Imperial College London

Advanced Research Project in Mathematics

Department of Computing

Final Report

Arithmetic Statistics for Elliptic Curves

Modelling the Selmer group, the Tate-Shafarevich group, and the Mordell-Weil rank of elliptic curves over number fields

Author
David Kurniadi Angdinata
01201743

Supervisor
Professor Toby Gee

Second marker
Professor Alexei Skorobogatov

June 2020

A project submitted in partial fulfillment of the requirement for the award of MEng Mathematics and Computer Science (Pure Mathematics and Computational Logic) degree of Imperial College London

Abstract

The Mordell-Weil theorem states that any elliptic curve E defined over a number field K is a finitely generated abelian group, so that $E(K)$ is isomorphic to a direct product of a finite torsion subgroup and a free abelian group of finite rank. Over the rationals, while the torsion subgroup is fully understood from a result by Mazur, the Mordell-Weil rank is much less understood. For instance, it remains an open question if it is bounded above, with a historical belief that it is not, due to much empirical evidence.

A recent probabilistic model proposed by Poonen et al provides theoretical evidence to refute this claim, namely that all but finitely many rational elliptic curves have rank at most 21. Their proposed heuristic is based on modelling Tate-Shafarevich groups using random alternating matrices, and has its grounds in a theorem that a p^e-Selmer group is almost always the intersection of two Lagrangian direct summands of a metabolic quadratic $\mathbb{Z}/p^e$-module of infinite rank, a consequence of standard arithmetic duality theorems.

This project aims to serve as an introduction to the style of arguments in arithmetic statistics by providing a full proof of this result, as well as verifying desired properties of a heuristic that models this result. As a consequence, important predictions on Selmer groups, Tate-Shafarevich groups, and Mordell-Weil ranks can be made, including the conjecture that n-Selmer groups have average size equal to the sum of divisors of n, as well as the folklore conjecture that there are finitely many rational elliptic curves of rank greater than 21.

Acknowledgements

I would like to express my sincere gratitude to everyone who have supported me academically and socially during the two months of report writing, as well as throughout my four years in Imperial.

In particular, I would like to thank Professor Johannes Nicaise for introducing me to the arithmetic of elliptic curves in a summer research project two years ago. His willingness to supervise me and the few conversations we had were very encouraging to my early mathematical career, and I have since delved deeper into the area and developed a keen research interest.

Moreover, I would like to thank Dr David Helm for introducing me to the machinery of Galois cohomology as applied to class field theory in a summer research project last year. Despite being busy, he was willing to meet me in the afternoons every week, and we engaged in many enthusiastic conversations on a broad range of number-theoretic ideas, albeit only at a high-level. His insights and viewpoints have since solidified my thoughts and improved my mathematical maturity.

Furthermore, I would like to thank my current project supervisors Professor Toby Gee and Professor Alexei Skorobogatov for their support and guidance throughout the duration of the research project. I had several doubts about the scope of the material early on, and some ideas I could not follow, but they clarified all of them in great detail through office hours and email exchanges.

Additionally, I would like to thank Mr Stephen Diehl and Adjoint UK Ltd for providing me with a summer internship opportunity last year on pairing-based elliptic curve cryptography. It was a very enjoyable experience working with number theory in Haskell, which helped me appreciate the existence of applications of pure mathematics outside of academia.

Last but not least, I would also like to thank all of my colleagues whom I have had intellectual discussions with, including Christopher Burns, Alberto Centelles, Jiang Wei, and Wu Peiran, who have all helped me one way or another in this project. I am especially grateful to Wu Peiran who did a thorough proofreading of my report, even after the submission deadline.

Contents

Chapter 1

Introduction

1.1 Motivational background

In the field of number theory, there are many important open problems that withstood the minds of countless number theorists over decades, a strong contender being the elusive Riemann hypothesis in analytic number theory. While a complete answer to these questions may seem out of reach at present, they remain conjectures widely believed by working mathematicians due to significant theoretical and numerical evidence.

A fascinating example of theoretical evidence is the probabilistic model offered by Cohen and Lenstra in their seminal paper on heuristics on class groups of number fields [CL84]. They introduced a plausible heuristic on the distribution of ideal class groups, claiming and justifying that their asymptotic behaviours mimick those of generic finite abelian groups weighted inversely by the size of their automorphism groups, which later turned out to match numerical results very well. Their paper was later followed on by Friedman and Washington who reinterpreted it on random matrices [FW89], and their ideas have since become a powerful source of predictions for number fields, which kickstarted the field of arithmetic statistics.

One route that arithmetic statistics took was in the direction of elliptic curves, a highly non-trivial theory with an ocean of deep unsolved problems. This was first observed by Delaunay, where he modelled Tate-Shafarevich groups of elliptic curves based on the Cohen-Lenstra heuristics [Del01]. This was in turn motivated by the strong analogy between number fields and elliptic curves, where the group of units corresponds to the rational points and the ideal class group corresponds to the Tate-Shafarevich group [Del07].

Two famous conjectures of elliptic curves proposed in the late twentieth century are often known as the **rank distribution conjecture** and **rank boundedness conjecture**. The first of these claims that half of all elliptic curves have Mordell-Weil rank zero and the remaining half have Mordell-Weil rank one, while higher Mordell-Weil ranks constitute zero percent of all elliptic curves over number fields, implying that a suitably-defined average rank would be $\frac{1}{2}$. Currently, the best results by Bhargava et al merely show that the average rank of elliptic curves over $\mathbb{Q}$ is strictly less than one, and that both rank zero and rank one cases comprise non-zero densities across all elliptic curves over $\mathbb{Q}$ [BS15a; BS15b].

The second of these asks whether there is an upper bound to the Mordell-Weil rank of elliptic curves over number fields [Sil09, Conjecture 10.1]. Over the past few decades, the general consensus amongst the experts has flip-flopped at least twice [PPVW19, Section 3]. Those in favour of unboundedness argue that this phenomenon provably occurs in other global fields, and that the proven lower bound for this upper bound increases every few years. For instance, Elkies discovered an elliptic curve over $\mathbb{Q}$ with Mordell-Weil rank at least 28, and very recently one with Mordell-Weil rank exactly 20 [EK20].

On the other hand, a recent series of papers by Poonen et al suggested otherwise, by providing a justified heuristic inspired by ideas from arithmetic statistics [Poo17]. They modelled the asymptotic behaviour of Mordell-Weil ranks through analysing the distribution of Tate-Shafarevich groups modelled by random alternating matrices [PPVW19], while providing sufficient theoretical evidence through proven theorems of Selmer groups [BKLPR15; PR12]. All of these groups are linked in a fundamental short exact sequence, and a large portion of the results in their papers are attempts to justify the plausibility of a model for the sequence. One of their final predictions is the surprising result that there are only finitely many isomorphism classes of elliptic curves over $\mathbb{Q}$ with Mordell-Weil rank greater than 21.

Undeniably, a thorough understanding of the structure of the Selmer group goes a long way towards proving results for the Mordell-Weil rank. This is highlighted not only in the papers by Poonen et al, but also in the papers by Bhargava et al, where they explicitly computed the average sizes of certain Selmer groups to deduce asymptotic results of Mordell-Weil ranks [BS13a; BS13b], and made the following conjecture.

(1.1.1) **Conjecture** ([BS13a, Conjecture 4]). *Let $E \in \mathcal{E}(K)$ be a elliptic curve chosen uniformly at random. Then*

$$\mathbb{E}\left[\#\mathcal{S}_n(K,E)\right] = \sigma_1(n), \qquad n \in \mathbb{N}^+,$$

where $\sigma_1 : \mathbb{N}^+ \to \mathbb{N}$ is the sum of divisors function. [1]

In their series of papers, Bhargava et al verified Conjecture 1.1.1 for $n = 2, 3, 4, 5$, and these were enough to deduce powerful partial results for the rank distribution conjecture. While the general claim remains a consensual open problem, the model for the Selmer group in the papers by Poonen et al does indeed satisfy Conjecture 1.1.1, further supporting both the conjecture and the validity of the model. Curiously, the analogous result seems to be true for elliptic curves over function fields of odd characteristic, albeit under a slightly different notion of heights than those for number fields [Lan20, Theorem 1.2].

1.2 Report structure

The aim of this report is to provide detailed proofs to two main results of Selmer groups and its model, labelled in the following chapters as Theorem 3.2.1 and Theorem 3.3.1, which combines to yield a hypothetical affirmative to Conjecture 1.1.1. The overarching idea follows the arguments in the series of papers by Poonen et al [Poo17; PPVW19; BKLPR15; PR12], but in many sections, more elementary proofs are provided whenever possible, and these are often a combination of various notions taken from other referenced sources.

While the first chapter is purely introductory, the second chapter will begin by providing any additional background required to bridge the gap between the papers and undergraduate mathematics, so as to make the report accessible to a typical undergraduate. This includes a short introduction to group and Galois cohomology, culminating in the statement of standard arithmetic duality theorems, which will be a recurring flavour in the rest of the report. Standard facts on elliptic curves will also be laid out succinctly, and the full definition of the Selmer and Tate-Shafarevich groups will be provided, along with an interpretation in terms of twists and torsors. The facts in this chapter will be freely used in other chapters without reference.

The third core chapter first provides basic definitions of quadratic modules, to allow for the statement of Theorem 3.2.1 and Theorem 3.3.1, while the remaining sections aim to provide a detailed proof of these theorems. Many interesting remarks will be presented without proofs alongside the overall argument, but they are unnecessary in the grand scheme of the proof and can be largely ignored. However, the final chapter will conclude the report by providing several consequences of the model, and will freely use these remarks.

My primary contribution is a coherent organisation and rephrasal of the arguments spread across several papers into a stand-alone report. I have replaced any proofs deemed relatively advanced, especially those with scheme-theoretic arguments, with more elementary arguments, and have filled in a lot of the details omitted by the original authors. I have also fixed a few minor sign issues and special cases that were disregarded by the original authors, and adapted an external proof to a conjecture in the original paper.

I have also attempted to maintain a set of consistent conventions and notation based on the standard Bourbaki notation. For instance, the variable F will always denote a field of characteristic zero, while E will always denote an elliptic curve. All rings are commutative with unity, and all varieties are quasi-projective. Whenever a group variety is defined without the field of definition, it will always be over the algebraic closure. Finally, the Hom and tensor product functors are always over $\mathbb{Z}$ unless explicitly denoted.

As it is not possible to fill in every detail there is, the reader is assumed to be familiar with undergraduate number theory, which includes basic commutative and homological algebra, classical algebraic geometry, and basic algebraic number theory. An acquaintance with the language of category theory, infinite group theory, and infinite Galois theory would be helpful, but they will not be used as freely. All other results will be included in the next chapter, where the proofs are deferred to references provided for the reader's convenience.

[1] The notation used here will be fully clarified in the following chapter.

Chapter 2

Preliminary background

This chapter aims to establish basic facts and notational conventions, well-known in the fields of algebraic number theory and arithmetic geometry, but typically not covered at the undergraduate level. All of the definitions and results are directly taken from either Silverman's book on elliptic curves [Sil09], Serre's book on local fields [Ser80], or Milne's books on arithmetic duality [Mil06] and class field theory [Mil13], with one result quoted from each of Silverman's advanced book on elliptic curves [Sil94], Mumford's book on abelian varieties [Mum70], and Hartshorne's book on algebraic geometry [Har77]. The relevant ideas and constructions are briefly sketched here for the reader's convenience, which will be quoted freely in the report without any additional reference, but the reader is invited to consult any one of the wonderful books above.

2.1 Galois cohomology

Throughout this section, let G be a group acting on a group A, so A is called a **G-group**, or a **G-module** when A is abelian. The action of G will be denoted multiplicatively, while the group operation of A will be denoted additively even in non-abelian contexts to distinguish it from its group action.

2.1.1 Group cohomology

The most prevalent theory in the modern literature involves the case of A being abelian, which furnishes the abelian category of G-modules consisting of abelian groups equipped with G-linear group actions and G-equivariant group homomorphisms, and can be identified with the category of modules over the group algebra $\mathbb{Z}[G]$ [Ser80, Section VII.1]. Taking G-invariants establishes a functor $(-)^G$ from this category to the category of abelian groups that is canonically isomorphic to the left exact covariant functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, which in turn provides a definition of the n-th **cohomology group** in terms of the derived functor

$$\mathrm{H}^n(G, A) \coloneqq \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A), \qquad n \in \mathbb{N}.$$

While this provides a succinct definition, certain computations often require explicit formulations of several low-dimensional cohomology groups. It is easy to see that $\mathrm{H}^0(G, A) \coloneqq A^G$, while

$$\mathrm{H}^1(G, A) \coloneqq \{\xi : G \to A \mid \forall \sigma, \tau \in G,\ \xi(\sigma\tau) = \xi(\sigma) + \sigma \cdot \xi(\tau)\} / \sim,$$

given the equivalence relation

$$\xi \sim \xi' \qquad \iff \qquad \exists a \in A,\ \forall \sigma \in G,\ a + \xi(\sigma) = \xi'(\sigma) + \sigma \cdot a.$$

Given such a description, it is easy to see that $\mathrm{H}^1(G, A) = \mathrm{Hom}(G, A)$ whenever the group action is trivial, and to verify that $\mathrm{H}^1(G, A)$ is n-torsion if G has finite order $n \in \mathbb{N}^+$ [Sil09, Exercise B.1]. In the latter scenario, if A is also finite of order $m \in \mathbb{N}^+$ coprime to n, then $\mathrm{H}^1(G, A)$ is mutually annihilated by m and by n, so the overall cohomology group must be trivial. Similarly, a description for $\mathrm{H}^2(G, A)$ is

$$\mathrm{H}^2(G, A) \coloneqq \{\xi : G \times G \to A \mid \forall \sigma, \tau, \upsilon \in G,\ \sigma \cdot \xi(\tau, \upsilon) + \xi(\sigma, \tau\upsilon) = \xi(\sigma\tau, \upsilon) + \xi(\sigma, \tau)\} / \sim,$$

given the equivalence relation

$$\xi \sim \xi' \qquad \iff \qquad \exists \chi : G \to A,\ \forall \sigma, \tau \in G,\ \chi(\sigma\tau) + \xi(\sigma, \tau) = \xi'(\sigma, \tau) + \chi(\sigma) + \sigma \cdot \chi(\tau),$$

while any higher-dimensional cohomology group $\mathrm{H}^n(G, A)$ generally consists of **n-cocycles** $\xi : G^n \to A$ satisfying certain crossed conditions modulo certain equivalence relations [Ser80, Section VII.3].

It turns out that group cohomology is a universal **cohomological δ-functor** [Ser80, Section VII.2]. In particular, this says that applying the group cohomology functor to a short row-exact diagram of G-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

functorially induces a long row-exact diagram of cohomology groups

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & \mathrm{H}^0(G, A) & \longrightarrow & \mathrm{H}^0(G, B) & \longrightarrow & \mathrm{H}^0(G, C) & \xrightarrow{\delta_0} & \mathrm{H}^1(G, A) & \longrightarrow & \mathrm{H}^1(G, B) & \longrightarrow & \mathrm{H}^1(G, C) \xrightarrow{\delta_1} \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{H}^0(G, A') & \longrightarrow & \mathrm{H}^0(G, B') & \longrightarrow & \mathrm{H}^0(G, C') & \longrightarrow & \mathrm{H}^1(G, A') & \longrightarrow & \mathrm{H}^1(G, B') & \longrightarrow & \mathrm{H}^1(G, C') \longrightarrow \dots \end{array},$$

which is not uncharacteristic of many cohomology theories. The **connecting homomorphisms** δ_0 and δ_1 in the top row can be explicitly described as follows. Let $c \in \mathrm{H}^0(G, C) = C^G$ be a G-invariant element, and let $\sigma \in G$ be a group element. By surjectivity of β, there is an element $b \in B$ such that $c = \beta(b)$. It is easy to see that $\sigma \cdot b - b \in \ker \beta = \operatorname{im} \alpha$, so there is an element $a_\sigma \in A$ such that $\sigma \cdot b - b = \alpha(a_\sigma)$. Then define

$$\delta_0(c) \coloneqq (\sigma \mapsto a_\sigma).$$

Likewise, let $\xi \in \mathrm{H}^1(G, C)$ be a 1-cocycle, and let $\sigma, \tau \in G$ be group elements. By surjectivity of β, there are elements $b_\sigma, b_\tau, b_{\sigma\tau} \in B$ such that $\xi(\sigma) = \beta(b_\sigma)$, $\xi(\tau) = \beta(b_\tau)$, and $\xi(\sigma\tau) = \beta(b_{\sigma\tau})$. It is again easy to see that there is an element $a_{\sigma,\tau} \in A$ such that $b_\sigma + \sigma \cdot b_\tau - b_{\sigma\tau} = \alpha(a_{\sigma,\tau})$. Then define

$$\delta_1(\xi) \coloneqq ((\sigma, \tau) \mapsto a_{\sigma,\tau}).$$

These can be verified, by the definition of cocycles, to be well-defined and independent of the choices of lifts.

The boundary of the well-known **Hochschild-Lyndon-Serre spectral sequence** establishes a relationship between the cohomology groups defined by G and a subgroup H, through a left exact **inflation-restriction exact sequence** of cohomology groups [Ser80, Proposition VII.5] given by

$$0 \to \mathrm{H}^n\left(G/H, A^H\right) \xrightarrow{\inf} \mathrm{H}^n(G, A) \xrightarrow{\mathrm{res}} \mathrm{H}^n(H, A), \qquad n \in \mathbb{N},$$

provided that $\mathrm{H}^i(H, A)$ is trivial for all $i = 1, \dots, n-1$. Here, the **restriction map** is a composition $\mathrm{res} : \mathrm{H}^n(G, A) \to \mathrm{H}^n(H, A)^{G/H} \to \mathrm{H}^n(H, A)$ induced by the inclusion $H \hookrightarrow G$, while the **inflation map** is a composition $\inf : \mathrm{H}^n\left(G/H, A^H\right) \to \mathrm{H}^n\left(G, A^H\right) \to \mathrm{H}^n(G, A)$ induced by the quotient $G \twoheadrightarrow G/H$ and the inclusion $A^H \hookrightarrow A$. When G is finite, by further defining an analogous **corestriction map**, it can be shown that the induced restriction map $\mathrm{res} : \mathrm{H}^n(G, A)_p \to \mathrm{H}^n(G_p, A)$ on a p-Sylow subgroup G_p is injective, where $\mathrm{H}^n(G, A)_p$ is the p-primary component of $\mathrm{H}^n(G, A)$ for some prime $p \in \mathbb{N}^+$ [Ser80, Theorem IX.4].

Another notable property of group cohomology relates the cohomology groups defined by A and another G-module B, through the existence of an alternating $\mathbb{Z}$-bilinear **cup product** [Ser80, Proposition VIII.5]

$$\begin{array}{rccc} \cup & : & \mathrm{H}^n(G, A) \times \mathrm{H}^m(G, B) & \longrightarrow & \mathrm{H}^{n+m}(G, A \otimes B) \\ & & (\xi, \xi') & \longmapsto & \xi \cup \xi' \end{array}, \qquad n, m \in \mathbb{N},$$

which is universal with respect to certain tensorial properties, and is defined by

$$\xi \cup \xi' \coloneqq ((\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m) \mapsto \xi(\sigma_1, \dots, \sigma_n) \otimes \sigma_1 \cdot \dots \cdot \sigma_n \cdot \xi'(\tau_1, \dots, \tau_m)).$$

This is an analogue of the topological cup product in singular cohomology.

2.1.2 Non-abelian cohomology

In the scenario where A is non-abelian, the positive-dimensional cohomologies are not necessarily groups, but merely **pointed sets** with a distinguished identity, so the notions of kernels and images in short exact sequences still make sense. The explicit descriptions of these pointed sets in terms of cocycles remain unchanged, except to account for non-commutativity of the respective group operations. Applying the **non-abelian group cohomology** functor to a short exact sequence of G-groups

$$0 \to A \to B \to C \to 0$$

still induces a truncated long exact sequence of cohomology pointed sets

$$0 \to \mathrm{H}^0(G, A) \to \mathrm{H}^0(G, B) \to \mathrm{H}^0(G, C) \xrightarrow{\delta_0} \mathrm{H}^1(G, A) \to \mathrm{H}^1(G, B) \to \mathrm{H}^1(G, C) \xrightarrow{\delta_1} \mathrm{H}^2(G, A),$$

but is exact at $\mathrm{H}^1(G, C)$ if and only if A injects into the centre of B [Ser80, Appendix VII]. The **connecting maps** δ_0 and δ_1 are again defined with non-commutativity in mind, but with this additional assumption, conjugation by B will preserve images of elements of A, such as the previously defined $\alpha(a_\sigma)$ and $\alpha(a_{\sigma,\tau})$. As with the abelian case, δ-functoriality holds and cup products are defined exactly the same way.

2.1.3 Galois cohomology

When G is a **profinite topological group** of potentially infinite order and A is a **topological G-module**, the definitions in the basic theory have to be slightly adjusted so as to behave well with direct and inverse limits. In particular, this says that G is an inverse limit of discrete finite groups, equipped with a compatible **profinite topology** with a basis of open sets around the identity consisting of finite index normal subgroups such that G is compact and Hausdorff, while A is equipped with a continuous G-action with respect to this topology. The n-th **profinite cohomology** group is then defined to be the direct limit

$$\mathrm{H}^n(G, A) \coloneqq \varinjlim_{H} \mathrm{H}^n\left(G/H, A^H\right), \qquad n \in \mathbb{N},$$

taken with respect to open finite index normal subgroups H of G and their natural inflation maps. With the restriction that cocycles are necessarily continuous with respect to this topology, all of the properties listed previously continue to hold for profinite cohomology groups by passage to the limit, and coincide in the finite discrete case [Ser80, Section X.3], so this shall be an underlying assumption moving forward.

A prominent example in number theory is the case where G is the Galois group of a possibly infinite Galois extension F' over a field F, constructed as a profinite topological group equipped with the **Krull topology**, which acts naturally on the F-rational points of a group variety A defined over F to realise it as a topological G-module. The respective n-th profinite **Galois cohomology** groups are then denoted as

$$\mathrm{H}^n(F'/F, A) \coloneqq \mathrm{H}^n\left(\mathrm{Gal}\left(F'/F\right), A\left(F'\right)\right), \qquad n \in \mathbb{N},$$

the latter of which, by the infinite version of the Galois correspondence, is the direct limit taken with respect to finite Galois extensions of F that are subfields of F'. In the case of the algebraic closure $\overline{F}$ of a general field F of characteristic zero, it is customary to omit the field extension and simply write

$$\mathrm{H}^n(F, A) \coloneqq \mathrm{H}^n\left(\mathrm{Gal}\left(\overline{F}/F\right), A\left(\overline{F}\right)\right), \qquad n \in \mathbb{N}.$$

Note that with this notation, $\mathrm{H}^n(F, \mathrm{GL}_1)$ refers to the n-th cohomology group of $\overline{F}^\times$ rather than of $F^\times$.

Applying non-abelian Galois cohomology to the general linear group varieties GL_n and PGL_n generalises Noether's formulation of **Hilbert's theorem 90** [Ser80, Proposition X.3] to establish the triviality

$$\mathrm{H}^1(F, \mathrm{GL}_n) = 0, \qquad n \in \mathbb{N}.$$

Applying this to the Galois cohomology groups induced by the obvious short exact sequence of groups

$$0 \to \overline{F}^\times \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 0, \qquad n \in \mathbb{N},$$

gives an injection of pointed sets [Ser80, Proposition X.8]

$$\mathrm{H}^1(F, \mathrm{PGL}_n) \hookrightarrow \mathrm{H}^2(F, \mathrm{GL}_1), \qquad n \in \mathbb{N},$$

the latter of which is isomorphic to the **Brauer group** $\mathrm{Br}\, F$ [Ser80, Proposition X.9], defined as the abelian group of F-central simple algebras modulo F-isomorphisms of their underlying F-division algebras.

2.1.4 Class field theory

A well-known application of the machinery of Galois cohomology is in the modern treatment of the proofs of local and global class field theory, namely **Artin's reciprocity law** [Mil13, Theorems V.3.5 and V.5.3], **Takagi's existence theorem** [Mil13, Theorems V.3.6 and V.5.5], and their local counterparts [Mil13, Theorems I.1.1 and I.1.4]. These statements are algebraic in nature, yet their original proofs were through the analysis of L-series where the local versions were deduced from the global statements, which were historically considered unsatifactory and were later revamped by Chevalley and Tate via the introduction of class formations. While the main statements will be elided here, several relevant consequences will be mentioned.

Let K be a number field, and let $\mathcal{V}_K$ be the set of all **places** of K. These are equivalence classes of all non-trivial absolute values on K, which by Ostrowski's theorem consists of the **non-archimedean places** $\mathcal{V}_K^0$ induced by $\mathfrak{p}$-adic norms and the **archimedean places** $\mathcal{V}_K^\infty$ induced by real and complex embeddings. Completing K with respect to a place $v \in \mathcal{V}_K$ yields a locally compact **local field** K_v, which has a finite residue field in the non-archimedean case, while K is itself a **global field** satisfying the product formula [Ser80, Section II.1]. Each non-archimedean place exhibits a canonical isomorphism [Mil13, Theorem III.2.1]

$$\mathrm{inv}_{K_v} : \mathrm{Br}\, K_v \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}, \qquad v \in \mathcal{V}_K^0,$$

while in the archimedean scenario, there are obvious identifications $\mathrm{Br}\,\mathbb{R} = \{\pm 1\}$ and $\mathrm{Br}\,\mathbb{C} = 0$ by any description of the Brauer group, so analogous monomorphisms can be constructed as

$$\mathrm{inv}_{\mathbb{R}} : \mathrm{Br}\,\mathbb{R} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}, \qquad \mathrm{inv}_{\mathbb{C}} : \mathrm{Br}\,\mathbb{C} \cong \mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

These monomorphisms are called **Hasse invariants**, and are relevant in the construction of class formations. Combining global class field theory and the **Albert-Brauer-Hasse-Noether theorem** for division algebras yields a short exact **fundamental sequence of global class field theory** [Mil13, Theorem VIII.4.2]

$$0 \to \mathrm{Br}\, K \xrightarrow{\hookrightarrow} \bigoplus_{v \in \mathcal{V}_K} \mathrm{Br}\, K_v \xrightarrow{\sum \mathrm{inv}_{K_v}} \mathbb{Q}/\mathbb{Z} \to 0,$$

where the latter map arises from summing finitely many local Hasse invariants.

Let L be a Galois extension of K. The choice of a place $w \in \mathcal{V}_L$ extending a place $v \in \mathcal{V}_K$ uniquely determines an embedding $K_v \hookrightarrow L_w$, and vice versa [Ser80, Corollary II.2]. Its Galois group $\mathrm{Gal}\,(L_w/K_v)$ is then canonically isomorphic to the **decomposition group**, the stabiliser of w in $\mathrm{Gal}\,(L/K)$ acting transitively on the places extending v [Ser80, Proposition I.19]. The archimedean scenario is relatively simple, since the decomposition group is either trivial or $\mathrm{Gal}\,(\mathbb{C}/\mathbb{R})$, the latter of which occurs precisely with ramification where $K_v \cong \mathbb{R}$ and $L_w \cong \mathbb{C}$. In the non-archimedean case, however, within the decomposition group lies the **inertia group**, the normal subgroup acting trivially on the residue field of K_v. This is in turn canonically isomorphic to the Galois group $\mathrm{Gal}\,(L_w/K_v^{\mathrm{u}})$, where K_v^{u} denotes the maximal unramified extension of K_v contained in L_w [Ser80, Proposition I.21], hence furnishing a short exact sequence of Galois groups

$$0 \to \mathrm{Gal}\,(L_w/K_v^{\mathrm{u}}) \to \mathrm{Gal}\,(L_w/K_v) \to \mathrm{Gal}\,(K_v^{\mathrm{u}}/K_v) \to 0,$$

where the first two Galois groups are identified with the inertia and decomposition groups respectively. When L is unramified over K, the inertia subgroup is trivial, so the decomposition group can be identified with the Galois group of the respective residue fields. This is in turn cyclic with a generator called the **Frobenius substitution** $\sigma_w \in \mathrm{Gal}\,(L/K)$ [Ser80, Section I.8], which is part of the map defining Artin's reciprocity law. Now an important consequence of global class field theory is **Chebotarev's density theorem**, which states that for any finite Galois extension L over K and any conjugacy class C of $\mathrm{Gal}\,(L/K)$, the set of places

$$\left\{ v \in \mathcal{V}_K^0 \text{ unramified} \;\middle|\; C = \{\sigma_w \in \mathrm{Gal}\,(L/K) \mid w \text{ extends } v\} \right\}$$

has density exactly $\#C/\,[L:K]$ amongst all non-archimedean places, for some well-defined limiting notion of density [Mil13, Theorem V.3.23]. In particular, this is a positive proportion of places in $\mathcal{V}_K$, so that when the extension is abelian and conjugacy classes are merely singletons, any element of $\mathrm{Gal}\,(L/K)$ generates a cyclic subgroup isomorphic to infinitely many decomposition groups generated by the Frobenius substitutions.

2.1.5 Arithmetic duality theorems

This final subsection states several standard yet powerful arithmetic duality theorems on local and global cohomology. For a place $v \in \mathcal{V}_K$, denote the **Pontryagin dual** and the **Cartier dual** respectively by

$$(-)^\star \coloneqq \operatorname{Hom}(-, \operatorname{Br} K_v), \qquad (-)^\dagger \coloneqq \operatorname{Hom}\left(-, \overline{K_v}^\times\right),$$

so that, in the non-archimedean case, the Pontryagin dual is the usual definition of $(-)^\star = \operatorname{Hom}(-, \mathbb{Q}/\mathbb{Z})$.

Let A be a finite $\operatorname{Gal}\left(\overline{K_v}/K_v\right)$-module for some place $v \in \mathcal{V}_K$. If v is non-archimedean, **Tate's local duality** establishes a canonical non-degenerate perfect pairing via the cup product [Mil06, Corollary I.2.3]

$$\cup : \mathrm{H}^n\left(K_v, A^\dagger\right) \times \mathrm{H}^{2-n}\left(K_v, A\right) \to \operatorname{Br} K_v, \qquad n = 0, 1, 2,$$

which, in the case $n = 1$, induces natural Pontryagin dualities between finite groups

$$\mathrm{H}^1\left(K_v, A^\dagger\right) \cong \mathrm{H}^1\left(K_v, A\right)^\star, \qquad \mathrm{H}^1\left(K_v, A\right) \cong \mathrm{H}^1\left(K_v, A^\dagger\right)^\star.$$

An essentially identical statement holds when v is archimedean [Mil06, Theorem I.2.13(a)], except that it uses the modified n-th **Tate cohomology** groups for $G = \operatorname{Gal}\left(\overline{K_v}/K_v\right)$, defined by

$$\mathcal{H}^n(G, A) \coloneqq \begin{cases} \mathrm{H}^n(G, A) & n > 1 \\ A^G/\mathrm{N}_G A & n = 0 \end{cases}, \qquad \mathrm{N}_G A \coloneqq \left\{ \sum_{\sigma \in G} \sigma \cdot a \;\middle|\; a \in A \right\},$$

whose extension to negative coefficients is relevant in the proof of Artin's reciprocity law. As a convention, since the statement of Tate's local duality, amongst other important dualities, differ in the archimedean case only for $\mathrm{H}^0\left(K_v, A\right)$, the zeroth cohomology group in the archimedean case will be abusively denoted

$$\mathrm{H}^0\left(K_v, A\right) \coloneqq \mathcal{H}^0\left(\operatorname{Gal}\left(\mathbb{C}/K_v\right), A\right), \qquad v \in \mathcal{V}_K^\infty,$$

which shall be the prevailing notation from now on.

For the global duality theorem, let A be a finite $\operatorname{Gal}\left(\overline{K}/K\right)$-module. For each place $v \in \mathcal{V}_K$, the inclusion of Galois groups $\operatorname{Gal}\left(\overline{K_v}/K_v\right) \hookrightarrow \operatorname{Gal}\left(\overline{K}/K\right)$ induced by the completion $K \hookrightarrow K_v$ supplies the local restriction maps $\mathrm{H}^n\left(K, A\right) \to \mathrm{H}^n\left(K_v, A\right)$. Define the n-th **unramified cohomology** group by

$$\mathrm{H}^n_{\mathrm{u}}\left(K_v, A\right) \coloneqq \mathrm{H}^n\left(K_v^{\mathrm{u}}/K_v, A^{\operatorname{Gal}\left(\overline{K_v}/K_v^{\mathrm{u}}\right)}\right), \qquad n \in \mathbb{N},$$

where the inflation-restriction exact sequence applied to $\operatorname{Gal}\left(\overline{K_v}/K_v\right) / \operatorname{Gal}\left(\overline{K_v}/K_v^{\mathrm{u}}\right) \cong \operatorname{Gal}\left(K_v^{\mathrm{u}}/K_v\right)$ yields

$$0 \to \mathrm{H}^n_{\mathrm{u}}\left(K_v, A\right) \xrightarrow{\inf} \mathrm{H}^n\left(K_v, A\right) \xrightarrow{\mathrm{res}} \mathrm{H}^n\left(K_v^{\mathrm{u}}, A\right), \qquad n \in \mathbb{N},$$

provided of course that $\mathrm{H}^i\left(K_v^{\mathrm{u}}, A\right)$ is trivial for all $i = 1, \ldots, n-1$. Then define the n-th **adelic cohomology** group $\mathrm{H}^n\left(\mathbb{A}_K, A\right)$ as the **restricted product** of $\left(\mathrm{H}^n\left(K_v, A\right)\right)_{v \in \mathcal{V}_K}$ with respect to $\left(\mathrm{H}^n_{\mathrm{u}}\left(K_v, A\right)\right)_{v \in \mathcal{V}_K}$, namely

$$\mathrm{H}^n\left(\mathbb{A}_K, A\right) \coloneqq \left\{ \left(\xi_v\right)_{v \in \mathcal{V}_K} \in \prod_{v \in \mathcal{V}_K} \mathrm{H}^n\left(K_v, A\right) \;\middle|\; \xi_v \in \mathrm{H}^n_{\mathrm{u}}\left(K_v, A\right) \text{ for all but finitely many } v \in \mathcal{V}_K \right\}, \quad n \in \mathbb{N}.$$

Now the images of the restriction maps $\mathrm{H}^n\left(K, A\right) \to \mathrm{H}^n\left(K_v, A\right)$ land in $\mathrm{H}^n_{\mathrm{u}}\left(K_v, A\right)$ for all but finitely many places $v \in \mathcal{V}_K$ [Mil06, Lemma I.4.8], furnishing well-defined embeddings

$$\tau^n : \mathrm{H}^n\left(K, A\right) \to \mathrm{H}^n\left(\mathbb{A}_K, A\right), \qquad n \in \mathbb{N},$$

and analogously $\tau^n_\dagger : \mathrm{H}^n\left(K, A^\dagger\right) \to \mathrm{H}^n\left(\mathbb{A}_K, A^\dagger\right)$ for the Cartier duals. In the relevant case of $n = 0, 1, 2$, Tate's local duality replaces this last group with $\mathrm{H}^{2-n}\left(\mathbb{A}_K, A\right)^\star$, so that taking Pontryagin duals of the maps $\tau^{2-n}_\dagger : \mathrm{H}^{2-n}\left(K, A^\dagger\right) \to \mathrm{H}^{2-n}\left(\mathbb{A}_K, A^\dagger\right)$ establishes well-defined maps

$$\sigma^n : \mathrm{H}^n\left(\mathbb{A}_K, A\right) \to \mathrm{H}^{2-n}\left(K, A^\dagger\right)^\star, \qquad n = 0, 1, 2.$$

Finally, define the n**-th Tate-Shafarevich group** by

$$Ш^n(K,A) \coloneqq \ker\left(\tau^n : \mathrm{H}^n(K,A) \to \mathrm{H}^n(\mathbb{A}_K,A)\right), \qquad n \in \mathbb{N},$$

a generalisation of the usual Tate-Shafarevich group for elliptic curves, to be defined later. Then **Tate's global duality** establishes a canonical non-degenerate perfect pairing

$$Ш^1(K,A) \times Ш^2\left(K,A^\dagger\right) \to \mathbb{Q}/\mathbb{Z},$$

which, together with its Cartier dual analogue, induce natural Pontryagin dualities between finite groups

$$Ш^2(K,A)^\star \xrightarrow{\sim} Ш^1\left(K,A^\dagger\right), \qquad Ш^1(K,A)^\star \xrightarrow{\sim} Ш^2\left(K,A^\dagger\right).$$

Furthermore, composing these isomorphisms with the obvious inclusions $Ш^n\left(K,A^\dagger\right) \hookrightarrow \mathrm{H}^n\left(K,A^\dagger\right)$ and their Pontryagin dual maps altogether yield two connecting maps

$$\rho : \mathrm{H}^2\left(K,A^\dagger\right)^\star \to \mathrm{H}^1(K,A), \qquad \rho' : \mathrm{H}^1\left(K,A^\dagger\right)^\star \to \mathrm{H}^2(K,A),$$

which fit in the nine-term **Poitou-Tate exact sequence** [Mil06, Theorem I.4.10]

$$\begin{array}{l} 0 \longrightarrow \mathrm{H}^0(K,A) \xrightarrow{\tau^0} \mathrm{H}^0(\mathbb{A}_K,A) \xrightarrow{\sigma^0} \mathrm{H}^2\left(K,A^\dagger\right)^\star \\ \qquad\qquad \xrightarrow{\rho} \\ \qquad \mathrm{H}^1(K,A) \xrightarrow{\tau^1} \mathrm{H}^1(\mathbb{A}_K,A) \xrightarrow{\sigma^1} \mathrm{H}^1\left(K,A^\dagger\right)^\star \\ \qquad\qquad \xrightarrow{\rho'} \\ \qquad \mathrm{H}^2(K,A) \xrightarrow{\tau^2} \mathrm{H}^2(\mathbb{A}_K,A) \xrightarrow{\sigma^2} \mathrm{H}^0\left(K,A^\dagger\right)^\star \longrightarrow 0 \end{array}.$$

The full statement of Tate's global duality encompasses a generalisation of the adelic cohomology groups defined for arbitrary subsets of places, and encodes the topology of these groups as well as the behaviour of higher-dimensional cohomology groups, but the statement as phrased suffices for the purpose of this report.

2.2 Elliptic curves

A primary object of interest in arithmetic geometry is an **elliptic curve** defined over a perfect field F, which is defined to be a smooth projective plane algebraic curve E of genus one over $\overline{F}$, equipped with a distinguished F-rational **basepoint** $\mathcal{O}$ and a $\mathrm{Gal}\left(\overline{F}/F\right)$-action whose invariant subgroup are exactly the F-rational points $E\left(F\right)$. Throughout this section, let E be an elliptic curve defined over a general field F of characteristic zero, typically a number field K or any completion K_v for a place $v \in \mathcal{V}_K$.

2.2.1 Elliptic curves

A characterising feature of elliptic curves amongst other quasi-projective varieties is its peculiar addition law, which realises an elliptic curve as an abelian group with $\mathcal{O}$ as the identity element [Sil09, Algorithm III.2.3], making it an **abelian variety**, and its F-rational points as a subgroup [Sil09, Proposition III.2.2(f)]. When $F = K$, the **Mordell-Weil theorem** and the structure theorem of finitely generated abelian groups characterises the **Mordell-Weil group** $E\left(K\right)$ as a direct sum [Sil09, Theorem VIII.6.7]

$$E\left(K\right) \cong \mathrm{tors}\left(E/K\right) \times \mathbb{Z}^{\mathrm{rk}(E/K)},$$

where $\mathrm{tors}\left(E/K\right)$ is its finite subgroup of torsion points and $\mathrm{rk}\left(E/K\right)$ is its rank as a free abelian group. While the torsion subgroup is finitely computable and well-understood by the **Lutz-Nagell theorem** [Sil09, Corollary VIII.7.2], the **reduction theorem** [Sil09, Application VII.3.2], and **Mazur's theorem** [Sil09, Theorem VIII.7.5], the rank is subtly more mysterious, lending itself to a multitude of important problems in number theory, most notably the **Birch-Swinnerton-Dyer conjecture** [Sil09, Conjecture C.16.5]. As a start, it is unknown if the rank has an upper bound, with a historical belief that it does not [Sil09, Conjecture VIII.10.1] due to several, albeit rare, findings of elliptic curves with large rank.

Due to the extra structure elliptic curves present as objects in the category of abelian varieties, there are two relevant notions of maps between elliptic curves, namely the usual **morphisms** of quasi-projective varieties, which behave irrespective of their basepoints, and **isogenies** of elliptic curves, which preserve basepoints and are automatically group homomorphisms [Sil09, Theorem III.4.8]. Hence morphisms of elliptic curves always refer to isogenies, while emphasis will be made in occasional mentions of F-morphisms of varieties, and any mention of morphisms of varieties without specifying the field of consideration always refers to morphisms over the algebraic closure. There are three main families of endomorphisms that will be relevant, the first of which is the natural **translation** map

$$\begin{array}{rccc} \tau_P & : & E & \longrightarrow & E \\ & & Q & \longmapsto & P+Q \end{array}, \qquad P \in E,$$

and its restriction to $E\left(F\right)$, which are merely isomorphisms of varieties as they shift the basepoint. Associated to such a map is the category-theoretic **pull-back** $\tau_P^* : \overline{F}\left(E\right) \to \overline{F}\left(E\right)$, which simply precomposes any rational function with a translation by $-P$. Next is the natural **multiplication by** n map

$$\begin{array}{rccc} [n] & : & E & \longrightarrow & E \\ & & Q & \longmapsto & nQ \end{array}, \qquad n \in \mathbb{N},$$

which is an isomorphism of elliptic curves whenever $n \neq 0$, whose kernel is by definition the n**-torsion subgroup** $E\left[n\right]$ that is isomorphic to $\left(\mathbb{Z}/n\right)^2$ after fixing a choice of basis points [Sil09, Corollary III.6.4(b)]. It is worth noting that restricting multiplication by n to $E\left(F\right)$ only produces an endomorphism of elliptic curves, which is surjective when F is algebraically closed [Sil09, Theorem II.2.3]. When $F = \mathbb{R}$, the group of real points is either connected and isomorphic to $\mathbb{R}/\mathbb{Z}$ as Lie groups, for which multiplication by n is surjective, or has two connected components and is isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2$, for which multiplication by n is also surjective when n is odd and has cokernel $\mathbb{Z}/2$ otherwise [Sil94, Corollary V.2.3.1]. Finally, allowing multiplication by -1 in the definition above gives the natural **inversion** map

$$\begin{array}{rccc} \iota & : & E & \longrightarrow & E \\ & & Q & \longmapsto & -Q \end{array},$$

and its restriction to $E\left(F\right)$, which are obviously isomorphisms of elliptic curves.

As a consequence of the **Riemann-Roch theorem** [Sil09, Theorem II.5.4], any elliptic curve as defined above is isomorphic as a variety to the projective plane algebraic curve given by a **Weierstrass equation**

$$E_{a,b} \coloneqq \left\{ [x:y:z] \in \mathbb{P}^2 \;\middle|\; y^2z = x^3 + axz^2 + bz^3 \right\}, \qquad \mathcal{O} \coloneqq [0:1:0], \qquad a,b \in F,$$

and conversely, any such **Weierstrass curve**, given the smoothness condition on the **discriminant**

$$\Delta\left(E_{a,b}\right) \coloneqq 4a^3 + 27b^2 \neq 0,$$

defines an elliptic curve [Sil09, Proposition III.3.1]. Two elliptic curves are F-isomorphic precisely when their Weierstrass equations are related by the change of variables $(x,y) \leftrightarrow \left(u^2x, u^3y\right)$ for some $u \in F^\times$, which relates the coefficients by $(a,b) \leftrightarrow \left(u^4a, u^6b\right)$, so that when $F = \overline{F}$, this equates to their **j-invariants**

$$\mathrm{j}\left(E_{a,b}\right) \coloneqq \frac{(4a)^3}{\Delta\left(E_{a,b}\right)}$$

being equal [Sil09, Proposition III.1.4(b)]. When $F = K$, the uniqueness of a Weierstrass representation can be guaranteed up to units by additionally requiring $0 \leq \mathrm{ord}_v\, a < 4$ and $0 \leq \mathrm{ord}_v\, b < 6$ for all non-archimedean places $v \in \mathcal{V}_K^0$. Thus the set of isomorphism classes of elliptic curves defined over K is representable by a set

$$\mathcal{E}\left(K\right) \coloneqq \left\{ E_{a,b} \;\middle|\; \begin{array}{l} a,b \in K,\ \Delta\left(E_{a,b}\right) \neq 0, \\ \forall v \in \mathcal{V}_K^0,\ 0 \leq \mathrm{ord}_v\, a < 4,\ 0 \leq \mathrm{ord}_v\, b < 6 \end{array} \right\}.$$

When $F = K_v$ for some non-archimedean place $v \in \mathcal{V}_K^0$, an analogous unique Weierstrass representation can be constructed with the requirement only for v, and these are called **minimal Weierstrass equations**.

Now any point in projective space can be equipped with an **absolute height**

$$\begin{array}{rccc} \mathfrak{h}_{\mathbb{P}^n} \;:\; & \mathbb{P}^n & \longrightarrow & \mathbb{N}^+ \\ & [x_0 : \cdots : x_n] & \longmapsto & \displaystyle\prod_{v \in \mathcal{V}_K} \max\left(\left|x_0\right|_v, \ldots, \left|x_n\right|_v\right)^{[K_v:\mathbb{Q}_v]} \end{array}, \qquad n \in \mathbb{N},$$

where $\left|-\right|_v$ are normalised absolute values for each place $v \in \mathcal{V}_K$. By the product formula, this is independent of the choice of homogeneous coordinates [Sil09, Proposition VIII.5.4], with only finitely many points with absolute height at most a fixed $h \in \mathbb{N}^+$ [Sil09, Theorem VIII.5.11], inducing a well-defined **natural density**

$$\delta_{\mathbb{P}^n}\left(\mathcal{P}\right) \coloneqq \lim_{h \to \infty} \frac{\#\left\{P \in \mathbb{P}^n \mid \mathcal{P}\left(P\right),\ \mathfrak{h}_{\mathbb{P}^n}\left(P\right) \leq h\right\}}{\#\left\{P \in \mathbb{P}^n \mid \mathfrak{h}_{\mathbb{P}^n}\left(P\right) \leq h\right\}},$$

where $\mathcal{P}$ is any predicate defined on $\mathbb{P}^n$. As such, define an absolute height on $\mathcal{E}\left(K\right)$ by

$$\begin{array}{rccc} \mathfrak{h} \;:\; & \mathcal{E}\left(K\right) & \longrightarrow & \mathbb{N}^+ \\ & E_{a,b} & \longmapsto & \mathfrak{h}_{\mathbb{P}^n}\left([a:b]\right) \end{array},$$

where $a,b \in K$ are defined under the conditions $0 \leq \mathrm{ord}_v\, a < 4$ and $0 \leq \mathrm{ord}_v\, b < 6$ for all non-archimedean places $v \in \mathcal{V}_K^0$, and if $\mathcal{P}$ is a predicate defined on $\mathcal{E}\left(K\right)$, define a natural density on $\mathcal{E}\left(K\right)$ by

$$\delta\left(\mathcal{P}\right) \coloneqq \delta_{\mathbb{P}^n}\left(\mathcal{P},\ \Delta\left(E_{a,b}\right) \neq 0\right).$$

This convenient notation paves way for results and conjectures on the asymptotic behaviour of invariants associated to elliptic curves, such as $\mathrm{tors}\left(E/K\right)$ and $\mathrm{rk}\left(E/K\right)$, and it makes sense to say that some predicate $\mathcal{P}$ holds for **almost all** elliptic curves $E \in \mathcal{E}\left(K\right)$ whenever $\delta\left(\mathcal{P}\right) = 1$ is meant.

Given a fixed $n \in \mathbb{N}^+$, the $\mathrm{Gal}\left(\overline{F}/F\right)$-action on $E\left[n\right]$ induces a homomorphism

$$\rho_{E[n]} : \mathrm{Gal}\left(\overline{F}/F\right) \to \mathrm{Aut}\, E\left[n\right] \cong \mathrm{GL}_2\left(\mathbb{Z}/n\right),$$

where the latter isomorphism arises from fixing a choice of basis points. This is called a two-dimensional **modulo n Galois representation**, and its kernel is precisely $\mathrm{Gal}\left(\overline{F}/F\left(E\left[n\right]\right)\right)$, where the **$n$-torsion field** $F\left(E\left[n\right]\right)$ is the adjunction of F with the coordinates of all non-trivial points in $E\left[n\right]$. The finite version of the Galois correspondence shows that the n-torsion field is also Galois over F, so that $\rho_{E[n]}$ descends to an embedding $\mathrm{Gal}\left(F\left(E\left[n\right]\right)/F\right) \hookrightarrow \mathrm{GL}_2\left(\mathbb{Z}/n\right)$. On the other hand, given an explicit Weierstrass equation for $E = E_{a,b}$, a series of **n-division polynomials** $\Psi_n \in F\left[a,b,X,Y\right]$ can be defined inductively for all $n \in \mathbb{N}^+$, which vanish exactly on the X-coordinates of all non-trivial points in $E\left[n\right]$ [Sil09, Exercise 3.7]. In other words, adjoining these X-coordinates to F yields the splitting field F_{Ψ_n} of Ψ_n, which is in turn a subfield of the n-torsion field obtained by adjoining both coordinates, realising an embedding $\mathrm{Gal}\left(F_{\Psi_n}/F\right) \hookrightarrow \mathrm{GL}_n\left(\mathbb{Z}/n\right)$.

2.2.2 Divisors and linear systems

This subsection records several basic facts about Weil divisors, a construction encoding points of an elliptic curve, taken from algebraic geometry. The **divisor group** $\operatorname{Div}\left(E/\overline{F}\right)$ is the free abelian group generated by all of the formal symbols $[Q]$ for all points $Q \in E$, so a **divisor** is a finite formal sum

$$D \coloneqq \sum_{Q \in E} n_Q \, [Q], \qquad n_Q \in \mathbb{Z}.$$

Given such a divisor, its **degree** is $\deg D \coloneqq \sum_{Q \in E} n_Q \in \mathbb{Z}$, and its **sum** is $\sum D \coloneqq \sum_{Q \in E} [n_Q] \, Q$. If $f \in \overline{F}\left(E\right)^{\times}$ is a non-zero rational function, it has an **associated divisor**

$$[f] \coloneqq \sum_{Q \in E} \left(\operatorname{ord}_Q f\right) [Q],$$

where each $\operatorname{ord}_Q f$ is by definition the normalised valuation of f on the discrete valuation ring $\overline{F}\left[E\right]_Q$, which is obtained by localising $\overline{F}\left[E\right]$ at the maximal ideal generated by rational functions vanishing on Q. A divisor $D \in \operatorname{Div}\left(E/\overline{F}\right)$ is then said to be **principal** if it is an associated divisor of some non-zero rational function, while two divisors $D, D' \in \operatorname{Div}\left(E/\overline{F}\right)$ are said to be **linearly equivalent**, or $D \sim D'$, if their difference is principal. This condition is equivalent to the simultaneous equalities $\deg D = \deg D'$ and $\sum D = \sum D'$ [Sil09, Corollary III.3.5], and using the easy computation [Sil09, Proposition II.3.6(b)] that

$$[\tau_P^* f] = \sum_{Q \in E} \left(\operatorname{ord}_Q f\right) [P + Q], \qquad P \in E,$$

it follows immediately that $P \in E\left[n\right]$ if and only if $n\left[\mathcal{O}\right] \sim n\left[P\right]$ for any $n \in \mathbb{N}^+$. Now, E can be canonically identified with the **Picard group** $\operatorname{Pic}_0\left(E/\overline{F}\right)$ of degree zero principal divisors, via the **Abel-Jacobi map** that sends a point $P \in E$ to the divisor class of $[P] - [\mathcal{O}]$ [Sil09, Proposition III.3.4], which also provides the Cartier self-duality $E\left[n\right] \cong \operatorname{Pic}_0\left(E/\overline{F}\right)\left[n\right] \cong E\left[n\right]^{\dagger}$ for any $n \in \mathbb{N}^+$ [Mum70, Theorem III.15.1]. This identification supplies an alternative group law on E, equivalent to the geometric group law by considering the non-zero rational **line function** $\mathrm{L}_{P,Q} \in \overline{F}\left(E\right)^{\times}$ joining the points $P, Q \in E$ with associated divisor

$$[\mathrm{L}_{P,Q}] = [P + Q] - [P] - [Q] + [\mathcal{O}].$$

Moreover, the identification also gives an exact sequence of abelian groups [Sil09, Remark III.3.5.1]

$$0 \to \overline{F}^{\times} \xrightarrow{\hookrightarrow} \overline{F}\left(E\right)^{\times} \xrightarrow{[-]} \operatorname{Div}_0\left(E/\overline{F}\right) \xrightarrow{\sum} E \cong \operatorname{Pic}_0\left(E/\overline{F}\right) \to 0,$$

where $\operatorname{Div}_0\left(E/\overline{F}\right)$ is the subgroup of degree zero divisors of $\operatorname{Div}\left(E/\overline{F}\right)$.

The notion of Weil divisors allows for the definition of certain morphisms arising from linear systems, which would first require the relevant divisors $D \in \operatorname{Div}\left(E/\overline{F}\right)$ to be **effective**, or $D \geq 0$, which says that all of its coefficients are non-negative. Then define the **complete linear system** of D by

$$\begin{aligned} \mathcal{L}\left(D\right) &\coloneqq \left\{D' \in \operatorname{Div}\left(E/\overline{F}\right) \;\middle|\; D' \geq 0,\ D' \sim D\right\} \\ &\cong \left\{f \in \overline{F}\left(E\right)^{\times} \;\middle|\; D + [f] \geq 0\right\} \cup \{0\}, \end{aligned}$$

which is a finite-dimensional $\overline{F}$-vector space of global sections [Sil09, Proposition II.5.2(b)]. The Riemann-Roch theorem computes its dimension to be $\dim_{\overline{F}} \mathcal{L}\left(D\right) = \deg D$ [Sil09, Proposition II.5.5(c)], and hence, after choosing a basis of global sections $f_i \in \mathcal{L}\left(D\right)$, there is a well-defined morphism abusively denoted

$$\begin{array}{rccc} \mathcal{L}\left(D\right) & : & E & \longrightarrow & \overline{F}^{\deg D} \\ & & Q & \longmapsto & \left(f_1\left(Q\right), \ldots, f_{\deg D}\left(Q\right)\right) \end{array}.$$

Since the valuation $\operatorname{ord}_Q f$ is normalised, the divisors of the basis functions remain unchanged upon scaling by elements of $\overline{F}^{\times}$, so further normalisation gives a projectivisation of the morphism, denoted

$$\begin{array}{rccc} \widehat{\mathcal{L}}\left(D\right) & : & E & \longrightarrow & \mathbb{P}^{\deg D - 1} \\ & & Q & \longmapsto & \left[f_1\left(Q\right) : \cdots : f_{\deg D}\left(Q\right)\right] \end{array}.$$

If two divisors $D, D' \in \mathrm{Div}\left(E/\overline{F}\right)$ are linearly equivalent, their complete linear systems $\mathcal{L}(D)$ and $\mathcal{L}(D')$ are isomorphic as $\overline{F}$-vector spaces [Sil09, Proposition II.5.2(c)], so their induced morphisms $\widehat{\mathcal{L}}(D)$ and $\widehat{\mathcal{L}}(D')$ are equal up to some projective transformation. This will be particularly relevant for the divisor $D = n[\mathcal{O}]$, for some fixed $n \in \mathbb{N}^+$, where the morphisms induced by the linear systems will simply be written as

$$\mathcal{L}_n \coloneqq \mathcal{L}(n[\mathcal{O}]) : E \to \overline{F}^n, \qquad \widehat{\mathcal{L}_n} \coloneqq \widehat{\mathcal{L}}(n[\mathcal{O}]) : E \to \mathbb{P}^{n-1}.$$

In fact, translating a general theorem of invertible sheaves [Har77, Theorem II.7.1] gives a unique projective transformation $\widehat{T_P} \in \mathrm{PGL}_n$ that only depends on the choice of $P \in E[n]$, where now $D \sim n[P]$, such that

$$\widehat{\mathcal{L}_n}(P+Q) = \widehat{T_P}\widehat{\mathcal{L}_n}(Q), \qquad Q \in E,$$

and conversely, if such an equality holds, then $D \sim n[P]$. Furthermore, lifting this matrix to GL_n through scaling also gives a linear transformation $T_P \in \mathrm{GL}_n$, which is unique only after fixing a basis of global sections chosen by fixing a non-zero rational function $f_P \in \overline{F}(E)^\times$ with associated divisor $[f_P] = n[P] - D$.

The language of Weil divisors also allows for the construction of a non-degenerate alternating $\mathbb{Z}$-bilinear pairing, whose image is an n-th root of unity, known as the **n-Weil pairing** [Sil09, Proposition III.8.1]

$$\mathrm{e}_n : E[n] \times E[n] \to \overline{F}^\times.$$

There are several definitions in the literature that are equivalent up to sign, one of which is outlined as follows [Sil09, Exercise 3.16]. To define $\mathrm{e}_n(P, P')$ for two points $P, P' \in E[n]$, first choose any two divisors

$$D \coloneqq \sum_{Q \in E} n_Q [Q] \in \mathrm{Div}\left(E/\overline{F}\right), \qquad D' \coloneqq \sum_{Q \in E} n'_Q [Q] \in \mathrm{Div}\left(E/\overline{F}\right),$$

satisfying $\deg D = \deg D' = 0$, and $\sum D = P$ and $\sum D' = P'$, with an extra **disjoint support** condition

$$\{Q \in E \mid n_Q \neq 0\} \cap \left\{Q \in E \;\middle|\; n'_Q \neq 0\right\} = \emptyset.$$

Then pick two non-zero rational functions $f, f' \in \overline{F}(E)^\times$ such that $[f] = nD$ and $[f'] = nD'$, and define

$$\mathrm{e}_n(P, P') \coloneqq \frac{f'(D)}{f(D')} \coloneqq \frac{\prod_{Q \in E} f'(Q)^{n_Q}}{\prod_{Q \in E} f(Q)^{n'_Q}},$$

which is indeed a well-defined finite product, independent of the choices of divisors and rational functions, and outputs an n-th root of unity. Perhaps more naturally, using the canonical identification $E \cong \mathrm{Pic}_0\left(E/\overline{F}\right)$, this transforms into a pairing of Picard groups with disjoint support

$$\begin{array}{rcccc} \widetilde{\mathrm{e}_n} & : & \mathrm{Pic}_0\left(E/\overline{F}\right)[n] \times \mathrm{Pic}_0\left(E/\overline{F}\right)[n] & \longrightarrow & \overline{F}^\times \\ & & (D, D') & \longmapsto & \dfrac{f'(D)}{f(D')} \end{array},$$

where $f, f' \in \overline{F}(E)^\times$ are the respective non-zero rational functions with associated divisors $[f] = nD$ and $[f'] = nD'$. With this formulation, the n-Weil pairing will be invariant after replacing D' with any linearly equivalent divisor $D'' \coloneqq D' + [g] \in \mathrm{Pic}_0\left(E/\overline{F}\right)$, for some non-zero rational function $g \in \overline{F}(E)^\times$. In particular, if $f'' \in \overline{F}(E)^\times$ is a non-zero rational function with associated divisor $[f''] = nD''$, then clearly $f'' = f'g^n$, and since Weil's reciprocity law [Sil09, Exercise 2.11] gives an equality $f([g]) = g([f]) = g^n(D)$,

$$\widetilde{\mathrm{e}_n}(D, D'') = \frac{f''(D)}{f(D'')} = \frac{f'(D)\, g^n(D)}{f(D')\, f([g])} = \frac{f'(D)}{f(D')} = \widetilde{\mathrm{e}_n}(D, D').$$

Thus the disjoint support condition can be relaxed, and it suffices to consider $D = [P] - [\mathcal{O}]$ and $D' = [P'] - [\mathcal{O}]$ by utilising the line function $\mathrm{L}_{P,Q} \in \overline{F}(E)^\times$, which coincides with the original definition of the pairing.

2.2.3 Selmer and Tate-Shafarevich groups

As hinted in the previous section, the primary application of Galois cohomology in this report will be to define and study fundamental invariants of elliptic curves and generally abelian varieties, namely the Selmer group and the Tate-Shafarevich group, which are the topics of this subsection. Fixing $n \in \mathbb{N}^+$, this begins by considering the short exact sequence of abelian groups induced by multiplication by n

$$0 \to E[n] \xrightarrow{\hookrightarrow} E \xrightarrow{[n]} E \to 0.$$

Applying Galois cohomology induces a long exact sequence of cohomology groups, which can be truncated at $\mathrm{H}^1(F, E[n])$ to establish a short exact **Kummer sequence** [Sil09, Sequence X.4(∗)]

$$0 \to E(F)/n \to \mathrm{H}^1(F, E[n]) \to \mathrm{H}^1(F, E)[n] \to 0.$$

Setting $F = K$ gives the global Kummer sequence, while setting $F = K_v$ for each place $v \in \mathcal{V}_K$ gives local Kummer sequences, and their individual groups are related by localisation maps induced by the natural inclusions $E\left(\overline{K}\right) \hookrightarrow E\left(\overline{K_v}\right)$ and $\mathrm{Gal}\left(\overline{K_v}/K_v\right) \hookrightarrow \mathrm{Gal}\left(\overline{K}/K\right)$. In particular, as discussed in the previous section, direct products of localisation maps of $\mathrm{H}^1(K, E[n])$ and $\mathrm{H}^1(K, E)$ have images landing in their respective first adelic cohomology groups. Likewise, the image of $E(K_v)$ in $\mathrm{H}^1(K_v, E[n])$ is unramified for any place $v \in \mathcal{V}_K$ except possibly those in the finite set

$$\mathcal{V}_K^\infty \cup \left\{ v \in \mathcal{V}_K^0 \;\middle|\; \widetilde{E}(\mathbb{F}_v) \text{ is singular} \right\} \cup \left\{ v \in \mathcal{V}_K^0 \;\middle|\; \mathrm{ord}_v\, n \neq 0 \right\},$$

where $\widetilde{E}(\mathbb{F}_v)$ denotes the reduction modulo v of the minimal Weierstrass equation for $E(K_v)$ [Sil09, Proposition VIII.2.1]. As such, the image of the zeroth adelic cohomology group, analogously denoted

$$E(\mathbb{A}_K) \coloneqq \prod_{v \in \mathcal{V}_K} E(K_v),$$

also lands in the first adelic cohomology group $\mathrm{H}^1(\mathbb{A}_K, E[n])$. Thus, combining the global and local Kummer sequences furnishes the crucial row-exact **Kummer diagram** [Sil09, Diagram X.4(∗∗)]

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/n & \xrightarrow{\alpha} & \mathrm{H}^1(K, E[n]) & \xrightarrow{\beta} & \mathrm{H}^1(K, E)[n] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \lambda} & \searrow^{\sigma} & \downarrow{\scriptstyle \tau} & & \\ 0 & \longrightarrow & E(\mathbb{A}_K)/n & \xrightarrow[\kappa]{} & \mathrm{H}^1(\mathbb{A}_K, E[n]) & \xrightarrow[\mu]{} & \mathrm{H}^1(\mathbb{A}_K, E)[n] & \longrightarrow & 0 \end{array},$$

where σ is the composition in either direction.

In the spirit of the weak Mordell-Weil theorem, it would be ideal if $\mathrm{H}^1(K, E[n])$ were finite, so that proving the finiteness of $E(K)/n$ would reduce to its finiteness, yet this is usually not the case. Rather, the usual proof considers a subgroup of $\mathrm{H}^1(K, E[n])$ containing $E(K)/n$ that is provably finite [Sil09, Theorem X.4.2(b)] and effectively computable [Sil09, Remark X.4.5]. This is the role played by the **n-Selmer group**

$$\mathcal{S}_n(K, E) \coloneqq \ker\left(\sigma : \mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(\mathbb{A}_K, E)[n]\right),$$

as determining the local images of $\operatorname{im}\kappa$ can be done via Hensel's lemma in contrast to the difficulty of the global image $\operatorname{im}\alpha$. On one hand, this contains the familiar first Tate-Shafarevich subgroup $Ш^1(K, E[n]) = \ker\lambda$, and by the first isomorphism theorem, their quotient can be characterised as an intersection

$$\mathcal{S}_n(K, E)/Ш^1(K, E[n]) = \ker(\mu \circ \lambda)/\ker\lambda \xrightarrow{\sim} \lambda(\ker(\mu \circ \lambda)) = \ker\mu \cap \operatorname{im}\lambda = \operatorname{im}\kappa \cap \operatorname{im}\lambda.$$

On the other hand, the classical **Tate-Shafarevich group** of an elliptic curve is defined to be

$$Ш(K, E) \coloneqq \ker\left(\mathrm{H}^1(K, E) \to \mathrm{H}^1(\mathbb{A}_K, E)\right),$$

so that $Ш(K, E)[n] = \ker\tau$, and an application of the snake lemma to the Kummer diagram yields a famous short exact sequence of abelian groups [Sil09, Theorem X.4.2(a)]

$$0 \to E(K) \otimes \mathbb{Z}/n \xrightarrow{\alpha} \mathcal{S}_n(K, E) \xrightarrow{\beta} Ш(K, E)[n] \to 0,$$

noting that $E(K)/n \cong E(K) \otimes \mathbb{Z}/n$. This result is fundamental, and implies the finiteness of both $E(K)/n$ and $Ш(K, E)[n]$, although patching up over all $n \in \mathbb{N}$ to produce $Ш(K, E)$ guarantees nothing and is exactly the content of the **Tate-Shafarevich conjecture** [Sil09, Conjecture X.4.13].

2.2.4 Twists and torsors

The abstract algebraic definitions of the Selmer group and the Tate-Shafarevich group can be interpreted geometrically as certain sets of twists of E. For a general definition, if V is a quasi-projective variety defined over F, then an **F-twist** of V is a quasi-projective variety C defined over F that is isomorphic to V, and two F-twists are considered equivalent if they are F-isomorphic. The set of all such twists is denoted

$$\mathrm{Twist}\,(V/F) \coloneqq \{F\text{-twists of } V\}\,.$$

Note that these are F-isomorphism classes of $\overline{F}$-isomorphisms, but the fact that they are equivalence classes will be implicit, and isomorphisms over $\overline{F}$ are just referred to as isomorphisms, as previously remarked. A general **twisting principle** in Galois descent says that the F-twists of V exactly parameterise the 1-cocycles of $\mathrm{H}^1\,(F, \mathrm{Aut}\,V)$ [Ser80, Proposition X.4], so there is a bijective correspondence of pointed sets

$$\mathrm{Twist}\,(V/F) \quad \leftrightsquigarrow \quad \mathrm{H}^1\,(F, \mathrm{Aut}\,V)\,,$$

where $\mathrm{Aut}\,V$ is the group of automorphisms of V. By this interpretation, the presence of non-trivial 1-cocycles measures the failure of these isomorphisms to be definable over F.

As a preliminary example, consider the group of automorphisms PGL_n of $\mathbb{P}^{n-1}$ for a fixed $n \in \mathbb{N}^+$. Applying the twisting principle to the pointed set $\mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right)$, conventionally called **F-Brauer-Severi varieties** of dimension n, gives a bijective correspondence of pointed sets [Ser80, Section X.6]

$$\begin{array}{rcl} \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right) & \leftrightsquigarrow & \mathrm{H}^1\,(F, \mathrm{PGL}_n) \\ C & \longmapsto & \left(\sigma \mapsto \sigma \cdot \phi_C \circ \phi_C^{-1}\right) \end{array}\,,$$

where $\phi_C : C \xrightarrow{\sim} \mathbb{P}^{n-1}$ is the automorphism encoded in the data of C that relates C and $\mathbb{P}^{n-1}$. Note that the dimension here, in contrast to the convention in literature, is defined to be one higher than the dimension of the overarching projective space, for convenience purposes later. Then an F-Brauer-Severi variety $C \in \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right)$ corresponds to the trivial class in $\mathrm{H}^1\,(F, \mathrm{PGL}_n)$ if and only if $C\,(F) \neq \emptyset$.

The twisting principle for E is also a bijective correspondence of pointed sets [Sil09, Theorem X.2.2]

$$\begin{array}{rcl} \mathrm{Twist}\,(E/F) & \leftrightsquigarrow & \mathrm{H}^1\,(F, \mathrm{Aut}\,E) \\ C & \longmapsto & \left(\sigma \mapsto \sigma \cdot \phi_C \circ \phi_C^{-1}\right) \end{array}\,,$$

where $\phi_C : C \xrightarrow{\sim} E$ denotes the automorphism relating C and E. Note that $\mathrm{Aut}\,E$ refers to the group of automorphisms of E as a quasi-projective variety, ignoring its group structure.

When the group structure of E is brought into the picture, a certain twist emerges by respecting actions of E on its twists. In particular, an **F-torsor** for E is an F-twist C of E equipped with a regular E-action, which are identified up to E-equivariant F-isomorphisms, forming the **Weil-Châtelet pointed set**

$$\mathrm{WC}\,(E/F) \coloneqq \{F\text{-torsors for } E\}\,,$$

where the trivial F-torsor exactly consists of E and its self-translations. Note that in common literature, the twisting is implicit and arises only after fixing an initial point $p_C \in C$ and mapping it to $\mathcal{O} \in E$, which produces an isomorphism $C \xrightarrow{\sim} E$ by relaying the group operations of E onto C [Sil09, Proposition X.3.2]. By the twisting principle, there is again a bijective correspondence of pointed sets [Sil09, Theorem X.3.6]

$$\begin{array}{rcl} \mathrm{WC}\,(E/F) & \leftrightsquigarrow & \mathrm{H}^1\,(F, E) \\ C & \longmapsto & (\sigma \mapsto \sigma \cdot p_C - p_C) \end{array}\,,$$

which also furnishes a group structure on $\mathrm{WC}\,(E/F)$. Then an F-torsor $C \in \mathrm{WC}\,(E/F)$ corresponds to the trivial class in $\mathrm{H}^1\,(F, E)$ if and only if $C\,(F) \neq \emptyset$ [Sil09, Proposition X.3.3]. By this interpretation, there is again a diagonal restriction map $\mathrm{WC}\,(E/K) \to \prod_{v \in \mathcal{V}_K} \mathrm{WC}\,(E/K_v)$ with kernel exactly the Tate-Shafarevich group $Ш\,(K, E)$. Thus $Ш\,(K, E)$ measures the failure of the **Hasse principle** in $\mathrm{WC}\,(E/K)$, namely the presence of K-torsor curves with K_v-rational points at every place $v \in \mathcal{V}_K$ but with no K-rational points. One may similarly interpret the n-Selmer group $\mathcal{S}_n\,(K, E)$ by parameterising 1-cocycles of $\mathrm{H}^1\,(K, E\,[n])$ in terms of K-torsors for $E\,[n]$ in some Weil-Châtelet group, but this is omitted for an alternative later.

2.2.5 Arithmetic duality theorems

As the overall theme of this report revolves around arithmetic duality, this final subsection reiterates the relevant consequences of Tate's local and global dualities for general abelian varieties, translated to the case of elliptic curves defined over general fields of characteristic zero. As a start, due the self-duality of the $\mathrm{Gal}\left(\overline{F}/F\right)$-module $E\left[n\right] \cong E\left[n\right]^{\dagger}$ for any $n \in \mathbb{N}^{+}$, when $F = K_v$ for a place $v \in \mathcal{V}_K$, Tate's local duality simplifies to a natural Pontryagin duality between finite groups

$$\mathrm{H}^1\left(K_v, E\left[n\right]\right) \cong \mathrm{H}^1\left(K_v, E\left[n\right]\right)^{\star}.$$

Similarly, when $F = K$, Tate's global duality simplifies to natural Pontryagin dualities between finite groups

$$Ш^1\left(K, E\left[n\right]\right) \cong Ш^2\left(K, E\left[n\right]\right)^{\star}, \qquad Ш^2\left(K, E\left[n\right]\right) \cong Ш^1\left(K, E\left[n\right]\right)^{\star},$$

and the middle terms of the Poitou-Tate exact sequence become

$$\cdots \to \mathrm{H}^1\left(K, E\left[n\right]\right) \xrightarrow{\tau^1} \mathrm{H}^1\left(\mathbb{A}_K, E\left[n\right]\right) \cong \mathrm{H}^1\left(\mathbb{A}_K, E\left[n\right]\right)^{\star} \xrightarrow{\sigma^1} \mathrm{H}^1\left(K, E\left[n\right]\right)^{\star} \to \ldots.$$

On the other hand, the $\mathrm{Gal}\left(\overline{F}/F\right)$-module $E \cong \mathrm{Pic}_0\left(E/\overline{F}\right)$, while self-dual as an abelian variety, is not finite, so the statements of arithmetic duality are formulated slightly differently. When $F = K_v$ for a place $v \in \mathcal{V}_K$, Tate's local duality establishes a canonical non-degenerate perfect pairing [Mil06, Corollary I.3.4]

$$\mathrm{H}^n\left(K_v, E\right) \times \mathrm{H}^{1-n}\left(K_v, E\right) \to \mathrm{Br}\, K_v, \qquad n = 0, 1,$$

which again induces natural Pontryagin dualities

$$\mathrm{H}^0\left(K_v, E\right) \cong \mathrm{H}^1\left(K_v, E\right)^{\star}, \qquad \mathrm{H}^1\left(K_v, E\right) \cong \mathrm{H}^0\left(K_v, E\right)^{\star},$$

between compact groups and discrete groups respectively. While the non-archimedean case has the expected identifications $\mathrm{Br}\, K_v \cong \mathbb{Q}/\mathbb{Z}$ and $\mathrm{H}^0\left(K_v, E\right) = E\left(K_v\right)$, the archimedean case uses the aforementioned convention of the zeroth Tate cohomology group [Mil06, Remark I.3.7], and the resulting dualities become

$$\pi_0\left(E\left(K_v\right)\right) \cong \mathrm{H}^1\left(K_v, E\right)^{\star}, \qquad \mathrm{H}^1\left(K_v, E\right) \cong \pi_0\left(E\left(K_v\right)\right)^{\star},$$

where π_0 is the group functor describing the number of connected components. In particular, $\pi_0\left(E\left(\mathbb{C}\right)\right)$ is clearly always trivial, while $\pi_0\left(E\left(\mathbb{R}\right)\right)$ is trivial when $E\left(\mathbb{R}\right)$ is connected and $\mathbb{Z}/2$ otherwise. When $F = K$, there is also a formulation of Tate's global duality [Mil06, Theorem I.6.13] in terms of a canonical non-degenerate alternating $\mathbb{Z}$-bilinear pairing, known as the **Cassels-Tate pairing**

$$Ш\left(K, E\right) \times Ш\left(K, E\right) \to \mathbb{Q}/\mathbb{Z}.$$

Assuming the Tate-Shafarevich conjecture, it follows that $Ш\left(K, E\right)$ and any of its p-primary components have orders perfect squares [Sil09, Theorem X.4.14]. There is also a ten-term version of the Poitou-Tate exact sequence [Mil06, Remark I.6.14], but both of these will not be used and will be elided for brevity.

Chapter 3

Modelling Selmer groups

This chapter will be dedicated to understanding and modelling the behaviour of Selmer groups across all elliptic curves defined over number fields. The first short section will provide basic definitions of quadratic modules and what it means to be a Lagrangian submodule of a metabolic quadratic module. The second section will prove, using arithmetic duality, that a Selmer group is naturally an intersection of two Lagrangian direct summands in a metabolic quadratic module of infinite rank. The third section will suggest a finite combinatorial construction mimicking this exact property, which induces a probabilistic distribution of orders of p^e-Selmer groups with average equal to the sum of divisors of a prime power $p^e \in \mathbb{N}^+$.

3.1 Quadratic modules

The elementary theory of quadratic forms is pervasive in algebra, geometry, and number theory alike. Yet, the common literature primarily considers the theory over finite fields, while much can also be said about the theory over other non-integral domains like $\mathbb{Z}/n$ for any $n \in \mathbb{N}^+$, as well as those quadratic forms taking values in an abelian group like $\mathbb{Q}/\mathbb{Z}$, which will be relevant to later discussions. Some of these definitions are non-standard, and will follow the convention of the paper on random maximal isotropic subspaces by Poonen and Rains [PR12]. Throughout this section, let R be a ring, and let M be an R-module.

3.1.1 Definitions

The following are several relevant definitions in the modified theory of quadratic forms over R-modules, noting the explicit distinction between maps of R-modules and maps of abelian groups.

Definition. A map $\omega_M : M \to \mathbb{Q}/\mathbb{Z}$ is **quadratic** if it has an induced symmetric $\mathbb{Z}$-bilinear pairing

$$\begin{array}{rccc} \langle -,- \rangle_M & : & M \times M & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & & (x,y) & \longmapsto & \omega_M(x+y) - \omega_M(x) - \omega_M(y) \end{array},$$

and **even** if $\omega_M = \omega_M \circ (-1)$. A **quadratic form** is simply an even quadratic map, and a **quadratic R-module** is an R-module equipped with a quadratic form.

Remark. The standard convention requires quadratic forms $\omega_M : M \to \mathbb{Q}/\mathbb{Z}$ to satisfy $\omega_M \circ n = n^2 \circ \omega_M$ for all $n \in \mathbb{N}^+$, but this is an immediate consequence of being even and quadratic [PR12, Remark 2.1].

Definition. A submodule N of a quadratic R-module M is **totally isotropic** if $\omega_M(N) = 0$, and **maximal** if it is equal to its **orthogonal complement**

$$\begin{aligned} N^\perp &\coloneqq \{x \in M \mid \forall y \in N,\ \langle x,y \rangle_M = 0\} \\ &= \{x \in M \mid \forall y \in N,\ \omega_M(x+y) = \omega_M(x) + \omega_M(y)\}. \end{aligned}$$

A **Lagrangian** submodule is simply a maximal totally isotropic submodule.

Remark. Total isotropy gives an obvious containment $N \subseteq N^\perp$, so that maximality makes semantic sense, otherwise these conditions are non-vacuous and independent of each other in general [PR12, Remark 2.3].

Definition. A quadratic R-module M is **non-degenerate** if $\langle -, - \rangle_M$ is a perfect pairing of abelian groups, or equivalently that the natural map from M to its Pontryagin dual $M^\star$ given by

$$\begin{array}{ccc} M & \longrightarrow & M^\star \\ x & \longmapsto & (y \mapsto \langle x, y \rangle_M) \end{array}$$

is an isomorphism of abelian groups. A quadratic R-module is **weakly metabolic** if it is non-degenerate and contains a Lagrangian submodule, and just **metabolic** if this submodule is also a direct summand.

Remark. The alternative convention requires that M is finite or at least locally compact, so that a nice topology can be equipped on it [PR12, Definition 2.13], but this requirement will be elided for simplicity.

3.1.2 Examples

There will be two primary examples relevant for each of the following two sections. The first example showcases a common quadratic R-module of finite rank, which will be used heavily in the final section.

Example. If R embeds into $\mathbb{Q}/\mathbb{Z}$, then the free R-module R^{2n} for some $n \in \mathbb{N}^+$, equipped with the **standard hyperbolic quadratic form**

$$\begin{array}{rccc} \omega_{R^{2n}} \quad : & R^{2n} & \longrightarrow & R \hookrightarrow \mathbb{Q}/\mathbb{Z} \\ & (x_1, \ldots, x_n, y_1, \ldots, y_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} x_i y_i \end{array} ,$$

is a quadratic R-module of finite rank, called the **standard hyperbolic R-module** of rank $2n$, which is metabolic with a Lagrangian direct summand $R^n \oplus 0^n$.

This example will be considered in the last section on the finite local rings $R = \mathbb{F}_p$ and $R = \mathbb{Z}/p^e$ for some prime power $p^e \in \mathbb{N}^+$, where R embeds into $\mathbb{Q}/\mathbb{Z}$ via the identifications $\mathbb{F}_p \cong (1/p)\,\mathbb{Z}/\mathbb{Z}$ and $\mathbb{Z}/p^e \cong (1/p^e)\,\mathbb{Z}/\mathbb{Z}$ respectively. Here, direct summands of free R-modules of finite rank, or equivalently projective R-modules of finite free rank, are finitely generated. Having the additional condition of locality, by Nakayama's lemma, ensures that direct summands of free R-modules of finite rank are also free.

Remark. The requirement of projectivity here allows for free direct summands to behave somewhat like vector subspaces over fields, whereas mere submodules are not necessarily free unless the ring is at least a principal ideal domain. By a general classification result [PR12, Remark 2.20], quadratic R-modules over a local ring R can be completely classified up to **isometries**, isomorphisms of R-modules that preserve their respective quadratic forms. For instance, any metabolic quadratic R-module has even rank, and is isometric to the standard hyperbolic R-module of the same rank with the exception of rings where $2 \notin R^\times$. This is almost true for rings where $2 \notin R^\times$, up to a non-invertible matrix defining the quadratic form.

The second example illustrates one where the above freeness argument does not immediately apply.

Example. If $(M_i)_{i \in I}$ are weakly metabolic quadratic R-modules with respective Lagrangian submodules $(N_i)_{i \in I}$ for some indexing set I, then the restricted product of $(M_i)_{i \in I}$ with respect to $(N_i)_{i \in I}$,

$$M \coloneqq \left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i \;\middle|\; x_i \in N_i \text{ for all but finitely many } i \in I \right\},$$

equipped with the quadratic form

$$\begin{array}{rccc} \omega_M \quad : & M & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & (x_i)_{i \in I} & \longmapsto & \displaystyle\sum_{i \in I} \omega_{M_i}(x_i) \end{array} ,$$

a finite sum by total isotropy of each N_i, is a quadratic R-module of infinite rank, which is also weakly metabolic with a Lagrangian submodule $\prod_{i \in I} N_i$.

An explicit example of this will be given in the following section on the finite ring $R = \mathbb{Z}/n$ for some $n \in \mathbb{N}^+$, which can again be decomposed into finite local rings $R = \mathbb{Z}/p^e$ by the Chinese remainder theorem.

Remark. By **Kaplansky's theorem**, projective modules over local rings are free even without finite generation [Kap58, Theorem 2], so the above freeness argument still applies, but this fact will not be used.

3.2 Arithmetic of Selmer groups

The behaviour of the Mordell-Weil group of an elliptic curve E over a number field K, and hence its Mordell-Weil rank, is largely governed by the behaviour of the n-Selmer group $\mathcal{S}_n(K,E)$ for all $n \in \mathbb{N}^+$, and a thorough understanding of its arithmetic will be the topic of this core section. As previously outlined, the n-Selmer group is constructed as the kernel of the localisation map λ in the Kummer diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/n & \xrightarrow{\alpha} & \mathrm{H}^1(K, E[n]) & \xrightarrow{\beta} & \mathrm{H}^1(K,E)[n] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \lambda} & \searrow^{\sigma} & \downarrow{\scriptstyle \tau} & & \\ 0 & \longrightarrow & E(\mathbb{A}_K)/n & \xrightarrow[\kappa]{} & \mathrm{H}^1(\mathbb{A}_K, E[n]) & \xrightarrow[\mu]{} & \mathrm{H}^1(\mathbb{A}_K, E)[n] & \longrightarrow & 0 \end{array},$$

while the first isomorphism theorem characterises the quotient $\mathcal{S}_n(K,E)/Ш^1(K,E[n])$ as the intersection of the images of κ and λ inside $\mathrm{H}^1(\mathbb{A}_K, E[n])$. It turns out that $\mathrm{H}^1(\mathbb{A}_K, E[n])$ is a weakly metabolic quadratic $\mathbb{Z}/n$-module of infinite rank, with Lagrangian submodules $\operatorname{im}\kappa$ and $\operatorname{im}\lambda$ lying within it. More importantly, it can be further shown that these submodules are often direct summands of the ambient module, in a rigorous sense, and that $Ш^1(K,E[p^e])$ vanishes often when $p^e \in \mathbb{N}^+$ is a prime power, so that the desired characterisation of $\mathcal{S}_{p^e}(K,E)$ is achieved. Thus the aim of this section is to prove the following result.

(3.2.1) **Theorem.** *For almost all elliptic curves $E \in \mathcal{E}(K)$, there is an isomorphism of abelian groups*

$$\mathcal{S}_{p^e}(K,E) \xrightarrow{\sim} L_1 \cap L_2,$$

where L_1 and L_2 are Lagrangian direct summands of a metabolic quadratic $\mathbb{Z}/p^e$-module of infinite rank.

Remark. The same result is already known albeit in a more limited context, namely the case for $p^e = 2$ and where the ambient module is a finite-dimensional $\mathbb{F}_2$-vector space [CSS98, Proposition 1.2.1].

The statement as phrased encompasses several parts whose proofs are all rather involved, so these will be split accordingly in the following five subsections, and are summarised as follows for reference.

Proof of Theorem 3.2.1. In light of the above elucidation, set $L_1 \coloneqq \operatorname{im}\kappa$ and $L_2 \coloneqq \operatorname{im}\lambda$ in the ambient module $\mathrm{H}^1(\mathbb{A}_K, E[n])$, which has infinitely many generators, even considering its relations, to account for all places. By first defining theta groups, its local components is equipped with a map of pointed sets $\mathrm{H}^1(K_v, E[n]) \to \mathbb{Q}/\mathbb{Z}$, which is a quadratic form by Corollary 3.2.5 and Proposition 3.2.6, and its non-degeneracy is verified using Tate's local duality in Corollary 3.2.7. By proving basic properties of Brauer-Severi diagrams, Proposition 3.2.11 and Proposition 3.2.12 show that the local components of L_1 are Lagrangian, and as a consequence, the ambient non-degenerate quadratic $\mathbb{Z}/n$-module $\mathrm{H}^1(\mathbb{A}_K, E[n])$ is well-defined by Corollary 3.2.13. The fact that L_1 and L_2 are Lagrangian follows soon after in Corollary 3.2.14 and Proposition 3.2.15, hence establishing weak metabolicity. In the specific case of $n = p^e$, a long-winded algebraic computation yields the triviality of $Ш^1(K,E[p^e])$ by introducing the criterion $\mathrm{SL}_2(\mathbb{Z}/p^e) \leq \operatorname{im}\rho_{E[p^e]}$, as summarised in Corollary 3.2.25. Strong metabolicity is established by proving that L_1 is a direct summand in Corollary 3.2.28, while the same holds for L_2 under the criterion, as in Proposition 3.2.32. Finally, the density of elliptic curves satisfying this criterion is justified in Proposition 3.2.35. □

Throughout this section, fix the notation of the relevant groups and homomorphisms as in the above Kummer diagram, and when the field of definition is irrelevant to an argument, consider the same elliptic curve E but defined over a general field F of characteristic zero.

3.2.1 Non-degeneracy of the local quadratic module

This subsection begins the proof by equipping the first local cohomology group $\mathrm{H}^1(K_v, E[n])$ with a well-defined quadratic form, making it a quadratic $\mathbb{Z}/n$-module, and verifying its non-degeneracy as an application of arithmetic duality. The proof primarily follows the arguments in the paper on random maximal isotropic subspaces by Poonen and Rains [PR12], noting the sign differences commonly disregarded in arithmetic duality, but with a short exposition of theta groups that was elided in their paper for a reference to Mumford's book on abelian varieties [Mum70]. To begin, consider the following purely algebraic result of homological algebra taken from Zarhin's paper on non-commutative cohomologies and Mumford groups [Zar74].

Let A and C be abelian groups, and let B be a central extension of C by A, such that

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is an exact sequence of groups. Let $c_1, c_2 \in C$ be elements. Since β is surjective, $c_1 = \beta(b_1)$ and $c_2 = \beta(b_2)$ for some elements $b_1, b_2 \in B$. Since C is abelian by assumption, the commutator $[b_1, b_2] \in B$ maps to the trivial element in C through β, so $[b_1, b_2] \in \ker\beta = \operatorname{im}\alpha$, and hence $[b_1, b_2] = \alpha(a)$ for some element $a \in A$. Now let G be a group acting on A, B, and C, and define a lifted commutator pairing by

$$\begin{array}{rccc} [-,-] & : & C \times C & \longrightarrow & A \\ & & (c_1, c_2) & \longmapsto & a \end{array}.$$

Applying non-abelian group cohomology and the universal property of tensor products, this induces an alternating $\mathbb{Z}$-bilinear commutator pairing $[-,-] : \mathrm{H}^2(G, C \otimes C) \to \mathrm{H}^2(G, A)$.

(3.2.2) **Lemma.** *There is a commutative triangle of pointed sets*

$$\begin{array}{ccc} \mathrm{H}^2(G, C \otimes C) & \xrightarrow{[-,-]} & \mathrm{H}^2(G, A) \\ \cup\uparrow & \nearrow_{(\xi_1,\xi_2)\mapsto\delta_1(\xi_1+\xi_2)-\delta_1(\xi_1)-\delta_1(\xi_2)} & \\ \mathrm{H}^1(G, C) \times \mathrm{H}^1(G, C) & & \end{array},$$

where δ_1 is the second connecting map between pointed sets.

Proof. This is an explicit computation with 1-cocycles. Let $\xi_1, \xi_2 \in \mathrm{H}^1(G, C)$ be 1-cocycles, and let $\sigma, \tau \in G$ be group elements. The construction of δ_1 gives elements $b^1_\sigma, b^1_\tau, b^1_{\sigma\tau}, b^2_\sigma, b^2_\tau, b^2_{\sigma\tau} \in B$ such that

$$\beta\left(b^i_g\right) = \xi_i(g), \qquad g \in \{\sigma, \tau, \sigma\tau\}, \qquad i \in \{1, 2\}.$$

Letting $b_g \coloneqq b^2_g + b^1_g \in B$ for $g \in \{\sigma, \tau, \sigma\tau\}$ yields

$$\beta(b_g) = \beta\left(b^2_g + b^1_g\right) = \beta\left(b^2_g\right) + \beta\left(b^1_g\right) = \beta\left(b^1_g\right) + \beta\left(b^2_g\right) = \xi_1(g) + \xi_2(g) = (\xi_1 + \xi_2)(g), \qquad g \in \{\sigma, \tau, \sigma\tau\}.$$

By the definition of the cup product,

$$(\xi_1 \cup \xi_2)(\sigma, \tau) = \xi_1(\sigma) \otimes \sigma \cdot \xi_2(\tau) = \beta\left(b^1_\sigma\right) \otimes \sigma \cdot \beta\left(b^2_\tau\right) = \beta\left(b^1_\sigma\right) \otimes \beta\left(\sigma \cdot b^2_\tau\right),$$

so that $[\xi_1, \xi_2](\sigma, \tau) = a$ for some element $a \in A$ such that

$$\alpha(a) = \left[b^1_\sigma, \sigma \cdot b^2_\tau\right] = b^1_\sigma + \sigma \cdot b^2_\tau - b^1_\sigma - \sigma \cdot b^2_\tau.$$

The construction of δ_1 again gives elements $a^1_{\sigma,\tau}, a^2_{\sigma,\tau} \in A$ such that

$$\alpha\left(a^1_{\sigma,\tau}\right) = b^1_\sigma + \sigma \cdot b^1_\tau - b^1_{\sigma\tau}, \qquad \alpha\left(a^2_{\sigma,\tau}\right) = b^2_\sigma + \sigma \cdot b^2_\tau - b^2_{\sigma\tau} = -b^2_{\sigma\tau} + b^2_\sigma + \sigma \cdot b^2_\tau,$$

so that $\delta_1(\xi_1)(\sigma, \tau) = a^1_{\sigma,\tau}$ and $\delta_1(\xi_2)(\sigma, \tau) = a^2_{\sigma,\tau}$, as well as an element $a_{\sigma,\tau} \in A$ such that

$$\alpha(a_{\sigma,\tau}) = b_\sigma + \sigma \cdot b_\tau - b_{\sigma\tau} = b^2_\sigma + b^1_\sigma + \sigma \cdot b^2_\tau + \sigma \cdot b^1_\tau - b^1_{\sigma\tau} - b^2_{\sigma\tau} = -b^2_{\sigma\tau} + b^2_\sigma + b^1_\sigma + \sigma \cdot b^2_\tau + \sigma \cdot b^1_\tau - b^1_{\sigma\tau},$$

so that $\delta_1(\xi_1 + \xi_2)(\sigma, \tau) = a_{\sigma,\tau}$. A short computation yields

$$\begin{aligned} \alpha\left(a_{\sigma,\tau} - a^1_{\sigma,\tau} - a^2_{\sigma,\tau}\right) &= \alpha(a_{\sigma,\tau}) - \alpha\left(a^1_{\sigma,\tau}\right) - \alpha\left(a^2_{\sigma,\tau}\right) \\ &= -b^2_{\sigma\tau} + b^2_\sigma + b^1_\sigma + \sigma \cdot b^2_\tau + \sigma \cdot b^1_\tau - b^1_{\sigma\tau} + b^1_{\sigma\tau} - \sigma \cdot b^1_\tau - b^1_\sigma - \sigma \cdot b^2_\tau - b^2_\sigma + b^2_{\sigma\tau} \\ &= b^1_\sigma + \sigma \cdot b^2_\tau - b^1_\sigma - \sigma \cdot b^2_\tau \\ &= \alpha(a). \end{aligned}$$

The result follows by the verification

$$[\xi_1, \xi_2](\sigma, \tau) = a = a_{\sigma,\tau} - a^1_{\sigma,\tau} - a^2_{\sigma,\tau} = \delta_1(\xi_1 + \xi_2)(\sigma, \tau) - \delta_1(\xi_1)(\sigma, \tau) - \delta_1(\xi_2)(\sigma, \tau),$$

since α is injective. □

Considering $G = \mathrm{Gal}\left(\overline{F}/F\right)$ and setting $A = \overline{F}^{\times}$ and $C = E[n]$, the quadratic behaviour of $\mathrm{H}^1(F, E[n])$ is perhaps evident from the diagram in Lemma 3.2.2, but the construction entails defining the central extension B, which will require defining the notion of a theta group.

Definition. An **F-theta group** of level n for E is a central extension of $E(F)[n]$ by $F^{\times}$ such that its induced commutator pairing $E(F)[n] \times E(F)[n] \to F^{\times}$ coincides with the n-Weil pairing.

While the general theory of theta groups in terms of invertible sheaves is extensively covered in the literature, for the purposes of defining the quadratic form in the remainder of this subsection, it suffices to provide an explicit construction of a specific theta group. Consider the set

$$\Theta \coloneqq \left\{ (P, f_P) \in E[n] \times \overline{F}(E)^{\times} \;\middle|\; [f_P] = n[P] - n[\mathcal{O}] \right\},$$

equipped with operations $(P, f_P) \cdot (P', f_{P'}) \coloneqq (P + P', f_{P+P'})$ and $(P, f_P)^{-1} \coloneqq (-P, f_{-P})$, where

$$f_{P+P'} \coloneqq f_P \cdot \tau_P^* f_{P'}, \qquad f_{-P} \coloneqq \frac{1}{\tau_{-P}^* f_P},$$

and a distinguished identity $(\mathcal{O}, x) \in \Theta$ for any $x \in \overline{F}^{\times}$. Additionally, write $\Theta(F)$ to denote the same set, but each instance of $\overline{F}$ is replaced by F, which is exactly the set of $\mathrm{Gal}\left(\overline{F}/F\right)$-invariant elements.

Remark. In terms of line bundles, Θ is a group scheme over F [Mum70, Section IV.23], so the notation expressing its F-rational points $\Theta(F)$, as well as that of the cohomology group $\mathrm{H}^1(F, \Theta)$, make sense.

A priori, Θ is only a pointed set, but its group axioms can be verified by manifesting it as a fibre product.

(3.2.3) **Proposition.** *There is a row-exact diagram of groups*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \overline{F}^{\times} & \xrightarrow{\alpha} & \Theta & \xrightarrow{\beta} & E[n] & \longrightarrow & 0 \\
 & & \Big\uparrow{\scriptstyle =} & & \Big\downarrow{\scriptstyle \zeta} & & \Big\downarrow{\scriptstyle \epsilon} & & \\
0 & \longrightarrow & \overline{F}^{\times} & \xrightarrow[\gamma]{} & \mathrm{GL}_n & \xrightarrow[\delta]{} & \mathrm{PGL}_n & \longrightarrow & 0
\end{array}.$$

Proof. Let $P, P' \in E[n]$ be points in general position, and let $f_P, f_{P'} \in \overline{F}(E)^{\times}$ be their associated non-zero rational functions in Θ. The fact that Θ is a group can be checked with the easy computation $[\tau_P^* f_{P'}] = n[P + P'] - n[P]$, where the group operations are well-defined from verifying that

$$[f_{P+P'}] = n[P + P'] - n[\mathcal{O}], \qquad [f_{-P}] = n[-P] - n[\mathcal{O}],$$

while the group axioms follow from expanding divisor terms and using the commutativity of $E[n]$. Now define the inclusion map α and the projection map β in the obvious way, and define the maps γ and δ using the identification $\mathrm{PGL}_n \cong \mathrm{GL}_n / \overline{F}^{\times}$. Then the translation map $\tau_P : E \to E$ extends to a unique projective transformation $\widehat{T_P} \in \mathrm{PGL}_n$ via the linear system $\widehat{\mathcal{L}_n} : E \to \mathbb{P}^{n-1}$ such that the square

$$\begin{array}{ccc}
E & \xrightarrow{\widehat{\mathcal{L}_n}} & \mathbb{P}^{n-1} \\
{\scriptstyle \tau_P}\downarrow{\scriptstyle \sim} & & {\scriptstyle \sim}\downarrow{\scriptstyle \widehat{T_P}} \\
E & \xrightarrow[\widehat{\mathcal{L}_n}]{} & \mathbb{P}^{n-1}
\end{array}, \qquad
\begin{array}{ccc}
Q & \longmapsto & \widehat{\mathcal{L}_n}(Q) \\
\downarrow & & \downarrow \\
P + Q & \mapsto \widehat{\mathcal{L}_n}(P + Q) & \overset{=}{\leftrightarrow} \widehat{T_P}\widehat{\mathcal{L}_n}(Q)
\end{array}$$

commutes, so this equates to the existence of a well-defined homomorphism ϵ. Likewise, lifting $\widehat{T_P} \in \mathrm{PGL}_n$ to a linear transformation $T_P \in \mathrm{GL}_n$ via the linear system $\mathcal{L}_n : E \to \overline{F}^n$ is unique up to a choice of a non-zero rational function $f_P \in \overline{F}(E)^{\times}$. This is conveniently supplied by the second component of Θ, so this establishes a well-defined map ζ, which is also a homomorphism by construction. Finally, the commutativity of the left square follows from the fact that $T_{\mathcal{O}} \in \mathrm{GL}_n$ is the identity matrix scaled by a non-zero constant, while the commutativity of the right square follows by the construction of ϵ and ζ. □

It remains to prove that the induced commutator pairing coincides with the Weil pairing, after which the centrality of the group extension follows immediately, so that Θ is an $\overline{F}$-theta group of level n for E.

(3.2.4) **Proposition.** *The commutator $[-,-]:\Theta\times\Theta\to\Theta$ induces a pairing that coincides exactly with the n-Weil pairing $\mathrm{e}_n : E[n]\times E[n]\to\overline{F}^{\times}$. That is,*

$$[x,y]=\alpha\left(\mathrm{e}_n\left(\beta(x),\beta(y)\right)\right),\qquad x,y\in\Theta.$$

Proof. Let $P,P'\in E[n]$ be points in general position, and let $f_P, f_{P'}\in\overline{F}(E)^{\times}$ be their associated non-zero rational functions in Θ. The commutativity of $E[n]$ immediately trivialises $[P,P']$, so it suffices to check that $[f_P,f_{P'}]$ is constant and equal to $\mathrm{e}_n(P,P')$. By the definition of the group operation,

$$[f_P,f_{P'}]=f_{P+P'-P-P'}=\frac{f_P\cdot\tau_P^*f_{P'}}{\tau_{P'}^*f_P\cdot f_{P'}},$$

so a simple divisorial computation yields

$$[[f_P,f_{P'}]]=(n[P]-n[\mathcal{O}])+(n[P+P']-n[P])-(n[P'+P]-n[P'])-(n[P']-n[\mathcal{O}])=0,$$

which is equivalent to saying that $[f_P,f_{P'}]\in\overline{F}^{\times}$. Now fix a point $Q\in E$ in general position such that $\{\mathcal{O},\pm P,\pm Q,\pm P\pm Q\}$ are pairwise distinct. Applying the Abel-Jacobi map to the points P and P' gives linearly equivalent divisors $[P]-[\mathcal{O}]\sim[Q+P]-[Q]$ and $[P']-[\mathcal{O}]\sim[Q+P']-[Q]$ related via the line functions $\mathrm{L}_{Q,P},\mathrm{L}_{Q,P'}\in\overline{F}(E)^{\times}$, so another divisorial computation yields

$$\mathrm{e}_n(P,P')=\widetilde{\mathrm{e}_n}\left([Q+P]-[Q],[Q+P']-[Q]\right)=\frac{f_P(Q)\,f_{P'}(Q+P)}{f_P(Q+P')\,f_{P'}(Q)}=[f_P,f_{P'}](Q),$$

which is well-defined and constant despite the choice of $Q\in E$. □

Remark. In explicit descent theory of elliptic curves, theta groups are also used to parameterise 1-cocycles of $\mathrm{H}^1(F,E[n])$. It can be shown that every $\overline{F}$-theta group of level n for E is a twist of Θ [Sto10, Proposition 1.6], and that $E[n]$ is isomorphic to the group of automorphisms of central extensions of $E[n]$ by $\overline{F}^{\times}$. Thus the $\overline{F}$-theta groups of level n for E, viewed as twists of Θ, exactly parameterise the 1-cocycles of $\mathrm{H}^1(F,E[n])$ up to F-isomorphism, by the twisting principle. Proving these facts is not difficult, but will be skipped for a more useful description in terms of Brauer-Severi diagrams to be described in the next subsection.

Applying non-abelian Galois cohomology to the diagram in Proposition 3.2.3, taking into account the $\mathrm{Gal}\left(\overline{F}/F\right)$-group structure of Θ, induces a long row-exact diagram of cohomology pointed sets, so truncating this at the second connecting homomorphism furnishes a commutative square

$$\begin{array}{ccc}\mathrm{H}^1(F,E[n]) & \xrightarrow{\mathrm{Ob}_F} & \mathrm{Br}\,F\\ {\scriptstyle \mathrm{H}^1(F,\epsilon)}\downarrow & & \updownarrow{=}\\ \mathrm{H}^1(F,\mathrm{PGL}_n) & \xhookrightarrow[\delta_1]{} & \mathrm{Br}\,F\end{array},$$

where the composition Ob_F will be called the **period-index obstruction**. By the description of the homomorphism ϵ, this is the induced map on cohomology that takes an automorphism $\sigma\in\mathrm{Gal}\left(\overline{F}/F\right)$ and sends a point $P_\sigma\in E[n]$ to a projective transformation $\widehat{T_{P_\sigma}}\in\mathrm{PGL}_n$, embedded into $\mathrm{Br}\,F$.

Remark. There are several interpretations of this map, one of which says that it measures the failure of elements in $\mathrm{H}^1(F,E[n])$ to be mappable into $\mathbb{P}^{n-1}$, and will be clear after discussing Brauer-Severi diagrams. Another interpretation that bestows the name of this map says that it measures the failure of the **period** of an F-torsor, its order in the torsion group $\mathrm{H}^1(F,E)$, to be equal to its **index**, the smallest degree of a line bundle on it that is definable over F. In particular, the period of a torsor always divides the index, and in many cases these quantities are equal, but there are examples where they differ [ONe01, Section 1].

Returning to the relevant case of $F=K_v$ for a fixed place $v\in\mathcal{V}_K$, it follows that $\mathrm{H}^1(K_v,E[n])$ can be equipped with a quadratic map, the local period-index obstruction $\mathrm{Ob}_{K_v}:\mathrm{H}^1(K_v,E[n])\to\mathrm{Br}\,K_v\hookrightarrow\mathbb{Q}/\mathbb{Z}$.

(3.2.5) **Corollary.** *The local period-index obstruction is quadratic. That is,*

$$\begin{array}{rcl} \mathrm{H}^1(K_v, E[n]) \times \mathrm{H}^1(K_v, E[n]) & \longrightarrow & \mathrm{Br}\, K_v \hookrightarrow \mathbb{Q}/\mathbb{Z} \\ (\xi_1, \xi_2) & \longmapsto & \mathrm{Ob}_{K_v}(\xi_1 + \xi_2) - \mathrm{Ob}_{K_v}(\xi_1) - \mathrm{Ob}_{K_v}(\xi_2) \end{array}$$

is a symmetric $\mathbb{Z}$-bilinear pairing.

Proof. Since the cup product and the commutator are both $\mathbb{Z}$-bilinear, and that the alternativity introduced by both pairings cancel out to establish symmetry, this follows immediately from Lemma 3.2.2. □

It is worth noting that if a submodule of $\mathrm{H}^1(K_v, E[n])$ is totally isotropic, so that this bilinear pairing is the zero map, then the local period-index obstruction is a homomorphism when restricted to this submodule. By making use of the specific $\overline{K_v}$-theta group Θ, this map can also be shown to be a quadratic form.

(3.2.6) **Proposition.** *The local period-index obstruction is even. That is,*

$$\mathrm{Ob}_{K_v}(\xi) = \mathrm{Ob}_{K_v}(-\xi), \qquad \xi \in \mathrm{H}^1(K_v, E[n]).$$

Proof. Consider the inversion of Θ defined by

$$\begin{aligned} -\Theta &\coloneqq \left\{ (P, f_P)^{-1} \in E[n] \times \overline{K_v}(E)^\times \;\middle|\; [f_P] = n[P] - n[\mathcal{O}] \right\} \\ &= \left\{ (-P, f_{-P}) \in E[n] \times \overline{K_v}(E)^\times \;\middle|\; [f_{-P}] = n[-P] - n[\mathcal{O}] \right\}, \end{aligned}$$

which is clearly isomorphic to Θ by the inversion map $\iota : E \to E$. Defining the inverted map $-\alpha : \overline{K_v}^\times \to -\Theta$ in the obvious way furnishes a row-exact diagram of groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \overline{K_v}^\times & \xrightarrow{\alpha} & \Theta & \xrightarrow{\beta} & E[n] & \longrightarrow & 0 \\ & & \Big\updownarrow{\scriptstyle =} & & \Big\downarrow{\scriptstyle \iota} & & \Big\downarrow{\scriptstyle \iota} & & \\ 0 & \longrightarrow & \overline{K_v}^\times & \xrightarrow[-\alpha]{} & -\Theta & \xrightarrow[\beta]{} & E[n] & \longrightarrow & 0 \end{array},$$

both rows of which induce the period-index obstruction on cohomology, by Proposition 3.2.3. Thus the δ-functoriality of non-abelian Galois cohomology establishes a commutative square of pointed sets

$$\begin{array}{ccc} \mathrm{H}^1(K_v, E[n]) & \xrightarrow{\mathrm{Ob}_{K_v}} & \mathrm{Br}\, K_v \\ {\scriptstyle \mathrm{H}^1(K_v, \iota)}\Big\downarrow & & \Big\updownarrow{\scriptstyle =} \\ \mathrm{H}^1(K_v, E[n]) & \xrightarrow[\mathrm{Ob}_{K_v}]{} & \mathrm{Br}\, K_v \end{array},$$

so that $\mathrm{Ob}_{K_v} = \mathrm{Ob}_{K_v} \circ \mathrm{H}^1(K_v, \iota)$. □

Remark. As the proofs of Corollary 3.2.5 and Proposition 3.2.6 did not use any facts about local fields, the same arguments and statements generalise to a general field F, provided the notion of a quadratic form taking values on an arbitrary abelian group is appropriately defined.

Thus $\mathrm{H}^1(K_v, E[n])$, equipped with the local period-index obstruction, is indeed a quadratic $\mathbb{Z}/n$-module. It then follows from local duality that it is also non-degenerate.

(3.2.7) **Corollary.** *The quadratic $\mathbb{Z}/n$-module $\mathrm{H}^1(K_v, E[n])$ is non-degenerate. That is,*

$$\begin{array}{rcl} \mathrm{H}^1(K_v, E[n]) & \longrightarrow & \mathrm{H}^1(K_v, E[n])^\star \\ \xi_1 & \longmapsto & (\xi_2 \mapsto \mathrm{Ob}_{K_v}(\xi_1 + \xi_2) - \mathrm{Ob}_{K_v}(\xi_1) - \mathrm{Ob}_{K_v}(\xi_2)) \end{array}$$

is an isomorphism of abelian groups.

Proof. The induced commutator pairing coincides with the non-degenerate n-Weil pairing by Proposition 3.2.4, while the non-degeneracy of the cup product follows by Tate's local duality for $E[n]$, and these exactly constitute the period-index obstruction by Lemma 3.2.2. □

Summing over all local period-index obstructions yields a global quadratic form, so that the full first adelic cohomology group $\mathrm{H}^1(\mathbb{A}_K, E[n])$ is the desired ambient quadratic $\mathbb{Z}/n$-module, but the map obtained is *a priori* not a well-defined sum, and proving this will be an immediate consequence in the next subsection.

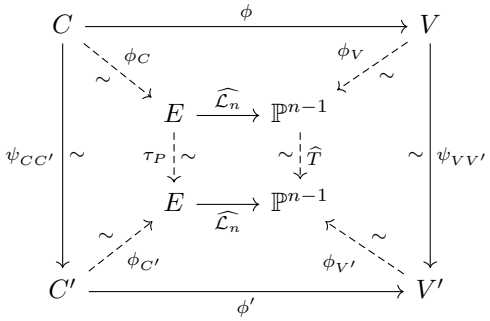
3.2.2 Lagrangian submodules and weak metabolicity

This subsection continues the proof by establishing the Lagrangian conditions for $\operatorname{im}\kappa$ and $\operatorname{im}\lambda$, and deducing that $\mathrm{H}^1(\mathbb{A}_K, E[n])$ is a well-defined non-degenerate quadratic $\mathbb{Z}/n$-module. The proof follows the arguments in the paper on random maximal isotropic subspaces by Poonen and Rains [PR12], but a more elementary proof is provided as an alternative to a key result in their paper. The alternative proof is based on the notion of Brauer-Severi diagrams, as detailed in the paper on explicit descent on elliptic curves by Cremona, Fisher, O'Neil, Simon, and Stoll [CFOSS06], with some arguments sketched from O'Neil's paper on the period-index obstruction [ONe01]. This is an abstract construct, extending the notion of Brauer-Severi varieties, with group of automorphisms isomorphic to $E[n]$, hence parameterising $\mathrm{H}^1(F, E[n])$ through the twisting principle. In what follows, let dashed arrows denote $\overline{F}$-isomorphisms.

Definition. An F**-Brauer-Severi diagram** $[\phi]$ of dimension n for E is an F-morphism $\phi : C \to V$ from an F-torsor $C \in \mathrm{WC}(E/F)[n]$ to an F-Brauer-Severi variety $V \in \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right)$ such that the square

$$\begin{array}{ccc} C & \xrightarrow{\phi} & V \\ {\scriptstyle\phi_C}\,\vdots\,{\scriptstyle\sim} & & {\scriptstyle\sim}\,\vdots\,{\scriptstyle\phi_V} \\ \downarrow & & \downarrow \\ E & \xrightarrow[\widehat{\mathcal{L}_n}]{} & \mathbb{P}^{n-1} \end{array}$$

commutes. Two F-Brauer-Severi diagrams $[\phi : C \to V]$ and $[\phi' : C' \to V']$ of dimension n for E are considered **equivalent** if there is a pair $(\psi_{CC'}, \psi_{VV'})$, consisting of an F-isomorphism of F-torsors $\psi_{CC'} : C \xrightarrow{\sim} C'$ and an F-isomorphism of varieties $\psi_{VV'} : V \xrightarrow{\sim} V'$, such that the diagram



commutes, for some point $P \in E$ and some projective transformation $\widehat{T} \in \mathrm{PGL}_n$. Finally, define the set

$$\mathrm{BS}_n(E/F) \coloneqq \{F\text{-Brauer-Severi diagrams of dimension } n \text{ for } E \text{ modulo equivalence}\},$$

pointed at a distinguished identity, abusively denoted $\mathcal{L} \coloneqq \left[\widehat{\mathcal{L}_n}\right]$, given by the linear system $\widehat{\mathcal{L}_n} : E \to \mathbb{P}^{n-1}$.

Conceptually, given any morphism $\phi : C \to V$ of F-twists $C \in \mathrm{WC}(E/F)[n]$ and $V \in \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right)$, the F-Brauer-Severi diagram $[\phi]$ can be viewed as an F-twist of $\mathcal{L}$, so applying the twisting principle to $\mathrm{BS}_n(E/F)$ would result in the group $\mathrm{H}^1(F, E[n])$. A formal proof of this entails a bit more work.

(3.2.8) **Proposition.** *There is an isomorphism of abelian groups*

$$E[n] \xrightarrow{\sim} \operatorname{Aut}\mathcal{L},$$

where $\operatorname{Aut}\mathcal{L}$ *denotes the group of automorphisms of* $\mathcal{L}$*.*

Proof. An element $P \in E[n]$ supplies an automorphism of F-torsors $\tau_P : E \to E$ that uniquely extends to an automorphism of varieties $\widehat{T_P} : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$, making the diagram commute as argued previously, and hence giving a well-defined automorphism $\left(\tau_P, \widehat{T_P}\right) \in \operatorname{Aut}\mathcal{L}$. Conversely, an automorphism $\left(\tau_P, \widehat{T}\right) \in \operatorname{Aut}\mathcal{L}$ consists of a translation map $\tau_P : E \to E$ for some point $P \in E$ that automatically fixes the unique projective transformation $\widehat{T} = \widehat{T_P} \in \mathrm{PGL}_n$, which in turn gives a linear equivalence $n[\mathcal{O}] \sim n[P]$. Thus there is a well-defined bijection of pointed sets sending P to $\left(\tau_P, \widehat{T_P}\right)$, which is a homomorphism by construction. □

The twisting principle now heuristically relates $\mathrm{BS}_n(E/F)$ and $\mathrm{H}^1(F, E[n])$, although a constructive sketch of the proof will be useful to define the correspondence explicitly.

(3.2.9) **Proposition.** *There is a bijective correspondence of pointed sets*

$$\begin{array}{ccc} \mathrm{BS}_n(E/F) & \rightsquigarrow & \mathrm{H}^1(F, E[n]) \\ [\phi : C \to V] & \longmapsto & (\sigma \mapsto P_\sigma) \end{array},$$

for a unique point $P_\sigma \in E[n]$, which supplies $\mathrm{BS}_n(E/F)$ with the structure of an abelian group.

Proof. Given an F-Brauer-Severi diagram $[\phi : C \to V] \in \mathrm{BS}_n(E/F)$, consider a sufficiently large finite Galois extension F' over F such that $C(F') \neq \emptyset$, so that, by taking direct limits over all such F', the result reduces to constructing a unique corresponding 1-cocycle in $\mathrm{H}^1(F'/F, E(F')[n])$. Now sending a fixed F'-rational point in C to $\mathcal{O} \in E$ yields an F'-isomorphism $\phi_{C(F')} : C(F') \xrightarrow{\sim} E(F')$, which, viewed as a self-translation map, uniquely extends to an F'-isomorphism $\phi_{V(F')} : V(F') \xrightarrow{\sim} \mathbb{P}^{n-1}(F')$ such that the square

$$\begin{array}{ccc} C(F') & \longrightarrow & V(F') \\ {\scriptstyle \phi_{C(F')}}\downarrow & & \downarrow{\scriptstyle \phi_{V(F')}} \\ E(F') & \longrightarrow & \mathbb{P}^{n-1}(F') \end{array}$$

commutes. Thus the 1-cocycle in $\mathrm{H}^1(F'/F, E(F')[n])$ sending an automorphism $\sigma \in \mathrm{Gal}(F'/F)$ to the automorphism of F-Brauer-Severi diagrams $\left(\tau_{P_\sigma}, \widehat{T_{P_\sigma}}\right) := \left(\sigma \cdot \phi_{C(F')} \circ \phi_{C(F')}^{-1}, \sigma \cdot \phi_{V(F')} \circ \phi_{V(F')}^{-1}\right) \in \mathrm{Aut}\,\mathcal{L}(F')$ is unique, and corresponds to a point $P_\sigma \in E(F')[n]$ by the finite version of Proposition 3.2.8. □

With the correspondence in Proposition 3.2.9, two forgetful maps can be constructed on $\mathrm{BS}_n(E/F)$. One map simply forgets the right half of the diagram containing the F-Brauer-Severi variety, by sending

$$\begin{array}{ccc} \mathrm{BS}_n(E/F) & \longrightarrow & \mathrm{WC}(E/F)[n] \\ [\phi : C \to V] & \longmapsto & C \end{array},$$

which is a homomorphism that corresponds to the right map $\mathrm{H}^1(F, E[n]) \to \mathrm{H}^1(F, E)[n]$ in the Kummer sequence. The other map simply forgets the left half of the diagram containing the F-torsor, by sending

$$\begin{array}{ccc} \mathrm{BS}_n(E/F) & \longrightarrow & \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right) \\ [\phi : C \to V] & \longmapsto & V \end{array},$$

which is only a map of pointed sets. To summarise, all of the aforementioned bijective correspondences, alongside the period-index obstruction, fit in a diagram of pointed sets

$$\begin{array}{ccccccccc} & & & & \mathrm{BS}_n(E/F) & \xleftrightarrow{\sim} & \mathrm{H}^1(F, E[n]) & & \\ & & & \swarrow & \downarrow & & & \searrow^{\mathrm{Ob}_F} & \\ \mathrm{H}^1(F, E)[n] & \xleftrightarrow[\sim]{} & \mathrm{WC}(E/F)[n] & \xrightarrow[\phi]{} & \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right) & \xleftrightarrow[\sim]{} & \mathrm{H}^1(F, \mathrm{PGL}_n) & \hookrightarrow & \mathrm{Br}\,F \end{array}.$$

It turns out that the right trapezium actually commutes, which says that the second forgetful map coincides exactly with the period-index obstruction, so the characterisation using theta groups also carry over.

(3.2.10) **Proposition.** *The period-index obstruction $\mathrm{Ob}_F : \mathrm{H}^1(F, E[n]) \to \mathrm{Br}\,F$ maps an F-Brauer-Severi diagram $[\phi : C \to V] \in \mathrm{BS}_n(E/F)$ to its F-Brauer-Severi variety $V \in \mathrm{Twist}\left(\mathbb{P}^{n-1}/F\right)$.*

Proof. Let $\sigma \in \mathrm{Gal}\left(\overline{F}/F\right)$ be a fixed automorphism. A 1-cocycle $\xi \in \mathrm{H}^1(F, E[n])$ mapping σ to a point $P_\sigma \in E[n]$ sends σ to the automorphism of F-Brauer-Severi diagrams $\left(\tau_{P_\sigma}, \widehat{T_{P_\sigma}}\right) \in \mathrm{Aut}\,\mathcal{L}$, by the description in Proposition 3.2.9. The second forgetful map then corresponds to sending this pair to the automorphism of varieties $\widehat{T_{P_\sigma}} : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$, so this is in fact a 1-cocycle $\xi \in \mathrm{H}^1(F, \mathrm{PGL}_n) \hookrightarrow \mathrm{Br}\,F$ that maps σ to a projective transformation $\widehat{T_{P_\sigma}} \in \mathrm{PGL}_n$, which coincides exactly with the description of Ob_F. □

Remark. Interestingly, an interpretation of n-Selmer group can be read off almost immediately from the construction of Brauer-Severi diagrams. In particular, there is a bijective correspondence of pointed sets

$$\mathcal{S}_n(K,E) \quad \leftrightsquigarrow \quad \left\{ \left[\phi : C \to \mathbb{P}^{n-1}\right] \in \mathrm{BS}_n(E/K) \;\middle|\; \forall v \in \mathcal{V}_K,\ C(K_v) \neq \emptyset \right\} \subseteq \mathrm{BS}_n(E/K),$$

so the latter subset also inherits a subgroup structure. This correspondence is an immediate consequence of the fundamental sequence of global class field theory and a simple diagram chase.

Returning to the original objective of proving weak metabolicity, first consider the case of $F = K_v$ for a fixed place $v \in \mathcal{V}_K$. For ease of notation, denote the left map in the local Kummer sequence by

$$\kappa_v : E(K_v)/n \hookrightarrow \mathrm{H}^1(K_v, E[n]),$$

so that the adelic injection κ is a direct product of the local injections κ_v. Proving that $\operatorname{im}\kappa_v$ is a Lagrangian submodule of $\mathrm{H}^1(K_v, E[n])$ reduces to proving total isotropy and maximality, but total isotropy follows from relating the period-index obstruction to the various correspondences of Brauer-Severi diagrams.

(3.2.11) **Proposition.** *The submodule* $\operatorname{im}\kappa_v$ *is totally isotropic. That is,*

$$\operatorname{im}\kappa_v \subseteq \ker \mathrm{Ob}_{K_v}.$$

Proof. Along with the local Kummer sequence, consider the diagram of pointed sets

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K_v)/n & \xrightarrow{\kappa_v} & \mathrm{H}^1(K_v, E[n]) & \xrightarrow{\mu_v} & \mathrm{H}^1(K_v, E)[n] & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{Ob}_{K_v}} & & \Big\updownarrow{\scriptstyle \sim} & & \Big\updownarrow{\scriptstyle \sim} & & \\
 & & & & \mathrm{BS}_n(E/K_v) & \xrightarrow[\mu_v']{} & \mathrm{WC}(E/K_v)[n] & & \\
 & & & & & & \Big\downarrow{\scriptstyle \phi} & & \\
 & & \mathrm{Br}\, K_v & \hookleftarrow & \mathrm{H}^1(K_v, \mathrm{PGL}_n) & \xleftarrow[\sim]{} & \mathrm{Twist}\left(\mathbb{P}^{n-1}/K_v\right) & &
\end{array},$$

which commutes by Proposition 3.2.10, where the dashed arrow denotes the induced map restricted to $E(K_v)/n$. Then $\operatorname{im}\kappa_v$ is exactly the kernel of μ_v, which corresponds to that of the forgetful map μ_v'. On the other hand, this sends a K_v-Brauer-Severi diagram $[\phi : C \to V] \in \mathrm{BS}_n(E/K_v)$ to its K_v-torsor $C \in \mathrm{WC}(E/K_v)[n]$, which corresponds to the trivial class in $\mathrm{H}^1(K_v, E[n])$ if and only if $C(K_v) \neq \emptyset$. Applying the K_v-morphism $\phi : C \to V$ also forces $V(K_v) \neq \emptyset$, which holds precisely when its K_v-Brauer-Severi variety $V \in \mathrm{Twist}\left(\mathbb{P}^{n-1}/K_v\right)$ corresponds to the trivial class in $\mathrm{H}^1(K_v, \mathrm{PGL}_n)$. Thus any element of $\operatorname{im}\kappa_v$ is sent via the period-index obstruction to the trivial class in $\mathrm{Br}\, K_v$. □

Remark. The proof of Proposition 3.2.11 is independent of locality, and would work for a general field F.

In a similar vein as before, proving maximality does utilise local duality.

(3.2.12) **Proposition.** *The submodule* $\operatorname{im}\kappa_v$ *is maximal. That is,*

$$\operatorname{im}\kappa_v = (\operatorname{im}\kappa_v)^{\perp}.$$

Proof. Consider the long exact sequence of cohomology groups inducing the local Kummer sequence

$$\cdots \to E(K_v) \xrightarrow{\kappa_v} \mathrm{H}^1(K_v, E[n]) \to \mathrm{H}^1(K_v, E) \to \ldots,$$

so that $\operatorname{im}\kappa_v$ is simultaneously the image of $E(K_v)$ and of $E(K_v)/n$ inside $\mathrm{H}^1(K_v, E[n])$. By Tate's local duality for $E[n]$, their Pontryagin dual maps are $\mathrm{H}^1(K_v, E[n]) \to E(K_v)^\star$ and $\mathrm{H}^1(K_v, E[n]) \to (E(K_v)/n)^\star$ respectively, whose kernels are both $(\operatorname{im}\kappa_v)^{\perp}$. It then suffices to identify $\mathrm{H}^1(K_v, E)$ with $E(K_v)^\star$ or $(E(K_v)/n)^\star$, after which the result follows by exactness, and doing this entails splitting into cases depending on the place $v \in \mathcal{V}_K$. The non-archimedean case follows immediately by Tate's local duality for elliptic curves. In the archimedean case of $\mathbb{C}$, completeness implies that $E(\mathbb{C})/n = 0$, while connectedness implies that $\pi_0(E(\mathbb{C})) = 0$, but the Pontryagin dual of the latter is exactly $\mathrm{H}^1(\mathbb{C}, E)$. Likewise, in the archimedean case of $\mathbb{R}$, completeness implies that $E(\mathbb{R})/n \cong \mathbb{Z}/2$ whenever n is even, which is equal to $\pi_0(E(\mathbb{C})) \cong \mathbb{Z}/2$, so Tate's local duality for elliptic curves applies again. The previous argument fails when n is odd, but in this case $\mathrm{H}^1(\mathbb{R}, E[n])$ is simultaneously 2-torsion, by virtue of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, and n-torsion, by virtue of $E[n]$, so it is in fact trivial. Thus $\operatorname{im}\kappa_v$ and $(\operatorname{im}\kappa_v)^{\perp}$ are both trivial and the result follows. □

Recall that the restricted product of weakly metabolic quadratic $\mathbb{Z}/n$-modules with respect to their Lagrangian submodules is naturally also weakly metabolic. Now apply this to $\mathrm{H}^1(\mathbb{A}_K, E[n])$, which was defined to be the restricted product of $\mathrm{H}^1(K_v, E[n])$ with respect to $\mathrm{H}^1_{\mathrm{u}}(K_v, E[n])$.

(3.2.13) **Corollary.** *The ambient module* $\mathrm{H}^1(\mathbb{A}_K, E[n])$*, equipped with the quadratic form*

$$\begin{array}{rccc} \mathfrak{q} & : & \mathrm{H}^1(\mathbb{A}_K, E[n]) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & & (\xi_v)_{v\in\mathcal{V}_K} & \longmapsto & \displaystyle\sum_{v\in\mathcal{V}_K} \mathrm{inv}_{K_v}(\mathrm{Ob}_{K_v}(\xi_v)) \end{array}$$

is a well-defined non-degenerate quadratic $\mathbb{Z}/n$*-module.*

Proof. Since the local Hasse invariant is a homomorphism, the fact that it is a non-degenerate quadratic $\mathbb{Z}/n$-module follows immediately from properties of the local period-index obstruction in Corollary 3.2.7, so it suffices to verify that it is a well-defined finitary sum, but this also follows from Proposition 3.2.11 and that $\operatorname{im}\kappa_v \cong E(K_v)/n \cong \mathrm{H}^1_{\mathrm{u}}(K_v, E[n])$ for all but finitely many places $v \in \mathcal{V}_K$. □

With a well-defined quadratic $\mathbb{Z}/n$-module, it now makes sense for its submodules to be Lagrangian.

(3.2.14) **Corollary.** *The submodule* $\operatorname{im}\kappa$ *is Lagrangian. That is,*

$$\operatorname{im}\kappa \subseteq \ker\mathfrak{q}, \qquad \operatorname{im}\kappa = (\operatorname{im}\kappa)^{\perp}.$$

Proof. This follows immediately from taking direct products of the local components in Proposition 3.2.11 and Proposition 3.2.12, together with the definition of the quadratic form in Corollary 3.2.13. □

Thus this establishes that $\mathrm{H}^1(\mathbb{A}_K, E[n])$ is weakly metabolic. Now the bulk of the work in this subsection deals with the submodule $\operatorname{im}\kappa$, while the fact that the submodule $\operatorname{im}\lambda$ is Lagrangian is almost an immediate consequence of global class field theory and Tate's global duality.

(3.2.15) **Proposition.** *The submodule* $\operatorname{im}\lambda$ *is Lagrangian. That is,*

$$\operatorname{im}\lambda \subseteq \ker\mathfrak{q}, \qquad \operatorname{im}\lambda = (\operatorname{im}\lambda)^{\perp}.$$

Proof. The fundamental sequence of global class field theory induces a row-exact diagram of abelian groups

$$\begin{array}{ccccccccc} & & \mathrm{H}^1(K, E[n]) & \xrightarrow{\lambda} & \mathrm{H}^1(\mathbb{A}_K, E[n]) & & & & \\ & & \downarrow{\scriptstyle \mathrm{Ob}_K} & & \downarrow{\scriptstyle \sum \mathrm{Ob}_{K_v}} & \searrow^{\mathfrak{q}} & & & \\ 0 & \longrightarrow & \mathrm{Br}\,K & \longrightarrow & \displaystyle\bigoplus_{v\in\mathcal{V}_K} \mathrm{Br}\,K_v & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array},$$

which commutes by δ-functoriality of Galois cohomology. Here, the composition $\mathfrak{q}\circ\lambda$ factors through the global period-index obstruction, and $\operatorname{im}\lambda$ is sent to the trivial class in $\mathbb{Q}/\mathbb{Z}$ upon summing the local Hasse invariants. Hence $\operatorname{im}\lambda$ is contained in $\ker\mathfrak{q}$, while for the equality of $\operatorname{im}\lambda$ and $(\operatorname{im}\lambda)^{\perp}$, extract the middle terms of the Poitou-Tate exact sequence to establish exactness at

$$\mathrm{H}^1(K, E[n]) \xrightarrow{\tau^1} \mathrm{H}^1(\mathbb{A}_K, E[n]) \cong \mathrm{H}^1(\mathbb{A}_K, E[n])^{\star} \xrightarrow{\sigma^1} \mathrm{H}^1(K, E[n])^{\star}.$$

The result then follows by identifying $\lambda = \tau^1$ and its Pontryagin dual map $\lambda^{\star} = \sigma^1$. □

With more work, it can be shown that $\operatorname{im}\kappa$ is also a direct summand, hence further establishing strong metabolicity, and that $\operatorname{im}\lambda$ is often a direct summand, at least for almost all elliptic curves. Describing when $\operatorname{im}\lambda$ is a direct summand would be more enlightening after writing down the explicit assumption in the following subsection, so the proof of strong metabolicity will be delayed to after the following subsection.

3.2.3 Triviality of the first Tate-Shafarevich group

The aim of this subsection is to attain a frequently applicable criterion for the vanishing of the first Tate-Shafarevich group $Ш^1(K, E[n])$ when $n = p^e \in \mathbb{N}^+$ is a prime power. The overall proof is a purely algebraic computation, detailing the arithmetic justification in the paper on modelling distributions of elliptic curves by Bhargava, Kane, Lenstra, Poonen, and Rains [BKLPR15]. This will involve a long-winded series of inflation-restriction exact sequences, beginning with the reduction to a more workable cohomology group.

Given a finite $\mathrm{Gal}(\overline{K}/K)$-module A, its $\mathrm{Gal}(\overline{K}/K)$-action induces a homomorphism

$$\rho_A : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, A.$$

On the other hand, any subgroup $G \leq \mathrm{im}\, \rho_A$ induces natural restriction maps

$$\mathrm{res}_G : \mathrm{H}^m(\mathrm{im}\, \rho_A, A) \to \mathrm{H}^m(G, A), \qquad m \in \mathbb{N},$$

where A is now considered as a finite $\mathrm{im}\, \rho_A$-module. Considering the direct sum of such restriction maps over all cyclic subgroups furnishes the m-th **cyclic cohomology** groups

$$\mathrm{H}^m_{\mathrm{c}}(\mathrm{im}\, \rho_A, A) \coloneqq \ker\left(\bigoplus \mathrm{res}_C : \mathrm{H}^m(\mathrm{im}\, \rho_A, A) \to \bigoplus_{C \leq \mathrm{im}\, \rho_A \text{ cyclic}} \mathrm{H}^m(C, A)\right), \qquad m \in \mathbb{N}.$$

The first result reduces the vanishing of the first Tate-Shafarevich group to a cyclic cohomology group.

(3.2.16) **Lemma.** *Let A be a finite $\mathrm{im}\, \rho_A$-module. Then there is a monomorphism*

$$Ш^1(K, A) \hookrightarrow \mathrm{H}^1_{\mathrm{c}}(\mathrm{im}\, \rho_A, A).$$

Proof. For this proof, write $R \coloneqq \mathrm{im}\, \rho_A$. The first isomorphism theorem gives an isomorphism of finite groups $R \cong \mathrm{Gal}(\overline{K}/K) / \ker \rho_A$, so the finite version of the Galois correspondence applies to identify $R \cong \mathrm{Gal}(L/K)$ for some fixed finite Galois extension L over K. Then the inflation-restriction exact sequence applied to the finite Galois group $\mathrm{Gal}(\overline{K}/K) / \mathrm{Gal}(\overline{K}/L) \cong \mathrm{Gal}(L/K)$ yields

$$0 \to \mathrm{H}^1(R, A) \xrightarrow{\mathrm{inf}} \mathrm{H}^1(K, A) \xrightarrow{\mathrm{res}} \mathrm{H}^1(L, A),$$

where $A^{\mathrm{Gal}(\overline{K}/L)} = A$ since $\mathrm{Gal}(\overline{K}/L)$ acts trivially on A by assumption. Now each place $v \in \mathcal{V}_K$ extends to a choice of a place $w \in \mathcal{V}_L$, so applying the same argument everywhere locally yields

$$0 \to \prod_{v \in \mathcal{V}_K} \mathrm{H}^1(R_v, A) \xrightarrow{\prod \mathrm{inf}_v} \prod_{v \in \mathcal{V}_K} \mathrm{H}^1(K_v, A) \xrightarrow{\prod \mathrm{res}_v} \prod_{v \in \mathcal{V}_K} \mathrm{H}^1(L_w, A),$$

where $R_v \coloneqq \mathrm{Gal}(L_w/K_v)$. Then combining both sequences with the obvious restriction maps and extracting the first few terms through the snake lemma, by definition, establishes a left exact sequence of abelian groups

$$0 \to Ш^1(L/K, A) \to Ш^1(K, A) \to Ш^1(L, A).$$

By Chebotarev's density theorem, any cyclic subgroup of R is isomorphic to a local Galois group R_v for some non-archimedean place $v \in \mathcal{V}_K^0$, so there is a monomorphism $Ш^1(L/K, A) \hookrightarrow \mathrm{H}^1_{\mathrm{c}}(R, A)$. On the other hand, any homomorphism $\mathrm{Gal}(\overline{K}/L) \to A$ that becomes trivial upon restriction to all cyclic subgroups $C \leq \mathrm{Gal}(\overline{K}/L)$ must also be trivial, so the direct sum of such restriction maps $\mathrm{res}_C : \mathrm{H}^1(L, A) \to \mathrm{H}^1(C, A)$ has trivial kernel. Thus Chebotarev's density theorem applies again to these cyclic subgroups for the triviality of $Ш^1(L, A)$, and the desired monomorphism is the composition $Ш^1(K, A) \cong Ш^1(L/K, A) \hookrightarrow \mathrm{H}^1_{\mathrm{c}}(R, A)$. □

More explicitly, the vanishing of $Ш^1(K, A)$ simply reduces to the injectivity of the restriction map $\mathrm{res}_C : \mathrm{H}^1(\mathrm{im}\, \rho_A, A) \to \mathrm{H}^1(C, A)$ for at least one cyclic subgroup $C \leq \mathrm{im}\, \rho_A$. Returning to the relevant case of the n-torsion subgroup $E[n]$, the induced homomorphism $\rho_{E[n]} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/n)$ is really a two-dimensional modulo n Galois representation, and triviality holds unconditionally when $n = p$ is prime.

(3.2.17) **Proposition.**

$$Ш^1(K, E[p]) = 0.$$

Proof. For this proof, write $R \coloneqq \operatorname{im} \rho_{E[p]}$. By Lemma 3.2.16, it suffices to show that the induced restriction map $\operatorname{res}_C : \mathrm{H}^1(R, E[p]) \to \mathrm{H}^1(C, E[p])$ is injective for some cyclic subgroup $C \leq R$. If $p \nmid \#R$, the group $\mathrm{H}^1(R, E[p])$ is trivially annihilated by p and the restriction map is vacuously injective, so now assume that $p \mid \#R$. Since $\#\operatorname{GL}_2(\mathbb{F}_p) = p(p+1)(p-1)^2$, by the Sylow theorems, the unique conjugacy class of p-Sylow subgroups of $\operatorname{GL}_2(\mathbb{F}_p) \cong \operatorname{Aut} \mathbb{F}_p^2 \cong \operatorname{Aut} E[p]$ precisely coincides with its cyclic subgroups of order p, and at least one such subgroup $C \leq \operatorname{GL}_2(\mathbb{F}_p)$ is also contained in R by assumption. Thus the result follows from the injectivity of restriction maps on p-Sylow subgroups. □

To prove the injectivity of the restriction map in the general case of $n = p^e$ entails further work, and the upcoming proof works only under the mild assumption that $\operatorname{SL}_2(\mathbb{Z}/p^e) \leq \operatorname{im} \rho_{E[p^e]}$, which begins with another reduction to a cyclic cohomology group.

(3.2.18) **Lemma.** *Assume that* $\operatorname{SL}_2(\mathbb{Z}/n) \leq \operatorname{im} \rho_{E[n]}$. *Then there is a monomorphism*

$$Ш^1(K, E[n]) \hookrightarrow \mathrm{H}^1_{\mathrm{c}}(\operatorname{SL}_2(\mathbb{Z}/n), E[n]).$$

Proof. For this proof, write $R \coloneqq \operatorname{im} \rho_{E[n]}$ and $S \coloneqq \operatorname{SL}_2(\mathbb{Z}/n)$, so the assumption reads $S \hookrightarrow R$. The inflation-restriction exact sequence applied to R/S yields

$$0 \to \mathrm{H}^1\left(R/S, E[n]^S\right) \xrightarrow{\inf} \mathrm{H}^1(R, E[n]) \xrightarrow{\operatorname{res}} \mathrm{H}^1(S, E[n]).$$

Any S-invariant element of $E[n] \cong (\mathbb{Z}/n)^2$ is in particular fixed by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in S$, which can only be the trivial element of $(\mathbb{Z}/n)^2$, so the invariant subgroup $E[n]^S$, and hence $\mathrm{H}^1\left(R/S, E[n]^S\right)$, is trivial. Thus the restriction map is injective, and the desired monomorphism is induced by the composition

$$\mathrm{H}^1(R, E[n]) \xhookrightarrow{\operatorname{res}} \mathrm{H}^1(S, E[n]) \xrightarrow{\bigoplus \operatorname{res}_C} \bigoplus_{C \leq S \text{ cyclic}} \mathrm{H}^1(C, E[n]) \xhookrightarrow{\subseteq} \bigoplus_{C \leq R \text{ cyclic}} \mathrm{H}^1(C, E[n]),$$

and then applying Lemma 3.2.16. □

The non-degenerate case of $p > 2$ is easy to deal with, by virtue of the subgroup $\{\pm 1\} \leq \operatorname{SL}_2(\mathbb{Z}/p^e)$.

(3.2.19) **Proposition.** *Let* $p > 2$. *Assume that* $\operatorname{SL}_2(\mathbb{Z}/p^e) \leq \operatorname{im} \rho_{E[p^e]}$. *Then*

$$Ш^1(K, E[p^e]) = 0.$$

Proof. For this proof, write $S \coloneqq \operatorname{SL}_2(\mathbb{Z}/p^e)$. By Lemma 3.2.18, it suffices to show a stronger condition that $\mathrm{H}^1(S, E[p^e])$ is trivial. The inflation-restriction exact sequence applied to $S/\{\pm 1\}$ yields

$$0 \to \mathrm{H}^1\left(S/\{\pm 1\}, E[p^e]^{\{\pm 1\}}\right) \xrightarrow{\inf} \mathrm{H}^1(S, E[p^e]) \xrightarrow{\operatorname{res}} \mathrm{H}^1(\{\pm 1\}, E[p^e]).$$

The natural $\{\pm 1\}$-action on $E[p^e] \cong (\mathbb{Z}/p^e)^2$ is either the identity map or the inversion map, so the invariant subgroup $E[p^e]^{\{\pm 1\}}$ is simply $E[p^e][2]$, which is simultaneously p-torsion and 2-torsion, and hence trivial. The same torsion argument applies for the triviality of $\mathrm{H}^1(\{\pm 1\}, E[p^e])$, so the result follows. □

The remainder of this subsection deals with the degenerate case of $p = 2$, which is significantly more cumbersome in both proof and notation. It suffices to consider $e > 1$, since the trivial scenario when $e = 1$ is already dealt with. First observe that reducing integers modulo 2^d induces natural quotient maps $\sigma_d^e : \operatorname{SL}_2(\mathbb{Z}/2^e) \twoheadrightarrow \operatorname{SL}_2\left(\mathbb{Z}/2^d\right)$, so for the remainder of this subsection, denote

$$\mathrm{S}_d \coloneqq \operatorname{SL}_2\left(\mathbb{Z}/2^d\right), \qquad \sigma_d^e : \mathrm{S}_e \twoheadrightarrow \mathrm{S}_d.$$

With this notation, the kernels of these reduction maps induce a descending filtration of groups

$$0 = \ker \sigma_e^e \leq \ker \sigma_{e-1}^e \leq \cdots \leq \ker \sigma_1^e \leq \ker \sigma_0^e = \mathrm{S}_e,$$

and a canonical isomorphism of groups $\mathrm{S}_e / \ker \sigma_d^e \cong \mathrm{S}_d$ by the first isomorphism theorem.

(3.2.20) **Lemma.** *Assume that* $\mathrm{S}_e \leq \operatorname{im} \rho_{E[2^e]}$. *Then there is an isomorphism of abelian groups*

$$\mathrm{H}^1\left(\mathrm{S}_e, E\left[2\right]\right) \xrightarrow{\sim} \mathrm{H}^1\left(\mathrm{S}_e, E\left[2^e\right]\right).$$

Proof. As per Proposition 3.2.19, the inflation-restriction exact sequence applied to $\mathrm{S}_e/\left\{\pm 1\right\}$ yields

$$0 \to \mathrm{H}^1\left(\mathrm{S}_e/\left\{\pm 1\right\}, E\left[2^e\right]^{\left\{\pm 1\right\}}\right) \xrightarrow{\inf} \mathrm{H}^1\left(\mathrm{S}_e, E\left[2^e\right]\right) \xrightarrow{\mathrm{res}} \mathrm{H}^1\left(\left\{\pm 1\right\}, E\left[2^e\right]\right),$$

but the invariant subgroup $E\left[2^e\right]^{\left\{\pm 1\right\}}$ is now $E\left[2\right]$, while an explicit cohomological computation yields

$$\mathrm{H}^1\left(\left\{\pm 1\right\}, E\left[2^e\right]\right) = E\left[2^e\right]/2E\left[2^e\right] \cong \left(\mathbb{Z}/2^e\right)^2/\left(2\mathbb{Z}/2^e\right)^2 \cong \left(\mathbb{Z}/2\right)^2,$$

by the third isomorphism theorem. Recall that the restriction map factors as a composition $\mathrm{H}^1\left(\mathrm{S}_e, E\left[2^e\right]\right) \to \mathrm{H}^1\left(\left\{\pm 1\right\}, E\left[2^e\right]\right)^{\mathrm{S}_e/\left\{\pm 1\right\}} \to \mathrm{H}^1\left(\left\{\pm 1\right\}, E\left[2^e\right]\right)$. As per Proposition 3.2.17, any $\mathrm{S}_e/\left\{\pm 1\right\}$-invariant element of $\left(\mathbb{Z}/2\right)^2$ is fixed by $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right) \in \mathrm{S}_e/\left\{\pm 1\right\}$, so the invariant subgroup $\mathrm{H}^1\left(\left\{\pm 1\right\}, E\left[2^e\right]\right)^{\mathrm{S}_e/\left\{\pm 1\right\}}$ must be trivial and the inflation map is an isomorphism. Recalling again that the inflation map factors as a composition $\mathrm{H}^1\left(\mathrm{S}_e/\left\{\pm 1\right\}, E\left[2\right]\right) \to \mathrm{H}^1\left(\mathrm{S}_e, E\left[2\right]\right) \to \mathrm{H}^1\left(\mathrm{S}_e, E\left[2^e\right]\right)$ gives a commutative diagram of abelian groups

$$\begin{array}{ccccccccc} & & & & \mathrm{H}^1\left(\mathrm{S}_e/\left\{\pm 1\right\}, E\left[2\right]\right) & & & & \\ & & & & \big\downarrow & \searrow^{\inf}_{\sim} & & & \\ \ldots & \longrightarrow & \mathrm{H}^0\left(\mathrm{S}_e, 2E\left[2^e\right]\right) & \xrightarrow{\delta_0} & \mathrm{H}^1\left(\mathrm{S}_e, E\left[2\right]\right) & \twoheadrightarrow & \mathrm{H}^1\left(\mathrm{S}_e, E\left[2^e\right]\right) & \longrightarrow & \mathrm{H}^1\left(\mathrm{S}_e, 2E\left[2^e\right]\right) \longrightarrow \ldots \end{array},$$

where the exact bottom row arises from applying group cohomology to the short exact sequence of abelian groups induced by multiplication by two

$$0 \to E\left[2\right] \xrightarrow{\hookrightarrow} E\left[2^e\right] \xrightarrow{[2]} 2E\left[2^e\right] \to 0.$$

Thus the required isomorphism follows from the triviality of $\mathrm{H}^0\left(\mathrm{S}_e, E\left[2^e\right]\right) = \left(2E\left[2^e\right]\right)^{\mathrm{S}_e} \cong \left(\left(2\mathbb{Z}/2^e\right)^2\right)^{\mathrm{S}_e}$, which holds by a similar invariance argument with $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right) \in \mathrm{S}_e$ as above. □

Next is a short analysis of the filtration of the kernels of the reduction maps $\sigma_d^e : \mathrm{S}_e \twoheadrightarrow \mathrm{S}_d$ for $e > 1$.

(3.2.21) **Lemma.** *Let* $e > 1$. *Then*

$$\left(\ker \sigma_1^e\right)^2 = \ker \sigma_2^e,$$

where $(-)^2$ *is the subgroup generated by the squares of all elements.*

Proof. This is an induction with two straightforward but tedious base cases $e = 2$ and $e = 3$ checked explicitly. If $e = 2$, an easy manipulation of congruence equations yields

$$\ker \sigma_1^2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{l} a, d \in \{1, 3\}, \\ b, c \in \{0, 2\}, \\ ad - bc \equiv 1 \mod 4 \end{array} \right\} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \;\middle|\; a, b, c \in \{0, 1\} \right\},$$

so $\left(\ker \sigma_1^2\right)^2 = 0 = \ker \sigma_2^2$ by definition. If $e = 3$, a further manipulation of congruence equations yields

$$\ker \sigma_1^3 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{l} a, d \in \{1, 3, 5, 7\}, \\ b, c \in \{0, 2, 4, 6\}, \\ ad - bc \equiv 1 \mod 8 \end{array} \right\} = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \;\middle|\; \begin{array}{l} a \in \{1, 3, 5, 7\}, \\ \begin{cases} b \in \{0, 2, 4, 6\}, & c \in \{0, 4\} \\ b \in \{0, 4\}, & c \in \{2, 6\} \end{cases} \end{array} \right\}$$
$$\cup \left\{ \begin{pmatrix} a & b \\ c & a + 4 \end{pmatrix} \;\middle|\; \begin{array}{l} a \in \{1, 3, 5, 7\}, \\ b, c \in \{2, 6\} \end{array} \right\},$$

$$\ker \sigma_2^3 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{l} a, d \in \{1, 5\}, \\ b, c \in \{0, 4\}, \\ ad - bc \equiv 1 \mod 8 \end{array} \right\} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 4\left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \;\middle|\; a, b, c \in \{0, 1\} \right\},$$

and it can also be verified that

$$\left(\ker \sigma_1^3\right)^2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix} \right\} = \ker \sigma_2^3.$$

Now assume the result for $e-1 \geq 3$. By the same manipulation as above,

$$\ker \sigma_{e-1}^e = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{l} a,d \in \left\{1, 2^{e-1}+1\right\}, \\ b,c \in \left\{0, 2^{e-1}\right\}, \\ ad - bc \equiv 1 \mod 2^e \end{array} \right\} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2^{e-1} \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \;\middle|\; a,b,c \in \{0,1\} \right\},$$

but $\left(2^{e-2}\right)^2$ becomes trivial in S_e since $e \geq 4$, so any matrix in $\ker \sigma_{e-1}^e$ can be written as

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2^{e-1} \begin{pmatrix} a & b \\ c & a \end{pmatrix} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2^{e-2} \begin{pmatrix} a & b \\ c & a \end{pmatrix} \right)^2 \in \left(\ker \sigma_1^e\right)^2,$$

giving the inclusion $\ker \sigma_{e-1}^e \leq \left(\ker \sigma_1^e\right)^2$. On the other hand, any matrix in S_e that becomes trivial in S_1 squares to also become trivial in S_2, so there is also an inclusion $\left(\ker \sigma_1^e\right)^2 \leq \ker \sigma_2^e$. Thus

$$\left(\ker \sigma_1^e\right)^2 / \ker \sigma_{e-1}^e = \left(\ker \sigma_1^e / \ker \sigma_{e-1}^e\right)^2 = \ker \sigma_2^e / \ker \sigma_{e-1}^e,$$

by the inductive hypothesis and the canonical isomorphism $\ker \sigma_d^{e-1} \cong \ker \sigma_d^e / \ker \sigma_{e-1}^e$, so a simple counting argument of cosets gives an equality $\left(\ker \sigma_1^e\right)^2 = \ker \sigma_2^e$. □

In particular, this says that any homomorphism from $\ker \sigma_1^e$ to a 2-torsion group contains $\ker \sigma_2^e$, so the restriction map $\mathrm{res} : \mathrm{H}^1\left(\ker \sigma_1^e, E\left[2\right]\right) \to \mathrm{H}^1\left(\ker \sigma_2^e, E\left[2\right]\right)$ is really the trivial map.

(3.2.22) **Lemma.** *Let $e > 1$. Then there is an isomorphism of abelian groups*

$$\mathrm{H}^1\left(\mathrm{S}_2, E\left[2\right]\right) \xrightarrow{\sim} \mathrm{H}^1\left(\mathrm{S}_e, E\left[2\right]\right).$$

Proof. The inflation-restriction exact sequence applied to $\mathrm{S}_e / \ker \sigma_2^e \cong \mathrm{S}_2$ yields

$$0 \to \mathrm{H}^1\left(\mathrm{S}_2, E\left[2\right]^{\ker \sigma_2^e}\right) \xrightarrow{\mathrm{inf}} \mathrm{H}^1\left(\mathrm{S}_e, E\left[2\right]\right) \xrightarrow{\mathrm{res}} \mathrm{H}^1\left(\ker \sigma_2^e, E\left[2\right]\right),$$

but $\ker \sigma_2^e$ clearly fixes $E\left[2\right] \cong \left(\mathbb{Z}/2\right)^2$, so the invariant subgroup $E\left[2\right]^{\ker \sigma_2^e}$ is $E\left[2\right]$. On the other hand, taking into account the filtration, this restriction map factors into a composition of two restriction maps

$$\mathrm{res} : \mathrm{H}^1\left(\mathrm{S}_e, E\left[2\right]\right) = \mathrm{H}^1\left(\ker \sigma_0^e, E\left[2\right]\right) \xrightarrow{\mathrm{res}_1} \mathrm{H}^1\left(\ker \sigma_1^e, E\left[2\right]\right) \xrightarrow{\mathrm{res}_2} \mathrm{H}^1\left(\ker \sigma_2^e, E\left[2\right]\right),$$

the second of which is trivial by Lemma 3.2.21. Thus the inflation map is the required isomorphism. □

It helps to reduce an arbitrary group $\mathrm{H}^1\left(\mathrm{S}_e, E\left[2^e\right]\right)$ down to $\mathrm{H}^1\left(\mathrm{S}_2, E\left[2\right]\right)$, since the latter can be reasonably computed by hand, which is achieved by considering the generators of S_2.

(3.2.23) **Lemma.** *Let $\xi \in \mathrm{H}^1\left(\mathrm{S}_2, E\left[2\right]\right)$ be a 1-cocycle such that $\xi\left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\right)$ and $\xi\left(\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\right)$ are both trivial. Then ξ is also trivial.*

Proof. It can be verified with an explicit computation that any matrix $M \in \mathrm{S}_2$ can be generated by products of powers of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, so the result can be acquired by induction. In particular, let $M = M_1 M_2$ be a decomposition into a product of two matrices $M_1, M_2 \in \mathrm{S}_2$ that are generated by strictly fewer total powers of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, and assume that $\xi\left(M_1\right)$ and $\xi\left(M_2\right)$ are both trivial. Then the crossed condition dictates that $\xi\left(M\right) = \xi\left(M_1\right) + M_1 \xi\left(M_2\right)$, so the result follows by the inductive hypothesis. □

While the elements $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{S}_2$ multiply to generate the whole group, they individually generate two cyclic subgroups within S_2, namely the upper and lower unitriangular matrix groups

$$\mathrm{U}_e \coloneqq \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Z}/2^e \right\}, \qquad \mathrm{L}_e \coloneqq \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Z}/2^e \right\},$$

equipped with the natural reduction modulo four maps $\upsilon_2^e : \mathrm{U}_e \twoheadrightarrow \mathrm{U}_2$ and $\tau_2^e : \mathrm{L}_e \twoheadrightarrow \mathrm{L}_2$, whose cohomology groups will serve as the final reduction. Note that the previous three results do not use the prevailing assumption that $\mathrm{S}_e \leq \mathrm{im}\, \rho_{E\left[2^e\right]}$, but the final result combines all of the previous results nonetheless.

(3.2.24) **Proposition.** *Let $e > 1$. Assume that $\mathrm{S}_e \leq \operatorname{im} \rho_{E[2^e]}$. Then*

$$Ш^1(K, E[2^e]) = 0.$$

Proof. By Lemma 3.2.18, it suffices to show that the induced restriction map

$$\mathrm{res}_{\mathrm{U}_e} \oplus \mathrm{res}_{\mathrm{L}_e} : \mathrm{H}^1(\mathrm{S}_e, E[2^e]) \to \mathrm{H}^1(\mathrm{U}_e, E[2^e]) \oplus \mathrm{H}^1(\mathrm{L}_e, E[2^e])$$

is injective. Combining Lemma 3.2.20 and Lemma 3.2.22 establishes isomorphisms of abelian groups

$$\mathrm{H}^1(\mathrm{S}_2, E[2]) \xrightarrow{\sim} \mathrm{H}^1(\mathrm{S}_e, E[2]) \xrightarrow{\sim} \mathrm{H}^1(\mathrm{S}_e, E[2^e]),$$

and analogous maps will now be constructed for the unitriangular matrix groups U_e and L_e as follows. As for the special linear group S_e, there is a canonical isomorphism of groups $\mathrm{U}_e / \ker \upsilon_2^e \cong \mathrm{U}_2$ by the first isomorphism theorem, and applying the inflation-restriction exact sequence to this yields

$$0 \to \mathrm{H}^1\left(\mathrm{U}_2, E[2]^{\ker \upsilon_2^e}\right) \xrightarrow{\inf} \mathrm{H}^1(\mathrm{U}_e, E[2]) \xrightarrow{\mathrm{res}} \mathrm{H}^1(\ker \upsilon_2^e, E[2]),$$

but $\ker \upsilon_2^e$, analogous to $\ker \sigma_2^e$, fixes $E[2] \cong (\mathbb{Z}/2)^2$, so the invariant subgroup $E[2]^{\ker \upsilon_2^e}$ is again $E[2]$. On the other hand, applying group cohomology to the short exact sequence of abelian groups

$$0 \to E[2] \xrightarrow{\hookrightarrow} E[2^e] \xrightarrow{[2]} 2E[2^e] \to 0,$$

yields a long exact sequence

$$\cdots \to \mathrm{H}^0(\mathrm{U}_e, E[2^e]) \xrightarrow{[2]} \mathrm{H}^0(\mathrm{U}_e, 2E[2^e]) \xrightarrow{\delta_0} \mathrm{H}^1(\mathrm{U}_e, E[2]) \xrightarrow{\phi} \mathrm{H}^1(\mathrm{U}_e, E[2^e]) \to \ldots.$$

However in this case, since $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \notin \mathrm{U}_e$, the same invariance argument fails, but it is still easy to see that

$$\mathrm{H}^0(\mathrm{U}_e, E[2^e]) = E[2^e]^{\mathrm{U}_e} \cong \left((\mathbb{Z}/2^e)^2\right)^{\mathrm{U}_e} \cong \mathbb{Z}/2^e \oplus 0,$$

$$\mathrm{H}^0(\mathrm{U}_e, 2E[2^e]) = (2E[2^e])^{\mathrm{U}_e} \cong \left((2\mathbb{Z}/2^e)^2\right)^{\mathrm{U}_e} \cong 2\mathbb{Z}/2^e \oplus 0,$$

so the first multiplication by two map is surjective, and it follows that the connecting homomorphism is the trivial map and the last map is injective. Completely analogously, there are similar constructions of this last monomorphism $\phi : \mathrm{H}^1(\mathrm{L}_e, E[2]) \hookrightarrow \mathrm{H}^1(\mathrm{L}_e, E[2^e])$ and the previous inflation map $\inf : \mathrm{H}^1(\mathrm{L}_2, E[2]) \hookrightarrow \mathrm{H}^1(\mathrm{L}_e, E[2])$ for L_e, which are again both injective. Combining all four of these monomorphisms with the isomorphisms for S_e establishes, by construction, a commutative diagram of abelian groups

$$\begin{array}{ccccc} \mathrm{H}^1(\mathrm{S}_2, E[2]) & \xrightarrow{\sim} & \mathrm{H}^1(\mathrm{S}_e, E[2]) & \xrightarrow{\sim} & \mathrm{H}^1(\mathrm{S}_e, E[2^e]) \\ \downarrow{\scriptstyle \mathrm{res}_2} & & \downarrow{\scriptstyle \mathrm{res}_e} & & \downarrow{\scriptstyle \mathrm{res}_{\mathrm{U}_e} \oplus \mathrm{res}_{\mathrm{L}_e}} \\ \mathrm{H}^1(\mathrm{U}_2, E[2]) \oplus \mathrm{H}^1(\mathrm{L}_2, E[2]) & \xrightarrow[\inf]{} & \mathrm{H}^1(\mathrm{U}_e, E[2]) \oplus \mathrm{H}^1(\mathrm{L}_e, E[2]) & \xrightarrow[\phi]{} & \mathrm{H}^1(\mathrm{U}_e, E[2^e]) \oplus \mathrm{H}^1(\mathrm{L}_e, E[2^e]) \end{array},$$

where the vertical restriction maps are induced by the obvious inclusion maps $\mathrm{U}_e \hookrightarrow \mathrm{S}_e$ and $\mathrm{L}_e \hookrightarrow \mathrm{S}_e$. Thus it suffices to show the injectivity of the left restriction map, after which the desired injection follows by the composition of all of these maps, but this is exactly the content of Lemma 3.2.23. □

The results of this subsection can now be summarised as follows.

(3.2.25) **Corollary.** *Assume that $\mathrm{SL}_2(\mathbb{Z}/p^e) \leq \operatorname{im} \rho_{E[p^e]}$. Then*

$$Ш^1(K, E[p^e]) = 0.$$

Proof. This follows immediately from Proposition 3.2.17, Proposition 3.2.19, and Proposition 3.2.24. □

Remark. Using similar cohomological methods, one can obtain various frequently applicable criteria for the vanishing of $Ш^1(K, M)$ for other finite $\mathrm{Gal}\left(\overline{K}/K\right)$-modules M [PR12, Proposition 3.3], so this result is itself unsurprising. There is also an analogue proven for elliptic curves defined over function fields under a slightly different hypothesis, namely that $\operatorname{im} \rho_{E[p^e]}$ needs to be cyclic, but this assumption, as with the above assumption, remains applicable to almost all elliptic curves [BKLPR15, Proposition 6.1].

3.2.4 Direct summands and strong metabolicity

This subsection finishes the proof that the two Lagrangian submodules $\operatorname{im}\kappa$ and $\operatorname{im}\lambda$ are often direct summands of $\mathrm{H}^1(\mathbb{A}_K, E[n])$, using purely group theoretic techniques. The proof combines the arguments in the paper on modelling distributions of elliptic curves by Bhargava, Kane, Lenstra, Poonen, and Rains [BKLPR15], and in the paper on Selmer groups and adelic cohomology by Gillibert, Gillibert, Gillibert, and Ranieri [GGGR19]. Several well-known results taken from Fuchs's book on infinite abelian groups [Fuc70] will be admitted without proof, as they are relatively straightforward but the technical arguments used are irrelevant for immediate elucidation. The first of these generalises the structure theorem of finite abelian groups to arbitrary torsion groups, and is often called **Prüfer's first theorem** in the literature.

(3.2.26) **Theorem** ([Fuc70, Theorem III.17.2])**.** *An n-torsion abelian group is a direct sum of cyclic groups.*

Assuming this statement, $\operatorname{im}\kappa$ is easily a direct summand, noting that $\mathbb{Z}/n$-modules are synonymous with n-torsion abelian groups. For each place $v \in \mathcal{V}_K$, again write κ_v to denote the local injection.

(3.2.27) **Proposition.** *The submodule $\operatorname{im}\kappa_v$ is a direct summand.*

Proof. Theorem 3.2.26, assuming the structure theorem, establishes a decomposition of abelian groups

$$\mathrm{H}^1(K_v, E)[n] \cong (\mathbb{Z}/p_1^{e_1})^{n_1} \oplus \cdots \oplus (\mathbb{Z}/p_k^{e_k})^{n_k}, \qquad n_i \in \mathbb{N}^+,$$

for distinct prime powers $p_i^{e_i} \in \mathbb{N}^+$. Then for each $p_i^{e_i}$, there is a row-exact diagram of abelian groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K_v)/p_i^{e_i} & \xrightarrow{\kappa_v'} & \mathrm{H}^1(K_v, E[p_i^{e_i}]) & \xrightarrow{\mu_v'} & \mathrm{H}^1(K_v, E)[p_i^{e_i}] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle\phi} & & \downarrow & & \\ 0 & \longrightarrow & E(K_v)/n & \xrightarrow[\kappa_v]{} & \mathrm{H}^1(K_v, E[n]) & \xrightarrow[\mu_v]{} & \mathrm{H}^1(K_v, E)[n] & \longrightarrow & 0 \end{array},$$

arising from including the respective local Kummer sequences. In particular, any 1-cocycle $\xi \in \mathrm{H}^1(K_v, E)[n]$ with order exactly $p_i^{e_i}$ belongs to some $\mathrm{H}^1(K_v, E)[p_i^{e_i}] \cong (\mathbb{Z}/p_i^{e_i})^{n_i}$, which by the surjectivity of μ_v' lifts to some 1-cocycle $\xi' \in \mathrm{H}^1(K_v, E[p_i^{e_i}])$ with order also exactly $p_i^{e_i}$, since it is also a $p_i^{e_i}$-torsion group. Applying the map ϕ sends ξ' to a 1-cocycle $\phi(\xi') \in \mathrm{H}^1(K_v, E[n])$ with order dividing $p_i^{e_i}$, but the commutativity of the right square ensures that $\mu_v(\phi(\xi')) = \xi$ and $\phi(\xi')$ has order exactly $p_i^{e_i}$. Thus this defines a partial section $\mathrm{H}^1(K_v, E)[n] \to \mathrm{H}^1(K_v, E[n])$ that glues across all $p_i^{e_i}$ to construct a well-defined section of μ_v, so the bottom short exact sequence splits as a direct sum decomposition $\mathrm{H}^1(K_v, E[n]) \cong \operatorname{im}\kappa_v \oplus \mathrm{H}^1(K_v, E)[n]$. □

Remark. The proof of Proposition 3.2.27 is irrespective of locality, so it generalises to arbitrary Kummer sequences, and indeed to a very general family of Kummer-like exact sequences [GG18, Theorem 1.1].

The fact that $\operatorname{im}\kappa$ is a direct summand follows immediately.

(3.2.28) **Corollary.** *The submodule $\operatorname{im}\kappa$ is a direct summand.*

Proof. This follows by repeatedly applying Proposition 3.2.27 to the adelic Kummer sequence. □

Proving that $\operatorname{im}\lambda$ is also a direct summand is slightly more involved, starting with the notion of a **pure subgroup** $A \subseteq B$ of abelian group, which says that $mA = A \cap mB$ for any $m \in \mathbb{N}^+$. This will be relevant only to quote two useful results abstractly characterising images of monomorphisms.

(3.2.29) **Lemma** ([Fuc70, Theorems V.28.2 and V.29.1(c)])**.** *Let $\phi : A \hookrightarrow B$ be a monomorphism of abelian groups.*

1. *$\operatorname{im}\phi \subseteq B$ is a direct summand if $\operatorname{im}\phi \subseteq B$ is pure and $B/\operatorname{im}\phi$ is a direct sum of cyclic groups.*
2. *$\operatorname{im}\phi \subseteq B$ is pure if and only if the induced maps $\phi_m : A/m \to B/m$ are injective for all $m \in \mathbb{N}^+$.*

The latter injectivity condition is equivalent to preserving divisibility of elements by any $m \in \mathbb{N}^+$ upon retracting from B to A, a step that will be utilised in the upcoming abstract diagram chasing arguments. Considering these two statements in the case of n-torsion abelian groups instead, this divisibility-preserving condition turns out to be necessary and sufficient for images of monomorphisms to be direct summands.

(3.2.30) **Lemma.** *Let $\phi : A \hookrightarrow B$ be a monomorphism of n-torsion abelian groups. Then $\operatorname{im}\phi \subseteq B$ is a direct summand if and only if the induced maps $\phi_m : A/m \to B/m$ are injective for all $m \mid n$.*

Proof. Assume that $\operatorname{im}\phi \subseteq B$ is a direct summand, so there is an internal direct sum decomposition $B = \operatorname{im}\phi \oplus C$ for some subgroup $C \subseteq B$. Let $m \mid n$, and let $a \in A$ be an element such that $\phi_m(a) = 0$ in B/m, so $\phi(a) = mb$ for some element $b \in B$. By assumption, there are elements $a' \in A$ and $c \in C$ such that $b = \phi(a') + c$, so $\phi(a) = mb = m\phi(a') + mc$. Then $\phi(a - ma') = \phi(a) - m\phi(a') = mc \in \operatorname{im}\phi \cap C = 0$, so $a = ma' \in mA$ by injectivity of ϕ. Hence $a = 0$ in A/m, so ϕ_m is injective. Conversely, assume that ϕ_m is injective for all $m \mid n$, which is equivalent to all $m \in \mathbb{N}^+$ by virtue of n-torsion. Then $\operatorname{im}\phi \subseteq B$ is pure by Lemma 3.2.29.2, and since $B/\operatorname{im}\phi$ is clearly n-torsion, it is also direct sum of cyclic groups by Theorem 3.2.26. Thus $\operatorname{im}\phi \subseteq B$ is a direct summand by Lemma 3.2.29.1. □

(3.2.31) **Lemma.** *Let*

$$\begin{array}{ccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\chi} & & \downarrow{\scriptstyle\psi} \\ A' & \xrightarrow[\alpha']{} & B' & \xrightarrow[\beta']{} & C' \end{array}$$

be a row-exact diagram of abelian groups, such that B' is n-torsion, $\operatorname{im}\beta = C[n]$, and the induced maps

$$\phi_m : A/m \to A'/m, \qquad \alpha'_m : A'/m \to B'/m, \qquad \psi_m : C/m \to C'/m$$

are injective for all $m \mid n$. Then the induced maps $\chi_m : B/m \to B'/m$ are injective for all $m \mid n$.

Proof. Let $m \mid n$, and let $b \in B$ be an element such that $\chi_m(b) = 0$ in B'/m, so $\chi(b) = mb'$ for some element $b' \in B'$. Commutativity of the right square yields $\psi(\beta(b)) = \beta'(\chi(b)) = \beta'(mb') = m\beta'(b')$, so $\beta(b) = mc$ for some element $c \in C$ by injectivity of ψ_m. Since B' is n-torsion, $\chi(nb/m) = n\chi(b)/m = nb' = 0$, so $nb/m = 0$ by injectivity of χ. Then $nc = n\beta(b)/m = \beta(nb/m) = 0$, so $c \in C[n] = \operatorname{im}\beta$, and hence $c = \beta(e)$ for some element $e \in B$. Now $\beta(b - me) = \beta(b) - m\beta(e) = 0$, so $b - me \in \ker\beta = \operatorname{im}\alpha$, and hence $b - me = \alpha(a)$ for some element $a \in A$. Commutativity of the left square yields $\alpha'(\phi(a)) = \chi(\alpha(a)) = \chi(b - me) = \chi(b) - m\chi(e) = m(b' - \chi(e))$, so $a = md$ for some element $d \in A$ by injectivity of ϕ_m and α'_m. Thus $b = \alpha(a) + me = m(\alpha(d) + e) = 0$ in B/m, so χ_m is injective. □

Returning to the discussion of $\operatorname{im}\lambda$, the various conditions in Lemma 3.2.31 can be verified for the Kummer diagram, but doing so will require an assumption on $Ш^1(K, E[m])$ for each $m \mid n$.

(3.2.32) **Proposition.** *Let $Ш^1(K, E[m])$ be trivial for all $m \mid n$. Then the submodule $\operatorname{im}\lambda$ is a direct summand.*

Proof. For each $m \mid n$, consider the long row-exact diagram of cohomology groups

$$\begin{array}{ccccccccc} \dots & \longrightarrow & E(K) & \xrightarrow{\alpha} & \mathrm{H}^1(K, E[m]) & \xrightarrow{\beta} & \mathrm{H}^1(K, E) & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\chi} & & \downarrow{\scriptstyle\psi} & & \\ \dots & \longrightarrow & \prod_{v\in\mathcal{V}_K} E(K_v) & \xrightarrow[\alpha']{} & \prod_{v\in\mathcal{V}_K} \mathrm{H}^1(K_v, E[m]) & \xrightarrow[\beta']{} & \prod_{v\in\mathcal{V}_K} \mathrm{H}^1(K_v, E) & \longrightarrow & \dots \end{array},$$

which induces the Kummer diagram if $m = n$, where each $\mathrm{H}^1(K_v, E[n])$ is n-torsion and $\operatorname{im}\beta = \mathrm{H}^1(K, E)[n]$. Zooming in at the first two connecting homomorphisms furnishes commutative squares of abelian groups

$$\begin{array}{ccc} E(K)/m & \xhookrightarrow{\alpha} & \mathrm{H}^1(K, E[m]) \\ {\scriptstyle\phi_m}\downarrow & & \downarrow{\scriptstyle\chi} \\ \prod_{v\in\mathcal{V}_K} E(K_v)/m & \xhookrightarrow[\alpha']{} & \prod_{v\in\mathcal{V}_K} \mathrm{H}^1(K_v, E[m]) \end{array}, \qquad \begin{array}{ccc} \mathrm{H}^1(K, E)/m & \xhookrightarrow{\delta_1} & \mathrm{H}^2(K, E[m]) \\ {\scriptstyle\psi_m}\downarrow & & \downarrow{\scriptstyle\chi'} \\ \prod_{v\in\mathcal{V}_K} \mathrm{H}^1(K_v, E)/m & \xhookrightarrow[\delta_1']{} & \prod_{v\in\mathcal{V}_K} \mathrm{H}^2(K_v, E[m]) \end{array}.$$

By Tate's global duality for $E[m]$, the assumption establishes the triviality of both $Ш^1(K, E[m]) = \ker\chi$ and $Ш^2(K, E[m]) = \ker\chi'$, so the induced maps ϕ_m and ψ_m are injective. Corollary 3.2.28 says that $\operatorname{im}\alpha'$ is a direct summand, which by Lemma 3.2.30 also gives the injectivity of α'_m. Thus the conditions of Lemma 3.2.31 are satisfied, and the result follows by the converse of Lemma 3.2.30. □

Remark. The result that $\operatorname{im}\lambda$ is a direct summand was originally a conjecture, and was thought to have no counterexamples [BKLPR15, Conjecture 6.9]. This is false [GGGR19, Theorem 1.4], but it is also possible to construct an explicit family of elliptic curves that always satisfies this [GGGR19, Corollary 1.3].

Fortunately, the assumption in Proposition 3.2.32 is satisfiable, at least for the purposes of proving the main result, since $Ш^1(K, E[p^e])$ is trivial for a prime power $p^e \in \mathbb{N}^+$ whenever $\mathrm{SL}_2(\mathbb{Z}/p^e) \leq \operatorname{im}\rho_{E[p^e]}$, by Corollary 3.2.25. It remains to justify that the latter assumption is a mild one.

3.2.5 Ubiquity of surjective Galois representations

This final short subsection elucidates why the assumption $\mathrm{SL}_2(\mathbb{Z}/n) \leq \operatorname{im}\rho_{E[n]}$ holds for almost all elliptic curves in $\mathcal{E}(K)$, for a fixed $n \in \mathbb{N}^+$. In fact, the stronger statement that $\rho_{E[n]}$ is usually surjective is also true, given a generic elliptic curve in $\mathcal{E}(K)$, which trivialises the assumption. This is really a consequence of **Hilbert's irreducibility theorem** and the theory of **modular curves**, but to avoid a potentially huge detour to both areas, the relevant results will be stated without proof. In its simplest form, Hilbert's irreducibility theorem says that an irreducible polynomial $f \in \mathbb{Q}[X, Y]$ remains irreducible after specialising X to some $x \in \mathbb{Q}$ and obtaining a polynomial $f(x, -) \in \mathbb{Q}[Y]$. This has since been extensively reformulated in the language of algebraic geometry, and a relevant consequence can be stated in terms of Galois groups.

(3.2.33) **Theorem** ([Zyw10, Theorem 1.1]). *Let $f \in F(X)[Y_1, \ldots, Y_n]$ be an irreducible polynomial, and let F_f be the splitting field of f over $F(X)$. Then for almost all $x \in F$ such that $f(x, -) \in F[Y_1, \ldots, Y_n]$ is separable, specialisation of X to x induces an isomorphism of Galois groups*

$$\mathrm{Gal}(F_f/F(X)) \cong \mathrm{Gal}\left(F_{f(x,-)}/F\right),$$

where $F_{f(x,-)}$ is the splitting field of $f(x, -)$ over F.

Remark. Hilbert's irreducibility theorem admits many applications in number theory, such as the partial resolution of the inverse Galois problem via polynomials in $\mathbb{Q}(t)$ under the above formulation [Ser89, Section 9.3]. Other applications within elliptic curves include the construction of elliptic curves with large rank, and showing that almost all elliptic curves have trivial torsion subgroups, the latter of which also involves the theory of modular curves [BKLPR15, Lemma 5.7]. Note that the infinitude and density of the specialisations can also be formulated in terms of Hilbert sets or thin sets [Ser89, Proposition 9.2.2].

The remaining ingredient arises as a result on elliptic curves defined over a transcendental extension of K, which is a corollary of showing that $\mathrm{Gal}(\mathbb{C}(T)(E[n])/\mathbb{C}(T)) \cong \mathrm{SL}_2(\mathbb{Z}/n)$. The proof itself builds the theory of modular curves and elliptic functions, and will bring the discussion too far afield.

(3.2.34) **Lemma** ([CSS97, Section III.1.1]). *Let E be an elliptic curve defined over the field of rational functions $\mathbb{Q}(T)$ with* j*-invariant T. Then the modulo n Galois representation induces an isomorphism of groups*

$$\mathrm{Gal}(\mathbb{Q}(T)(E[n])/\mathbb{Q}(T)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}/n).$$

Assuming these two results, a brief sketch of the proof goes as follows.

(3.2.35) **Proposition.** *The modulo n Galois representation is surjective for almost all elliptic curves $E \in \mathcal{E}(K)$.*

Proof sketch. Pick a generic elliptic curve defined over $K(T)$, and apply the number field analogue of Lemma 3.2.34 to relate the Galois group of $K(T)(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n)$. Then use its n-division polynomial characterisation to construct irreducible polynomials in $K(T)[X, Y]$, and obtain the required isomorphism with the Galois group of $K(E[n])$ to almost all specialisations of T by Theorem 3.2.33. □

Remark. This result is heuristically expected, since by **Serre's open image theorem**, the modulo p Galois representations of elliptic curves without complex multiplication are surjective for all but finitely many primes $p \in \mathbb{N}^+$ [Sil09, Theorem III.7.9]. An explicit elliptic curve can also be constructed with surjective modulo n Galois representations for all odd $n \in \mathbb{N}^+$ not divisible by its conductor [Ser89, Section 10.4]. Furthermore, using sieve-theoretic techniques, one can obtain an asymptotic upper bound on the decreasing proportion of elliptic curves where the criterion $\mathrm{SL}_2(\mathbb{Z}/p^e) \leq \operatorname{im}\rho_{E[p^e]}$ fails [Zyw18, Proposition 5.6]. In general, images of modulo n Galois representations are usually quite large, and any further discussion on this well-studied subject would be too much to fit in this remark.

Thus the initial assumption is justified by Proposition 3.2.35, and the proof of Theorem 3.2.1 is complete.

3.3 Model for Selmer groups

Instead of tackling Conjecture 1.1.1 directly, Theorem 3.2.1 suggests a probabilistic model based on the idea that a p^e-Selmer group, for some prime power $p^e \in \mathbb{N}^+$, is almost always a natural intersection of two Lagrangian direct summands in an ambient metabolic quadratic $\mathbb{Z}/p^e$-module of infinite rank. On the other hand, the resulting distribution of such a pseudo p^e-Selmer group could be attained more simply by considering an ambient metabolic quadratic $\mathbb{Z}/p^e$-module of finite rank, hence utilising counting tricks in finitary combinatorics, then taking the limiting average as the rank tends to infinity. Recall that $(\mathbb{Z}/p^e)^{2n}$, for any $n \in \mathbb{N}^+$, equipped with the standard hyperbolic quadratic form

$$\begin{array}{rccc} \omega_{(\mathbb{Z}/p^e)^{2n}} & : & (\mathbb{Z}/p^e)^{2n} & \longrightarrow & \mathbb{Z}/p^e \\ & & (x_1, \ldots, x_n, y_1, \ldots, y_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} x_i y_i \end{array},$$

is a metabolic quadratic $\mathbb{Z}/p^e$-module, called the standard hyperbolic $\mathbb{Z}/p^e$-module, with a Lagrangian direct summand $(\mathbb{Z}/p^e)^n \oplus 0^n$. Thus the aim of this section is to prove the following heuristic.

(3.3.1) **Theorem.** *Let $L_1, L_2 \in \mathrm{LG}\,(\mathbb{Z}/p^e)^{2n}$ be Lagrangian direct summands chosen uniformly at random. Then*

$$\lim_{n\to\infty} \mathbb{E}\left[\#\left(L_1 \cap L_2\right)\right] = \sigma_1\left(p^e\right),$$

where $\sigma_1 : \mathbb{N}^+ \to \mathbb{N}$ is the sum of divisors function.

The only missing piece here is the mysterious set $\mathrm{LG}\,(\mathbb{Z}/p^e)^{2n}$ and its associated measure, but this will be clarified in the next short subsection, and the proof itself proceeds in three steps spanning across the following three subsections. By first building up some pseudo-linear algebraic results, the size of the relevant sample space can be computed, which is then used to deduce the average size of the pseudo p^e-Selmer group. Finally, a potential flaw with the model is justified in the final subsection. The overall argument is adapted from the paper on modelling distributions of elliptic curves by Bhargava, Kane, Lenstra, Poonen, and Rains [BKLPR15], with an alternative, more elementary, proof for a key result on the size of the sample space taken from the paper on MDS codes by Dougherty, Kim, and Kulosman [DKK08]. Throughout this section, R will be one of the finite local rings $\mathbb{F}_p$ or $\mathbb{Z}/p^e$ for a prime power $p^e \in \mathbb{N}^+$, and M will be a free R-module, with $N \leq M$ denoting that N is a direct summand of M, while $k, l, m, n \in \mathbb{N}$ will be arbitrary.

3.3.1 Lagrangian Grassmannians

Consider the sample space of all Lagrangian direct summands of a metabolic quadratic R-module M.

Definition. The **Lagrangian Grassmannian** $\mathrm{LG}\,(M)$ is the space of Lagrangian direct summands of M.

Remark. In fact, the Lagrangian Grassmannian of a metabolic quadratic R-module of rank $2n$, or sometimes referred to as the orthogonal Grassmannian, is a functor representable by a smooth projective scheme over $\mathbb{Z}$ of relative dimension $\frac{1}{2}n\left(n-1\right)$ [BKLPR15, Proposition 4.4], a fact useful in a later remark.

A general Lagrangian Grassmannian can be equipped with a canonical measure, which induces a distribution to sample Lagrangian direct summands from, but, unlike the case of sampling elliptic curves, is more complicated to describe. Fortunately, in the relevant case of the finite $\mathbb{Z}/p^e$-module $(\mathbb{Z}/p^e)^{2n}$, there is an alternative construction by simply considering the discrete uniform distribution on $\mathrm{LG}\,(\mathbb{Z}/p^e)^{2n}$, so relevant notions like the average size of the intersection $L_1 \cap L_2$ can be defined by

$$\mathbb{E}\left[\#\left(L_1 \cap L_2\right)\right] \coloneqq \left(\#\,\mathrm{LG}\,(\mathbb{Z}/p^e)^{2n}\right)^{-2} \sum_{L_1, L_2 \in \mathrm{LG}(\mathbb{Z}/p^e)^{2n}} \#\left(L_1 \cap L_2\right),$$

which is the uniform average of all possible intersections. It now makes sense to choose elements uniformly at random from $\mathrm{LG}\,(\mathbb{Z}/p^e)^{2n}$, and this will be the prevailing assumption from now on.

Remark. There is a perhaps more canonical measure to equip on the $\mathbb{Z}_p$-scheme of finite type $\mathrm{LG}\,(\mathbb{Z}_p)^{2n}$ that considers $\mathrm{LG}\,(\mathbb{Z}/p^e)^{2n}$ for all $p^e \in \mathbb{N}^+$ at once [BKLPR15, Proposition 2.1], which is constructed as a generalisation of the normalised Haar measure on orthogonal groups in the usual Grassmannian variety.

3.3.2 Combinatorial linear algebra

This subsection details several results generalising linear algebra to free $\mathbb{Z}/p^e$-modules, starting with the formalisation of the notion that free submodules are indeed equivalent to internal direct summands, as per the reasoning in the first section. Statements will be made as general as provably possible, so there is no assumption that M has to be $(\mathbb{Z}/p^e)^{2n}$, nor that it is equipped with any quadratic form.

(3.3.2) **Lemma.** *Let M be a free $\mathbb{Z}/p^e$-module of finite rank, and let $N \subseteq M$ be a submodule. Then N is free if and only if $N \leq M$ is a direct summand.*

Proof. If N is a free $\mathbb{Z}/p^e$-module of finite rank, it is isomorphic to a finite direct product of the base ring $\mathbb{Z}/p^e$, which is injective as a module over itself, so N is itself injective, and hence being a submodule of M is equivalent to being a internal direct summand of M. Conversely, if N is an internal direct summand of M, it is also a free $\mathbb{Z}/p^e$-module, as a consequence of Nakayama's lemma applied to the local ring $\mathbb{Z}/p^e$. □

(3.3.3) **Proposition.** *Let M be a free $\mathbb{Z}/p^e$-module of rank m, and let $N \leq M$ be a direct summand of rank k. Then there is a bijective correspondence of $\mathbb{Z}/p^e$-modules*

$$\begin{array}{ccc} \{L \leq M \mid N \leq L\} & \leftrightsquigarrow & \{L/N \leq M/N\} \\ L & \longmapsto & L/N \end{array}.$$

Proof. The fourth isomorphism theorem gives a bijective correspondence of $\mathbb{Z}/p^e$-modules

$$\begin{array}{ccc} \{L \subseteq M \mid N \subseteq L\} & \leftrightsquigarrow & \{L/N \subseteq M/N\} \\ L & \longmapsto & L/N \end{array},$$

so, by Lemma 3.3.2, it suffices to prove that L is free precisely when L/N is free. As per the previous argument, the assumption on N makes it injective, so the short exact sequence of $\mathbb{Z}/p^e$-modules

$$0 \to N \to L \to L/N \to 0$$

splits as a direct sum decomposition $L \cong N \oplus L/N$. Applying Nakayama's lemma again shows that the freeness of L/N is equivalent to its projectivity, which holds whenever L is free by this isomorphism, while the converse follows immediately by assumption, so the bijective correspondence follows. □

(3.3.4) **Corollary.** *Let M be a free $\mathbb{Z}/p^e$-module of rank m, and let $N \leq M$ be a direct summand of rank k. Then M/N is a free $\mathbb{Z}/p^e$-module of rank $m - k$.*

Proof. Setting $L = M$ in the proof of Proposition 3.3.3 and applying the same argument for M/N proves that it is free, while a simple finite counting argument verifies its rank to be exactly $m - k$. □

Remark. The proof really only uses the locality and self-injectivity of $\mathbb{Z}/p^e$, so the same statement would generalise to free modules over local self-injective rings, which are admittedly rather rare.

Next is a result arising as a variant of a usual combinatorial argument accounting for zero divisors.

(3.3.5) **Lemma.** *Let M be a free $\mathbb{Z}/p^e$-module of rank m, and let $x_1, \ldots, x_k \in M$ be k linearly independent elements. Then*

$$\#\langle \mathfrak{m}M, x_1, \ldots, x_k \rangle = p^{(e-1)m+k},$$

where $\mathfrak{m} \coloneqq p\mathbb{Z}/p^e \subseteq \mathbb{Z}/p^e$ is the unique maximal ideal.

Proof. This primarily relies on the fact that, by tensoring with $\mathbb{F}_p$ over $\mathbb{Z}/p^e$, Nakayama's lemma naturally lifts a basis of the m-dimensional $\mathbb{F}_p$-vector space $M/\mathfrak{m}M$ to a basis of m linearly independent elements of the free $\mathbb{Z}/p^e$-module M, and vice versa. Since the ideal $\langle x_1, \ldots, x_k \rangle$ is free, it is an internal direct summand of M by Lemma 3.3.2, so there is an internal direct sum decomposition $M = \langle x_1, \ldots, x_k \rangle \oplus \langle x_{k+1}, \ldots, x_m \rangle$ for some $m - k$ linearly independent elements $x_{k+1}, \ldots, x_m \in M$. Thus it is easy to see that

$$\#\langle x_1, \ldots, x_k \rangle \oplus \#\mathfrak{m}\langle x_{k+1}, \ldots, x_m \rangle = (\#(\mathbb{Z}/p^e))^k (\#\mathfrak{m})^{m-k} = (p^e)^k \left(p^{e-1}\right)^{m-k} = p^{(e-1)m+k},$$

so the result follows. □

(3.3.6) **Proposition.** *Let M be a free $\mathbb{Z}/p^e$-module of rank m. Then*

$$\#\left\{L \leq M \;\middle|\; \mathrm{rk}_{\mathbb{Z}/p^e} L = l\right\} = \binom{m}{l}_{p^e} \coloneqq \begin{cases} p^{(e-1)(m-l)l} \prod_{i=0}^{l-1} \frac{p^m - p^i}{p^l - p^i} & m \geq l \\ 0 & m < l \end{cases}.$$

Proof. It suffices to count the number of ways to pick l linearly independent elements in M that generate a free submodule L, and divide this quantity by the number of ways to generate the same free submodule, ensuring at each step that the element chosen contains at least one component outside the unique maximal ideal $\mathfrak{m} \coloneqq \langle p \rangle \subseteq \mathbb{Z}/p^e$ so as to generate the complete free submodule. Now there are always p^{em} elements to choose from, but $p^{(e-1)m+k}$ of these are either zero divisors in $\mathfrak{m}$ or are linearly dependent after k choices are made, by Lemma 3.3.5. Thus the coefficients compute to be exactly

$$\binom{m}{l}_{p^e} = \frac{\prod_{i=0}^{l-1} \left(p^{em} - p^{(e-1)m+i}\right)}{\prod_{i=0}^{l-1} \left(p^{el} - p^{(e-1)l+i}\right)} = \frac{p^{(e-1)ml} \prod_{i=0}^{l-1} \left(p^m - p^i\right)}{p^{(e-1)l^2} \prod_{i=0}^{l-1} \left(p^l - p^i\right)} = p^{(e-1)(m-l)l} \prod_{i=0}^{l-1} \frac{p^m - p^i}{p^l - p^i},$$

whenever $m \geq l$, and clearly zero otherwise. □

Remark. This set of coefficients is a generalisation of the usual **Gaussian p-binomial coefficients** in combinatorics, which omits the left factor when $e = 1$, and counts the number of l-dimensional subspaces of an m-dimensional $\mathbb{F}_p$-vector space in the usual Grassmannian variety. This also further generalises, by simply replacing p with a prime power $q \in \mathbb{N}^+$, to free modules over Galois rings $(\mathbb{Z}/q)[X] / \langle f(X) \rangle$, for any monic irreducible polynomial $f(X) \in (\mathbb{Z}/q)[X]$ of degree e [DKK08, Theorem 3.7].

(3.3.7) **Corollary.** *Let M be a free $\mathbb{Z}/p^e$-module of rank m, and let $N \leq M$ be a direct summand of rank k. Then*

$$\#\left\{L \leq M \;\middle|\; \mathrm{rk}_{\mathbb{Z}/p^e} L = l,\ N \leq L\right\} = \binom{m-k}{l-k}_{p^e}.$$

Proof. This follows immediately from Corollary 3.3.4 and Proposition 3.3.6. □

Now are several results on metabolic quadratic $\mathbb{Z}/p^e$-modules and Lagrangian direct summands.

(3.3.8) **Lemma.** *Let M be a quadratic $\mathbb{Z}/p^e$-module of rank m, and let $N \leq M$ be totally isotropic direct summand of rank k. Then $N^\perp$ is a free $\mathbb{Z}/p^e$-module of rank $m - k$.*

Proof. Composing the pairing isomorphism $M \xrightarrow{\sim} M^\star$ and the map $M^\star \to N^\star$ dual to the inclusion map $N \hookrightarrow M$ furnishes a short exact sequence of $\mathbb{Z}/p^e$-modules

$$0 \to N^\perp \to M \to N^\star \to 0,$$

where $N^\perp$ fits into the sequence by definition. Since $N^\star \cong N$ is a free of rank k, it is projective, so the sequence splits as a direct sum decomposition $M \cong N^\perp \oplus N^\star$. Thus $N^\perp$ is projective over a local ring $\mathbb{Z}/p^e$, and hence free of rank $m - k$, again as a consequence of Nakayama's lemma. □

(3.3.9) **Proposition.** *Let M be a metabolic quadratic $\mathbb{Z}/p^e$-module of rank m, let $L \in \mathrm{LG}(M)$ be a Lagrangian direct summand, and let $N \leq M$ be a totally isotropic direct summand of rank k. Then the free $\mathbb{Z}/p^e$-module $N^\perp/N$, equipped with the quadratic form*

$$\begin{array}{rccc} \omega_{N^\perp/N} & : & N^\perp/N & \longrightarrow & \mathbb{Z}/p^e \\ & & x + N & \longmapsto & \omega_M(x) \end{array},$$

is a metabolic quadratic $\mathbb{Z}/p^e$-module of rank $m - 2k$, with a Lagrangian direct summand $\pi_N(L)$, where

$$\begin{array}{rccc} \pi_N & : & \mathrm{LG}(M) & \longrightarrow & \mathrm{LG}\left(N^\perp/N\right) \\ & & L & \longmapsto & \left(L \cap N^\perp + N\right)/N \end{array}.$$

Thus $\pi_N : \mathrm{LG}(M) \to \mathrm{LG}\left(N^\perp/N\right)$ is surjective and induces a bijective correspondence of spaces

$$\begin{array}{rccc} \{L \in \mathrm{LG}(M) \mid N \leq L\} & \leftrightsquigarrow & \mathrm{LG}\left(N^\perp/N\right) \\ L & \longmapsto & L/N \end{array}.$$

Proof. Assuming that the prior statements are true, the bijective correspondence follows immediately from Proposition 3.3.3 and the construction of the quadratic form, while the freeness of $N^\perp/N$ and its rank follows immediately from Corollary 3.3.4 and Lemma 3.3.8. Now it remains to verify that the induced map $\omega_{N^\perp/N} : N^\perp/N \to \mathbb{Z}/p^e$ is well-defined, that it is a non-degenerate quadratic form, and that the induced map $\pi_N : \mathrm{LG}(M) \to \mathrm{LG}\left(N^\perp/N\right)$ is well-defined in the sense that $\pi_N(L)$ is a Lagrangian direct summand, but all of these hold by construction through reducing the corresponding properties to M and noting the total isotropy of $L = L^\perp$. For instance, whenever $x, y \in N^\perp$ are elements such that $x - y \in N$, then

$$\omega_{N^\perp/N}(x+N) = \omega_M(x) = \omega_M(x-y) + \omega_M(y) = \omega_M(y) = \omega_{N^\perp/N}(y+N),$$

by the definition of orthogonal complements, so $\omega_{N^\perp/N}$ is well-defined. □

Remark. The same statement is clearly also true for any choice of quadratic form.

(3.3.10) **Corollary.** *Let M be a quadratic $\mathbb{Z}/p^e$-module of rank m, and let $L \in \mathrm{LG}(M)$ be a Lagrangian direct summand. Then m is even, and L is a free $\mathbb{Z}/p^e$-module of rank $\frac{1}{2}m$.*

Proof. This follows immediately from Lemma 3.3.8 and the maximality of L. □

3.3.3 Sizes of Lagrangian Grassmannians

The aim of this subsection will be to compute the size of the Lagrangian Grassmannian $\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n}$, with detailed calculations on the particular case of $\mathrm{LG}\left(\mathbb{F}_p\right)^{2n}$. In the latter case, the $\mathbb{F}_p$-module of rank $2n$ becomes synonymous to the $2n$-dimensional $\mathbb{F}_p$-vector space, and all submodules, or simply referred to as subspaces, are trivially free direct summands, so computations are easier. The proof will be a slightly long-winded induction, where the base case is $n = 1$ and can be counted by explicit elimination.

(3.3.11) **Proposition.**

$$\#\,\mathrm{LG}\left(\mathbb{F}_p\right)^2 = 2.$$

Proof. Let $L \subseteq \mathbb{F}_p^2$ be a Lagrangian subspace, and let $(x_1, x_2) \in \mathbb{F}_p^2$ and $(y_1, y_2) \in L$ be two arbitrary vectors. The condition that $\langle (x_1, x_2), (y_1, y_2) \rangle_{\mathbb{F}_p^{2n}} = 0$ is simply $(x_1 + y_1)(x_2 + y_2) = x_1x_2 + y_1y_2$, which is equivalent to $x_1y_2 + y_1x_2 = 0$, and this holds for all vectors $(x_1, x_2) \in \mathbb{F}_p^2$. Since $y_1y_2 = 0$ for all vectors $(y_1, y_2) \in L$ by total isotropy, there are only two distinct possibilities for the one-dimensional Lagrangian subspace L, namely one where all $x_1 = y_1 = 0$ and another where all $x_2 = y_2 = 0$. □

By the surjection $\pi_N : \mathrm{LG}(M) \to \mathrm{LG}\left(N^\perp/N\right)$, any Lagrangian direct summand of $N^\perp/N$ for a totally isotropic direct summand $N \leq M$ is of the form $\pi_N(L) \in \mathrm{LG}\left(N^\perp/N\right)$ for a non-unique Lagrangian direct summand $L \in \mathrm{LG}(M)$. Yet this map is nowhere injective, and its fibre is constant and readily computed in the relevant case of $M = \mathbb{F}_p^{2n}$ through first establishing a bijective correspondence.

(3.3.12) **Lemma.** *Let $N \subseteq \mathbb{F}_p^{2n}$ be a one-dimensional subspace, and let $\pi_N(L) \in \mathrm{LG}\left(N^\perp/N\right)$ be a Lagrangian subspace for some Lagrangian subspace $L \in \mathrm{LG}\left(\mathbb{F}_p\right)^{2n}$. Then there is a bijective correspondence of spaces*

$$\begin{array}{ccc} \left\{ L' \in \mathrm{LG}\left(\mathbb{F}_p\right)^{2n} \;\middle|\; \pi_N(L') = \pi_N(L) \right\} & \leftrightsquigarrow & \{N' \subseteq L \mid \dim N' = n-1,\ N \not\subseteq N'\} \cup \{L\} \\ L' & \longmapsto & L' \cap L \end{array}.$$

Proof. To check that the map is well-defined, first consider the case where $N \subseteq L'$, which in turn bijectively corresponds to L and hence $L' \cap L = L$, so it suffices to consider the case where $N \not\subseteq L'$. If $x \in L' \cap N^\perp$, then $x + N \in \left(L' \cap N^\perp + N\right)/N = \pi_N(L') = \pi_N(L) = L/N$, so $x \in L$ and hence $L' \cap N^\perp \subseteq L \subseteq N^\perp$, where the latter inclusion is by total isotropy. The second isomorphism theorem gives an isomorphism of groups

$$\left(L' \cap N^\perp + N\right)/N \cong \left(L' \cap N^\perp\right) / \left(L' \cap N^\perp \cap N\right) \cong L' \cap N^\perp,$$

the latter isomorphism of which follows by $L' \cap N = \emptyset$. Then

$$\dim_{\mathbb{F}_p}(L' \cap L) = \dim_{\mathbb{F}_p}\left(L' \cap N^\perp\right) = \dim_{\mathbb{F}_p} \pi_N(L') = \dim_{\mathbb{F}_p} \pi_N(L) = \dim_{\mathbb{F}_p}(L/N) = n-1,$$

where the last equality follows from Corollary 3.3.10 and dimension subtraction, so the map is well-defined. Now to obtain the bijective correspondence, it suffices to show that any $(n-1)$-dimensional subspace $N' \subseteq L$ not containing N is contained in a unique Lagrangian subspace $L' \in \mathrm{LG}\left(\mathbb{F}_p\right)^{2n}$ such that $\pi_N\left(L'\right) = \pi_N\left(L\right)$ and $L \neq L'$. Applying Proposition 3.3.9 again establishes a bijective correspondence of spaces

$$\begin{array}{ccc} \left\{ L' \in \mathrm{LG}\left(\mathbb{F}_p\right)^{2n} \;\middle|\; N' \subseteq L' \right\} & \leftrightsquigarrow & \mathrm{LG}\left(N'^{\perp}/N'\right) \\ L' & \longmapsto & L'/N' \end{array},$$

but $N'^{\perp}/N'$ is a two-dimensional $\mathbb{F}_p$-vector space equipped with a quadratic form induced by $\mathbb{F}_p^{2n}$, so has exactly two Lagrangian subspaces by Proposition 3.3.11, one of which is the Lagrangian subspace $L/N' \in \mathrm{LG}\left(N'^{\perp}/N'\right)$. Thus the remaining Lagrangian subspace $L'/N' \in \mathrm{LG}\left(N'^{\perp}/N'\right)$ uniquely satisfies $\pi_N\left(L'\right) = \pi_N\left(L\right)$ and maps to $L' \cap L = N'$ by construction, so the bijective correspondence follows. □

The fibre of $\pi_N : \mathrm{LG}\left(M\right) \to \mathrm{LG}\left(N^{\perp}/N\right)$ is exactly the left set in the bijective correspondence, so it remains to count the cardinality of the right set, which is an easy consequence of previous results.

(3.3.13) **Corollary.** *Let $N \subseteq \mathbb{F}_p^{2n}$ be a one-dimensional subspace, and let $\pi_N\left(L\right) \in \mathrm{LG}\left(N^{\perp}/N\right)$ be a Lagrangian subspace for some Lagrangian subspace $L \in \mathrm{LG}\left(\mathbb{F}_p\right)^{2n}$. Then*

$$\#\pi_N^{-1}\left(\pi_N\left(L\right)\right) = p^{n-1} + 1.$$

Proof. With the bijective correspondence in Lemma 3.3.12, it remains to count the number of $(n-1)$-dimensional subspaces of L that does not contain N, but Corollary 3.3.7 computes this to be exactly

$$\binom{n}{n-1}_p - \binom{n-1}{n-2}_p = \prod_{i=0}^{n-2} \frac{p^n - p^i}{p^{n-1} - p^i} - \prod_{i=0}^{n-3} \frac{p^{n-1} - p^i}{p^{n-2} - p^i} = \frac{\left(p^n - 1\right)p^{n-2}}{p^{n-1} - p^{n-2}} - \frac{\left(p^{n-1} - 1\right)p^{n-3}}{p^{n-2} - p^{n-3}} = p^{n-1}.$$

Thus the result follows after including the singleton $\{L\}$ in the bijective correspondence. □

Computing the size of $\mathrm{LG}\left(\mathbb{F}_p\right)^{2n}$ is then a simple matter of induction from Corollary 3.3.13.

(3.3.14) **Proposition.**

$$\#\,\mathrm{LG}\left(\mathbb{F}_p\right)^{2n} = \prod_{i=0}^{n-1} \left(p^i + 1\right).$$

Proof. The base case is Proposition 3.3.11, so assume the result for $n-1$. Then taking a one-dimensional subspace $N \subseteq \mathbb{F}_p^{2n}$ and considering the quotient $N^{\perp}/N$ reduces to the inductive hypothesis, after which there are exactly $p^{n-1} + 1$ distinct choices for N that map to the same Lagrangian subspace in $\mathbb{F}_p^{2(n-1)}$ by Corollary 3.3.13. Thus the result for n follows from multiplying $p^{n-1} + 1$ by the result for $n-1$. □

There are several ways to extend Proposition 3.3.14 to $M = \left(\mathbb{Z}/p^e\right)^{2n}$, one of which simply involves meticulously tracing the computations in this subsection to the general case, taking into account subtle corrections in the presence of zero divisors, and reusing the general results proven in the previous subsection. For the sake of brevity, the final result will just be stated. Note that the formula above can be rewritten as

$$\#\,\mathrm{LG}\left(\mathbb{F}_p\right)^{2n} = \prod_{i=0}^{n-1} \left(p^i + 1\right) = \prod_{i=0}^{n-1} p^i \prod_{i=0}^{n-1} \left(1 + p^{-i}\right) = p^{\sum_{i=0}^{n-1} i} \prod_{i=1-n}^{0} \left(1 + p^i\right) = p^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} \left(1 + p^{i-n}\right),$$

which ties in directly with the formula below.

(3.3.15) **Proposition.**

$$\#\,\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n} = p^{\frac{1}{2}en(n-1)} \prod_{i=1}^{n} \left(1 + p^{i-n}\right).$$

Proof sketch. Obtain $\mathbb{Z}/p^e$ analogues of results in this subsection using results in the previous subsection. □

Remark. A fancier approach to deduce the general result is to realise the Lagrangian Grassmannian as a projective scheme over $\mathbb{Z}$ that is smooth of relative dimension $\frac{1}{2}n\left(n-1\right)$ [BKLPR15, Lemma 4.8]. Via a generalisation of Hensel's lemma, each Lagrangian Grassmannian over $\mathbb{F}_p$ can be lifted to one over $\mathbb{Z}/p^e$ by smoothness, while the relative dimension dictates the sizes of each fibre.

3.3.4 Average sizes of Selmer groups

This subsection finishes the proof that the intersection of two Lagrangian direct summands chosen uniformly at random from $\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n}$ has average size equal to the sum of divisors of p^e, hence providing a heuristic model for the average size of p^e-Selmer groups. This is achieved through probing the size of an intersection by counting the number of possible monomorphisms of $\mathbb{Z}/p^e$-modules into it. First define the finite set

$$\mathrm{Hom}_R^{\hookrightarrow}(M) \coloneqq \{\phi \in \mathrm{Hom}_R(R, M) \mid \phi : R \hookrightarrow M\}.$$

(3.3.16) **Lemma.** *Let M be a free $\mathbb{Z}/p^e$-module of rank m. Then*

$$\#\,\mathrm{Hom}_{\mathbb{Z}/p^e}^{\hookrightarrow}(M) = p^{em} - p^{(e-1)m}.$$

Proof. A monomorphism $\mathbb{Z}/p^e \hookrightarrow M$ is uniquely determined by an element of M with order exactly p^e. Each component has $\Phi\left(p^e\right) = p^{e-1}(p-1)$ elements of $\mathbb{Z}/p^e$ that induce elements of M with order exactly p^e, so there are $p^e - p^{e-1}(p-1) = p^{e-1}$ elements of $\mathbb{Z}/p^e$ that induce elements of M with order strictly less than p^e in each component. Thus, considering all components and subtracting this from the total number of elements of M, the desired number of monomorphisms $\mathbb{Z}/p^e \hookrightarrow M$ is $\left(p^e\right)^m - \left(p^{e-1}\right)^m = p^{em} - p^{(e-1)m}$. □

It is also possible to compute the proportion of monomorphisms $\mathbb{Z}/p^e \hookrightarrow M$ that land in a particular submodule of M, albeit with some tedious calculations. Instead, if the rank of M will eventually be made to tend to infinity, the same computations can be heavily simplified with a limiting probabilistic argument.

(3.3.17) **Proposition.** *Let $L_1, L_2 \in \mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n}$ be Lagrangian direct summands chosen uniformly at random. Then*

$$\lim_{n\to\infty} \mathbb{E}\left[\#\,\mathrm{Hom}_{\mathbb{Z}/p^e}^{\hookrightarrow}(L_1 \cap L_2)\right] = p^e.$$

Proof. With n tending to infinity in mind, the desired limiting average is simply the number of monomorphisms $\mathbb{Z}/p^e \hookrightarrow L_1$, multiplied by the probability that a randomly chosen Lagrangian direct summand $L_2 \in \mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n}$ contains the image of some monomorphism of $\mathbb{Z}/p^e$-modules $\phi : \mathbb{Z}/p^e \hookrightarrow L_1$, the result of which may or may not be an integer. The former number is exactly $p^{en} - p^{(e-1)n}$ by Corollary 3.3.10 and Lemma 3.3.16, while the latter probability, by the bijective correspondence in Proposition 3.3.9, is exactly the proportion of $\mathrm{LG}\left(\operatorname{im}\phi^\perp/\operatorname{im}\phi\right)$ as a space living inside $\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n}$. The construction of the metabolic quadratic $\mathbb{Z}/p^e$-module $\operatorname{im}\phi^\perp/\operatorname{im}\phi$ ensures that it is a free $\mathbb{Z}/p^e$-module of rank $2n-2$ that is isomorphic to $\left(\mathbb{Z}/p^e\right)^{2n-2}$, so Proposition 3.3.15 computes the final probability to be

$$\frac{\#\,\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n-2}}{\#\,\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2n}} = \frac{p^{\frac{1}{2}e(n-1)(n-2)}\prod_{i=1}^{n-1}\left(1+p^{i-n+1}\right)}{p^{\frac{1}{2}en(n-1)}\prod_{i=1}^{n}\left(1+p^{i-n}\right)} = p^{e(1-n)}\left(1+p^{1-n}\right).$$

Thus multiplying both quantities yields

$$\mathbb{E}\left[\#\,\mathrm{Hom}_{\mathbb{Z}/p^e}^{\hookrightarrow}(L_1 \cap L_2)\right] \to \left(p^{en} - p^{(e-1)n}\right)\left(p^{e(1-n)}\left(1+p^{1-n}\right)\right) = p^e + p^{e+1-n} - p^{e-n} - p^{e+1-2n},$$

which clearly tends to p^e as n tends to infinity. □

The main result of this section can now be proven with a simple telescoping argument.

Proof of Theorem 3.3.1. As per a previous argument, a monomorphism $\mathbb{Z}/p^e \hookrightarrow L_1 \cap L_2$ is uniquely determined by an element of $L_1 \cap L_2$ with order exactly p^e, but there are exactly $\#\left(L_1 \cap L_2\right) - \#\left(L_1 \cap L_2\right)\left[p^{e-1}\right]$ such elements, and Proposition 3.3.17 shows that the limiting average of this quantity is p^e. Now observe that $\left(L_1 \cap L_2\right)\left[p^d\right]$ is also $\mathbb{Z}/p^d$-module for any $d \leq e$, so the same principle applies to compute the limiting average number of monomorphisms $\mathbb{Z}/p^d \hookrightarrow \left(L_1 \cap L_2\right)\left[p^d\right]$ to be p^d. Thus, as n tends to infinity,

$$\mathbb{E}\left[\#\left(L_1 \cap L_2\right)\right] = \sum_{d=0}^{e} \mathbb{E}\left[\#\left(L_1 \cap L_2\right)\left[p^d\right] - \#\left(L_1 \cap L_2\right)\left[p^{d-1}\right]\right] \to \sum_{d=0}^{e} p^d,$$

which is exactly the sum of divisors of p^e. □

Remark. With a further inclusion-exclusion argument, given another free $\mathbb{Z}/p^e$-module N of rank k, it is easy to compute the number of monomorphisms $N \hookrightarrow M$ in terms of m and k [BKLPR15, Theorem 5.10]. On the other hand, it is more noteworthy that this is always a finite value, so that when M is randomly sampled, such as the case of $L_1 \cap L_2$, this implies that the limiting k-th moment for $\#M$ is bounded. As such, under the assumption that $L_1 \cap L_2$ does indeed model $\mathcal{S}_{p^e}(K, E)$ for an elliptic curve E defined over a number field K, and assuming the conjecture that the limiting moments of $\#\mathcal{S}_{p^e}(K, E)$ are also bounded, this yields the actual average number of monomorphisms of N into $\mathcal{S}_{p^e}(K, E)$ [BKLPR15, Remark 5.13]. This in turn provides a method of computing the higher moments of $\#\mathcal{S}_{p^e}(K, E)$, including its actual average.

3.3.5 Freeness of the ambient module

This final short subsection identifies an important issue of the model with regards to the ambient module. In particular, the construction of the free ambient module $(\mathbb{Z}/p^e)^{2n}$ in this subsection implicitly assumes that the ambient module $\mathrm{H}^1(\mathbb{A}_K, E[p^e])$ in the previous subsection is free, although it is almost never the case.

(3.3.18) **Proposition.** *Let $e > 2$. Then $\mathrm{H}^1(\mathbb{A}_K, E[p^e])$ is not free for almost all elliptic curves $E \in \mathcal{E}(K)$.*

Proof. It suffices to show, for almost all elliptic curves $E \in \mathcal{E}(K)$, that $E(K_v)/p^e$ is not a free $\mathbb{Z}/p^e$-module for some place $v \in \mathcal{V}_K$, since it is a direct summand of $\mathrm{H}^1(K_v, E[p^e])$, by Proposition 3.2.27, and hence of $\mathrm{H}^1(\mathbb{A}_K, E[p^e])$. Proposition 3.2.35 yields the surjectivity of modulo p^e Galois representations for almost all elliptic curves $E \in \mathcal{E}(K)$, so for any such elliptic curve, there is an automorphism $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ such that

$$\rho_{E[p^e]}(\sigma) = \begin{pmatrix} p+1 & 0 \\ 0 & p+1 \end{pmatrix}.$$

By Chebotarev's density theorem, σ corresponds to a Frobenius substitution $\sigma_w \in \mathrm{Gal}\left(\overline{K}/K\right)$ of a non-archimedean place $w \in \mathcal{V}_{\overline{K}}^0$ extending some non-archimedean place $v \in \mathcal{V}_K^0$. The $\mathrm{Gal}\left(\overline{K_v}/K_v\right)$-action on $E[p^e]$ is governed by $\rho_{E[p^e]}(\sigma)$, so its invariant subgroup $E(K_v)[p^e]$ consists of precisely the elements in $(\mathbb{Z}/p^e)^2$ annihilated by p, which is exactly $\mathbb{F}_p^2$. Now the first isomorphism theorem equates the cardinalities of the finite groups $E(K_v)/p^e$ and $E(K_v)[p^e] \cong \mathbb{F}_p^2$, so the former cannot be a free $\mathbb{Z}/p^e$-module. □

Remark. The same is also true for $e = 2$ using a similar argument by checking cases, or alternatively noting that $E(K_v)[p^e]$ is a direct summand of $E(K_v)$ [BKLPR15, Proposition 6.13].

In spite of this drawback, it is heuristically expected that the consequences induced by the model continue to hold due to its compatibility with known results and conjectures, while a potentially more complicated linear algebraic model incorporating freeness of the ambient module remains open-ended.

Chapter 4

Heuristic consequences

This final chapter briefly presents several consequences, assuming that the p^e-Selmer group is indeed modelled by the intersection of two Lagrangian direct summands chosen uniformly at random from $\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2m}$ when m tends to infinity, as in the previous chapter. In what follows, the arguments will mostly be presented without proof, and their details will be deferred to the paper on modelling distributions of elliptic curves by Bhargava, Kane, Lenstra, Poonen, and Rains [BKLPR15] and to the paper on boundedness of ranks of elliptic curves by Park, Poonen, Voight, and Wood [PPVW19]. Throughout this chapter, let E be an elliptic curve defined over a number field K, let $m, n \in \mathbb{N}^+$ be arbitrary, and let $p^e \in \mathbb{N}^+$ be a prime power.

4.1 Modelling short exact sequences

Despite Theorem 3.2.1 presenting only the case of p^e-Selmer groups, general n-Selmer groups behave well under p^e-torsion subgroups, in the sense that for almost all elliptic curves $E \in \mathcal{E}(K)$,

$$\mathcal{S}_n(K,E)\left[p^e\right] \cong \mathcal{S}_{p^e}(K,E), \qquad p^e \mid n,$$

a purely cohomological result relying on the fact that almost all elliptic curves have trivial torsion subgroups [BKLPR15, Proposition 5.9]. As such, a general n-Selmer group is built up from gluing p^e-Selmer groups in some fashion, each of which modelled by intersecting two Lagrangian direct summands in $\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2m}$. One may then wonder if the tempting analogue of Theorem 3.3.1 holds for $L_1, L_2 \in \mathrm{LG}\left(\mathbb{Z}/n\right)^{2m}$, namely if

$$\lim_{m\to\infty} \mathbb{E}\left[\#\left(L_1 \cap L_2\right)\right] = \sigma_1(n),$$

where $\sigma_1 : \mathbb{N}^+ \to \mathbb{N}$ is the sum of divisors function, since this would affirm Conjecture 1.1.1 under appropriately bounded second moments. While it may be possible to prove this by considering each $\left(L_1 \cap L_2\right)\left[p^e\right]$ and using the multiplicativity of σ_1, deriving properties of $\mathbb{Z}/n$-modules analogous to those in the previous chapter would pose a significant challenge, especially in the size computation of $\mathrm{LG}\left(\mathbb{Z}/n\right)^{2m}$.

Instead, a viable alternative model based on short exact sequences can be constructed as follows. Take the direct limit of multiplication by p maps over all prime powers $n = p^e$, and denote $\mathcal{S}_{p^\infty}(K,E) \coloneqq \varinjlim_e \mathcal{S}_{p^e}(K,E)$. There is a fundamental short exact sequence of abelian groups

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{S}_{p^\infty}(K,E) \to Ш(K,E)\left[p^\infty\right] \to 0, \tag{4.1}$$

and each of these can be endowed with the structure of a $\mathbb{Z}_p$-module. Now for two arbitrary Lagrangian direct summands $L_1, L_2 \in \mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}$, construct three $\mathbb{Z}_p$-modules by

$$R \coloneqq \left(L_1 \cap L_2\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p, \qquad S \coloneqq \left(L_1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\right) \cap \left(L_2 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\right), \qquad T \coloneqq S/R.$$

These fit in a split short exact sequence of $\mathbb{Z}_p$-modules [BKLPR15, Corollary 5.3]

$$0 \to R \to S \to T \to 0, \tag{4.2}$$

which all have finitely generated Pontryagin duals.

As remarked previously, it turns out that one can define a canonical measure on $\mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}$ that restricts to a uniform measure on each $\mathrm{LG}\left(\mathbb{Z}/p^e\right)^{2m}$, so that choosing $L_1, L_2 \in \mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}$ uniformly at random induces a discrete probability distribution on the set of isomorphism classes of short exact sequences of $\mathbb{Z}_p$-modules whose Pontryagin duals are finitely generated, which converges when m tends to infinity [BKLPR15, Theorem 1.2]. Thus (4.2) would supply a conjectural model for (4.1) [BKLPR15, Conjecture 1.3], and the distributions of the Mordell-Weil rank $\mathrm{rk}\left(E/K\right)$, the p^∞-Selmer group $\mathcal{S}_{p^\infty}\left(K,E\right)$, and the p-primary component of the Tate-Shafarevich group $Ш\left(K,E\right)\left[p^\infty\right]$ can be modelled simultaneously.

It then remains to justify the construction of this model. Amongst other desirable consequences, the truthfulness of this model is heuristically supported by various evidence.

- There is an isomorphism of abelian groups $R \cong \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{\mathrm{rk}(E/K)}$, while the same is true for $E\left(K\right) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ by the Mordell-Weil theorem. Moreover, by splitting $\mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}$ into spaces of Lagrangian Grassmannians with odd or even dimensions [BKLPR15, Proposition 4.5] and computing the dimensions of Schubert subschemes [BKLPR15, Proposition 4.9], the model would also affirm the rank distribution conjecture that $\delta\left(\mathrm{rk}\left(E/K\right)=0\right) = \delta\left(\mathrm{rk}\left(E/K\right)=1\right) = \frac{1}{2}$ [BKLPR15, Proposition 5.6].
- The construction of S mirrors the model for all $\mathcal{S}_{p^e}\left(K,E\right)$ simultaneously. Moreover, due to the isomorphisms $\mathcal{S}_{p^\infty}\left(K,E\right)\left[p^e\right] \cong \mathcal{S}_{p^e}\left(K,E\right)$ and $S\left[p^e\right] \cong \left(L_1/p^e\right) \cap \left(L_2/p^e\right)$ [BKLPR15, Proposition 5.4], the distribution of $\mathcal{S}_{p^e}\left(K,E\right)$ would coincide with the limiting distribution of $L_1 \cap L_2$ for each p^e.
- The finiteness of T [BKLPR15, Corollary 5.2] would imply the finiteness of $Ш\left(K,E\right)\left[p^\infty\right]$, at least for almost all elliptic curves $E \in \mathcal{E}\left(K\right)$, and this is part of the Tate-Shafarevich conjecture. Moreover, T can be equipped with a natural non-degenerate alternating $\mathbb{Z}$-bilinear pairing [BKLPR15, Proposition 5.5], which mirrors the Cassels-Tate pairing on $Ш\left(K,E\right)\left[p^\infty\right]$.

Assuming its truthfulness, however, a plausible model for a general n-Selmer group

$$\mathcal{S}_n\left(K,E\right) \cong \bigoplus_p \mathcal{S}_{p^\infty}\left(K,E\right)\left[p^{\mathrm{ord}_p\, n}\right], \tag{4.3}$$

which is ideally obtained from S, still requires an understanding of the behaviour of R and T.

4.2 Modelling Tate-Shafarevich groups

The rank distribution conjecture predicts that $\delta\left(\mathrm{rk}\left(E/K\right) \geq 2\right) = 0$, which is reflected in this model in such a way that, if $L_1, L_2 \in \mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}$ were Lagrangian direct summands chosen uniformly at random, the set

$$\mathrm{LG}_r^m \coloneqq \left\{ \left(L_1, L_2\right) \in \left(\mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}\right)^2 \;\middle|\; \mathrm{rk}_{\mathbb{Z}_p}\left(L_1 \cap L_2\right) = r \right\}$$

would have measure zero for any fixed $r \in \mathbb{N}_{\geq 2}$. Unfortunately, this means that the induced distribution of T, and hence of $Ш\left(K,E\right)\left[p^\infty\right]$, where $E \in \mathcal{E}\left(K\right)$ is sampled with the condition $\mathrm{rk}\left(E/K\right) = r$, cannot be predicted. There are at least three proposed workarounds to this, outlined as follows.

- Choose a tuple $\left(L_1, L_2\right)$ uniformly at random directly from the set LG_r^m, which carries a product measure induced by $\mathrm{LG}\left(\mathbb{Z}_p\right)^{2m}$. This induces a natural discrete probability distribution on the set of isomorphism classes of T, which converges when m tends to infinity [BKLPR15, Theorem 1.6].
- In accordance with Delaunay's interpretation of the Cohen-Lenstra heuristics for ideal class groups, consider the set of all **symplectic p-groups**, finite abelian groups G of orders powers of p and equipped with a non-degenerate alternating pairing $G \times G \to \mathbb{Q}_p/\mathbb{Z}_p$, and identify them up to isomorphisms respecting the pairing. Define a probability distribution on this set by

  $$\mathrm{Prob}\, G \coloneqq \frac{\left(\#G\right)^{1-r}}{\#\,\mathrm{Aut}\, G} \prod_{i>r} \left(1 - p^{1-2i}\right),$$

  where $\mathrm{Aut}\, G$ denotes the group of automorphisms of G respecting the symplectic structure. This generalises Delaunay's distributions to elliptic curves of rank r [BKLPR15, Section 5.6].

- Choose a matrix M uniformly at random from the space of matrices

$$\mathrm{Mat}_r^m \coloneqq \left\{ M \in \mathrm{Mat}_m \mathbb{Z}_p \;\middle|\; M^\intercal = -M,\ \mathrm{rk}_{\mathbb{Z}_p}(\ker M) = r \right\}, \qquad m \equiv r \mod 2,$$

  which also carries a Haar-like measure as a $\mathbb{Z}_p$-scheme of finite type. This induces a probability distribution on the set of isomorphism classes of $(\mathrm{coker}\, M)_{\mathrm{tors}}$, which converges when $m \equiv r \mod 2$ tends to infinity [BKLPR15, Theorem 1.10]. Furthermore, $(\mathrm{coker}\, M)_{\mathrm{tors}}$ can also be equipped with a non-degenerate alternating pairing [BKLPR15, Section 3.5], making it a symplectic p-group. It is worth noting that the construction is inspired by, and analogous to, the Friedman-Washington interpretation of the Cohen-Lenstra heuristics for ideal class groups [BKLPR15, Remark 1.11].

It turns out that all three distributions coincide [BKLPR15, Theorems 1.6(c) and 1.10(b)], establishing a new model for T via isomorphism classes of symplectic p-groups compatible with the short exact sequence.

All of the above discussion culminates in a model for a general n-Selmer group defined as follows. Since the three distributions for T are now conditioned on $\mathrm{rk}(E/K) = r$, and the original model for T distributes r uniformly amongst $\{0, 1\}$, choose $r \in \{0, 1\}$ uniformly at random. Choose a symplectic p-group T_p at random for each prime $p \in \mathbb{N}^+$ using any of the three distributions, and define

$$S_n \coloneqq (\mathbb{Z}/n)^r \oplus \left(\bigoplus_p T_p \right)[n]. \tag{4.4}$$

Then (4.4) would precisely model (4.3), and by the previous chapter, this would affirm Conjecture 1.1.1 [BKLPR15, Section 5.7], noting that the p-primary components of S_n are independent for distinct primes p.

4.3 Modelling Mordell-Weil ranks

Coincidentally, the third distribution above also suggests a model for the Mordell-Weil rank. Since conditioning on r yields a distribution with the prescribed Mordell-Weil rank, removing this condition would ideally cause r to be distributed like the Mordell-Weil rank instead. This cannot be literally true, since an alternating matrix always has even rank and $m \equiv r \mod 2$. Furthermore, due to a similar measure zero issue for $r \geq 2$, this distribution cannot predict the relative frequencies of higher Mordell-Weil ranks.

Rather, a model can be constructed such that m is sampled uniformly from odd and even natural numbers, and M is sampled from a subspace of matrices with entries bounded by a constant. Letting both sampling processes depend on an appropriate notion of height of the elliptic curve to be modelled, the refined model would solve both issues and provide a conjectural distribution for the Mordell-Weil rank. In particular, the model for an elliptic curve of height $h \in \mathbb{N}$ is proposed as follows.

- Choose functions $X : \mathbb{N} \to \mathbb{R}$ and $Y : \mathbb{N} \to \mathbb{R}$ such that $X(x)^{Y(x)} = x^{1/12 + \mathrm{o}(1)}$ as $x \to \infty$.
- Choose m uniformly at random from $\{\lceil Y(h) \rceil, \lceil Y(h) \rceil + 1\}$.
- Choose M uniformly at random from $\mathrm{Mat}_m \mathbb{Z}$ such that $M^\intercal = -M$ with entries bounded by $X(h)$.

The choice of condition for the functions here is made with significant arithmetic justification, namely the expectation that the average size of the Tate-Shafarevich group of elliptic curves of height h and rank zero is $h^{1/12 + \mathrm{o}(1)}$, the proof of which is elided for brevity [PPVW19, Theorem 6.4.2(c)]. Further theoretical evidence to the validity of this model is the agreement with the three distributions above and the rank distribution conjecture [PPVW19, Section 8.1], with much computational evidence as well [PPVW19, Section 10.1].

Using sieve-theoretic techniques, the construction culminates in a very surprising result, namely that all but finitely many elliptic curves $E \in \mathcal{E}(\mathbb{Q})$, under a slightly different notion of heights, satisfy $\mathrm{rk}(E/K)\,\mathbb{Q} \leq 21$ [PPVW19, Theorem 7.3.3(a)]. This would mean that there is an upper bound to the Mordell-Weil rank of rational elliptic curves, which ultimately answers the rank boundedness conjecture in the affirmative.

Bibliography

[BKLPR15] M. Bhargava, D. Kane, H. Lenstra, B. Poonen and E. Rains. 'Modelling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves'. In: *Camb. J. Math. 3* (2015).

[BS13a] M. Bhargava and A. Shankar. *The average number of elements in the 4-Selmer groups of elliptic curves is 7*. Preprint, arXiv:1312.7333. 2013.

[BS13b] M. Bhargava and A. Shankar. *The average size of the 5-Selmer group of elliptic curves is 6*. Preprint, arXiv:1312.7859. 2013.

[BS15a] M. Bhargava and A. Shankar. 'Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves'. In: *Ann. of Math. 181* (2015).

[BS15b] M. Bhargava and A. Shankar. 'Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0'. In: *Ann. of Math. 181* (2015).

[CFOSS06] J. Cremona, T. Fisher, C. O'Neil, D. Simon and M. Stoll. 'Explicit n-descent on elliptic curves I. Algebra'. In: *Math. Comp. 84* (2006).

[CL84] H. Cohen and H. Lenstra. 'Heuristics on class groups of number fields'. In: *Number theory, Noordwijkerhout* (1984).

[CSS97] G. Cornell, J. Silverman and G. Stevens. *Modular forms and Fermat's last theorem*. Springer-Verlag, 1997.

[CSS98] J.-L. Colliot-Thelene, A. Skorobogatov and P. Swinnerton-Dyer. 'Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points'. In: *Invent. Math. 134* (1998).

[Del01] C. Delaunay. 'Heuristics on Tate-Shafarevitch groups of elliptic curves defined over Q'. In: *Exp. Math. 10* (2001).

[Del07] C. Delaunay. 'Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics'. In: *London Math. Soc. Lecture Note Ser. 341* (2007).

[DKK08] S. Dougherty, J.-L. Kim and H. Kulosman. 'MDS codes over finite principal ideal rings'. In: *Des. Codes Cryptogr. 50* (2008).

[EK20] N. Elkies and Z. Klagsbrun. *New records for ranks of elliptic curves with torsion*. Preprint, arXiv:2003.00077. 2020.

[Fuc70] L. Fuchs. *Infinite abelian groups*. Academic Press, 1970.

[FW89] E. Friedman and L. Washington. 'On the distribution of divisor class groups of curves over a finite field'. In: *Theorie des nombres* (1989).

[GG18] J. Gillibert and P. Gillibert. 'On the splitting of the Kummer exact sequence'. In: *Publications mathematiques de Besancon, algebre et theorie des nombres* (2018).

[GGGR19] F. Gillibert, J. Gillibert, P. Gillibert and G. Ranieri. 'Selmer groups are intersection of two direct summands of the adelic cohomology'. In: *Bull. London Math. Soc. 51* (2019).

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, 1977.

[Kap58] I. Kaplansky. 'Projective modules'. In: *Ann. of Math. 68* (1958).

[Lan20] A. Landesman. *The geometric average size of Selmer groups over function fields*. Preprint, arXiv:1811.00966. 2020.

[Mil06] J. Milne. *Arithmetic duality theorems*. BookSurge, 2006.

[Mil13] J. Milne. *Class field theory*. https://www.jmilne.org/math/CourseNotes/CFT.pdf. 2013.

[Mum70] D. Mumford. *Abelian Varieties*. Oxford University Press, 1970.

[ONe01] C. O'Neil. 'The period-index obstruction for elliptic curves'. In: *J. Number Theory 95* (2001).

[Poo17] B. Poonen. *Heuristics for the arithmetic of elliptic curves*. 2017.

[PPVW19] J. Park, B. Poonen, J. Voight and M. Wood. 'A heuristic for boundedness of ranks of elliptic curves'. In: *J. Eur. Math. Soc* (2019).

[PR12] B. Poonen and E. Rains. 'Random maximal isotropic subspaces and Selmer groups'. In: *J. Amer. Math. Soc 25* (2012).

[Ser80] J.-P. Serre. *Local fields*. Springer-Verlag, 1980.

[Ser89] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Amer Mathematical Society, 1989.

[Sil09] J. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 2009.

[Sil94] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, 1994.

[Sto10] M. Stoll. *Descent on elliptic curves*. arXiv:math/0611694. 2010.

[Zar74] Y. Zarhin. 'Noncommutative cohomologies and Mumford groups'. In: *Mat. Zametki 15* (1974).

[Zyw10] D. Zywina. *Hilbert's irreducibility Theorem and the Larger Sieve*. Preprint, arXiv:1011.6465. 2010.

[Zyw18] D. Zywina. 'Elliptic curves with maximal Galois action on their torsion points'. In: *Bull. London Math. Soc. 42* (2018).