UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DEPARTMENT OF MATHEMATICS "TULLIO LEVI-CIVITA"

Master Degree in Mathematics

Kolyvagin's work on modular elliptic curves

Master Candidate:
Francesco Feltrin

Student ID: 2119988

Supervisor:
Prof. Matteo Longo

Academic Year 2025/2026

Graduation date 17/07/2026

Contents

Introduction

The Mordell-Weil Theorem states that, for an elliptic curve E over a number field K, the abelian group of K-rational points $E(K)$ is finitely generated:

$$E(K) = E(K)_{\text{tors}} \oplus \langle P_1, \cdots, P_r \rangle \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r.$$

The proof of this result, however, doesn't provide an explicit algorithm to compute r for a given general elliptic curve: this is actually an open problem regarding elliptic curves, and it's connected to two conjectures in the field, namely the Birch and Swinnerton-Dyer conjecture (BSD) and the Shafarevich-Tate conjecture. The former is probably the major open question concerning elliptic curves: it claims that $r = \text{rk}_{\mathbb{Z}} E(K)$ is equal to the order of vanishing at $s = 1$ of the L-series $L(E, s)$ attached to the curve E; furthermore, it predicts the exact value of the coefficient of the first non-zero term in the Taylor expansion of $L(E, s)$ at $s = 1$, given in terms of some arithmetic quantities associated with E. Among them there is the order of the Shafarevich-Tate group $Ш(E/K)$, a very important torsion abelian group attached to E that emerges from the cohomology of Galois groups; the finiteness of this group is in fact the claim of the homonymous conjecture.

The main achievements regarding these conjectures have been attained in the case that the considered elliptic curve has rank equal to 0 or 1, thanks to the work of Kolyvagin, Gross, Zagier, Rubin and others. In this thesis we are going to discuss the ideas and the tools that were used to obtain those results, and we present the proof one of these theorems, which gives sufficient conditions to prove certain constraints on the rank r and on the divisibility in the group $Ш(E/K)$:

Theorem 0.0.1 (Theorem 2.1.4)**.** Consider an elliptic curve $E/\mathbb{Q}$ of conductor N, and an imaginary quadratic field K where all prime factors of N split. Let p be an odd prime such that $\text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$; finally, assume that the *Heegner point* y_K has infinite order in $E(K)$ and is not divisible by p in $E(K)$. Then

1. the rank of $E(K)$ is 1.
2. the p-torsion subgroup $Ш(E/K)_p$ is trivial.

The construction of the point y_K depends on the Modularity Theorem and will be explained at the beginning of Chapter 2.

Before arriving to this, in the first chapter we introduce the necessary background definitions and results: the basics of elliptic curves, together with some aspects of the theory of modularity; the Galois cohomology of an elliptic curve and the definitions of the Selmer and Shafarevich-Tate groups; the definitions and properties of the *ring class fields* K_n, which are certain abelian extensions of an imaginary quadratic number field K.

In Section 2.1 we begin to discuss our problem, defining the curve E and the quadratic field K, and we state the results we aim to prove. The strategy of the proof of 2.1.4, following [4], has several steps. The first one is the definition of the so called *Heegner points* on the modular curve $X_0(N)$, and the use of the Modularity Theorem to obtain an *Euler system*: a collection of points y_n on the curve E which satisfy strong compatibility conditions, described by Proposition 2.2.10. Using these points y_n to define classes $[P_n] \in E(K_n)/pE(K_n)$, we construct certain cohomology classes $c(n) \in H^1(K, E_p)$ and $d(n) \in H^1(K, E)_p$: these elements, called *Kolyvagin classes*, will be ubiquitous in the sequel.

In the last part of Chapter 2 we analyze the global and local properties of the classes $c(n)$ and $d(n)$: the main result of this sections, Theorem 2.5.2, relates the local behaviour of $d(n)$, i.e. the restrictions $\mathrm{res}_\lambda(d(n)) \in H^1(K_\lambda, E)_p$, to the p-divisibility of the points P_m in $E(K_\lambda)$ (here K_λ is the completion of the field K at a prime λ).

Chapter 3 is devoted to explaining how Kolyvagin classes may give information on the structure of the Selmer group $\mathrm{Sel}^{(p)}(E/K)$, and therefore of $Ш(E/K)_p$ in view of the fundamental exact sequence 1.21. The most important result is Proposition 3.1.9, which will play a crucial role in the final proofs: it states that a class $d(n)$ which is locally trivial almost everywhere (in the precise sense given in the statement) gives strong conditions on the localized elements of the Selmer group. To prove 3.1.9, in Section 3.1 we briefly recall some facts of local and global class field theory. Subsequently we state and prove some auxiliary results, the main goal being a computation of the Selmer group: in the last section we will prove in several steps that, under our assumptions, this group is cyclic of order p. From this powerful result we will easily deduce the proof of Theorem 2.1.4.

Chapter 1

Elliptic curves

1.1 First definitions and properties

Our main reference is [21].

Definition 1.1.1. Let k be a field. An *elliptic curve* over k is a projective plane curve E over k of degree 3 and genus 1, together with a specified point $O \in E(k)$.

It is known that any elliptic curve has a *Weierstrass equation*, i.e. it is the zero locus of an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3;$$

when $a_i \in k$ for all i, we say that E is defined over k and write E/k. The main feature of elliptic curves is that they are an instance of *abelian varieties*, i.e. a projective algebraic variety with a group structure defined by regular maps. Hence, for any field K, the set $E(K)$ of K-rational points is an abelian group.

Since elliptic curves are abelian varieties, the correct notion of morphism between them is the following.

Definition 1.1.2. Let E, E' be elliptic curves. An *isogeny* from E to E' is a map $\psi\colon E \to E'$ which is a morphism of algebraic varieties *and* a group homomorphism. If $E' = E$, the set of all isogenies $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is a ring of characteristic zero under addition and composition.

For any integer n, the multiplication by n in the abelian group $E(K)$ is an isogeny. Therefore we always have $\mathrm{End}(E) \supset \mathbb{Z}$. If this ring is strictly larger than $\mathbb{Z}$, E is said to be an elliptic curve *with complex multiplication* (abbreviated CM).

One of the most interesting objects attached to an elliptic curve E is the set of *n-torsion points*:

$$E_n = E_n(\overline{K}) = \ker([n]) = \left\{ P \in E(\overline{K}) \;\middle|\; nP = 0 \right\}.$$

For any field K, we write $E_n(K)$ for $E_n \cap E(K)$, the n-torsion rational over K. We have the following important result:

Proposition 1.1.3. Fix a prime integer p. If E is an elliptic curve defined over a field K of characteristic zero or $\mathrm{char}(K) = l$, $l \neq p$, then $E_p(\overline{K}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. See [21], p. 86, Corollary 6.4. □

Remark 1.1.4. Let $F = \mathbb{Q}(E_p)$ be the extension of $\mathbb{Q}$ obtained by adjoining the coordinates x_P, y_P of all the p-torsion points $P \in E(\overline{\mathbb{Q}})_p$. The extension $F/\mathbb{Q}$ is algebraic and finite, because x_P and y_P are algebraic numbers for all such points P: the reason is that they are the roots of some polynomials in $\mathbb{Q}[x]$ obtained by the explicit formulas for the multiplication by p in E. Moreover F is a Galois extension of $\mathbb{Q}$, since a $\mathbb{Q}$-automorphism of F permutes the set $E_p(\overline{\mathbb{Q}}) = E_p(F)$. For the details see e.g. [23], p. 218, Proposition 6.5.
Lastly, the group $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of $GL_2(\mathbb{F}_p)$. To see this, consider the representation

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_p) \cong GL_2(\mathbb{F}_p);$$

Since the kernel of ρ is $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, we have

$$\mathrm{Gal}(F/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{F}_p). \tag{1.1}$$

Another important notion is that of *good and bad reduction*, that we now define.

Definition 1.1.5. Let K be a number field, E/K an elliptic curve and v a prime of K; write k for the residue field $\mathcal{O}_K/v$. Let $\widetilde{E}$ be the curve obtained by reducing modulo v a Weierstrass equation for E. We say that

1. E has *good reduction at* v if $\widetilde{E}$ is nonsingular;
2. E has *bad, additive reduction at* v if $\widetilde{E}$ has a cusp;
3. E has *bad, split multiplicative reduction at* v if $\widetilde{E}$ has a node and the slopes of the tangent lines at the node are in k;
4. E has *bad, nonsplit multiplicative reduction at* v if $\widetilde{E}$ has a node and the slopes of the tangent lines at the node are not in k.

Finally, we define two more objects attached to an elliptic curve $E/\mathbb{Q}$.

Definition 1.1.6. For an elliptic curve $E/\mathbb{Q}$ defined over $\mathbb{Q}$, the *conductor of* E is defined as

$$N = N_E = \prod_{p \text{ prime}} p^{f_p},$$

where

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p; \\ 1 & \text{if } E \text{ has multiplicative reduction at } p; \\ 2 + \delta_p & \text{if } E \text{ has additive reduction at } p; \end{cases}$$

the precise definition of δ_p is quite complicated: see ([21], Chapter IV, Section 10) for the details. In any case, $\delta_v = 0$ for any $p \geq 5$.

Definition 1.1.7. For an elliptic curve E defined over $\mathbb{Q}$ of conductor N, the *L-series of* E is defined as

$$L(E, s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-s})^{-1} \prod_{p \mid N} (1 - a_p p^{-s})^{-1}, \tag{1.2}$$

with

$$a_p = \begin{cases} p + 1 - \#\widetilde{E}(\mathbb{F}_p) & \text{if } E \text{ has good reduction at } p; \\ +1 & \text{if } E \text{ has split multiplicative reduction at } p; \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p; \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

1.2 Elliptic curves and modular forms

In this section we present the main definitions of the theory of modularity and state some important results.

Definition 1.2.1. For any integer $N \geq 1$, the following subgroups of $SL_2(\mathbb{Z})$ are defined:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0, a \equiv d \equiv 1 \pmod{N} \right\}$$
$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \mathbb{I}_2 \pmod{N} \right\}$$

We have that $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq SL_2(\mathbb{Z})$. A *congruence subgroup of* $SL_2(\mathbb{Z})$ is a subgroup $\Gamma \leq SL_2(\mathbb{Z})$ containing $\Gamma(N)$ for some N. We will be interested mainly in $\Gamma_0(N)$.

Let $\mathbb{H} = \{ z \in \mathbb{C} \mid Im(z) > 0 \}$ be the complex upper half-plane; a congruence subgroup Γ acts on $\mathbb{H}$ by Moebius transformations:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathbb{H} \to \mathbb{H}, \quad z \mapsto \gamma(z) = \frac{az+b}{cz+d}.$$

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$; it is possible to extend the action of Γ on $\mathbb{H}$ to an action on $\mathbb{H}^*$, and to define a topology on $\mathbb{H}^*$ such that the quotient spaces $\mathbb{H}/\Gamma$ and $\mathbb{H}^*/\Gamma$ become Riemann surfaces. Moreover, the action of Γ on $\mathbb{H}^* \setminus \mathbb{H}$ has finitely many orbits: the images of these orbits in $\mathbb{H}^*/\Gamma$ are called the *cusps* of Γ (and of $\mathbb{H}^*/\Gamma$). See e.g. [11], Chapter III for the details.

Definition 1.2.2. Consider the congruence subgroup $\Gamma_0(N) \leq SL_2(\mathbb{Z})$. Define

$$X_0(N) = \mathbb{H}^*/\Gamma_0(N), \quad Y_0(N) = \mathbb{H}/\Gamma_0(N);$$

more precisely, define $X_0(N)$ to be the projective algebraic curve over $\mathbb{C}$ whose complex points $X_0(N)(\mathbb{C})$ are identified with the Riemann surface $\mathbb{H}^*/\Gamma$.

This modular curve has the following properties, the most notable being the first one.

Remark 1.2.3. The curve $X_0(N)$ is defined over $\mathbb{Q}$. It has only two cusps, that are commonly denoted as 0 and ∞. See [17], Chapter V, Section 2. The curve $X_0(N)$ is called the *classical modular curve of level* N; it is a compact Riemann surface. It is a *moduli space* in the sense that its points represent equivalence classes of pairs (E, S) where E is an elliptic curve defined over $\mathbb{C}$ and $S \leq E$ is a cyclic subgroup of order N; equivalently, its points represent equivalence classes of triples (E, E', ψ), where ψ is a *cyclic* N*-isogeny* $\psi \colon E \to E'$, i.e. $\ker(\psi) = S \leq E$ is cyclic of order N.

Definition 1.2.4. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A meromorphic function $f \colon \mathbb{H} \to \mathbb{C}$ is called a *modular function of weight* k *for* Γ if it satisfies

1. $f(\gamma\tau) = (cz+d)^k f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$;

2. f is "meromorphic at infinity", i.e. the Fourier series

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n, \qquad \text{where } q = e^{2\pi i z}, \tag{1.3}$$

has at most finitely many nonzero a_n with $n < 0$;

3. f is meromorphic at all the cusps of $\mathbb{H}^*/\Gamma$ (for the precise definitions, see [11], Chapter III, Section 3).

If, in addition, f is actually holomorphic on $\mathbb{H}$, at infinity (i.e. $a_n = 0$ for all $n < 0$) and at all the cusps, then f is called a *modular form of weight k for Γ*.

Finally, if f "vanishes at infinity" (i.e. $a_n = 0$) and at all the cusps, then it is called a *cusp-form of weight k for Γ*. The complex vector space of weight k cusp-forms is denoted $S_k(\Gamma)$.

Definition 1.2.5. For an algebraic curve C we define the *Jacobian curve* $J(C)$ to be

$$J(C) = \mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C),$$

the group of degree-zero divisors modulo the subgroup of principal divisors. It is itself an abelian variety.

Theorem 1.2.6 (Modularity Theorem)**.** Every elliptic curve defined over $\mathbb{Q}$ is modular: if $E/\mathbb{Q}$ is an elliptic curve, then there exist an integer N and a surjective morphism

$$\phi\colon X_0(N) \to E$$

defined over $\mathbb{Q}$. More precisely, N may be taken to be the conductor of E. The morphism ϕ is also called *modular parametrization for E*; it is given by a composition of two maps

$$X_0(N) \longrightarrow J(X_0(N)) \longrightarrow E, \tag{1.4}$$

where the first map sends a point P to the class of the degree zero divisor $(P) - (\infty)$. (see [17], Chapter V, p. 214). In this way, ϕ maps the cusp ∞ of $X_0(N)$ to the origin of E. Furthermore, there exists a unique cusp form $f \in S_2(\Gamma_0(N))$ such that its Fourier expansion (1.3) satisfies

$$f(z) = \sum_{n \geq 1} a_n q^n \text{ and } \sum_{n \geq 1} \frac{a_n}{n^s} = L(E, s), \tag{1.5}$$

where $L(E, s)$ is the L-function of E defined in (1.2).

Remark 1.2.7. The cusp-form f is commonly called a *newform*: roughly speaking, it is an eigenvector of some important operators on the space $S_k(\Gamma_0(N))$ called *Hecke operators*. We are not going in this direction, but still adopt this terminology.

Remark 1.2.8. There exists a distinguished automorphism w_N of the $\mathbb{C}$-vector space $S_k(\Gamma_0(N))$, satisfying $w_N^2 = 1$, called *Fricke involution*. For us it will suffice to know that the newform f of (1.5) is an eigenvector of w_N: there exists $\varepsilon = \pm 1$ such that $w_N f = \varepsilon f$.

1.3 Correspondences between curves

Definition 1.3.1. Given X, X' two nonsingular projective curves over a field k, a *correspondence* T *from* X *to* X' is a pair

$$X \xleftarrow[\alpha]{} Y \xrightarrow{\beta} X' \tag{1.6}$$

of two finite surjective morphisms α and β from another nonsingular projective curve Y to, respectively, X and X'.

A correspondence induces a map

$$T\colon \mathrm{Div}(X) \to \mathrm{Div}(X'), \quad P \mapsto \sum_{Q \in \alpha^{-1}(P)} \beta(Q);$$

it can be shown that T preserves degree zero and principal divisors, so it defines a map $T\colon J(X) \to J(X')$.

Example 1.3.2. Any morphism $\alpha\colon X \to X'$ defines a correspondence

$$X \xleftarrow[\alpha]{} Y = \mathrm{graph}(\alpha) \xrightarrow{\beta} X' \tag{1.7}$$

where $Y \subset X \times X'$ is the graph of α and the maps are the projections. The induced map $\mathrm{Div}(X) \to \mathrm{Div}(X')$ is given simply by $(P) \mapsto (\alpha(P))$ (we sometimes omit parentheses for divisors and write P instead of (P)).

Example 1.3.3. If T is a correspondence from X to X' as in (1.6), the *dual correspondence* T' is defined as

$$X' \xleftarrow[\beta]{} Y \xrightarrow{\alpha} X.$$

The dual correspondence of (1.7) induces on the divisor groups the map

$$\mathrm{Div}(X') \to \mathrm{Div}(X), \quad P \mapsto \sum_{Q \in \alpha^{-1}(P)} Q$$

Definition 1.3.4. Consider the modular curve $Y_0(N)$, and a prime integer p which does not divide N. The *Hecke correspondence* $T(p)$ is defined as

$$Y_0(N) \xleftarrow[\alpha]{} Y_0(pN) \xrightarrow{\beta} Y_0(N), \tag{1.8}$$

where α is the canonical projection and β is the map induced by $\mathbb{H} \to \mathbb{H}, z \mapsto pz$. For a description of the action of $T(p)$ on the points (E, S) of $Y_0(N)$ see e.g. [17], Chapter V, Section 7. There exists a unique extension of $T(p)$ to $X_0(N)$, and this is called Hecke correspondence, too.

Theorem 1.3.5 (Eichler - Shimura relation)**.** Consider the modular curve $X_0(N)$ and fix a prime p that does not divide N. Let $T(p)$ be the Hecke correspondence on $X_0(N)$, and φ_p the Frobenius automorphism of $\overline{\mathbb{F}}_p$. Then

$$T(p) = \varphi_p + \varphi_p'$$

in the ring of correspondences on $\widetilde{X}_0(N)(\overline{\mathbb{F}}_p)$ (and so also in $\mathrm{End}(J(\widetilde{X}_0(N)(\overline{\mathbb{F}}_p)))$).

Proof. See [17], Chapter V, Theorem 7.4. □

Remark 1.3.6. As correspondences on $X_0(N)$, $T(p)$ and $\varphi_p + \varphi'_p$ induce maps $\mathrm{Div}(X_0(N)) \to \mathrm{Div}(X_0(N))$. In particular, by the examples 1.3.2 and 1.3.3, we have

$$\varphi_p + \varphi'_p \colon \mathrm{Div}\left(\widetilde{X}_0(N)(\overline{\mathbb{F}}_p)\right) \to \mathrm{Div}\left(\widetilde{X}_0(N)(\overline{\mathbb{F}}_p)\right), \tag{1.9}$$
$$P \mapsto P^l + \sum_{Q^l = P} Q.$$

1.4 Group cohomology

In this section we recall the basics notions of group cohomology needed for the construction of the Selmer and Shafarevich-Tate groups.

Definition 1.4.1. Let G be a profinite group. An abelian group M is called a *G-module* if there exists an action of G on M, continuous with respect to the Krull topology of G and the discrete topology of M, which is compatible with the group operation of M; that is, G acts on M via continuous automorphisms. We'll write G multiplicatively, M additively and the action exponentially:

$$(m+n)^g = m^g + n^g \quad \forall m, n \in M, \forall g \in G.$$

If M and N are G-modules, a *G-module homomorphism* is a group homomorphism $\varphi \colon M \to N$ commuting with the actions of G:

$$\varphi(m^g) = \varphi(m)^g \quad \forall m \in M, \forall g \in G.$$

Definition 1.4.2. For a group G and a G-module M, define the *0-th cohomology group*

$$H^0(G, M) = M^G = \{\, m \in M \mid m^g = m \ \forall g \in G \,\}$$

and the *first cohomology group*

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)} = \frac{\left\{\, \xi \colon G \to M \text{ continuous} \;\middle|\; \xi(gh) = \xi(g)^h + \xi(h)\ \forall g, h \in G \,\right\}}{\{\, \xi \colon G \to M \mid \exists m \in M \text{ s.t. } \xi(g) = m^g - m \ \forall g \in G \,\}}.$$

The latter is the group of crossed homomorphisms, or *1-cocycles*, from G to M modulo the subgroup of principal cocycles, or *1-coboundaries*. We'll write $[\xi]$ for the class of a cocycle ξ.

Remark 1.4.3. Even if a cocycle ξ is not a group homomorphism, we still have $\xi(1) = 0$: $\xi(1) = \xi(1 \cdot 1) = \xi(1)^1 + \xi(1) = 2\xi(1)$, so $0 = \xi(1)$.

Remark 1.4.4. If the action of G on M is trivial, then a 1-cocycle is simply a group homomorphism, and $B^1(G, M) = 0$. So in this case $H^0(G, M) = M$ and $H^1(G, M) = \mathrm{Hom}_{\mathrm{Gr}}(G, M)$.

The first fundamental result is a version of the Snake lemma.

Lemma 1.4.5. For any exact sequence of G-modules

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$$

there is a sequence of cohomology groups

$$\begin{array}{l} 0 \longrightarrow H^0(G, M) \xrightarrow{\varphi'} H^0(G, N) \xrightarrow{\psi'} H^0(G, P) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\ \delta\ } \\ \qquad H^1(G, M) \xrightarrow{\varphi^*} H^1(G, N) \xrightarrow{\psi^*} H^1(G, P) \end{array} \tag{1.10}$$

which is exact.

In (1.10), φ' and ψ' are respectively the restrictions of φ and ψ to the subgroups $H^0(G,M) = M^G \leq M$ and $H^0(G,N) = N^G \leq N$; φ^* (and similarly ψ^*) is defined by composition: $\varphi^*([\xi]) = [\varphi \circ \xi]$. Finally the map δ, called *connecting homomorphism*, is defined as follows. For $p \in P^G$, choose $n \in \psi^{-1}(p)$; the map $g \mapsto n^g - n$ takes value in M, and defines a cocycle $G \to M$; define $\delta(p)$ to be the class of this cocycle. The proof that all these maps are well defined and that (1.10) is exact is routine.

Definition 1.4.6. Let $H \triangleleft G$ be a normal subgroup. The map

$$\mathrm{Res}\colon H^1(G,M) \to H^1(H,M), [\xi] \mapsto [\xi|_H]$$

is a group homomorphism.

Notice that M^H is a G/H-module: the action is given by $m^{gH} = m^g$. There is a group homomorphism

$$\mathrm{Inf}\colon H^1(G/H, M^H) \to H^1(G,M)$$

defined as follows: for $[\eta] \in H^1(G/H, M^H)$, consider the diagram

$$\begin{array}{ccc} G & & M \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle i} \\ G/H & \xrightarrow{\eta} & M^H \end{array} \tag{1.11}$$

and set $\mathrm{Inf}([\eta]) = [i \circ \eta \circ \pi]$. These maps are called respectively *Restriction* and *Inflation.*

Lemma 1.4.7 (Inflation-Restriction)**.** The following sequence of abelian groups

$$0 \longrightarrow H^1(G/H, M^H) \xhookrightarrow{\mathrm{Inf}} H^1(G,M) \xrightarrow{\mathrm{Res}} H^1(H,M) \tag{1.12}$$

is well defined and exact.

Proof. See for example [21], Appendix B, Proposition 1.3, on p. 417. □

Remark 1.4.8. We note here that G/H acts on $H^1(H,M)$, and the image of the map Res is actually contained in $H^1(H,M)^{G/H} = H^0(G/H, H^1(H,M))$.

1. *Action.* For $gH \in G/H$ and $[\xi] \in H^1(H,M)$, define $[\xi]^{gH}$ to be the class of the cocycle

$$\xi^{gH}\colon h \mapsto \xi(h^g)^{g^{-1}} = \xi(g^{-1}hg)^{g^{-1}}.$$

This is indeed a cocycle: $\xi^{gH}(hk) = \xi(h^g k^g)^{g^{-1}} = (\xi(h^g)^{k^g} + \xi(k^g))^{g^{-1}} = (\xi(h^g)^{k^g})^{g^{-1}} + (\xi(k^g))^{g^{-1}} = \xi(h^g)^{g^{-1}kgg^{-1}} + \xi(k^g)^{g^{-1}} = (\xi(h^g)^{g^{-1}})^k + (\xi(k^g))^{g^{-1}} = \xi^{gH}(h)^k + \xi^{gH}(k)$. Next we show that $[\xi^{gH}]$ is well defined: if $gH = fH$, then $[\xi^{gH}] = [\xi^{fH}]$. Equivalently: if $g \in H$, then $[\xi^{gH}] = [\xi^H] = [\xi]$, that is $\xi^{gH} - \xi \in B^1(H,M)$. Explicitly, we have to show that there exists $m \in M$, depending only on ξ and g, such that

$$\xi^{gH}(h) - \xi(h) = m^h - m \quad \forall h \in H.$$

The left hand side of the equation is $\xi(h^g)^{g^{-1}} - \xi(h) = \xi(g^{-1}hg)^{g^{-1}} - \xi(h) = (\xi(g^{-1}h)^g + \xi(g))^{g^{-1}} - \xi(h) = \xi(g^{-1}h) + \xi(g)^{g^{-1}} - \xi(h) = \xi(g^{-1})^h + \xi(h) + \xi(g)^{g^{-1}} - \xi(h) = \xi(g^{-1})^h + \xi(g)^{g^{-1}} = \xi(g^{-1})^h - \xi(g^{-1})$. For the last equality, notice that $\xi(g)^{g^{-1}} = -\xi(g^{-1})$, i.e. $\xi(g)^{g^{-1}} + \xi(g^{-1}) = 0$: we have $\xi(g)^{g^{-1}} + \xi(g^{-1}) = \xi(g \cdot g^{-1}) = \xi(1) = 0$. We then conclude setting $m = \xi(g^{-1})$.

2. *Res*$(H^1(G,M)) \subseteq H^1(H,M)^{G/H}$. Let $\xi \in Z^1(G,M)$; we have to show that Res$([\xi])$ is fixed by the action of G/H. Take any class gH; we need to prove Res$([\xi])^{gH} =$ Res$([\xi])$, i.e. $[\xi|_H]^{gH} = [\xi|_H]$, i.e. $(\xi|_H)^{gH} - \xi|_H \in B^1(H,M)$, i.e. that there exists $m \in M$, depending only on ξ and g, such that

$$(\xi|_H)^{gH}(h) - \xi|_H(h) = m^h - m \quad \forall h \in H.$$

Since $\xi|_H$ is the restriction of a cocycle defined on G, we may consider $m = \xi(g^{-1})$; the remaining computations are the same of point 1, so we omit them.

Lemma 1.4.9 (Lyndon-Hochschild-Serre's spectral sequence)**.** Suppose M is a G-module, and $H \triangleleft G$ a normal subgroup. Then the sequence

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G,M) \xrightarrow{\text{Res}} H^1(H,M)^{G/H} \xrightarrow{d} H^2(G/H, M^H) \tag{1.13}$$

is exact.

Proof. See for example [19], p. 568, Theorem 9.84. □

1.5 Galois cohomology of an elliptic curve

For an abelian group A and a natural number $n \in \mathbb{N}$, define $A_n = A[n]$ to be the n-torsion subgroup of A. Let K be a number field, $G = \text{Gal}(\overline{K}/K) = \text{Gal}(\overline{\mathbb{Q}}/K)$, and E an elliptic curve defined over K. One of the most important objects in our treatise will be $E_p(K) = E(K)[p]$, the p-torsion subgroup of the abelian group $E(K)$, where p is a prime number. It is known that $E_p(\overline{K}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (see e.g. [21], p. 86, Corollary 6.4).

The abelian group $E(\overline{K})$ has a natural structure of G-module, given by setting $P = (x,y) \mapsto P^\sigma = (x^\sigma, y^\sigma)$, and noting that $(P+Q)^\sigma = P^\sigma + Q^\sigma$. Thus, since $(pP)^\sigma = pP^\sigma$, the subgroup $E_p(\overline{K}) \leq E(\overline{K})$ inherits this G-module structure. We now apply the results of the previous section to the following exact sequence of $\text{Gal}(\overline{K}/\mathbb{Q})$-modules.

Proposition 1.5.1. The sequence

$$0 \longrightarrow E_p(\overline{K}) \xhookrightarrow{i} E(\overline{K}) \xrightarrow{\cdot p} E(\overline{K}) \longrightarrow 0 \tag{1.14}$$

is exact.

Proof. The map i is the inclusion, and by definition $\ker(\cdot p) = \text{im}(i)$; the only non trivial fact is that the multiplication by p is surjective. This follows since it is a non constant rational map between algebraic curves [[7], Chapter II, Proposition 6.8]. □

Applying Lemma 1.4.5 to (1.14) gives the following long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G,E_p(\overline{K})) \xhookrightarrow{i} H^0(G,E(\overline{K})) \xrightarrow{\cdot p} H^0(G,E(\overline{K})) \xrightarrow{\delta} \\ H^1(G,E_p(\overline{K})) \xrightarrow{i^*} H^1(G,E(\overline{K})) \xrightarrow{(\cdot p)^*} H^1(G,E(\overline{K})). \end{aligned} \tag{1.15}$$

The map i^* sends $[\xi]$ to $[i \circ \xi]$, and we denote this map by α; $(\cdot p)^*$ sends $[\xi]$ to $[\cdot p \circ \xi]$ (it is precisely the multiplication by p in the abelian group $H^1(G,E(\overline{K}))$, so from now on we don't write "*").

Note moreover that $H^0(G, E_p(\overline{K})) = E_p(K)$ and $H^0(G, E(\overline{K})) = E(K)$. It is customary in literature to shorten $H^1(\mathrm{Gal}(\overline{K}/K), E_p(\overline{K}))$ to $H^1(K, E_p)$. So, sequence 1.15 reads

$$\begin{array}{ccccccc} 0 & \longrightarrow & E_p(K) & \xhookrightarrow{i} & E(K) & \xrightarrow{\cdot p} & E(K) \\ & & & & & & \downarrow \delta \\ & & H^1(K, E_p) & \xrightarrow{\alpha} & H^1(K, E) & \xrightarrow{\cdot p} & H^1(K, E). \end{array} \tag{1.16}$$

Finally, from this sequence we can extract the so called *fundamental sequence of the p-torsion points of E*:

$$0 \longrightarrow E(K)/pE(K) \xhookrightarrow{\delta} H^1(K, E_p) \xrightarrow{\alpha} H^1(K, E)_p \longrightarrow 0. \tag{1.17}$$

Exactness is clear: δ is injective because we modded out $\ker(\delta) = \mathrm{im}(\cdot p) = pE(K)$; $\ker(\alpha) = \mathrm{im}(\delta)$ by the above sequence; α is surjective on its image $\mathrm{im}(\alpha) = \ker(\cdot p) \equiv H^1(K, E)_p$. The connecting homomorphism δ, here called *Kummer map*, sends the class $[P] = P + pE(K)$ to the class of the cocycle $\xi\colon \sigma \mapsto Q^\sigma - Q$, where Q is a fixed p-th root of P (see the comments after 1.4.5). We will also write such a point Q as $\frac{1}{p}P$.

Remark 1.5.2. Notice that all the abelian groups in (1.17) are annihilated by p, so they are actually $\mathbb{F}_p$-vector spaces: this is clear for the first one and the third one; for the middle one, this is true since $E_p = E_p(\overline{K}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is p-torsion, so $p[\xi] = 0$ for any cocycle ξ.

1.6 The Selmer and Shafarevich-Tate groups

If we regard E as an elliptic curve over K_v, the completion of K at a prime v (finite or infinite), we may rewrite (1.17) replacing K by K_v and $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ by $\mathrm{Gal}(\overline{K_v}/K_v)$:

$$0 \longrightarrow E(K_v)/pE(K_v) \xhookrightarrow{\delta_v} H^1(K_v, E_p) \xrightarrow{\alpha_v} H^1(K_v, E)_p \longrightarrow 0. \tag{1.18}$$

The restriction map

$$\mathrm{Gal}(\overline{K_v}/K_v) \to \mathrm{Gal}(\overline{K}/K), \quad \sigma \mapsto \sigma|_{\overline{K}}$$

defines a homomorphism

$$\mathrm{res}_v\colon H^1(K, E) \to H^1(K_v, E), \quad [\xi] \mapsto \mathrm{res}_v([\xi]) \equiv [\xi]_v = [\sigma \mapsto \xi(\sigma|_{\overline{K}})]; \tag{1.19}$$

similarly, $\mathrm{res}_v\colon H^1(K, E_p) \to H^1(K_v, E_p)$ is defined.

Lastly, there is a homomorphism

$$E(K)/pE(K) \to E(K_v)/pE(K_v), \quad P + pE(K) \mapsto P + pE(K_v).$$

If we now consider simultaneously all the primes of K, i.e. the maps $\prod_v \mathrm{res}_v$, we get the following fundamental diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xhookrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\alpha} & H^1(K, E)_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v \equiv \beta} & & \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \xhookrightarrow{\prod_v \delta_v} & \prod_v H^1(K_v, E_p) & \xrightarrow{\prod_v \alpha_v} & \prod_v H^1(K_v, E)_p & \longrightarrow & 0 \end{array} \tag{1.20}$$

We are finally ready to define the groups we are mainly interested in.

Definition 1.6.1. In the above setting, define the *p-Selmer group of* E/K to be

$$\mathrm{Sel}^{(p)}(E/K) = \ker(\beta \circ \alpha) = \ker\left(H^1(K, E_p) \to \prod_v H^1(K_v, E)_p\right)$$

and the *Shafarevich-Tate group of* E/K as

$$Ш(E/K) = \ker\left(H^1(K, E) \to \prod_v H^1(K_v, E)\right),$$

so that its p-torsion subgroup $Ш(E/K)_p$ satisfies

$$Ш(E/K)_p = \ker(\beta).$$

Remark 1.6.2. $\mathrm{Sel}^{(p)}(E/K) \leq H^1(K, E_p)$ and $Ш(E/K)_p \leq H^1(K, E)_p$, so they are $\mathbb{F}_p$-vector spaces by 1.5.2; $Ш(E/K)$ is a subgroup of $H^1(K, E)$: it consists of the classes $c = [\xi]$ that become trivial over any completion K_v, i.e. $\mathrm{res}_v(c) = 0$ for all v (finite or infinite). In other words, (see (1.19)) the cocycle $\sigma \mapsto \xi(\sigma|_{\overline{K}})$ is a coboundary in $Z^1(\mathrm{Gal}(\overline{K_v}/K_v), E)$ for all v. The importance of the Selmer and Shafarevich-Tate groups will be explained shortly.

The following crucial property is a direct consequence of the above definitions.

Proposition 1.6.3. The sequence of $\mathbb{F}_p$-vector spaces

$$0 \longrightarrow E(K)/pE(K) \xhookrightarrow{\delta} \mathrm{Sel}^{(p)}(E/K) \xrightarrow{\alpha} Ш(E/K)_p \longrightarrow 0 \tag{1.21}$$

is well defined and exact.

Proof. The image of δ is contained in the Selmer group since $\alpha \circ \delta = 0$, and we already knew that δ is injective; $\mathrm{Sel}^{(p)}(E/K) = \ker(\beta \circ \alpha) = \alpha^{-1}(\ker(\beta)) = \alpha^{-1}(Ш(E/K)_p)$, so α is surjective; $\ker(\alpha) = \mathrm{im}(\delta)$ by the exactness of the first row of diagram 1.20. □

Remark 1.6.4. Sequence (1.21) is the reason why these groups are so important. It is known that the Selmer group is finite (see e.g. [21], Chapter X, Theorem 4.2); hence, so are $E(K)/pE(K)$ and $Ш(E/K)_p$. In particular, the finiteness of the Selmer group immediately implies a historically fundamental result, the weak Mordell-Weil Theorem: $E(K)/nE(K)$ is a finite group for any integer n (we could have defined everything replacing p with any integer n).

Regarding the whole $Ш(E/K)$, it is only conjectured that it is always finite. Its order appears in the Birch and Swinnerton-Dyer conjecture, the major open question in the field of elliptic curves. Besides, proving its finiteness, or finding a bound for divisibility in it (for example, computing $Ш(E/K)[p^\infty]$ for some p, or proving $Ш(E/K)[p^\infty] = 0$ for some p - or for an infinite number of primes p) would shed light on the problem of finding an algorithm to compute generators for $E(K)/pE(K)$: this is another important question in the topic of the arithmetic of elliptic curves.

1.7 Ring class fields

In this section we review the definitions and properties of the *ring class fields* of an imaginary quadratic field K.

Definition 1.7.1. Let K be a quadratic number field. An *order* of K is a subset $\mathcal{O} \subset K$ such that

(1) $\mathcal{O}$ is a subring with 1;
(2) $\mathcal{O}$ is finitely generated as an abelian group;
(3) $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

It follows from the definitions that $\mathcal{O}$ is a free abelian group of rank 2, and that the quotient field of $\mathcal{O}$ is K. Moreover, the ring of integers $\mathcal{O}_K$ is the *maximal order* of K, in the sense that it contains any other order.

Proposition 1.7.2. Let $\mathcal{O}$ be an order in a quadratic field K. Then the index $|\mathcal{O}_K : \mathcal{O}|$ is finite; moreover, if we set $n = |\mathcal{O}_K : \mathcal{O}|$ we have

$$\mathcal{O} = \mathbb{Z} + n\mathcal{O}_K.$$

Proof. See [2], Lemma 7.2, p.133. □

We may thus write $\mathcal{O}_n$ for *the* order of index n in $\mathcal{O}_K$, i.e. $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$. In particular, $\mathcal{O}_1 = \mathcal{O}_K$. Moreover, we obtain that the inclusions between different orders of K are given by divisibility between the indices:

Lemma 1.7.3. $\mathcal{O}_n \subseteq \mathcal{O}_m$ if and only if m divides n.

The following is the main result of the section.

Theorem 1.7.4. Let K be an imaginary quadratic field. For any positive integer n there exists a unique extension K_n/K with the following properties:

(1) K_n/K is an abelian extension, i.e. it is Galois with $\mathrm{Gal}(K_n/K)$ abelian;

(2) the extension is unramified outside the set of primes of K dividing n: if $\mathfrak{p} \triangleleft \mathcal{O}_K$ ramifies in K_n, then $\mathfrak{p}$ divides the ideal $n\mathcal{O}_K$;

(3) Suppose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is principal, $\mathfrak{p} = \alpha\mathcal{O}_K$, with $\alpha \equiv a \bmod n\mathcal{O}_K$ for an integer a. If $(a, n) = 1$, then $\mathfrak{p}$ splits completely in K_n.

The field K_n is called the *ring class field* of the order $\mathcal{O}_n$. Moreover, we have that $K_m \leq K_n$ for any $m \mid n$.

Proof. See [2], Chapter Two, Section 9. □

Remark 1.7.5. In the case $n = 1$, the field K_1 is called the *Hilbert class field* of K: it is the maximal unramified abelian extension of K. Moreover, $\mathrm{Gal}(K_1/K) \cong \mathrm{Pic}(\mathcal{O}_K) = \mathrm{Cl}(\mathcal{O}_K) = I_K/P_K$, the ideal class group of K.

Proposition 1.7.6. Let K_n be the ring class field of $\mathcal{O}_n \subset \mathcal{O}_K$. Then K_n is Galois over $\mathbb{Q}$, with group

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathrm{Gal}(K_n/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K_n/K) \rtimes \langle\tau\rangle,$$

where the action of τ on $\mathrm{Gal}(K_n/K)$ is given by

$$\sigma^\tau = \tau\sigma\tau = \sigma^{-1}. \tag{1.22}$$

We say that $\mathrm{Gal}(K_n/\mathbb{Q})$ is a *generalized dihedral group.*

Proof. See [2], Lemma 9.3, p. 180. □

Theorem 1.7.7. Let K be an imaginary quadratic field, and $n = l_1 \cdot \ldots \cdot l_r$ a square-free integer such that every prime factor l_i of n is inert in K: $l_i\mathcal{O}_K = \lambda_i$. Let $\mathcal{O}_n$ be the order of index n, and K_n its associated ring class field. In this case we have:

$$\mathrm{Gal}(K_n/K_1) \cong \frac{(\mathcal{O}_K/n\mathcal{O}_K)^\times}{(\mathbb{Z}/n\mathbb{Z})^\times}. \tag{1.23}$$

Proof. See [2], Theorem 7.24, p. 146. □

Remark 1.7.8. In this situation, since $n\mathcal{O}_K = \prod_{l|n} l\mathcal{O}_K = \prod_{i=1}^r \lambda_i$, by the Chinese Remainder Theorem we have

$$\mathrm{Gal}(K_n/K_1) \cong \frac{(\mathcal{O}_K/n\mathcal{O}_K)^\times}{(\mathbb{Z}/n\mathbb{Z})^\times} \cong \prod_{i=1}^r \frac{(\mathcal{O}_K/\lambda_i)^\times}{(\mathbb{Z}/l_i\mathbb{Z})^\times} \cong \prod_{i=1}^r \frac{(\mathbb{F}_{l_i^2})^\times}{(\mathbb{F}_{l_i})^\times} \cong \prod_{i=1}^r \frac{C_{l_i^2-1}}{C_{l_i-1}} \cong \prod_{i=1}^r C_{l_i+1}, \tag{1.24}$$

where $C_{l+1} = \mathbb{Z}/(l+1)\mathbb{Z}$ denotes the cyclic group of order $l+1$. Notice that this gives in particular

$$|K_n \colon K_1| = \prod_{l|n}(l+1).$$

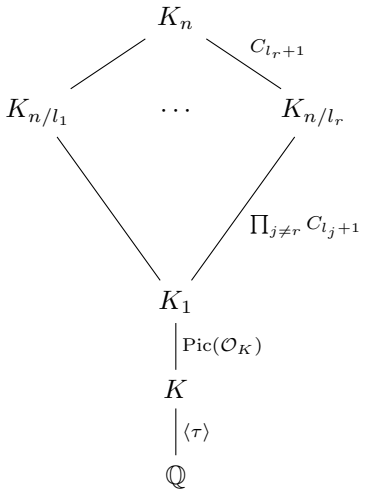
Applying (1.24) to the integers n/l_i we obtain:

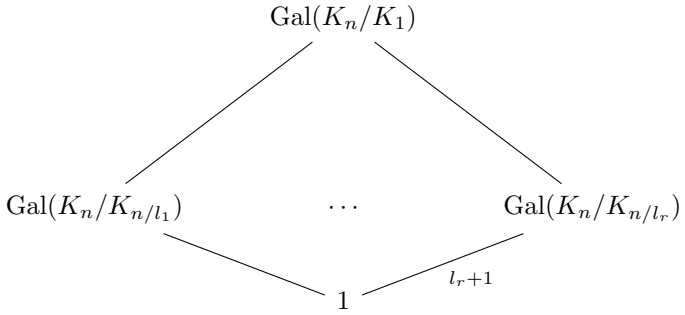
$$\mathrm{Gal}(K_{n/l_i}/K_1) \cong \prod_{j\neq i} C_{l_j+1}.$$

It follows that

$$\mathrm{Gal}(K_n/K_{n/l_i}) \cong C_{l_i+1}.$$

We have thus the following diagrams:





(1.25)

For any $i \neq j$ we have $K_{n/l_i}K_{n/l_j} = K_n$, and so $\mathrm{Gal}(K_n/K_{n/l_i}) \cap \mathrm{Gal}(K_n/K_{n/l_j}) = 1$; it follows that $\mathrm{Gal}(K_n/K_1) = \mathrm{Gal}(K_n/K_{n/l_1}) \ldots \mathrm{Gal}(K_n/K_{n/l_r})$. Since all this subgroups are normal and pairwise disjoint, we find again

$$\mathrm{Gal}(K_n/K_1) \cong \mathrm{Gal}(K_n/K_{n/l_1}) \times \cdots \times \mathrm{Gal}(K_n/K_{n/l_r}) \cong C_{l_1+1} \times \cdots \times C_{l_r+1}.$$

The statements of this section are consequences of the so called *Existence Theorem* (see e.g. [2], Chapter Two, Section 8, Theorem 8.6), one of the main results of global class field theory: we will often use another important fact, that we now state.

Theorem 1.7.9. (Čebotarev Density Theorem) Let K be a number field, L/K a Galois extension with Galois group G, and σ^G the conjugacy class of an element $\sigma \in G$. Then the set

$$S = \left\{ \mathfrak{p} \in \mathrm{Spec}(O_K) \;\middle|\; \mathfrak{p} \text{ is unramified in } L \text{ and } \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma^G \right\},$$

where $\left(\frac{L/K}{\mathfrak{p}}\right)$ is the conjugacy class of the Frobenius automorphisms of the primes $\mathfrak{P}$ over $\mathfrak{p}$, has *Dirichlet density*

$$\delta(S) = \frac{|\sigma^G|}{|G|} = \frac{|\sigma^G|}{|L:K|}.$$

Proof. For a proof of this result see e.g. [9], Chapter V, Theorem 10.4. □

Remark 1.7.10. We don't give the precise definition of Dirichlet density here, but for our purposes it will suffice to say that a set with positive density must be infinite. Therefore, Theorem 1.7.9 is often invoked to show that there is an infinite number of primes having a prescribed (conjugacy class of) automorphism(s) as their Frobenius element. Another classical consequence of Theorem 1.7.9 is Dirichlet's theorem on primes in arithmetic progressions, which in turn is used to show that there is an infinite number of primes satisfying a required congruence relation:

Theorem 1.7.11 (Dirichlet)**.** Let a and b be two coprime integers. The arithmetic progression

$$\{\, a + nb \mid n \in \mathbb{N} \,\}$$

contains an infinite number of primes.

Chapter 2

Kolyvagin classes

2.1 Summary

Consider a positive integer N and a (modular) elliptic curve $E/\mathbb{Q}$ of conductor N; let

$$\phi\colon X_0(N) \to E$$

be the modular parametrization whose existence is granted by the Modularity Theorem 1.2.6. Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field of discriminant $-D$ where all prime factors of N are split (it is certainly possible to choose a number D with this properties, because it amounts to solve a system of congruences); let $\mathcal{O}_K$ be the ring of integers of K. We further assume $D \neq 3, 4$: in this way, $U(\mathcal{O}_K) = \{\pm 1\}$.

Choose an ideal $\mathcal{N} \triangleleft \mathcal{O}_K$ with $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. The ring $\mathcal{O}_K$ and the fractional ideal $\mathcal{N}^{-1}$ are lattices in $\mathbb{C}$; then, the complex tori $\mathbb{C}/\mathcal{O}_K$ and $\mathbb{C}/\mathcal{N}^{-1}$ are complex elliptic curves related by the cyclic N-isogeny

$$\psi\colon \mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}, \quad z + \mathcal{O}_K \mapsto z + \mathcal{N}^{-1}.$$

Therefore, the point

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathbb{C}/\mathcal{N}^{-1}, \psi)$$

is a point of the moduli space $X_0(N)(\mathbb{C})$. Let K_1 be the Hilbert class field of K defined in Remark 1.7.5; the theory of complex multiplication shows that x_1 is actually rational over K_1, i.e. we have $x_1 \in X_0(N)(K_1)$ (for a proof of this fact see e.g. [3], Chapter III, Theorem 3.6). Define $y_1 = \phi(x_1) \in E(K_1)$. Finally, set

$$y_K = \mathrm{Tr}_{K_1/K}(y_1) = \sum_{\sigma \in \mathrm{Gal}(K_1/K)} {y_K}^{\sigma} \in E(K),$$

the sum being made with the group operation of E. The point y_K is particularly relevant in view of this property:

Theorem 2.1.1. (Gross-Zagier) The point y_K has infinite order in $E(K)$ if and only if $L'(E/K, 1) \neq 0$.

Proof. See [6], Chapter I, 6.5. □

Suppose that y_K has infinite order in the abelian group $E(K)$. Then, by Theorem 2.1.1, the analytic rank of E/K is at most one. But then the BSD conjecture predicts the algebraic rank to be at most one, too; since we have a point of infinite order by assumption, then we should have $\mathrm{rk}_{\mathbb{Z}} E(K) = 1$. Indeed, Victor Kolyvagin has proven the following result ([10], Theorem A).

Theorem 2.1.2 (Kolyvagin)**.** Assume that the point y_K has infinite order in $E(K)$. Then

1. the group $E(K)$ has rank 1;
2. the group $Ш(E/K)$ is finite.

Actually, the theorem is even stronger: it gives an upper bound on the order of $Ш(E/K)$. We are not going to prove the full Theorem, but instead will sketch the proof of a slightly weaker result; in doing so, we will illustrate the tools, techniques and main arguments employed by Kolyvagin. From now on, we are going to assume the following:

1. The curve E does *not* have complex multiplication, i.e. $\mathrm{End}(E) = \mathbb{Z}$;
2. $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$;

in fact, Serre has showed that assumption (2) is verified for all sufficiently large primes p ([20], Theorem 2).

Remark 2.1.3. Under these assumptions, the curve E has no p-torsion rational over $\mathbb{Q}$, i.e. $E(\mathbb{Q})_p = 0$. Indeed, the only other possibilities are $E(\mathbb{Q})_p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and $E(\mathbb{Q})_p \cong \mathbb{Z}/p\mathbb{Z}$, but in any case the representation

$$\rho\colon \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \to GL_2(\mathbb{F}_p) \tag{2.1}$$

defined in (1.1) would not be surjective. The first case can't occur because we would have $\mathbb{Q}(E_p) = \mathbb{Q}$. The second case is impossible too: if existed a nontrivial point $P \in E_p \cap E(\mathbb{Q})$ we could choose it as the first element of a basis of E_p; then, the image of ρ would be contained in a subgroup of the form

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

The main result we are going to establish in this thesis is the following.

Theorem 2.1.4. Let p be an odd prime such that $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$ and $y_K \notin pE(K)$. Then

1. the rank of $E(K)$ is 1.
2. $Ш(E/K)_p = 0$.

Remark 2.1.5. Since the group $E(K)$ is finitely generated, the point y_K is not infinitely divisible: there exist only finitely many integers n such that y_K lies in $nE(K)$. Therefore, the assumption $y_K \notin pE(K)$ made in the statement of the Theorem excludes only finitely many primes.

We recall here the fundamental exact sequence (1.21) of the Selmer and Shafarevich-Tate groups:

$$0 \longrightarrow E(K)/pE(K) \xhookrightarrow{\delta} \mathrm{Sel}^{(p)}(E/K) \xrightarrow{\alpha} Ш(E/K)_p \longrightarrow 0 \tag{2.2}$$

The proof of 2.1.4 will be an easy consequence of the following.

Proposition 2.1.6. Let p be an odd prime satisfying the hypotheses of Theorem 2.1.4.
Then $\mathrm{Sel}^{(p)}(E/K) = \langle \delta y_K \rangle$, cyclic of order p.

2.2 The Euler system of Heegner points

The first step towards the proof of Proposition 2.1.6 is the construction of a collection of points y_n, called *Heegner points*, on the curve E which are rational over the ring class fields K_n. This family of points enjoys some compatibility properties, which will be explained in Proposition 2.2.10, that make it an *Euler system*.

Let $n \in \mathbb{N}$ be prime to N and consider $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$, the order of conductor n in $\mathcal{O}_K$; let $\mathcal{N} \triangleleft \mathcal{O}_K$ be as in the previous section. The ideal $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$ is an invertible $\mathcal{O}_n$-module, and we have $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$. It follows that the map

$$\psi_n \colon \mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}$$

is a cyclic N-isogeny. Hence, it defines a point x_n of the modular curve $X_0(N)$. The theory of complex multiplication shows that x_n is rational over K_n, the ring class field of $\mathcal{O}_n$.

Remark 2.2.1. Notice that we have already defined y_1 in the previous section, as $\mathcal{O}_1 = \mathcal{O}_K$.

For any $n \geq 1$ we have the following field diagram, with Galois groups indicated (see (1.25)):

$$\begin{array}{c} K_n \\ \Big| {\scriptstyle G_n \cong (\mathcal{O}_K/n\mathcal{O}_K)^\times/(\mathbb{Z}/n\mathbb{Z})^\times} \\ K_1 \\ \Big| {\scriptstyle \mathrm{Pic}(\mathcal{O}_K)} \\ K \\ \Big| {\scriptstyle \langle\tau\rangle} \\ \mathbb{Q} \end{array} \tag{2.3}$$

From now on, we are going to consider only squarefree integers n: write $n = \prod l$; furthermore, we ask that $(n, 2pND) = 1 = (pN, D)$. Since $x_n \in X_0(N)$ and $X_0(N)$, E,ϕ are defined over $\mathbb{Q}$, we may define $y_n = \phi(x_n) \in E(K_n)$.

Lemma 2.2.2. For any prime divisor l of n, l is unramified in the extension $L = K(E_p)$.

Proof. It is enough to show that l is unramified both in K and $\mathbb{Q}(E_p)$. The first assertion is straightforward, since l does not divide $2D$. For the second, notice that the assumption that l does not divide N, and the fact that N is the conductor of E, imply that E has good reduction at l. Now we need the following result.

Lemma 2.2.3. Let E be an elliptic curve defined over $\mathbb{Q}$, l a prime number of good reduction for E and $F = \mathbb{Q}(E_p)$; then $E_p(F)$ is unramified at l, i.e.: for all primes Λ of F over l, the inertia subgroup $I_{\Lambda/l}$ of $\mathrm{Gal}(F/\mathbb{Q})$ acts trivially on $E_p(\overline{\mathbb{Q}}) = E_p(F)$.

Proof. This is a particular case of Theorem (3.3) in [8] (p. 297), which is a consequence of the criterion of Néron-Ogg-Shafarevich. □

Recall that $\#I_{\Lambda/l} = e(\Lambda/l)$, the ramification index. Since $I_{\Lambda/l}$ fixes $E_p(F)$ by the lemma, we have that

$$(x^\sigma, y^\sigma) = (x, y) \quad \forall (x, y) \in E_p(F),\ \forall \sigma \in I_{\Lambda/l},$$

i.e. $I_{\Lambda/l}$ fixes $\mathbb{Q}(E_p) = F$. Hence $I_{\Lambda/l} \leq \mathrm{Gal}(F/F) = 1$, so l is unramified in $F = \mathbb{Q}(E_p)$. □

Remark 2.2.4. Notice that we have also proved that $K \cap \mathbb{Q}(E_p) = \mathbb{Q}$. Indeed, the primes that ramify in K are the divisors of D; but these primes are unramified in $\mathbb{Q}(E_p)$ being primes of good reduction, since $(D, pN) = 1$. Therefore we can't have $K \leq \mathbb{Q}(E_p)$, and so the claim follows (remember that $|K : \mathbb{Q}| = 2$).

Since l is unramified in $L = K(E_p)$, we can consider its Frobenius conjugacy class $\left(\frac{L/\mathbb{Q}}{l}\right)$. We recall the definition: for a prime Λ of L dividing l, the Frobenius element $\left(\frac{L/\mathbb{Q}}{\Lambda}\right)$ is the generator of the decomposition group $D_{\Lambda/l} \leq \mathrm{Gal}(L/\mathbb{Q})$. We also denote it by writing σ_Λ; it is the only element of $\mathrm{Gal}(L/K)$ satisfying the property

$$\sigma_\Lambda(x) \equiv x^l \bmod \Lambda, \ \forall x \in \mathcal{O}_L.$$

If Λ' is another prime over l, then σ_Λ and $\sigma_{\Lambda'}$ are conjugate elements of $\mathrm{Gal}(L/\mathbb{Q})$: more precisely, we can write $\Lambda' = \rho(\Lambda)$ for an element $\rho \in \mathrm{Gal}(L/\mathbb{Q})$, and we have the relation

$$\left(\frac{L/\mathbb{Q}}{\rho(\Lambda)}\right) = \rho \left(\frac{L/\mathbb{Q}}{\Lambda}\right) \rho^{-1}$$

(see e.g. [9], Chapter III, Property 2.2). The conjugacy class of σ_Λ and $\sigma_{\Lambda'}$ is denoted as $\left(\frac{L/\mathbb{Q}}{l}\right)$, or $\mathrm{Frob}(l)$. We ask this class to be equal to $\mathrm{Frob}(\infty)$, the class of the complex conjugation $\widetilde{\tau} \in \mathrm{Gal}(L/\mathbb{Q})$ (of course L is not a real field). By the Čebotarev density theorem, the density of the set of primes l satisfying this requirement is positive, so there is an infinite number of them.

Lemma 2.2.5. Any prime number l satisfying these conditions is inert in K.

Proof. For any prime Λ of L lying over l, σ_Λ and $\widetilde{\tau}$ are conjugate in $\mathrm{Gal}(L/\mathbb{Q})$: hence, their images $\sigma_\Lambda|_K$ and $\widetilde{\tau}|_K = \tau$ in $\mathrm{Gal}(K/\mathbb{Q})$ are conjugate, and so equal. This means that l does not split in K and thus, being unramified, is inert. □

In view of this fact we may write $(l)\mathcal{O}_K = \lambda$, and note that $\mathcal{O}_K/\lambda \cong \mathbb{F}_{l^2}$; we denote this residue field by F_λ. Note moreover that λ splits completely in L: since the Frobenius automorphism $\left(\frac{L/\mathbb{Q}}{l}\right)$ is conjugate to $\widetilde{\tau}$, it has order 2, and so $2 = \#D_{\Lambda/l} = |\mathcal{O}_L/\Lambda : \mathbb{Z}/l\mathbb{Z}|$. Thus the residue degrees are $f(\Lambda/l) = 2 = f(\lambda/l)$, and this implies that $f(\Lambda/\lambda) = 1$; but we already knew that the ramification index $e(\Lambda/\lambda)$ was equal to 1, and the claimed assertion follows.

Lemma 2.2.6. Consider the reduction $\widetilde{E}$ of E over $\mathbb{F}_l$, and define $a_l = l + 1 - \#\widetilde{E}(\mathbb{F}_l)$. Then:

$$a_l \equiv l + 1 \equiv 0 \mod p.$$

Proof. Denote with φ the Frobenius automorphism of $\widetilde{E}(\overline{\mathbb{F}}_l)$, which sends (x, y) to (x^l, y^l). From the theory of elliptic curves over finite fields (see for example [21], Chapter V, section 1), we know that the characteristic polynomials of φ and τ acting on $\widetilde{E}(\overline{\mathbb{F}}_l)$ are respectively $x^2 - a_l x + l$ and $x^2 - 1$. Since the automorphisms φ and τ of the $\mathbb{F}_p$-vector space $\widetilde{E}(\overline{\mathbb{F}}_l)_p$ are conjugate, their characteristic polynomials are equal: $-a_l \equiv 0$ and $l \equiv -1 \bmod (p)$. □

Remark 2.2.7. As a consequence, $p \mid l + 1 \pm a_l$. It is actually possible to ask, and we will make this assumption, that the prime l also satisfies $p^2 \nmid l + 1 \pm a_l$, and there exist infinitely many such primes by Čebotarev density theorem. For a proof, see [12], Proposition 3.27, end of the proof.

We make here an observation which will be useful later on.

Lemma 2.2.8. We have: $\widetilde{E}(F_\lambda)_p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. Recall that $\widetilde{E}(\overline{F}_\lambda)_p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by remark 1.1.3. A known fact about elliptic curves over finite fields (see again [21], Chapter V, section 1) is that $\#\widetilde{E}(F_\lambda) = (l+1-a_l)(l+1+a_l)$; let τ act on $\widetilde{E}(F_\lambda)$ and denote the eigenspaces as $\widetilde{E}(F_\lambda)^+$ and $\widetilde{E}(F_\lambda)^-$. We have $\#\widetilde{E}(F_\lambda)^+ = \#\widetilde{E}(\mathbb{F}_l) = l+1-a_l$, so $\#\widetilde{E}(F_\lambda)^- = l+1+a_l$. Since both these numbers are multiple of p by 2.2.6, taking the p-torsion subgroups of the two eigenspaces yields $\widetilde{E}(F_\lambda)_p^+ \cong \mathbb{Z}/p\mathbb{Z} \cong \widetilde{E}(F_\lambda)_p^-$, and so the claim. □

Write now $n = \prod l$ and define $G_n = \mathrm{Gal}(K_n/K_1)$; then we have $G_n \cong \prod_l G_l$, where, for any l, $G_l = \mathrm{Gal}(K_n/K_{n/l})$ (see (1.25)). For each l, these subgroups are cyclic of order $l+1$: ; write $G_l = \langle \sigma_l \rangle$. Consider the group ring

$$\mathbb{Z}[G_l] = \left\{ \sum_{i=0}^{l} m_i \sigma_l^i \;\middle|\; m_i \in \mathbb{Z} \right\};$$

the augmentation ideal of this ring, i.e. the kernel of the augmentation map

$$\varepsilon \colon \mathbb{Z}[G_l] \to \mathbb{Z}, \quad \sum_{i=0}^{l} m_i \sigma_l^i \mapsto \sum_i m_i,$$

is a principal ideal generated by the element $\sigma_l - 1$ ([19], p. 521, Lemma 9.24).

Define $\mathrm{Tr}_l = \sum_{\sigma \in G_l} \sigma = \sum_{i=0}^{l} \sigma_l^i$; since $\varepsilon(\mathrm{Tr}_l) = l+1$, we have $l+1-\mathrm{Tr}_l \in \ker(\varepsilon) = (\sigma_l - 1)$. So there exists $D_l \in \mathbb{Z}[G_l]$ such that

$$(\sigma_l - 1) \cdot D_l = l + 1 - \mathrm{Tr}_l. \tag{2.4}$$

Finally, define $D_n = \prod_l D_l \in \mathbb{Z}[G_n]$.

Proposition 2.2.9. The point $D_n y_n \in E(K_n)$ gives a class $[D_n y_n] \in E(K_n)/pE(K_n)$ which is fixed by the action of G_n.

Proof. The group $G_n = \mathrm{Gal}(K_n/K_1)$ naturally acts on $E(K_n)$, hence also on $E(K_n)/pE(K_n)$: if $\sigma \in G_n$, $\sigma([P]) = [P]^\sigma := [P^\sigma]$. The action is well defined because $P \in pE(K_n)$ implies $P^\sigma \in pE(K_n)$: $P = pQ$ implies $P^\sigma = (pQ)^\sigma = pQ^\sigma$. Moreover, we may write the action on the left as well as on the right because G_n is abelian.

It is sufficient to prove $[D_n y_n]^{\sigma_l} = [D_n y_n]$, i.e. $(D_n y_n)^{\sigma_l} - D_n y_n \in pE(K_n)$, for all l, because $\langle \sigma_l \,|\, l \text{ divides } n \rangle = G_n$. As said, we also write $(D_n y_n)^{\sigma_l} = \sigma_l(D_n y_n)$, and $(D_n y_n)^{\sigma_l} - D_n y_n = (\sigma_l - 1) D_n y_n$; what we need to prove is then $(\sigma_l - 1) D_n y_n \in pE(K_n)$.

Write $n = lm$. By the defining property of D_l we have

$$(\sigma_l - 1) D_n = (\sigma_l - 1) D_l D_m = (l + 1 - \mathrm{Tr}_l) D_m,$$

so

$$(\sigma_l - 1) D_n y_n = (l + 1 - \mathrm{Tr}_l) D_m y_n = (l+1) D_m y_n - D_m \mathrm{Tr}_l y_n.$$

By Lemma 2.2.6, p divides $l+1$; so it is enough to show $\mathrm{Tr}_l y_n \in pE(K_m) \subseteq pE(K_n)$. This follows from the following proposition. □

Proposition 2.2.10. Write as before $n = l \cdot m$. Then:

1. $\mathrm{Tr}_l y_n = a_l y_m \in E(K_m)$;

2. Consider the inclusions of fields $\mathbb{Q} \leq K \leq K_m \leq K_n$. Write $\lambda_m \triangleleft \mathcal{O}_{K_m}$ and $\lambda_n \triangleleft \mathcal{O}_{K_n}$ for prime ideals above $\lambda = (l)\mathcal{O}_K$. We have the following congruence relation:

$$y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \pmod{\lambda_n},$$

where $\mathrm{Frob}(\lambda_m) = \left(\frac{K_m/\mathbb{Q}}{\lambda_m}\right)$.

Proof. 1) This is a consequence of the corresponding facts about x_n and x_m in $X_0(N)(K_n)$. Denote with $T_l = T(l)$ the Hecke correspondence defined in (1.8), and recall that $\phi\colon X_0(N) \to E$ is the modular parametrization of E. We have

$$\mathrm{Tr}_l(x_n) = T_l(x_m) \in \mathrm{Div}(X_0(N)(K_m)); \tag{2.5}$$

moreover, $\phi(T_l d) = a_l \cdot \phi(d)$ for any divisor d on $X_0(N)$ (see [5], Section 6 for the proofs of these equalities). Applying this equality to $d = x_m$ gives

$$a_l y_m = a_l \phi(x_m) = \phi(T_l x_m) = \phi(\mathrm{Tr}_l(x_n)) = \mathrm{Tr}_l(\phi(x_n)) = \mathrm{Tr}_l y_n, \tag{2.6}$$

which is what we needed to prove.

2) By class field theory, λ splits completely in K_m and any prime λ_m of K_m over λ is totally ramified in K_n: $\lambda_m \mathcal{O}_{K_n} = \lambda_n^{l+1}$. In particular, the residue fields are all isomorphic: $F_{\lambda_n} \cong F_{\lambda_m} \cong F_\lambda \cong \mathbb{F}_{l^2}$.

Lemma 2.2.11. We have the congruence relation

$$x_n \equiv \mathrm{Frob}\lambda_m(x_m) \quad \text{on } \widetilde{X}_0(N)(F_{\lambda_n}).$$

Proof. We apply the Eichler-Shimura relation (Theorem 1.3.5) to the correspondence T_l of $X_0(N)$:

$$T_l = \varphi_l + \varphi_l' \in \mathrm{End}\left(\mathrm{Div}\left(\widetilde{X}_0(N)(F_\lambda)\right)\right).$$

Recall that $\varphi_l + \varphi_l'$ acts on divisors as $P \mapsto P^l + \sum_{Q^l = P} Q$; but $F_\lambda = \mathbb{F}_{l^2}$, so $Q^l = P \iff Q = P^l$. Then, $\varphi_l + \varphi_l'$ sends P to $P^l + lP^l = (l+1)P^l$. If we evaluate this at the divisor $(\widetilde{x}_m)$ we obtain

$$T_l(\widetilde{x}_m) = (l+1)(\widetilde{x}_m^l);$$

putting this together with (2.5) we have

$$(l+1)(\widetilde{x}_m^l) = T_l(\widetilde{x}_m) = \mathrm{Tr}_l(\widetilde{x}_n) = \sum_{i=0}^{l} \sigma_l^i(\widetilde{x}_n) = \sum_{i=0}^{l} (\widetilde{x}_n) = (l+1)(\widetilde{x}_n)$$

(we used that $\sigma_l(x_n) \equiv (x_n) \bmod \lambda_n$: the extension K_n/K_m is totally ramified at λ_m and $\langle \sigma_l \rangle = I(\lambda_n/\lambda_m) = D(\lambda_n/\lambda_m)$). We conclude that $x_n \equiv x_m^l \equiv \mathrm{Frob}\lambda_m(x_m)$, which is what we wanted to prove. □

The result of the Proposition follows by applying the modular parametrization ϕ to this congruence. □

This completes the proof of Proposition 2.2.9, because $\mathrm{Tr}_l y_n = a_l y_m \in pE(K_m)$ since a_l is a multiple of p by 2.2.6.

2.3 Construction of the classes

Write $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$, so that we have the following exact sequence of abelian groups:

$$0 \to G_n \to \mathcal{G}_n \to \mathrm{Gal}(K_1/K) \to 0.$$

Let S be a transversal for G_n in $\mathcal{G}_n$, i.e. a complete system of coset representatives: $\#S = |\mathcal{G}_n : G_n|$ and $\mathcal{G}_n = \bigcup_{\sigma\in S} \sigma G_n$. For any $m|n$, define

$$P_m = \sum_{\sigma\in S} \sigma(D_m y_m) \in E(K_m). \tag{2.7}$$

Remark 2.3.1. This definition depends on the choice of S; what will be relevant for us is that the class of P_m in $E(K_m)/pE(K_m)$, which we denote by $[P_m]$, does not depend on this choice. Indeed, suppose S' is another transversal; then for any $\sigma' \in S$ there is a unique $\sigma \in S$ such that $\sigma'\sigma^{-1} \in G_n$. Then, $[D_m y_m]^{\sigma'\sigma^{-1}} = [D_m y_m]$, i.e. $[D_m y_m]^{\sigma'} = [D_m y_m]^{\sigma}$. So we have

$$\left[\sum_{\sigma'\in S'} \sigma'(D_m y_m)\right] = \sum_{\sigma'\in S'} \sigma'([D_m y_m]) = \sum_{\sigma\in S} \sigma([D_m y_m]) = [P_m].$$

Remark 2.3.2. For $m = 1$, we have

$$P_1 = \sum_{\sigma\in S} \sigma(D_1 y_1) = \sum_{\sigma\in S} \sigma(y_1) = \sum_{\sigma\in \mathrm{Gal}(K_1/K)} \sigma(y_1) = \mathrm{Tr}_{K_1/K}(y_1) = y_K.$$

Lemma 2.3.3. The class $[P_n]$ belongs to $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.

Proof. Since $[P_n]$ is fixed by G_n by Proposition 2.2.9, $\mathcal{G}_n = \bigcup_{\sigma\in S} \sigma G_n$ and $\mathcal{G}_n$ is abelian, it is enough to show $[P_n]^\sigma = [P_n]$ for $\sigma \in S$. For $\rho \in S$ we have

$$[P_n]^\rho = [P_n^\rho] = \sum_{\sigma\in S} [\rho\sigma(D_n y_n)] = [P_n],$$

because ρS is another set of coset representatives for G_n in $\mathcal{G}_n$, so the last equality is given by remark 2.3.1. □

Consider now the following diagram.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(K_n/K, E(K_n))_p & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & E(K)/pE(K) & \xhookrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\alpha} & H^1(K, E)_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xhookrightarrow{\delta_n} & H^1(K_n, E_p)^{\mathcal{G}_n} & \xrightarrow{\alpha_n} & H^1(K_n, E)_p^{\mathcal{G}_n} & &
\end{array} \tag{2.8}$$

The rows and the right column are exact; the right column is obtained taking the p-torsion subgroups in the Inflation-Restriction exact sequence 1.4.7, with $G = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$, $G/H = \mathrm{Gal}(K_n/K) = \mathcal{G}_n$, $M = E(\overline{\mathbb{Q}})$ and $M^H = E(K_n)$. We use the notation $H^1(K_n/K, E(K_n))$ for $H^1(\mathrm{Gal}(K_n/K), E(K_n))$.

Lemma 2.3.4. In diagram (2.8) the vertical middle map,

$$\mathrm{Res}\colon H^1(K, E_p) \to H^1(K_n, E_p)^{\mathcal{G}_n},$$

is an isomorphism.

Proof. Lemma 1.4.9 for $M = E_p$, $G = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$ (so that $G/H = \mathrm{Gal}(K_n/K) = \mathcal{G}_n$ and $M^H = E_p(K_n)$) gives

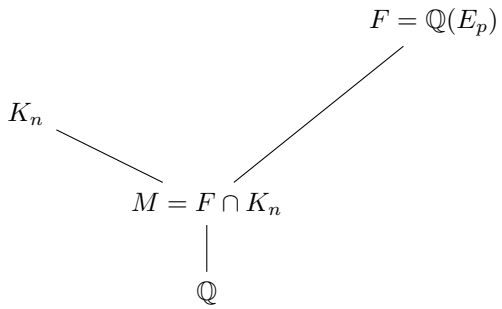
$$0 \longrightarrow H^1(\mathcal{G}_n, E_p(K_n)) \xrightarrow{\mathrm{Inf}} H^1(K, E_p) \xrightarrow{\mathrm{Res}} H^1(K_n, E_p)^{\mathcal{G}_n} \xrightarrow{d} H^2(\mathcal{G}_n, E_p(K_n)) \quad (2.9)$$

Since $H^1(\mathcal{G}_n, E_p(K_n)) = 0 = H^2(\mathcal{G}_n, E_p(K_n))$ by the following lemma, then $\ker(\mathrm{Res}) = \mathrm{im}(\mathrm{Inf}) = 0$ and $\mathrm{coker}(\mathrm{Res}) = 0$, and the conclusion follows. □

Lemma 2.3.5. The curve E has no p-torsion rational over K_n, i.e. $E_p(K_n) = 0$.

Proof. Fix n. We prove the result by excluding the other two possibilities, which are $E_p(K_n) = \mathbb{Z}/p\mathbb{Z}$ and $E_p(K_n) = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by remark 1.1.3.

First case: $E_p(K_n) \cong \mathbb{Z}/p\mathbb{Z}$. Let $F = \mathbb{Q}(E_p)$ and $M = F \cap K_n$; consider the following field diagram.



(2.10)

We know that $F/\mathbb{Q}$ is Galois, with group $\mathrm{Gal}(F/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$; K_n is a Galois extension of $\mathbb{Q}$ (actually an abelian one, but here we don't need this), and so also $M/\mathbb{Q}$ is Galois. The group $\mathrm{Gal}(F/\mathbb{Q})$ acts faithfully on $E_p(F)$, because the representation

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_p)$$

has kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$; write with an abuse of notation

$$\rho\colon \mathrm{Gal}(F/\mathbb{Q}) \to GL_2(\mathbb{F}_p).$$

Since $E_p(K_n) \cong \mathbb{Z}/p\mathbb{Z}$, there exists a non zero point $P \in E_p(K_n) \cap E_p(F) = E_p(M)$. M is Galois over $\mathbb{Q}$, so

$$P^\sigma \in E_p(M) = \mathbb{Z}/p\mathbb{Z} \cdot P \quad \forall \sigma \in \mathrm{Gal}(F/\mathbb{Q});$$

then

$$\forall \sigma \in \mathrm{Gal}(F/\mathbb{Q}) \ \exists a_\sigma \in (\mathbb{Z}/p\mathbb{Z})^* \text{ such that } P^\sigma = a_\sigma P.$$

If we choose a basis for $E_p(F) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ whose first element is P, it follows that $\rho(\sigma)$ is an upper triangular matrix for any $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$; this contradicts the surjectivity of the representation.

Second case: $E_p(K_n) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In this case, $K_n \geq \mathbb{Q}(E_p)$, so there is a surjective homomorphism $\mathrm{Gal}(K_n/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$. But when $p \geq 2$, $GL_2(\mathbb{F}_p)$ is not a quotient of a group of dihedral type. □

We are now ready to define Kolyvagin's classes, with a diagram chase in (2.8). The class $[P_n]$ lies in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$; consider its image $\delta_n[P_n] \in H^1(K_n, E_p)^{\mathcal{G}_n}$. From what we have just proved, there exist a unique class $c(n) \in H^1(K, E_p)$ such that

$$\mathrm{Res}(c(n)) = \delta_n[P_n] \in H^1(K_n, E_p)^{\mathcal{G}}_n.$$

Define

$$d(n) = \alpha(c(n)) \in H^1(K, E)_p;$$

note that $\mathrm{Res}(d(n)) = \mathrm{Res}(\alpha(c(n))) = \alpha_n(\mathrm{Res}(c(n))) = \alpha_n(\delta_n P_n) = 0$. So $d(n) \in \ker(\mathrm{Res}) = \mathrm{im}(\mathrm{Inf})$: define $\widetilde{d}(n)$ to be the only element of $H^1(\mathrm{Gal}(K_n/K), E)_p$ such that

$$\mathrm{Inf}(\widetilde{d}(n)) = d(n) \in H^1(K, E)_p.$$

The following result gives a concrete description of the classes.

Lemma 2.3.6. Let $\frac{1}{p}P_n$ be a fixed p-th root of P_n in $E(\overline{\mathbb{Q}})$.

(1) The class $c(n)$ is represented by the cocycle

$$\xi_n \colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to E_p(\overline{\mathbb{Q}}), \quad \sigma \mapsto \xi_n(\sigma) = \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{(\sigma-1)P_n}{p},$$

where $\frac{(\sigma-1)P_n}{p}$ is the unique p-th root of $(\sigma-1)P_n$ in $E(K_n)$.

(2) The class $\widetilde{d}(n)$ is represented by the cocycle

$$\eta_n \colon \mathrm{Gal}(K_n/K) \to E(K_n), \quad \sigma \mapsto \eta_n(\sigma) = -\frac{(\sigma-1)P_n}{p}.$$

Proof. (1) First of all notice that $\frac{(\sigma-1)P_n}{p}$ is indeed rational over K_n: for a fixed σ, Lemma 2.3.3 implies $\sigma P_n - P_n \in pE(K_n)$. Uniqueness follows from Lemma 2.3.5. Uniqueness implies that the application $\chi \colon \sigma \mapsto \frac{(\sigma-1)P_n}{p}$ is a cocycle, because both $\chi(\rho\sigma) = \frac{(\rho\sigma-1)P_n}{p}$ and $\sigma\chi(\rho) + \chi(\sigma) = \sigma\frac{(\rho-1)P_n}{p} + \frac{(\sigma-1)P_n}{p}$ are points of $E(K_n)$ which are p-th roots of $\sigma\rho P_n - P_n = \rho\sigma P_n - P_n$ (remember that $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$ is abelian).

So the map ξ_n is a cocycle; it takes value in E_p because $p\xi_n(\sigma) = \sigma(P_n) - P_n - \sigma(P_n) + P_n = 0$ for all σ; finally, its restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$ is

$$\xi_n \colon \mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \to E_p(\overline{\mathbb{Q}}), \quad \sigma \mapsto \xi_n(\sigma) = \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n$$

because $(\sigma-1)P_n = 0$. Therefore (see diagram 2.8), $\mathrm{Res}([\xi_n]) = \delta_n[P_n]$, and this proves that $[\xi_n] = c(n)$.

(2) We proved above that η_n is indeed a cocycle. Consider $\mathrm{Inf}([\eta_n]) \in H^1(K, E)_p$: we need to show it is equal to $d(n) = \alpha[\xi_n]$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ we have

$$\xi_n(\sigma) - \eta_n(\sigma|_{K_n}) = \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n,$$

which is a coboundary since $\frac{1}{p}P_n \in E(\overline{K})$. We conclude that $\mathrm{Inf}([\eta_n]) = d(n)$, so $[\eta_n] = \widetilde{d}(n)$ by the injectivity of the Inflation map. □

Proposition 2.3.7. 1. The class $c(n)$ is trivial in $H^1(K, E_p)$ if and only if $P_n \in pE(K_n)$;

2. the class $d(n)$ is trivial in $H^1(K, E)_p$, and the class $\widetilde{d}(n)$ is trivial in $H^1(K_n/K, E)_p$, if and only if $P_n \in pE(K_n) + E(K)$.

Proof. This follows from the definitions and diagram (2.8):
(1) $c(n) = 0 \in H^1(K, E_p) \iff \mathrm{Res}(c(n)) = 0 \iff \delta_n[P_n] = 0 \iff [P_n] = 0 \iff P_n \in pE(K_n)$.
(2) We have that

$$\begin{aligned} d(n) = 0 \in H^1(K, E)_p &\iff c(n) \in \ker(\alpha) = \mathrm{im}(\delta) \\ &\iff c(n) = \delta(P + pE(K)) \ \exists P \in E(K) \\ &\iff \mathrm{Res}(\delta(P + pE(K))) = \delta_n(P_n + pE(K_n)) \ \exists P \in E(K) \\ &\iff \delta_n(P + pE(K_n)) = \delta_n(P_n + pE(K_n)) \ \exists P \in E(K) \\ &\iff P + pE(K_n) = P_n + pE(K_n) \ \exists P \in E(K) \\ &\iff P_n \in E(K) + pE(K_n). \end{aligned}$$

□

The following proposition specializes 2.3.7 to the case $n = 1$.

Proposition 2.3.8. (1) The class c_1 is trivial if and only if $P_1 = y_K$ is divisible by p in $E(K)$;

(2) the classes d_1 and $\widetilde{d}_1$ are always trivial.

Proof. (1) By the previous proposition, $c_1 = 0 \iff P_1 = y_K \in pE(K_1)$; since $y_K \in E(K)$, the conclusion follows by the equality $E(K) \cap pE(K_1) = pE(K)$, that we now prove.
($\supseteq$) this inclusion is trivial: if $P \in pE(K)$, $P = pQ$ for a point $Q \in E(K)$; $E(K) \subseteq E(K_1)$, so $P \in pE(K_1)$.
($\subseteq$) take $P \in E(K)$ and assume $P = pQ$ for a $Q \in E(K_1)$: we need to prove that Q actually lies in $E(K)$. For any $\sigma \in \mathrm{Gal}(K_1/K)$, $pQ^\sigma = (pQ)^\sigma = P^\sigma = P$, so Q^σ is another p-th root of P: in other words, $Q^\sigma - Q \in E(K_1)_p$. But the latter group is trivial by lemma 2.3.5, and so $Q^\sigma = Q$ for any σ: this is equivalent to $Q \in E(K)$.
(2) $d_1 = 0 \iff P_1 = y_K \in pE(K_1) + E(K)$, which is true since $y_K \in E(K)$. □

2.4 Global properties of the classes

Notice that $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ acts on $H^1(K, E_p)$ by remark 1.4.8 applied to $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, $G/H = \mathrm{Gal}(K/\mathbb{Q})$, $M = E_p(\overline{\mathbb{Q}})$. Since $\tau^2 = 1$ and p is odd (so that $x^2 - 1$ has two distinct eigenvalues), there is the following decomposition into eigenspaces for τ:

$$H^1(K, E_p) = H^1(K, E_p)^+ \oplus H^1(K, E_p)^-$$

We are going to show that each Kolyvagin class $c(n)$ lies in one of these eigenspaces.

Observe that complex conjugation τ acts also on the Galois extension K_n, and hence on the point $y_n \in E(K_n)$.

Recall that f, the newform attached to the modular curve E by the Modularity Theorem 1.2.6, is an ε-eigenvector for the Fricke involution w_N, i.e. $w_N(f) = \varepsilon f = \pm f$. With the next results we are going to relate ε and the classes $c(n)$, $d(n)$.

Lemma 2.4.1. There exists $\sigma' \in \mathcal{G}_n = \mathrm{Gal}(K_n/K)$ such that

$$y_n^\tau \equiv \varepsilon \cdot y_n^{\sigma'} \mod E(K_n)_{\mathrm{tors}}.$$

Proof. By [5], paragraph 5, there exists $\sigma' \in \mathcal{G}_n$ satisfying

$$x_n^\tau = w_N(x_n^{\sigma'})$$

on $X_0(N)$. Hence on $J(X_0(N))$ we have

$$(x_n - \infty)^\tau = w_N(x_n - \infty)^{\sigma'} + (w_N\infty - \infty)$$

A known fact is that $(w_N\infty - \infty) = (0 - \infty)$ is torsion in $J(X_0(N))$ (see e.g. [13], Chapter II, Section 11, Proposition 11.1); this gives the claim on E. □

Proposition 2.4.2. Write $f_n = \#\{\, l \mid l \text{ divides } n \,\}$, and let $\varepsilon_n = \varepsilon \cdot (-1)^{f_n}$.

(1) $[P_n]$ belongs to the ε_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$, i.e.

$$[P_n]^\tau = \varepsilon_n [P_n].$$

(2) $c(n)$ belongs to $H^1(K, E_p)^{\varepsilon_n}$, and $d(n)$ belongs to $H^1(K, E)_p^{\varepsilon_n}$, i.e.

$$c(n)^\tau = \varepsilon_n c(n) \text{ and } d(n)^\tau = \varepsilon_n d(n).$$

Proof. (1) We are going to compute $\tau P_n \in E(K_n)$, and then we'll pass to the quotient $E(K_n)/pE(K_n)$. Recall that, by definition, $P_n = \sum_{\sigma \in S} \sigma D_n y_n$, and that we have $\tau\sigma = \sigma^{-1}\tau$ for all $\sigma \in \mathrm{Gal}(K_n/K)$. We now claim that for any $l \mid n$ there exists an integer k_l such that

$$\tau D_l = -\sigma_l D_l \tau + k_l \mathrm{Tr}_l \in \mathbb{Z}[\mathrm{Gal}(K_n/\mathbb{Q})] \tag{2.11}$$

Remember that, by definition of D_l, it holds

$$(\sigma_l - 1)D_l = l + 1 - \mathrm{Tr}_l.$$

Multiplying both sides by τ both on the left and on the right we get

$$\tau(\sigma_l - 1)D_l = \tau(l + 1 - \mathrm{Tr}_l) = (l + 1 - \mathrm{Tr}_l)\tau = (\sigma_l - 1)D_l\tau,$$

i.e.

$$(\sigma_l - 1)D_l\tau = \tau(\sigma_l - 1)D_l. \tag{2.12}$$

We used the fact that $\tau\mathrm{Tr}_l = \mathrm{Tr}_l\tau$: since $\tau\sigma_l^i\tau = \sigma_l^{-i}$ for all i, we have

$$\tau\mathrm{Tr}_l = \tau\sum_{i=0}^{l}\sigma_l^i = \sum_{i=0}^{l}\tau\sigma_l^i =$$
$$= \sum_{i=0}^{l}\sigma_l^{-i}\tau = \left(\sum_{i=0}^{l}(\sigma_l^{-1})^i\right)\tau = \mathrm{Tr}_l\tau.$$

We now manipulate the right hand side of 2.12:

$$\tau(\sigma_l - 1)D_l = (\tau\sigma_l - \tau)D_l = (\sigma_l^{-1}\tau - \tau)D_l =$$
$$= (\sigma_l^{-1} - 1)\tau D_l = -\sigma_l^{-1}(-1 + \sigma_l)\tau D_l =$$
$$= -\sigma_l^{-1}(\sigma_l - 1)\tau D_l,$$

so that 2.12 becomes

$$(\sigma_l - 1)D_l\tau = -\sigma_l^{-1}(\sigma_l - 1)\tau D_l.$$

Multiplying by σ_l on the left we obtain

$$\begin{aligned}
&\sigma_l(\sigma_l - 1)D_l\tau = -(\sigma_l - 1)\tau D_l \iff \\
&(\sigma_l - 1)\sigma_l D_l\tau = -(\sigma_l - 1)\tau D_l \iff \\
&(\sigma_l - 1)(\sigma_l D_l\tau + \tau D_l) = 0,
\end{aligned}$$

i.e. $\sigma_l D_l\tau + \tau D_l$ is annihilated by $(\sigma_l - 1)$.

Lemma 2.4.3. In $\mathbb{Z}[G_l]$ we have that

$$\{\, \rho \in \mathbb{Z}[G_l] \mid (\sigma_l - 1)\rho = 0 \,\} = \mathbb{Z}\mathrm{Tr}_l.$$

Proof. ($\supseteq$) for any $k \in \mathbb{Z}$, we have

$$(\sigma_l - 1)k\mathrm{Tr}_l = (\sigma_l - 1)k\sum_{i=0}^{l}\sigma^i = k(\sigma_l - 1)\frac{\sigma^{l+1} - 1}{\sigma_l - 1} = k(\sigma^{l+1} - 1) = 0.$$

($\subseteq$) suppose $\rho = \sum_i a_i\sigma_l^i$ satisfies $(\sigma_l - 1)\rho = 0$, i.e.

$$\begin{aligned}
0 = \sum_{i=0}^{l} a_i\sigma_l^{i+1} - \sum_{i=0}^{l} a_i\sigma_l^i = a_l\sigma_l^{l+1} + \sum_{i=1}^{l}(a_{i-1} - a_i)\sigma_l^i - a_0 = \\
= a_l - a_0 + \sum_{i=1}^{l}(a_{i-1} - a_i)\sigma_l^i.
\end{aligned}$$

This implies $a_{i-1} = a_i$ for all i, $1 \le i \le l$, and $a_0 = a_l$; that is, $\rho = \sum_i a_0\sigma_l^i = a_0\mathrm{Tr}_l$. □

This lemma gives that

$$\sigma_l D_l\tau + \tau D_l = k_l\mathrm{Tr}_l$$

for a certain integer k_l; so, claim 2.11 is proved.

Now we compute $\tau P_n \bmod (pE(K_n))$, and we are going to use the fact that, for all $l \mid n$, $\mathrm{Tr}_l y_n \in pE(K_n)$ (see 2.2.10, (1)).

$$\begin{aligned}
&\tau P_n = \tau\sum_{\sigma\in S}\sigma D_n y_n = \sum_{\sigma\in S}\tau\sigma D_n y_n = \sum_{\sigma\in S}\sigma^{-1}\tau D_n y_n = \\
&= \sum_{\sigma\in S}\sigma^{-1}\tau\prod_{l\mid n} D_l y_n = \sum_{\sigma\in S}\sigma^{-1}(\tau D_{l_1})(D_{l_2}\cdot\ldots\cdot D_{l_{f_n}})y_n = \\
&= \sum_{\sigma\in S}\sigma^{-1}(-\sigma_{l_1}D_{l_1}\tau + k_{l_1}\mathrm{Tr}_{l_1})(D_{l_2}\cdot\ldots\cdot D_{l_{f_n}})y_n = \\
&= \sum_{\sigma\in S}\sigma^{-1}\big(-\sigma_{l_1}D_{l_1}\tau D_{l_2}\cdot\ldots\cdot D_{l_{f_n}}y_n + k_{l_1}\mathrm{Tr}_{l_1}D_{l_2}\cdot\ldots\cdot D_{l_{f_n}}y_n\big) = \\
&= \sum_{\sigma\in S}\sigma^{-1}\big(-\sigma_{l_1}D_{l_1}\tau D_{l_2}\cdot\ldots\cdot D_{l_{f_n}}y_n + k_{l_1}D_{l_2}\cdot\ldots\cdot D_{l_{f_n}}\mathrm{Tr}_{l_1}y_n\big) \equiv \mod (pE(K_n)) \\
&\equiv \sum_{\sigma\in S}\sigma^{-1}\big(-\sigma_{l_1}D_{l_1}(\tau D_{l_2})\cdot D_{l_3}\cdot\ldots\cdot D_{l_{f_n}}y_n\big) =
\end{aligned}$$

$$= \sum_{\sigma\in S} \sigma^{-1}\big(- \sigma_{l_1} D_{l_1}(-\sigma_{l_2} D_{l_2}\tau + k_{l_2}\mathrm{Tr}_{l_2}) \cdot D_{l_3} \cdot \ldots \cdot D_{l_{f_n}} y_n\big) =$$
$$= \cdots =$$
$$= \sum_{\sigma\in S} \sigma^{-1} \left(\prod_{l|n} -\sigma_l D_l\right) \tau y_n = \sum_{\sigma\in S} \sigma^{-1}(-1)^{f_n} \left(\prod_{l|n} \sigma_l \prod_{l|n} D_l\right) \tau y_n =$$
$$= (-1)^{f_n} \prod_{l|n} \sigma_l \sum_{\sigma\in S} \sigma^{-1} D_n \tau y_n.$$

Since $y_n^\tau = \varepsilon \cdot y_n^{\sigma'} + Q$ for $Q \in E(K_n)_{\mathrm{tors}}$ by Lemma 2.4.1, we have

$$\tau P_n \equiv (-1)^{f_n} \prod_{l|n} \sigma_l \sum_{\sigma\in S} \sigma^{-1} D_n(\varepsilon \cdot y_n^{\sigma'} + Q) \equiv$$
$$\equiv \varepsilon(-1)^{f_n} \prod_{l|n} \sigma_l \sum_{\sigma\in S} \sigma^{-1} D_n y_n^{\sigma'} \mod (pE(K_n)).$$

For this congruence, notice that $Q \in E(K_n)_{\mathrm{tors}} \subseteq pE(K_n)$: since $E_p(K_n) = 0$ by lemma 2.3.5, the multiplication by p in the finite abelian group $E(K_n)_{\mathrm{tors}}$ is an isomorphism, thus $E(K_n)_{\mathrm{tors}} = pE(K_n)_{\mathrm{tors}} \subseteq pE(K_n)$.

Concluding the computation we have:

$$\tau P_n \equiv \varepsilon_n \prod_{l|n} \sigma_l \sum_{\sigma\in S} \sigma^{-1} D_n \sigma' y_n =$$
$$= \varepsilon_n \prod_{l|n} \sigma_l \sigma' \sum_{\sigma\in S} \sigma^{-1} D_n y_n \equiv$$
$$\equiv \varepsilon_n \prod_{l|n} \sigma_l \sigma' P_n \equiv \varepsilon_n P_n.$$

The last equality holds because $[P_n]$ is fixed by $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$. We can conclude that

$$[P_n]^\tau = \varepsilon_n [P_n],$$

which was the first assertion of the proposition.

(2) Follows easily from the previous point, since the maps in diagram (2.8) commute with the action of $\langle\tau\rangle = \mathrm{Gal}(K/\mathbb{Q})$: $[P_n]^\tau = \varepsilon_n[P_n]$ implies $\delta_n[P_n]^\tau = \varepsilon_n\delta_n[P_n]$, and applying the map Res^{-1} we obtain $c(n)^\tau = \varepsilon_n c(n)$. Finally, applying the map α, we get $d(n)^\tau = \varepsilon_n d(n)$. □

Remark 2.4.4. For $n = 1$, we have $f_n = 0$, hence $\varepsilon_n = \varepsilon$, and we get

$$[P_1]^\tau = [y_K]^\tau = \varepsilon[y_K]. \tag{2.13}$$

For $n = l$ prime, we have $f_n = 1$, hence $\varepsilon_n = -\varepsilon$ and we get

$$[P_l]^\tau = -\varepsilon[P_l], \quad c(l)^\tau = -\varepsilon c(l), \quad d(l)^\tau = -\varepsilon d(l). \tag{2.14}$$

We have thus an improved version of Proposition 2.3.7:

Corollary 2.4.5. The class $d(n)$ is trivial in $H^1(K,E)_p^{\varepsilon_n}$ if and only if $P_n \in pE(K_n) + E(K)^{\varepsilon_n}$.

2.5 Local properties of the classes

In this paragraph we inspect further properties of the Kolyvagin classes, in particular the behaviour of the restrictions $d(n)_v$, for v any prime of K. Recall that $c(n) \in H^1(K, E_p)$ and $d(n) \in H^1(K, E)_p$; we wish to know if $c(n)$ actually lies in $\mathrm{Sel}^{(p)}(E/K)$, i.e. if $d(n)$ lies in $Ш(E/K)_p$.

Lemma 2.5.1. Let K be an imaginary quadratic number field, λ a prime ideal of $\mathcal{O}_K$ which splits completely in an extension K_m/K. For any prime ideal λ_m of $\mathcal{O}_{K_m}$ over λ, the completions K_λ and $(K_m)_{\lambda_m}$ are equal.

Proof. Follows easily from the fact that $\mathrm{Gal}((K_m)_{\lambda_m}/K_\lambda)$ is isomorphic to $D(\lambda_m/\lambda)$, the decomposition group of λ_m over λ (see [18], Chapter II, Proposition 9.6), through the restriction homomorphism

$$\mathrm{Gal}((K_m)_{\lambda_m}/K_\lambda) \to D(\lambda_m/\lambda), \quad \sigma \mapsto \sigma|_{K_m}; \tag{2.15}$$

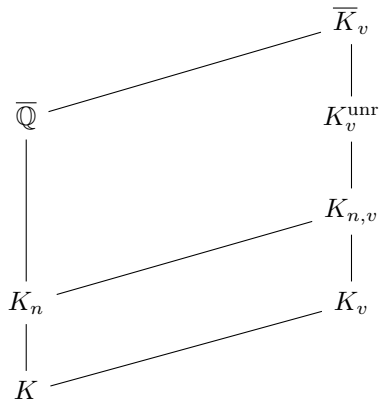
we notice here that injectivity follows from the fact that K_m is dense in the completion $(K_m)_{\lambda_m}$ and the automorphisms $\sigma \in D(\lambda_m/\lambda)$ are continuous with respect to the λ_m-adic topology. The decomposition group is cyclic of order $f = f(\lambda_m/\lambda)$, the inertial degree of λ_m over λ: since $f = 1$ by assumption, we conclude that $(K_m)_{\lambda_m} = K_\lambda$. □

We wil also write K_{λ_m} or $K_{m,\lambda}$ for $(K_m)_{\lambda_m}$. The following is the key result which characterizes the local behaviour of the classes $d(n)$.

Theorem 2.5.2.
1. The class $d(n)_v$ is locally trivial in $H^1(K_v, E)_p$ at the archimedean place $v = \infty$, and at all the finite places v of K which don't divide n.
2. Write $n = l \cdot m$ and $\lambda = (l)O_K$; the class $d(n)_\lambda$ is locally trivial in $H^1(K_\lambda, E)_p$ if and only if $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$ for one (and hence for all) place λ_m of K_m dividing λ.

Proof. (1) First case: $v = \infty$. In this case, $K_\infty = \mathbb{C}$, which is algebraically closed: the Galois cohomology of E is then trivial, because $H^1(K_v, E_p) = H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{C}), E_p) = 0$.

Second case: v finite, $v \nmid n, v \nmid N$. Since N is the conductor of E, in this case E has good reduction at v. Write $K_{n,v}$ for the completion of K_n at a prime over v. Since $v \nmid n$, Theorem 1.7.4 implies that the extension K_n/K is unramified at v: then, also the local extension $K_{n,v}/K_v$ is unramified. Let K_v^{unr} be the maximal unramified extension of K_v; we have therefore $K_{n,v} \leq K_v^{\mathrm{unr}}$.



(2.16)

We deduce the following commutative diagram of cohomology groups:

$$\begin{array}{ccc} H^1(K_n/K, E(K_n))_p & \xrightarrow{\mathrm{res}_v} & H^1(K_{n,v}/K_v, E(K_{n,v}))_p \\ \downarrow \mathrm{Inf} & & \downarrow \mathrm{inf} \\ H^1(\overline{\mathbb{Q}}/K, E)_p & \xrightarrow{\mathrm{res}_v} & H^1(\overline{K}_v/K_v, E)_p \\ \downarrow \mathrm{Res} & & \downarrow \mathrm{res} \equiv f \\ H^1(\overline{\mathbb{Q}}/K_n, E)_p^{\mathcal{G}_n} & \xrightarrow{\mathrm{res}_v} & H^1(\overline{K}_v/K_{n,v}, E)_p \end{array} \tag{2.17}$$

as well as the inflation-restriction exact sequence for $\mathrm{Gal}(\overline{K}_v/K_v^{\mathrm{unr}}) \leq \mathrm{Gal}(\overline{K}_v/K_v)$:

$$H^1(K_v^{\mathrm{unr}}/K_v, E(K_v^{\mathrm{unr}})) \xrightarrow{\mathrm{inf}} H^1(\overline{K}_v/K_v, E) \xrightarrow{\mathrm{res} \equiv h} H^1(\overline{K}_v/K_v^{\mathrm{unr}}, E). \tag{2.18}$$

Consider now the class $d(n)_v \in H^1(\overline{K}_v/K_v, E)_p$. Since $d(n) = \mathrm{Inf}\left(\widetilde{d}(n)\right)$, we have $d(n)_v = \mathrm{inf}\left(\widetilde{d}(n)_v\right)$. Therefore, $\mathrm{res}(d(n)_v) = 0 \in H^1(\overline{K}_v/K_{n,v}, E)$.

$$H^1(\overline{K}_v/K_v, E) \xrightarrow{f} H^1(\overline{K}_v/K_{n,v}, E) \xrightarrow{\mathrm{res} \equiv g} H^1(\overline{K}_v/K_v^{\mathrm{unr}}, E) \tag{2.19}$$

By (2.19), the image of $d(n)_v$ in $H^1(\overline{K}_v/K_v^{\mathrm{unr}}, E)$ is zero, too. By the exactness of (2.18) and by the equality $g \circ f = h$, we have $d(n)_v \in \ker(h) = \mathrm{im}(\mathrm{inf})$, and so $d(n)_v \in H^1(K_v^{\mathrm{unr}}/K_v, E)$. But this group is trivial when E has good reduction at v, i.e. if $v \nmid N$, by [15], Chapter I, Section 3: so we have $d(n)_v = 0$.

Third case: v finite, $v \nmid n, v \mid N$. In this case E has bad reduction at v. Still, we have the following exact sequence:

$$0 \longrightarrow E^1(K_\lambda) \hookrightarrow E^0(K_\lambda) \xrightarrow{\pi} \widetilde{E}_{\mathrm{ns}}(F_\lambda) \longrightarrow 0, \tag{2.20}$$

where $\widetilde{E}_{\mathrm{ns}}$ is the set of non-singular points in the reduced curve, $E^0 \leq E$ is the group of the points of good reduction, and E^1 is the kernel of reduction (see [21], Chapter VII, Proposition 2.1). Moreover, $\phi = E/E^0$ is a finite group (Kodaira-Néron Theorem, [21], Chapter VII, Theorem 6.1). As in (1), we have that

$$d(n)_v \in H^1(K_v^{\mathrm{unr}}/K_v, E(K_v^{\mathrm{unr}}))_p,$$

but in this case the group is not trivial. Take a prime w of K_n over v, and write $K_{n,w}$ for $(K_n)_w$. From the exact sequence

$$0 \longrightarrow E^0(K_v^{\mathrm{unr}}) \hookrightarrow E(K_v^{\mathrm{unr}}) \xrightarrow{\varpi} \phi \longrightarrow 0$$

we obtain

$$H^1(K_v^{\mathrm{unr}}/K_v, E^0(K_v^{\mathrm{unr}})) \longrightarrow H^1(K_v^{\mathrm{unr}}/K_v, E(K_v^{\mathrm{unr}})) \xrightarrow{\varpi^*} H^1(\overline{F}_v/F_v, \phi)). \tag{2.21}$$

By [15], Chapter I, Proposition 3.8, the first group of sequence (2.21) is trivial: therefore, ϖ^* is injective, and to show $d(n)_v = 0$ it will suffice to prove $\varpi^*(d(n)_v) = 0$. By [6], III, 3.1, the Heegner divisor $(x_n) - (\infty)$ in $J(X_0(N))(K_{n,w}) \equiv J(K_{n,w})$ satisfies

$$(x_n) - (\infty) \in (0) - (\infty) + J^0;$$

since $(0)-(\infty)$ is a point of rational torsion in the Jacobian, computing images through the modular parametrization we obtain

$$y_n \in E(\mathbb{Q})_{\mathrm{tors}} + E^0(K_v^{\mathrm{unr}})$$

on the curve E. Applying ϖ we see that $\varpi(y_n)$, and therefore also $\varpi(D_n y_n)$ and $\varpi(P_n)$, have order coprime with p in $\phi = E/E_0$, because $E(\mathbb{Q})_p = 0$ (see 2.1.3). But then we conclude that $\varpi^*(d(n)_v) = 0$, since it is annihilated by the two coprime integers $|\varpi(P_n)|$ and p. This concludes the proof of the third case, and so of the first assertion of the theorem.

(2) Recall that λ splits completely in K_m, and for any λ_m of K_m over λ we have $\lambda_m \mathcal{O}_{K_n} = \lambda_n^{l+1}$ (see Proposition 2.2.10). Moreover, $(K_m)_{\lambda_m} = K_\lambda$, $\mathrm{Gal}((K_n)_{\lambda_n}/(K_m)_{\lambda_m}) \cong \mathrm{Gal}(K_n/K_m) = G_l = \langle \sigma_l \rangle \cong C_{l+1}$, and the residue fields F_{λ_n}, F_{λ_m}, F_λ are all isomorphic to $\mathbb{F}_{l^2}$. We'll write $K_{n,\lambda}$ for $(K_n)_{\lambda_n}$.

As in the proof of (1), second case, we have $d(n)_\lambda = \inf\left(\widetilde{d}(n)_\lambda\right)$: abusing notation we'll identify them and write

$$d(n)_\lambda \in H^1(K_{n,\lambda}/K_\lambda, E(K_{n,\lambda}))_p = H^1(\mathrm{Gal}(K_{n,\lambda}/K_{m,\lambda}), E)_p \cong H^1(G_l, E(K_{n,\lambda}))_p.$$

By Lemma 2.3.6, $d(n)_\lambda$ is represented in $H^1(G_l, E(K_{\lambda_n}))$ by the cocycle $\sigma \mapsto -\frac{(\sigma-1)P_n}{p}$, where $\frac{(\sigma-1)P_n}{p}$ is the unique p-th root of $(\sigma-1)P_n$ in $E(K_n) \leq E(K_{n,\lambda})$.

Since $l \nmid N$, E has good reduction at λ: therefore, equation (2.20) in this case reads

$$0 \longrightarrow E^1(K_{n,\lambda}) \hookrightarrow E(K_{n,\lambda}) \overset{\pi}{\twoheadrightarrow} \widetilde{E}(F_{\lambda_n}) \longrightarrow 0.$$

Applying Lemma 1.4.5 to this exact sequence and taking the p-torsion subgroups we obtain

$$H^1(G_l, E^1(K_{n,\lambda}))_p \longrightarrow H^1(G_l, E(K_{n,\lambda}))_p \overset{\pi^*}{\longrightarrow} H^1(G_l, \widetilde{E}(F_{\lambda_n}))_p.$$

The group $E^1(K_{n,\lambda})$ is isomorphic to the formal group associated with $E(K_{n,\lambda})$ ([21], Chapter VII, Proposition 2.2), and every element of $E^1(K_{n,\lambda})_{\mathrm{tors}}$ has order which is a power of l ([21], Chapter IV, Proposition 3.2 (b)). This implies that $H^1(G_l, E^1(K_{\lambda_n}))_p = 0$. It follows that π^* is injective: $d(n)_\lambda = 0$ if and only if $\pi^*(d(n)_\lambda) = 0$.

The image of $d(n)_\lambda$ in $H^1(G_l, \widetilde{E}(F_{\lambda_n}))_p$ is

$$\pi^*\left(d(n)_\lambda\right) = \pi^*\left(\left[\sigma \mapsto -\frac{(\sigma-1)P_n}{p}\right]\right) = \left[\sigma \mapsto -\pi\left(\frac{(\sigma-1)P_n}{p}\right)\right].$$

Write $Q_n = \frac{(\sigma_l-1)P_n}{p} \in E(K_n) \leq E(K_{n,\lambda})$; $G_l = \langle \sigma_l \rangle$, so

$$\pi^*(d(n)_\lambda) = 0 \iff \pi(Q_n) = 0.$$

We also write $\widetilde{Q}_n$ for $\pi(Q_n)$.

Lemma 2.5.3. Write as always $\mathrm{Frob}\lambda_m = \left(\frac{K_m/\mathbb{Q}}{\lambda_m}\right) \in \mathrm{Gal}(K_m/\mathbb{Q})$. We have the congruence:

$$Q_n \equiv \frac{(l+1)(\mathrm{Frob}\lambda_m) - a_l}{p} P_m \pmod{\lambda_n} \tag{2.22}$$

in $E(K_n)$, where λ_n is the unique prime of K_n over λ_m.

Proof. We first of all notice that

$$Q_n = \sum_{\sigma \in S} \sigma D_m \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right). \tag{2.23}$$

Indeed, Q_n is by definition the only p-th root of $(\sigma_l - 1)P_n$ in $E(K_n)$ (see the proof of 2.3.6); the right-hand-side of the equation is also a point of $E(K_n)$ satisfying

$$\begin{aligned} & p \sum_{\sigma \in S} \sigma D_m \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) = p \sum_{\sigma \in S} \sigma D_m \left(\frac{l+1}{p} y_n - \frac{\mathrm{Tr}_l y_n}{p} \right) = \\ & = p \sum_{\sigma \in S} \sigma D_m \left(\frac{l+1-\mathrm{Tr}_l}{p} y_n \right) = p \sum_{\sigma \in S} \sigma D_m \left(\frac{(\sigma_l - 1) D_l}{p} y_n \right) = \\ & = \sum_{\sigma \in S} (\sigma_l - 1) \sigma D_m D_l y_n = (\sigma_l - 1) \sum_{\sigma \in S} \sigma D_n y_n = (\sigma_l - 1) P_n, \end{aligned}$$

and so (2.23) holds. We have used Proposition 2.2.10, the definition of D_l (see (2.4)) and the definition of P_n (see (2.7)).

For any λ_n dividing λ in K_n, by Proposition 2.2.10 (second part) we have the congruence

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \frac{(l+1)\mathrm{Frob}\lambda_m - a_l}{p} y_m \pmod{\lambda_n};$$

for any $\sigma \in \mathcal{G}_n = \mathrm{Gal}(K_n/K)$ we also have

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \frac{(l+1)\mathrm{Frob}(\sigma^{-1}\lambda_m) - a_l}{p} y_m \pmod{\sigma^{-1}\lambda_n}.$$

We may conjugate this last congruence to obtain

$$\sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \sigma \left(\frac{(l+1)\mathrm{Frob}(\sigma^{-1}\lambda_m) - a_l}{p} \right) y_m \pmod{\lambda_n}.$$

Remember that we have $\mathrm{Frob}(\sigma^{-1}\lambda_m) = \sigma^{-1}\mathrm{Frob}\lambda_m\sigma$, and so $\sigma\mathrm{Frob}(\sigma^{-1}\lambda_m) = \mathrm{Frob}\lambda_m\sigma$. So, the last congruence becomes

$$\sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \left(\frac{(l+1)\mathrm{Frob}\lambda_m - a_l}{p} \right) \sigma y_m \pmod{\lambda_n}.$$

Finally, using (2.23), we obtain

$$\begin{aligned} & Q_n = \sum_{\sigma \in S} \sigma D_m \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) = \sum_{\sigma \in S} D_m \sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \\ & \equiv \sum_{\sigma \in S} D_m \left(\frac{(l+1)\mathrm{Frob}\lambda_m - a_l}{p} \right) \sigma y_m \equiv \frac{(l+1)\mathrm{Frob}\lambda_m - a_l}{p} \sum_{\sigma \in S} \sigma D_m y_m \equiv \\ & \equiv \frac{(l+1)\mathrm{Frob}\lambda_m - a_l}{p} P_m \pmod{\lambda_n}. \end{aligned}$$

The lemma is thus proved. □

We are going to work in the reduced curve $\widetilde{E}(F_\lambda)$; notice that, since $F_{\lambda_m} = F_\lambda$, Frob$\lambda_m$ and Frob(l) both act on $F_\lambda \cong \mathbb{F}_{l^2}$ as $x \mapsto x^l$.

Lemma 2.5.4. The reduction $\widetilde{Q}_n$ is trivial if and only if $\widetilde{P}_m$ lies in $p\widetilde{E}(F_\lambda)$.

Proof. Write $\tau = \text{Frob}\lambda_m = \text{Frob}(l)$ and consider the group homomorphism $\psi = \frac{l+1}{p}\tau - \frac{a_l}{p}$:

$$\psi\colon \widetilde{E}(F_\lambda) \to \widetilde{E}(F_\lambda)_p,$$

$$P \mapsto \frac{l+1}{p}\text{Frob}\lambda_m(P) - \frac{a_l}{p}P = \frac{l+1}{p}P^l - \frac{a_l}{p}P.$$

This map really takes value in $\widetilde{E}(F_\lambda)$. Indeed, $p\psi(P) = (l+1)\tau(P) - a_l P = 0$, because $(l+1)\tau - a_l$ annihilates $\widetilde{E}(F_\lambda)$: in the proof of Lemma 2.2.6 we saw that $\tau^2 = 1$ and $\tau^2 - a_l\tau + l = 0$, and this implies that $(l+1) - a_l\tau = 0$, hence $0 = \tau((l+1) - a_l\tau) = (l+1)\tau - a_l\tau^2 = (l+1)\tau - a_l$. For the same reason, $\ker(\psi) \supseteq p\widetilde{E}(F_\lambda)$: therefore we obtain a map

$$\Psi\colon \widetilde{E}(F_\lambda)/p\widetilde{E}(F_\lambda) \to \widetilde{E}(F_\lambda)_p,$$

$$[P] \mapsto \frac{l+1}{p}P^l - \frac{a_l}{p}P,$$

which is a homomorphism of $\mathbb{F}_p$-vector spaces of dimension two. To prove the lemma, it is enough to show that Ψ is injective: in this case $\widetilde{Q}_n = \Psi([\widetilde{P}_m]) = 0 \iff [\widetilde{P}_m] = 0 \iff \widetilde{P}_m \in pE(F_\lambda)$. The map Ψ commutes with the action of $\tau = \text{Frob}(l)$, so we can restrict to the eigenspaces for τ

$$\Psi\colon \left(\widetilde{E}(F_\lambda)/p\widetilde{E}(F_\lambda)\right)^{\pm} \to \widetilde{E}(F_\lambda)_p^{\pm}$$

to get two linear maps of one-dimensional $\mathbb{F}_p$-vector spaces. On these subspaces, $P^l = \pm P$ by definition: so, Ψ acts as the multiplication by $\frac{l+1\pm a_l}{p}$. Since $p^2 \nmid l + 1 \pm a_l$ by the assumption we made in Remark 2.2.7, we conclude that $\frac{l+1\pm a_l}{p} \not\equiv 0 \bmod p$: this proves that Ψ is injective. □

We'll conclude the proof using this third and last lemma:

Lemma 2.5.5. Let P be a point in $E(K_{m,\lambda})$. Then, $\widetilde{P}$ lies in $p\widetilde{E}(F_\lambda)$ if and only if P lies in $pE(K_{m,\lambda}) = pE(K_\lambda)$.

Proof. The "if" part is trivial, because $P = pQ$ implies $\widetilde{P} = p\widetilde{Q}$. Suppose now $\widetilde{P} = p\widetilde{Q}$ for $Q \in E(K_{m,\lambda})$. We need to show $P \in pE(K_{m,\lambda})$. It is known that $E^1(K_{m,\lambda})$ is p-divisible, i.e. the multiplication by p is an isomorphism on E^1, because $(p, l) = 1$ (see again [21], Chapter IV, Proposition 2.3 (b)):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E^1(K_{m,\lambda}) & \hookrightarrow & E(K_{m,\lambda}) & \overset{\pi}{\twoheadrightarrow} & \widetilde{E}(F_\lambda) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot p} & & \downarrow{\scriptstyle \cdot p} & & \downarrow{\scriptstyle \cdot p} & & \\
0 & \longrightarrow & E^1(K_{m,\lambda}) & \hookrightarrow & E(K_{m,\lambda}) & \overset{\pi}{\twoheadrightarrow} & \widetilde{E}(F_\lambda) & \longrightarrow & 0.
\end{array}$$

Since $\pi(pQ - P) = p\widetilde{Q} - \widetilde{P} = 0$, $pQ - P$ is an element of E^1: therefore, there exists $R \in E^1(K_{m,\lambda})$ such that $pR = pQ - P$. Hence $P = pQ - pR = p(Q - R) \in pE(K_{m,\lambda})$. □

In conclusion, using the results given by the lemmas, we have

$$d(n)_\lambda = 0 \iff \pi^*(d(n)_\lambda) = 0 \iff \widetilde{Q}_n = 0 \iff \widetilde{P}_m \in p\widetilde{E}(F_\lambda) \iff P_m \in pE(K_\lambda),$$

which is what we needed to prove. This concludes the proof of the theorem. □

Remark 2.5.6. For $n = l$ prime, this important result gives that $d(l)_v \neq 0$ for all $v \neq \lambda$, and $d(l)_\lambda = 0$ if and only if $P_1 = y_K$ lies in $pE(K_\lambda)$.

Chapter 3

Bounding the Selmer group

3.1 The local and global pairings

In this section we are going to use some results of local Tate duality and class field theory, which we briefly recall. Our main references are [16] and [15].

In Section 1.4 we defined the first two cohomology groups for a G-module M; the description was very concrete, in terms of fixed elements and cocycles. Is it actually possible to define the cohomology groups $H^n(G, M)$ for all n via the right derived functor of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$:

$$H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

(for the details see e.g. [19],Chapter 9, Section 2); actually, we will need only $H^2(G, M)$, which is strictly related to Brauer groups.

Definition 3.1.1. Let k be a field. The *Brauer group* of k is the set

$$\mathrm{Br}(k) = \{\, [A] \mid A \text{ is a central simple } k\text{-algebra} \,\}$$

with binary operation $[A][B] = [A \otimes_k B]$.

Without going into details, this group classifies equivalence classes of central simple k-algebras over k. The particular case that will be relevant for us is that of local fields.

Proposition 3.1.2. Let K_v be a local field. Then we have

$$\mathrm{Br}(K_v) \cong \mathbb{Q}/\mathbb{Z}.$$

The isomorphism is given by the so called *invariant map of local class field theory.*

Proof. See for example [16], Chapter III, Theorem 2.1. □

Finally, the result that links Brauer groups and cohomology is the following.

Theorem 3.1.3. For a field k we have

$$\mathrm{Br}(k) \cong H^2\left(\mathrm{Gal}(\overline{k}/k), \overline{k}^{\times}\right). \tag{3.1}$$

Proof. See [16], Chapter IV, Corollary 3.16. □

Proposition 3.1.4. For any bilinear G-equivariant pairing of G-modules

$$M \times N \to P$$

there is a family of *cup-product pairings*

$$H^r(G, M) \times H^s(G, N) \to H^{r+s}(G, P), \quad (x, y) \mapsto x \cup y$$

which are bilinear and commute with the inflation and restriction maps.

Proof. See [1], Chapter IV, Section 7, Theorem 4. □

We apply this result to $M = N = E_p = E_p(\overline{K}_\lambda)$, $G = \mathrm{Gal}(\overline{K}_\lambda/K)$ and $P = \mu_p = \mu_p(\overline{K}_\lambda)$, i.e. to the *Weil pairing*

$$E_p \times E_p \to \mu_p$$

(see [21], Chapter III, Section 8 for the precise definition): in this way we get the pairing

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \to H^2(K_\lambda, \mu_p).$$

Finally, by (3.1) and 3.1.2 we have that $H^2(K_\lambda, \mu_p) \cong \mathrm{Br}(K_\lambda)_p \cong \frac{1}{p}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$; therefore the pairing becomes

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \to \mathbb{F}_p. \tag{3.2}$$

By [15], Chapter I, Corollary 2.3, this pairing is alternating and non-degenerate.

The last result we invoke is one of the most important of class field theory.

Theorem 3.1.5. For any number field K, the sequence

$$0 \longrightarrow \mathrm{Br}(K) \xrightarrow{\prod_v \mathrm{res}_v} \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{3.3}$$

is exact. This sequence is called *Fundamental exact sequence of global class field theory.*

Proof. See [16], Chapter VII, Section 4, Theorem 4.2. □

Remark 3.1.6. Notice that $\bigoplus_v \mathrm{Br}(K_v) \cong \bigoplus_v \mathbb{Q}/\mathbb{Z}$ by 3.1.2.

We now apply these results to our case of interest.

Proposition 3.1.7. The pairing defined in (3.2) induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces:

$$\langle\,,\rangle\colon E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \to \mathbb{Z}/p\mathbb{Z}. \tag{3.4}$$

Proof. Recall that the pairing defined in (3.2) was

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \to \mathbb{F}_p.$$

The key point is that the subspace $E(K_\lambda)/pE(K_\lambda) \leq H^1(K, E_p)$ is isotropic for pairing (3.2); therefore, (3.4) is defined as

$$([P], d) \mapsto \langle [P], d\rangle := \langle [P], c\rangle, \tag{3.5}$$

for $c \in \alpha^{-1}(d) \subset H^1(K, E_p)$. For the detailed proof we refer the reader to [4], Proposition 7.5. □

Proposition 3.1.8. (1) The eigenspaces $(E(K_\lambda)/pE(K_\lambda))^\pm$ and $H^1(K_\lambda, E)_p^\pm$ for the action of $\mathrm{Gal}(K/\mathbb{Q})$ are $\mathbb{Z}/p\mathbb{Z}$-vector spaces of dimension one.

(2) The pairing (3.4) induces two non-degenerate pairings of $\mathbb{Z}/p\mathbb{Z}$-vector spaces:

$$\langle\,,\rangle\colon (E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(K_\lambda, E)_p^\pm \to \mathbb{Z}/p\mathbb{Z}.$$

Proof. (1) See [4], Proposition 8.1.

(2) To show non-degeneracy, it is enough to prove that the eigenspaces relative to different eigenvalues are othogonal: in this case, for a fixed $x \in (E(K_\lambda)/pE(K_\lambda))^\pm$, $\langle x, y\rangle = 0\,\forall y \in H^1(K_\lambda, E)_p^\mp$ implies $\langle x, y\rangle = 0\,\forall y \in H^1(K_\lambda, E)_p$ and so $x = 0$. Since the pairing is equivariant for the action of τ, we have

$$\langle \tau c_1, \tau c_2\rangle = \tau\langle c_1, c_2\rangle = \langle c_1, c_2\rangle \quad \forall (c_1, c_2) \in E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p;$$

the last equality holds because the action of τ on $\mathbb{F}_p$ is trivial. Then, for $c_1 \in (E(K_\lambda)/pE(K_\lambda))^\pm$ and $c_2 \in H^1(K_\lambda, E)_p^\mp$ we have

$$\langle c_1, c_2\rangle = \langle \tau c_1, \tau c_2\rangle = \langle \pm c_1, \mp c_2\rangle = -\langle c_1, c_2\rangle$$

in $\mathbb{F}_p$; since $p \neq 2$, this implies $\langle c_1, c_2\rangle = 0$. □

The main result of this section is the following.

Proposition 3.1.9. Assume that a class $d \in H^1(K, E)_p^\pm$ is locally trivial for all places $v \neq \lambda$ of K, but is not trivial at λ: $d_v = \mathrm{res}_v(d) = 0$ for all $v \neq \lambda$, but $d_\lambda = \mathrm{res}_\lambda(d) \neq 0$. Then, for any $s \in \mathrm{Sel}^{(p)}(E/K)^\pm \subseteq H^1(K, E_p)^\pm$, we have $s_\lambda = 0$ in $H^1(K_\lambda, E_p)^\pm$.

Proof. By definition of the Selmer group, s_λ is an element of $(E(K_\lambda)/pE(K_\lambda))^\pm$: we may thus apply Proposition 3.1.8 and so, to show $s_\lambda = 0$, it suffices to show that $\langle s_\lambda, d_\lambda\rangle = 0$.

To do this, choose a class $c \in H^1(K, E_p)$ which is mapped to d through α. Applying Proposition 3.1.4 to the Weil pairing

$$E_p \times E_p \to \mu_p$$

first with $G = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and then with $G = \mathrm{Gal}(\overline{K}_v/K_v)$ we obtain the following commutative diagram:

$$\begin{array}{ccc} H^1(K, E_p) \times H^1(K, E_p) & \xrightarrow{\langle\text{-};\text{-}\rangle_K} & \mathrm{Br}(K)_p \\ \downarrow{\scriptstyle (\mathrm{res}_v;\mathrm{res}_v)} & & \downarrow{\scriptstyle \mathrm{res}_v} \\ H^1(K_v, E_p) \times H^1(K_v, E_p) & \xrightarrow{\langle\text{-};\text{-}\rangle_v} & \mathrm{Br}(K_v)_p \end{array}$$

(we denote the global pairing as $\langle\,,\rangle_K$ and the local pairing as $\langle\,,\rangle_v$). The commutativity of the diagram implies $(\langle s, c\rangle_K)_v = \langle s_v, c_v\rangle_v$ for each prime v. Combining this with the Fundamental exact sequence of global class field theory (3.3) we have

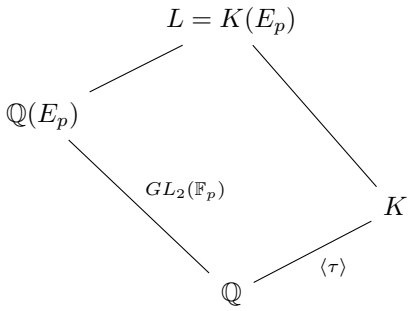
$$\sum_v \langle s_v, c_v\rangle_v = \sum_v (\langle s, c\rangle_K)_v = 0.$$

By assumption, $\langle s_v, c_v\rangle_v = \langle s_v, d_v\rangle_v = \langle s_v, 0\rangle_v = 0$ for all $v \neq \lambda$ (we used equation (3.5)). Therefore, also $\langle s_\lambda, c_\lambda\rangle_\lambda = \langle s_\lambda, d_\lambda\rangle_\lambda$ is zero. □

Remark 3.1.10. We stress that this Proposition guarantees the local triviality of all s which belong to the eigenspace $\mathrm{Sel}^{(p)}(E/K)^\pm$ *of the same sign* as the eigenspace $H^1(K, E)_p^\pm$ which contains the class d.

3.2 Towards the computation of the Selmer group

In this section we prove some auxiliary results in view of our main goal, which is to give a concrete description of the Selmer group $\mathrm{Sel}^{(p)}(E/K) \leq H^1(K, E_p)$; remember that we are working under the assumptions that $p \neq 2$ and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$.



Since $\mathbb{Q}(E_p) \cap K = \mathbb{Q}$ by 2.2.4, we have $\mathrm{Gal}(L/K) \cong GL_2(\mathbb{F}_p)$. Write $\mathcal{G} = \mathrm{Gal}(L/K)$.

Remark 3.2.1. E_p is a simple $\mathcal{G}$-module: if $W \leq E_p$ satisfies $W^\sigma = W$ for all $\sigma \in \mathcal{G}$, then $W = 0$ or $W = E_p$. This is the irreducibility of the representation $\mathcal{G} \cong GL_2(\mathbb{F}_p) \to \mathrm{Aut}(E_p)$.

Proposition 3.2.2. We have $H^n(\mathcal{G}, E_p) = 0$ for all $n \geq 0$. The restriction of classes gives an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules:

$$\mathrm{Res}\colon H^1(K, E_p) \to H^1(L, E_p)^{\mathcal{G}} = \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), E_p(L)).$$

Proof. See [4], Proposition 9.1. □

From Proposition 3.2.2 we obtain a pairing:

$$\begin{aligned} [\,,\,]\colon H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) &\to E_p(L), \\ (s, \rho) &\mapsto [s, \rho] = \mathrm{Res}(s)(\rho), \end{aligned} \tag{3.6}$$

which satisfies $[s^\sigma, \rho^\sigma] = [s, \rho^\sigma] = [s, \rho]^\sigma$ for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ and $\sigma \in \mathcal{G} = \mathrm{Gal}(L/K)$. If $[s, \rho] = 0$ for all $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, then $s = 0$ by the injectivity of the restriction map Res.

Let $S \leq H^1(K, E_p)$ be a finite subgroup, and define

$$\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{ \rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) \;\middle|\; [s, \rho] = 0 \;\forall s \in S \right\}; \tag{3.7}$$

finally, let L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$, so that $\mathrm{Gal}(\overline{\mathbb{Q}}/L_S) = \mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$.

Remark 3.2.3. Notice that L_S is a finite Galois extension of L, because $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ is an open normal subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$: if we write

$$s = [s, -]\colon \mathrm{Gal}(\overline{\mathbb{Q}}/L) \to E_p, \quad \rho \mapsto [s, \rho]$$

we have

$$\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \bigcap_{s \in S} s^{-1}(0),$$

which is a finite intersection of open normal subgroups of finite index.

Remark 3.2.4. If $S' \leq S \leq H^1(K, E_p)$, then $\mathrm{Gal}_{S'}(\overline{\mathbb{Q}}/L) \geq \mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$, i.e. $\mathrm{Gal}(\overline{\mathbb{Q}}/L_{S'}) \geq \mathrm{Gal}(\overline{\mathbb{Q}}/L_S)$. So, $L_{S'} \leq L_S$.

Proposition 3.2.5. Pairing (3.6) induces a *non-degenerate* pairing

$$[\,,\,]\colon S \times \mathrm{Gal}(L_S/L) \to E_p(L),$$

which in turn induces an isomorphism of $\mathcal{G}$-modules,

$$\mathrm{Gal}(L_S/L) \to \mathrm{Hom}(S, E_p(L)), \tag{3.8}$$

$$\rho \mapsto (s \mapsto [s, \rho])$$

and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules

$$S \to \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L)), \tag{3.9}$$

$$s \mapsto (\rho \mapsto [s, \rho]).$$

Proof. The definition of the pairing is the following: for $(s, \rho) \in S \times \mathrm{Gal}(L_S/L)$, choose a lift $\widetilde{\rho} \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ of ρ, and define $[s, \rho] = [s, \widetilde{\rho}] = \mathrm{Res}(s)(\widetilde{\rho})$ (see (3.6)). The definition is well-posed: if $\widetilde{\rho} \in \mathrm{Gal}(\overline{\mathbb{Q}}/L_S)$, $[s, \rho] = [s, \widetilde{\rho}] = 0$ by the very definition of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \mathrm{Gal}(\overline{\mathbb{Q}}/L_S)$. The map (3.9) is an injection because the restriction map Res is injective (see the comments below (3.6)); the map (3.8) is also an injection because $[s, \rho] = 0\, \forall s \in S$ implies (by definition of the group $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$) $\widetilde{\rho} \in \mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \mathrm{Gal}(\overline{\mathbb{Q}}/L_S)$, i.e. $\rho = 0 \in \mathrm{Gal}(L_S/L)$.

Recall that $S = \mathrm{Sel}^{(p)}(E/K)$ is a finite-dimensional $\mathbb{F}_p$-vector space: write $r = \dim_{\mathbb{F}_p} S$. Then, $\mathrm{Hom}(S, E_p) \cong \mathrm{Hom}((\mathbb{F}_p)^r, E_p) \cong E_p^r$; by what we have just seen, $\mathrm{Gal}(L_S/L)$ injects into $\mathrm{Hom}(S, E_p) \cong E_p^r$. E_p is a simple $\mathcal{G}$-module (see 3.2.1), so E_p^r is semi-simple (direct sum of simple modules). Any submodule of a semi-simple module is semi-simple, so

$$\mathrm{Gal}(L_S/L) \cong E_p^s \quad \exists s \leq r. \tag{3.10}$$

Then we have

$$\mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p) \cong \mathrm{Hom}_{\mathcal{G}}(E_p^s, E_p) \cong \mathbb{F}_p^s \tag{3.11}$$

(where the last isomorphism follows from the fact that $\mathrm{Hom}_{\mathcal{G}}(E_p, E_p)$ is isomorphic to $\mathbb{F}_p$). From the above-proven fact that $S \cong \mathbb{F}_p^r$ injects into this group, we find $r \leq s$. Therefore, $s = r$ and both the injections (3.8) and (3.9) are isomorphisms.

□

We are going to apply Proposition 3.2.5 to the finite subgroups $S = \mathrm{Sel}^{(p)}(E/K)$ and $S' = \langle \delta y_K \rangle$. Recall that, in the hypotheses of 2.1.4, we are assuming that y_K is not divisible by p in $E(K)$, so that $\delta y_K \neq 0$.

$S' \leq S$ implies $L_{S'} \leq L_S$, so $L_{\langle \delta y_K \rangle} \leq L_S$.

Lemma 3.2.6. $L_{\langle \delta y_K \rangle} = L(\frac{1}{p} y_K)$. Moreover, $\mathrm{Gal}(L(\frac{1}{p} y_K)/L) \cong E_p(L) = E_p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. Write $Q = \frac{1}{p} y_K$. We are going to show that $\mathrm{Gal}(\overline{\mathbb{Q}}/L(Q)) = \mathrm{Gal}(\overline{\mathbb{Q}}/L_{\langle \delta y_K \rangle})$. By (3.7), an element ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ lies in $\mathrm{Gal}(\overline{\mathbb{Q}}/L_{\langle \delta y_K \rangle}) = \mathrm{Gal}_{\langle \delta y_K \rangle}(\overline{\mathbb{Q}}/L)$ if and only if $[\delta y_K, \rho] = 0$. We know that δy_K is the class of the cocycle $\sigma \mapsto Q^\sigma - Q$, so $[\delta y_K, \rho] = 0$ if and only if $Q^\rho = Q$, if and only if ρ fixes $L(Q)$ pointwise. For the second assertion, notice that

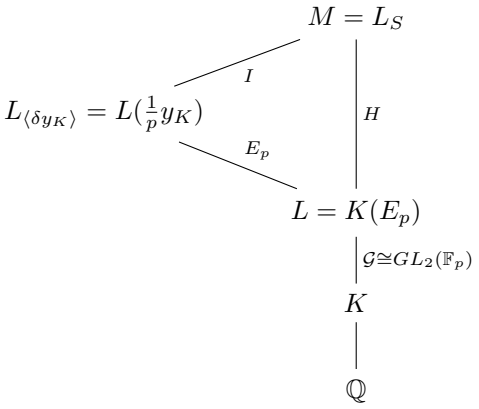
$$\mathrm{Gal}(L_{\langle \delta y_K \rangle}/L) \cong \mathrm{Hom}(\langle \delta y_K \rangle, E_p) \tag{3.12}$$

by 3.2.5; the latter group is isomorphic to $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, E_p) \cong E_p$. Notice that (3.12) is explicitly given by

$$\mathrm{Gal}(L(Q)/L) \to E_p, \quad \sigma \mapsto Q^\sigma - Q. \tag{3.13}$$

□

Write now $M = L_S$, $H = \mathrm{Gal}(M/L)$, $I = \mathrm{Gal}(M/L(\frac{1}{p}y_K))$. We have the following field diagram.



(3.14)

Remark 3.2.7. Notice that H is an abelian group, since it is isomorphic to $\mathrm{Hom}(\mathrm{Sel}^{(p)}(E/K), E_p)$ by 3.2.5. In fact, we know a lot more: $\mathrm{Sel}^{(p)}(E/K)$ is a finite-dimensional $\mathbb{F}_p$-vector space by what we said in 1.6.4, and $E_p \cong \mathbb{F}_p^2$: then, H is itself a finite-dimensional $\mathbb{F}_p$-vector space. In particular, the order of the abelian group H is a power of p.

Let τ be a fixed complex conjugation of $\mathrm{Gal}(M/\mathbb{Q})$; τ acts on the normal subgroups I and H: as always, write H^+ and I^+ for the $+1$-eigenspaces for τ.

Proposition 3.2.8. (1) We have the equalities

$$H^+ = \left\{ (\tau h)^2 \;\middle|\; h \in H \right\}, \quad I^+ = \left\{ (\tau i)^2 \;\middle|\; i \in I \right\}.$$

Moreover, $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$.

(2) Recall that, for $S = \mathrm{Sel}^{(p)}(E/K)$, the pairing defined in Proposition 3.2.5 is

$$[\,,\,] \colon \mathrm{Sel}^{(p)}(E/K) \times H \to E_p(L). \tag{3.15}$$

Let $s \in \mathrm{Sel}^{(p)}(E/K)^{\pm}$. The following are equivalent:
(a) $[s, \rho] = 0$ for all $\rho \in H$;
(b) $[s, \rho] = 0$ for all $\rho \in H^+$;
(c) $[s, \rho] = 0$ for all $\rho \in H^+ \smallsetminus I^+$;
(d) $s = 0$.

Proof. (1) We claim that $p \neq 2$ implies $H^+ = H^{\tau+1}$, where the latter group is by definition $\{ h^\tau \cdot h \mid h \in H \}$. First of all, the inclusion "$\supseteq$" is straightforward: $(h^\tau h)^\tau = h^{\tau^2} h^\tau = h h^\tau = h^\tau h$ (remember that $\tau^2 = 1$ and H is abelian). To prove the equality, write any $h \in H$ as $h = \sqrt{h \cdot h^\tau} \cdot \sqrt{h \cdot (h^\tau)^{-1}}$. This is possible: the map $h \mapsto h^2$ is an isomorphism, being H an abelian group of odd order (3.2.7). Writing $u = \sqrt{h h^\tau} \in H^+$ and $v = \sqrt{h (h^\tau)^{-1}} \in H^-$, we

see that $h = uv$ satisfies $h^\tau = h$ if and only if $u^\tau v^\tau = uv$, if and only if $v^\tau = v$. This means $v \in H^+ \cap H^- = 1$ ($v^2 = 1$ implies $v = 1$). Now we are done, because

$$H^+ = H^{\tau+1} = \{\, h^\tau h \mid h \in H \,\} = \{\, \tau h \tau h \mid h \in H \,\} = \left\{\, (\tau h)^2 \;\middle|\; h \in H \,\right\}.$$

The same argument works for I, so the first assertion of (1) is proved. For the second one:

$$H^+/I^+ = (H/I)^+ \cong E_p^+ \cong \mathbb{Z}/p\mathbb{Z},$$

and this concludes the first part of the proposition.

(2) we have (d) $\Rightarrow$ (a) $\Rightarrow$ (b) $\Rightarrow$ (c), and (d) $\Leftarrow$ (a) by the non-degeneracy of the pairing (3.15); for the remaining implications:

(c) $\Rightarrow$ (b). The map $s\colon H^+ \to E_p$, $h \mapsto [s,h]$ is a group homomorphism; I^+ has index p in H^+, so $s(H^+ \smallsetminus I^+) = 0$ immediately implies $\ker(s) = H^+$.

(b) $\Rightarrow$ (a). Since the pairing is equivariant for the action of $\langle\tau\rangle$ and $s \in \mathrm{Sel}^{(p)}(E/K)^{\pm}$, s induces a $\mathcal{G}$- homomorphism $H \to E_p$ such that $s(H^+) \subseteq E_p^{\pm}$ and $s(H^-) \subseteq E_p^{\mp}$. If $s(H^+) = 0$, then $s(H) \subseteq s(H^-) \subseteq E_p^{\mp}$; but $s(H)$ is a $\mathcal{G}$-submodule of the simple $\mathcal{G}$-module E_p. So from $s(H) \neq E_p$ we necessarily have $s(H) = 0$. □

Let now $\lambda \triangleleft \mathcal{O}_K$ be a prime ideal that is unramified in M; we assume further that λ splits completely in L. Let λ_M be a prime factor of λ in M.

Lemma 3.2.9. The Frobenius substitution of λ_M in $\mathrm{Gal}(M/K)$ actually lies in the subgroup $H = \mathrm{Gal}(M/L)$:

$$\left(\frac{M/K}{\lambda_M}\right) \in H = \mathrm{Gal}(M/L).$$

Proof. Write $\pi\colon \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ for the canonical projection (restriction map), and $\lambda_L = \lambda_M \cap \mathcal{O}_L$. Since λ splits completely in L, we have

$$1 = \left(\frac{L/K}{\lambda_L}\right) = \pi\left(\frac{M/K}{\lambda_M}\right),$$

i.e. $\left(\frac{M/K}{\lambda_M}\right) \in \ker(\pi) = H$. □

Remark 3.2.10. Recall that H is an abelian normal subgroup of $\mathrm{Gal}(M/K)$, so the factor group $\mathrm{Gal}(M/K)/H = \mathcal{G}$ acts naturally on H: for $g \in \mathcal{G}$ and $h \in H$, lift g to an element $\widetilde{g}$ of $\mathrm{Gal}(M/K)$ and set $h^g = h^{\widetilde{g}}$.

We as usual denote by $\mathrm{Frob}(\lambda)$ the orbit of $\left(\frac{M/K}{\lambda_M}\right)$ under the conjugation action of $\mathrm{Gal}(M/K)$ (recall that this orbit only depends on λ, and not on λ_M); we have of course $\mathrm{Frob}(\lambda) \subset H$ since H is normal, and this set $\mathrm{Frob}(\lambda)$ is equal to the orbit of $\left(\frac{M/K}{\lambda_M}\right)$ under the above defined action of $\mathcal{G}$ on H.

Write now $[s, \mathrm{Frob}(\lambda)] = 0$ if $[s,\rho] = 0$ for all $\rho \in \mathrm{Frob}(\lambda)$.

Proposition 3.2.11. Let $s \in \mathrm{Sel}^{(p)}(E/K) \subset H^1(K, E_p)$. The following are equivalent:

(a) $[s,\rho] = 0$ for $\rho = \left(\frac{M/K}{\lambda_M}\right) \in H$;

(b) $[s, \mathrm{Frob}(\lambda)] = 0$;

(c) $s_\lambda = 0 \in H^1(K_\lambda, E_p)$.

Proof. (a) $\Leftrightarrow$ (b) follows immediately from the equivariance of the pairing (see (3.6)), i.e. $[s, \rho^\sigma] = [s, \rho]^\sigma$, for any $\sigma \in \mathcal{G}$.

(a) $\Leftrightarrow$ (c). Take $s \in S = \mathrm{Sel}^{(p)}(E/K) \subset H^1(K, E_p)$ and consider the following diagram.

$$\begin{array}{ccccc}
E(K)/pE(K) & \xhookrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\alpha} & H^1(K, E)_p \\
\downarrow & & \downarrow{\scriptstyle \mathrm{res}_\lambda} & & \downarrow{\scriptstyle \mathrm{res}_\lambda} \\
E(K_\lambda)/pE(K_\lambda) & \xhookrightarrow{\delta_\lambda} & H^1(K_\lambda, E_p) & \xrightarrow{\alpha_\lambda} & H^1(K_\lambda, E)_p \\
\downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow \\
E(M_{\lambda_M})/pE(M_{\lambda_M}) & \xhookrightarrow{\delta_{\lambda_M}} & H^1(M_{\lambda_M}, E_p) & \xrightarrow{\alpha_{\lambda_M}} & H^1(M_{\lambda_M}, E)_p.
\end{array}$$

By definition of the Selmer group, $0 = \mathrm{res}_\lambda(\alpha(s)) = \alpha_\lambda(\mathrm{res}_\lambda(s))$, so $s_\lambda = \mathrm{res}_\lambda(s) \in \ker(\alpha_\lambda) = \mathrm{im}(\delta_\lambda)$: write $s_\lambda = \delta_\lambda[P_\lambda]$ for a point $P_\lambda \in E(K_\lambda)$. Remember that this means, by the definition of the Kummer map δ_λ, that s_λ is represented by the cocycle

$$\mathrm{Gal}(\overline{K}_\lambda/K_\lambda) \to E_p, \quad \sigma \mapsto Q_\lambda^\sigma - Q_\lambda,$$

where $Q_\lambda = \frac{1}{p}P_\lambda \in E(\overline{K}_\lambda)$ is a fixed p-th root of P_λ. Therefore,

$$s_\lambda = 0 \iff Q_\lambda^\sigma = Q_\lambda \ \forall \sigma \in \mathrm{Gal}(\overline{K}_\lambda/K_\lambda) \iff Q_\lambda \in E(K_\lambda). \tag{3.16}$$

We claim that Q_λ is rational over M_{λ_M}. This is equivalent to the condition

$$\mathrm{Res}(s_\lambda) = 0 \in H^1(\overline{K}_\lambda/M_{\lambda_M}, E_p), \tag{3.17}$$

because $\mathrm{Res}(s_\lambda) = \delta_{\lambda_M}(P_\lambda + pE(M_{\lambda_M}))$ is trivial if and only if P_λ lies in $pE(M_{\lambda_M})$, if and only if $Q_\lambda = \frac{1}{p}P_\lambda$ is in $E(M_{\lambda_M})$.

Consider the restriction maps

$$H^1(\overline{\mathbb{Q}}/K, E_p) \longrightarrow H^1(\overline{\mathbb{Q}}/M, E_p) \longrightarrow H^1(\overline{K}_\lambda/M_{\lambda_M}, E_p); \tag{3.18}$$

since $M_{\lambda_M} \geq M \geq L = K(E_p)$, M and M_{λ_M} contain all the p torsion E_p. So E_p is a trivial $\mathrm{Gal}(\overline{K}_\lambda/M_{\lambda_M})$-module and a trivial $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$-module; hence, by 1.4.4, we may actually rewrite (3.18) as

$$H^1(\overline{\mathbb{Q}}/K, E_p) \longrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/M), E_p) \longrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{K}_\lambda/M_{\lambda_M}), E_p); \tag{3.19}$$

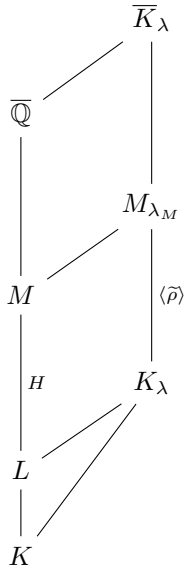
This means that the image of s in $H^1(M, E_p)$ is the homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/M) \to E_p$, $\sigma \mapsto [s, \sigma]$.

Remember that $M = L_S$ and $S = \mathrm{Sel}^{(p)}(E/K)$, so by definition (3.7) we have

$$[s, \sigma] = 0 \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/M). \tag{3.20}$$

In other words, s is trivial in $H^1(M, E_p)$. But then we see that it is trivial also in $H^1(M_{\lambda_M}, E_p)$, which is claim (3.17).

Consider now the following field diagram (recall that $L_{\lambda_L} = K_\lambda$ because λ splits completely in L).



Remember that we defined $\rho = \left(\frac{M/K}{\lambda_M}\right) \in H \leq \mathrm{Gal}(M/K)$; by what we saw in the proof of Lemma 2.5.1, ρ extends uniquely to a K_λ-automorphism $\widetilde{\rho}$ of M_{λ_M}, and actually $\mathrm{Gal}(M_{\lambda_M}/K_\lambda) = \langle\widetilde{\rho}\rangle$. So,

$$Q_\lambda \in E(K_\lambda) \iff Q_\lambda^{\widetilde{\rho}} = Q_\lambda \iff Q_\lambda^{\widetilde{\rho}} - Q_\lambda = 0. \tag{3.21}$$

Now, lift ρ to $\overline{\rho} \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\widetilde{\rho}$ to $\overline{\widetilde{\rho}} \in \mathrm{Gal}(\overline{K}_\lambda/K_\lambda)$, asking $\overline{\widetilde{\rho}}|_{\overline{\mathbb{Q}}} = \overline{\rho}$. Evaluating s at these automorphisms we get

$$Q_\lambda^{\widetilde{\rho}} - Q_\lambda = Q_\lambda^{\overline{\widetilde{\rho}}} - Q_\lambda = [s, \overline{\widetilde{\rho}}] = [s, \overline{\rho}] = [s, \rho]. \tag{3.22}$$

Putting together equations (3.16), (3.21) and (3.22) we obtain

$$s_\lambda = 0 \iff [s, \rho] = 0,$$

which is what we needed to prove. □

3.3 Proofs of the main results

Remember that $[y_K] = [P_1] \in (E(K)/pE(K))^\varepsilon$ by 2.4.4, and so $\delta y_K \in (\mathrm{Sel}^{(p)}(E/K))^\varepsilon$. We are going to analyze separately the eigenspaces $(\mathrm{Sel}^{(p)}(E/K))^{-\varepsilon}$ and $(\mathrm{Sel}^{(p)}(E/K))^\varepsilon$, using in a substantial way Propositions 3.2.8 and 3.2.11.

Proposition 3.3.1. $\mathrm{Sel}^{(p)}(E/K)^{-\varepsilon} = 0$.

Proof. Fix an element s in $\mathrm{Sel}^{(p)}(E/K)^{-\varepsilon}$. To show $s = 0$ it is enough, by the second part of Proposition 3.2.8, to show that $[s, \rho] = 0$ for all $\rho \in H^+ \smallsetminus I^+$. These elements have the form $\rho = (\tau h)^2$, for $h \in H \smallsetminus I$: let such an h be fixed.

Choose now a prime number $l_h = l$ which is unramified in M and has a prime factor λ_M in $\mathcal{O}_M$ satisfying

$$\left(\frac{M/\mathbb{Q}}{\lambda_M}\right) = \tau h \in \mathrm{Gal}(M/\mathbb{Q}).$$

Such primes exist and have positive density by Čebotarev's Density Theorem.

Lemma 3.3.2. Under these assumptions, l is inert in K: write as usual $(l)\mathcal{O}_K = \lambda$; moreover, λ splits completely in L. Finally, we have

$$\left(\frac{M/K}{\lambda_M}\right) = (\tau h)^2 \in H.$$

Proof. Since the restriction of τh to $\mathrm{Gal}(K/\mathbb{Q})$ is τ, l is inert in K; the restriction of τh to $\mathrm{Gal}(L/\mathbb{Q})$ is an element of order 2, so $2 = f(\lambda_L/l) = f(\lambda_L/\lambda)f(\lambda/l)$: we deduce $f(\lambda_L/\lambda) = 1$. Since the extension is unramified at λ, we obtain that λ splits completely in L. For the last point, recall that the Frobenius automorphism $\left(\frac{M/K}{\lambda_M}\right)$ is characterized by the property of being the unique $\sigma \in \mathrm{Gal}(M/K)$ satisfying

$$\sigma(x) \equiv x^{l^2} \mod \lambda_M \ \forall x \in \mathcal{O}_M;$$

the element $(\tau h)^2$ indeed satisfies this: $(\tau h)^2(x) = \tau h \tau h x \equiv \tau h x^l = (\tau h x)^l \equiv (x^l)^l = x^{l^2}$, since $\tau h = \left(\frac{M/\mathbb{Q}}{l}\right)$. □

By the last part of the lemma and by Proposition 3.2.11, to prove $[s, \rho] = 0$ it suffices to show that $s_\lambda = 0 \in H^1(K_\lambda, E_p)$: we are going to deduce this by using 3.1.9.

Let $c(l) \in H^1(K, E_p)$ be the Kolyvagin class associated with the prime number l, and $d(l)$ its image in $H^1(K, E)_p$. Remember their properties: $c(l)^\tau = -c(l)$ and $d(l)^\tau = -d(l)$ by 2.4.4; from 2.5.6 we know that $d(l)_v \neq 0$ for all primes v of K different from λ, i.e. $d(l)$ is locally trivial except perhaps at λ. We are going to show that $d(l)_\lambda \neq 0$; in other words, $d(l)$ isn't always locally trivial (this will enable us to apply 3.1.9). Again by 2.5.6 we know that $d(l)_\lambda$ is equal to 0 if and only if $P_1 = y_K$ is divisible by p in $E(K_\lambda)$, i.e. if and only if $y_K \in pE(K_\lambda)$. This last assertion holds if and only if λ splits completely in the field $L(\frac{1}{p}y_K)$ (see diagram (3.14)):

$$\lambda \text{ splits completely in } L\left(\frac{1}{p}y_K\right) \iff L\left(\frac{1}{p}y_K\right)_\lambda = K_\lambda \iff \frac{1}{p}y_K \in E(K_\lambda);$$

the first equivalence follows from Lemma 2.5.1 (with an abuse of notation, we use the subscript λ also for the completion of the bigger field). Suppose, by contradiction, that λ indeed splits completely in $L(\frac{1}{p}y_K)$: this would be equivalent, by the same argument we employed in Lemma 3.2.9, to

$$(\tau h)^2 = \left(\frac{M/K}{\lambda_M}\right) \in \mathrm{Gal}\left(M/L\left(\frac{1}{p}y_K\right)\right) = I.$$

But then $(\tau h)^2 \in H^+ \cap I = I^+$, against the hypotheses on $h \in H^+ \smallsetminus I^+$. Therefore, λ does not split completely in $L(\frac{1}{p}y_K)$, so $d(l)_\lambda \neq 0$.

We are thus in position to apply Proposition 3.1.9, which gives us that $s_\lambda = 0$. Therefore, by Proposition 3.2.11, we obtain that $[s, \rho] = [s, (\tau h)^2] = 0$. If we now repeat this argument for any h in the finite set $H^+ \smallsetminus I^+$, choosing each time a suitable prime $l = l_h$, we obtain that $s = 0$, by the second part of Proposition 3.2.8.

□

Proposition 3.3.3. Assume that $y_K \notin pE(K)$; let l be a prime integer which is unramified in $M/\mathbb{Q}$ and has a factor λ_M in $\mathcal{O}_M$ satisfying $\left(\frac{M/\mathbb{Q}}{\lambda_M}\right) = \tau h$, for $h \in H$. Then l is inert in K, and $\lambda = (l)\mathcal{O}_K$ splits completely in L. Moreover, the following are equivalent:

(1) $c(l) = 0 \in H^1(K, E_p)$
(2) $c(l) \in \mathrm{Sel}^{(p)}(E/K) \subset H^1(K, E_p)$
(3) $P_l \in pE(K_l)$
(4) $d(l) = 0 \in H^1(K, E)_p$
(5) $d(l)_\lambda = 0 \in H^1(K_\lambda, E)_p$
(6) $P_1 = y_K \in pE(K_\lambda)$
(7) $h^{1+\tau} \in I^+$.

Proof. The assertions on the behaviour of l in K and in L were already proved in Lemma 3.3.2.

(1 $\Leftrightarrow$ 2) We have that $c(l) \in H^1(K, E_p)^{-\epsilon}$ by Proposition 2.4.2, and $\mathrm{Sel}^{(p)}(E/K)^{-\varepsilon} = 0$ by Proposition 3.3.1; so, if $c(l)$ lies in $\mathrm{Sel}^{(p)}(E/K)$, it is trivial.

(1 $\Leftrightarrow$ 3) is Proposition 2.3.7, with $n = l$.

(1 $\Leftrightarrow$ 4) Recall that $d(l) = \alpha(c(l))$, so sufficiency is trivial; if $d(l) = 0$, $c(l) \in \ker(\alpha) = \mathrm{im}(\delta) = \delta((E(K)/pE(K))^{-\varepsilon}) = 0$ by 3.3.1.

(4 $\Leftrightarrow$ 5) Again sufficiency is trivial, since $d(l)_\lambda = \mathrm{Res}_\lambda(d(l))$. Suppose now $d(l)_\lambda = 0$; since we always have $d(l)_v = 0$ for all $v \neq \lambda$, this is equivalent to $d(l) \in Ш(E/K)_p$, or better $d(l) \in Ш(E/K)_p^{-\varepsilon}$; the last group is zero, again by 3.3.1.

(5 $\Leftrightarrow$ 6) is given by Theorem 2.5.2, again with $n = l$.

(6 $\Leftrightarrow$ 7) Notice that $h^{1+\tau} = hh^\tau = h(\tau h \tau) = (\tau h \tau)h = (\tau h)^2 = \left(\frac{M/K}{\lambda_M}\right)$, as we showed in Lemma 3.3.2. In the proof of Proposition 3.3.1 we obtained the equivalences

$$(\tau h)^2 \in I \iff \lambda \text{ splits completely in } L\left(\frac{1}{p}y_K\right) \iff y_K \in pE(K_\lambda),$$

which is exactly our claim, given that $h^{1+\tau} = (\tau h)^2$ already belongs to H^+. □

Proposition 3.3.4. $\mathrm{Sel}^{(p)}(E/K)^\varepsilon = \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$.

Proof. Remember that δy_K is indeed in $\mathrm{Sel}^{(p)}(E/K)^\varepsilon$ (see 2.4.4). Let s be a non-zero element of $\mathrm{Sel}^{(p)}(E/K)^\varepsilon$. To show that s is a multiple of δy_K, it is enough to show that $[s, \rho] = 0$ for all $\rho \in I$. Indeed, if this is the case, the morphism $s\colon H \to E_p$, $h \mapsto [s, h]$ factors through H/I: $s \in \mathrm{Hom}_{\mathcal{G}}(H/I, E_p) \cong \mathrm{Hom}_{\mathcal{G}}(E_p, E_p) \cong \mathbb{F}_p \delta y_K$ (see (3.11)). Actually, by the same arguments we used in the proof of Proposition 3.2.8, it is enough to show that $[s, \rho] = 0$ for all $\rho \in I^+$. These elements have the form $\rho = (\tau i)^2$, for $i \in I$; let such an i be fixed.

Choose now a prime number $q_i = q$ satisfying $c(q) \neq 0 \in H^1(K, E_p)$. By Proposition 3.3.3, we may obtain this q by asking that it has a prime factor $\mathfrak{q}_M$ in M with Frobenius substitution

$$\left(\frac{M/\mathbb{Q}}{\mathfrak{q}_M}\right) = \tau h \in \mathrm{Gal}(M/\mathbb{Q}), \quad h \in H.$$

We also know, again by Proposition 3.3.3, that $h^{1+\tau} \notin I^+$ and $c(q) \in H^1(K, E_p) \smallsetminus \mathrm{Sel}^{(p)}(E/K)$. Notice that q is inert in K, by Lemma 3.3.2; write $(q)\mathcal{O}_K = \mathfrak{q}$. Consider the field $L' = L_{\langle c(q) \rangle}$,

which corresponds by Galois Theory to the subgroup $\mathrm{Gal}_{\langle c(q)\rangle}(\overline{\mathbb{Q}}/L) \leq \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ (see the constructions in (3.7)).

Lemma 3.3.5. $\mathrm{Gal}(L'/L) \cong E_p$, and $L' \cap M = L$.

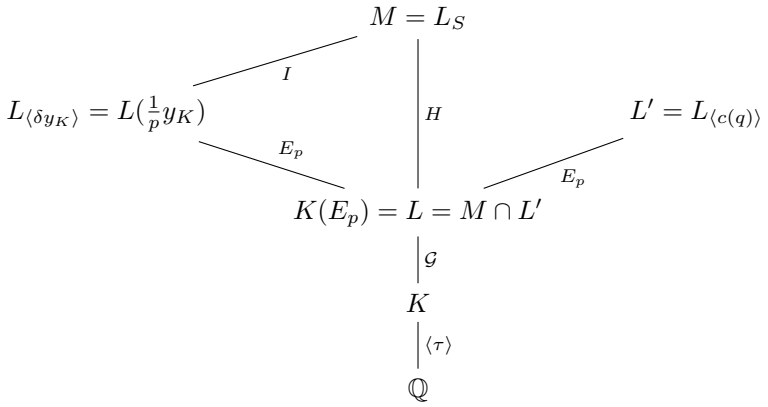
Proof. The first assertion follows from 3.8:

$$\mathrm{Gal}(L'/L) = \mathrm{Gal}(L_{\langle c(q)\rangle}/L) \cong \mathrm{Hom}(\langle c(q)\rangle, E_p(L)) \cong \mathrm{Hom}(\mathbb{F}_p, E_p) \cong E_p.$$

For the second assertion: $F = L' \cap M$ is a Galois extension of L; $\mathcal{G} = \mathrm{Gal}(L/K)$ acts both on $\mathrm{Gal}(L'/F) \lhd \mathrm{Gal}(L'/L)$ and on E_p. So, $\mathrm{Gal}(L'/F)$ is a $\mathcal{G}$-submodule of the simple module $\mathrm{Gal}(L'/L) \cong E_p$. It follows that $F = L$ or $F = L'$: the latter case can't happen, because $L' \leq M = L_S$ would imply $\mathrm{Gal}(\overline{\mathbb{Q}}/L') \geq \mathrm{Gal}(\overline{\mathbb{Q}}/L_S)$, i.e. $\mathrm{Gal}_{\langle c(q)\rangle}(\overline{\mathbb{Q}}/L) \geq \mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$, which is false since $c(q) \notin S$.

□

We have therefore the following field diagram.



Le now $l = l_i$ be a prime integer with the following properties :

$$\mathrm{Gal}(M/\mathbb{Q}) \supset \left(\frac{M/\mathbb{Q}}{l}\right) \ni \tau i \quad \exists i \in I; \tag{3.23}$$

$$\mathrm{Gal}(L'/\mathbb{Q}) \supset \left(\frac{L'/\mathbb{Q}}{l}\right) \ni \tau j \quad \exists j \in \mathrm{Gal}(L'/L);\ j^{1+\tau} \neq 1. \tag{3.24}$$

Since $M \cap L' = L$, these two conditions may be satisfied simultaneously. We are now going to apply Theorem 2.5.2 to $n = lq$. In this case, $\varepsilon_n = \varepsilon \cdot (-1)^{f_n} = \varepsilon \cdot (-1)^2 = \varepsilon$, so $d(lq) \in H^1(K, E)^{\varepsilon}_p$ by 2.4.2. We claim that $d(lq)$ is locally trivial for all places $v \neq \lambda$ of K, but that $d(lq)_\lambda \neq 0$.

First case: $v = \infty$ or $v \nmid n = lq$, i. e. $v \neq \lambda, \mathfrak{q}$. Then we have immediately $d(lq)_v = 0$ by the first part of Theorem 2.5.2.

Second case: $v = \mathfrak{q}$. Consider the ring class field K_l, and recall that $q \neq l$ splits completely in K_l by 1.7.4. The second part of Theorem 2.5.2 gives us that

$$d(ql)_\mathfrak{q} = 0 \in H^1(K_\mathfrak{q}, E)_p \iff P_l \in pE((K_l)_\mathfrak{Q}) = pE(K_\mathfrak{q}) \text{ for one, hence all, } \mathfrak{Q} \text{ over } \mathfrak{q} \text{ in } K_l. \tag{3.25}$$

Since the prime l satisfies (3.23), Proposition 3.3.3 with $h = i$ gives $h^{1+\tau} = i^{1+\tau} \in I^+$, hence $c(l) = 0$ in $H^1(K, E_p)$ and $P_l \in pE(K_l)$. Therefore, $P_l \in pE((K_l)_\mathfrak{Q}) = pE(K_\mathfrak{q})$, and we conclude by 3.25.

Third case: $v = \lambda$. As before, but switching the roles of l and q, we know that l splits completely in the ring class field K_q and

$$d(lq)_\lambda = 0 \in H^1(K_\lambda, E)_p \iff P_q \in pE((K_q)_{\mathfrak{L}}) = pE(K_\lambda) \text{ for one, hence all, } \mathfrak{L} \text{ over } \lambda \text{ in } K_q. \tag{3.26}$$

Suppose by contradiction that $d(lq)_\lambda = 0$. Then $P_q \in pE(K_\lambda)$. We claim that, in this case, λ would split completely in L'.

Lemma 3.3.6. If P_q is locally divisible by p in $E(K_\lambda)$, then λ splits completely in L'.

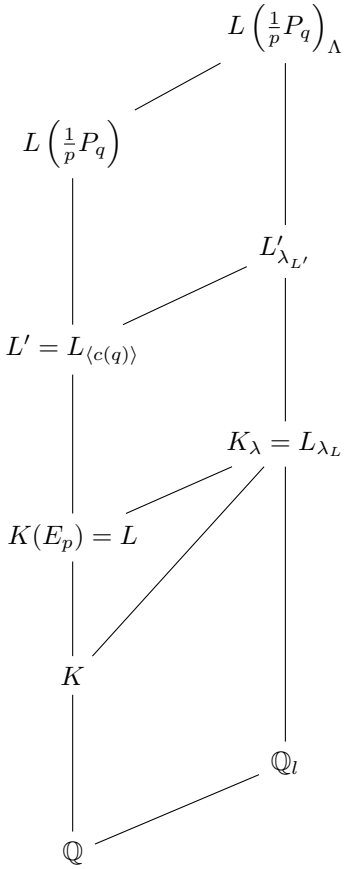
Proof. We first show that $L' \leq L\left(\frac{1}{p}P_q\right)$: equivalently, that

$$\mathrm{Gal}(\overline{\mathbb{Q}}/L') \geq \mathrm{Gal}\left(\overline{\mathbb{Q}}/L\left(\frac{1}{p}P_q\right)\right).$$

Suppose $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ fixes $\frac{1}{p}P_q$: we shall prove that $[c(q), \sigma] = 0$. Recall that $c(q)$ was represented by the cocycle

$$\sigma \mapsto \sigma\left(\frac{1}{p}P_q\right) - \frac{1}{p}P_q - \frac{(\sigma - 1)P_q}{p}$$

for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and so also for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ (see Lemma 2.3.6). Since our σ fixes $\frac{1}{p}P_q$, it fixes also P_q; hence, $[c(q), \sigma] = 0$.



Assume now $P_q \in pE(K_\lambda)$, i.e. $\frac{1}{p}P_q \in E(K_\lambda)$. We are going to prove that λ splits completely in $L\left(\frac{1}{p}P_q\right)$: this will imply that λ splits completely also in $L' \leq L\left(\frac{1}{p}P_q\right)$.

Recall that $K_\lambda = L_{\lambda_L}$ because λ is assumed to split completely in L; moreover, since λ splits completely in the ring class field K_q, we also have $(K_q)_{\mathfrak{L}} = K_\lambda$ for any prime $\mathfrak{L}$ of K_q over λ. Then, $P_q \in E(K_q) \leq E(K_\lambda)$. Assume now the stronger condition $\frac{1}{p}P_q \in E(K_\lambda)$. In this case the field K_λ, which contains L, contains also $L\left(\frac{1}{p}P_q\right)$. Then $L\left(\frac{1}{p}P_q\right)_\Lambda = K_\lambda$, which occurs if and only if λ splits completely in $L\left(\frac{1}{p}P_q\right)$. □

We proved that, under the assumption $d(lq)_\lambda = 0$, λ splits completely in L': this implies that τj has order 2 in $\mathrm{Gal}(L'/\mathbb{Q})$ (see (3.24)). But $1 = (\tau j)^2 = \tau(j\tau j) = (j\tau j)\tau = jj^\tau = j^{1+\tau}$ contradicts our assumption $j^{1+\tau} \neq 1$. We can conlcude that $d(lq)_\lambda$ is not trivial.

We have shown that the class $d(lq)$ is locally trivial at each $v \neq \lambda$ and $d(lq)_\lambda \neq 0$. We may thus apply Proposition 3.1.9 with $d = d(lq) \in H^1(K, E)^\varepsilon_p$ to conclude that $s_\lambda = 0$ in $H^1(K_\lambda, E_p)^\varepsilon$ (remember that s was an element of $\mathrm{Sel}^{(p)}(E/K)^\varepsilon$). By Proposition 3.2.11, $[s, \rho] = [s, (\tau i)^2] = 0$. If we repeat this argument for any i in the finite group I, choosing each time a suitable prime $l = l_i$, we obtain that $[s, (\tau i)^2] = 0$ for all i in I, which was we claimed in the beginning of the proof. □

Propositions 3.3.1 and 3.3.4 give immediately the proof of Proposition 2.1.6:

$$\mathrm{Sel}^{(p)}(E/K) = \mathrm{Sel}^{(p)}(E/K)^\varepsilon \oplus \mathrm{Sel}^{(p)}(E/K)^{-\varepsilon} = \mathrm{Sel}^{(p)}(E/K)^\varepsilon = \langle \delta y_K \rangle.$$

We may finally prove Theorem 2.1.4.

Proof of Theorem 2.1.4. Consider again the exact sequence

$$0 \longrightarrow E(K)/pE(K) \xhookrightarrow{\delta} \mathrm{Sel}^{(p)}(E/K) \xrightarrow{\alpha} Ш(E/K)_p \longrightarrow 0.$$

We proved Proposition 2.1.6, which implies that δ is an isomorphism: therefore $Ш(E/K)_p = \mathrm{coker}(\delta) = 0$, which was the second assertion. For the first, notice that

$$r = \mathrm{rk}_{\mathbb{Z}} E(K) = \dim_{\mathbb{F}_p} E(K)/pE(K).$$

Indeed we have

$$E(K) = E(K)_{\mathrm{tors}} \oplus \langle P_1, \cdots, P_r \rangle \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$$

and multiplication by p is an isomorphism in the finite abelian group $E(K)_{\mathrm{tors}}$ because $E(K)_p = 0$: therefore, $E(K)/pE(K) \cong \mathbb{Z}^r/p\mathbb{Z}^r \cong \mathbb{F}_p^r$. Then we conclude, because $\dim_{\mathbb{F}_p} E(K)/pE(K) = \dim_{\mathbb{F}_p} \mathrm{Sel}^{(p)}(E/K) = \dim_{\mathbb{F}_p} \langle \delta y_K \rangle = 1$, so that $E(K)$ has rank 1 as claimed. □

Bibliography

[1] J. Cassels and A. Fröhlich (editors), *Algebraic Number Theory - Proceedings of an instructional conference organized by the London Mathematical Society*, Academic Press Inc. (London), 1967.

[2] D. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, second edition, John Wiley & Sons, Inc., 1989.

[3] H. Darmon, *Rational points on modular elliptic curves*, Lecture notes, 2003.

[4] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, 1989, in *L-functions and arithmetic*, pages 253-256, Cambridge Univ. Press, Cambridge 1991.

[5] B. H. Gross, *Heegner points on $X_0(N)$*, in *Modular Forms*, 87-106, Ellis Horwood, Chichester, 1984.

[6] B. H. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84, pages 225-320, 1986.

[7] R. Hartshorne, *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1977.

[8] D. Husemöller, *Elliptic curves*, second edition, volume 111 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2004.

[9] G. J. Janusz, *Algebraic number fields*, Academic Press, New York-London, 1973

[10] V. A. Kolyvagin, *Euler systems*, in The Grothendieck Festschrift, Vol. II, 435-483, Progr. Math. 87, Birkhäuser Boston, Boston, MA, 1990.

[11] N. Koblitz, *Introduction to elliptic curves and modular forms*, second edition, volume 97 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1993.

[12] M. Longo and S. Vigni, *A refined Beilinson-Bloch conjecture for motives of modular forms*, available at https://www.math.unipd.it/ mlongo/docs/RefinedBB.pdf

[13] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications mathématiques de l'I.H.É.S., tome 47, p. 33-186, 1977.

[14] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, in *L-functions and arithmetic*, Cambridge Univ. Press, Cambridge 1991.

[15] J. S. Milne, *Arithmetic Duality Theorems*, volume 1 of *Perspective in Mathematics*, Academic Press Inc., Boston, 1986.

[16] J. S. Milne, *Class Field Theory*, 2020, notes available at www.jmilne.org/math/

[17] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, 2006.

[18] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[19] J. J. Rotman, *An Introduction to Homological Algebra*, second edition, Springer, New York 2009.

[20] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15, 259-331, 1972.

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, volume 106 of *Graduate Texts in Mathematics* Springer, New York, 2009.

[22] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1994.

[23] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*, second edition, Springer, 2015.

[24] *Graduate Number Theory Seminar: Kolyvagin's Application of Euler Systems to Elliptic Curves*, MIT Seminar, Lecture notes available at https://kskedlaya.org/kolyvagin-seminar/