ell(2 + a)$ if $n = 1$.

- Suppose that G_ℓ contains an element u as in part (1b). Then we have

$$D_k := u^k D u^{-k} = \begin{pmatrix} a & b\varepsilon^k \\ b\varepsilon^{-k} & a \end{pmatrix}.$$

Letting $\tilde{u}$ be a lift of u to $G_{\ell^{n+1}}$ we obtain that for every non-negative integer k the group $G_{\ell^{n+1}}$ contains

$$\tilde{u}^k C' \tilde{u}^{-k} = (1+\ell)^2 \operatorname{Id} + \ell^n D_k.$$

Thus, using the fact that $\sum_{k=0}^{\ell-2} \varepsilon^k = \frac{\varepsilon^{\ell-1}-1}{\varepsilon-1} = 0$, we see that $G_{\ell^{n+1}}$ also contains

$$\begin{aligned} \prod_{k=0}^{\ell-2} \tilde{u}^k C' \tilde{u}^{-k} &\equiv \prod_{k=0}^{\ell-2} \left((1+\ell)^2 \operatorname{Id} + \ell^n D_k\right) \pmod{\ell^{n+1}} \\ &\equiv (1+\ell)^{2(\ell-1)} \operatorname{Id} + \ell^n (1+\ell)^{2(\ell-2)} \sum_{k=0}^{\ell-2} D_k \pmod{\ell^{n+1}} \\ &\equiv (1+\ell)^{2(\ell-1)} \operatorname{Id} - \ell^n \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \pmod{\ell^{n+1}}, \end{aligned}$$

which is a scalar matrix congruent to $1-2\ell$ modulo ℓ^2 if $n > 1$ or to $1-(2+a)\ell$ if $n = 1$.

In any case, using our assumption that $a = \operatorname{tr}(B) \not\equiv -2 \pmod{\ell}$ if $n = 1$, we see that $G_{\ell^{n+1}}$ contains a scalar matrix $\lambda \operatorname{Id}$ with $v_\ell(\lambda - 1) = 1$. We can now apply Lemma 2.1 to the subgroup of $\mathbb{Z}_\ell^\times$ given by the inverse image of $G_{\ell^{n+1}} \cap (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^\times$ under the natural projection, and we conclude that $(1+\ell)\operatorname{Id} \in G_{\ell^{n+1}}$ as desired.

Finally, if $\mathbb{F}_\ell^\times$ is contained in G_ℓ, Lemma 3.1 shows that G contains a Teichmüller lift of every element of $\mathbb{F}_\ell^\times$. By Lemma 2.2 this is enough to conclude that G contains $\mathbb{Z}_\ell^\times$. □

Lemma 3.6. *Let $\ell \geqslant 5$ be a prime number and G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Suppose that $\det(G) = \mathbb{Z}_\ell^\times$. If $\ell \mid \#G_\ell$ and G_ℓ acts irreducibly on $\mathbb{F}_\ell^2$, then $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Proof. Since $\ell \mid \#G_\ell$, the classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ (Theorem 2.8) shows that either G_ℓ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. However, any subgroup of a Borel acts reducibly on $\mathbb{F}_\ell^2$ by definition, hence we see that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. By a lemma due to Serre (see [Ser97, IV-23, Lemme 3] and [Lom15, Lemma 3.15] for this exact version), this implies that G contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$. From $\det(G) = \mathbb{Z}_\ell^\times$ we then obtain $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$ as desired. □

Corollary 3.7. *Let $\ell > 2$ be a prime and let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with $\det(G) = \mathbb{Z}_\ell^\times$. Suppose that (at least) one of the following holds:*

1. *$G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ contains (up to conjugacy) the normaliser of a split or non-split Cartan, and if $\ell \mid \#G_\ell$ then $\ell \neq 3$.*
2. *$\ell \equiv 2 \pmod 3$, and $G_\ell \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ contains (up to conjugacy) the subgroup of cubes in the normaliser of a non-split Cartan.*

Then G contains $\mathbb{Z}_\ell^\times$.

Proof. Suppose first that $\ell \mid \#G_\ell$ (hence in particular $\ell > 3$). The normaliser of a (split or non-split) Cartan, or an index-3 subgroup of a non-split Cartan, acts irreducibly on $\mathbb{F}_\ell^2$, so Lemma 3.6 implies $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$, which in particular contains $\mathbb{Z}_\ell^\times$.

Suppose on the other hand that $\ell \nmid \#G_\ell$. Notice that – since the scalar matrices are contained in the centre of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ – the conclusion of Proposition 3.4 is invariant under a change of basis for $\mathbb{Z}_\ell^2$, so it suffices to check that the group G satisfies the hypotheses of Proposition 3.4 after a suitable change of basis.

1. By what we already remarked, and up to conjugation in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we may assume that G_ℓ contains the group $N_\ell^*(\varepsilon)$ described in Remark 2.7, or an index-3 subgroup thereof. The explicit description shows that every group of the form $N_\ell^*(\varepsilon)$ contains $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; since this matrix is equal to its cube, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is also contained in the subgroup of cubes in $N_\ell^*(\varepsilon)$.

   The normaliser of a split Cartan subgroup contains all anti-diagonal matrices, hence in particular it contains $u = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The normaliser of a non-split Cartan contains $u = \begin{pmatrix} \varepsilon & -1 \\ 1 & -\varepsilon \end{pmatrix}$. Finally, the subgroup of cubes of such a normaliser contains $\begin{pmatrix} \varepsilon & -1 \\ 1 & -\varepsilon \end{pmatrix}^3 = (\varepsilon^2 - 1)\begin{pmatrix} \varepsilon & -1 \\ 1 & -\varepsilon \end{pmatrix}$. In all cases we have thus shown that G_ℓ contains an element of the form required to apply Proposition 3.4 (1), see Remark 3.5.

2. As for hypothesis (2) of Proposition 3.4, observe that all scalar matrices are contained in the normaliser of every (split or non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. When $\ell \equiv 2 \pmod 3$ they are also contained in the subgroup of cubes of a non-split Cartan: indeed, in this case $x \mapsto x^3$ is an automorphism of $\mathbb{F}_\ell^\times$, so every scalar matrix is a cube.

□

3.2 Scalars in the presence of an isogeny

We now specialise to the case of $G = G_{\ell^\infty} \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ being the image of the ℓ-adic representation attached to an elliptic curve $E/\mathbb{Q}$. Our aim is again to prove that G contains an (explicitly identifiable) subgroup of $\mathbb{Z}_\ell^\times$. We begin by considering the case when $\ell \geqslant 7$ and E admits an isogeny of degree ℓ defined over $\mathbb{Q}$. The relevant results are essentially already in the literature, and in this short section we reformulate them in the form needed for our applications.

Definition 3.8 ([GRSS14, Definition 1.1])**.** Let ℓ be a prime. An elliptic curve E over $\mathbb{Q}$ is called **ℓ-exceptional** if E has an isogeny of degree ℓ defined over $\mathbb{Q}$ and G_{ℓ^∞} does not contain a Sylow pro-ℓ subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Combining [Gre12, Theorem 1] with [Gre12, Remark 4.2.1] and [GRSS14, Theorem 5.5] one obtains:

Theorem 3.9. *Let $\ell \geqslant 7$ be a prime. There are no non-CM ℓ-exceptional elliptic curves defined over $\mathbb{Q}$.*

For the case $\ell = 5$ we instead rely on the following result:

Theorem 3.10 ([Gre12, Theorem 2])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Suppose that E has an isogeny of degree 5 defined over $\mathbb{Q}$. If none of the elliptic curves in the $\mathbb{Q}$-isogeny class of E has two independent isogenies of degree 5, then E is not 5-exceptional. Otherwise, the index $[\mathrm{GL}_2(\mathbb{Z}_5) : G_{5^\infty}]$ is divisible by 5, but not by 25.*

Corollary 3.11. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, let $\ell \geqslant 5$ be a prime number, and suppose that the Galois module $E[\ell]$ is reducible. Then G_{ℓ^∞} contains $1 + \ell\mathbb{Z}_\ell$.*

Proof. A specific Sylow pro-ℓ subgroup S of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is given by

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; a \equiv d \equiv 1 \pmod{\ell},\ c \equiv 0 \pmod{\ell} \right\}.$$

It is clear that $1 + \ell\mathbb{Z}_\ell$ is contained in S. However, since all the pro-ℓ Sylow subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ are conjugate to each other and $1+\ell\mathbb{Z}_\ell$ lies in the center of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (hence is stable under conjugation), it follows that $1 + \ell\mathbb{Z}_\ell$ is contained in *all* the Sylow pro-ℓ subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. For $\ell \geqslant 7$ the statement then becomes a direct consequence of Theorem 3.9. For $\ell = 5$ the claim similarly follows from Theorem 3.10 if no elliptic curve in the $\mathbb{Q}$-isogeny class of E admits two independent 5-isogenies. To treat this last case, observe that the intersection $G_{\ell^\infty} \cap \mathbb{Z}_\ell^\times$ is the same for all the elliptic curves in a given $\mathbb{Q}$-isogeny class (see e.g. [Gre12, §2.4]), so we may assume that E admits two independent 5-isogenies

defined over $\mathbb{Q}$. In particular, the Galois module $E[5]$ decomposes as the direct sum of two 1-dimensional modules, which implies that in a suitable basis G_5 consists of diagonal matrices. Hence $[\mathrm{GL}_2(\mathbb{F}_5) : G_5]$ is divisible by 5, and on the other hand $25 \nmid [\mathrm{GL}_2(\mathbb{Z}_5) : G_{5^\infty}]$ by Theorem 3.10 again. It follows immediately that $\ker(\mathrm{GL}_2(\mathbb{Z}_5) \to \mathrm{GL}_2(\mathbb{F}_5))$, which is a pro-5 group, is entirely contained in G_{5^∞}, hence in particular that $1 + 5\mathbb{Z}_5 \subseteq G_{5^\infty}$, as desired. □

3.3 The 3-adic case

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Relying on the group-theoretic results of Appendix 2.A we now prove that the 3-adic Galois representation attached to E contains all scalars congruent to 1 modulo 27. We treat separately the two cases when the Galois module $E[3]$ is respectively irreducible or reducible.

Irreducible case

When $E[3]$ is irreducible for the Galois action, it is not hard to prove that G_{3^∞} contains all scalars:

Proposition 3.12. *Suppose $E[3]$ is an irreducible Galois module. Then G_{3^∞} contains $\mathbb{Z}_3^\times$.*

Proof. Up to conjugation, we can assume that G_3 contains $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (the image of complex conjugation). A short direct computation shows that (up to conjugacy) there are only 3 possibilities for G_3, namely $\mathrm{GL}_2(\mathbb{F}_3)$, a 2-Sylow subgroup, or the group $H := \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$ of order 8. In particular, in all cases we may assume that $H \subseteq G_3$. The hypotheses of Proposition 3.4 (2) are then satisfied, hence G_{3^∞} contains $\mathbb{Z}_3^\times$. □

Reducible case

We now consider the much harder case when $E[3]$ is reducible under the Galois action. Our analysis is based on the purely group-theoretic Proposition 2.A.1. To motivate the hypotheses that appear in its statement, we consider a non-CM elliptic curve $E/\mathbb{Q}$ for which the Galois module $E[3]$ is reducible, and denote as usual by G_{3^n} the image of the modulo-3^n representation attached to $E/\mathbb{Q}$ and by G_{3^∞} the image of the 3-adic representation. The following hold:

1. Any elliptic curve $\tilde{E}/\mathbb{Q}$ that is $\mathbb{Q}$-isogenous to E gives rise to a 3-adic Galois image $\tilde{G}_{3^\infty}$ for which $G_{3^\infty} \cap \mathbb{Z}_3^\times = \tilde{G}_{3^\infty} \cap \mathbb{Z}_3^\times$ (notice that this equality is independent of the choice of basis for $T_3E, T_3\tilde{E}$), see for example [Gre12,

§2.4]. For all such curves $\tilde{E}/\mathbb{Q}$, the Galois module $\tilde{E}[3]$ is clearly reducible, and at least one $\tilde{E}$ of this form does not admit two independent cyclic isogenies of degree 3 defined over $\mathbb{Q}$. Hence, up to replacing E with $\tilde{E}$, we may assume that G_3 is contained (up to conjugacy) in a Borel subgroup and that G_3 only fixes one nontrivial $\mathbb{F}_3$-subspace of $E[3]$. This implies $3 \mid \#G_3$.

2. G_{27} acts on $E[27]$ without fixing any cyclic subgroup of order 27. Indeed, the three rational points on $X_0(27)$ are two cusps and a single non-cuspidal point corresponding to a CM elliptic curve [Ogg73, p. 229].

3. $\det(G_{3^\infty}) = \mathbb{Z}_3^\times$: as already discussed, this follows from the surjectivity of the 3-adic cyclotomic character.

4. G_{3^∞} contains the image of (any) complex conjugation, which is an element c of order 2 with determinant -1.

We now check that this information is sufficient to apply Proposition 2.A.1. Up to a change of basis, we may assume that the element $c \in G_{3^\infty}$ is represented by the matrix $C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. This easily implies that G_3 is contained in the Borel of upper- or lower-triangular matrices (see also Remark 2.A.4). Take now H to be the pro-3 Sylow subgroup of G_{3^∞} (which is normal, hence unique: it is the inverse image in G_{3^∞} of the 3-Sylow of G_3, which is easily checked to be normal). We claim that this group satisfies all the assumptions of Proposition 2.A.1 with $p = 3$ and $k = 3$. Hypothesis (1) is satisfied by (1) above. Hypothesis (3) is clear from the equality $\det(G_{3^\infty}) = \mathbb{Z}_3^\times$, and (4) follows from the fact that $C \in G_{3^\infty}$ and H is normal in G_{3^∞}. As for (2), recall that G_3 is contained in the upper- or lower-triangular Borel subgroup, and this implies easily that G_{3^∞} is generated by H, C, and possibly $-\mathrm{Id}$. Since both C and $-\mathrm{Id}$ are diagonal, we see that if H_{3^3} is upper- or lower- triangular, then so is G_{3^3}, contradiction, because we know that E does not admit any cyclic 27-isogeny defined over $\mathbb{Q}$. Hence from Proposition 2.A.1 we obtain:

Proposition 3.13. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve for which $E[3]$ is a reducible Galois module. Then G_{3^∞} contains all scalars congruent to* 1 *modulo* 27*.*

Combining this result with Proposition 3.12 we have then proved:

Corollary 3.14. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. The group G_{3^∞} contains all scalars congruent to* 1 *modulo* 27*.*

Remark 3.15. The results of [RSZB21], which appeared almost simultaneously to the present work, imply that for every non-CM elliptic curve over $\mathbb{Q}$ with a

rational 3-isogeny the group G_{3^∞} contains all scalars congruent to 1 modulo 9 (hence, by Proposition 3.12, the same holds for every non-CM $E/\mathbb{Q}$). The proof in [RSZB21] relies on the explicit determination of the rational points of suitable modular curves. As pointed out in the introduction, we think our approach – which derives the result from properties of isogenies (hence relying only on the more well-studied modular curves $X_0(N)$) – has the advantage of being easier to extend to number fields different from $\mathbb{Q}$.

3.4 Main theorem

We are now ready to prove our uniform result for scalars in the image of Galois representations:

Theorem 3.16. *Let E be a non-CM elliptic curve over $\mathbb{Q}$ and let ℓ be a prime number. Define*

$$s_\ell := \begin{cases} 4, & \text{if } \ell = 2 \\ 3, & \text{if } \ell = 3 \\ 1, & \text{if } \ell = 5, 7, 11, 13, 17, 37 \\ 0, & \text{if } \ell \geqslant 19 \text{ and } \ell \neq 37 \end{cases}$$

The image G_{ℓ^∞} of the ℓ-adic Galois representation attached to $E/\mathbb{Q}$ contains all scalars congruent to 1 modulo ℓ^{s_ℓ}.

Proof. For $\ell = 2$ and $\ell = 3$ the theorem follows from the results of [RZB15] and Corollary 3.14 respectively. We may therefore assume $\ell \geqslant 5$. We distinguish several cases:

1. the G_ℓ-module $E[\ell]$ is reducible. The claim follows from Corollary 3.11.
2. the G_ℓ-module $E[\ell]$ is irreducible and $\ell \mid \#G_\ell$. By Lemma 3.6 we obtain $G_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$, and the claim follows.
3. the G_ℓ-module $E[\ell]$ is irreducible and $\ell \nmid \#G_\ell$. Suppose first that $\ell \geqslant 17$: then the claim follows from [Zyw15a, Proposition 1.13] (the exceptional j-invariants correspond to elliptic curves for which G_ℓ does not act irreducibly on $E[\ell]$, see [Zyw15a, Theorem 1.10]). For $\ell = 5, 7, 11$, Theorems 1.4, 1.5 and 1.6 in [Zyw15a] completely describe the possible mod-ℓ images G_ℓ. Since G_ℓ acts irreducibly on $E[\ell]$ by assumption, we need to consider the following cases:
   (a) for $\ell = 5$, up to conjugacy the group G_ℓ contains either the index-3 subgroup of a non-split Cartan or the full normaliser of a split Cartan. In both cases we may apply Corollary 3.7. Similarly, for $\ell = 11$, up

to conjugacy the only possibility is that G_ℓ is the full normaliser of a non-split Cartan, and again we conclude by Corollary 3.7.

(b) for $\ell = 7$, up to conjugacy we have that G_ℓ is the normaliser of a (split or non-split) Cartan subgroup, or that it contains $\langle \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \rangle$. The first case is handled as above. In the other case, one checks that G_ℓ contains $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and clearly it contains $\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$, so the hypothesis of Proposition 3.4 (1b) is satisfied (see Remark 3.5) and the claim follows.

This only leaves the prime $\ell = 13$. By [Zyw15a, §1.6], the maximal proper subgroups of $\mathrm{GL}_2(\mathbb{F}_{13})$ not contained in a Borel are (up to conjugacy) the normalisers of (split and non-split) Cartan subgroups and the group

$$G_{S_4} = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \right\rangle.$$

The main result of [BDM$^+$19] (precisely, Theorem 1.1 and Corollary 1.3 in op. cit.) shows that G_{13} is not conjugate to a subgroup of a (split or non-split) Cartan. It remains to understand the case $G_{13} \subseteq G_{S_4}$. Consider the collection $\mathcal{C}$ of subgroups $H \subseteq G_{S_4}$ that satisfy all of the following conditions:

(a) $\det H = \mathbb{F}_{13}^\times$;

(b) H contains an element h with $h^2 = \mathrm{Id}$ and $\mathrm{tr}(h) = 0$;

(c) the projective image $H/(H \cap \mathbb{F}_{13}^\times)$ has exponent at least 3;

(d) H acts irreducibly on $E[13]$.

If E is a non-CM elliptic curve over $\mathbb{Q}$ such that G_{13} is contained (up to a choice of basis for $E[13]$) in G_{S_4} and not contained in a Borel subgroup, then G_{13} is a member of $\mathcal{C}$: (a) follows from the surjectivity of the mod-13 cyclotomic character over $\mathbb{Q}$, (b) holds because the image of complex conjugation has these properties, (c) holds by [Dav11, Lemma 2.4], and (d) is true by definition. One checks easily that all the groups H in class $\mathcal{C}$ contain both $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, hence once again Proposition 3.4 (1) applies to show that $1 + 13\mathbb{Z}_{13} \subseteq G_{13^\infty}$, as desired.

□

Remark 3.17. Theorem 1.1 in the very recent preprint [BDM$^+$21], combined with [BC14], gives the finite list of j-invariants of non-CM elliptic curves $E/\mathbb{Q}$

for which G_{13} is contained (up to conjugation) in G_{S_4}. For each of these elliptic curves, the image of G_{13} in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to S_4: while this is not necessary for our proof, it can be used to simplify the case $\ell = 13$ of the previous argument.

We also have a similar result in the CM case:

Proposition 3.18. *Let $E/\mathbb{Q}$ be an elliptic curve with CM and let ℓ be a prime number. Define*

$$n'_\ell = \begin{cases} 3, & \text{if } \ell = 2 \\ 1, & \text{if } \ell = 3, 7, 11, 19, 43, 67, 163 \\ 0, & \text{if } \ell \neq 2, 3, 7, 11, 19, 43, 67, 163 \end{cases}$$

The image G_{ℓ^∞} of the ℓ-adic Galois representation attached to $E/\mathbb{Q}$ contains all scalars congruent to 1 modulo $\ell^{n'_\ell}$. Moreover, for $\ell \geqslant 5$ the image G_{ℓ^∞} contains a scalar not congruent to $\pm 1 \pmod{\ell}$.

Proof. Let K be the imaginary quadratic field of complex multiplication of E, let Δ_K be its discriminant, and let $\mathcal{O}_{K,f}$ be the endomorphism ring of $E_{\overline{\mathbb{Q}}}$, seen as a subring of $\mathcal{O}_K$ (here f denotes the conductor of the order $\mathcal{O}_{K,f}$ in $\mathcal{O}_K$). It is well-known that there are 13 possible pairs (K, f), given by $K = \mathbb{Q}(i)$ and $f = 1, 2$, $K = \mathbb{Q}(\zeta_3)$ and $f = 1, 2, 3$, $K = \mathbb{Q}(\sqrt{-7})$ and $f = 1, 2$, and $K = \mathbb{Q}(\sqrt{-d})$ for $d = 2, 11, 19, 43, 67, 163$ with $f = 1$ (see for example [Sil94, Appendix A, §3]). If $\ell \nmid 2f\Delta_K$, then by [LR18, Theorem 1.2 (4) and Theorem 1.4] the ℓ-adic image G_{ℓ^∞} contains all scalars. If $\ell \mid f\Delta_K$ and $\ell > 2$, then G_{ℓ^∞} contains $\mathbb{Z}_\ell^{\times 2}$ by [LR18, Theorem 1.5]: notice that by the above this is only possible for $\ell = 3, 7, 11, 19, 43, 67, 163$, and that for $\ell \geqslant 7$ the group $\mathbb{Z}_\ell^{\times 2}$ contains scalars not congruent to $\pm 1 \pmod{\ell}$. Finally, for $\ell = 2$ we have by [LR18, Theorems 1.6, 1.7, 1.8] that G_{2^∞} contains all scalars congruent to 1 modulo 8. □

Remark 3.19. A slightly worse result can be obtained more easily (without the need to distinguish cases) by applying [Lom17, Theorem 1.5].

3.5 Complements to Theorem 3.16

For future use, we record here the following modest strengthening of Theorem 3.16:

Proposition 3.20. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Let $\ell \in \{13, 17, 37\}$. The image of the ℓ-adic Galois representation attached to $E/\mathbb{Q}$ contains a scalar λ with $v_\ell(\lambda^2 - 1) = 0$.*

Proof. By Corollary 3.2 it suffices to show that G_ℓ contains a scalar different from ± 1. For $\ell = 17, 37$, this follows directly from the results of [Zyw15a] (specifically, Theorem 1.10 and Proposition 1.13). For $\ell = 13$, by Theorem 2.8 and the fact that G_{13} has surjective determinant we know that G_{13} satisfies one of the following:

1. $G_{13} = \mathrm{GL}_2(\mathbb{F}_{13})$: in this case the conclusion is obvious.

2. G_{13} is contained up to conjugacy in a Borel subgroup: by [Zyw15a, Theorem 1.8], the possible groups that arise in this way all contain a scalar different from ± 1.

3. G_{13} is contained up to conjugacy in the normaliser of a (split or nonsplit) Cartan subgroup: this is impossible by the main result of [BDM$^+$19].

4. the projective image of G_{13} is isomorphic to a subgroup of S_4 or A_5: the claim follows from Lemma 3.21 below.

□

Lemma 3.21. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_{13})$ having projective image isomorphic to a subgroup of S_4 or A_5. Suppose that $\det(G) = \mathbb{F}_{13}^\times$: then G contains a scalar different from $\pm \mathrm{Id}$.*

Proof. The hypothesis implies that the cyclic group $\mathbb{F}_{13}^\times$ is a quotient of G, so G contains an element of order 12. If the claim were false, the projection map $G \to \mathrm{PGL}_2(\mathbb{F}_{13})$ would have kernel of order at most 2. The maximal order of an element in S_4 is 4, and in A_5 is 5. It would follow that the maximal order of an element in G is at most 10, contradiction. □

4 Galois cohomology of torsion points

In this section we show that there exists a universal constant $e > 0$ such that, for all elliptic curves $E/\mathbb{Q}$ and all positive integers M, N with $N \mid M$, the cohomology group $H^1(\mathrm{Gal}(\mathbb{Q}_M \mid \mathbb{Q}), E[N])$ is killed by multiplication by e (which we denote by $[e]$). We also provide an explicit admissible value for e.

We begin by showing that it suffices to consider the cohomology groups $H^1(G_\infty, E[N])$.

Lemma 4.1. *Let E/K be an elliptic curve over a number field K and let M, N be positive integers with $N \mid M$. Suppose that $H^1(G_\infty, E[N])$ is killed by $[e]$: then $H^1(\mathrm{Gal}(K_M \mid K), E[N])$ is also killed by $[e]$.*

Proof. Denote by H the kernel of the natural map $G_\infty \to \mathrm{Gal}(K_M \mid K)$. As H acts trivially on $E[N]$ by the assumption $N \mid M$, the inflation-restriction exact sequence gives an injection of $H^1(G_\infty/H, E[N]) = H^1(\mathrm{Gal}(K_M \mid K), E[N])$ into $H^1(G_\infty, E[N])$, and the claim follows. □

On the other hand, if $H^1(\mathrm{Gal}(K_M \mid K), E[N])$ is killed by $[e]$ for all M divisible by N, passing to the limit in M we also obtain that $[e]$ kills $H^1(G_\infty, E[N])$. The statement we aim for is thus equivalent to saying that, for every $E/\mathbb{Q}$ and positive integer N, the group $H^1(G_\infty, E[N])$ has finite exponent dividing e. Our main tool for bounding the exponent of cohomology groups is the following lemma (see for example [BR03, Lemma A.2] for a proof).

Lemma 4.2 (Sah's Lemma)**.** *Let G be a profinite group, let M be a continuous G-module and let g be in the centre of G. Then the endomorphism $x \mapsto gx - x$ of M induces the zero map on $H^1(G, M)$. In particular, if $x \mapsto gx - x$ is an isomorphism, then $H^1(G, M) = 0$.*

Remark 4.3. In our applications of Lemma 4.2 we will have $G \subseteq \mathrm{GL}_2(R)$ for a certain ring R – either $\mathbb{Z}_\ell$ for some prime ℓ or $\widehat{\mathbb{Z}}$ – and M will be a submodule of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2$ or $(\mathbb{Q}/\mathbb{Z})^2$. Notice that these objects carry a natural action of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ respectively. We will take g to be a scalar multiple of the identity, that is, $g = \lambda\,\mathrm{Id}$ for some $\lambda \in R^\times$. The conclusion is then that the R-module $H^1(G, M)$ is killed by $\lambda - 1$; when $R = \mathbb{Z}_\ell$, this is equivalent to saying that $H^1(G, M)$ is killed by $\ell^{v_\ell(\lambda-1)}$.

Generalising the results of [LW15] we now give a uniform result on the cohomology of torsion points of elliptic curves over $\mathbb{Q}$ for all powers of primes.

Theorem 4.4. *Let ℓ be a prime number and let $E/\mathbb{Q}$ be a non-CM elliptic curve. For every $m \geqslant 1$, the exponent of $H^1(G_{\ell^\infty}, E[\ell^m])$ divides ℓ^{n_ℓ}, where*

$$n_\ell := \begin{cases} 3 & \text{for } \ell = 2, 3, \\ 1 & \text{for } \ell = 5, 7, 11, \\ 0 & \text{for } \ell \geqslant 13\,. \end{cases} \tag{4.1}$$

Proof. For $\ell > 2$ we apply Lemma 4.2 (in the form of Remark 4.3) with $g = \lambda\,\mathrm{Id}$, where $\lambda \in \mathbb{Z}_\ell^\times \cap G_{\ell^\infty}$ is such that $v_\ell(\lambda - 1) = n_\ell$. Note that such a λ exists by Theorem 3.16 and Proposition 3.20.

For $\ell = 2$ the proof is based on the classification of all possible 2-adic images provided by [RZB15], and is in part computational. As G_{2^∞} is the inverse limit of the groups G_{2^n}, it suffices to show that for all integers $n \geqslant m \geqslant 1$ the exponent of $H^1(G_{2^n}, E[2^m])$ divides 8. If G_{2^∞} contains a scalar λ with $v_2(\lambda - 1) \leqslant 3$ the result follows immediately from Lemma 4.2 as above, so let us assume that this is not

the case. This leaves us with only 8 groups left, namely those with Rouse–Zureick-Brown labels X238a, X238b, X238c, X238d, X239a, X239b, X239c, X239d. All of these groups are the inverse images of their reduction modulo 2^5 and contain $17\,\mathrm{Id}$. Let now $\xi : G_{2^n} \to E[2^m]$ be a 1-cocycle and let $\lambda \in G_{2^n}$ be the scalar $17\,\mathrm{Id}$. Notice that there is nothing to prove if $m \leqslant 3$, so we may assume $n \geqslant m \geqslant 4$. Reasoning as in the proof of Sah's lemma, we observe that

$$\xi(\lambda g) = \xi(g\lambda) \Rightarrow (\lambda - 1)\xi(g) = g \cdot \xi(\lambda) - \xi(\lambda).$$

This formula shows both that 16ξ is a coboundary, and that $\xi(\lambda)$ is such that $g \cdot \xi(\lambda) - \xi(\lambda)$ is divisible by 16 in $E[2^m]$. Imposing this condition for g varying in a set of generators of G_{2^∞} (recall that we only have finitely many groups to test) we obtain that $\xi(\lambda)$ is divisible by 8. Let us write $\xi(\lambda) = 8a$ for some (non-unique) $a \in E[2^m]$. As a consequence, we have that for every $g \in G_{2^n}$

$$8 \cdot 2\xi(g) = g \cdot \xi(\lambda) - \xi(\lambda) = 8(g \cdot a - a).$$

Letting ψ be the coboundary $g \mapsto g \cdot a - a$ we then obtain that 2ξ is cohomologous to the cocycle $2\xi - \psi$, which by the above takes values in $E[8]$. A direct verification, for which we give details below, shows that $H^1(G_{2^n}, E[8])$ has exponent dividing 4 for all $n \geqslant 3$. This implies in particular that $4 \cdot (2\xi) : G_{2^n} \to E[8]$ is a coboundary, hence a fortiori $8\xi : G_{2^n} \to E[2^m]$ is also a coboundary, and therefore $[8]$ kills $H^1(G_{2^n}, E[2^m])$ as desired.

To check that $H^1(G_{2^n}, E[8])$ has exponent dividing 4 we proceed as follows. Notice first that by Lemma 4.1 it suffices to show that $[4]$ is zero on $H^1(G_{2^\infty}, E[8])$. On the other hand, consider an element $g \in G_{2^\infty}$ that is the 8-th power of an element h congruent to the identity modulo 8, and let $\xi : G_{2^\infty} \to E[8]$ be any cocycle. As h acts trivially on $E[8]$, the restriction of ξ to the subgroup generated by h is a homomorphism, hence $\xi(g) = \xi(h^8) = 8\xi(h) = 0$. This proves that ξ factors via the finite quotient

$$G_{2^\infty}/\langle g^8 : g \equiv \mathrm{Id} \pmod 8\rangle.$$

For all the cases of interest we know from [RZB15] that G_{2^∞} contains all matrices congruent to 1 modulo 2^5, hence $\langle g^8 : g \equiv \mathrm{Id} \pmod 8\rangle$ contains all matrices congruent to Id modulo 2^8. We are thus reduced to considering the group $Q := G_{2^8}/\langle g^8 : g \equiv \mathrm{Id} \pmod 8\rangle$ and checking that the exponent of $H^1(Q, E[8])$ divides 4, which we do by explicit computations in MAGMA. □

In order to bound the exponent of $H^1(G_\infty, E[N])$ we will apply the following technical result, which is worth stating in a general form.

Proposition 4.5. *Let G_∞ be a closed subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and for every prime ℓ denote by G_{ℓ^∞} the projection of G_∞ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Let J_ℓ be the kernel of the*

projection $G_\infty \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\overline{J}_\ell$ be the image of J_ℓ in $\prod_{p\ prime}\mathrm{GL}_2(\mathbb{F}_p)$. Finally let T be any G_∞-submodule of $(\mathbb{Q}/\mathbb{Z})^2$. Assume that for every prime ℓ there are a positive integer a_ℓ and non-negative integers n_ℓ, m_ℓ such that the following hold:

1. *For all but finitely many primes ℓ we have $v_\ell(a_\ell) = n_\ell = m_\ell = 0$.*
2. *For every prime ℓ the exponent of $H^1(G_{\ell^\infty}, T[\ell^\infty])$ divides ℓ^{n_ℓ}.*
3. *For every prime ℓ there is a scalar $g_\ell \in G_{\ell^\infty}$ such that $v_\ell(g_\ell - 1) \leqslant m_\ell$.*
4. *For every prime ℓ and every $x \in J_\ell$ the image of $[\tilde{g}_\ell, x^{a_\ell}]$ in $\overline{J}_\ell$ is contained in $[\overline{J}_\ell, \overline{J}_\ell]$ for some lift $\tilde{g}_\ell \in G_\infty$ of g_ℓ, where g_ℓ is as above.*

The cohomology group $H^1(G_\infty, T)$ has finite exponent dividing $\prod_\ell \ell^{n_\ell+m_\ell+v_\ell(a_\ell)}$.

Proof. We will write elements x of G_∞ as sequences $(x_p)_p$ indexed by the prime numbers p, where each x_p is in $\mathrm{GL}_2(\mathbb{Z}_p)$. Denoting the ℓ-part of T by $T[\ell^\infty]$ we have

$$T = \bigoplus_\ell T[\ell^\infty]$$

and since cohomology of profinite groups commutes with direct limits (see [Har20, Proposition 4.18]), hence with direct sums, we get

$$H^1(G_\infty, T) \cong \bigoplus_\ell H^1(G_\infty, T[\ell^\infty]).$$

Fix now a prime ℓ. The inflation-restriction exact sequence for $J_\ell \triangleleft G_\infty$ gives

$$0 \to H^1\left(G_{\ell^\infty}, T[\ell^\infty]^{J_\ell}\right) \to H^1\left(G_\infty, T[\ell^\infty]\right) \to H^1(J_\ell, T[\ell^\infty])^{G_{\ell^\infty}}. \tag{4.2}$$

Since J_ℓ acts trivially on $T[\ell^\infty]$ we have

$$T[\ell^\infty]^{J_\ell} = T[\ell^\infty] \quad \text{and} \quad H^1(J_\ell, T[\ell^\infty]) = \mathrm{Hom}(J_\ell, T[\ell^\infty]),$$

and the action of G_{ℓ^∞} on the latter group is given, for every $g \in G_{\ell^\infty}$, every $\varphi \in \mathrm{Hom}(J_\ell, T[\ell^\infty])$ and every $x \in J_\ell$, by

$$(g\varphi)(x) = g\varphi(\tilde{g}^{-1}x\tilde{g})$$

where $\tilde{g} \in G_\infty$ is any element mapping to g in G_{ℓ^∞} (see for example [Ros95, Theorem 4.1.20]). By assumption, the cohomology group $H^1(G_{\ell^\infty}, T[\ell^\infty]^{J_\ell})$ is killed by ℓ^{n_ℓ}.

Since every element of $T[\ell^\infty]$ has order a power of ℓ and the kernel of the quotient map $J_\ell \to \overline{J}_\ell$ is contained in the product of pro-p groups for $p \neq \ell$, every group homomorphism from J_ℓ to $T[\ell^\infty]$ factors via $\overline{J}_\ell$. Moreover, since $T[\ell^\infty]$ is abelian, we have

$$\mathrm{Hom}(J_\ell, T[\ell^\infty]) = \mathrm{Hom}(\overline{J}_\ell^{\mathrm{ab}}, T[\ell^\infty])\,.$$

Assume now that $\varphi \in \mathrm{Hom}(J_\ell, T[\ell^\infty])$ is G_{ℓ^∞}-invariant. For every $x \in J_\ell$ and any lift $\tilde{g}_\ell \in G_\infty$ of g_ℓ such that $[\tilde{g}_\ell, x^{a_\ell}] \in [\overline{J}_\ell, \overline{J}_\ell]$ (hence in particular $\varphi([\tilde{g}_\ell, x^{a_\ell}]) = 0$) we have

$$a_\ell \varphi(x) = \varphi(x^{a_\ell}) = (g_\ell \varphi)(x^{a_\ell}) = g_\ell \varphi(\tilde{g}_\ell^{-1} x^{a_\ell} \tilde{g}_\ell) = a_\ell g_\ell \varphi(x),$$

so we get $a_\ell(g_\ell - 1)\varphi(x) = 0$. Since $v_\ell(g_\ell - 1) \leqslant m_\ell$ we have that $\mathrm{Hom}(J_\ell, T[\ell^\infty])^{G_{\ell^\infty}}$ is killed by $\ell^{m_\ell + v_\ell(a_\ell)}$. From these estimates and the exact sequence (4.2) we conclude that the exponent of $H^1(G_\infty, T)$ divides

$$\prod_\ell \ell^{n_\ell + m_\ell + v_\ell(a_\ell)}\,,$$

as required. □

Remark 4.6. If, in the previous proposition, one does not assume that g_ℓ be a scalar, the conclusion still holds by letting m_ℓ be a non-negative integer such that $v_\ell(\det(g_\ell - \mathrm{Id})) \leqslant m_\ell$. This may be established by a slight variation of the argument above: we only need to notice that $a_\ell(g_\ell - \mathrm{Id})\varphi(x) = 0$ implies $a_\ell \det(g_\ell - \mathrm{Id})\varphi(x) = 0$ (this can be seen for example by multiplying by the adjoint of $g_\ell - \mathrm{Id}$). The more specialised statement given above will allow us to obtain better numerical constants at the end.

Lemma 4.7. *Let G be a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, let $\overline{G}$ be the image of G under the quotient map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \prod_{\ell\ prime} \mathrm{GL}_2(\mathbb{F}_\ell)$, and let $p > 5$ be a prime. If $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs in G (see §2.3), then $\overline{G}$ contains $\mathrm{SL}_2(\mathbb{F}_p) \times \prod_{\ell \neq p} \{1\}$.*

Proof. Consider the kernel N of the quotient map $G \to \prod_\ell \mathrm{GL}_2(\mathbb{F}_\ell)$. Every composition factor of N is abelian, and a composition factor of G that does not occur in N must occur in $\overline{G}$. In particular, since $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple and non-abelian, it must occur in $\overline{G}$. Consider now the projection $\overline{G} \to \prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{F}_\ell)$ and let N' be its kernel: since $\mathrm{PSL}_2(\mathbb{F}_p)$ does not occur in $\mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell \neq p$, it must occur in N'. Then by [Ser97, IV-25] we must have that $\overline{G}$ contains $\mathrm{SL}_2(\mathbb{F}_p) \times \prod_{\ell \neq p} \{1\}$. □

We now come to our main result on the Galois cohomology of elliptic curves over $\mathbb{Q}$.

Theorem 4.8. *Let E be a non-CM elliptic curve over $\mathbb{Q}$ and let N be a positive integer. The cohomology group*

$$H^1(\mathrm{Gal}(\mathbb{Q}(E_{\mathrm{tors}}) \mid \mathbb{Q}), E[N])$$

has finite exponent dividing

$$e := 2^{12} \times 3^8 \times 5^3 \times 7^3 \times 11^2 .$$

Proof. After fixing an isomorphism $E_{\mathrm{tors}} \cong (\mathbb{Q}/\mathbb{Z})^2$, let $G_\infty \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be the image of the adelic Galois representation associated with $E/\mathbb{Q}$ and let G_{ℓ^∞}, J_ℓ and $\overline{J}_\ell$ be as in the statement of Proposition 4.5. For every prime ℓ we let n_ℓ be as in Equation (4.1) and $\lambda_\ell \in G_{\ell^\infty}$ be a scalar such that $v_\ell(\lambda_\ell - 1) = n_\ell + v_\ell(2)$ and, for $\ell \geqslant 13$, such that $\lambda_\ell^2 \not\equiv 1 \pmod{\ell}$. The elements λ_ℓ exists by Theorem 3.16 and Proposition 3.20. Let $g \in G_\infty$ be an element whose ℓ-component is λ_ℓ and set $\tilde{g}_\ell := g^2$. Finally, let

$$a_\ell = \mathrm{lcm}\,\{\exp \mathrm{PGL}_2(\mathbb{F}_p) \mid p \in \mathcal{T}_0,\, p \neq \ell\}$$

and $m_\ell = n_\ell + v_\ell(4)$. We now check that these choices satisfy all the assumptions of Proposition 4.5, with $T = E[N]$. Clearly $v_\ell(a_\ell) = n_\ell = m_\ell = 0$ for all but finitely many primes ℓ, and one checks that $v_\ell({\lambda_\ell}^2 - 1) = m_\ell$ for all primes ℓ. Theorem 4.4 shows that $H^1(G_{\ell^\infty}, T[\ell^\infty])$ is killed by ℓ^{n_ℓ}. It only remains to check property (4), that is, we wish to prove that for every $x = (x_p)_p \in J_\ell$ the image $\overline{h}$ of $h = [\tilde{g}_\ell, x^{a_\ell}]$ in $\overline{J}_\ell$ is contained in $[\overline{J}_\ell, \overline{J}_\ell]$. To see this, notice first of all that the ℓ-component of $\overline{h}$ in $\overline{J}_\ell$ is trivial, since $x_\ell = 1$. The p-component of $\overline{h}$ is trivial for every prime $p \in \mathcal{T}_0$, because $x_p^{a_\ell} \in \mathrm{GL}_2(\mathbb{F}_p)$ is a scalar (its image in $\mathrm{PGL}_2(\mathbb{F}_p)$ is trivial). Moreover, the p-component of $\overline{h}$ is also trivial for every prime $p \notin \mathcal{T}_0$ such that G_p is contained in the normalizer of a Cartan subgroup. To see this, notice that a_ℓ is even and the p-component of $\tilde{g}_\ell$ is a square (since $\tilde{g}_\ell$ itself is a square), so that both $(\tilde{g}_\ell)_p$ and x^{a_ℓ} belong to the Cartan subgroup itself, which is abelian.

For all other primes p, the mod-p Galois representation is surjective. Indeed by Theorem 2.9 we know that G_p acts irreducibly on $E[p]$ (since $p \notin \mathcal{T}_0$), by [Maz77, p. 36] we know that G_p is not contained in an exceptional subgroup, and by assumption G_p is not contained in the normaliser of a Cartan subgroup. By Theorem 2.8 we then obtain $\mathrm{SL}_2(\mathbb{F}_p) \subseteq G_p$, so in particular $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs in G_∞. Since by [Ser97, p. IV-25] it cannot occur in G_{ℓ^∞}, which is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, it must occur in J_ℓ. Then by Lemma 4.7, applied to $G = J_\ell$, we have that $S_p := \mathrm{SL}_2(\mathbb{F}_p) \times \prod_{q \neq p} \{1\}$ is contained in $\overline{J}_\ell$ for such primes p.

For each prime p, let H_p be the trivial group if p is in $\mathcal{T}_0$, if ρ_p is not surjective, or if $p = \ell$, and let $H_p = \mathrm{SL}_2(\mathbb{F}_p)$ otherwise. By the above, we have $(\overline{h})_p = \mathrm{Id} \in H_p$ for $p = \ell$, for all $p \in \mathcal{T}_0$, and for all p such that ρ_p is not surjective, and

$(\overline{h})_p \in H_p = \mathrm{SL}_2(\mathbb{F}_p)$ for all other p. We now show that $[\overline{J}_\ell, \overline{J}_\ell]$ contains $\prod_p H_p$. This product is topologically generated by the groups S_p for $p \notin \mathcal{T}_0 \cup \{\ell\}$ such that the mod-p representation attached to E is surjective, so it suffices to show that the closed subgroup $[\overline{J}_\ell, \overline{J}_\ell]$ contains S_p for every such p. This follows from the fact that $\mathrm{SL}_2(\mathbb{F}_p)$ is a perfect group, that is it coincides with its own commutator subgroup, so $[\overline{J}_\ell, \overline{J}_\ell] \supseteq [S_p, S_p] = S_p$. Thus we get $\overline{h} \in \prod_p H_p \subseteq [\overline{J}_\ell, \overline{J}_\ell]$.

We have then checked all the hypotheses needed to apply Proposition 4.5, and we conclude by noting that

$$v_\ell(a_\ell) = \begin{cases} 4 & \text{if } \ell = 2, \\ 2 & \text{if } \ell = 3, \\ 1 & \text{if } \ell = 5, 7, \\ 0 & \text{if } \ell \geqslant 11. \end{cases}$$

□

In the CM case we can say something much stronger: we prove a bound that is valid for all number fields and only depends on the degree of the field of definition of the elliptic curve.

Theorem 4.9. *Let K be a number field of degree d and let E/K be an elliptic curve such that $E_{\overline{K}}$ has CM by an order R in the quadratic imaginary field F. Let $h = \#R^\times \in \{2, 4, 6\}$ and $g = [FK : K] \in \{1, 2\}$. For every prime ℓ, let $e_\ell = \min_{a \in \mathbb{Z}_\ell^\times} v_\ell(a^{hd} - 1)$. Then e_ℓ is finite for all primes ℓ and zero for all but finitely many ℓ, and the exponent of the cohomology group $H^1(G_\infty, T)$ divides $g \prod_\ell \ell^{e_\ell}$ for all Galois submodules T of E_{tors}.*

Proof. Let $H = \mathrm{Gal}(K_\infty \mid KF)$, so that H is a subgroup of G_∞ of index g (recall that the field of complex multiplication is contained in K_∞). Let Cor and Res denote respectively the corestriction map from $H^1(H, -)$ to $H^1(G_\infty, -)$ and the restriction map from $H^1(G_\infty, -)$ to $H^1(H, -)$. As is well-known, one has the equality $\mathrm{Cor} \circ \mathrm{Res} = [g]$. Let e be the exponent of $H^1(G_\infty, T)$ and e' be the exponent of $H^1(H, T)$. Observe now that $[e']$ is zero on $H^1(H, T)$, so one gets

$$[ge'] = [e'] \circ \mathrm{Cor} \circ \mathrm{Res} = \mathrm{Cor} \circ [e'] \circ \mathrm{Res} = \mathrm{Cor} \circ [0] = [0]$$

on $H^1(G_\infty, T)$. Thus the exponent of this latter group divides ge'; it now suffices to bound e'.

By the theory of complex multiplication the Galois group H is abelian. We identify this group with a subgroup of $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, and regard $g \in H$ as a collection $(g_\ell)_\ell$ of elements in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Since H is abelian, Lemma 4.2 applies to any $(g_\ell)_\ell \in H$, so $H^1(H, T)$ is killed by $(g_\ell - 1)_\ell$. Writing $H^1(H, T) =$

$\bigoplus_\ell H^1(H, T[\ell^\infty])$, we see that each direct summand $H^1(H, T[\ell^\infty])$ (which is the pro-ℓ part of $H^1(H,T)$) is killed by $g_\ell - 1$ for every $(g_\ell)_\ell \in H$.

Let now H_{ℓ^∞} be the projection of H to $\mathrm{GL}_2(\mathbb{Z}_\ell)$, or equivalently the image of the ℓ-adic representation attached to E/FK. We know from [Lom17, Theorem 6.6] (or [BC20a, Theorem 1.1(a)]) that H_{ℓ^∞} is contained in $(R \otimes \mathbb{Z}_\ell)^\times$, and that $[(R\otimes\mathbb{Z}_\ell)^\times : H_{\ell^\infty}] \mid \frac{h}{2}[FK:\mathbb{Q}]$. Notice that [Lom17, Theorem 6.6] only gives an inequality, but it is clear from the proof that we actually have divisibility. In particular, $[\mathbb{Z}_\ell^\times : \mathbb{Z}_\ell^\times \cap H_{\ell^\infty}]$ divides $\frac{h}{2}[FK:\mathbb{Q}]$, so for every $a \in \mathbb{Z}_\ell^\times$ the scalar $a^{h[FK:\mathbb{Q}]/2}$ is in H_{ℓ^∞}, and multiplication by $a^{h[FK:\mathbb{Q}]/2}-1$ kills $H^1(H, T[\ell^\infty])$. Notice that $h[FK:\mathbb{Q}]/2$ divides hd, so the same statement holds with $a^{h[FK:\mathbb{Q}]/2}-1$ replaced by $a^{hd}-1$. As $H^1(H, T[\ell^\infty])$ is a (pro-)ℓ group, this shows that the exponent of $H^1(H, T[\ell^\infty])$ is finite and divides ℓ^{e_ℓ}. Finally, for $\ell - 1 > hd$, choosing a that is a primitive root modulo ℓ gives $v_\ell(a^{hd}-1) = 0$, hence $e_\ell = 0$ and $H^1(H, T[\ell^\infty])$ is trivial for all such primes. The theorem now follows from the fact that the exponent e' of $H^1(H,T)$ is the least common multiple of the exponents of the groups $H^1(H, T[\ell^\infty])$ as ℓ varies among the primes. □

In the special case $K = \mathbb{Q}$ we may further improve the previous result.

Proposition 4.10. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E_{\overline{\mathbb{Q}}}$ has CM. The exponent e of the cohomology group $H^1(G_\infty, T)$ divides $2^2\cdot 3$ for all Galois submodules T of E_{tors}.*

Proof. Let F be the field of complex multiplication of E, let $\mathcal{O}$ be the endomorphism ring of E_F, and let $H = \rho_\infty(\mathrm{Gal}(\overline{F}/F))$, considered as a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. There are inclusions $\widehat{\mathbb{Z}}^\times \cap H \subseteq H \subseteq (\mathcal{O}\otimes\widehat{\mathbb{Z}})^\times$, and $[\widehat{\mathbb{Z}}^\times : \widehat{\mathbb{Z}}^\times \cap H] \leqslant [(\mathcal{O}\otimes\widehat{\mathbb{Z}})^\times : H]$. Suppose first $j \notin \{0, 1728\}$. Then $[(\mathcal{O}\otimes\widehat{\mathbb{Z}})^\times : H] \leqslant 2$ by [BC20a, Corollary 1.5], hence $[\widehat{\mathbb{Z}}^\times : \widehat{\mathbb{Z}}^\times \cap H] \leqslant 2$. This implies easily that H (hence G_∞) contains an element $\lambda = (\lambda_\ell) \in \prod_\ell \mathbb{Z}_\ell^\times = \widehat{\mathbb{Z}}^\times$ with $v_2(\lambda_2 - 1) \leqslant 2$, $v_3(\lambda_3 - 1) \leqslant 1$ and $v_\ell(\lambda_\ell - 1) = 0$ for all $\ell \geqslant 5$ (for $\ell = 2$ notice that a subgroup of index at most 2 of $\widehat{\mathbb{Z}}^\times$ cannot be trivial modulo 8). The claim in this case thus follows from Lemma 4.2. When $j \in \{0, 1728\}$ the argument is similar, but one also needs to rely on the classification of the possible ℓ-adic images of Galois for $\ell \leqslant 7$ provided by [LR18]. We give some more details for $\ell = 2$, the other cases being similar and easier.

Suppose that all the scalars $\lambda = (\lambda_\ell)$ in $H \cap \widehat{\mathbb{Z}}^\times$ satisfy $v_2(\lambda_2 - 1) \geqslant 3$. Then $[\widehat{\mathbb{Z}}^\times : \widehat{\mathbb{Z}}^\times \cap H]$ is a multiple of 4, which (since $\widehat{\mathbb{Z}}^\times$ is a normal subgroup of H) implies $4 \mid [(\mathcal{O}\otimes\widehat{\mathbb{Z}})^\times : H]$. Due to [BC20a, Corollary 1.5] this must be an equality, and we must have $\mathcal{O} = \mathbb{Z}[i]$ and $j = 1728$. On the other hand, from the proof of Theorem 4.9 we know that the 2-part of the exponent of $H^1(G_\infty, T)$ is at most twice the 2-part of the exponent of $H^1(H,T)$, so if the latter is not divisible by 4 we are already done. Moreover, 4 can divide this exponent only if all the scalars

in $\rho_{2^\infty}(\mathrm{Gal}(\overline{F}/F))$ are congruent to 1 modulo 4. By [LR18, Theorem 1.7], this implies that $[(\mathcal{O}\otimes\mathbb{Z}_2)^\times : \rho_{2^\infty}(\mathrm{Gal}(\overline{F}/F))] = 4$. Combined with $[(\mathcal{O}\otimes\widehat{\mathbb{Z}})^\times : H] = 4$, this shows that H is the product $\rho_{2^\infty}(\mathrm{Gal}(\overline{F}/F)) \times \prod_{\ell\geqslant 3}(\mathcal{O}\otimes\mathbb{Z}_\ell)^\times$. By [LR18, Theorem 1.7] again, the factor $\rho_{2^\infty}(\mathrm{Gal}(\overline{F}/F))$ contains a scalar λ_2 with $v_2(\lambda_2 - 1) = 2$. Since H is the above direct product, we obtain that H (hence G_∞) contains $(\lambda_2, -1, -1, \ldots)$. Applying Sah's lemma to this element then shows that the 2-part of the exponent of $H^1(G_\infty, T)$ divides 4. □

To conclude this section we discuss the case of *Serre curves*, namely those elliptic curves over $\mathbb{Q}$ for which $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_\infty]$ is minimal (hence equal to 2, see [Ser72]). It is known that, when ordered by height, 100% of elliptic curves over $\mathbb{Q}$ are Serre curves [Jon10], so our next theorem describes the 'generic' situation. The proof combines many of the same ingredients that already appear in Theorems 4.8 and 4.4.

Theorem 4.11. *Suppose $E/\mathbb{Q}$ is a Serre curve. For every Galois submodule T of E_{tors} we have*

$$H^1(G_\infty, T) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } T[2] \neq \{0\} \\ \{0\}, & \text{if } T[2] = \{0\}. \end{cases}$$

Proof. The description of Serre curves given in [Jon10, Section 5] implies that G_∞ contains $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. We will make use of two special elements of $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \subset G_\infty$: one is $-\mathrm{Id}$, while the other is $h = (h_2, \mathrm{Id}, \mathrm{Id}, \ldots)$, where $h_2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_2)$. Notice that $h_2 - \mathrm{Id}$ is invertible over $\mathbb{Z}_2$. Let $\xi : G_\infty \to E_{\mathrm{tors}}$ be any cocycle and let $g \in G_\infty$ be arbitrary. We have the equality

$$\xi(-\mathrm{Id}) - \xi(g) = \xi((-\mathrm{Id})\cdot g) = \xi(g\cdot(-\mathrm{Id})) = \xi(g) + g\xi(-\mathrm{Id}).$$

Choosing $g = h$ gives $-2\xi(h) = (h - \mathrm{Id})\cdot\xi(-\mathrm{Id})$ in $T = \bigoplus_\ell T[\ell^\infty]$. Taking into account that the 2-adic component of $h - \mathrm{Id}$ is invertible, while multiplication by 2 is invertible on $T[\ell^\infty]$ for each $\ell > 2$, we obtain that $\xi(-\mathrm{Id})$ is divisible by 2 in T. Writing $\xi(-\mathrm{Id}) = -2a$ for some $a \in T$ we then have $2(\xi(g) - (g\cdot a - a)) = 0$, that is, the cocycle ξ is cohomologous to the cocycle $g \mapsto \xi(g) - (g\cdot a - a)$ with values in $T[2]$.

We have thus shown that the natural map $H^1(G_\infty, T[2]) \to H^1(G_\infty, T)$ is surjective. It is also injective, as one sees by taking the cohomology of the exact sequence $0 \to T[2] \to T \to 2T \to 0$ and observing that $H^0(G_\infty, T) = H^0(G_\infty, 2T) = (0)$. Hence $H^1(G_\infty, T) = H^1(G_\infty, T[2])$. We now describe this group. Let $N = \ker(G_\infty \to G_{2^\infty})$, so that $G_\infty/N \cong G_{2^\infty} = \mathrm{GL}_2(\mathbb{Z}_2)$. The inflation-restriction sequence yields

$$0 \to H^1(G/N, T[2]) \to H^1(G_\infty, T[2]) \to H^1(N, T[2])^{G_\infty},$$

so it suffices to show that $H^1(\mathrm{GL}_2(\mathbb{Z}_2), T[2])$ is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ according to whether $T[2]$ is trivial or not, while $H^1(N, T[2])^{G_\infty}$ vanishes. We prove the latter statement first. Since N acts trivially on $T[2]$ by construction we have $H^1(N, T[2])^{G_\infty} = \mathrm{Hom}(N, T[2])^{G_\infty}$. The conjugation action of $h \in G_\infty$ on N is trivial (the only nontrivial coordinate of h is h_2, while elements of N have trivial 2-adic component), so a homomorphism $\varphi \in \mathrm{Hom}(N, T[2])$ is h-invariant if and only if for all $n \in N$ we have $\varphi(n) = (h\varphi)(n) = h \cdot \varphi(h^{-1}nh) = h \cdot \varphi(n)$. Since h acts on $T[2]$ via h_2, which has no nonzero fixed points on $T[2]$, this implies that the only h-invariant homomorphism $N \to T[2]$ is the trivial one. Thus $H^1(N, T[2])^{G_\infty}$ vanishes as claimed. Finally consider $H^1(\mathrm{GL}_2(\mathbb{Z}_2), T[2])$. Notice that $T[2]$ is a Galois submodule of $E[2]$, so we either have $T[2] = E[2]$ or $T[2] = \{0\}$. In the latter case the cohomology group certainly vanishes, so we can assume $T[2] = E[2]$. As in the proof of Theorem 4.4, every cocycle $\mathrm{GL}_2(\mathbb{Z}_2) \to E[2]$ factors via $\mathrm{GL}_2(\mathbb{Z}_2)/\langle g^2 : g \equiv \mathrm{Id} \pmod 2\rangle$, hence in particular via $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. Thus it suffices to check that $H^1(\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}), E[2]) = \mathbb{Z}/2\mathbb{Z}$, which is easy to do directly with the help of a computer algebra sofware. □

5 The algebra $\mathbb{Z}_\ell[G_{\ell^\infty}]$

Following the strategy suggested by [Chapter 1, Proposition 4.12], in order to study the degrees of Kummer extensions in the next section we now study the algebra $A = \mathbb{Z}_\ell[G_{\ell^\infty}]$, by which we mean the *closed* subalgebra of $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ generated by $G_{\ell^\infty} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$. The hardest case is when the action of G_ℓ on $E[\ell]$ is reducible, and to handle this situation we rely on the following general estimate for A.

Proposition 5.1. *Let E be an elliptic curve over a number field K having at least one real place. Let $\ell > 2$ be a prime number. Suppose that G_ℓ acts reducibly on $E[\ell]$ and let ℓ^m be the maximal degree of an ℓ-power cyclic isogeny $E \to E'$ defined over K. The algebra $A = \mathbb{Z}_\ell[G_{\ell^\infty}]$ contains $\ell^m \,\mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$.*

Proof. We claim that there exists a basis of $T_\ell E$ with respect to which G_{ℓ^∞} contains $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. To see this, let $\tau \in \mathrm{Gal}(\overline{K}/K)$ be a complex conjugation, corresponding to a real embedding $K \hookrightarrow \mathbb{R}$ (one exists by assumption), and let $h = \rho_{\ell^\infty}(\tau)$. Then we have $h^2 = \mathrm{Id}$ and $\det h = \chi_{\ell^\infty}(\tau) = -1$, which implies that the eigenvalues of h are ± 1. It follows that h can be diagonalised over $\mathbb{Q}_\ell$, and also over $\mathbb{Z}_\ell$ since its eigenvalues are distinct modulo $\ell \neq 2$. As the conclusion of the proposition is independent of the choice of basis, we may assume that $h = \rho_{\ell^\infty}(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in A$. It follows that $E_{11} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}(1 + h)$

and $E_{22} := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}(1-h)$ are in A. By assumption, E does not admit a cyclic isogeny of degree ℓ^{m+1} defined over K. In terms of the matrix representation of the Galois action, this implies in particular that G_{ℓ^∞} contains a matrix M_1 whose coefficient in position $(2,1)$ is nonzero modulo ℓ^{m+1} (for otherwise, $\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \subset (\mathbb{Z}/\ell^{m+1}\mathbb{Z})^2 \cong E[\ell^{m+1}]$ would be a Galois-stable cyclic subgroup of order ℓ^{m+1}), and similarly it also contains a matrix M_2 whose $(1,2)$-coefficient is nonzero modulo $\ell^{m_\ell+1}$. Thus we have $E_{22}M_1E_{11} = \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}$ with $v_\ell(a) \leqslant m$ and $E_{11}M_2E_{22} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ with $v_\ell(b) \leqslant m$. The four matrices $E_{11}, E_{22}, E_{22}M_1E_{11}$ and $E_{11}M_2E_{22}$ are all in A, and their $\mathbb{Z}_\ell$-span contains $\ell^m \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)$. □

Remark 5.2. The exponent m is optimal. Indeed, if E admits a K-rational isogeny of degree ℓ^m, choosing a suitable basis of $T_\ell E$ we can ensure that G_{ℓ^m} consists of upper-triangular matrices. In particular, the (2,1)-coefficient of all matrices in $\mathbb{Z}_\ell[G_{\ell^\infty}]$ is divisible by ℓ^m, so that the result cannot be improved.

We also give a variant of the previous result for $\ell = 2$. Notice that in this case we do not require that $E[2]$ be reducible.

Proposition 5.3. *Let E be an elliptic curve over a number field K having at least one real place. Let 2^m be the maximal degree of a 2-power cyclic isogeny $E \to E'$ defined over K (including $m = 0$ if there are no such isogenies). The algebra $A = \mathbb{Z}_2[G_{2^\infty}]$ contains $2^{m+1}\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$.*

Proof. Let $\tau \in \operatorname{Gal}(\overline{K} \mid K)$ be a complex conjugation. There is a basis of T_2E whose first element is fixed by $\rho_{2^\infty}(\tau)$: indeed, τ fixes all torsion points in $E(\mathbb{R})$, whose identity component is isomorphic to the circle group, hence contains a compatible family of 2^n-torsion points. It follows easily that $\rho_{2^\infty}(\tau)$ is $\mathrm{GL}_2(\mathbb{Z}_2)$-conjugate to either $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. In the first case one may reason as in Proposition 5.1 to obtain that $\mathbb{Z}_2[G_{2^\infty}]$ contains $2E_{11}, 2E_{22}, 2E_{22}M_1$, and $2M_2E_{22}$, hence that it contains $2^{m+1}\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$. In the second case, suppose first that G_2 acts on $E[2]$ with a fixed point P, which is necessarily the first 2-torsion point in the given basis of $E[2] \cong T_2E/2T_2E$. Let $E \to E'$ be the 2-isogeny with kernel $\langle P \rangle$. The 2-adic representations attached to E, E' differ by conjugation by $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. The 2-adic representation attached to E' maps τ to $\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, which is $\mathrm{GL}_2(\mathbb{Z}_2)$-conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Moreover, the maximal degree of a 2-power isogeny $E' \to E''$ is at most $2^{\max\{m-1,1\}}$

The previous arguments then apply to E', hence the corresponding algebra A' contains $2^{\max\{m-1,1\}+1}\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$. Conjugating back we find that A contains $2^{\max\{m,2\}+1}\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$, and a direct check for $m = 1$ finishes the proof in this case. Finally, if $\rho_{2^\infty}(\tau) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ and $E[2]$ is an irreducible Galois module (hence $m = 0$), then $G_2 = \mathrm{GL}_2(\mathbb{F}_2)$ (notice that $\#G_2$ is even since $\rho_2(\tau)$ is nontrivial). This implies $G_2 = \mathrm{GL}_2(\mathbb{F}_2)$, from which it follows that the reduction modulo 2 of A is all of $\operatorname{Mat}_{2\times 2}(\mathbb{F}_\ell)$. By Nakayama's lemma we obtain $A = \operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$. □

For the irreducible case (and $\ell > 2$) we rely instead on the following two observations. The first one is well-known (see for example [BJR91, Remark after Theorem 2]); it is usually stated for elliptic curves over $\mathbb{Q}$, but – as in the previous propositions – it only depends on the number field having a real place.

Lemma 5.4. *Let K be a number field having at least one real place, $\ell > 2$ be a prime number, E/K be an elliptic curve, and $G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of the mod-ℓ Galois representation. The action of G_ℓ on $E[\ell]$ is either reducible or absolutely irreducible.*

Corollary 5.5. *Let K be a number field having at least one real place, $\ell > 2$ be a prime number, and E/K be an elliptic curve. If $E[\ell]$ is an irreducible Galois module, then the algebra $A = \mathbb{Z}_\ell[G_{\ell^\infty}]$ is all of $\operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)$.*

Proof. Let $\overline{A} \subseteq \operatorname{Mat}_{2\times 2}(\mathbb{F}_\ell)$ be the image of A under reduction modulo ℓ. By Nakayama's lemma, it suffices to prove that $\overline{A} = \operatorname{Mat}_{2\times 2}(\mathbb{F}_\ell)$. Notice that $\overline{A} = \mathbb{F}_\ell[G_\ell]$. As G_ℓ acts irreducibly on $E[\ell] \cong \mathbb{F}_\ell^2$ by assumption, Lemma 5.4 shows that it also acts irreducibly on $E[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}_\ell}$, hence the natural module $\overline{\mathbb{F}_\ell}^2$ for $\overline{A} \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}_\ell}$ is irreducible. By [EGH+11, Theorem 3.2.2] we obtain $\overline{A} \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}_\ell} = \operatorname{Mat}_{2\times 2}(\overline{\mathbb{F}_\ell})$, which implies $\overline{A} = \operatorname{Mat}_{2\times 2}(\mathbb{F}_\ell)$. □

We now specialise to the case $K = \mathbb{Q}$. For $\ell = 2$ we have the following.

Proposition 5.6. *Let E be an elliptic curve over $\mathbb{Q}$. The algebra $\mathbb{Z}_2[G_{2^\infty}]$ contains $2^4\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$, and if E has potential complex multiplication it also contains $2^3\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$.*

Proof. If E does not have complex multiplication over $\overline{\mathbb{Q}}$ we can check the claim directly by a short computer calculation, looping over all subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ that can arise as the image of the 2-adic representation (the list of such groups is known as a consequence of the results in [RZB15]). If E has CM over $\overline{\mathbb{Q}}$, then every 2-power isogeny $E \to E'$ defined over $\mathbb{Q}$ has degree dividing 4 (see for example [BC20b, Remark 5.2]). It follows from Proposition 5.3 that A contains $2^3\operatorname{Mat}_{2\times 2}(\mathbb{Z}_2)$. □

Remark 5.7. The result is optimal. This follows from [RZB15] in the non-CM case, while in the CM case it suffices to consider an elliptic curve with CM by $\mathbb{Z}[\sqrt{-4}]$, see [LR18, Theorem 1.6].

We are now ready to obtain a uniform lower bound on the algebra A.

Theorem 5.8. *Let E be an elliptic curve over $\mathbb{Q}$ and let ℓ be a prime number. Set*

$$m_{\text{non-CM},\ell} = \begin{cases} 4, & \text{if } \ell = 2 \\ 2, & \text{if } \ell = 3, 5 \\ 1, & \text{if } \ell = 7, 11, 13, 17, 37 \\ 0, & \text{otherwise} \end{cases} \qquad m_{\text{CM},\ell} = \begin{cases} 3, & \text{if } \ell = 2, 3 \\ 1, & \text{if } \ell = 7, 11, 19, 43, 67, 163 \\ 0, & \text{otherwise} \end{cases}$$

and $m_\ell = m_{\text{CM},\ell}$ or $m_\ell = m_{\text{non-CM},\ell}$ according to whether or not $E_{\overline{\mathbb{Q}}}$ has CM. The algebra $A = \mathbb{Z}_\ell[G_{\ell^\infty}]$ contains $\ell^{m_\ell} \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)$.

Proof. The case $\ell = 2$ is covered by Proposition 5.6. If $\ell \notin \mathcal{T}_0 \cup \{19, 43, 67, 163\}$ (or just $\ell \notin \mathcal{T}_0$ if E is not CM), by Theorem 2.9 the curve E does not admit any rational subgroup of order ℓ, so $E[\ell]$ is irreducible as a G_ℓ-module and we can apply Corollary 5.5. For the remaining cases we apply Proposition 5.1, reading from [Ken82, Theorem 1] the maximal degrees of cyclic isogenies of ℓ-power degree. Notice that isogenies of degree 3^3 are possible only for CM elliptic curves, see [Ogg73, p. 229]. Also notice that ℓ-isogenies between rational CM elliptic curves are only possible for $\ell \in \{2, 3, 7, 11, 19, 43, 167\}$, as follows for example from [BC20b, §5]. □

6 Kummer degrees

Let E be an elliptic curve over a number field K and let $\alpha \in E(K)$ be a point of infinite order. We give a brief description of the construction of the Kummer extensions of K attached to (E, α), and refer the reader to [Chapter 1, Section 2.3], [JR10, Section 3], [BP21], or [LP21] for more details.

Let (M, N) be either a pair of positive integers with $N \mid M$, or (∞, N) with N a positive integer. We define $K_{M,N}$ as the extension of K_M generated by the coordinates of all points $\beta \in E(\overline{K})$ such that $N\beta = \alpha$. The homomorphism

$$\begin{array}{rccc} \kappa_{M,N} : & \operatorname{Gal}(\overline{K} \mid K_M) & \to & E[N] \\ & \sigma & \mapsto & \sigma(\beta) - \beta \end{array} \tag{6.1}$$

is independent of the choice of $\beta \in E(\overline{K})$ such that $N\beta = \alpha$, and has kernel $\operatorname{Gal}(\overline{K} \mid K_{M,N})$, hence identifies $\operatorname{Gal}(K_{M,N} \mid K_M)$ with a subgroup of $E[N]$. We

will also need to pass to the limit in N: if ℓ is a prime number, we denote by K_{∞,ℓ^∞} the extension of K_∞ generated by the coordinates of the points $\beta \in E(\overline{K})$ that satisfy $\ell^n\beta = \alpha$ for some $n \geqslant 0$. Similarly, we write $K_{\infty,\infty}$ for the extension of K_∞ generated by the coordinates of the points $\beta \in E(\overline{K})$ that satisfy $N\beta = \alpha$ for some $N \geqslant 1$. Passing to the limit in N in Equation (6.1) we obtain an identification of $\mathrm{Gal}(K_{\infty,\ell^\infty} \mid K_\infty)$ with a $\mathbb{Z}_\ell$-submodule V_{ℓ^∞} of $T_\ell E \cong \mathbb{Z}_\ell^2$, and of $\mathrm{Gal}(K_{\infty,\infty} \mid K_\infty)$ with a $\widehat{\mathbb{Z}}$-submodule V_∞ of $TE \cong \widehat{\mathbb{Z}}^2$. We remark that V_{ℓ^∞} is the projection of V_∞ to $\mathbb{Z}_\ell^2$, and since V_{ℓ^∞} is a pro-ℓ group and there are no nontrivial continuous morphisms from a pro-ℓ group to a pro-ℓ' group for $\ell \neq \ell'$ we have $V_\infty = \prod_\ell V_{\ell^\infty}$. Finally, we recall the following fact, which will be crucial in our applications.

Lemma 6.1 ([Chapter 1, Lemma 2.5])**.** *For every prime ℓ, the $\mathbb{Z}_\ell$-module $V_{\ell^\infty} \subseteq \mathbb{Z}_\ell^2$ is also a module for the natural action of $G_{\ell^\infty} \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ on $\mathbb{Z}_\ell^2$.*

We are interested in studying the degrees

$$[K_{M,N} : K_M] \tag{6.2}$$

as the positive integers $N \mid M$ vary. As explained above, the Galois group $\mathrm{Gal}(K_{M,N} \mid K_M)$ is isomorphic to a subgroup of $E[N]$, which has order N^2, so the ratio

$$\frac{N^2}{[K_{M,N} : K_M]} \tag{6.3}$$

is an integer. It is well-known that (6.3) is bounded independently of the integers M and N (see for example [Ber88, Théorème 1], [Hin88, Lemme 14], or [Rib79]). In [Chapter 1] we have shown that, if $K = \mathbb{Q}$ and the image of α in the free abelian group $E(K)/E(K)_{\mathrm{tors}}$ is not divisible by any $n > 1$, this ratio can be bounded independently also of E and α. We will now provide an explicit value for this bound.

Remark 6.2. It is immediate to check that the ratio (6.3) divides $\dfrac{N^2}{[K_{\infty,N} : K_\infty]}$, which in turn divides the index of V_∞ in $\widehat{\mathbb{Z}}^2$.

Lemma 6.3. *Let E be an elliptic curve over a number field K and let $\alpha \in E(K)$ be a point whose image in the free abelian group $E(K)/E(K)_{\mathrm{tors}}$ is not divisible by any $n > 1$. Let e be a positive integer such that, for all positive integers N, the group $H^1(G_\infty, E[N])$ has exponent dividing e. For every prime ℓ the group V_{ℓ^∞} contains an element of ℓ-adic valuation at most $v_\ell(e)$.*

Proof. This follows immediately from [Chapter 1, Lemma 7.8(1)] since for any positive integers M, N with $N \mid M$ the exponent of $H^1(G_M, E[N])$ divides e (Lemma 4.1). □

Lemma 6.4. *Let E be an elliptic curve over a number field K and let $\alpha \in E(K)$. Suppose that V_{ℓ^∞} contains an element v of ℓ-adic valuation at most d and that $\mathbb{Z}_\ell[G_{\ell^\infty}] \supseteq \ell^n \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ for some non-negative integer n. Then $[T_\ell E : V_{\ell^\infty}]$ divides ℓ^{n+2d}.*

Proof. We may assume without loss of generality that v has exact valuation d. Up to a choice of isomorphism $T_\ell E \cong \mathbb{Z}_\ell^2$ we may then further assume $v = \ell^d \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. The $\mathbb{Z}_\ell[G_{\ell^\infty}]$-module V_{ℓ^∞} contains $\ell^n \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell) \cdot v$, hence in particular contains $\ell^{n+d} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and the claim follows immediately. □

Theorem 6.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let*

$$B_{non\text{-}CM} := (2^{24} \times 3^{16} \times 5^6 \times 7^6 \times 11^4) \times (2^4 \times 3^2 \times 5^2 \times 7 \times 11 \times 13 \times 17 \times 37)$$

$$B_{CM} := (2^4 \times 3^2) \times (2^3 \times 3^3 \times 7 \times 11 \times 19 \times 43 \times 67 \times 163).$$

Set $B = B_{CM}$ or $B = B_{non\text{-}CM}$ according to whether or not $E_{\overline{\mathbb{Q}}}$ has complex multiplication. For all positive integers M and N with $N \mid M$ the ratio (6.3) divides B.

Proof. Let e be a positive integer such that $[e]$ kills $H^1(G_\infty, E[N])$ for all positive integers N. For every prime ℓ let m_ℓ be a non-negative integer such that $\mathbb{Z}_\ell[G_{\ell^\infty}]$ contains $\ell^{m_\ell} \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)$. As explained above, the ratio (6.3) divides

$$[\widehat{\mathbb{Z}}^2 : V_\infty] = \prod_\ell [\mathbb{Z}_\ell^2 : V_{\ell^\infty}],$$

and by Lemmas 6.3 and 6.4 we have that

$$[\mathbb{Z}_\ell^2 : V_{\ell^\infty}] \qquad \text{divides} \qquad \ell^{m_\ell + 2v_\ell(e)}.$$

The conclusion then follows by taking e as in Theorem 4.8 (for the non-CM case) or as in Proposition 4.10 (for the CM case), and m_ℓ as in Theorem 5.8. □

Remark 6.6. Taking into account Remark 3.15, one can take $v_3(e) = 6$ instead of 8 in Theorem 4.8, so that the exponent of 3 in $B_{\text{non-CM}}$ can be improved from 18 to 14.

7 Examples

In this short section we give examples showing that most of our results are sharp or close to being sharp. We start with Theorems 4.4 and 4.8. For every positive integer N we have an exact sequence of $\operatorname{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$-modules

$$0 \to E[N] \to E_{\text{tors}} \xrightarrow{[N]} E_{\text{tors}} \to 0,$$

and taking Galois cohomology we get

$$0 \to \frac{E(\mathbb{Q})_{\mathrm{tors}}}{NE(\mathbb{Q})_{\mathrm{tors}}} \to H^1(G_\infty, E[N]) \to H^1(G_\infty, E_{\mathrm{tors}})[N] \to 0.$$

As it is well-known that there exist elliptic curves over $\mathbb{Q}$ with torsion points of order $2^3, 3^2, 5, 7$, taking N equal to each of these numbers in turn shows that the constant of Theorem 4.8 has to be divisible at least by $2^3 \cdot 3^2 \cdot 5 \cdot 7$. Moreover, by [LW15, Theorem 1] we know that there exists an elliptic curve $E/\mathbb{Q}$ with $H^1(G_{11}, E[11]) \neq 0$. Thus in particular all the primes appearing in the constant of Theorem 4.8 are necessary. A simple variant of this argument, working with $E[\ell^\infty]$ instead of E_{tors}, also shows that Theorem 4.4 is optimal at least for $\ell \neq 3$. As already remarked in the introduction we do not seek to obtain the best possible value for $\ell = 3$, but in any case our estimate is not far from sharp: the previous argument shows that the optimal value of n_3 is at least 2, while Theorem 4.4 shows that 3 suffices.

Consider now the CM case and Proposition 4.10. The elliptic curve with LMFDB label 27.a2 [LMF22, 27.a2] admits a rational 3-torsion point and no other 3-isogenies defined over $\mathbb{Q}$, hence it satisfies the hypotheses of [LW15, Theorem 1], which proves that for this curve $H^1(G_3, E[3]) \neq 0$. Thus the factor 3 in Proposition 4.10 is necessary. As for the power of 2, the curve with LMFDB label 32.a2 [LMF22, 32.a2] has potential CM and a rational 4-torsion point, which as above shows that $H^1(G_{2^\infty}, E[4])$ has exponent 4. Thus Proposition 4.10 is sharp.

Finally we turn to the primes that can appear in the ratio of Equation (6.3). In order to find examples where a given prime ℓ divides the degree (6.3) we proceed as follows. Let $E/\mathbb{Q}$ be a rational elliptic curve and let $P \in E(\mathbb{Q})$ be a point not divisible by any $n > 1$ in $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$. For a fixed prime $\ell > 2$, we write the multiplication by ℓ map as

$$[\ell](x, y) = \left(\frac{\phi_\ell(x)}{\psi_\ell(x)^2}, \frac{\omega_\ell(x, y)}{\psi_\ell(x)^3} \right)$$

as in [Sil09, Exercise 3.7] and consider the polynomial $g(x) = \phi_\ell(x) - x(P)\psi_\ell(x)^2 \in \mathbb{Q}[x]$. Suppose that this polynomial has an irreducible factor $g_1(x) \in \mathbb{Q}[x]$ of degree strictly less than $\frac{\ell^2}{2}$ (equivalently, for $\ell > 2$, that $g(x)$ is reducible), and let L be the field generated over $\mathbb{Q}$ by a root x_1 of $g_1(x)$. Over an at most quadratic extension L' of L, the elliptic curve E admits a point Q with x-coordinate equal to x_1. It follows that $[\ell]Q = \left(\frac{\phi_\ell(x_1)}{\psi_\ell(x_1)^2}, y([\ell]Q) \right) = (x(P), y([\ell]Q)) = \pm P$, because the only two points on E with x-coordinate equal to $x(P)$ are $\pm P$. In particular, at least one ℓ-division point of P (namely $\pm Q$) is defined over L', which has degree strictly less than ℓ^2 over $\mathbb{Q}$. Since all ℓ-division points of P are obtained from $\pm Q$ by adding a ℓ-torsion point, the field $\mathbb{Q}_{\ell,\ell}$ is the compositum of L' and

ℓ	E	LMFDB Label	P
2	$y^2 + xy + y = x^3 - x^2 - 41x + 96$	117.a3	$(2, -6)$
3	$y^2 + y = x^3 + x^2 - 7x + 5$	91.b2	$(-1, 3)$
5	$y^2 = x^3 - x^2 - x - 1$	704.c3	$(2, 1)$
7	$y^2 + xy = x^3 - x^2 - 389x - 2859$	338.c1	$(26, 51)$
11	$y^2 + xy + y = x^3 - x^2 - 32693x - 2267130$	1089.c1	$(212, 438)$
13	$y^2 + y = x^3 - 8211x - 286610$	441.a1	$(235, 3280)$
17	$y^2 + xy + y = x^3 - x^2 - 27365x - 1735513$	130050.gu2	$(\frac{4047}{4}, \frac{249623}{8})$
37	$y^2 + xy + y = x^3 + x^2 - 208083x - 36621194$	1225.b1	$(1190, 36857)$

Table 2.1: Primes ℓ dividing the relative Kummer degree (6.3), non-CM curves.

$\mathbb{Q}(E[\ell])$, hence $[\mathbb{Q}_{\ell,\ell} : \mathbb{Q}(E[\ell])] \leqslant [L' : \mathbb{Q}] < \ell^2$. It follows that in this case the prime ℓ divides the ratio (6.3) for $M = N = \ell$.

We have considered several pairs (E, P) taken from the LMFDB [LMF22], and have computed (for well-chosen primes ℓ) the factorisation of the polynomial $g(x)$ above. For each prime ℓ appearing as a factor of the constants of Theorem 6.5, we have thus been able to find examples of pairs (E, P) for which ℓ divides the index (6.3) in the case $M = N = \ell$, and this both for CM and non-CM curves (for $\ell = 2$ we proceeded differently and explicitly computed the field generated by the 2-division points of P; this easily yields examples). In particular, this shows that the prime factors of the constants of Theorem 6.5 are all necessary.

We would like to point out that for most primes ℓ we have found several examples of the behaviour described above (for $\ell = 163$ we have only been able to test two curves, and only one of them yielded an example). It is hard to make conjectures based on the limited evidence we have collected, but it seems plausible that ℓ divides the Kummer degree (6.3) (with $M = N = \ell$) for a positive proportion of rank-1 curves $E/\mathbb{Q}$ whose mod-ℓ Galois representation lands in a Borel (when P is taken to be a generator of the free part of $E(\mathbb{Q})$). In Tables 2.1 and 2.2 we give one explicit example for every relevant prime, both for non-CM and CM curves, specifying the curve $E/\mathbb{Q}$ together with its LMFDB label and the point $P \in E(\mathbb{Q})$.

The points P_{43} and P_{67} are given by $P_{43} = \left(\frac{66276734}{29929}, -\frac{419567566482}{5177717}\right)$ and

$$P_{67} = \left(\frac{4997007755485621045591 3}{1635061583290810756}, \frac{109560850843927181143959973189779 93}{2090745506172424414999081096}\right)$$

ℓ	E	LMFDB Label	P
2	$y^2 = x^3 - 36x$	576.c3	$(-2, -8)$
3	$y^2 + y = x^3 - 34$	225.c1	$(6, 13)$
7	$y^2 = x^3 - 1715x - 33614$	784.f2	$(57, 232)$
11	$y^2 + y = x^3 - x^2 - 887x - 10143$	121.b1	$(81, 665)$
19	$y^2 + y = x^3 - 13718x - 619025$	361.a1	$(2527, 126891)$
43	$y^2 + y = x^3 - 1590140x - 771794326$	1849.b1	P_{43}
67	$y^2 + y = x^3 - 33083930x - 73244287055$	4489.b1	P_{67}
163	$y^2 + y = x^3 - 57772164980x - 5344733777551611$	26569.a1	P_{163}

Table 2.2: Primes ℓ dividing the relative Kummer degree (6.3), CM curves.

respectively. The point P_{163} is the unique generator of $E(\mathbb{Q}) \cong \mathbb{Z}$ with positive y-coordinate; it has canonical height approximately equal to 373.48, so its coordinates are too large to be displayed here, but they can be found at [LMF22, Elliptic Curve 26569.a1].

We have also considered the divisibility of (6.3) by higher powers of ℓ. Experiments analogous to the above are computationally intensive, so we only studied the very small primes 2 and 3. An example where the index (6.3) is divisible by 16 was found by Rouse and Cerchia [CR21]: letting $E : y^2 = x^3 - 343x + 2401$ and $P = (0, -49)$, there is a point $P_4 \in E(\mathbb{Q}(E[8]))$ such that $4P_4 = P$. This implies that 2^4 divides (6.3) for $N = 4, M = 8$. We found several other examples in which (6.3) is divisible by 2^4 for suitable values of M, N, but no example involving higher powers of 2. This might in part be due to the fact that – for computational reasons – we have only been able to extend our search to $M = 8, N \mid M$.

Remark 7.1. J. Rouse recently informed us that he constructed an example where (6.3) is divisible by 2^6 when M and N are sufficiently large powers of 2.

For $\ell = 3$ we consider

$$E : y^2 + y = x^3 - 6924x + 221760$$

and $P = (2354/49, -176/343)$, which is a generator of $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Write $g(x)$ for the polynomial whose roots are the x-coordinates of the 9-division points of P: one may check that $g(x) \in \mathbb{Q}[x]$ has an irreducible factor $g_1(x)$ of degree 9. Further denote by $\psi_9(x)$ the 9-th division polynomial of E, whose roots are the x-coordinates of the points in $E[9]$. We have also computed that the Galois groups

of $\psi_9(x), g_1(x)$ and $\psi_9(x)g_1(x)$ over $\mathbb{Q}$ have order 462, 27 and $3 \cdot 462$ respectively. This proves that the Galois group of $g_1(x)$ over $\mathbb{Q}(E[9])$ has order 3, hence in particular that $g_1(x)$ becomes reducible over $\mathbb{Q}(E[9])$. A 9-division point of P is then defined over an extension of $\mathbb{Q}(E[9])$ of degree at most (and in fact exactly) 3. As before, all other 9-division points are defined over the same field, hence the relative Kummer degree (6.3) is divisible by 3^3 for $M = N = 9$. We have found other examples where 3^3 divides (6.3), but none involving a factor 3^4; as with $\ell = 2$, it is entirely possible that this is only due to the limits of our search range.

2.A Scalars in pro-p subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$

In this appendix we prove an abstract group-theoretic result, used in Section 3.3 to study the subgroup of scalar matrices in the image of the 3-adic representation attached to a non-CM elliptic curve over $\mathbb{Q}$. In the statement and proof of Proposition 2.A.1 we will employ the notation H_{p^n} for the reduction modulo p^n of a closed subgroup H of $\mathrm{GL}_2(\mathbb{Z}_p)$ (cf. Section 3.1).

Proposition 2.A.1. *Let p be an odd prime, H be a closed pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, and k be a positive integer. Suppose that the following hold:*

1. *H_p has order p,*
2. *H_{p^k} is not contained in the subgroup of upper- or lower-triangular matrices;*
3. *$\det(H) = 1 + p\mathbb{Z}_p$;*
4. *H is normalised by $C := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.*

Then H contains all scalars congruent to 1 modulo p^k.

Remark 2.A.2. From a group-theoretic point of view this result is optimal, at least in the case $p = 3, k = 3$ that we are interested in. The subgroup H of $\mathrm{GL}_2(\mathbb{Z}_3)$ given by the inverse image of the subgroup of $\mathrm{GL}_2(\mathbb{Z}/3^3\mathbb{Z})$ generated by the matrices

$$\begin{pmatrix} 10 & 0 \\ 0 & 16 \end{pmatrix}, \quad \begin{pmatrix} 10 & 9 \\ 23 & 10 \end{pmatrix}$$

satisfies all the properties (1)-(4) in the statement, and

$$H \cap \mathbb{Z}_3^\times = \{\lambda \in \mathbb{Z}_3^\times : \lambda \equiv 1 \pmod{3^3}\}.$$

Remark 2.A.3. We also note that the methods of [Pin93] and [Lom15, §4] are not easily applicable here, since there is no reason to expect a group H as in the statement of Proposition 2.A.1 to be open in $\mathrm{GL}_2(\mathbb{Z}_p)$. This implies that the $\mathbb{Z}_p$-integral Lie algebra L attached to H by [Pin93] could be quite small, with $L/[L,L]$ infinite, which makes it hard to extract useful information from the main theorem of [Pin93].

The proof of the proposition is by induction: we will show that, for every $n \geqslant k$, the group H_{p^n} contains all scalars congruent to 1 modulo p^k. Since H is closed this gives the desired conclusion.

Remark 2.A.4. The group H_p is cyclic, generated by any element g of order p. The condition that H be stable under conjugation by C implies easily that g is either upper- or lower-unitriangular (that is, triangular with diagonal coefficients equal to 1). This shows in particular that for every $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$ we have $a \equiv d \equiv 1 \pmod{p}$, so that the diagonal entries of $h - \mathrm{Id}$ are divisible by p. Any $h \in H$ may therefore be written as $h = \lambda\,\mathrm{Id} + D + A$, where $\lambda = \frac{1}{2}\operatorname{tr}(h) \equiv 1 \pmod{p}$, D is diagonal, $\operatorname{tr}(D) = 0$, $D \equiv 0 \pmod{p}$, and A is anti-diagonal. This decomposition will play an important role in the proof.

The following lemma will be key in our approach.

Lemma 2.A.5. *Let p be an odd prime, let H_{p^n} be a p-subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ stable under conjugation by $C := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and let M be an element of H_{p^n}. Consider the sequence of elements of H_{p^n} defined by $M_0 = M$ and $M_{i+1} = M_i \cdot CM_iC^{-1}$. Then:*

1. *for every $i \geqslant 0$, the elements $\det M_i$ and $\det M$ generate the same subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$;*
2. *write each M_i as $\lambda_i\,\mathrm{Id} + D_i + A_i$, where D_i is diagonal and has trace 0 and A_i is anti-diagonal. Then there exists a scalar $\mu_i \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $D_i = \mu_i D_0$;*
3. *the matrix M_i is diagonal for all $i \geqslant n$.*

Proof. For the first statement we have $\det(M_{i+1}) = \det(M_i)^2$ and the map $x \mapsto x^2$ is an automorphism of the abelian p-group $\det(H)$. Write now $M_i = \lambda_i\,\mathrm{Id} + D_i + A_i$ as in the statement. It follows from Remark 2.A.4 that $D_i \equiv 0$

(mod p). One computes $CM_iC^{-1} = \lambda_i \operatorname{Id} + D_i - A_i$ and therefore

$$\begin{aligned} M_{i+1} &= (\lambda_i \operatorname{Id} + D_i + A_i)(\lambda_i \operatorname{Id} + D_i - A_i) \\ &= \lambda_i^2 + D_i^2 + 2\lambda_i D_i - A_i^2 + [A_i, D_i]. \end{aligned}$$

Notice that D_i^2 is a multiple of the identity (since the two diagonal elements of D_i are opposite to each other, hence have the same square), and so is A_i^2, while $[A_i, D_i]$ is anti-diagonal. Hence

$$\begin{cases} D_{i+1} = 2\lambda_i D_i \\ A_{i+1} = [A_i, D_i], \end{cases}$$

which immediately implies the statement about D_i since $(2\lambda_i, p) = 1$. Moreover, since $v_p(D_i) \geqslant 1$ we have $v_p(A_{i+1}) \geqslant v_p(A_i) + 1$: in particular, for $i \geqslant n$ we have $v_p(A_i) \geqslant n$, hence for such i the matrix A_i is 0 and M_i is diagonal. □

We notice in particular the following immediate consequence of the previous lemma:

Corollary 2.A.6. *Let H_{p^n} be a p-subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ stable under conjugation by C, and let $\mathcal{D}_n$ be the subgroup of diagonal matrices in H_{p^n}. Then* $\det(H_{p^n}) = \det(\mathcal{D}_n)$.

Proof. The group $\det(H_{p^n})$ is contained in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, hence is cyclic. Let $M \in H_{p^n}$ be a matrix whose determinant generates $\det(H_{p^n})$: by the previous lemma, we can find a diagonal matrix whose determinant generates the same subgroup as $\det(M)$. □

Before proving Proposition 2.A.1 we need one further definition:

Definition 2.A.7. For $n \geqslant 1$ we let L_n be the image of the map

$$\begin{array}{ccc} \ker(H_{p^{n+1}} \to H_{p^n}) & \to & \mathrm{Mat}_{2\times 2}(\mathbb{F}_p) \\ g & \mapsto & \frac{g - \operatorname{Id}}{p^n}. \end{array}$$

The formulas

$$(\operatorname{Id} + p^n M_1)(\operatorname{Id} + p^n M_2) \equiv \operatorname{Id} + p^n(M_1 + M_2) \pmod{p^{n+1}}$$

and $(\operatorname{Id} + p^n M)^p \equiv \operatorname{Id} + p^{n+1} M \pmod{p^{n+2}}$, valid for all $n \geqslant 1$, show that the set L_n is an additive subgroup of $\mathrm{Mat}_{2\times 2}(\mathbb{F}_p)$, and that moreover $L_n \subseteq L_{n+1}$ for all $n \geqslant 1$.

We further observe that since C normalises H the subspace L_n of $\mathrm{Mat}_{2\times 2}(\mathbb{F}_p)$ is stable under conjugation by C. Since p is odd, the conjugation action of C

on $\mathrm{Mat}_{2\times 2}(\mathbb{F}_p)$ decomposes it as the direct sum of the subspaces of diagonal and anti-diagonal matrices. We then have a corresponding decomposition $L_n = \mathfrak{d}_n \oplus \mathfrak{a}_n$, where $\mathfrak{d}_n$ (respectively $\mathfrak{a}_n$) is the subspace of diagonal (resp. anti-diagonal) matrices in L_n. We are now ready to begin the proof proper.

Proof of Proposition 2.A.1. We show by induction on n that H_{p^n} contains all scalar matrices congruent to 1 modulo p^k. Notice that the claim is trivial for $n \leqslant k$, so we only need to take care of the inductive step. For each positive integer n we denote by $\mathcal{D}_n$ the subgroup of diagonal matrices in H_{p^n} and by Λ_n the subgroup $\{\lambda \in (\mathbb{Z}/p^n\mathbb{Z})^\times : \lambda \equiv 1 \pmod p\}$ of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. By Corollary 2.A.6 and the hypothesis $\det(H) = 1 + p\mathbb{Z}_p$ (hence $\det(H_{p^n}) = \Lambda_n$) we have $\#\mathcal{D}_n \geqslant \#\Lambda_n = p^{n-1}$ for all $n \geqslant 1$. The kernel of the reduction map $\mathcal{D}_{n+1} \to \mathcal{D}_n$ is isomorphic to $\mathfrak{d}_n$ by construction. Notice that $\#\mathfrak{d}_n \in \{1, p, p^2\}$.

If $\#\mathfrak{d}_n = p^2$, the map $\mathcal{D}_{n+1} \to \mathcal{D}_n$ is p^2-to-1, which implies that, for every element in $\mathcal{D}_n$, *all* its p^2 diagonal lifts to $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ are in $\mathcal{D}_{n+1}$. In particular, since $(1 + p^k)\,\mathrm{Id} \bmod p^n$ is an element of $\mathcal{D}_n$ by the inductive hypothesis and $(1 + p^k)\,\mathrm{Id} \bmod p^{n+1}$ is one such possible lift, we obtain immediately that $(1 + p^k)\,\mathrm{Id}$ is in $H_{p^{n+1}}$, and the induction step is complete (notice that the cyclic subgroup generated by $(1 + p^k)\,\mathrm{Id}$ contains all scalars congruent to 1 modulo p^k).

Suppose on the other hand that $\#\mathfrak{d}_n \mid p$. Then, using the fact that $\#\mathfrak{d}_i$ divides $\#\mathfrak{d}_{i+1}$, we obtain immediately

$$\#\mathcal{D}_{n+1} = \#\mathcal{D}_1 \cdot \#\mathfrak{d}_1 \cdots \#\mathfrak{d}_n \mid p^n,$$

which combined with our previous observation $\#\mathcal{D}_{n+1} \geqslant p^n$ implies $\#\mathcal{D}_{n+1} = p^n$. In particular,

$$\det : \mathcal{D}_{n+1} \to \Lambda_{n+1}$$

is a surjective group homomorphism between groups of the same order, hence is an isomorphism. This also implies that the only diagonal matrix in $H_{p^{n+1}}$ with determinant 1 is the identity.

Let now $d : \Lambda_{n+1} \to \mathcal{D}_{n+1}$ be the isomorphism given by the inverse of the determinant, which we write as

$$d(x) = \begin{pmatrix} \alpha(x) & 0 \\ 0 & \beta(x) \end{pmatrix}$$

for suitable group homomorphisms $\alpha(x), \beta(x) : \Lambda_{n+1} \to \Lambda_{n+1}$. As Λ_{n+1} is a cyclic group, we have $\alpha(x) = x^a$ and $\beta(x) = x^b$ for suitable integers a, b. Since $d(x)$ is inverse to the determinant, we have $x = \det(d(x)) = \alpha(x)\beta(x) = x^{a+b}$, so that in particular $a + b$ is relatively prime to p. This implies that at least one between a and b is prime to p.

We now show that the intersection $S_{n+1} := H_{p^{n+1}} \cap \mathrm{SL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ consists of matrices of the form $\lambda \,\mathrm{Id} + A$, where $\lambda \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ is a scalar and A is antidiagonal. To see this, let $M \in S_{n+1}$, and write it as $M = \lambda \,\mathrm{Id} + D + A$, with D diagonal of trace 0 and A antidiagonal. Lemma 2.A.5 yields a diagonal matrix $M' = \lambda' \,\mathrm{Id} + D'$ in S_{n+1} (in particular, $\det(M') = 1$) with $D' = \mu D$ for some scalar μ prime to p. Since the only diagonal matrix with determinant 1 in $H_{p^{n+1}}$ is the identity, we get $\lambda' = 1$ and $D' = 0$. As μ is invertible, this implies $D = 0$ as desired.

On the other hand, S_{n+1} – being the kernel of the determinant – is normal in $H_{p^{n+1}}$, hence in particular is stable under conjugation by the diagonal matrices $d(x)$. Let $M = \lambda \,\mathrm{Id} + A$ be any element of S_{n+1} and let $x \in \Lambda_{n+1}$. Then S_{n+1} also contains $d(x) \cdot M \cdot d(x)^{-1}$ and their product $M \cdot d(x) \cdot M \cdot d(x)^{-1}$, that is,

$$(\lambda \,\mathrm{Id} + A)(\lambda \,\mathrm{Id} + d(x) \cdot A \cdot d(x)^{-1}). \tag{2.A.1}$$

Like all elements of S_{n+1}, this matrix has the form $\lambda' \,\mathrm{Id} + A'$ for some scalar λ' and some anti-diagonal matrix A'. The diagonal part of (2.A.1) is $\lambda^2 + A \cdot d(x) \cdot A \cdot d(x)^{-1}$, so $A \cdot d(x) \cdot A \cdot d(x)^{-1}$ is a multiple of the identity modulo p^{n+1}. Writing $A = \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}$, the condition becomes

$$yz \left(\frac{\alpha(x)}{\beta(x)} - \frac{\beta(x)}{\alpha(x)} \right) \equiv 0 \pmod{p^{n+1}}. \tag{2.A.2}$$

We will show below that there exists $M \in S_{n+1}$, $M = \lambda \,\mathrm{Id} + \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}$, with $v_p(yz) \leqslant k-1$. Assuming for now that we have such an M, in Equation (2.A.2) we may assume $v_p(yz) \leqslant k-1$, hence we obtain $\left(\frac{\alpha(x)}{\beta(x)}\right)^2 \equiv 1 \pmod{p^{n+2-k}}$. Recalling that $\alpha(x) = x^a, \beta(x) = x^b$, this rewrites as $x^a \equiv x^b \pmod{p^{n+2-k}}$ (notice that $x \mapsto x^2$ is an automorphism of Λ_{n+1}). Raising to the p^{k-1}-th power we get $x^{p^{k-1}a} \equiv x^{p^{k-1}b} \pmod{p^{n+1}}$, hence

$$x^{p^{k-1}a} \,\mathrm{Id} = x^{p^{k-1}b} \,\mathrm{Id} = d\left(x^{p^{k-1}}\right) \in H_{p^{n+1}}$$

for every $x \in \Lambda_{n+1}$. Recall now that at least one between a and b is prime to p, say $(a, p) = 1$: then $x \mapsto x^a$ is an automorphism of Λ_{n+1}, so it follows that all the p^{k-1}-th powers of the scalars $\equiv 1 \pmod{p}$ are in $H_{p^{n+1}}$. The induction step is now complete, because all scalars congruent to 1 modulo p^k are p^{k-1}-th powers in Λ_{n+1}.

It only remains to show that we can find an element $M \in S_{n+1}$ such that, writing $M = \lambda \mathrm{Id} + \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}$, we have $v_p(yz) \leqslant k-1$. We first prove that it is enough to find $N = \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} \in H_{p^{n+1}}$ with $v_p(n_{12}n_{21}) \leqslant k-1$. Indeed, given such an N, we know from above that there is a diagonal matrix $Q = \begin{pmatrix} q_{11} & 0 \\ 0 & q_{22} \end{pmatrix} \in H_{p^{n+1}}$ with $\det(Q) = \det(N)^{-1}$. Notice that q_{11}, q_{22} are invertible. Then $NQ = \begin{pmatrix} q_{11}n_{11} & q_{22}n_{12} \\ q_{11}n_{21} & q_{22}n_{22} \end{pmatrix}$ belongs to S_{n+1}, so it is automatically of the form $\lambda \mathrm{Id} + A$, and its anti-diagonal part satisfies $v_p(q_{22}n_{12}\, q_{11}n_{21}) = v_p(n_{12}n_{21}) \leqslant k-1$ as desired. Thus it suffices to find $N \in H_{p^{n+1}}$, of arbitrary determinant, with $v_p(n_{12}n_{21}) \leqslant k-1$.

By Remark 2.A.4, there exists $g \in H$ that reduces modulo p to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$: for simplicity of exposition, we only discuss the former case, the latter being completely analogous. Consider the image $\begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$ of g in H_{p^k}: since $v_p(g_{12}) = 0$, if $v_p(g_{21}) \leqslant k-1$ we are done by taking $N = g \bmod p^{n+1}$. Otherwise, let $h \in H$ be an element whose image $\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix}$ in H_{p^k} satisfies $v_p(h_{21}) \leqslant k-1$: such an element exists, for otherwise H_{p^k} would be contained in the subgroup of upper-triangular matrices. If $v_p(h_{12}) = 0$ we are done by taking $N = h \bmod p^{n+1}$, while if $v_p(h_{12}) > 0$ it is easy to check that we can take $N = hg \bmod p^{n+1}$. □

Remark 2.A.8. Part of the proof is inspired by the structure theorem for reductive groups. Indeed, in the course of the argument we prove that the diagonal torus of $H_{p^{n+1}}$ is isomorphic to Λ_{n+1}, which is the pro-p subgroup of $\mathbb{G}_m(\mathbb{Z}/p^{n+1}\mathbb{Z})$, that $S_{n+1} = H_{p^{n+1}} \cap \mathrm{SL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ (morally, the derived subgroup) intersects the diagonal torus trivially, and finally that the conjugation action of the torus on the "semisimple part" S_{n+1} is (essentially) trivial, so that

the diagonal torus (essentially) consists of scalar matrices. This is reminiscent of the decomposition $G = Z(G).G'$ that holds for reductive groups, and indeed hypothesis (2) of the proposition may be seen as a discrete analogue of the statement "H is reductive".

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 $K\left(n^{-1}A\right)$, 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

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

where s is the unique positive integer such that $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$ for all $n \geqslant 1$, 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 $\mathrm{End}_K(E) = \mathbb{Z}$ 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 α in $E(K)/E(K)_{\mathrm{tors}}$, was given.

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

(1) The finitess of the divisibility of α in $E(K)/E(K)_{\mathrm{tors}}$;

(2) Properties of the ℓ-adic Galois representations associated with E, for every prime ℓ;

(3) The finiteness of the exponent of $H^1(\mathrm{Gal}(K(E(\overline{K})_{\mathrm{tors}}) \mid K), E(\overline{K})_{\mathrm{tors}})$.

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 $n \geqslant 1$. Let H denote, after a choice of basis, the image of the adelic Galois representation associated with G over K*

$$\mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_s(\widehat{\mathbb{Z}}).$$

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

(1) There is an integer $d_A \geqslant 1$ such that

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

(2) There is an integer $N \geqslant 1$ such that $\mathbb{Z}_\ell[H_\ell] \supseteq N\,\mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$ for every prime ℓ.

(3) There is an integer $M \geqslant 1$ such that the exponent of the cohomology group $H^1(\mathrm{Gal}(K_\infty \mid K), G(\overline{K})_{\mathrm{tors}})$ divides M, where $K_\infty = K(G(\overline{K})_{\mathrm{tors}})$.

Then for every $n \geqslant 1$ 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 $G(K)/G(K)_{\mathrm{tors}}$, 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 $\mathrm{End}_K(E) = \mathbb{Z}$. 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 $n \geqslant 1$*

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

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

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

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

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_{tors} the subgroup consisting of all elements of A of finite order. We denote by $\mathrm{rk}(A)$ 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 commutive ring, then we denote by $\mathrm{Mat}_{n\times m}(R)$ 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 $\mathrm{Mat}_{n\times m}(R)$ is the R-module ring (or trivial R-algebra if $n = m = 0$). For $n > 0$ we denote by $\mathrm{GL}_n(R)$ the group of invertible $n \times n$ matrices with entries in R.

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

If K is a number field and $\overline{K}$ is a fixed algebraic closure of K, we denote by ζ_n a primitive n-th root of unity in $\overline{K}$, 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 $G(\overline{K})$, we denote by $K(S)$ the subfield of $\overline{K}$ whose elements are fixed by

$$H = \left\{ g \in \mathrm{Gal}(\overline{K} \mid K) \mid g(P) = P \quad \forall\, P \in S \right\}.$$

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 $\widehat{\mathbb{Z}}$-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 $\mathrm{Hom}(G, S^1)$ 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

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

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

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

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

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

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

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 $r, s \geqslant 1$, the group $\mathrm{Hom}((\mathbb{Q}/\mathbb{Z})^r, (\mathbb{Q}/\mathbb{Z})^s)$ can be identified with $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$. This can be seen

directly on the finite level as follows: let

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

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

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

Theorem 2.3 (Pontryagin duality, see [Pon66, Theorems 39 and 40])**.** *The hom-functor* $\mathrm{Hom}(-, S^1)$ *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*

$$\begin{array}{ccc} \{\textit{closed subgroups of } G\} & \leftrightarrow & \{\textit{closed subgroups of } G^\wedge\} \\ U & \mapsto & \mathrm{Ann}\, U = \{f \in G^\wedge \mid f(u) = 0\, \forall\, u \in U\} \\ \{g \in G \mid f(g) = 0\, \forall f \in V\} = \mathrm{Ann}\, V & \hookleftarrow & V \end{array}$$

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 $\mathrm{Hom}_A(B, C)$ the set of homomorphisms $B \to C$ that restrict to the identity on A. Similarly we define the ring of endomorphisms $\mathrm{End}_A(B)$. We also denote by $\mathrm{Aut}_A(B)$ the group of all automorphisms of B that restrict to the identity on A, that is the group of invertible elements in the ring $\mathrm{End}_A(B)$. We call any element of $\mathrm{Aut}_A(B)$ 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 $f : A \to N$ and $g : B \to N$ are group homomorphisms such that $f_{|A\cap B} = g_{|A\cap B}$, then there exists a unique map $\varphi : A+B \to N$ 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 $A \cap B \hookrightarrow B$. □

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 $\mathrm{Aut}_A(M)$ 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 $\mathrm{Aut}_A(M) \to \mathrm{Hom}_A(B, M)$ factors via $\mathrm{Aut}_A(B)$. In this situation we call this map $\mathrm{Aut}_A(M) \to \mathrm{Aut}_A(B)$ 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 $\mathrm{Aut}_{A\cap B}(A + B) \to \mathrm{Aut}_{A\cap B}(B)$ induces an isomorphism*

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

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

Let $\sigma \in \mathrm{Aut}_{A\cap B}(B)$ and let $\tilde{\sigma} : A + B \to A + B$ be the homomorphism obtained by applying Lemma 2.4 to σ and 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 ρ is an isomorphism. □

2.3 Projective limits of exact sequences

Remark 2.9. Let

$$1 \to A \to G \to H \to 1$$

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 $\widehat{h}$ is a different lift of h then $\widehat{h} = \tilde{h}b$ for some $b \in A$, and we have $\widehat{h}a\widehat{h}^{-1} = \tilde{h}bab^{-1}\tilde{h}^{-1} = \tilde{h}a\tilde{h}^{-1}$. 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*

$$1 \to A_i' \to A_i \to A_i'' \to 1$$

such that A_i' and A_i'' have the subspace and quotient topology with respect to A_i, respectively. For every $i \leqslant j$ let $\rho_{ij} : \mathcal{A}_j \to \mathcal{A}_i$ 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

$$1 \to A' \to A \to A'' \to 1\,.$$

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. □

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_{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 $B = \bigcup_{n \geqslant 1} B_n$.

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

$$\begin{array}{ccc} n_B^{-1}a & \to & B[n] \\ b & \mapsto & b - b_0 \end{array}$$

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 $\varphi : B \to C$ 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 $\varphi : B \to C$ be a group homomorphism that is the identity on A. The kernel of φ is contained in B_{tors}. Moreover, if for every prime ℓ the restriction of φ to $B[\ell]$ is injective, then φ 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 ℓ be a prime dividing the order of b. But then b has a multiple of order ℓ 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 $\varphi : B \to B$ be an endomorphism that is the identity on A. If φ is injective, then it is an automorphism.*

Proof. Assume first that φ 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 φ 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 $\mathrm{Hom}_{A\cap C}(C,B) \subseteq \mathrm{Hom}_{A\cap C}(C,C)$, 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 $\sigma \in \mathrm{Aut}_{A\cap C}(A + C)$ and consider its restriction $\sigma_C : C \to A + C$. We then have

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

Moreover σ_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 $\tau \in \mathrm{Aut}_A(B)$ and consider its restriction $\tau_{A+C} : A + C \to B$. Since τ 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 τ_{A+C} is contained in $A + C$. Since τ is injective, by applying Lemma 3.7 we see that τ_{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 $\mathrm{Hom}_{A'\cap C}(C, B')$ is contained in $\mathrm{Hom}_{A\cap C}(C, B)$. □

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_{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 $\mathrm{Hom}_{A\cap C}(C, B) \subseteq \mathrm{Hom}_{A\cap C}(C, C)$.

(2) If $C = B_n$ for some positive integer n, then by Lemma 3.5 we have $\mathrm{Hom}_A(B_n, B) \subseteq \mathrm{Hom}_A(B_n, B_n)$ and hence

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

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 $\mathrm{Aut}_A(B)$ 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 $\mathrm{Aut}_A(B) \to \mathrm{Hom}_{A\cap C}(C, B)$ is $\mathrm{Aut}_{A\cap C}(C)$.*

Proof. By Lemma 2.8 we have $\mathrm{Aut}_A(A + C) \cong \mathrm{Aut}_{A\cap C}(C)$ via the restriction map, so it is enough to show that the restriction $\mathrm{Aut}_A(B) \to \mathrm{Aut}_A(A+C)$, 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 $\varphi \in \mathrm{Aut}(C)$ can be extended to an injective homomorphism $B \to B$. Consider the set of pairs (M, ϕ), where M is a subgroup of B containing C and $\phi : M \to B$ is an injective homomorphism extending φ, ordered by inclusion

$$(M, \phi) \subseteq (M', \phi') \qquad \Longleftrightarrow \qquad M \subseteq M' \quad \text{and} \quad \phi'_{|M} = \phi.$$

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 $\langle \tilde{B}, x\rangle \to B$.

Assume first that the order of x is a prime number ℓ. 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 $\#\tilde{B}[\ell] < \#B[\ell]$, 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 $y \in \mathrm{Im}(\tilde{\varphi})$, 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 $\langle \tilde{B}, x\rangle \to B$ that we obtain is still injective.

We conclude that $\tilde{B} = B$, thus the restriction map $\mathrm{Aut}_A(B) \to \mathrm{Aut}_A(C)$ is surjective. □

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

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

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

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

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

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

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

is also a group homomorphism. To see this, let $\sigma, \tau \in \mathrm{Aut}_{A+B_{\mathrm{tors}}}(B)$. Notice that, since $\tau(b) - b \in B_{\mathrm{tors}}$ 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 φ is injective, because if $\varphi_\sigma = 0$ then $\sigma(b) = b$ for all $b \in B$. To see that φ is surjective, for any $\psi \in \mathrm{Hom}(B/(A + B_{\mathrm{tors}}), B_{\mathrm{tors}})$ 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 $A + B_{\mathrm{tors}}$. 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 $\sigma_\psi \in \mathrm{Aut}_{A+B_{\mathrm{tors}}}(B)$ and clearly $\varphi_{\sigma_\psi} = \psi$, so φ is surjective. We conclude that φ is an isomorphism. □

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*

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

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

Proof. Notice that B_{tors} is A-normal in B by Example 3.9, so the restriction $\text{Aut}_A(B) \to \text{Aut}_{A_{\text{tors}}}(B_{\text{tors}})$ 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 $\sigma_\psi : b \to b + \psi([b])$ 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 τ to $\text{Aut}_A(B)$. Then for every $b \in B$ we have

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

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. □

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_{tors} and $B/(A+B_{\text{tors}})$ are finite, since A is finitely generated, B/A has finite exponent and B_{tors} embeds in $(\mathbb{Q}/\mathbb{Z})^s$. □

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

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

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

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

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

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

$$\mathrm{Aut}_{A+B_{m,\mathrm{tors}}}(B_m) \to \mathrm{Aut}_{A+B_{n,\mathrm{tors}}}(B_n)$$

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

- The group B_n is A-normal in B_m by Example 3.9(2) and Proposition 3.8.

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

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

Proof. By Proposition 3.10 the restriction map $\rho_m : \mathrm{Aut}_A(B) \to \mathrm{Aut}_A(B_m)$ is surjective for every m. Since for every $n \mid m$ we have $\rho_n = \rho_{nm} \circ \rho_m$, the map ρ_{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 $\varphi_n : G \to \mathrm{Aut}_A(B_n)$. Then we can define a map $\varphi : G \to \mathrm{Aut}_A(B)$ 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 $G \to \mathrm{Aut}_A(B)$ compatible with the projections. □

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

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

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, $\mathrm{Hom}\,(B/(A+B_{\mathrm{tors}}), B_{\mathrm{tors}})$ and $\mathrm{Aut}_{A_{\mathrm{tors}}}(B_{\mathrm{tors}})$ have the subspace and quotient topology, respectively (see Lemma 2.10). Notice also that $\mathrm{Hom}\,(B/(A+B_{\mathrm{tors}}), B_{\mathrm{tors}})$, being the kernel of a continuous homomorphism, is a closed normal subgroup of $\mathrm{Aut}_A(B)$.

We have obtained the following refinement of Proposition 3.12.

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

There is an exact sequence of profinite groups

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

Moreover, the group $\mathrm{Aut}_{A_{\mathrm{tors}}}(B_{\mathrm{tors}})$ acts on $\mathrm{Hom}\,(B/(A+B_{\mathrm{tors}}), B_{\mathrm{tors}})$ 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 Γ of A is called *full* if Γ is a divisible abelian group and $\Gamma_{\mathrm{tors}} \cong (\mathbb{Q}/\mathbb{Z})^s$.

Remark 3.17. Recall from Remark 3.2 that a necessary condition for A to admit any s-extension is that A_{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

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

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

$$0 \to \Gamma_{\mathrm{tors}} \to \Gamma \to \Gamma/\Gamma_{\mathrm{tors}} \to 0$$

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

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 Γ. There is a canonical isomorphism*

$$\Gamma/\Gamma_{\mathrm{tors}} \xrightarrow{\sim} A \otimes_{\mathbb{Z}} \mathbb{Q} \tag{3.1}$$

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

Moreover, there is an isomorphism

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

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

Proof. Since Γ/A is torsion, for every $b \in \Gamma$ there is an integer $n \geqslant 1$ such that $nb \in A$. Let $n_b := \min\{n \in \mathbb{N}_{\geqslant 1} \mid nb \in A\}$. 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 ψ is a group homomorphism. To see this, notice first that for every $b \in \Gamma$ and every $n \in \mathbb{N}_{\geqslant 1}$ 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 ψ is also surjective: in fact, let $a \in A$ and $n \in \mathbb{N}_{\geqslant 1}$. Since Γ 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 $\ker \psi = \Gamma_{\mathrm{tors}}$. If $b \in \Gamma$ has order $n \geqslant 1$, 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 $b \in \Gamma_{\mathrm{tors}}$. So we get an isomorphism which sends A/A_{tors} to $\overline{A}$.

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 $\Gamma/\Gamma_{\mathrm{tors}} \xrightarrow{\sim} \mathbb{Q}^r$ that sends A/A_{tors} to $\mathbb{Z}^r \subseteq \mathbb{Q}^r$. The conclusion follows by combining this with any isomorphism $\Gamma \xrightarrow{\sim} (\Gamma/\Gamma_{\mathrm{tors}}) \oplus (\mathbb{Q}/\mathbb{Z})^s$ (see Remark 3.18). □

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_{tors}), a splitting isomorphism $\Gamma \cong (\Gamma/\Gamma_{\mathrm{tors}}) \oplus \Gamma_{\mathrm{tors}}$ (see Remark 3.18) and an isomorphism $\Gamma_{\mathrm{tors}} \cong (\mathbb{Q}/\mathbb{Z})^s$.

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 Γ be a full s-extension of A. Notice that, since $A_{\mathrm{tors}} = 0$, we have $\mathrm{Aut}_{A_{\mathrm{tors}}}(\Gamma_{\mathrm{tors}}) = \mathrm{Aut}(\Gamma_{\mathrm{tors}})$ and $\Gamma_{n,\mathrm{tors}} = \Gamma[n]$ 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

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

Recall from Remark 2.2 that we have canonical isomorphisms

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

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

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

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

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

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

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

and

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

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 Γ be a full s-extension of A. Consider the group $\mathrm{Aut}_A(\Gamma)$ with the profinite topology described in Section 3.3 and the groups $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ and $\mathrm{GL}_s(\widehat{\mathbb{Z}})$ 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

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

Moreover, the action of $\mathrm{Aut}(\Gamma_{\mathrm{tors}})$ on $\mathrm{Hom}\,(\Gamma/(A+\Gamma_{\mathrm{tors}}), \Gamma_{\mathrm{tors}})$ 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 $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ as a left $\mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$-module.

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

Proposition 4.1. *Let $R := \mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$ and view $M := \mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ 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 $(\mathbb{Q}/\mathbb{Z})^r \to (\mathbb{Q}/\mathbb{Z})^s$, we have*

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

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 $N\otimes_{\widehat{\mathbb{Z}}} L \to R$:

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

whose inverse is

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

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

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

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 $(\mathbb{Q}/\mathbb{Z})^r \to \mathbb{Q}/\mathbb{Z}$, 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 ψ 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 $V \supseteq nM$. □

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

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

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. □

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

Proposition 4.3. *Let $R := \mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$ and view $M := \mathrm{Mat}_{s\times r}(\mathbb{Z}_\ell)$ as a left R-module. Let H be a closed subgroup of $\mathrm{GL}_s(\mathbb{Z}_\ell)$ 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 $V \supseteq S \cdot V \supseteq \ell^m R \cdot V = \ell^m W \supseteq \ell^m \cdot \ell^n M$. □

The following result is an adelic version of Proposition 4.3.

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

(1) $W \supseteq nM$*;*

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

Then we have $V \supseteq nmM$.

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

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

Let moreover V_ℓ and W_ℓ denote the images of V and W in M_ℓ, respectively. Notice that V_ℓ is an H_ℓ-submodule of M_ℓ and that W_ℓ is the R_ℓ-submodule of M_ℓ generated by V_ℓ.

By (1) we have that W_ℓ contains the image of nM in M_ℓ, which is nM_ℓ. By (2) we have $\mathbb{Z}_\ell[H_\ell] \supseteq m\,\mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$, 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 ℓ-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_ℓ is the image of V under the natural projection, for every ℓ there must be $\tilde{w}_\ell \in V$ whose ℓ-component is w_ℓ. Then the infinite sum

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

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

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

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

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

for some integer N and some open neighbourhoods U_ℓ of w_ℓ in M_ℓ; then clearly $x_k \in U$ for all $k \geqslant N$.

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 ℓ the multiplication-by-ℓ endomorphism on a $\widehat{\mathbb{Z}}$-module is invertible on all prime-to-ℓ 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. □

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 $G(\overline{K})$

$$\Gamma := \left\{P \in G(\overline{K}) \mid \exists\, n \in \mathbb{N}_{\geqslant 1} :\ nP \in A\right\} \tag{5.1}$$

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

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

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

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

Definition 5.1. We call any integer $d_A > 1$ such that $d_A(\Gamma \cap G(K)) \subseteq A + G(K)_{\mathrm{tors}}$ 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 $(\Gamma \cap G(K))/(A + G(K)_{\mathrm{tors}})$ 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 ℓ there is a non-negative integer m_ℓ such that the ℓ-power torsion of $(\Gamma \cap G(K))/(A + G(K)_{\mathrm{tors}})$ is contained in

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

and that we can take $m_\ell = 0$ for all but finitely many primes ℓ. The first part is just [DP16, Lemma 12]. As for the second part, assume that A admits a strongly ℓ-independent basis $a_1, \dots, a_r$ as in [PS19, Definition 2.1], which is true for all but finitely many ℓ 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 $m \geqslant 1$. 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 ℓ. Since the a_i are strongly ℓ-independent, every x_i is divisible by ℓ^m. This means that $b \in A \cdot \mu(K) = A + G(K)_{\mathrm{tors}}$, 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

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

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 $K(G_{\mathrm{tors}})$ by K_∞. 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 $\mathrm{Gal}(\overline{K} \mid K)$ on $G(\overline{K})$ gives rise, for every $n \geqslant 1$, to injective homomorphisms

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

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

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

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

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

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

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

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

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

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

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

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

Then we get a diagram with exact rows

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

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

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

the **Kummer representation**, and the map

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

the **torsion representation**.

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

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 $\operatorname{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ and $\operatorname{GL}_2(\widehat{\mathbb{Z}})$, 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 $\operatorname{Ent}(A) \cong \operatorname{Mat}_{s\times r}(\widehat{\mathbb{Z}})/V(A)$.

Remark 5.5. It follows from the existence of the Kummer representation that for any $n \geqslant 1$ 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 $\operatorname{Aut}_A(\Gamma)$ by the image of $\operatorname{Gal}(K(\Gamma) \mid K)$, 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 $\mathrm{Ent}(A)$ is finite, then for every $n \geqslant 1$*

$$\frac{n^{rs}}{[K\left(n^{-1}A\right) : K\left(G[n]\right)]} \quad \textit{divides} \quad \#\,\mathrm{Ent}(A)\,.$$

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

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

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

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

□

5.3 Bounding the entanglement group

We now give some sufficient conditions for the finiteness of the entanglement group $\mathrm{Ent}(A)$. 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 $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ as maps $(\mathbb{Q}/\mathbb{Z})^r \to (\mathbb{Q}/\mathbb{Z})^s$. The image of any $[b] \in \Gamma/(A + G_{\mathrm{tors}})$ 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 $\sigma \in \mathrm{Gal}(K(\Gamma) \mid K_\infty)$, that is if and only if $b \in G(K_\infty)$. So we have

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

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

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

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

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

which we also denote by φ.

Proposition 5.8. *The kernel of $\varphi : S(A) \to H^1(\mathrm{Gal}(K_\infty \mid K), G_{\mathrm{tors}})$ is contained in $S(A)[d_A]$. In particular, if $H^1(\mathrm{Gal}(K_\infty \mid K), G_{\mathrm{tors}})$ 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 φ_b is a coboundary. We want to show that $d_A b \in A + G_{\mathrm{tors}}$. Since φ_b is a coboundary, there is $t_0 \in G_{\mathrm{tors}}$ such that for all $\sigma \in \mathrm{Gal}(K_\infty \mid K)$ 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 $d_A b = d_A(b - t_0) + d_A t_0 \in d_A(\Gamma \cap G(K)) + G_{\mathrm{tors}}$. Since d_A is a divisibility parameter for A we have

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

so that

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

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

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 $n \geqslant 1$ and that $H(G)$ denotes the image of $\mathrm{Gal}(K_\infty \mid K)$ in $\mathrm{GL}_s(\widehat{\mathbb{Z}})$.

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 ℓ, let $H_\ell(G)$ denote the image of $H(G)$ under the projection $\mathrm{GL}_s(\widehat{\mathbb{Z}}) \to \mathrm{GL}_s(\mathbb{Z}_\ell)$ and denote by $\mathbb{Z}_\ell[H_\ell(G)]$ the closed sub-$\mathbb{Z}_\ell$-algebra of $\mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$ 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 $n \geqslant 1$ such that $\mathbb{Z}_\ell[H_\ell(G)] \supseteq n\,\mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$ for every prime ℓ.

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

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

Proof. Let $\Gamma := \left\{P \in G(\overline{K}) \mid \exists\, n \in \mathbb{N}_{\geqslant 1} : nP \in A\right\}$ 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 $\mathrm{GL}_s(\widehat{\mathbb{Z}})$ and $V(A)$ with a subgroup of $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$, 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 $\mathrm{GL}_s(\widehat{\mathbb{Z}})$-submodule of $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ generated by $V(A)$ contains $d_A m\,\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$. This property and (2) allow us to apply Proposition 4.4 and deduce that the index of $V(A)$ in $\mathrm{Mat}_{s\times r}(\widehat{\mathbb{Z}})$ divides $(d_A nm)^{rs}$. □

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 $C \geqslant 1$ such that for every $n \geqslant 1$ the ratio

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

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

(1) The group A has finite divisibility (see Example 5.2).

(2) The torsion representation $\tau : \mathrm{Gal}(K_\infty \mid K) \to \mathrm{GL}_1(\widehat{\mathbb{Z}}) = \widehat{\mathbb{Z}}^\times$ 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 $[K : \mathbb{Q}]\,\mathrm{Mat}_{s\times s}(\mathbb{Z}_\ell)$ for every prime ℓ.

(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

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

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 $\mathrm{End}_K(E) = \mathbb{Z}$. 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 $\mathrm{Ent}(A)$. 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 $E(K)/E(K)_{\mathrm{tors}}$, then we can compute d_A effectively. In fact, let $\overline{E(K)} = E(K)/E(K)_{\mathrm{tors}}$ 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 $P \in \mathrm{GL}_\rho(\mathbb{Z})$ and $Q \in \mathrm{GL}_t(\mathbb{Z})$ 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 $d_1 \mid d_2 \mid \cdots \mid d_r$ 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 Γ is defined as in (5.1), we have that $(\Gamma \cap E(K))/E(K)_{\mathrm{tors}}$ is generated by $\{\mathbf{f}_1, \dots, \mathbf{f}_r\}$. We then have that $d_r(\Gamma \cap E(K)) \subseteq A + E(K)_{\mathrm{tors}}$, 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

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

and we will denote its image by $H(E)$. If ℓ is a prime we will denote by τ_ℓ the composition of τ_∞ with the natural projection $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ and by $H_\ell(E)$ the image of τ_ℓ.

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 $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ congruent to the identity modulo m_E. If ℓ is a prime, we call an integer $n_\ell \geqslant 1$ such that $H_\ell(E) \supseteq I + \ell^{n_\ell} \mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ a *parameter of maximal growth* for the ℓ-adic torsion representation. If $\ell = 2$ we require $n_\ell \geqslant 2$.

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_ℓ by just letting $n_\ell = \max(1, v_\ell(m_E))$. However, it is possible to give an effective bound for each n_ℓ (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 $m_E H^1(\mathrm{Gal}(K_\infty \mid K), E_{\mathrm{tors}}) = 0$.*

Proof. Let $G = \mathrm{Gal}(K_\infty \mid K)$ 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. □

Definition 6.4. Let K be a number field with absolute discriminant Δ_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 ℓ 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 ℓ.

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_{ℓ^∞} for the compositum of all ℓ-power division fields of E over K, and $K_{S(E)}$ for the compositum of the fields K_{ℓ^∞} 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*

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

is an isomorphism.

Remark 6.7. For every prime $\ell \notin S(E)$, the ℓ-adic representation associated with E is surjective. This follows from the fact that the mod ℓ torsion representation associated with E and the ℓ-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_ℓ be a parameter of maximal growth for the ℓ-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 $\mathrm{Gal}(K_\infty \mid K)$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ contains

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

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

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

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

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

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

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

Remark 6.9. We can give an explicit bound for the integers m_ℓ of the above corollary:

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

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 $\mathcal{O}_E = \mathrm{End}_{\overline{K}}(E)$ of E, which is an order in an imaginary quadratic number field F.

For every prime ℓ, the group

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

can be identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ via the action of $\mathcal{O}_E$ on the ℓ-power torsion of E, and is called the *Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ 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 γ and δ, 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 ℓ that either ramify in $K \cdot F$ or are such that E has bad reduction at some prime of K of characteristic ℓ. 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 $[\mathcal{C}(E) : H(E)] \leqslant 3[K : \mathbb{Q}]$ if $F \subseteq K$ and $[\mathcal{C}(E) : \mathcal{C}(E) \cap H(E)] \leqslant 6[K : \mathbb{Q}]$ 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 ℓ such that $(\ell - 1)$ divides e_K. Then we have $m_K H^1(\mathrm{Gal}(K_\infty \mid K), E_{\mathrm{tors}}) = 0$.

Proof. Let $k_2 = 3$ and, for any odd prime ℓ, let k_ℓ be an integer whose class modulo ℓ 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 $H^1(\mathrm{Gal}(K_\infty \mid K), E_{\mathrm{tors}})$. Since

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

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 $H^1(\mathrm{Gal}(K_\infty \mid K), E_{\mathrm{tors}}) = 0$ divides m_K. □

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

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

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

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 $\overline{K}$. 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_ℓ be a parameter of maximal growth for the ℓ-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 $n \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ for every prime number ℓ. 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 $H^1\left(\operatorname{Gal}(K_\infty \mid K), E_{\mathrm{tors}}\right)$ divides m.

Then by Theorem 5.9 we have that the order of $\operatorname{Ent}(A)$ divides $(d_A nm)^{2r}$. □

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

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

Theorem 6.16. *Let E be an elliptic curve over a number field K, with CM over $\overline{K}$ 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 ℓ let n_ℓ be a parameter of maximal growth for the ℓ-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 $\operatorname{Mat}_{r\times 2}(\widehat{\mathbb{Z}})$. More precisely, the order of $\operatorname{Ent}(A)$ 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 ℓ.

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

1. for every prime $\ell \notin S(E)$ we have
$$\mathbb{Z}_\ell[H_\ell(E)] = \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)\,;$$
2. for every prime $\ell \in S(E)$ we have
$$\mathbb{Z}_\ell[H_\ell(E)] \supseteq \ell^{n_\ell + v_\ell(4\delta_\ell)} \operatorname{Mat}_{2\times 2}(\mathbb{Z}_\ell)\,.$$

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]. □

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

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 ℓ-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 $H^1(\mathrm{Gal}(\mathbb{Q}_\infty \mid \mathbb{Q}), E_{\mathrm{tors}})$ divides C_1. The conclusion then follows from Theorem 5.9. □

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

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

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

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

which, by Lemma 5.7, implies that $\mathrm{Ent}(A)$ 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].

Chapter 4

Division in modules and Kummer theory

by Sebastiano Tronto [Tro21]

1 Introduction

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

If $G = \mathbb{G}_m$ is the multiplicative group, extensions of this kind are studied by classical Kummer theory. Explicit results for this case can be found for example in [PS19], [PST20b] and [PST20a]. 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 is free of rank r with a basis of points that are linearly independent over $\mathrm{End}_K(G)$, it is known that the ratio

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

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

In the case of elliptic curves, one may hope to obtain an explicit version of this result. Indeed the results of [Chapter 1] and [Chapter 3] provide such a statement under the assumption that $\mathrm{End}_K(G) = \mathbb{Z}$, and they show that an effective bound depends only on the abelian group structure of A and on the ℓ-adic Galois representations associated with the torsion of G for every prime ℓ.

It is clear from the above discussion that the existence of non-trivial endomorphisms defined over K plays an essential role in this theory. Without loss of generality we can take A to be an $\mathrm{End}_K(G)$-module, as done by Javan Peykar in his thesis [JP21]. This approach leads to an explicit "open image theorem" for Kummer extensions for CM elliptic curves, albeit under certain technical assuptions on $\mathrm{End}_K(G)$.

Motivated by [JP21] and by the author's previous results [Chapter 3], most of this paper is devoted to developing a general abstract framework for the study of certain *division modules* of a fixed R-module M, where R is any unitary ring. We strive to develop this theory in a way that is independent from the "ambient module" $G(\overline{K})$, taking inspiration from [Pal04] as well.

We introduce a natural generalization of the concept of injective modules, which to the author's knowledge is new. We also define a category of (J,T)-*extensions*, which shares many interesting properties with the category of field extensions. We believe that these topics are interesting in their own right.

At the end of the paper we prove the following result, which was previously known in this effective form only under certain restrictions on $\mathrm{End}_K(E)$:

Theorem. *Let E be an elliptic curve over a number field K, let $R = \mathrm{End}_K(E)$ and let M be an R-submodule of $E(K)$. There exists a positive integer c, depending only on the R-module structure of M and on the image of the Galois representations associated with the torsion of E, such that for every positive integer n*

$$\frac{n^{2\,\mathrm{rk}_R(M)}}{[K(n^{-1}M) : K(E[n])]} \qquad \textit{divides} \qquad c\,.$$

This result follows from Theorem 5.11, which is essentially an application of Theorem 5.4, which in turn is a generalization of [Chapter 3, Theorem 5.9]. The results on Galois representations needed to apply this general theorem are mostly taken from [Chapter 1], and it can be easily seen that the given bounds only depend on the ℓ-adic representations, so that the constant c of our main theorem is effectively computable.

1.1 Notation

In this paper, rings are assumed to be unitary, but not necessarily commutative; subrings always contain the multiplicative unit 1. Unless otherwise specified, by ideal of a ring we mean a right ideal and by module over a ring we mean a left module. If R is a ring and n is a positive integer, we will denote by $\mathrm{Mat}_{n\times n}(R)$ the ring of $n \times n$ matrices with coefficients in R.

We denote by $\mathbb{Z}$ the integers and by $\mathbb{Z}_{>0}$ the set of positive integers. If p is a prime number we denote by $\mathbb{Z}_p$ the completion of the ring $\mathbb{Z}$ at the ideal (p). We denote by $\widehat{\mathbb{Z}}$ the product of $\mathbb{Z}_p$ over all primes p, which we identify with $\varprojlim_{n\in\mathbb{Z}_{>0}} \mathbb{Z}/n\mathbb{Z}$.

1.2 Structure of the paper

In Section 2 we introduce the concept of *ideal filter* and of division module by an ideal filter. This provides us with a way to generalize the notion of injective module, and we are able to show the equivalent of Baer's criterion for injectivity and the existence of the analogue of injective hulls in this setting. At the end of Section 2 we prove a certain duality result for J-injective modules that will be applied in Section 5.

In Section 3 we construct the category of (J, T)-extensions, our abstraction for the modules of division points of an algebraic group. This category behaves similarly to that of field extensions of a given field. After studying an interesting pair of adjoint functors, we conclude this section by proving the existence of a *maximal* (J, T)-extension, in analogy with field theory.

Section 4 is devoted to the study of automorphism groups of (J, T)-extensions. The fundamental exact sequence of Theorem 4.10 gives us a framework to study the Galois groups of Kummer extensions associated with a commutative algebraic group, provided that some technical assumptions hold. This is what we do in Section 5, and we conclude by applying these results to elliptic curves.

Acknowledgements

I would like to thank my supervisors Antonella Perucca and Peter Bruin for their constant support. I would also like to thank Hendrik Lenstra and Peter Stevenhagen for the interesting discussion about the results of [JP21] which gave me the main ideas for this paper. Last but not least, I would like to thank Davide Lombardo for his comments on this paper, in particular for suggesting Remarks 5.1 and 5.12.

2 J-injectivity

2.1 Ideal filters and division in modules

In order to study division in modules over a general ring, we take inspiration from [JP21]. However, instead of using Steinitz ideals (that is, ideals of the completion of a ring), we use a more general concept that we now introduce.

Definition 2.1. Let R be a ring. We call a non-empty set J of right ideals of R an *ideal filter* if the following conditions hold:

1. If $I, I' \in J$ then $I \cap I' \in J$.
2. If $I \in J$ and I' is a right ideal containing I, then $I' \in J$.

The minimal ideal filter is $\{R\}$, while the maximal ideal filter contains all ideals (equivalently, it contains the zero ideal): we denote the former by 1 and the latter by 0.

For any ring R and any set S of right ideals of R we call the ideal filter *generated* by S the smallest ideal filter containing S: it consists of all ideals of R which contain a finite intersection of elements of S.

Example 2.2. We will be interested in the ideal filters generated by the powers of a given prime number p

$$p^\infty := \{I \text{ right ideal of } R \mid I \supseteq p^n R \text{ for some } n \in \mathbb{N}\}$$

and the one generated by all non-zero integers

$$\infty := \{I \text{ right ideal of } R \mid I \supseteq nR \text{ for some } n \in \mathbb{Z}_{>0}\} .$$

Notice that if $p^n = 0$ (resp. $n = 0$) for some $n \in \mathbb{Z}_{>0}$ then p^∞ (resp. ∞) is simply the maximal ideal filter 0. We will often consider such ideal filters in the case where R is a commutative integral domain of characteristic different from p (resp. characteristic 0).

Fix for the remainder of this section a ring R.

Definition 2.3. If $M \subseteq N$ are left R-modules, for any right ideal I of R we call

$$(M :_N I) := \{x \in N \mid Ix \subseteq M\}$$

the *I-division module of M in N*.

A similar concept for ideals of R is sometimes referred to as *quotient ideal*, but we deemed a change of terminology appropriate.

We can easily generalize this notion to ideal filters of R.

Definition 2.4. Let J be an ideal filter of R and let $M \subseteq N$ be left R-modules. We call

$$(M :_N J) := \bigcup_{I \in J} (M :_N I)$$

the *J-division module of M in N*. One can easily check that $(M :_N J)$ is an R-submodule of N.

Moreover, we call $N[J] := (0 :_N J)$ the *J-torsion submodule* of N. We call N a *J-torsion module* if $N = N[J]$.

Remark 2.5. If $J = 0$ then $(M :_N J) = N$ and $M[J] = M$. On the other hand, if $J = 1$ then $(M :_N J) = M$ and $M[J] = 0$.

Remark 2.6. Let $M \subseteq N$ be left R-modules and let J and J' be ideal filters of R with $J' \subseteq J$. If $M' \subseteq M$ and $N' \subseteq N$ are submodules with $M' \subseteq N'$, then it is clear from the definition of J-division module that $(M' :_{N'} J') \subseteq (M :_N J)$.

Definition 2.7. We say that an ideal filter J of R is *complete* if for every left R-module N and every submodule $M \subseteq N$ we have

$$((M :_N J) :_N J) = (M :_N J) \ .$$

We say that an ideal filter J is *product-closed* if for any $I, I' \in J$ we have $II' \in J$.

Proposition 2.8. *Let R be a ring and let J be a product-closed ideal filter of R. If for every $I \in J$ the left ideal RI is finitely generated, then J is complete. In particular, every product-closed ideal filter over a left-Noetherian ring is complete.*

Proof. Let J be a product-closed ideal filter of R and let $M \subseteq N$ be left R-modules. The inclusion $(M :_N J) \subseteq ((M :_N J) :_N J)$ is always true, so let us prove the other inclusion. Let $x \in N$ be such that there is $I \in J$ with $Ix \subseteq (M :_N J)$. Let $\{y_1, \dots y_n\}$ be a set of generators for the left ideal RI. Then for every $i = 1, \dots n$ there is $I_i \in J$ such that $I_i y_i x \subseteq M$. By definition of ideal filter we have $I' := \bigcap_{i=1}^n I_i \in J$ and since J is product-closed we have $I'I \in J$. Since $\{y_1, \dots, y_n\}$ is a set of generators of the left ideal RI and I' is a right ideal we have $I'Ix = I'(RI)x \subseteq M$, which shows that J is complete. □

Example 2.9. The ideal filters introduced in Example 2.2 are both product-closed. If, for example, R is Noetherian, then they are also complete.

We conclude this subsection with a list of properties of division modules.

Lemma 2.10. *Let $M \subseteq N \subseteq P$ and M' be left R-modules and let J and J' be ideal filters of R. Then the following properties hold:*

1. $(M :_N J) = (M :_P J) \cap N$.
2. $\left(M :_{(M:_N J)} J\right) = (M :_N J)$.
3. $(N/M)[J] = (M :_N J)/M$.
4. $(M :_N J) = N$ *if and only if* N/M *is* J*-torsion.*
5. $(M \oplus M')[J] = M[J] \oplus M'[J]$.

Proof.

1. The inclusion "$\subseteq$" is obvious; for the other inclusion it suffices to notice that if $n \in N$ is such that $In \subseteq M$ for some $I \in J$ then by definition $n \in (M :_N J)$.
2. Follows directly from (1).
3. We have
$$\begin{aligned}(N/M)[J] &= \bigcup_{I\in J}(N/M)[I] = \\ &= \bigcup_{I\in J}\{n+M \in N/M \mid I(n+M) = M\} = \\ &= \bigcup_{I\in J}\{n \in N \mid In \subseteq M\}/M = \\ &= \bigcup_{I\in J}(M :_N I)/M = \\ &= (M :_N J)/M\,.\end{aligned}$$
4. By (3) we have that $(N/M)[J] = N/M$ if and only if $(M :_N J) = N$.
5. For any right ideal I and any $(m, m') \in M \oplus M'$ we have that $I(m, m') = 0$ if and only if $Im = Im' = 0$. This implies that $(M \oplus M')[I] = M[I] \oplus M'[I]$, so we have
$$\begin{aligned}(M \oplus M')[J] &= \bigcup_{I\in J}(M \oplus M')[I] = \\ &= \bigcup_{I\in J} M[I] \oplus M'[I] = \\ &= M[J] \oplus M'[J].\end{aligned}$$

□

2.2 J-maps and J-extensions

Fix for this section a ring R and a complete ideal filter J of R. We introduce here some simple notions that will lead us closer to our definition of (J,T)-extensions.

Definition 2.11. Let M be a left R-module. An R-module homomorphism $\varphi : M \to N$ is called a *J-map* if $(\varphi(M) :_N J) = N$. If φ is injective we will call it a *J-extension*, and we say that N is a J-extension of M.

Remark 2.12. By Lemma 2.10(4) a homomorphism $\varphi : M \to N$ is a J-map if and only if $N/\varphi(M)$ is J-torsion. In particular, if $J = 0$, then every homomorphism of R-modules is a J-map.

It is clear from the definition that, if $\varphi : M \to N$ and $\psi : M \to P$ are two J-maps, then any R-module homomorphism $f : N \to P$ such that $f \circ \varphi = \psi$ is also a J-map.

The following lemma, which strongly relies on the assumption that J is complete, shows moreover that R-modules and J-maps form a subcategory of the category of R-modules.

Lemma 2.13. *Let M, N and P be R-modules and let $\varphi : M \to N$ and $\psi : N \to P$ be R-module homomorphisms. If φ and ψ are J-maps, then so is $\psi \circ \varphi$.*

Proof. Since J is complete we have

$$\begin{aligned} P &= (\psi(N) :_P J) = \\ &= \big((\psi\varphi(M) :_{\psi(N)} J) :_P J\big) \subseteq \\ &\subseteq ((\psi\varphi(M) :_P J) :_P J) = \\ &= (\psi\varphi(M) :_P J) \end{aligned}$$

hence $(\psi\varphi(M) :_P J) = P$ and $\psi \circ \varphi$ is a J-map. □

Remark 2.14. Any homomorphism of R-modules $\varphi : M \to N$ such that N is J-torsion is a J-map. In particular, the restriction of an R-module homomorphism to the J-torsion submodule is a J-map.

The following lemma illustrates how certain properties of a J-map largely depend on its restriction to the J-torsion submodule. Recall that an injective R-module homomorphism $f : M \hookrightarrow N$ is called an *essential extension* if for every submodule $N' \subseteq N$ we have $N' \cap f(M) = 0 \implies N' = 0$.

Lemma 2.15. *A J-map $\varphi : M \to N$ is essential if and only if $\varphi|_{M[J]} : M[J] \to N[J]$ is.*

Proof. Notice that the statement is trivially true in case $J = 0$, so we may assume that $J \neq 0$. If φ is essential then clearly so is $\varphi|_{M[J]}$, because any submodule N' of $N[J]$ such that $N' \cap \varphi(M[J]) = 0$ is in particular a submodule of N such that $N' \cap \varphi(M) = 0$.

Assume than that $\varphi|_{M[J]} : M[J] \to N[J]$ is essential. Let $N' \subseteq N$ be a non-trivial submodule and let $n \in N'$ be a non-zero element. If $n \in N[J]$ then $N' \cap N[J]$ is non-trivial, and since $\varphi|_{M[J]}$ is essential then $N' \cap \varphi(M)[J]$ is non-trivial as well. So we may assume that $n \notin N[J]$.

Since $\varphi : M \to N$ is a J-map, there is $I \in J$ such that $In \subseteq \varphi(M)$. In particular, since $0 \notin J$ and n is not J-torsion, there is $r \in R$ such that $0 \neq rn \in \varphi(M)$. Since N' is a submodule we have $rn \in N' \cap \varphi(M)$, so $\varphi : M \to N$ is an essential extension. □

Lemma 2.16. *Let $\varphi : M \to N$ be a J-map and let $f, g : N \to P$ be R-module homomorphisms such that $f \circ \varphi = g \circ \varphi$. Then for every $n \in N$ we have that $f(n) - g(n) \in P[J]$.*

Proof. The statement is clearly true for $J = 0$, so we may assume that $J \neq 0$. Since $(\varphi(M) :_N J) = N$ there is $I \in J$ such that $In \subseteq \varphi(M)$. In particular there is a non-zero $r \in I$ such that $rn \in \varphi(M)$, say $rn = \varphi(m)$ for some $m \in M$. This implies that

$$r(f(n) - g(n)) = f(\varphi(m)) - g(\varphi(m)) = 0$$

thus $f(n) - g(n) \in P[J]$. □

2.3 J-injective modules and J-hulls

Fix for this section a ring R and a complete ideal filter J of R. We introduce the notion of *J-injective module*, which generalizes the classical notion of injectivity.

Definition 2.17. A left R-module Q is called *J-injective* if for every J-extension $i : M \hookrightarrow N$ and every R-module homomorphism $f : M \to Q$ there exists a homomorphism $g : N \to Q$ such that $g \circ i = f$.

Remark 2.18. Notice that in case $J = 0$ the definition of J-injective R-module coincides with that of injective module. Moreover, if J' is a complete ideal filter of R such that $J' \subseteq J$, then a J-injective module is also J'-injective.

Example 2.19. A $\mathbb{Z}$-module is p^∞-injective if and only if it is p-divisible as an abelian group. The proof of this fact is completely analogous to that of the well-known result that a $\mathbb{Z}$-module is injective if and only if it is divisible.

The following proposition is an analogue of the well-known Baer's criterion in the classical case of injective modules.

Proposition 2.20. *A left R-module Q is J-injective if and only if for every two-sided ideal $I \in J$ and every R-module homomorphism $f : I \to Q$ there is an R-module homomorphism $g : R \to Q$ that extends f.*

Proof. The "only if" part is trivial, because any two-sided ideal of R is also a left R-module and $I \hookrightarrow R$ is a J-extension if $I \in J$. For the other implication, let $i : M \hookrightarrow N$ be a J-extension and let $f : M \to Q$ be any R-module homomorphism. By Zorn's Lemma there is a submodule N' of N and an extension $g' : N' \to Q$ of f to N' that is maximal in the sense that it cannot be extended to any larger submodule of N. If $N' = N$ we are done, so assume that $N' \neq N$ and let $x \in N \setminus N'$.

Let I be the two-sided ideal of R generated by $\{r \in R \mid rx \in N'\}$. Since $i(M) \subseteq N'$ and $(i(M) :_N J) = N$ there is $I' \in J$ such that $I'x \subseteq N'$, which implies $I' \subseteq I$, so also $I \in J$. By assumption the map $I \to Q$ that sends $y \in I$ to $g'(yx)$ extends to a map $h : R \to Q$. Since $\ker(R \to Rx)$ is contained in $\ker(h)$, the map h gives rise to a map $h' : Rx \to Q$ by sending $rx \in Rx$ to $h(r)$. By definition the restrictions of g' and h' to $N' \cap Rx$ coincide, so we can define a map $g'' : N' + Rx \to Q$ that extends both. This contradicts the maximality of g', so we conclude that $N' = N$. □

Remark 2.21. Let R be an integral domain and let J be the ideal filter 0 on R. Since R is an integral domain, the set of ideals $J' = J \setminus \{0\}$ is an ideal filter. Using Proposition 2.20 one can easily show that an R-module Q is J-injective if and only if it is J'-injective. Indeed, one implication holds, as remarked above, because $J \subseteq J'$, and for the other it is enough to notice that the unique map $0 \to Q$ can always be extended to the zero map on R.

One advantage of using J' instead of J is that the J'-torsion submodule may be different from the whole module.

Example 2.22. Let M be an abelian group, let p be a prime and let $J = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2. Then the localization $M[p^{-1}]$ is a J-injective $\mathbb{Z}$-module. Indeed, if $i : N \hookrightarrow P$ is a J-extension and $f : N \to M[p^{-1}]$ is any homomorphism then for every $x \in P$ there is $k \in \mathbb{N}$ such that $p^k x \in i(N)$, and one can define $g(x) := \frac{f(p^k x)}{p^k}$. It is easy to check that g is a well-defined group homomorphism such that $g \circ i = f$.

Proposition 2.23. *Let M be a J-injective R-module. If $f : M \hookrightarrow N$ is an essential J-extension, then it is an isomorphism.*

Proof. By definition of J-injectivity there is a map $g : N \to M$ such that $g \circ f = \mathrm{id}_M$. Then g is surjective and since f is an essential extension g is also injective, so it is an isomorphism. □

Recall that an *injective hull* of an R-module M is an essential extension $i : M \hookrightarrow N$ such that N is injective as an R-module. It is well-known that every R-module M admits an injective hull and that any two injective hulls $i : M \hookrightarrow \Omega$ and $j : M \hookrightarrow \Gamma$ are isomorphic via a (not necessarily unique) isomorphism that commutes with i and j, see [Bae40], [ES53] or [Fle68].

Lemma 2.24. *Let R be a ring and let M be a left R-module. If $i : M \hookrightarrow \Omega$ is an injective hull and $j : M \hookrightarrow N$ is an essential extension, there is an injective R-module homomorphism $\varphi : N \hookrightarrow \Omega$ such that $\varphi \circ j = i$. Moreover, $\varphi : N \hookrightarrow \Omega$ is an injective hull.*

Proof. Since Ω is injective there exists an R-module homomorphism $\varphi : N \to \Omega$ such that $\varphi \circ j = i$. Since i is injective and j is an essential extension, then also φ is injective.

The last part follows from the fact that Ω is injective and $\varphi : N \hookrightarrow \Omega$ is an essential extension, since $i : M \hookrightarrow \Omega$ is. □

We conclude this section by proving that every R-module admits a *J-hull*, which is the generalization of an injective hull:

Definition 2.25. Let M be a left R-module. A J-extension $\iota : M \hookrightarrow \Omega$ is called a *J-hull* of M if it is an essential extension and Ω is J-injective.

Remark 2.26. If $J = 0$ the definition of J-hull coincides with that of injective hull.

Remark 2.27. If $f_i : M_i \hookrightarrow N_i$, for $i = 1, \ldots, k$, are J-hulls, then the finite sum

$$\oplus_i f_i : \bigoplus_{i=1}^{k} M_i \hookrightarrow \bigoplus_{i=1}^{k} N_i$$

is a J-hull. Indeed $\bigoplus_i N_i$ is J-injective because it is a finite direct sum of J-injective modules, and it is easy to see that it is also an essential J-extension of $\bigoplus_i M_i$.

Lemma 2.28. *Let Q be a J-injective R-module and let $P \subseteq Q$ be any submodule. Then $(P :_Q J)$ is J-injective.*

Proof. Let $i : M \hookrightarrow N$ be a J-extension and let $f : M \to (P :_Q J)$ be any R-module homomorphism. Denote by $j : (P :_Q J) \hookrightarrow Q$ the inclusion. Since Q is J-injective, there is a map $g : N \to Q$ such that $g \circ i = j \circ f$. For every $x \in N$ there is some $I \in J$ such that $Ix \subseteq i(M)$ and thus $Ig(x) = g(Ix) \subseteq g(i(M)) = j(f(M))$, which means that the image of g is contained in $(P :_Q J)$. This shows that $(P :_Q J)$ is J-injective. □

Theorem 2.29. *Every left R-module M admits a J-hull. Moreover, the following holds for any J-hull $\iota : M \hookrightarrow \Omega$ of M:*

1. *For every J-extension $i : M \hookrightarrow N$ there is a J-hull $j : N \hookrightarrow \Omega$ with $j \circ i = \iota$.*
2. *For every J-hull $\iota' : M \hookrightarrow \Omega'$ there is an isomorphism $\varphi : \Omega \xrightarrow{\sim} \Omega'$ with $\varphi \circ \iota = \iota'$.*

Proof. Let $\iota : M \hookrightarrow \Gamma$ be an injective hull of M and let $\Omega := (\iota(M) :_\Gamma J)$. Since $\iota : M \hookrightarrow \Gamma$ is an essential extension then also $\iota : M \hookrightarrow \Omega$ is, and by Lemma 2.10(2) we have $(\iota(M) :_\Omega J) = \Omega$, so $\iota : M \hookrightarrow \Omega$ is a J-extension of M. By Lemma 2.28 the R-module Ω is J-injective, so it is a J-hull of M.

For (1), since Ω is J-injective there is a map $j : N \to \Omega$ such that $j \circ i = \iota$. Moreover since $\iota : M \hookrightarrow \Omega$ is an essential extension also $j : N \hookrightarrow \Omega$ is, so it is a J-hull.

For (2), let $\iota : M \hookrightarrow \Omega$ and $\iota' : M \hookrightarrow \Omega'$ be two J-hulls. Since Ω' is J-injective there is an R-module homomorphism $f : \Omega \to \Omega'$ such that $f \circ \iota = \iota'$, so since ι is an essential extension f is injective. But then, since $\mathrm{id}_\Omega : \Omega \hookrightarrow \Omega$ is a J-hull by (1), there is an R-module homomorphism $g : \Omega' \to \Omega$ such that $g \circ f = \mathrm{id}_\Omega$, so in particular g is surjective. But we also have $g \circ \iota' = \iota$, and since ι' is an essential extension then g must be injective too, hence it is an isomorphism. □

Example 2.30. Let M be a finitely generated abelian group, let p be a prime number and let $J = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2. Write M as

$$M = \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p^{e_i}\mathbb{Z} \oplus M[n]$$

where n is a positive integer coprime to p and the e_i's are suitable exponents. Let

$$\Gamma = (\mathbb{Z}[p^{-1}])^r \oplus (\mathbb{Z}[p^{-1}]/\mathbb{Z})^k \oplus M[n]$$

and

$$\begin{array}{rccc} \iota : & M & \to & \Gamma \\ & (z, (s_i \bmod p^{e_i})_i, t) & \mapsto & \left(\frac{z}{1}, \left(\frac{s}{p^{e_i}} \bmod \mathbb{Z}\right)_i, t\right) \end{array}$$

Then $\iota : M \to \Gamma$ is a J-hull. To see this it is enough to show that $f : \mathbb{Z}^r \hookrightarrow (\mathbb{Z}[p^{-1}])^r$ and $g_i : \mathbb{Z}/p^{e_i}\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]/\mathbb{Z}$ for every $i = 1, \ldots, k$ are J-hulls, and that $M[n]$ is J-injective, being trivially an essential extension of itself. The assertions about f and $M[n]$ follow from Example 2.22, noticing that multiplication by p is an automorphism of $M[n]$ and that $\mathbb{Z}^r \hookrightarrow (\mathbb{Z}[p^{-1}])^r$ is an essential J-extension.

So we are left to show that for every positive integer e the map $g : \mathbb{Z}/p^e\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]/\mathbb{Z}$ defined by $(s \bmod p^e) \mapsto (\frac{s}{p^e} \bmod \mathbb{Z})$ is a J-hull. It is a J-extension, because the Prüfer group $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ itself is J-torsion, and it is also essential because every subgroup of $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ is of the form $\frac{1}{p^d}\mathbb{Z}$, so it intersects the image of g in $\frac{1}{p^{\min(e,d)}}\mathbb{Z}$.

Finally, $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ is divisible as an abelian group, so in particular it is J-injective, since in this case it is equivalent to being p-divisible.

2.4 Duality

Fix again a ring R and a complete ideal filter J of R. Fix as well a left R-module M and a J-injective and J-torsion left R-module T and let $E = \mathrm{End}_R(T)$.

In this section we prove an elementary duality result that will be key to the proof of our main Kummer-theoretic results (Theorem 5.3).

Definition 2.31. If V is a subset of $\mathrm{Hom}_R(M,T)$ we denote by $\ker(V)$ the submodule of M given by

$$\ker(V) := \bigcap_{f \in V} \ker(f)$$

and we call it the *joint kernel* of V.

If M' is a submodule of M we will identify $\mathrm{Hom}_R(M/M', T)$ with the submodule $\{f \in \mathrm{Hom}_R(M,T) \mid \ker(f) \supseteq M'\}$ of $\mathrm{Hom}_R(M,T)$.

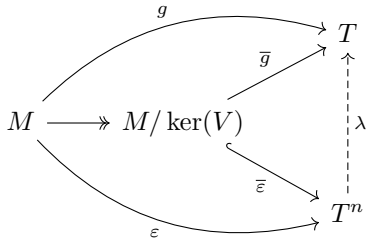
Proposition 2.32. *If V is a finitely generated E-submodule of $\mathrm{Hom}_R(M,T)$ we have $V = \mathrm{Hom}_R(M/\ker(V), T)$.*

Proof. Notice that the inclusion $V \subseteq \mathrm{Hom}_R(M/\ker(V), T)$ is obvious. For the other inclusion we want to show that every homomorphism $g : M \to T$ with $\ker(g) \supseteq \ker(V)$ belongs to V. Let then g be such a map and let $\overline{g} : M/\ker(V) \to T$ be its factorization through the quotient $M/\ker(V)$. Let $\{f_1, \ldots, f_n\}$ be a set of generators for V as an E-module and let

$$\begin{aligned} \varepsilon : M &\to T^n \\ x &\mapsto (f_1(x), \ldots, f_n(x)) \end{aligned}$$

We have $\ker(\varepsilon) = \ker(V)$, so that ε factors as an injective map $\overline{\varepsilon} : M/\ker(V) \to T^n$. Since T is J-torsion, so is T^n, hence $\overline{\varepsilon}$ is a J-extension. Since T is J-injective

there is an R-linear map $\lambda : T^n \to T$ such that $\lambda \circ \overline{\varepsilon} = \overline{g}$, or equivalently $\lambda \circ \varepsilon = g$.



Since $\mathrm{Hom}_R(T^n, T) \cong \bigoplus_{i=1}^n \mathrm{End}_R(T)$, there are elements $e_1, \ldots, e_n \in \mathrm{End}_R(T)$ such that $\lambda(t_1, \ldots, t_n) = e_1(t_1) + \cdots + e_n(t_n)$ for every $(t_1, \ldots, t_n) \in T^n$. Then for $x \in M$ we get

$$\begin{aligned} \lambda(\varepsilon(x)) &= \lambda(f_1(x), \ldots, f_n(x)) \\ &= e_1(f_1(x)) + \cdots + e_n(f_n(x)) \end{aligned}$$

which means that $g = e_1 \circ f_1 + \cdots + e_n \circ f_n \in V$ because V is an E-module. □

Remark 2.33. Proposition 2.32 is a generalization of the following fact from linear algebra: let V be a finite-dimensional vector space over a field K and let $f_1, \ldots, f_n : V \to K$ be linear functions. If $f : V \to K$ is a linear function such that $\ker(f) \supseteq \bigcap_{i=1}^n \ker(f_i)$, then f is a linear combination of $f_1, \ldots, f_n$.

Definition 2.34. Let N and Q be left R-modules. We say that Q is a *cogenerator* for N if $\ker(\mathrm{Hom}_R(N, Q)) = 0$.

Theorem 2.35. *Let R be a ring and let J be a complete ideal filter on R. Let T be a J-injective and J-torsion left R-module and let M be any left R-module. Assume that T is a cogenerator for every quotient of M and that* $\mathrm{Hom}_R(M, T)$ *is Noetherian as an* $\mathrm{End}_R(T)$*-module. The maps*

$$\begin{array}{ccc} \{R\text{-submodules of } M\} & \to & \{\mathrm{End}_R(T)\text{-submodules of } \mathrm{Hom}_R(M,T)\} \\ M' & \mapsto & \mathrm{Hom}_R(M/M', T) \\ \ker(V) & \leftarrow\!\shortmid & V \end{array}$$

define an inclusion-reversing bijection between the set of R-submodules of M and that of $\mathrm{End}_R(T)$*-submodules of* $\mathrm{Hom}_R(M, T)$.

Proof. Notice first the above maps are well-defined and they are both inclusion-reversing. Since $\mathrm{Hom}_R(M, T)$ is Noetherian as an $\mathrm{End}_R(T)$-module, every submodule is finitely generated, so we may apply Proposition 2.32. Since T is a cogenerator for every quotient of M we can conclude that the two given maps are inverse of each other. □

Example 2.36. Let $R = \mathbb{Z}$, let $J = \infty$ and let $T = (\mathbb{Q}/\mathbb{Z})^s$ for some positive integer s. Let M be a finitely generated abelian group. Notice that T is J-torsion and, since it is injective, it is in particular J-injective. Since $\mathbb{Q}/\mathbb{Z}$ is a cogenerator for every abelian group, so is T. We have $\mathrm{End}_R(T) = \mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$ and since M is finitely generated $\mathrm{Hom}_R(M,T)$ is Noetherian over $\mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$. We are then in the setting of Theorem 2.35.

3 The category of (J,T)-extensions

Fix for this section a ring R, a complete ideal filter J of R and a J-torsion and J-injective left R-module T.

In this section we introduce (J,T)-extensions, which are essentially J-extensions whose J-torsion is contained in an R-module T as above (see Definition 3.12). These extensions of R-modules share many interesting properties with field extensions, and in fact at the end of this section we will be able to prove the existence of a "maximal" (J,T)-extension, analogous to an algebraic closure in field theory.

3.1 T-pointed R-modules

In order to define (J,T)-extensions we first introduce the more fundamental concept of T-pointed R-module.

Definition 3.1. A *T-pointed R-module* is a pair (M,s), where M is a left R-module and $s : M[J] \hookrightarrow T$ is an injective homomorphism.

If (L,r) and (M,s) are two T-pointed R-modules, we call an R-module homomorphism $\varphi : L \to M$ a *homomorphism* or *map of T-pointed R-modules* if $s \circ \varphi|_{L[J]} = r$.

In the following we will sometimes omit the map s from the notation and simply refer to *the T-pointed R-module M*.

Remark 3.2. A map $\varphi : (L,r) \to (M,s)$ of T-pointed R-modules is injective on $L[J]$. Indeed $s \circ \varphi|_{L[J]} = r$ is injective, so $\varphi|_{L[J]}$ must be injective as well.

Definition 3.3. If (M,s) is a T-pointed R-module we denote the T-pointed R-module $(M[J],s)$ by $\mathfrak{tor}(M,s)$, or simply by $\mathfrak{tor}(M)$. We will denote the natural inclusion $\mathfrak{tor}(M) \hookrightarrow M$ by $\mathfrak{t}_M$.

Example 3.4. Let $R = \mathbb{Z}$ and let J be the complete ideal filter ∞ on $\mathbb{Z}$. Let $T = (\mathbb{Q}/\mathbb{Z})^2$, which is ∞-injective and ∞-torsion. The abelian group $M = \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ together with the map $s : \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that sends $(1,0)$ to $\left(\frac{1}{6},0\right)$ and $(0,1)$ to $\left(0,\frac{1}{2}\right)$ is a T-pointed R-module.

As is the case with field extensions, pushouts do not always exist in our newly-defined category. However the pushout of two maps of T-pointed R-modules exists if at least one of the two is injective and "as little a J-map as possible".

Definition 3.5. We say that a map $f : L \to M$ of T-pointed R-modules is *pure* if $(f(L) :_M J) = f(L) + M[J]$.

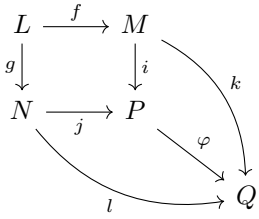
Proposition 3.6. *Let (L, r), (M, s) and (N, t) be T-pointed R-modules and let $f : L \to M$ and $g : L \to N$ be maps of T-pointed R-modules. Assume that f is injective and pure. Then the pushout $M \xrightarrow{i} P \xleftarrow{j} N$ of f along g exists in the category of T-pointed R-modules.*

Moreover the pushout map $j : N \to P$ is injective, and if g is injective the pushout map $i : M \to P$ is injective.

Proof. We have to show that there is a T-pointed R-module (P, u) with maps $i : M \to P$ and $j : N \to P$ such that the diagram

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle i} \\ N & \xrightarrow[j]{} & P \end{array}$$

commutes and such that for every T-pointed R-module (Q, v) with maps $k : M \to Q$ and $l : N \to Q$ with $k \circ f = l \circ g$ there is a unique map $\varphi : L \to Q$ such that the diagram



commutes.

Let P' be the pushout of f along g as maps of R-modules, and let $i' : M \to P'$ and $j' : N \to P'$ be the pushout maps. Write P' as $(M \oplus N)/S$ where $S = \{(f(\lambda), -g(\lambda)) \mid \lambda \in L\}$. Let $\pi : P' \to P$ be the quotient by the submodule

$$K := \langle \{[(m, -n)] \mid \text{for all } m \in M[J],\, n \in N[J] \text{ such that } s(m) = t(n)\} \rangle$$

and let $i = \pi \circ i'$ and $j = \pi \circ j'$. Notice that $i \circ f = j \circ g$.

We claim that $P'[J]$ is generated by $i'(M[J])$ and $j'(N[J])$. The claim is obviously true if $J = 0$, so we may assume that $J \neq 0$. To prove the claim, notice

that by Lemma 2.10(3) we have $P'[J] = (S :_{M\oplus N} J)/S$, so any element of $P'[J]$ is represented by a pair (m,n) such that $I(m,n) \subseteq S$ for some $I \in J$. Then since f is a pure map we have $m = f(\lambda) + t_m$ for some $\lambda \in L$ and some $t_m \in M[J]$.

Let $I' \in J$ be such that $I't_m = 0$. Then $I \cap I' \in J$ and for any nonzero $h \in I \cap I'$ we have $(f(h\lambda), hn) = h(m - t_m, n) = h(m,n) \in S$, which means that $hn = -g(h\lambda + z)$ for some $z \in \ker(f)$. Since f is injective we have that $n = -g(\lambda) + t_n$ for some $t_n \in N[J]$. It follows that the class of (m,n) in $P'[J]$ is the same as that of (t_m, t_n), which proves our claim.

Since $K \subseteq P'[J]$, it follows easily from our claim that $P[J] = P'[J]/K$ and thus that the map

$$\begin{aligned} u : P[J] &\to T \\ [(m,n)] &\mapsto s(m) + t(n) \end{aligned}$$

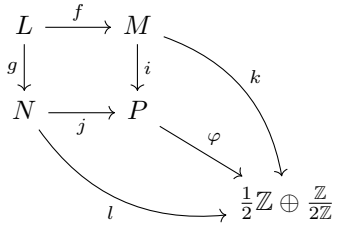
is well-defined and injective. This shows that (P,u) is a T-pointed R-module and that $i : M \to P$ and $j : N \to P$ are maps of T-pointed R-modules.

Let now (Q,v), k and l be as above. By the universal property of the pushout there is a unique R-module homomorphism $\varphi' : P' \to Q$ such that $\varphi' \circ i' = k$ and $\varphi' \circ j' = l$. Since k is a map of T-pointed R-modules, this implies that $v \circ \varphi' \circ i' = s$ and $v \circ \varphi' \circ j' = t$, so that φ' factors through P as a T-pointed R-module homomorphism $\varphi : P \to Q$.

For the last assertion we first notice that if g is injective, then so is the R-module pushout map i'. Then we claim that $i'(M) \cap K = 0$. Indeed if $[(m_0, 0)] = [(m, -n)]$ in P' for some $m_0 \in m$, $m \in M[J]$ and $n \in N[J]$ such that $s(m) = t(n)$, then there is some $\lambda \in L$ such that $m - m_0 = f(\lambda)$ and $n = g(\lambda)$. Since g is injective λ is J-torsion, and we have $r(\lambda) = s(m) - s(m_0) = t(n)$. But, since $s(m) = t(n)$, we must have $m_0 = 0$, and we conclude that $i'(M) \cap K = 0$. It follows that $i = \pi \circ i'$ is injective. Analogously, injectivity of f implies that of j. □

Remark 3.7. Let $R = \mathbb{Z}$, $J = 2^\infty$, $T = \mathbb{Z}\left[\frac{1}{2}\right]/\mathbb{Z}$, $L = \mathbb{Z}$ and $M = N = \frac{1}{2}\mathbb{Z}$. The R-modules L, M and N are T-pointed via the zero map, since their J-torsion is trivial. Let $f : L \hookrightarrow M$ and $g : L \hookrightarrow N$ be the natural inclusion and notice that they are maps of T-pointed R-modules that are not pure. We claim that the pushout of f along g does not exist in the category of T-pointed R-modules.

Suppose instead that (P,u) is a pushout of f along g and consider the T-pointed R-module $\left(\frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, z\right)$, where $z : \mathbb{Z}/2\mathbb{Z} \to T$ is the only possible injective map. Consider the diagram



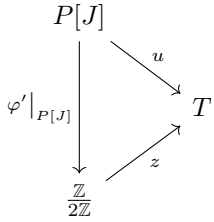
where the maps k and l are defined as

$$k: \begin{array}{ccc} \frac{1}{2}\mathbb{Z} & \to & \frac{1}{2}\mathbb{Z} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \\ \frac{1}{2} & \mapsto & \left(\frac{1}{2}, 0\right) \end{array} \qquad l: \begin{array}{ccc} \frac{1}{2}\mathbb{Z} & \to & \frac{1}{2}\mathbb{Z} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \\ \frac{1}{2} & \mapsto & \left(\frac{1}{2}, 1\right) \end{array}$$

and

Notice that k and l are maps of T-pointed R-modules such that $k \circ f = l \circ g$. Then by assumption there exists a unique map of T-pointed R-modules $\varphi : P \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that makes the diagram commute. In particular we have $\varphi(j(\frac{1}{2})) \neq \varphi(i(\frac{1}{2}))$, which implies that $j(\frac{1}{2}) \neq i(\frac{1}{2})$. But since $2j(\frac{1}{2}) = j(g(1)) = i(f(1)) = i(\frac{1}{2})$ we have that $t := j(\frac{1}{2}) - i(\frac{1}{2})$ is a 2-torsion element of P, and we must have $u(t) = \frac{1}{2}$.

Consider now the map $k' : M \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ mapping $\frac{1}{2}$ to $\left(\frac{1}{2}, 0\right)$, just as l does. This is again a map of T-pointed R-modules such that $k' \circ f = l \circ g$, so there must be a map of T-pointed R-modules $\varphi' : P \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that makes this new diagram commute. Such a map φ' must map t to 0, because $\varphi'(j(\frac{1}{2})) = \left(\frac{1}{2}, 0\right) = \varphi'(i(\frac{1}{2}))$. But then the diagram of structural maps into T



would not commute, which is a contradiction. This proves our claim.

The class of T-pointed R-modules whose torsion submodule is isomorphic to T will be particularly important for us.

Definition 3.8. Let (M, s) be a T-pointed R-module. We say that (M, s) is *saturated* if $\mathfrak{t}_M : M[J] \hookrightarrow T$ is surjective (and hence an isomorphism).

Remark 3.9. The map $\mathfrak{t}_M$ is a pure and injective map.

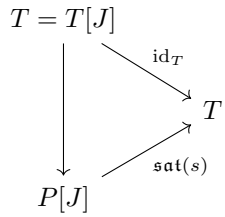
Every T-pointed R-module can be embedded in a saturated module, and the smallest saturated module containing a given one can be constructed as a pushout.

Definition 3.10. If (M, s) is a T-pointed R-module we call *saturation* of (M, s), denoted by $\mathfrak{sat}(M, s)$ or simply by $\mathfrak{sat}(M)$, the T-pointed R-module (P, u) which is the pushout (in the category of T-pointed R-modules) of the diagram

$$\begin{array}{ccc} M[J] & \xhookrightarrow{\mathfrak{t}_M} & M \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle \mathfrak{s}_M} \\ T & \longrightarrow & P \end{array}$$

We will also denote by $\mathfrak{sat}(s)$ the map u and by $\mathfrak{s}_M$ the pushout map $M \to P$.

Remark 3.11. Notice that the pushout map $T \to P$ of Definition 3.10 is an isomorphism onto $P[J]$. Indeed by definition of T-pointed R-module the following diagram commutes:



where the vertical map on the left is the pushout map. It follows that $\mathfrak{sat}(s)$, which is injective by definition, is also surjective, hence an isomorphism, and the pushout map is its inverse. In other words, the saturation of a T-pointed R-module is saturated.

3.2 (J, T)-extensions

We can finally introduce the main object of study of this section.

Definition 3.12. Let (M, s) be a T-pointed R-module. A (J, T)-*extension* of (M, s) is a triple (N, i, t) such that (N, t) is a T-pointed R-module and $i : M \hookrightarrow N$ is a map of T-pointed R-modules and a J-extension.

If (N, i, t) and (P, j, u) are two (J, T)-extensions of (M, s) we call a homomorphism of T-pointed R-modules $\varphi : N \to P$ a *homomorphism* or *map of* (J, T)-*extensions* if $\varphi \circ i = j$.

We denote by $\mathfrak{JT}(M, s)$ the category of (J, T)-extensions of (M, s).

In the following we will sometimes omit the maps i and t from the notation and simply refer to *the* (J,T)*-extension* N *of* M.

Remark 3.13. Let (N,i,t) and (P,j,u) be (J,T)-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of (J,T)-extensions. Then (P,φ,u) is a (J,T)-extension of (N,t). In fact we have

$$(\varphi(N) :_P J) \supseteq (j(M) :_P J) = P\,.$$

Example 3.14. Let $R = \mathbb{Z}$, let J be the complete ideal filter 2^∞ of $\mathbb{Z}$ and let T be the 2^∞-torsion and 2^∞-injective $\mathbb{Z}$-module $\left(\mathbb{Z}\left[\frac{1}{2}\right]/\mathbb{Z}\right)^2$. If $M = \mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ then the map $s : \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \to T$ that sends $(1,0)$ to $\left(\frac{1}{2},0\right)$ and $(0,1)$ to $\left(0,\frac{1}{2}\right)$ turns (M,s) into a T-pointed R-module.

Let $N = \frac{1}{2}\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. The maps

$$\begin{array}{rcl} t_1 : \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & \to & T \\ (1,0) & \mapsto & \left(\frac{1}{4},0\right) \\ (0,1) & \mapsto & \left(0,\frac{1}{2}\right) \end{array} \quad \text{and} \quad \begin{array}{rcl} t_2 : \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & \to & T \\ (1,0) & \mapsto & \left(0,\frac{1}{4}\right) \\ (0,1) & \mapsto & \left(\frac{1}{2},0\right) \end{array}$$

define two different T-pointed R-module structures (N,t_1) and (N,t_2) on N. The componentwise inclusion $f : M \hookrightarrow N$ is a 2^∞ extension. Since it is compatible with all the maps to T, both (N,f,t_1) and (N,f,t_2) are $(2^\infty,T)$-extensions of M. They are not isomorphic as $(2^\infty,T)$-extensions, because they are not isomorphic as T-pointed R-modules.

We can immediately see some similarities between (J,T)-extensions and field extensions: every map is injective, and every surjective map is an isomorphism.

Lemma 3.15. *Every map of* (J,T)*-extensions is injective.*

Proof. Let (N,i,t) and (P,j,u) be (J,T)-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of (J,T)-extensions. Let $n \in \ker\varphi$. Since $i : M \hookrightarrow N$ is a J-extension there is $I \in J$ such that $In \subseteq i(M)$. But since $j : M \hookrightarrow P$ is injective and $\varphi(In) = 0$, we must have $In = 0$, hence n is J-torsion. But since φ is a map of T-pointed R-modules it is injective on $M[J]$ (see Remark 3.2) so $n = 0$. □

Corollary 3.16. *Every surjective map of* (J,T)*-extensions is an isomorphism.*

Proof. Let (N,i,t) and (P,j,u) be (J,T)-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of (J,T)-extensions. In view of Lemma 3.15 it is enough to show that if φ is an isomorphism of R-modules, then its inverse $\varphi^{-1} : P \xrightarrow{\sim} N$ is also a map of (J,T)-extensions. But the fact that $\varphi^{-1}\circ j = i$ follows directly from $\varphi\circ i = j$ while $t = u\circ\varphi|^{-1}_{P[J]} = u$ follows from $u\circ\varphi|_{N[J]} = t$. □

Proposition 3.17. *Let (M, s) be a T-pointed R-module, let (N, i, t) be a (J, T)-extension of (M, s) and let (P, j, u) be a (J, T)-extension of (N, t). Then $(P, j \circ i, u)$ is a (J, T)-extension of (M, s).*

Proof. The map $j \circ i$ is clearly a J-injective map of T-pointed R-modules, and it is a J-map by Lemma 2.13. □

3.3 Pullback and pushforward

One can recover much information about the (J, T)-extensions of a certain T-pointed R-module by studying the extensions of its torsion submodule and of its saturation – see for example our construction of the maximal (J, T)-extension in Section 3.4. In order to study the relation between these categories, we introduce the more general pullback and pushforward functors which, interestingly, form an adjoint pair.

Definition 3.18. If $\varphi : L \to M$ is a map of T-pointed R-modules and (N, i, t) is a (J, T)-extension of M, we let

$$\varphi^* N := (i(\varphi(L)) :_N J) , \qquad \varphi^* i := i|_{\varphi(L)} , \qquad \varphi^* t := t|_{(\varphi^* N)[J]}$$

and we call them the *pullback along* φ of N, i and t respectively.

Lemma 3.19. *Let $\varphi : L \to M$ be a map of T-pointed R-modules and let (N, i, t) be a (J, T)-extension of M. Then $(\varphi^* N, \varphi^* i, \varphi^* t)$ is a (J, T)-extension of $\varphi(L)$.*

Proof. Clearly $(\varphi^* N, \varphi^* t)$ is a T-pointed R-module and

$$\varphi^* t \circ \varphi^* i|_{\varphi(L)[J]} = t \circ i|_{\varphi(L)[J]} = s|_{\varphi(L)}$$

so $\varphi^* i : (\varphi(L), s|_{\varphi(L)}) \to (\varphi^* N, \varphi^* t)$ is an injective map of T-pointed R-modules.

Moreover $(\varphi^* i(\varphi(L)) :_{\varphi^* N} J) = \varphi^* N$ by definition and by Lemma 2.10(2), so that $(\varphi^* N, \varphi^* i, \varphi^* t)$ is a J-extension. □

Definition 3.20. If $\varphi : L \to M$ is a map of T-pointed R-modules, N and P are (J, T)-extensions of M and $f : N \to P$ is a map of (J, T)-extensions, the map

$$f|_{\varphi^* N} : \varphi^* N \to \varphi^* P$$

is a map of (J, T)-extensions of $\varphi(L)$, which we denote by $\varphi^* f$.

Proposition 3.21. *Let $\varphi : L \to M$ be a map of T-pointed R-modules. The diagram*

$$\begin{array}{ccc} (N,i,t) & \longmapsto & (\varphi^*N, \varphi^*i, \varphi^*t) \\ \downarrow f & & \downarrow \varphi^* f \\ (P,j,u) & \longmapsto & (\varphi^*P, \varphi^*j, \varphi^*u) \end{array}$$

defines a functor from $\mathfrak{JT}(M,s)$ *to* $\mathfrak{JT}(\varphi(L),\, s|_{\varphi(L)})$.

Proof. In view of Lemma 3.19 we only need to check that φ^* behaves well with the respect to the composition of maps of (J,T)-extensions. If

$$N \xrightarrow{f} P \xrightarrow{g} Q$$

are maps of (J,T)-extensions of (M,s), we have

$$\varphi^* g \circ \varphi^* f = g|_{\varphi^* P} \circ f|_{\varphi^* N} = (g \circ f)|_{\varphi^* N} = \varphi^*(g \circ f)\,.$$

□

Definition 3.22. We call the functor of Proposition 3.21 the *pullback along* φ, and we denote it by φ^*.

Definition 3.23. If $\varphi : L \to M$ is an injective and pure map of T-pointed R-modules and (N,i,t) is a (J,T)-extension of L we denote by $\varphi_* i : M \to \varphi_* N$ the pushout of i along φ.

Lemma 3.24. *Let* $\varphi : L \to M$ *be an injective and pure map of* T*-pointed* R*-modules and let* (N,i,t) *be a* (J,T)*-extension of* L*. Then* $(\varphi_* N, \varphi_* i, \varphi_* t)$ *is a* (J,T)*-extension of* (M,s).

Proof. This follows from the fact that $\varphi_* i$ is injective and $\varphi_* N/(\varphi_* i)(M) \cong N/i(L)$ is J-torsion, because $i : L \to N$ is a J-extension. □

Lemma 3.25. *Let* $\varphi : L \to M$ *be an injective and pure map of* T*-pointed* R*-modules, let* (N,i,t) *and* (P,j,u) *be* (J,T)*-extensions of* L *and let* $f : N \to P$ *be a map of* (J,T)*-extensions. Then there is a unique map of* (J,T)*-extensions of* M

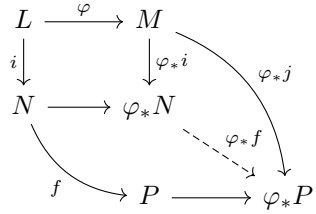
$$\varphi_* f : \varphi_* N \to \varphi_* P$$

such that the diagram

$$\begin{array}{ccc} N & \longrightarrow & \varphi_* N \\ \downarrow f & & \downarrow \varphi_* f \\ P & \longrightarrow & \varphi_* P \end{array}$$

commutes, where the horizontal maps are the pushout maps.

Proof. It is enough to apply the universal property of the pushout of $\varphi_* N$ to the diagram



Indeed the map $\varphi_* f : \varphi_* N \to \varphi_* P$, whose existence is ensured by the universal property, is such that $\varphi_* P / \varphi_* f(\varphi_* N) \cong P/f(N)$ is J-torsion. □

Proposition 3.26. *Let $\varphi : L \to M$ be an injective and pure map of T-pointed R-modules. The diagram*

$$\begin{array}{ccc} (N,i,t) & \longmapsto & (\varphi_* N, \varphi_* i, \varphi_* t) \\ \downarrow f & & \downarrow \varphi_* f \\ (P,j,u) & \longmapsto & (\varphi_* P, \varphi_* j, \varphi_* u) \end{array}$$

where $\varphi_* f$ is as in Lemma 3.25, defines a functor from $\mathfrak{JT}(L,r)$ to $\mathfrak{JT}(M,s)$.

Proof. In view of Lemmas 3.24 and 3.25 it is enough to show that φ_* behaves well with respect to the composition of maps of (J,T)-extensions. This is immediate from the construction in Lemma 3.25 and the uniqueness part of the universal property of the pushout. □

Definition 3.27. We call the functor of Proposition 3.26 the *pushforward along* φ, and we denote it by φ_*.

Theorem 3.28. *Let $\varphi : (L,r) \hookrightarrow (M,s)$ be an injective pure map of T-pointed R-modules. Then the functor φ_* is left adjoint to φ^*.*

Proof. Since φ is injective we will, for simplicity, denote $\varphi(L)$ by L.

Let (N,i,t) be a (J,T)-extension of L and let (P,j,u) be a (J,T)-extension of M. We want to show that we have

$$\mathrm{Hom}_{\mathfrak{JT}(L,r)}(N, \varphi^* P) \cong \mathrm{Hom}_{\mathfrak{JT}(M,s)}(\varphi_* N, P)$$

naturally in N and P.

Let $f : N \to \varphi^* P$ be a map of (J,T)-extensions of L; notice that in particular $f \circ i = \varphi^* j$. Composing f with the natural inclusion $\varphi^* P \hookrightarrow P$ we get a map of

T-pointed R-modules $f' : N \to P$ such that $f' \circ i = j \circ \varphi$, so by the universal property of the pushout there exists a unique map $g : \varphi_* N \to P$ that is a map of (J,T)-extensions of M.

We define a map

$$\Psi_{N,P} : \mathrm{Hom}_{\mathfrak{J}\mathfrak{T}(L,r)}(N, \varphi^* P) \to \mathrm{Hom}_{\mathfrak{J}\mathfrak{T}(M,s)}(\varphi_* N, P)$$

by letting $\Psi_{N,P}(f) := g$. The map Ψ is natural in N and P, since it is defined by means of a universal property. Indeed, if $h : N' \to N$ is a map of (J,T)-extensions of L and $f' = f \circ h$ then $\Psi_{N',P}(f')$ is by definition the unique map $\varphi_* N' \to P$ that makes the pushout diagram commute so it must coincide with $g \circ \varphi_* h$. Similarly if $k : P \to P'$ is a map of (J,T)-extensions of M then $\Psi_{N,P'}(\varphi^* k \circ f)$ must coincide with $k \circ g$.

To see that the map $\Psi_{N,P}$ is injective, let $f' : N \to \varphi^* P$ be another map and assume that $\Psi_{N,P}(f) = \Psi_{N,P}(f')$. But then the composition of $\Psi_{N,P}(f)$ with the pushout map $N \to \varphi_* N$ coincides with the composition of f and the natural inclusion $\varphi^* P \hookrightarrow P$, and analogously for f', so we conclude that $f = f'$.

To see that $\Psi_{N,P}$ is surjective, let $g' : \varphi_* N \to P$ be a map of (J,T)-extensions of M. Then by definition of pullback its composition with $N \to \varphi_* N$ factors through $\varphi^* P \hookrightarrow P$ as a map of (J,T)-extensions $f' : N \to \varphi^* P$, and again by the uniqueness of the map of the universal property of the pushout one can check that $\Psi_{N,P}(f') = g'$. □

Remark 3.29. Let $\varphi : L \hookrightarrow M$ be an injective and pure map of T-pointed R-modules and let (N, i, t) and (P, j, u) be (J,T)-extensions of L and M respectively. We can give an explicit description of the unit

$$\eta_N : N \to \varphi^* \varphi_* N$$

and the counit

$$\varepsilon_P : \varphi_* \varphi^* P \to P$$

of the adjunction.

Notice that the pushout map $N \to \varphi_* N$ is injective. Moreover, since N is a J-extension of L, the image of this map is contained in $\varphi^* \varphi_* N = (\varphi_* i(\varphi(L)) :_{\varphi_* N} J)$. The resulting inclusion $N \hookrightarrow \varphi^* \varphi_* N$ is the unit η_N.

By definition $\varphi^* P$ is contained in P, and the diagram

$$\begin{array}{ccc} L & \xhookrightarrow{\varphi} & M \\ \downarrow & & \downarrow j \\ \varphi^* P & \hookrightarrow & P \end{array}$$

commutes, so by the universal property of the pushout there exists a map $\varphi_* \varphi^* P \to P$. This map is the counit ε_P.

The following examples of pullback and pushforward functors are of particular importance to us, because they will be key to the construction of maximal (J,T)-extensions.

Definition 3.30. Let M be a T-pointed R-module and let $\mathfrak{t}_M : M[J] \to M$ be the natural inclusion of its torsion submodule. We will call the pullback functor $\mathfrak{t}_M^*$ the *torsion* functor and we will denote it by $\mathfrak{tor}$.

Remark 3.31. For every (J,T)-extension of $\mathfrak{tor}(M)$ the unit map

$$\eta_N : \mathfrak{tor}((\mathfrak{t}_M)_* N) \to N$$

is an isomorphism. Indeed, we have $\mathfrak{tor}((\mathfrak{t}_M)_* N) = ((\mathfrak{t}_M)_* N)[J] = N[J]$, and since N is a (J,T)-extension of a J-torsion module and J is complete then $N[J] = N$.

Notice that the inclusion $\mathfrak{s}_M$ of a T-pointed R-module into its saturation is injective and pure.

Definition 3.32. Let M be a T-pointed R-module and let $\mathfrak{s}_M : M \to \mathfrak{sat}(M)$ be the inclusion into its saturation. We will call the pushforward functor $(\mathfrak{s}_M)_*$ the *saturation* functor and we will denote it by $\mathfrak{sat}$.

Remark 3.33. The counit map $\varepsilon_P : P \to \mathfrak{sat}(\mathfrak{s}_M^* P)$ is an isomorphism. Indeed, one can see from the definition of pullback that $\mathfrak{s}_M^* P = P$ is saturated, hence it coincides with its own saturation.

3.4 Maximal (J,T)-extensions

Maximal (J,T)-extensions are the analogue of algebraic closures in field theory. The main result of this section is the proof of the existence of a maximal (J,T)-extension for any T-pointed R-module, and we achieve this by first constructing such an extension for its torsion and its saturation.

Definition 3.34. A (J,T)-extension Γ of the T-pointed R-module M is called *maximal* if for every (J,T)-extension N of M there is a map of (J,T)-extensions $\varphi : N \hookrightarrow \Gamma$.

The definition of T-pointed R-module already provides a maximal (J,T)-extension for any J-torsion module.

Lemma 3.35. *Let (M,s) be a T-pointed R-module. If M is J-torsion, then (T,s,id_T) is a maximal (J,T)-extension of (M,s).*

Proof. If (N,i,t) is a (J,T)-extension of M, then in particular we have

$$N = (i(M) :_N J) = \big((0 :_{i(M)} J) :_N J\big) \subseteq ((0 :_N J) :_N J) = (0 :_N J) = N[J]$$

so N is J-torsion. Then $t : N \hookrightarrow T$ satisfies $t \circ i = s$ and $\mathrm{id}_T \circ t = t$, so it is a map of (J,T)-extensions. □

The existence of a maximal (J,T)-extension of a saturated module comes from the existence of a J-hull, and it requires only a little more technical work.

Lemma 3.36. *Let (M,s) be a saturated T-pointed R-module and let $\iota : M \hookrightarrow \Gamma$ be a J-hull of M. Then*

1. *$\iota|_{M[J]} : M[J] \hookrightarrow \Gamma[J]$ is an isomorphism.*

2. *(Γ, ι, τ) is a maximal (J,T)-extension of (M,s), where $\tau := s \circ \iota|^{-1}_{M[J]}$.*

Proof. For (1) notice that $\iota|_{M[J]} : M[J] \hookrightarrow \Gamma[J]$ is an essential extension by Lemma 2.15, so it is an isomorphism by Proposition 2.23.

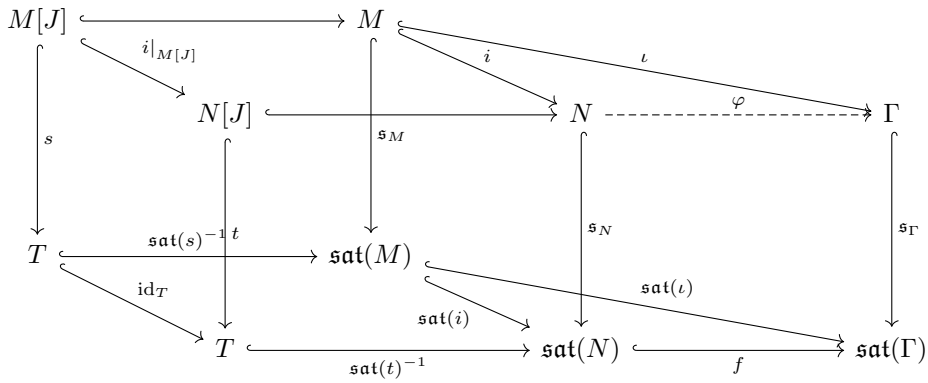
For (2) we have that Γ is a (J,T)-extension of M, because it is a J-extension and $\tau \circ \iota|_{M[J]} = s$. Let (N,i,t) be any (J,T)-extension of M. Since $i : M \hookrightarrow N$ is a J-extension, there is a homomorphism $\varphi : N \to \Gamma$ such that $\varphi \circ i = \iota$. Moreover, since $t \circ i|_{M[J]} = s$ and $\tau \circ (\varphi \circ i)|_{M[J]} = \tau \circ \iota|_{[M[J]} = s$, we have $\tau \circ \varphi|_{N[J]} = t$, so φ is a map of (J,T)-extensions. It follows that Γ is a maximal (J,T)-extension of M. □

Finally we can construct a (J,T)-extension of any T-pointed R-module.

Proposition 3.37. *Let (Γ, ι, τ) be a (J,T)-extension of the T-pointed R-module (M,s) such that Γ is saturated. Then Γ is a maximal (J,T)-extension of M if and only if $\mathfrak{sat}(\Gamma)$ is a maximal (J,T)-extension of $\mathfrak{sat}(M)$.*

Proof. Assume first that Γ is a maximal (J,T)-extension of M and let (N,i,t) be a (J,T)-extension of $\mathfrak{sat}(M)$. Then there is a map $\varphi : \mathfrak{s}^*_M N \to \Gamma$ of (J,T)-extensions of M, so there is a map $\mathfrak{sat}(\varphi) : \mathfrak{sat}(\mathfrak{s}^*_M N) \to \mathfrak{sat}(\Gamma)$ of (J,T)-extensions of $\mathfrak{sat}(M)$. By Remark 3.33 we have $N \cong \mathfrak{sat}(\mathfrak{s}^*_M N)$, so there is also a map $N \to \mathfrak{sat}(\Gamma)$. This proves that $\mathfrak{sat}(\Gamma, \iota, \tau)$ is a maximal (J,T)-extension of $\mathfrak{sat}(M)$.

Assume now that $\mathfrak{sat}(\Gamma)$ is a maximal (J,T)-extension of $\mathfrak{sat}(M)$. Let (N,i,t) be a (J,T)-extension of M. Then there is a map of (J,T)-extensions $f : \mathfrak{sat}(N) \to \mathfrak{sat}(\Gamma)$ completing the following diagram:



Notice that since Γ is saturated the map $\mathfrak{s}_\Gamma : \Gamma \hookrightarrow \mathfrak{sat}(\Gamma)$ is an isomorphism. So we can define $\varphi := \mathfrak{s}_\Gamma^{-1} \circ f \circ \mathfrak{s}_N : N \to \Gamma$ and we have

$$\mathfrak{s}_\Gamma \circ \varphi \circ i = f \circ \mathfrak{s}_N \circ i = f \circ \mathfrak{sat}(i) \circ \mathfrak{s}_M = \mathfrak{sat}(\iota) \circ \mathfrak{s}_s = \mathfrak{s}_\Gamma \circ \iota$$

hence $\varphi \circ i = \iota$. Moreover, since $\mathfrak{sat}(\tau) \circ \mathfrak{s}_\Gamma = \tau$, we have

$$\begin{aligned} \tau \circ \varphi|_{N[J]} &= \tau \circ \mathfrak{s}_\Gamma^{-1} \circ f \circ \mathfrak{s}_N|_{N[J]} = \\ &= \tau \circ \mathfrak{s}_\Gamma^{-1} \circ f \circ \mathfrak{sat}(t)^{-1} \circ t = \\ &= \tau \circ \mathfrak{s}_\Gamma^{-1} \circ \mathfrak{sat}(\tau)^{-1} \circ t = \\ &= t \end{aligned}$$

so φ is a map of (J,T)-extensions. Hence Γ is a maximal (J,T)-extension of M. □

Theorem 3.38. *Every T-pointed R-module M admits a maximal (J,T)-extension. Moreover, for any maximal (J,T)-extension Γ of M the following hold:*

1. *If Γ' is another maximal (J,T)-extension of M, then $\Gamma \cong \Gamma'$ as (J,T)-extensions;*
2. *The module Γ is saturated;*
3. *The module Γ is J-injective;*
4. *If (N,i,t) is a (J,T)-extension of M and $\varphi : N \to \Gamma$ is a map of (J,T)-extensions, then (Γ,φ,τ) is a maximal (J,T)-extension of (N,t).*

Proof. Let $j : \mathfrak{sat}(M) \hookrightarrow \Gamma$ be a J-hull of the saturation of M and let $\tau := \mathfrak{sat}(s) \circ j|^{-1}_{\mathfrak{sat}(M)[J]}$. By Lemma 3.36 we have that (Γ, j, τ) is a maximal (J,T)-extension of $\mathfrak{sat}(M)$. By Remark 3.33 we have that $(\Gamma, \iota, \tau) = \mathfrak{t}^*_M(\Gamma, j, \tau)$ is a (J,T)-extension of M such that $\mathfrak{sat}(\Gamma, \iota, \tau) \cong (\Gamma, j, \tau)$, so by Proposition 3.37 we conclude that it is a maximal (J,T)-extension of M.

Let now (Γ', ι', τ') be another maximal (J,T)-extension of (M,s). Then there is a map of (J,T)-extensions $f : \Gamma \hookrightarrow \Gamma'$ which is an essential J-extension by Lemma 2.15, as it is an isomorphism on the J-torsion. Since Γ is J-injective we have that f is an isomorphism by Proposition 2.23. This shows that any maximal (J,T)-extension of M is isomorphic to Γ, which proves (1), (2) and (3) at once.

For (4) it is enough to notice that if $j : \mathfrak{sat}(M) \hookrightarrow \Gamma$ is a J-hull, then so is $\mathfrak{sat}(\varphi)$, thus by the same argument as above Γ is a maximal (J,T)-extension of N. □

4 Automorphisms of (J,T)-extensions

Fix for this section a ring R, a complete ideal filter J of R and a J-torsion and J-injective left R-module T. Fix moreover a T-pointed R-module (M,s) and a maximal (J,T)-extension (Γ, ι, τ) of (M,s).

4.1 Normal extensions

We define normal extensions in analogy with field theory.

Definition 4.1. A (J,T)-extension $i : M \hookrightarrow N$ is called *normal* if every injective J-map $f : N \hookrightarrow \Gamma$ such that $f \circ i = \iota$ has the same image.

Notice that we are considering all injective J-maps that respect $\iota : M \hookrightarrow \Gamma$, even if they are not maps of (J,T)-extensions, that is even if they do not respect the embeddings of the torsion submodules into T.

Remark 4.2. Although we will not make use of it, it interesting to notice that the group $\mathrm{Aut}_M(N)$ acts on $\mathrm{Emb}_M(N,\Gamma)$ by composition on the right. It is then easy to see that N is normal if and only if this action is transitive.

This is reminiscent of Galois theory *à la Grothendieck*. One might wonder if, assuming the necessary finiteness conditions on automorphism groups hold, the category of (J,T)-extensions is indeed a Galois category with fundamental functor $\mathrm{Emb}_M(-,\Gamma)$. Unfortunately, the fact that in general pushouts of (J,T)-extensions do not exist (see Remark 3.7) implies that this is not the case.

We may refine this question as follows: does the category of (J,T)-extensions embed as the subcategory of connected objects of some Galois category?

Proposition 4.3. *Every saturated (J,T)-extension of M is normal.*

Proof. Assume that M is saturated, let $i : M \hookrightarrow N$ be a (J,T)-extension and let $f, g : N \hookrightarrow \Gamma$ be injective J-maps with $f \circ i = g \circ i = \iota$. If $f(N) \neq g(N)$, we may assume without loss of generality that there is $n \in N$ with $f(n) \notin g(N)$. Then $t := f(n) - g(n) \in \Gamma[J]$ by Lemma 2.16. Since N is saturated and g is injective we have $t \in g(N)$, thus $f(n) = g(n) + t \in g(N)$, a contradiction. We deduce that $f(N) = g(N)$, so N is normal. □

Corollary 4.4. *Every maximal (J,T)-extension is normal.*

4.2 A fundamental exact sequence

Proposition 4.5. *Let (N, i, t) be a normal (J,T)-extension of (M, s) and let $\mathrm{Aut}_{M+N[J]}(N)$ denote the subgroup of $\mathrm{Aut}_M(N)$ consisting of those automorphisms that restrict to the identity on the submodule of N generated by $i(M)$ and $N[J]$. Then the restriction map along $\mathfrak{s}_N : N \to \mathfrak{sat}(N)$*

$$\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \to \mathrm{Aut}_{M+N[J]}(N)$$

is a well-defined group isomorphism.

Proof. Let us identify for simplicity N with its image $\mathfrak{s}_N(N)$ in $\mathfrak{sat}(N)$, and let $\sigma \in \mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$. To see that the image of $\sigma|_N$ is contained in N, let $f : \mathfrak{sat}(N) \hookrightarrow \Gamma$ be a map of (J,T)-extensions of $\mathfrak{sat}(M)$, which is necessarily also a map of (J,T)-extensions of M. Since $\mathfrak{sat}(s)$ is an isomorphism, also $f \circ \sigma$ is a map of (J,T)-extensions of $\mathfrak{sat}(M)$, and since N is normal we have that the image of N in Γ under f and under $f \circ \sigma$ are the same, which shows that $\sigma(N) = N$. Since this holds for both σ and its inverse, we have that $\sigma|_N \in \mathrm{Aut}_M(N)$, and clearly σ is the indentity on $N[J]$.

To show that the restriction to N is an isomorphism, we construct an inverse. Let now $\sigma \in \mathrm{Aut}_{M+N[J]}(N)$, and recall that we can see it as a map of (J,T)-extensions of (M, s)

$$\sigma : (N, t) \to (N, t \circ \sigma|_{N[J]}) .$$

Composing it with $\mathfrak{s}_N$ we get a map

$$\mathfrak{s}_N \circ \sigma : (N, t) \to (\mathfrak{sat}(N), (\mathfrak{s}_N)_*(t \circ \sigma|_{N[J]})) .$$

Moreover, the map $\mathfrak{sat}(i)$ is also a map of (J,T)-extensions

$$\mathfrak{sat}(i) : (\mathfrak{sat}(M), (\mathfrak{s}_M)_* s) \to (\mathfrak{sat}(N), (\mathfrak{s}_N)_*(t \circ \sigma|_{N[J]}))$$

so by the universal property of the pushout there is a map of (J,T)-extensions

$$\sigma' : (\mathfrak{sat}(N), (\mathfrak{s}_N)_* t), (\mathfrak{sat}(N), (\mathfrak{s}_N)_*(t \circ \sigma|_{N[J]})) .$$

It is straightforward to check that $\sigma \mapsto \sigma'$ provides an inverse for the restriction map $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \to \mathrm{Aut}_M(N)$, which is then an isomorphism. □

Proposition 4.6. *Let (N,i,t) be a (J,T)-extension of (M,s). Then the map*

$$\begin{aligned}\varphi : \mathrm{Aut}_{M+N[J]}(N) &\to \mathrm{Hom}\left(\frac{N}{i(M)+N[J]}, N[J]\right)\\ \sigma &\mapsto (\varphi_\sigma : [n] \mapsto \sigma(n) - n)\end{aligned}$$

is an isomorphism of groups. In particular, $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$ is abelian.

Proof. We will denote by $[n]$ the class of an element $n \in N$ in $N/(i(M)+N[J])$. Notice that for any $\sigma \in \mathrm{Aut}_{M+N[J]}(N)$ we have $\sigma(n)-n \in N[J]$ by Lemma 2.16, and φ_σ is a homomorphism of R-modules. To see that $\sigma \mapsto \varphi_\sigma$ is a group homomorphism, let $\sigma' \in \mathrm{Aut}_{M+N[J]}(N)$. Then, since σ is the identity on $N[J]$ and $\sigma'(n) - n \in N[J]$, we have

$$\begin{aligned}\sigma(\sigma'(n)) - n &= \sigma(\sigma'(n)) - n + \sigma'(n) - n - \sigma(\sigma'(n) - n)\\ &= \sigma(n) - n + \sigma'(n) - n\end{aligned}$$

which shows that φ is a group homomorphism. It is also clearly injective, because if $\varphi_\sigma(n) = n$ then σ must be the identity.

To prove surjectivity it is enough to show that for any R-module homomorphism $h : N/(i(M)+N[J]) \to N[J]$ the map

$$\begin{aligned}\sigma_h : N &\to N\\ n &\mapsto n + h([n])\end{aligned}$$

which is clearly the identity on $i(M)+N[J]$, is an automorphism of N. It is injective, because if $n = -h([n])$ then in particular n is torsion and thus $[n] = 0$. It is also surjective, because for any $n \in N$ we have

$$\begin{aligned}\sigma_h(n - h([n])) &= n - h([n]) + h([n - h([n])])\\ &= n - h([n] - [n + h([n])])\\ &= n\end{aligned}$$

□

Corollary 4.7. *Let (N,i,t) be a normal (J,T)-extension of M. Denoting for simplicity by $\mathfrak{sat}(M)$ the image of $\mathfrak{sat}(M)$ inside $\mathfrak{sat}(N)$ we have*

$$\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \cong \mathrm{Hom}\left(\frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, \mathfrak{tor}(N)\right).$$

Proof. The claim follows from the two propositions above and the fact that

$$\frac{N}{i(M)+N[J]} \cong \frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}.$$

To see that the two quotients are isomorphic, consider the following map:

$$\begin{aligned} N &\to \mathfrak{sat}(N)/\mathfrak{sat}(M) \\ n &\mapsto \mathfrak{s}_N(n) + \mathfrak{sat}(M) \end{aligned}$$

Its kernel is $i(M) + N[J]$ and it is surjective because $\mathfrak{sat}(N)$ is generated by the images of N and T. □

Remark 4.8. Let N be a (J,T)-extension of M and let $\sigma \in \mathrm{Aut}_M(N)$. The restriction of σ to $N[J]$ is an element of $\mathrm{Aut}_{M[J]}(N[J])$. Indeed, the image of a J-torsion element under a map of (J,T)-extensions is again a J-torsion element; since this is true for both σ and σ^{-1} we can conclude that $\sigma|_{N[J]} : N[J] \to N[J]$ is an automorphism.

Lemma 4.9. *If (N,i,t) is a normal (J,T)-extension of (M,s), the restriction map*

$$\mathrm{Aut}_M(N) \to \mathrm{Aut}_{M[J]}(N[J])$$

is surjective.

Proof. Let $\sigma \in \mathrm{Aut}_{M[J]}(N[J])$. Notice that $(N,i,t\circ\sigma)$ is also a (J,T)-extension of M, and let $f : (N,i,t) \hookrightarrow (\Gamma,\iota,\tau)$ and $g : (N,i,t\circ\sigma) \hookrightarrow (\Gamma,\iota,\tau)$ be maps of (J,T)-extensions. Since N is normal we have $f(N) = g(N)$, thus $f^{-1}\circ g$ is an automorphism of N that restricts to σ. □

The exact sequence appearing in the following theorem has been studied, in some particular cases, in [JP21], [Pal14] and [Chapter 3].

Theorem 4.10. *Let M be a T-pointed R-module and let N be a normal (J,T)-extension of M. Then there is an exact sequence of groups*

$$1 \to \mathrm{Hom}\left(\frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, \mathfrak{tor}(N)\right) \to \mathrm{Aut}_M(N) \to \mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N)) \to 1$$

Moreover $\mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ *acts on* $\mathrm{Hom}(\mathfrak{sat}(N)/\mathfrak{sat}(M), \mathfrak{tor}(N))$ *by composition.*

Proof. By Lemma 4.9 the map $\mathrm{Aut}_M(N) \to \mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ is surjective and its kernel is $\mathrm{Aut}_{i(M)+N[J]}(N)$ by definition. By Proposition 4.5 this group is

isomorphic to $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$ via the restriction under $\mathfrak{s}_N : N \to \mathfrak{sat}(N)$. Combining this with Corollary 4.7 we get the desired exact sequence.

The fact that $\mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ acts on $\mathrm{Aut}_{i(M)+N[J]}$ by conjugation is a standard result on short exact sequences with abelian kernel, and one can trace this action under the isomorphisms described above to check that on $\mathrm{Hom}(\mathfrak{sat}(N)/\mathfrak{sat}(M), \mathfrak{tor}(N))$ this action is indeed the composition of maps, similarly to [Chapter 3, Proposition 3.12]. □

5 Kummer theory for algebraic groups

5.1 General theory

Let K be a field and fix a separable closure K_s of K. Let G be a commutative algebraic group over K, let $R \subseteq \mathrm{End}_K(G)$ be a subring of the ring of K-endomorphisms of G and let $M \subseteq G(K)$ be an R-submodule. Let J be a complete ideal filter of R, let $T := G(\overline{K})[J]$ and let $\Gamma := \left(M :_{G(\overline{K})} J\right)$.

We are interested in studying the field extension $K(\Gamma)$ of K, that is the fixed field of the subgroup of $\mathrm{Gal}(K_s \mid K)$ that acts trivially on Γ, and we want to do so using the theory of (J,T)-extensions introduced in the previous section. A necesary and sufficient condition in order to proceed this way is that $T = G(\overline{K})[J]$ be J-injective: indeed in this case Γ is a saturated, and thus normal, (J,T)-extension of M.

Remark 5.1. The condition that T is J-injective for some, and in fact for all, ideal filters J, holds for example if G is a simple abelian variety with R a maximal order in the division algebra $\mathrm{End}_{\overline{K}}(G) \otimes \mathbb{Q}$. Indeed in this case every non-zero element r of R is surjective on $G(\overline{K})$, which implies that T is divisible: if an element $u \in G(\overline{K})$ is such that $ru = t \in T$ and $I \in J$ is such that $It = 0$, then since I is a right ideal we have $Iu = 0$, so $u \in T$; hence $r : T \to T$ is surjective and T is divisible.

It follows that T is injective: this is a well-known statement if R is a Dedekind domain, but the proof can be adapted to the non-commutative case as follows. Let I be a left ideal of R and let $f : I \to T$ be a map that we wish to extend to a map $\tilde{f} : R \to T$. By [Rei75, Theorem 22.7] there is a right *fractional* ideal J of R such that $IJ = R$ and $1 \in JI \subseteq R$. In particular there are non-zero elements $b_1, \ldots, b_n \in J$ and $a_1, \ldots, a_n \in I$ such that $\sum_{i=1}^n b_i a_i = 1$, and since T is divisible there are $x_1, \ldots, x_n \in T$ such that $a_i x_i = f(a_i)$. It follows that for every $y \in I$ we have

$$f(y) = f\left(y \sum_{i=1}^n b_i a_i\right) = \sum_{i=1}^n (y b_i) f(a_i) = y \sum_{i=1}^n (b_i a_i) x_i$$

and we can let $\tilde{f}(r) = r\sum_{i=1}^{n}(b_i a_i)x_i$ for every $r \in R$.

Let us then assume that $T = G(\overline{K})[J]$ is J-injective, so that Γ is a saturated, therefore normal, (J,T)-extension of M. Then the standard exact sequence of groups coming from the tower of Galois extensions $K \subseteq K(T) \subseteq K(\Gamma)$ maps into the exact sequence 4.10 via the Galois action on the points of G, and we obtain the following commutative diagram of groups with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(K(\Gamma) \mid K(T)) & \longrightarrow & \mathrm{Gal}(K(\Gamma) \mid K) & \longrightarrow & \mathrm{Gal}(K(T) \mid K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \tau} & & \\
1 & \longrightarrow & \mathrm{Hom}\left(\frac{\Gamma}{\mathfrak{sat}(M)}, T\right) & \longrightarrow & \mathrm{Aut}_M(\Gamma) & \longrightarrow & \mathrm{Aut}_{\mathfrak{tor}(M)}(T) & \longrightarrow & 1
\end{array}$$

Notice that the action of $\mathrm{Aut}_{M[J]}(T)$ on $\mathrm{Hom}(\Gamma/(M+T), T)$ restricts to an action of $\mathrm{Im}(\tau)$ on $\mathrm{Im}(\kappa)$.

Definition 5.2. In the situation described above we will call the maps κ, τ and ρ the *Kummer representation*, the *torsion representation* and the *torsion-Kummer representation*, respectively.

As in Section 2.4, if N and P are R-modules and S is a subset of $\mathrm{Hom}_R(N,P)$ we let $\ker(S) = \bigcap_{f\in S}\ker(f)$.

Theorem 5.3. *There is an exact sequence of abelian groups*

$$0 \to \frac{\left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} J\right)}{\mathfrak{sat}(M)} \to \ker(\mathrm{Im}(\kappa)) \to H^1(\mathrm{Im}(\tau), T)$$

Proof. By Lemma 2.16 for any $b \in G(K(T))$ we may define a map

$$\begin{aligned} \varphi_b : \mathrm{Im}(\kappa) &\to T \\ \sigma &\mapsto \sigma(b) - b \end{aligned}$$

which is a cocycle. It follows that the map

$$\begin{aligned} \varphi : G(K(T)) &\to H^1(\mathrm{Im}(\tau), T) \\ b &\mapsto \varphi_b \end{aligned}$$

is a group homomorphism. Moreover its kernel is

$$\begin{aligned} \ker(\varphi) &= \{b \in G(K(T)) \mid \varphi_b \text{ is a coboundary}\} \\ &= \{b \in G(K(T)) \mid \exists\, t \in T \text{ such that } \sigma(b) - b = \sigma(t) - t \,\forall\, \sigma \in \mathrm{Im}(\kappa)\} \\ &= \{b \in G(K(T)) \mid \exists\, t \in T \text{ such that } \sigma(b - t) = b - t \,\forall\, \sigma \in \mathrm{Im}(\kappa)\} \\ &= G(K) + T \end{aligned}$$

so that we have an exact sequence

$$0 \to G(K) + T \to G(K(T)) \to H^1(\mathrm{Im}(\tau), T)$$

and considering the intersection of the first two terms with Γ we get

$$0 \to \Gamma \cap (G(K) + T) \to \Gamma \cap G(K(T)) \to H^1(\mathrm{Im}(\tau), T)\,.$$

Since $M + T \subseteq \Gamma \cap (G(K) + T)$ we also have

$$0 \to \frac{\Gamma \cap (G(K) + T)}{M + T} \to \frac{\Gamma \cap G(K(T))}{M + T} \to H^1(\mathrm{Im}(\tau), T)\,.$$

Rewriting $M + T = \mathfrak{sat}(M)$ and $G(K) + T = \mathfrak{sat}(G(K))$, noticing that

$$\Gamma \cap \mathfrak{sat}(G(K)) = \left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} J\right)$$

and that

$$\begin{aligned}\ker(\mathrm{Im}(\kappa)) &= \left\{ x \in \frac{\Gamma}{M+T} \mid f(x) = 0 \,\forall\, f \in \mathrm{Im}(\kappa) \right\} \\ &= \frac{\{\tilde{x} \in \Gamma \mid \sigma(\tilde{x}) = \tilde{x} \,\forall\, \sigma \in \mathrm{Im}(\kappa)\}}{M+T} \\ &= \frac{\Gamma \cap G(K(T))}{M+T}\end{aligned}$$

we get the desired exact sequence. □

The following theorem generalizes [Chapter 3, Theorem 5.9].

Theorem 5.4. *Assume that the* $\mathrm{End}(T)$*-submodule of* $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ *generated by* $\mathrm{Im}(\kappa)$ *is finitely generated. Suppose that the following three conditions hold*

1. *There is a positive integer* d *such that*

$$d \cdot \left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} J\right) \subseteq \mathfrak{sat}(M)\,.$$

2. *There is a positive integer* n *such that*

$$n \cdot H^1(\mathrm{Im}(\tau), T) = 0\,.$$

3. *There is a positive integer* m *such that the subring of* $\mathrm{End}(T)$ *generated by* $\mathrm{Im}(\tau)$ *contains*

$$m \cdot \mathrm{End}(T)\,.$$

Then $\mathrm{Im}(\kappa)$ *contains* $dnm \cdot \mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$.

Proof. Let V be the $\mathrm{End}(T)$-submodule of $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ generated by $\mathrm{Im}(\kappa)$ and let $X = \Gamma/\mathfrak{sat}(M)$. From (1) and (2) it follows that $\ker(V) = \ker(\mathrm{Im}\,\kappa) \subseteq X[dn]$. Since V is finitely generated as an $\mathrm{End}(T)$-module, by Proposition 2.32 we have

$$V = \mathrm{Hom}\left(\frac{X}{\ker(V)}, T\right) \supseteq \mathrm{Hom}\left(\frac{X}{X[dn]}, T\right) \supseteq dn \cdot \mathrm{Hom}(X, T)\,.$$

Since $\mathrm{Im}(\kappa)$ is an $\mathrm{Im}(\tau)$-module, we have

$$\mathrm{Im}(\kappa) = \mathrm{Im}(\tau) \cdot \mathrm{Im}(\kappa) \supseteq m \cdot \mathrm{End}(T) \cdot \mathrm{Im}(\kappa) = m \cdot V \supseteq dnm \cdot \mathrm{Hom}(X, T)$$

and we conclude. □

5.2 Elliptic curves over number fields

We keep the notation of the previous section and we further assume that K is a number field, that $G = E$ is an elliptic curve and that $R = \mathrm{End}_K(E)$. In particular we have that $K_s = \overline{K}$ and that R is either $\mathbb{Z}$ or an order in an imaginary quadratic number field. Up to replacing K by an extension of degree 2 we may assume that $\mathrm{End}_K(E) = \mathrm{End}_{\overline{K}}(E)$.

Notice that $T = E(\overline{K})[J]$ is contained in $E(\overline{K})_{\mathrm{tors}}$: indeed, if $x \in T$ then there is $I \in J$ such that $Ix = 0$. Since R is an order in a number field there is some non-zero integer $n \in I$, so $nx = 0$ and x is torsion.

Proposition 5.5. *The* R*-module* $E(\overline{K})[J]$ *is* J*-injective.*

Proof. By [LJ96, Proposition 5.1] the R-module $E(\overline{K})_{\mathrm{tors}}$ is injective, thus in particular J-injective. Since $E(\overline{K})[J] = \left(0 :_{E(\overline{K})_{\mathrm{tors}}} J\right)$ it follows from Lemma 2.28 that $E(\overline{K})[J]$ is J-injective. □

Remark 5.6. Although not necessary for our applications, it is interesting to notice that in this setting Γ is a maximal (J, T)-extension of M. Indeed $E(\overline{K})/E(\overline{K})_{\mathrm{tors}}$ is a torsion-free module over the commutative integral domain R, so it is injective. Then the short exact sequence of R-modules

$$0 \to E(\overline{K})_{\mathrm{tors}} \to E(\overline{K}) \to E(\overline{K})/E(\overline{K})_{\mathrm{tors}} \to 0$$

splits, so that $E(\overline{K}) \cong E(\overline{K})/T \oplus T$ as R-modules and since R is Noetherian it follows that $E(\overline{K})$ is injective. As in the above proposition we may conclude that Γ is J-injective, thus it is a maximal (J, T)-extension of M.

We now specialize to the case $J = \infty$.

Remark 5.7. Notice that in case $J = \infty$ we have $T = G(\overline{K})_{\mathrm{tors}}$ and

$$\Gamma = \left\{ x \in E(\overline{K}) \mid nx \in M \text{ for some } n \in \mathbb{Z}_{>0} \right\} .$$

If $R = \mathbb{Z}$ then $\mathrm{End}_R(T)$ is isomorphic, after fixing an isomorphism $T \cong (\mathbb{Q}/\mathbb{Z})^2$, to $\mathrm{Mat}_{2\times 2}(\widehat{\mathbb{Z}})$. If R is instead an order in an imaginary quadratic field then $\mathrm{End}_R(T) \cong R \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. Indeed, fix for every prime p a $\mathbb{Z}_p$-basis for $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and consider the $\widehat{\mathbb{Z}}$-subalgebra $C = \prod_p C_p$ of $\mathrm{Mat}_{2\times 2}(\widehat{\mathbb{Z}}) = \prod_p \mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$, where C_p is the image of the embedding of R_p into $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$ given by its multiplication action on the $\mathbb{Z}_p$-module $\mathbb{Z}_p^2 \cong R_p$. Then $R \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \cong C$ is a $\widehat{\mathbb{Z}}$-algebra free of rank 2 as a $\widehat{\mathbb{Z}}$-module, since every C_p is a $\mathbb{Z}_p$-algebra of rank 2. Then for a suitable choice of an isomorphism $T \cong (\mathbb{Q}/\mathbb{Z})^2$ we have

$$\begin{aligned} \mathrm{End}_R(T) &= \{\varphi \in \mathrm{End}_{\mathbb{Z}}(T) \mid f(r(t)) = r(f(t)) \, \forall r \in R,\, t \in T\} \\ &= \left\{ \varphi \in \mathrm{Mat}_{2\times 2}(\widehat{\mathbb{Z}}) \mid fc = cf \, \forall c \in C \right\} \\ &= C \end{aligned}$$

where the last equality follows by applying the Centralizer Theorem to the central simple $\mathbb{Q}_p$-subalgebra $R \otimes_{\mathbb{Z}} \mathbb{Q}_p$ of $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ and then restricting the coefficients to $\mathbb{Z}_p$.

In both cases, the map τ coincides with the usual Galois representation associated with the torsion of E.

Proposition 5.8. *Assume that the abelian group structure of $E(K)$ is known and that M is given in terms of set of generators for $E(K)$. Then there exists an effectively computable positive integer d such that*

$$d \cdot \left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} \infty \right) \subseteq \mathfrak{sat}(M) .$$

Proof. First of all notice that $\mathfrak{sat}(M) = M + T$ and $\mathfrak{sat}(G(K)) = G(K) + T$ seen as subgroups of $E(\overline{K})$. We conclude thanks to the considerations of [Chapter 3, Section 6.1]. □

Proposition 5.9. *There exists an effectively computable positive integer n such that*

$$n \cdot H^1(\mathrm{Im}(\tau), T) = 0 .$$

Proof. This follows from [Chapter 3, Proposition 6.3] and [Chapter 3, Corollary 6.8] in the non-CM case and from [Chapter 3, Proposition 6.12] in the CM case. □

Proposition 5.10. *There exists an effectively computable positive integer m such that the subring of $\mathrm{End}_R(T)$ generated by $\mathrm{Im}(\tau)$ contains $m \cdot \mathrm{End}_R(T)$.*

Proof. This follows again from [Chapter 3, Corollary 6.8] in the case $R = \mathbb{Z}$ and from [Lom17, Theorem 1.5] in the CM case. □

Theorem 5.11. *Assume that the abelian group structures of $E(K)$ and M are effectively computable. Then there exists an effectively computable positive constant c such that the index of $\mathrm{Im}(\kappa)$ in $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ divides c.*

Proof. This is a direct consequence of Theorem 5.4 and the three propositions above. □

Remark 5.12. Since Theorem 5.4 is stated in a fairly general form, one might wonder if it can be applied to obtain a version of Theorem 5.11 for higer-dimensional abelian varieties.

Provided that one is in, or can reduce to, a case in which T is a J-injective R-module (for example if the abelian variety is simple and its endomorphism ring is a maximal order in a division algebra, see Remark 5.1), the key steps are finding effective bounds for the integers n and m of Theorem 5.4. Effective bounds for m are known, see for example [RG20, Théorème 1.5(2)].

It is also known (see [Chapter 1]) that a bound for n can be obtained by finding explicit homotheties in $\mathrm{Im}(\tau)$. This seems a harder problem to tackle, but one can hope to reduce to finding homotheties in the images of the ℓ-adic representations, as done in [Chapter 1, Section 7]. Explicit results on the existence of homotheties in the image of ℓ-adic representations attached to abelian varieties are obtained for example in [GM20].

Bibliography

[Ach05] Jeffrey D. Achter. Detecting complex multiplication. In *Computational aspects of algebraic curves*, pages 38–50. World Scientific, 2005.

[Ara08] Keisuke Arai. On uniform lower bound of the Galois images associated to elliptic curves. *Journal de théorie des nombres de Bordeaux*, 20(1):23–43, 2008.

[Bae40] Reinhold Baer. Abelian groups that are direct summands of every containing abelian group. *Bulletin of the American Mathematical Society*, 46(10):800–806, 1940.

[BC14] Barinder S. Banwait and John E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra & Number Theory*, 8(5):1201–1229, 2014.

[BC20a] Abbey Bourdon and Pete L. Clark. Torsion points and Galois representations on CM elliptic curves. *Pacific Journal of Mathematics*, 305(1):43–88, 2020.

[BC20b] Abbey Bourdon and Pete L. Clark. Torsion points and isogenies on CM elliptic curves. *Journal of the London Mathematical Society. Second Series*, 102(2):580–622, 2020.

[BDM+19] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Annals of Mathematics. Second Series*, 189(3):885–944, 2019.

[BDM+21] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. *arXiv preprint arXiv:2101.01862*, 2021.

[Ber88] Daniel Bertrand. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge University Press, Cambridge, 1988.

[BJR91] Nigel Boston, Hendrik W. Lenstra Jr., and Kenneth A. Ribet. Quotients of group rings arising from two-dimensional representations. *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, 312(4):323–328, 1991.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Annals of Mathematics*, 173(1):569–584, 2011.

[BP21] Peter Bruin and Antonella Perucca. Reductions of points on algebraic groups, II. *Glasgow Mathematical Journal*, 63(2):484–502, 2021.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. 63(3):957–984, 2013.

[BR03] Matthew H. Baker and Kenneth A. Ribet. Galois theory and torsion points on curves. *Journal de Théorie des Nombres de Bordeaux*, 15(1):11–32, 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Mathematics of Computations*, 88:1303–1339, 2019.

[Coa70] John Coates. An application of the division theory of elliptic functions to Diophantine approximation. *Inventiones Mathematicae*, 11:167–182, 1970.

[Coh07] Henri Cohen. *Number theory: Volume I: Tools and Diophantine equations*. Springer, 2007.

[CP20] Francesco Campagna and Riccardo Pengo. Entanglement in the family of division fields of elliptic curves with complex multiplication. *arXiv preprint arXiv:2006.00883*, 2020.

[CR21] Michael Cerchia and Jeremy Rouse. Uniform bounds on the image of the arboreal Galois representations attached to non-CM elliptic curves. *Proceedings of the American Mathematical Society*, 149(2):583–589, 2021.

[Cre97] John E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[CS19] Francesco Campagna and Peter Stevenhagen. Cyclic reduction of elliptic curves. *arXiv preprint arXiv:2001.00028*, 2019.

[Dav11] Agnès David. Borne uniforme pour les homothéties dans l'image de Galois associée aux courbes elliptiques. *Journal of Number Theory*, 131(11):2175 – 2191, 2011.

[Deu53] Max Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachrichten von der Akademie der Wissenschaften Göttingen Mathematisch-Physikalische Klasse. IIa, Mathematisch-Physikalisch-Chemische Abteilung*, 1953:85–94, 1953.

[Deu58] Max Deuring. Die Klassenkorper der komplexen Multiplikation. In *Enzyklopädie der mathematischen Wissenschaften*, volume I2, Heft 10, Teil II. Teubner Verlag, Stuttgart, 1958.

[DLM21] Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow. Towards a classification of entanglements of Galois representations attached to elliptic curves. *arXiv preprint arXiv:2105:02060*, 2021.

[DP16] Christophe Debry and Antonella Perucca. Reductions of algebraic integers. *Journal of Number Theory*, 167:259–283, 2016.

[EGH+11] Pavel I. Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to representation theory.* American Mathematical Society, 2011.

[ES53] Beno Eckmann and A Schopf. Über injektive Moduln. *Archiv der Mathematik*, 4(2):75–78, 1953.

[Fle68] Isidore Fleischer. A new construction of the injective hull. *Canadian Mathematical Bulletin*, 11(1):19–21, 1968.

[GM20] Aurélien Galateau and César Martínez. Homothéties explicites des représentations ℓ-adiques. *arXiv preprint arXiv:2006.07401*, 2020.

[Gou97] Fernando Q. Gouvêa. *p-adic Numbers.* Springer, 1997.

[Gre12] Ralph Greenberg. The image of Galois representations attached to elliptic curves with an isogeny. *American Journal of Mathematics*, 134(5):1167–1196, 2012.

[Gro91] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, pages 235–256. Cambridge University Press, Cambridge, 1991.

[GRSS14] Ralph Greenberg, Karl Rubin, Alice Silverberg, and Michael Stoll. On elliptic curves with an isogeny of degree 7. *American Journal of Mathematics*, 136(1):77–109, 2014.

[Har20] David Harari. *Galois cohomology and class field theory*. Springer, 2020.

[Hin88] Marc Hindry. Autour d'une conjecture de Serge Lang. *Inventiones Mathematicae*, 94(3):575–603, 1988.

[Jac12] Nathan Jacobson. *Basic algebra I*. Courier Corporation, 2012.

[Jon10] Nathan Jones. Almost all elliptic curves are Serre curves. *Transactions of the American Mathematical Society*, 362(3):1547–1570, 2010.

[JP21] Abtien Javan Peykar. *Division points in arithmetic*. PhD thesis, Leiden University, 2021.

[JR10] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proceedings of the London Mathematical Society*, 100(3):763–794, 2010.

[Ken82] Monsur A. Kenku. On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class. *Journal of Number Theory*, 15(2):199–202, 1982.

[Lan02] Serge Lang. *Algebra*. Springer-Verlag, New York, 2002.

[LFL21] Samuel Le Fourn and Pedro Lemos. Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan. *Algebra & Number Theory*, 15(3):747–771, 2021.

[LJ96] Hendrik W. Lenstra Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022. [Online; accessed 25 January 2022].

[Lom15] Davide Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra & Number Theory*, 9(10):2347–2395, 2015.

[Lom17] Davide Lombardo. Galois representations attached to abelian varieties of CM type. *Bulletin de la Société Mathématique de France*, 145(3):469–501, 2017.

[Lom19] Davide Lombardo. Computing the geometric endomorphism ring of a genus-2 Jacobian. *Mathematics of Computation*, 88(316):889–929, 2019.

[LP17] Davide Lombardo and Antonella Perucca. The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. *New York Journal of Mathematics*, 23, 2017.

[LP21] Davide Lombardo and Antonella Perucca. Reductions of points on algebraic groups. *Journal of the Institute of Mathematics of Jussieu*, 20(5):1637–1669, 2021.

[LR18] Álvaro Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. *arXiv preprint arXiv:1809.02584*, 2018.

[LT21a] Davide Lombardo and Sebastiano Tronto. Effective Kummer Theory for Elliptic Curves. *International Mathematics Research Notices*, 08 2021.

[LT21b] Davide Lombardo and Sebastiano Tronto. Some uniform bounds for elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:2106.09950*, 2021. Submitted for publication.

[LV14] Eric Larson and Dmitry Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *Journal de l'Institut de Mathématiques de Jussieu*, 13(3):517–559, 2014. With an appendix by Brian Conrad.

[LW15] Tyler Lawson and Christian Wuthrich. Vanishing of some Galois cohomology groups for elliptic curves. In *Elliptic Curves, Modular Forms and Iwasawa Theory – Conference in honour of the 70th birthday of John Coates*, pages 373–399. Springer, 2015.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, (47):33–186, 1977. With an appendix by Barry Mazur and Michael Rapoport.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1-3):437–449, 1996.

[MG78] Barry Mazur and Dorian Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[Mor12] Pieter Moree. Artin's primitive root conjecture–a survey. *Integers*, 12(6):1305–1416, 2012.

[Mor19] Jackson S. Morrow. Composite images of Galois for elliptic curves over $\mathbb{Q}$ and entanglement fields. *Mathematics of Computation*, 88(319):2389–2421, 2019.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Springer Science & Business Media, 2013.

[Ogg73] Andrew P. Ogg. Rational points on certain elliptic modular curves. In *Proceedings of Symposia in Pure Mathematics*, volume 24, pages 221–231, 1973.

[Pal04] Willem J. Palenstijn. Galois action on division points. Master's thesis, Leiden University, 2004.

[Pal14] Willem J. Palenstijn. *Radicals in arithmetic*. PhD thesis, Leiden University, 2014.

[Par96] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *Journal für die reine und angewandte Mathematik*, 1999:116 – 85, 1996.

[Per08] Antonella Perucca. *On the order of the reductions of points on abelian varieties and tori*. PhD thesis, Tor Vergata University of Rome, 2008.

[Per11] Antonella Perucca. On the reduction of points on abelian varieties and tori. *International Mathematics Research Notices*, 2011(2):293–308, 2011.

[Per15] Antonella Perucca. The order of the reductions of an algebraic integer. *Journal of Number Theory*, 148:121–136, 2015.

[Pet06] Clayton Petsche. Small rational points on elliptic curves over number fields. *The New York Journal of Mathematics*, 12:257–268, 2006.

[Pin93] Richard Pink. Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime. *Compositio Mathematica*, 88(3):251–264, 1993.

[Pin04] Richard Pink. On the order of the reduction of a point on an abelian variety. *Mathematische Annalen*, 330(2):275–291, 2004.

[Pon66] Lev S. Pontryagin. *Topological groups*. Gordon and Breach, 1966.

[PS19] Antonella Perucca and Pietro Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *International Journal of Number Theory*, 15, 04 2019.

[PST20a] Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. The degree of Kummer extensions of number fields. *International Journal of Number Theory*, 17:1–20, 10 2020.

[PST20b] Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. Explicit Kummer theory for the rational numbers. *International Journal of Number Theory*, 16, 06 2020.

[Rei75] Irving Reiner. Maximal orders. *New York-London*, 1975.

[RG20] Gaël Rémond and Eric Gaudron. Nouveaux théorèmes d'isogénies. Preprint available at https://hal.archives-ouvertes.fr/hal-02445032, January 2020.

[Rib79] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Mathematical Journal*, 46(4):745–761, 1979.

[Ros95] Jonathan Rosenberg. *Algebraic K-theory and its applications*. Springer Science & Business Media, 1995.

[RSZB21] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:2106.11141*, 2021.

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Research in Number Theory*, 1(1):1–34, 2015.

[Sah68] Chih-Han Sah. Automorphisms of finite groups. *Journal of Algebra*, 10(1):47–68, 1968.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.

[Ser97] Jean-Pierre Serre. *Abelian l-Adic Representations and Elliptic Curves*. CRC Press, 1997.

[Ser13] Jean-Pierre Serre. *Local fields*. Springer Science & Business Media, 2013.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer Science & Business Media, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, 2009.

[The] The Sage Developers. *SageMath, the Sage Mathematics Software System*. `https://www.sagemath.org`.

[The19] The PARI Group, University of Bordeaux. *PARI/GP version 2.11.2*, 2019. available from `http://pari.math.u-bordeaux.fr/`.

[Tro19] Sebastiano Tronto. Kummer Degrees, 2019. GitHub repository `https://github.com/sebastianotronto/kummer-degrees`.

[Tro20] Sebastiano Tronto. Radical entanglement for elliptic curves. *arXiv preprint arXiv:2009.08298*, 2020. Submitted for publication.

[Tro21] Sebastiano Tronto. Division in modules and Kummer theory. *arXiv preprint arXiv:2111.14363*, 2021. Submitted for publication.

[Yel15] Jeffrey Yelton. Dyadic torsion of elliptic curves. *European Journal of Mathematics*, 1(4):704–716, 2015.

[Zyw11] David Zywina. Bounds for Serre's open image theorem. *arXiv preprint arXiv:1102.4656*, 2011.

[Zyw15a] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015.

[Zyw15b] David Zywina. On the surjectivity of mod ℓ representations associated to elliptic curves. *arXiv preprint arXiv:1508.07661*, 2015.

[Zyw15c] David Zywina. Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07663*, 2015.

Curriculum Vitae

Sebastiano Tronto was born in Feltre, Italy in 1994. During high school he competed in many Mathematics and programming competitions, obtaining multiple medals at the national level and a qualification for the *International Olympiad in Informatics* in 2012.

In 2013 he enrolled at the University of Trento, where he obtained his bachelor degree *with honour* in 2016 with a thesis on Galois groups and fundamental groups, under the supervision of prof. Edoardo Ballico.

He then joined the ALGANT Master program, spending one year at the University of Milan and one year at Leiden University. He wrote his thesis, entitled *The Brauer-Manin obstruction to strong approximation*, under the supervision of Dr. Martin Bright at Leiden University. He was awarded his Masters diploma *cum laude* by the University of Milan and *summa cum laude* by Leiden University.

After completing his master program, he started his PhD in a cotutelle between the University of Luxembourg and Leiden University, under the supervision of Antonella Perucca and Peter Bruin.

After his PhD he is starting a carreer outside academia, where he can put to work the problem-solving skills he developed as a Mathematics student.