Antonio de Jesus Campos Rodriguez

Parametrizing the 2-Selmer group and the 3-Selmer group of an elliptic curve

Master thesis

Thesis advisor: dr. P. J. Bruin

Date master exam: 30 May 2016

Mathematisch Instituut, Universiteit Leiden

Acknowledgements

I express my deep gratitude to Peter Bruin who kindly accepted to supervise my master's thesis, to David Holmes for helping me so much since I started my master's program in Leiden, to Bas Edixhoven for helping me in a crucial moment, and finally to Antoine Chambert-Loir and Pierre-Guy Plamondon who helped me a lot during difficult times in Orsay.

Finally, I dedicate this work to my brother Jesus Campos Rodriguez and my mother Silvia Rodriguez Martinez. You mean everything to me.

Contents

Introduction

Let E/k be an elliptic curve over a field k of characteristic 0. Let $n \geq 2$ be a positive integer. In this work we will study the following diagrams where the $\leftrightarrow$ indicate bijections between the left side and the right side up to equivalence. The first is

$$\begin{array}{ccc} \mathrm{Sel}_n(E/k) & \longleftrightarrow & \{\text{locally soluble } n\text{-coverings of } E/k\} \\ \rotatebox{90}{$\subset$} & & \rotatebox{90}{$\subset$} \\ H^1(k, E[n]) & \longleftrightarrow & \{n\text{-coverings of } E/k\} \end{array}$$

and the second is

$$\begin{array}{ccc} H^1(k, E) & \longleftrightarrow & \{\text{homogeneous spaces of } E/k\} \\ \rotatebox{90}{$\subset$} & & \rotatebox{90}{$\subset$} \\ H^1(k, \mathrm{Isom}(E)) & \longleftrightarrow & \{\text{twists of } E/k\} \end{array}$$

We will parametrize $H^1(k, E[n])$ by n-coverings of E/k (definition 1.2.1), by Brauer-Severi diagrams (definition 0.6.1), by twists of $[E \to \mathbb{P}^{n-1}, \omega_E]$ (definition 1.3.1) and by torsor-divisor class pairs (definition 1.4.1). Using these parametrizations and the above diagrams, we will study the cases $n = 2$ and $n = 3$. If we consider the invariants $I(E), J(E)$ of the elliptic curve E/k, then the parametrization

$$H^1(k, E[n]) \leftrightarrow \{n\text{-coverings of } E/k\}$$

when $n = 2$ will imply the bijection

$$\mathrm{Sel}_2(E/k) \leftrightarrow \left\{ \begin{array}{c} \text{binary quartic forms } g(x,z) \\ \text{with invariants } \lambda^4 I(E), \lambda^6 J(E) \text{ for some } \lambda \in k^* \\ \text{such that } y^2 = g(x,1) \text{ is locally soluble} \end{array} \right\}$$

and the parametrization

$$H^1(k, E[n]) \leftrightarrow \{\text{twists of } [E \to \mathbb{P}^{n-1}, \omega_E]\}$$

when $n = 3$ will imply the bijection

$$\mathrm{Sel}_3(E/k) \leftrightarrow \{ \begin{array}{c} \text{locally soluble ternary cubic forms} \\ \text{with invariants } I(E), J(E) \end{array} \},$$

In Chapter 0 we will introduce the first definitions and results to understand the aforementioned diagrams and parametrizations. In particular, we prove the bijection

$$H^1(k, \mathrm{Isom}(E)) \leftrightarrow \{\text{twists of } E/k\}.$$

In Chapter 1 we treat the bijection

$$H^1(k, E) \leftrightarrow \{\text{homogeneous spaces of } E/k\}.$$

Then we will parametrize $H^1(k, E[n])$ in terms of n-coverings of E/k and we explain how it induces the bijection

$$\mathrm{Sel}_n(E/k) \leftrightarrow \{\text{locally soluble } n\text{-coverings of } E/k\}.$$

After this, we consider the remaining parametrizations of $H^1(k, E[n])$ in terms of twists of $[E \to \mathbb{P}^{n-1}, \omega_E]$, Brauer-Severi diagrams and torsor-divisor class pairs. Finally, we will say a few words about the period-index problem for elliptic curves.

In Chapter 2 we will study how the diagrams and parametrizations yield the bijection between the 2-Selmer group of E/k and the equivalence classes of binary quartic forms $g(x, z)$ with invariants $\lambda^4 I(E), \lambda^6 J(E)$ for some $\lambda \in k^*$ and such that $y^2 = g(x, 1)$ is locally soluble, and also the bijection between the 3-Selmer group of E/k and the equivalence classes of locally soluble ternary cubic forms with invariants $I(E), J(E)$.

Chapter 0 - Preliminaries

In this chapter we review some definitions and results which are used in chapters 1 and 2. Throughout chapters 0, 1 and 2 we assume that k is an algebraic number field.

0.1 Differentials and Riemann-Roch for curves

For a smooth curve C/k, we recall that the space of differential forms is the $\overline{k}$-vector space Ω_C generated by elements of the form df for all $f \in \overline{k}(C)$ subject to the rules $d(f+g) = df + dg$, $d(fg) = gdf + fdg$ and $da = 0$ for all $a \in \overline{k}$.

0.1.1 Example Consider a ternary cubic form $U(x,y,z) = ax^3+by^3+cz^3+a_2x^2y+a_3x^2z+b_1xy^2+b_3y^2z+c_1xz^2+c_2yz^2+mxyz$. We have the relation $\frac{1}{z^2}\frac{\partial U}{\partial x}d(\frac{x}{z}) + \frac{1}{z^2}\frac{\partial U}{\partial y}d(\frac{y}{z}) = 0$ because factoring z^2 from the partial derivative of U with respect to x and y yields

$$\frac{1}{z^2}\frac{\partial U}{\partial x}(x,y,z)d(\frac{x}{z}) + \frac{1}{z^2}\frac{\partial U}{\partial y}(x,y,z)d(\frac{y}{z}) = \frac{\partial U(x,y,1)}{\partial x}d(\frac{x}{z}) + \frac{\partial U(x,y,1)}{\partial y}d(\frac{y}{z})$$

and by means of a change of variables $X := \frac{x}{z}$, $Y := \frac{y}{z}$ and defining $u(X,Y) := U(\frac{x}{z}, \frac{y}{z}, 1)$ we have

$$\frac{1}{z^2}\frac{\partial U}{\partial x}(x,y,z)d(\frac{x}{z}) + \frac{1}{z^2}\frac{\partial U}{\partial y}(x,y,z)d(\frac{y}{z}) = \frac{\partial U(x,y,1)}{\partial x}d(\frac{x}{z}) + \frac{\partial U(x,y,1)}{\partial y}d(\frac{y}{z})$$

$$= \frac{\partial u(X,Y)}{\partial X}d(X) + \frac{\partial u(X,Y)}{\partial Y}d(Y) = d(u(X,Y)) = 0$$

Another familiar example is obtained by considering an elliptic curve E/k of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. In this case, the invariant differential of E/k is defined by $\omega_E := \frac{dy}{2y+a_1x+a_3}$.

Now we recall the Riemann-Roch theorem for curves. For this, one ingredient that we need is the canonical divisor class of a curve C/k. Recall that for any point $P \in C$, we define a uniformizer for C at P as an function $t \in \overline{k}(C)$ which is a generator of the maximal ideal of the local ring of C at P. Now take any nonzero $\omega \in \Omega_C$. Then there exists a unique $g \in \overline{k}(C)$ such that $\omega = gdt$ (proposition 4.3 of chapter II in [17]), and we are allowed to define $\mathrm{ord}_P(\omega) := \mathrm{ord}_P(g)$ and the divisor $\mathrm{div}(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega)P$ which is an element of $\mathrm{Div}(C)$. The image of this divisor in $\mathrm{Pic}(C)$ is called the canonical divisor class on C and any representative of this class is called a canonical divisor on C.

Another ingredient is the $\overline{k}$-vector space $\mathcal{L}(D) := \{f \in \overline{k}(C)^* : \mathrm{div}(f) + D \geq O\} \cup \{0\}$. The dimension of this vector space is finite, and we denote it by $l(D)$.

0.1.2 Theorem For a smooth curve C of genus g and a canonical divisor K_C on C, we have $l(D) - l(K_C - D) = \deg(D) - g + 1$.

Proof: See theorem 5.4, chapter II in [17]. □

We also recall that when we have a morphism between curves $\phi : C_1 \to C_2$ over k, there is an induced morphism $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ given by $\omega := \sum_i f_i dg_i \mapsto \sum_i \phi^*(f_i) d\phi^*(g_i)$, where in general $\phi^*(f) = f \circ \phi$ for all $f \in \overline{k}(C_2)$ so that $f \circ \phi \in \overline{k}(C_1)$. We also recall that Ω_C is a 1-dimensional $\overline{k}(C)$-vector space.

Consider a smooth curve C/k and a divisor D on C. We recall that D is called k-rational if $D^\sigma = D$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

0.1.3 Proposition: If C/k is a smooth curve and D is a k-rational divisor on C then $\mathcal{L}(D)$ has a basis consisting of functions in $k(C)$.

Proof: See proposition 5.8, chapter II in [17]. □

0.2 Some algebraic geometry

The objective is to describe how the divisor nO on an elliptic curve E/k defines a morphism $E \to \mathbb{P}^{n-1}$.

We recall that giving a morphism of k-schemes from X to $\mathbb{P}^{n-1}$ is equivalent to taking an invertible sheaf $\mathcal{L}$ on X together with n global sections $s_0, \ldots, s_{n-1} \in \Gamma(X, \mathcal{L})$ such that they generate $\mathcal{L}$. This equivalence is described in the proposition below. For this, we consider the k-scheme $\mathbb{P}^{n-1}_k$ and we will also consider the twisting sheaf of Serre $\mathcal{O}_X(1)$ (see section 5 of chapter II in [9]). Also, if $f : X \to Y$ is a morphism of schemes and $\mathcal{L}$ is an invertible sheaf on Y, then we will also consider the pullback $f^*\mathcal{L}$ (section 5 of chapter II in [9]) which is an invertible sheaf on X. The proposition is the following.

0.2.1 Proposition (i) Suppose that $\phi : X \to \mathbb{P}^{n-1}$ is a morphism of k-schemes. Consider the invertible sheaf $\mathcal{O}_Y(1)$ where $Y := \mathbb{P}^{n-1}$. Then $\mathcal{L} := \phi^*\mathcal{O}_Y(1)$ is an invertible sheaf on X and it's generated by the n global sections ϕ^*x_0, ..., ϕ^*x_{n-1}.

(ii) If $\mathcal{L}$ is an invertible sheaf on X generated by n global sections $s_0, \ldots, s_n$, then there exists a unique morphism $\phi : X \to \mathbb{P}^{n-1}$ of k-schemes such that $\phi^*\mathcal{O}_Y(1)$ is isomorphic to $\mathcal{L}$ and such that $s_0 = \phi^*x_0$, ..., $s_{n-1} = \phi^*x_{n-1}$.

Proof: See theorem 7.1, chapter II in [9]. □

If we are in the situation (ii) of the previous proposition, then the map ϕ can be described explicitly. Consider any $x \in X(k)$. We have n global

sections $s_0, \ldots, s_n$ which generate $\mathcal{L}$. This implies that there exists some i such that $s_i(x) \in \mathcal{L}_x \otimes_{\mathcal{O}_{X,x}} k(x)$ does not vanish. So for each j, there exists a unique $\alpha_j \in k(x) = k$ such that $s_j(x) = \alpha_j s_i(x)$, and we define $\phi(x) := (\alpha_0 : \ldots : \alpha_{n-1}) \in \mathbb{P}^{n-1}$. It can be shown that this map does not depend on the chosen i, and we denote the point $(\alpha_0 : \ldots : \alpha_{n-1})$ by $(s_0(x) : \ldots : s_{n-1}(x))$. Note that if we choose another set of global sections $s'_0, \ldots, s'_{n-1}$ which also generates $\mathcal{L}$, then the morphism $\phi' : X \to \mathbb{P}^{n-1}$ differs from ϕ by to an automorphism of $\mathbb{P}^{n-1}$.

Now let C be a smooth projective curve of genus 1 over k, and let D be a divisor of degree n on C. We denote by $|D|$ the set of effective divisors on C of degree n which are linearly equivalent to D, and we call $|D|$ a complete linear system. In the previous section we defined the k-vector space $\mathcal{L}(D)$. It turns out that we can identify the projective space $\mathbb{P}(\mathcal{L}(D)) = \mathbb{P}_k^{n-1}$ with the complete linear system $|D|$ (proposition 7.7, chapter II in [9]).

In order to apply the previous proposition to any smooth curve C/k of genus 1, we define the invertible sheaf $\mathcal{O}_C(D)$ by assigning to U the k-vector space $\{f \in k(C) : \mathrm{div}(f)_{|U} + D \geq 0\}$. We have $\mathcal{L}(D) = \Gamma(C, \mathcal{O}_C(D))$, and we know by the Riemann-Roch theorem that $\mathcal{L}(D)$ has dimension n. If we take a basis $s_0, \ldots, s_{n-1}$ of $\mathcal{L}(D)$, then we have n global sections which generate $\mathcal{O}_C(D)$ and we apply (ii) of the previous proposition to obtain a morphism $C \to \mathbb{P}^{n-1}$, which is explicitly given by $x \mapsto (s_0(x) : \ldots : s_{n-1}(x))$. Note again that choosing another basis $s'_0, \ldots, s'_n$ yields the same morphism $C \to \mathbb{P}^{n-1}$ up to an automorphism of $\mathbb{P}^{n-1}$. We will say that the morphism $C \to \mathbb{P}^{n-1}$ is the morphism induced by the linear system $|D|$. It can be shown that the degree of the morphism $C \to \mathbb{P}^{n-1}$ induced by the linear system $|D|$ has degree n, and also that this morphism is an embedding if $n \geq 3$. In the case $n = 2$ we get a two-to-one map, which is called a double cover.

Now we talk about divisors. Let X be a scheme. Recall that a Cartier divisor is a global section of the sheaf $\mathcal{H}_X^*/\mathcal{O}_X^*$ where $\mathcal{H}_X$ is the sheaf of total quotient rings, and a principal Cartier divisor is a Cartier divisor which belongs to the image of the map $\Gamma(X, \mathcal{H}_X^*) \to \Gamma(X, \mathcal{H}_X^*/\mathcal{O}_X^*)$, and two Cartier divisors are linearly equivalent if their difference is a principal divisor. The set of Cartier divisors modulo principal divisors is denoted by $\mathrm{CaCl}(X)$.

Suppose that X is a scheme which is Noetherian, integral, separated and such that every local ring $\mathcal{O}_{X,x}$ of dimension 1 is regular. A prime divisor on X is a closed integral subscheme of X such that $\mathcal{O}_{X,\xi}$ has dimension 1, where ξ is the generic point of the closed integral subscheme, and a Weil divisor is an element of the free abelian group generated by the prime divisors on X. For each closed integral subscheme Y of X, we take the corresponding generic point ξ. The local ring $\mathcal{O}_{Y,\xi}$ is a discrete valuation ring whose quotient field is $k(X)$, and we consider the corresponding valuation v_Y. The divisor of an element $f \in k(X)^*$ is $\sum_{\substack{Y \\ \text{prime} \\ \text{divisor}}} v_Y(f)Y$ and this is called a principal Weil divisor. The group of Weil divisors modulo principal Weil divisors is denote by $\mathrm{Cl}(X)$.

Also, recall that $\mathrm{Pic}(X)$ denotes the group of isomorphism classes of invertible sheaves on X under the operation $\otimes$.

We will apply the following proposition when X is an elliptic curve E/k.

0.2.2 Proposition If X is an integral scheme, then $\mathrm{CaCl}(X) \cong \mathrm{Pic}(X)$.

Proof: See proposition 6.15, chapter II in [9]. □

And we will apply the following proposition in the case $X = \mathbb{P}_k^{n-1}$.

0.2.3 Proposition Suppose that X is a scheme whose local rings are unique factorization domains. If X is Noetherian, integral and separated, then $\mathrm{Cl}(X) \cong \mathrm{Pic}(X)$.

Proof: See corollary 6.16, chapter II in [9]. □

We will consider the morphism $E \to \mathbb{P}_k^{n-1}$ induced by the linear system $|nO|$, and we will view a hyperplane H contained in $\mathbb{P}_k^{n-1}$ as a Weil divisor. By the previous proposition, we know that $\mathrm{Cl}(\mathbb{P}_k^{n-1}) \cong \mathrm{Pic}(\mathbb{P}_k^{n-1})$, and in this isomorphism the class of H corresponds to the class of the invertible sheaf $\mathcal{O}_X(1)$ (see the proof of corollary 6.17, chapter II in [9]). Now it makes sense to talk about the pullback of the class in $\mathrm{Cl}(X)$ of our divisor H. Indeed, we will define this as the class in $\mathrm{Pic}(X)$ of the pullback of the invertible sheaf $\mathcal{O}_X(1)$. In the next chapter we will make use of all this.

We conclude with the following lemma which we will use frequently.

0.2.4 Lemma Consider an elliptic curve E/k. Then:

(i) The only $\overline{k}$-isomorphisms of curves ϕ from E to itself satisfying $\phi^*\omega_E = \omega_E$ are the translation maps τ_P for all $P \in E$.

(ii) Two divisors D and D' on E are linearly equivalent if and only if they have the same degree and the same sum when viewed as elements of the abelian group defined on E.

(iii) Suppose that $P \in E$. Then $\tau_P^*(nO)$ is linearly equivalent to nO if and only if $P \in E[n]$.

(iv) Suppose that $\phi : E \to E$ is a $\overline{k}$-isomorphism of curves. Then $\phi^*(nO)$ is linearly equivalent to nO if and only if ϕ extends to a $\overline{k}$-isomorphism $\varphi : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$.

Proof: (i) We know that the translations maps τ_P satisfy $\tau_P^*\omega_E = \omega_E$. Conversely, suppose that ϕ is a $\overline{k}$-automorphism of E such that $\phi^*\omega_E = \omega_E$. Consider the composition $\phi' = \tau_{-\phi(O)} \circ \phi$. Then $\phi'(O) = O$ and this means that ϕ' belongs to $\mathrm{End}(E)$, i.e. the morphisms $E \to E$ such that O is mapped to O. Also note that $\phi'^*\omega_E = \omega_E$ because $\tau_{-\phi(O)}^*\omega_E = \omega_E$. But we know that there is a ring homomorphism $\mathrm{End}(E) \to \overline{k}^*$ given by $\varphi \mapsto a_\varphi$ where $\varphi \in \mathrm{End}(E)$, $a_\varphi \in \overline{k}$ and $\varphi^*\omega_E = a_\varphi \omega_E$. Furthermore, because the characteristic of k is 0 we

know that this ring homomorphism injects into $\overline{k}^*$ (see the proof of corollary 5.6 (c), chapter III in [17]). So the equality $\phi'^*\omega_E = \omega_E$ implies that ϕ' is the identity on E. In other words, ϕ is the translation map by $\phi(O)$.

(ii) This is a consequence of corollary 3.5, chapter III in [17].

(iii) We have $\tau_P^*(nO) = n(-P)$. So if $\tau_P^*(nO)$ is linearly equivalent to nO, then (ii) implies that $n(-P)$ is equal to nO when we view them as elements of the abelian group on E, but $nO = O$ in this abelian group structure, which implies that $-P$ is an n-torsion point. Hence, $P \in E[n]$. Conversely, if $P \in E[n]$ then also $-P$ and the divisors $n(-P)$ and nO have the same degree and they are equal when we view them as elements of the abelian group on E. So (ii) implies that $\tau_P^*(nO)$ is linearly equivalent to nO.

(iv) Suppose that nO is linearly equivalent to $\phi^*(nO)$. The complete linear systems $|nO|$ and $|\phi^*(nO)|$ define morphisms $E \to \mathbb{P}^{n-1}$, and the linear equivalence implies that these morphisms are equal up to a $\overline{k}$-automorphism of $\mathbb{P}^{n-1}$ (this follows from proposition 0.2.1) and this is the isomorphism extending ϕ. Conversely, if a $\overline{k}$-automorphism of $\mathbb{P}^{n-1}$ extends ϕ then the morphisms defined by $|nO|$ and $|\phi^*(nO)|$ are equal up to this automorphism of $\mathbb{P}^{n-1}$ (which follows again from proposition 0.2.1). This implies that nO is linearly equivalent to $\phi^*(nO)$. □

0.3 The Brauer group of a field and Brauer-Severi varieties

We review the definition of central simple algebras and the Brauer group. Also, we recall an example of the local-global principle related to central simple algebras over number fields.

0.3.1 Definition Consider a field k and a k-algebra A. We call A a central simple k-algebra if the image of $k \to A$ is equal to the center of A, and if A has exactly two two-sided ideals, namely (0) and A. We say that A is finite if the dimension of A over k is finite as k-vector space, and the dimension is called the rank.

As example, we can take $A := k$ where k is any field, and in this case A has rank 1 over k. Another example is $A := \mathrm{Mat}_n(k)$ which has rank n^2 over k.

If we have a central simple k-algebra A, then there exists a unique division algebra D over k and a unique natural number $n \geq 1$ such that $A \cong M_n(D)$ as k-algebras (lemma 3.1 in [11]). Using this, we can define an equivalence relation on the set of central simple k-algebras which will induce the definition of the Brauer group of k.

0.3.2 Definition The Brauer group of a field k, denoted by $\mathrm{Br}(k)$, is the (abelian) group given by the equivalence classes of central simple k-algebras, where the equivalence relation is defined as follows: if A and B are two central simple k-algebras, let D_1 and D_2 be the corresponding division algebras over k

and $n, m \geq 1$ such that $A \cong M_n(D_1)$ and $B \cong M_m(D_2)$. We say that A and B are equivalent if $D_1 \cong D_2$ as k-algebras. It can be shown that the tensor product of two central simple algebras over k is again a central simple algebra over k. The group operation on the set of equivalence classes is defined by means of this tensor product.

As examples, it can be shown that the Brauer group of a finite field is trivial and the Brauer group of an algebraically closed field is trivial as well. Also, $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ and if $k/\mathbb{Q}_p$ is a finite extension for some prime p then $\mathrm{Br}(k) \cong \mathbb{Q}/\mathbb{Z}$.

The definition 0.3.2 allow us to understand an example of the local-global principle:

0.3.3 Theorem (Brauer-Hasse-Noether) Let k be a number field and let n be a positive integer. Denote by k_v the completion of k at the place v. Suppose that A is a central simple algebra over k of rank n such that $A \otimes_k k_v \cong \mathrm{Mat}_n(k_v)$ as k-algebras for every place v of k. Then $A \cong A \otimes_k k \cong \mathrm{Mat}_n(k)$ as k-algebras.

Proof: See [10]. □

We will frequently talk about twists of a variety X/k.

0.3.4 Definition (i) A twist of a variety X/k is another variety Y/k such that $X_{\overline{k}} \cong Y_{\overline{k}}$, i.e. they become isomorphic after base change to $\mathrm{Spec}(\overline{k})$.
(ii) We say that two twists $Y/k, Y'/k$ of X/k are k-equivalent if there exists an isomorphism $\theta : Y' \to Y$ defined over k. The set of k-equivalence classes of twists of a variety X/k is denoted by $\mathrm{Twists}(X/k)$.

A useful description of the Brauer group of k is given in terms of twists of $\mathbb{P}^{n-1}$.

0.3.5 Proposition There is a bijection between k-equivalence classes of central simple algebras over k of dimension n^2 and twists of $\mathbb{P}^{n-1}/k$, up to k-isomorphism.
Proof: Corollary 5.3 in [11]. □

We will consider Brauer-Severi varieties as well.

0.3.6 Definition A Brauer-Severi variety is a k-variety X such that it becomes isomorphic to $\mathbb{P}^n$ over $\overline{k}$ for some $n \geq 1$.

Using the two previous proposition of this section, it is possible to check that any Brauer-Severi variety over a number field k satisfies the local-global principle.

0.3.7 Proposition If X is a Brauer-Severi variety over a number field k such that $X(k_v) \neq \emptyset$ for every place v of k, then $X(k) \neq \emptyset$.

The proof of this proposition (which we will prove in section 0.5) makes use of the following refinement of proposition 0.3.5.

0.3.8 Theorem For any central simple k-algebra A of dimension n^2 there exists a unique Brauer-Severi variety X_A over k (up to k-isomorphism) of dimension $n-1$ such that the following two properties hold: (a) the assignment $A \mapsto X_A$ induces a bijection between equivalence classes of central simple k-algebras of dimension n^2 and k-isomorphic classes of Brauer-Severi varieties over k of dimension $n-1$, and (b) any field extension k'/k is a splitting field for A, i.e. $A \otimes_k k' \cong \mathrm{Mat}_m(k')$ for some $m \geq 1$, if and only if $X_A(k') \neq \emptyset$.

Proof: See theorem 5.1 and corollaries 5.2 and 5.3 in [11]. □

In the last section of this chapter we will talk about the obstruction map. This map can be defined in two ways, and we will mention the first in the last section of this chapter and the second in Chapter 1. For the second, we need the following.

For a smooth projective variety X/k with base change $X_{\overline{k}}$, we know that there is an exact sequence of Galois modules (see section 0.5) given by

$$0 \to \overline{k}^* \to \overline{k}(X)^* \to \mathrm{Div}(X_{\overline{k}}) \to \mathrm{Pic}(X_{\overline{k}}) \to 0$$

After splitting into short exact sequences and taking Galois cohomology (section 0.5) we obtain the following proposition.

0.3.9 Proposition: There is an exact sequence

$$0 \to k^* \to k(X)^* \to \mathrm{Div}(X_{\overline{k}})^{G_k} \to \mathrm{Pic}(X_{\overline{k}})^{G_k} \xrightarrow{\delta_X} \mathrm{Br}(k)$$

where $\mathrm{Div}(X_{\overline{k}})^{G_k}$ and $\mathrm{Pic}(X_{\overline{k}})^{G_k}$ are the elements in $\mathrm{Div}(X_{\overline{k}})$ and $\mathrm{Pic}(X_{\overline{k}})$ fixed by $G_k = \mathrm{Gal}(\overline{k}/k)$, and δ_X is defined as in [12].

Proof: See [12]. □

0.4 Homogeneous spaces for elliptic curves and Jacobians

Consider an elliptic curve E/k with distinguished point O.

0.4.1 Definition (i) A homogeneous space C for E/k (also called a torsor under E) is a genus 1 smooth projective curve equipped with a morphism $\mu : C \times E \to C$ defined over k which defines a simply transitive right action of

E on C. This means that, for any $\overline{k}$-points $p \in C$ and $P \in E$, if we define $p+P := \mu(p,P)$ then μ satisfies the rules $p+O=p$, $(p+P)+Q = p+(P+Q)$, and given $p,q \in C$ there exists a unique point in E, denoted by $q-p$, such that $p+(q-p)=p$.

(ii) Two homogeneous spaces C/k and C'/k are k-equivalent if there is a morphism $\theta : C \to C'$ defined over k and compatible with the action of E on C and C'. In other words, $\theta(p+P) = \theta(p) +' P$ where $+$ corresponds to the action of E on C and $+'$ corresponds to the action of E on C'.

Note that E defines a right action on itself by means of a translation map, i.e. for $P,Q \in E$ define $\mu(P,Q) = P+Q$. The k-equivalence class of this homogeneous space structure on E is called the trivial class.

0.4.2 Observation Note that for every point $R \in E$, the translation map $\tau_R : E \to E$ satisfies $\tau_R(P+Q) = \tau_R(P) + R$ for all $P,Q \in R$. Conversely, if $\phi : E \to E$ satisfies $\phi(P+Q) = \phi(P) + Q$ for all $P,Q \in E$, then choose $P = O$ to obtain $\phi(Q) = \phi(O) + Q$, i.e. ϕ is the translation map τ_R with $R = \phi(O)$. In particular, the only isomorphisms from E to itself respecting the torsor structure on E are the translation maps τ_R.

The symbols $+, -$ behave as expected:

0.4.3 Lemma: If C/k is a homogeneous space for E/k, then for all $p,q \in C$, $P,Q \in E$ we have (i) $p+O=p$, (ii) $p-p=O$, (iii) $p+(q-p)=q$, (iv) $(p+P)-p=P$, (v) $(q+Q)-(p+P) = (q-p)+Q-P$.

Proof: Lemma 3.1, chapter X of [17] □

0.4.4 Theorem If C/k is a homogeneous space for E/k and p_0 is a fixed point of C, the map $\phi : \mathrm{Div}^0(C) \to E$ given by $\sum_i n_i p_i \mapsto \sum_i [n_i](p_i - p_0)$ defines an isomorphism of $\mathrm{Gal}(\overline{k}/k)$-modules $\phi : \mathrm{Pic}^0(C) \to E$ and ϕ does not depend on p_0. Furthermore, we have an exact sequence

$$0 \to \overline{k}^* \to \overline{k}(C)^* \stackrel{\mathrm{div}}{\to} \mathrm{Div}^0(C) \stackrel{\phi}{\to} E \to 0$$

Proof: See page 329, [17]. □

One important consequence of this is that $\mathrm{Pic}^0_k(C) \cong E(k)$, where $\mathrm{Div}^0_k(C)$ is the group of degree 0 divisors defined over k.

0.4.5 Observation Suppose that C is a torsor under E/k. Then we may regard E as the Jacobian of C. To see this, choose a fixed point $Q \in C$. We define a $\overline{k}$-isomorphism $\phi' : E \to C$ given by $\phi'(P) := Q+P$, and we note that $Q+P \in C$ and that ϕ' is a $\overline{k}$-isomorphism thanks to the properties of the torsor structure on C. Also, we define a $\overline{k}$-isomorphism $\phi : C \to \mathrm{Jac}(C)$ given

by $\phi(P) = [P - Q]$, and we note that $P - Q$ is a divisor of degree 0 and that it is a $\overline{k}$-isomorphism thanks to the previous theorem. Then the composition $\phi \circ \phi' : E \to \mathrm{Jac}(C)$ is a $\overline{k}$-isomorphism as well.

We consider another point of view regarding Jacobians.

0.4.6 Theorem Given a curve C of genus one defined over k, there exists an elliptic curve E and a birational map $\phi : C \to E$ such that for every $\sigma \in \mathrm{Gal}(\overline{k}/k)$ the map $\phi^\sigma \circ \phi^{-1} : E \to E$ takes the form $P \mapsto P + Q_\sigma$ for some $Q_\sigma \in E(k)$.

Proof: Section 20 of [6]. □

In the proof of this theorem, one ingredient is the following lemma which we mention because we use it later.

0.4.7 Lemma If $E_1 : y^2 = x^3 + A_1x + B_1$ and $E_2 : y^2 = x^3 + A_2x + B_2$ are two elliptic curves defined over k and $\phi : E_1 \to E_2$ is a birational map defined over k' with k'/k a field extension, then there exists $s \in k'$ such that $A_2 = s^4A_1$ and $B_2 = s^6B_1$. Furthermore, E_1 and E_2 have the same j-invariant.

Proof: Section 20 of [6]. □

0.4.8 Example Consider a plane cubic $C \subseteq \mathbb{P}^2$ given by $U(x, y, z) = ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz$. There are associated invariants $I(U), J(U)$ (see definition 2.2.2 in chapter 2), and if $U(x, y, z)$ is nonsingular, then the Jacobian of C is given by $E : y^2 = x^3 - 27I(U)x - 54J(U)$.

0.4.9 Example The following can be found in [1], theorem 3.1. Suppose that C is the complete nonsingular genus 1 curve over k given by the affine equation $C : y^2 = g(x, 1)$ where $g(x, z) = a_0x^4 + 4a_1x^3z + 6a_2x^2z^2 + 4a_3xz^3 + a_4z^4$ with coefficients in k. Consider the partial derivatives $g_x, g_z, g_{xz}, g_{xx}, g_{zz}$ and define $G(x, z) = \frac{1}{144}(g_{xz}^2 - g_{xx}g_{zz})$, and now consider the derivatives G_x, G_z to define $H(x, z) = \frac{1}{8}\det\begin{pmatrix} g_x & g_z \\ G_x & G_z \end{pmatrix}$. Define $I' := a_0a_4 - 4a_1a_3 + 3a_2^2$ and $J' := a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3$. The polynomials G and H together with the numbers I' and J' are related by the identity $H(x, z)^2 = 4G(x, z)^3 - I'G(x, z)g(x, z)^2 - J'g(x, z)^3$ in $k[x, z]$ and it can be shown that the Jacobian of C is given by $E : v^2 = 4u^3 - I'u - J'$ in $k[u, v]$. Together with the Jacobian E, we have a map $\phi : C \to E$ of degree 4 defined by

$$\phi(x, y, z) := \left(\frac{G(x, z)}{y^2z^2}, \frac{H(x, z)}{y^3z^3}\right)$$

Denote by ∞ the point $[0, 1, 0]$ on E and denote by D the divisor at infinity on C. Then the map ϕ defined before is the map defined by the linear system $|D|$.

Later, after reviewing some Galois cohomology we will identify the group $H^1(k,E)$ with the set of homogeneous spaces for the elliptic curve E/k up to k-equivalence. In the proof of this identification, one step is to realize every homogeneous space C for E/k as a twist of E/k.

0.4.10 Lemma For an elliptic curve E/k, every homogeneous space C/k of E/k is a twist of E/k.

Proof: We choose a fixed point $p_0 \in C$ and consider the morphism $\varphi : E \to C$ defined by $P \mapsto p_0 + P$. The inverse of this morphism is the morphism $\phi : C \to E$ defined by $p \mapsto p - p_0$. For any $p \in C$, lemma 0.4.3 (iii) implies

$$\varphi(\phi(p)) = \varphi(p - p_0) = p_0 + (p - p_0) = p$$

whereas for any $P \in E$, lemma 0.4.3 (iv) implies

$$\phi(\varphi(P)) = \phi(p_0 + P) = (p_0 + P) - p_0 = P$$

It follows that $\phi : C \to E$ is a $\overline{k}$-isomorphism. In particular, C is a twist of E. □

0.5 Galois cohomology and the parametrization of $H^1(k, \mathrm{Isom}(E))$ by homogeneous spaces of E/k

We will denote the group consisting of $\overline{k}$-isomorphisms of curves from E to itself by $\mathrm{Isom}(E)$. To avoid confusion, we will denote by $\mathrm{Aut}(E)$ the group consisting of $\overline{k}$-isomorphisms of curves from E to itself which also map O to O. We observe that $\mathrm{Isom}(E) \neq \mathrm{Aut}(E)$: if $P \in E$ and $P \neq O$, then the translation map τ_P belongs to $\mathrm{Isom}(E)$ but does not belong to $\mathrm{Aut}(E)$.

From now on, we will be interested only in $\mathrm{Isom}(E)$. Our goal is to identify the group $H^1(k, \mathrm{Isom}(E))$ with the set of homogeneous spaces of the elliptic curve E/k (up to k-equivalence). For this and also to define the n-Selmer group and the Tate-Shafarevich group, we recall some definitions from group cohomology.

Consider a finite group G acting on an abelian group M in a compatible way with the group structure $+$ of M. If we denote the action of $\sigma \in G$ on m by m^σ, then 'compatible' means that $m^1 = m$, $(m + m')^\sigma = m^\sigma + m'^\sigma$ and $(m^\sigma)^\tau = m^{\sigma\tau}$ for all $m, m' \in M$, $\alpha, \tau \in G$ and we say that M is a G-module.

Define $H^0(G,M) := \{m \in M : m^\sigma = m\}$. For $n \geq 1$, consider the group $C^n(G,M) := \{f : G^n \to M\}$ and consider the case $n = 1$. We can extract from $C^1(G,M)$ the subgroup $Z^1(G,M)$ defined by $\{\xi \in C^1(G,M) : \xi_{\sigma\tau} = \xi_\sigma + \xi_\tau^\sigma\} \subseteq C^1(G,M)$ where ξ_σ denotes the image of $\sigma \in G$ under the map $\xi \in C^1(G,M)$. Further, from $Z^1(G,M)$ we can extract the subgroup $B^1(G,M) := \{\xi \in C^1(G,M) : \xi_\sigma = m^\sigma - m \text{ for some fixed } m \in M\}$, and by following

the definitions we can verify that $B^1(G,M)$ is indeed a subgroup of $Z^1(G,M)$. The resulting quotient $Z^1(G,M)/B^1(G,M)$ is denoted by $H^1(G,M)$. It is also important to say that the groups $Z^1(G,M)$, $B^1(G,M)$ and $H^1(G,M)$ are abelian groups.

A slight variation of the previous paragraph is given by Galois cohomology, which we want to use from now on in this work. The procedure is almost the same as in the previous paragraph, except that our group G will be the profinite (instead of finite) group $G_k := \mathrm{Gal}(\overline{k}/k)$ for k a perfect field. We can view G_k as the profinite group given by the inverse limit of $\mathrm{Gal}(L/k)$ when L is running over the finite Galois extensions L/k. As a profinite group, G_k is given the profinite topology, and if M is a G_k-module, we should give M the discrete topology and we should require the action of G_k on M to be continuous, i.e. the map $M \times G_k \to M$ should be continuous.

For $n = 0$, we define $H^0(G_k, M) := M^{G_k}$ just like before. However, instead of taking $Z^1(G_k, M)$ we will take $Z^1_{\mathrm{cont}}(G_k, M)$ which are the continuous elements of $Z^1(G_k, M)$, and similarly we define $B^1_{\mathrm{cont}}(G_k, M)$ (although $B^1_{\mathrm{cont}}(G_k, M)$ is actually equal to $B^1(G_k, M)$ because M is discrete). The resulting quotient is denoted $H^1(G_k, M)$, or $H^1(k, M)$.

Also, we can consider homomorphisms between G-modules (respectively, G_k-modules) $f : M \to N$. This means that f satisfies the property $f(m^\sigma) = f(m)^\sigma$ for all $m \in M$, $\sigma \in G$ (respectively, $\sigma \in G_k$). We have the following proposition.

0.5.1 Proposition For $0 \to M \to N \to L \to 0$ an exact sequence of G-modules (respectively G_k-modules), there is an induced long exact sequence of the form

$$0 \to H^0(G,M) \to H^0(G,N) \to H^0(G,L) \xrightarrow{\delta} H^1(G,M) \to H^1(G,N) \to H^1(G,L)$$

(respectively,

$$0 \to H^0(G_k,M) \to H^0(G_k,N) \to H^0(G_k,L) \xrightarrow{\delta} H^1(G_k,M) \to H^1(G_k,N) \to H^1(G_k,L)$$

in the case of G_k-modules) and the connecting arrow δ is defined by mapping $l \in H^0(G,L) = L^G$ to the image in $H^1(G,M)$ of the 1-cocycle ξ defined by $\sigma \mapsto \xi_\sigma := n^\sigma - n$ with $n \in N$ such that it is mapped to l under the surjective map $N \to L$.

Proof: See [17], page 417. □

For an elliptic curve E/k, we apply Galois cohomology to the G_k-modules E and $E[n]$ with $n \geq 1$, where the action of G_k on each point $P = (x, y)$ is coordinate-wise. We recall that that an isogeny between elliptic curves is either constant or surjective. In particular, multiplication by n is surjective and we have the exact sequence of G_k-modules $0 \to E[n] \to E \to E \to 0$. Using the proposition and that $E^{G_k} = E(k)$ and $E[n]^{G_k} = E[n](k)$ will give the long exact sequence

$$0 \to H^0(k, E[n]) = E[n](k) \to H^0(k, E) = E(k) \to H^0(k, E) = E(k)$$

$$\xrightarrow{\delta} H^1(k, E[n]) \to H^1(k, E) \to H^1(k, E)$$

which in turn induces $0 \to E(k)/nE(k) \to H^1(k, E[n]) \to H^1(k, E)[n] \to 0$.

Now suppose that M is a $G_k = \mathrm{Gal}(\overline{k}/k)$-module and $n \geq 1$. Suppose that for each place v of k we have a $G_{k_v} := \mathrm{Gal}(\overline{k_v}/k_v)$-module M_v together with morphisms of G_{k_v}-modules $M \to M_v$. If we choose an embedding $\overline{k} \hookrightarrow \overline{k_v}$ and if H_v denotes the subgroup of G_{k_v} consisting of those automorphisms which fix $\overline{k}$ pointwise, then we can identify G_{k_v}/H_v with a subgroup of G_k. So suppose that the isomorphism of G_k-modules $\sigma : M \to M$ induced by $\sigma \in G_k$ extends (not necessarily uniquely) to an isomorphism of G_{k_v}-modules $M_v \to M_v$. Then we have a natural restriction map $H^n(G_k, M) \to H^n(G_{k_v}, M_v)$ which does not depend on the embedding $\overline{k} \hookrightarrow \overline{k_v}$ (because if i, i' are two such embeddings, then there is $\sigma \in G_k$ such that $i' = i\sigma$). All these restriction maps give rise to a natural map $H^1(G_k, M) \to \prod_v H^1(G_{k_v}, M_v)$ which maps an element $x \in H^1(G_k, M)$ to the element in the product whose v-th factor is the image of x under the corresponding restriction map $H^1(G_k, M) \to H^1(G_{k_v}, M_v)$. With this in mind, we define the n-Selmer group and the Tate-Shafarevich group of an elliptic curve E/k.

0.5.2 Definition The n-Selmer group $\mathrm{Sel}_n(E/k)$ of an elliptic curve E/k is

$$\mathrm{Sel}_n(E/k) := \ker(H^1(k, E[n]) \to \prod_v H^1(k_v, E(\overline{k_v})))$$

where the product is running over all the places v of k.

Similarly, the Tate-Shafarevich group $Ш(E/k)$ is

$$Ш(E/k) := \ker(H^1(k, E) \to \prod_v H^1(k_v, E(\overline{k_v})))$$

0.5.3 Proposition The n-Selmer and Tate-Shafarevich groups of an elliptic curve E/k are related by the following exact sequence

$$0 \to E(k)/nE(k) \to \mathrm{Sel}_n(E/k) \to Ш(E/k)[n] \to 0$$

Proof: See theorem 4.2, chapter X of [17]. □

Previously, to define Galois cohomology we considered the case when M is an abelian group. However, we can do something similar when M is no longer abelian. Let G be a finite group acting on M which is a group but not necessarily abelian. As before, we define $H^0(G, M) := M^G$. If we write the group law on M multiplicatively, then we define a 1-cocycle as a map $\xi : G \to M$ satisfying the cocycle relation $\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau$ for all $\sigma, \tau \in G$. Since M is not abelian, the set of 1-cocycles is not a group in general. However we can still define two cocycles ξ, ζ to be cohomologous if there exists $m \in M$ such that $m^\sigma \xi_\sigma = \zeta_\sigma m$ for all $\sigma \in M$,

which turns out to be an equivalence relation, and still define $H^1(G, M)$ as the set of 1-cocycles modulo this equivalence relation. This quotient is a pointed set with distinguished element, namely the equivalence class of the identity cocycle. To extent this discussion to Galois cohomology, we consider any group M (not necessarily abelian) and suppose that G_k acts discretely on M (i.e. the stabilizer of any element of M is a subgroup of G_k of finite index). As before, we define a 1-cocycle as a map $\xi : G_k \to M$ which is continuous (here G_k is given the profinite topology and M is given the discrete topology), and we define an equivalence relation on the set of 1-cocycles where two 1-cocycles ξ, ζ are cohomologous if there exists $m \in M$ such that $m^\sigma \xi_\sigma = \zeta_\sigma m$ for all $\sigma \in G_k$. Again, we define $H^0(G_k, M) = M^{G_k}$ and $H^1(G_k, M)$ is defined as the set of continuous 1-cocycles from G_k to M modulo the equivalence relation defined before.

Now, to prove our next theorem we should consider the following construction.

Consider an elliptic curve E/k and take any element in $H^1(k, \mathrm{Isom}(E))$. This element is given by a 1-cocycle $\xi : G_k \to \mathrm{Isom}(E)$. We want to construct a twist C/k arising from ξ. We do this in steps.

(1) Construct a field $\mathcal{F}$. This will be the function field of the twist C/k that we are looking for.

For this, take any field L isomorphic to $\overline{k}(E)$ and let $l : \overline{k}(E) \to L$ be an isomorphism of fields. We can view any element in L of the form $l(f)$ for a unique $f \in \overline{k}(E)$. Instead of looking at the natural action of G_k on $\overline{k}(E)$, we will use l to define a new action of G_k on L. Define $l(f)^\sigma := l(f^\sigma \xi_\sigma)$ where f is viewed as a function $E \to \mathbb{P}^1$ and $f^\sigma \xi_\sigma$ is viewed as a composition of functions. Equivalently, $f^\sigma \xi_\sigma$ is equal to $\xi_\sigma^*(f^\sigma)$. Now we define $\mathcal{F} := L^{G_k}$.

(2) Check that $\mathcal{F} \cap \overline{k} = k$ and $\overline{k}\mathcal{F} = L$.

For the first, note that we already have $k \subseteq \mathcal{F} \cap \overline{k}$, so we check the other containment. If $l(f) \in \mathcal{F} \cap \overline{k}$, then $l(f) \in \overline{k}$ and so $f \in \overline{k}$ because l is the identity on $\overline{k}$. Since $l(f) \in \mathcal{F}$, the definition of $\mathcal{F}$ implies that $l(f) = l(f)^\sigma = l(f^\sigma \xi_\sigma)$. We have $l(f^\sigma \xi_\sigma) = l(\xi_\sigma^*(f^\sigma))$, and note that ξ_σ^* will fix any element of $\overline{k}$, in particular ξ_σ^* will fix $f^\sigma \in \overline{k}$. So we obtain $l(\xi_\sigma^*(f^\sigma)) = l(f^\sigma)$. It follows that $l(f) = l(f^\sigma)$ for all $\sigma \in G_k$, but l is injective and so $f = f^\sigma$ for all $\sigma \in G_k$, which implies that $f \in k$.

For the second, recall that if V is a $\overline{k}$-vector space and G_k acts continuously on V and compatibly with its action on $\overline{k}$, then V has a basis consisting of G_k-invariant vectors (lemma 5.8.1, chapter II in [17]). Apply this to the $\overline{k}$-vector space L to obtain a basis consisting of G_k-invariant elements in L, i.e. a basis contained in $L^{G_k} = \mathcal{F}$. Therefore, $\overline{k}\mathcal{F} = L$.

(3) Find C/k.

Step (2) shows that $\mathcal{F}/k$ is a finitely generated extension of transcendence degree one such that $\mathcal{F} \cap \overline{k} = k$. And we know that there is an equivalence between the category of finitely generated field extensions K/k of transcendence degree one with $K \cap \overline{k} = k$ and the category of smooth curves over k (theorem

2.4 and remark 2.5 of chapter II in [17]). Then there exists a smooth curve C'/k and a k-morphism $\phi : E \to C'$ such that $\phi^*(k(C')) = \mathcal{F}$.

(4) Show that C/k is a twist of E/k.

From step (3) we know that $\mathcal{F} \cong k(C)$. This implies

$$\overline{k}(C) \cong \overline{k} \cdot k(C) \cong \overline{k} \cdot \mathcal{F} = L \cong \overline{k}(E)$$

which means that C/k is isomorphic to E/k over $\overline{k}$. Furthermore, the equivalence of categories implies that such a $\overline{k}$-isomorphism $\phi : C \to E$ satisfies that $\phi^* = l$. We conclude that C/k is a twist of E/k.

The main idea of the next theorem is useful later in Chapter 1. In this theorem we use nonabelian cohomology for the group $\mathrm{Isom}(E)$ because $\mathrm{Isom}(E)$ is not abelian, and also the previous construction.

0.5.4 Theorem Let E/k be an elliptic curve. Then there is a bijection between the $\mathrm{Twists}(E/k)$ and $H^1(k, \mathrm{Isom}(E))$.

Proof: Let $\{C/k\}$ be a k-equivalence class of a twist C/k of E/k. Take any isomorphism $\phi : C \to E$ defined over $\overline{k}$ and map $\{C/k\}$ to the image in $H^1(k, \mathrm{Isom}(E))$ of the 1-cocycle ξ defined by $\sigma \mapsto \xi_\sigma$ where $\xi_\sigma := \phi^\sigma \phi^{-1}$ for all $\sigma \in G_k$ (note that $\xi_\sigma \in \mathrm{Isom}(E)$). We note that ξ is a 1-cocycle because for all $\sigma, \tau \in G_k$ we have

$$\phi^{\sigma\tau}\phi^{-1} = \phi^{\sigma\tau}(\phi^\sigma)^{-1}\phi^\sigma\phi^{-1} = (\phi^\tau\phi^{-1})^\sigma(\phi^\sigma\phi^{-1})$$

Also, note that the image of ξ in $H^1(k, \mathrm{Isom}(E))$ does not depend on the chosen ϕ. To see this, suppose that $\phi' : C \to E$ is another $\overline{k}$-isomorphism. Then take $\alpha := \phi'\phi^{-1} \in \mathrm{Isom}(E)$ and and note that

$$\begin{aligned}
\alpha^\sigma(\phi^\sigma\phi^{-1}) &= (\phi'\phi^{-1})^\sigma(\phi^\sigma\phi^{-1}) \\
&= \phi'^\sigma\phi^{-1} \\
&= (\phi'^\sigma\phi'^{-1})(\phi'\phi^{-1}) \\
&= (\phi'^\sigma\phi'^{-1})\alpha
\end{aligned}$$

and so the 1-cocycles differ by the 1-coboundary induced by α (in the sense of non-abelian Galois cohomology). The next thing to do is to check that this map is well-defined, injective and surjective.

Well-defined: Suppose that $C/k, C'/k$ are two k-isomorphic twists of E/k. Let $\phi : C \to E$ be a $\overline{k}$-isomorphism and ξ the 1-cocycle defined by ϕ as before, and similarly let $\phi' : C' \to E$ be a $\overline{k}$-isomorphism and ξ' the 1-cocycle defined by ϕ'. We must verify that the 1-cocycles $\sigma \mapsto \xi_\sigma$ and $\sigma \mapsto \xi'_\sigma$ differ by a 1-coboundary in the sense of non-abelian Galois cohomology. By hypothesis, C, C' are k-isomorphic and so we choose a k-isomorphism $\theta : C \to C'$. We claim that the 1-coboundary is induced by $\alpha := \phi' \circ \theta \circ \phi^{-1} \in \mathrm{Isom}(E)$. Indeed, we have

$$\begin{aligned}\alpha^\sigma(\phi^\sigma\phi^{-1}) &= (\phi'\theta\phi^{-1})^\sigma(\phi^\sigma\phi^{-1}) \\ &= \phi'^\sigma\theta^\sigma\phi^{-1} \\ &= (\phi'^\sigma\phi'^{-1})(\phi'\theta\phi^{-1}) \\ &= (\phi'^\sigma\phi'^{-1})\alpha\end{aligned}$$

where we use that $\theta^\sigma = \theta$ since θ is defined over k. Therefore, $\phi^\sigma\phi^{-1}$ and $\phi'^\sigma\phi'^{-1}$ differ by a 1-coboundary.

Injective: Suppose that $\{C/k\}$ and $\{C'/k\}$ are two k-equivalence classes of twists of E/k which are mapped to the 1-cocycles $\sigma \mapsto \phi^\sigma\phi^{-1}$ and $\sigma \mapsto \phi'^\sigma\phi'^{-1}$ and suppose that they are cohomologous. Then we can choose a fixed $\alpha \in \mathrm{Isom}(E)$ such that $\alpha^\sigma(\phi'^\sigma\phi'^{-1}) = (\phi^\sigma\phi^{-1})\alpha$ for all $\sigma \in G_k$. We should find a k-isomorphism $\theta : C' \to C$ and so we naturally choose $\phi^{-1}\alpha\phi' : C' \to C$ which is a $\overline{k}$-isomorphism from C' to C. We note that θ is a k-isomorphism as well because

$$\begin{aligned}\theta^\sigma &= (\phi^{-1}\alpha\phi')^\sigma \\ &= (\phi^\sigma)^{-1}(\alpha^\sigma\phi'^\sigma) \\ &= (\phi^\sigma)^{-1}((\phi^\sigma\phi^{-1})\alpha\phi') \\ &= (\phi^\sigma)^{-1}\phi^\sigma(\phi^{-1}\alpha\phi') \\ &= \phi^{-1}\alpha\phi' \\ &= \theta\end{aligned}$$

where the third equality comes from $\alpha^\sigma(\phi'^\sigma\phi'^{-1}) = (\phi^\sigma\phi^{-1})\alpha$. So we obtain injectivity.

Surjective: Take any element in $H^1(k, \mathrm{Isom}(E))$ and let $\xi : G_k \to \mathrm{Isom}(E)$ be a 1-cocycle inducing this element. Let C/k be the twist of E/k from the construction before. In step (1) of that construction we consider an isomorphism of fields $l : \overline{k}(E) \to L$, and for any element in L of the form $l(f)$ for some $f \in \overline{k}(E)$ the action $l(f)^\sigma = l(f^\sigma\xi_\sigma)$. And in step (4), a $\overline{k}$-isomorphism $\phi : C \to E$ such that $\phi^* = l$. So, for all $f \in \overline{k}(E)$ and $\sigma \in G_k$ the equality

$$l(f)^\sigma = l(f^\sigma\xi_\sigma)$$

is equivalent to

$$\phi^*(f)^\sigma = \phi^*(f^\sigma\xi_\sigma)$$

which is equivalent to

$$(f \circ \phi)^\sigma = f^\sigma \circ \phi^\sigma = f^\sigma \circ \xi_\sigma \circ \phi$$

It follows that $\phi^\sigma = \xi_\sigma\phi$, or equivalently $\phi^\sigma\phi^{-1} = \xi_\sigma$. We conclude that $\{C/k\}$ is mapped to the image in $H^1(k, \mathrm{Isom}(E))$ of the 1-cocycle ξ. □

0.5.5 Observation The previous result holds for any smooth curve C/k, i.e. $\mathrm{Twist}(C/k) \cong H^1(k, \mathrm{Isom}(C))$.

Galois cohomology allows us to study Brauer-Severi varieties. For example, PGL_n is a group with a G_k-action given by mapping a pair (σ, ϕ), where $\sigma \in G_k$ and $\phi : \mathbb{P}_k^{n-1} \to \mathbb{P}_k^{n-1}$ is a $\overline{k}$-automorphism, to ϕ^σ which is also a $\overline{k}$-automorphism of $\mathbb{P}^{n-1}$. So we can consider $H^1(k, \mathrm{PGL}_n(\overline{k}))$ and we have the following parametrization.

0.5.6 Proposition The set of k-equivalence classes of twists of $\mathbb{P}_k^n$ is parametrized by $H^1(k, \mathrm{PGL}_n(\overline{k}))$.

Proof: See page 160, [16]. □

In other words, proposition 0.5.6 says that there is a bijection between $H^1(k, \mathrm{PGL}_n(\overline{k}))$ and the set of Brauer-Severi varieties of dimension $n-1$, up to k-isomorphism. In this setting, it is useful to know when a Brauer-Severi variety of dimension $n-1$ corresponds to the trivial element in $H^1(k, \mathrm{PGL}_n(\overline{k}))$.

0.5.7 Proposition: If X is a Brauer-Severi variety of dimension $n-1$, then its k-equivalence class $[X]$ corresponds to the identity element in $H^1(k, \mathrm{PGL}_n(\overline{k}))$ if and only if $X(k) \neq \emptyset$.

Proof: See proposition 4.8, [11]. □

Now we prove proposition 0.3.7.

Proof of proposition 0.3.7: By proposition 0.5.6, showing that a Brauer-Severi variety X over k of dimension $n-1$ satisfies the Hasse principle is equivalent to showing that the natural map $H^1(k, \mathrm{PGL}_n(\overline{k})) \to \prod_v H^1(k_v, \mathrm{PGL}_n(\overline{k_v}))$ is injective. So suppose that $[X]$ (the k-isomorphism class of X) belongs to $H^1(k, \mathrm{PGL}_n(\overline{k}))$ and suppose that its image in $\prod_v H^1(k_v, \mathrm{PGL}_n(\overline{k_v}))$ is trivial, i.e. $X(k_v) \neq \emptyset$ for all v. By theorem 0.3.8 (a) and propositions 0.5.6 and 0.3.5, it follows that we can identify $[X]$ with the equivalence class $[A]$ of some central simple k-algebra A of dimension n^2. But since $X(k_v) \neq \emptyset$ for all v then theorem 0.3.8 (b) implies that k_v is a splitting field for A. By theorem 0.3.3, it follows that k is a splitting field for A and so again theorem 0.3.8 (b) implies that $X(k) \neq \emptyset$, i.e. $[X]$ is the trivial element in $H^1(k, \mathrm{PGL}_n(\overline{k}))$ as desired. □

Now we will recall Hilbert's Theorem 90 and a theorem by Hasse. We are interested in these results because we will use them in Chapter 1 to construct a divisor.

0.5.8 Theorem (Hilbert 90): For any Galois extension L/k we have $H^1(\mathrm{Gal}(L/k), L^*) = 0$.

Proof: See corollary 10.4, chapter II in [13]. □

Now, in order to state Hasse's theorem we review the construction of the second cohomology group.

If G is a group and M is any G-module, we define a 2-cocycle as a function $f : G \times G \to M$ satisfying that for all $\sigma, \tau, \rho \in G$ we have $f(\sigma, \tau) + f(\sigma\tau, \rho) = \sigma f(\tau, \rho) + f(\sigma, \tau\rho)$. Also, we call 2-coboundaries to those functions $f : G \times G \to M$ satisfying that for each $\sigma \in G$ there exists $m_\sigma \in M$ such that for all $\sigma, \tau \in G$ we have $f(\sigma, \tau) = m_\sigma + \sigma m_\tau - m_{\sigma\tau}$. It can be shown that 2-coboundaries are 2-cocycles, and so we define $H^2(G, M) :=$ 2-cocycles modulo 2-coboundaries. So as we did before in the case $H^1(G, M)$, we will copy almost the same construction but now taking G a profinite group with the induced profinite topology, M with the discrete topology, and then we will take continuous 2-cocycles modulo continuous 2-coboundaries and this will be the second cohomology group in the sense of Galois cohomology.

0.5.9 Proposition Let k be a number field. Then $\mathrm{Br}(k) \cong H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^*)$.

Proof: See section 5, chapter X in [16]. □

Now we can state Hasse's theorem which is an equivalence of the previous example of the local-global principle.

0.5.10 Theorem (Hasse) Consider the natural map $H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^*) \to \prod_v H^2(\mathrm{Gal}(\overline{k_v}/k_v), \overline{k_v}^*)$. Then if $x \in H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^*)$ is mapped to 0 (i.e. x is trivial in each factor $H^2(\mathrm{Gal}(\overline{k_v}/k_v), \overline{k}^*)$) then x is the trivial element in $H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^*)$.

Proof: By the previous proposition, the statement is equivalent to proving that the map $\mathrm{Br}(k) \to \prod_v \mathrm{Br}(k_v)$ is injective. Let A be a central simple k-algebra such that its equivalence class $[A]$ belongs to the kernel of this map. For each place v, the image of $[A]$ in $\mathrm{Br}(k_v)$ is $[A \otimes_k k_v]$. Write $A \otimes_k k_v \cong M_n(D_v)$ for some (unique) division algebra D_v over k_v and some (unique) $n \geq 1$. The zero element in $\mathrm{Br}(k_v)$ is $[k_v] = [M_1(k_v)]$, so by hypothesis we have $[M_n(D_v)] = [M_1(k_v)]$, and by definition of equivalence in $\mathrm{Br}(k_v)$, it means that $D_v \cong k_v$ as k_v-algebras. So we can assume that $A \otimes_k k_v \cong M_n(k_v)$, and this holds for every place v. By theorem 0.3.3, it follows that $A \cong M_n(k)$ and we note that $[A] = [M_n(k)] = [M_1(k)] = [k]$ which is the zero element in $\mathrm{Br}(k)$. □

0.6 The obstruction map

For an elliptic curve E/k, the obstruction map will be a map $H^1(k, E[n]) \to \mathrm{Br}(k)$ which in general will not be a group isomorphism. There are several ways to define this map, however the most useful for us uses the parametrization of $H^1(k, E[n])$ as Brauer-Severi diagrams (which we will study in chapter 1).

0.6.1 Definition (i) Let E/k be an elliptic curve and $n \geq 2$ a fixed positive integer. Let $E \to \mathbb{P}^{n-1}$ be the morphism given by the linear system $|nO|$.

A Brauer-Severi diagram of dimension $n-1$ is a morphism $C \to S$ from a homogeneous space C for E/k to a Brauer-Severi variety S of dimension $n-1$, such that there exists a $\overline{k}$-isomorphism $\phi : C \to E$ respecting the torsor structure on C and E and a $\overline{k}$-isomorphism $\varphi : S \to \mathbb{P}^{n-1}$ in such a way that the following diagram commutes

$$\begin{array}{ccc} C & \longrightarrow & S \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} \\ E & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

We denote this Brauer-Severi diagram by $[C \to S]$.

(ii) We say that two Brauer-Severi diagrams $[C \to S]$ and $[C' \to S']$ of dimension $n-1$ are k-isomorphic if there exists a k-isomorphism $\phi : C \to C'$ respecting the torsor structure on C and C' and a k-isomorphism $\varphi : S \to S'$ such that the following diagram commutes

$$\begin{array}{ccc} C & \longrightarrow & S \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} \\ C' & \longrightarrow & S' \end{array}$$

We will introduce some notation regarding the previous definition. For this, note that if we take $\phi := \mathrm{Id}_E$ and $\varphi := \mathrm{Id}_{\mathbb{P}^{n-1}}$ in definition 0.6.1 (i), then $[E \to \mathbb{P}^{n-1}]$ is a Brauer-Severi diagram of dimension $n-1$. Furthermore, $[E \to \mathbb{P}^{n-1}]$ is k-isomorphic to itself in the sense of definition 0.6.1 (ii). Now consider the set of pairs (ϕ, φ) where $\phi : E \to E$ and $\varphi : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ are k-isomorphisms such that $[E \to \mathbb{P}^{n-1}]$ becomes k-isomorphic to itself (for example, $(\mathrm{Id}_E, \mathrm{Id}_{\mathbb{P}^{n-1}})$ belongs to this set). Then this set becomes a group if we define the operation $(\phi, \varphi) \cdot (\phi', \varphi') = (\phi' \circ \phi, \varphi' \circ \varphi)$, where the identity element is $(\mathrm{Id}_E, \mathrm{Id}_{\mathbb{P}^{n-1}})$ and the inverse of (ϕ, φ) is $(\phi^{-1}, \varphi^{-1})$. This group is denoted by $\mathrm{Aut}([E \to \mathbb{P}^{n-1}])$.

Let L/k be a field extension. There is a subgroup of $\mathrm{Aut}([E \to \mathbb{P}^{n-1}])$ consisting of those pairs $(\phi, \varphi) \in \mathrm{Aut}([E \to \mathbb{P}^{n-1}])$ such that ϕ and φ are L-isomorphisms. We denote this subgroup by $\mathrm{Aut}([E \to \mathbb{P}^{n-1}])(L)$.

Definition 0.6.1 allows us to parametrize $H^1(k, E[n])$:

0.6.2 Proposition If E/k is an elliptic curve, the group $H^1(k, E[n])$ is parametrized, up to k-isomorphism, by the Brauer-Severi diagrams $[C \to S]$ of dimension $n-1$.

We will sketch a proof of this proposition in Chapter 1. Meanwhile, this proposition is useful to define the obstruction map:

0.6.3 Definition Let E/k be an elliptic curve. The obstruction map $\mathrm{Ob} : H^1(k, E[n]) \to \mathrm{Br}(k)$ is defined by $[C \to S] \mapsto [S]$ where $[S]$ is the k-isomorphism class of S.

Note that in this definition we are using proposition 0.3.5 to view S as an element of $\mathrm{Br}(k)$.

We will consider the kernel of the obstruction map in chapter 2. Here we note that $\ker(\mathrm{Ob})$ is not necessarily a group either since Ob is not always a group homomorphism.

Chapter 1 - Some parametrizations for $H^1(k, E[n])$

In this chapter we study a few parametrizations for the group $H^1(k, E[n])$. To achieve this, we will verify in theorem 1.1.5 the bijection between $H^1(k, E)$ and the set of homogeneous spaces of E/k (up to k-equivalence).

1.1 The bijection $\mathrm{WC}(E/k) \leftrightarrow H^1(k, E)$

We require a lemma, an observation and another lemma:

1.1.1 Lemma: Suppose that C/k and C'/k are equivalent homogeneous spaces of E/k by some isomorphism $\theta : C \to C'$ over k, and denote $+, -$ and $+', -'$ the operations on C and C', respectively. Then $P - Q = \theta(P) -' \theta(Q)$ $\forall$ $P, Q \in C$.

Proof: We know that θ satisfies $\theta(R+S) = \theta(R) +' S$ for all $R \in C$, $S \in E$. So we have

$$\begin{aligned} \theta(P) -' \theta(Q) &= ([\theta(P) +' (Q - P)] -' \theta(Q)) -' (Q - P) \\ &= (\theta(P + (Q - P)) -' \theta(Q)) - (Q - P) \\ &= P - Q \end{aligned}$$

□

1.1.2 Observation For any elliptic curve E/k we have that $H^1(k, E)$ and $H^1(k, E[n])$ are subgroups of $H^1(k, \mathrm{Isom}(E))$, where we are viewing E and $E[n]$ as subgroups of $\mathrm{Isom}(E)$ by means of the map $P \mapsto \tau_P$, τ_P the translation by P.

We saw before that any homogeneous space of E/k is a twist of E/k. However, the converse is not necessarily true. The following lemma describes some conditions to have the converse. We will use this lemma to prove surjectivity in theorem 1.1.5.

1.1.3 Lemma Consider any element $x \in H^1(k, E)$ given by a 1-cocycle $\xi : G_k \to E$ and define $\xi_\sigma := \xi(\sigma) \in E$ for all $\sigma \in G_k$. Let y be the image in $H^1(k, E)$ of the 1-cocycle $-\xi : G_k \to E$ defined as $\sigma \mapsto -\xi_\sigma$, and view x and y as elements of $H^1(k, \mathrm{Isom}(E))$ as in observation 1.1.2. If $\{C/k\}$ is the element in $\mathrm{Twist}(E/k)$ corresponding to y under the bijection of theorem 0.5.4, then C/k has also a structure of homogeneous space of E/k.

Proof: Recall that the bijection between $\mathrm{Twist}(E/k)$ and $H^1(k, \mathrm{Isom}(E))$ is given by sending a twist C/k induced by some $\overline{k}$-isomorphism $\phi : C \to E$ to the 1-cocycle $\sigma \mapsto \phi^\sigma \phi^{-1}$. Since we are viewing E as a subgroup of $\mathrm{Isom}(E)$

by means of the translation maps τ_P with $P \in E$, it follows that ϕ satisfies $\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma}$ for all $\sigma \in G_k$. Then C/k will have the following homogeneous space structure: define $\mu : C \times E \to C$ by the map $(p, P) \mapsto \phi^{-1}(\phi(p) + P)$. We verify that it is simply transitive and defined over k.

Simply transitive: if $p, q \in C$, then the point $P \in E$ such that $\mu(p, P) = q$ is given by $P := \phi(q) - \phi(p)$ because $\phi^{-1}(\phi(p) + P) = q$, and the uniqueness of P comes from the fact that ϕ is an isomorphism.

Defined over k: We use twice the equality $\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma}$, or equivalently $\phi^\sigma = \tau_{-\xi_\sigma}\phi$. We have

$$\begin{aligned}
\mu(p,P)^\sigma &= (\phi^{-1})^\sigma(\phi(p)^\sigma + P^\sigma) \\
&= (\phi^{-1})^\sigma(\phi^\sigma(p^\sigma) + P^\sigma) \\
&= (\phi^{-1})^\sigma(\phi(p^\sigma) + P^\sigma - \xi_\sigma) \\
&= \phi^{-1}((\phi(p^\sigma) + P^\sigma - \xi_\sigma) + \xi_\sigma) \\
&= \mu(p^\sigma, P^\sigma)
\end{aligned}$$

□

Next, we define the Weil-Chatelet group of an elliptic curve E/k.

1.1.4 Definition Denote by $\mathrm{WC}(E/k)$ the set of k-equivalence classes of homogeneous spaces of E/k, where we define k-equivalence between two homogeneous spaces of E/k as in definition 0.4.1.

1.1.5 Theorem There is a bijection $\mathrm{WC}(E/k) \to H^1(k, E)$ defined by $\{C/k\} \mapsto \{\sigma \mapsto p_0^\sigma - p_0\}$ where p_0 is any fixed point of C, $\{C/k\}$ is the equivalence class of C, and $\{\sigma \mapsto p_0^\sigma - p_0\}$ is the element in $H^1(k, E)$ induced by such a 1-cocycle.

Proof: Well-defined: If $\theta : C \to C'$ defines two equivalent homogeneous spaces C/k and C'/k and if $p_0 \in C$, $p_0' \in C'$, then the idea is that the 1-cocycles $\sigma \mapsto p_0^\sigma - p_0$ and $\sigma \mapsto {p_0'}^\sigma -' p_0'$ differ by the coboundary $\sigma \mapsto (\theta(p_0) - p_0')^\sigma - (\theta(p_0) - p_0')$: thanks to lemma 1.1.1 we have $p_0^\sigma - p_0 = \theta(p_0^\sigma) -' \theta(p_0)$. We have

$$\begin{aligned}
p_0^\sigma - p_0 &= \theta(p_0^\sigma) -' \theta(p_0) \\
&= \theta(p_0^\sigma) -' \theta(p_0) + (p_0' -' p_0') + ({p_0'}^\sigma -' {p_0'}^\sigma) \\
&= ({p_0'}^\sigma -' p_0') + [(\theta(p_0) -' p_0')^\sigma - (\theta(p_0) -' p_0')]
\end{aligned}$$

where we are also using that $\theta(p_0)^\sigma = \theta(p_0^\sigma)$ because θ is defined over k. This implies that our 1-cocycles are cohomologous.

Injective: Suppose that $\{C/k\} \mapsto \{\sigma \mapsto p_0^\sigma - p_0\}$, $\{C'/k\} \mapsto \{\sigma \mapsto {p_0'}^\sigma - p_0'\}$ are such that $\{\sigma \mapsto p_0^\sigma - p_0\}$ and $\{\sigma \mapsto {p_0'}^\sigma - p_0'\}$ are equal in $H^1(k, E)$. This means that we can find $P_0 \in E$ such that the 1-coboundary $\sigma \mapsto P_0^\sigma - P_0$ satisfies $p_0^\sigma - p_0 = ({p_0'}^\sigma - p_0') + (P_0^\sigma - P_0)$. We will define $\theta : C \to C'$ as $p \mapsto p_0' +' (p - p_0) +' P_0$ and we will check that $\theta(p)^\sigma = \theta(p^\sigma)$ for all $\sigma \in G_k$. Since $({p_0'}^\sigma -' p_0') + (P_0^\sigma - P_0) - (p_0^\sigma - p_0) = O$, we obtain

$$\begin{aligned}\theta(p)^\sigma &= {p'_0}^\sigma + (p^\sigma - p_0^\sigma) + P_0^\sigma \\ &= {p'_0}^\sigma + (p^\sigma - p_0^\sigma) + P_0^\sigma + (p_0 - p_0) + (p'_0 - p'_0) + (P_0 - P_0) \\ &= [p'_0 + (p^\sigma - p_0) + P_0] + [({p'_0}^\sigma - p'_0) + (P_0^\sigma - P_0) - (p_0^\sigma - p_0)] \\ &= [p'_0 + (p^\sigma - p_0) + P_0] + O \\ &= \theta(p^\sigma)\end{aligned}$$

and so θ is defined over k. Plus, from the definition we have that θ respects the action of E on C, C' and it's an isomorphism over $\overline{k}$.

Surjective: If $x \in H^1(k, E)$ is given by some 1-cocycle ξ then observation 1.1.2 allows us to view ξ as an element of $H^1(k, \mathrm{Isom}(E))$, and lemma 1.1.3 gives us a homogeneous space C/k of E/k coming from a $\overline{k}$-isomorphism $\phi : C \to E$ such that $\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma}$. We claim that the equivalence class of the homogeneous space C/k is mapped to x. Indeed, note that our map is defined by sending $\{C/k\}$ to $\{\sigma \mapsto p_0^\sigma - p_0\}$ for any fixed $p_0 \in C$. In particular, we can choose $p_0 := \phi^{-1}(O)$. We have

$$\begin{aligned}p_0^\sigma - p_0 &= \phi^{-1}(O)^\sigma - \phi^{-1}(O) \\ &= (\phi^{-1})^\sigma(O^\sigma) - \phi^{-1}(O) \\ &= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) \\ &= (\phi^{-1}\tau_{-\xi_\sigma}^{-1})(O) - \phi^{-1}(O) \\ &= \phi^{-1}(O + \xi_\sigma) - \phi^{-1}(O) \\ &= \phi^{-1}(\xi_\sigma) - \phi^{-1}(O)\end{aligned}$$

where we are using that $\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma}$. If we can prove that $\xi_\sigma = \phi^{-1}(\xi_\sigma) - \phi^{-1}(O)$ then we would be done: in that case we would have $p_0^\sigma - p_0 = \phi^{-1}(\xi_\sigma) - \phi^{-1}(O) = \xi_\sigma$ which would imply that the 1-cocycles $\sigma \mapsto p_0^\sigma - p_0$ and $\sigma \mapsto \xi_\sigma$ are equal (in particular cohomologous). Indeed, the equality $\xi_\sigma = \phi^{-1}(\xi_\sigma) - \phi^{-1}(O)$ holds because $\phi^{-1}(O) + ((\phi^{-1})^\sigma(O) - \phi^{-1}(O)) = (\phi^{-1})^\sigma(O)$, which means that $\phi^{-1}(\phi(\phi^{-1}(O)) + [(\phi^{-1})^\sigma(O) - \phi^{-1}(O)]) = (\phi^{-1})^\sigma(O)$. Using that $(\phi^{-1})^\sigma = (\phi^\sigma)^{-1}$ and that $\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma}$ together with the last equality, it follows that $\phi^{-1}((\phi^\sigma)^{-1}(O) - \phi^{-1}(O)) = (\phi^{-1}\tau_{-\xi_\sigma}^{-1})(O)$. Applying ϕ to both sides of the last equality and using again that $\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma}$, we obtain $(\phi^{-1}\tau_{-\xi_\sigma}^{-1})(O) - \phi^{-1}(O) = \xi_\sigma$, in other words, $\phi^{-1}(\xi_\sigma) - \phi^{-1}(O) = \xi_\sigma$, as desired. □

In the previous bijection, it's important to know when an element of $\mathrm{WC}(E/K)$ corresponds to the identity in $H^1(k, E)$.

1.1.6 Corollary If C/k is a homogeneous space for E/k, then its equivalence class $\{C\} \in \mathrm{WC}(E/k)$ corresponds to the zero element in $H^1(k, E)$ if and only if $C(k) \neq \emptyset$.

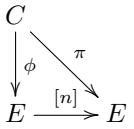
Proof: Suppose that $C(k) \neq \emptyset$ and choose a point $p_0 \in C(k)$. By theorem 1.1.5, we know that $\{C/k\}$ is mapped to the image in $H^1(k, E)$ of the 1-cocycle

$\sigma \mapsto p_0^\sigma - p_0$. But $p_0^\sigma = p_0$, so the image in $H^1(k,E)$ of our 1-cocycle is the zero element. Conversely, suppose that $\{C/k\}$ corresponds to the zero element in $H^1(k,E)$ and choose any $p_0 \in C$. Using the map given in theorem 1.1.5, we obtain that the image in $H^1(k,E)$ of the 1-cocycle $\sigma \mapsto p_0^\sigma - p_0$ is equal to the image in $H^1(k,E)$ of the trivial 1-cocycle $\sigma \mapsto O$. This means that we can find $P_0 \in E$ such that $p_0^\sigma - p_0 = O + (P_0^\sigma - P_0)$, which in turn implies that $p_0^\sigma - P_0^\sigma = p_0 - P_0$. It follows that the point $p_0 - P_0 \in C$ belongs to $C(k)$. $\square$

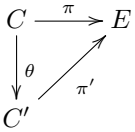
1.2 $H^1(k, E[n])$ in terms of n-coverings

We need the definition of a n-covering of E/k.

1.2.1 Definition (i) An n-covering of E/k is a pair (C,π) given by a smooth projective curve C and a nonconstant morphism $\pi : C \to E$ over k such that (C,π) is a twist of the pair $(E,[n])$ given by the multiplication by n, $[n] : E \to E$. This means that there exists a $\overline{k}$-isomorphism $\phi : C \to E$ such that the following diagram is commutative



(ii) We say that two n-coverings (C,π) and (C',π') are k-isomorphic if there is an k-isomorphism $\theta : C \to C'$ such that the following diagram commutes



1.2.2 Remark If we have an n-covering (C,π) of E/k with $\phi : C \to E$ the induced $\overline{k}$-isomorphism, then we can give C a structure of homogeneous space of E/k by taking the action $C \times E \to C$ defined by $(P,Q) \mapsto \phi^{-1}(\phi(P)+Q)$ and this action does not depend on ϕ. See page 128 in [7].

In particular, the set of n-coverings of E/k can be mapped to the set of homogeneous spaces of E/k via the map $H^1(k,E[n]) \to H^1(k,E)$ arising from the exact sequence $0 \to E[n] \to E \to E \to 0$. The map $H^1(k,E[n]) \to H^1(k,E)$ is not injective, which geometrically means that we can give different n-covering structures to the same homogeneous space.

1.2.3 Remark If (C,π) is an n-covering of E/k, then we can assume that E is the Jacobian of C. This follows from remark 1.2.2 and observation 0.4.5.

Furthermore, if we take a $\overline{k}$-isomorphism $\phi : C \to E$ coming from the definition of the n-covering (C, π), then we can assume that $\phi : C \to E \cong \mathrm{Jac}(C)$ is defined by $P \mapsto [P - Q]$ for some fixed $Q \in C$. This follows again from observation 0.4.5.

1.2.4 Example A trivial example of the above definition is taking $C = E$ and $\pi := [n] \circ \phi$ where $\phi := \mathrm{Id}_E$. This is called the trivial n-covering of E/k and denoted by $(E, [n])$.

1.2.5 Example Consider the curve $C : y^2 = g(x)$ where $g(x) = ax^4 + bx^3 + cx^2 + dx + e$ with $a, b, c, d, e \in k$. Assume that $g(x)$ has discriminant not equal to zero, so that C is nonsingular of genus 1. Then we can take the elliptic curve E defined by $E := \mathrm{Pic}^0(C)$, the Jacobian of E. Define $\pi : C \to E$ by $\pi(P) := 2[P - Q_0]$, where $Q_0 = (\xi, 0)$ with ξ any root of $g(x)$. We know that for any fixed point $Q \in C$ the map $\phi : C \to E$ given by $\phi(P) = [P - Q]$ yields an isomorphism over $\overline{k}$. This implies that when we choose $Q := Q_0$, we will have $[2] \circ \phi = \pi$ and $\phi(P) := [P - Q_0]$ will be a $\overline{k}$-isomorphism. We should check that π is defined over k. For this, note that showing $\pi^\sigma = \pi$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$ is equivalent to showing $2[P - (\xi, 0)^\sigma] = 2[P - (\xi, 0)]$, i.e. that $2(\xi^\sigma, 0) - 2(\xi, 0)$ is a principal divisor and this is true because we can take the rational function $\frac{x - \xi^\sigma}{x - \xi} \in \overline{k}(x, y)$ and compute $\mathrm{div}(\frac{x - \xi^\sigma}{x - \xi}) = 2(\xi^\sigma, 0) - 2(\xi, 0)$.

In the previous definition, we note that for $n \geq 2$, the $\overline{k}$-isomorphism ϕ might not be unique.

Now the idea is to follow the proof of theorem 1.1.5, but this time restricting to those homogeneous spaces with a structure of n-covering (n-coverings of E/k are homogeneous spaces of E/k by remark 1.2.2). For this purpose, the following lemma is useful.

1.2.6 Lemma Suppose that (C, π) and (C', π') are two k-equivalent n-coverings of E/k. Choose $\theta : C \to C'$ so that $\pi'\theta = \pi$ and choose $\overline{k}$-isomorphisms $\phi : C \to E$ and $\phi' : C' \to E$ such that the corresponding diagrams commute

$$\begin{array}{ccc} C & & \\ \downarrow{\scriptstyle \phi} & \searrow^{\pi} & \\ E & \xrightarrow{[n]} & E \end{array} \qquad \begin{array}{ccc} C' & & \\ \downarrow{\scriptstyle \phi'} & \searrow^{\pi'} & \\ E & \xrightarrow{[n]} & E \end{array}$$

Then there exists $P \in E[n]$ such that the following diagram is commutative

$$\begin{array}{ccc} C & \xrightarrow{\theta} & C' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ E & \xrightarrow{\tau_P} & E \end{array}$$

Proof: We observe that $\phi : C \to E$ composed with $[n] : E \to E$ is equal to $\phi'\theta : C \to E$ composed with $[n] : E \to E$. This is true because on the one hand, we have $[n]\phi = \pi$ by hypothesis, and on the other hand we have $[n](\phi'\theta) = ([n]\phi')\theta = \pi'\theta$ since $[n]\phi' = \pi'$. But $\pi = \pi'\theta$ by hypothesis as well.

The equality $[n](\phi) = [n](\phi'\theta)$ implies $[n](\phi - \phi'\theta) = 0$. We note that we can view $\phi - \phi'\theta$ as a morphism $C \to E[n]$ over $\overline{k}$, and this morphism has image contained in $E[n]$. However, $E[n]$ is discrete and this implies that the image should be equal to some fixed point $P \in E[n]$. It follows that $\phi'\theta = \tau_P\phi$ and we get the result. □

1.2.7 Observation Given an elliptic curve E/k, consider the set of triples (C, ϕ, π) consisting of a smooth curve C, a $\overline{k}$-isomorphism $\phi : C \to E$ and a k-morphism $C \to E$ such that the following diagram commutes

$$\begin{array}{ccc} C & & \\ \downarrow{\scriptstyle \phi} & \searrow{\scriptstyle \pi} & \\ E & \xrightarrow{[n]} & E \end{array}$$

Also, define two triples (C, ϕ, π) and (C', ϕ', π') to be equivalent if there exists $P \in E[n]$ and a k-isomorphism $\theta : C \to C'$ such that the following diagram commutes

$$\begin{array}{ccc} C & \xrightarrow{\theta} & C' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ E & \xrightarrow{\tau_P} & E \end{array}$$

Then there is a bijection between the set of equivalence classes of triples (C, ϕ, π) and the set of equivalence classes of n-coverings of E/k. Indeed, consider the map $(C, \phi, \pi) \mapsto (C, \pi)$. It is well-defined: if (C, ϕ, π) and (C', ϕ', π') are equivalent, then for some $P \in E[n]$ we have $\phi'\theta = \tau_P\phi$ and so $[n]\phi'\theta = [n]\tau_P\phi = [n]\phi$, where the last equality holds because $P \in E[n]$. So $\pi\theta = [n]\phi'\theta = [n]\phi = \pi$ and we conclude that (C, π) and (C', π') are equivalent. Injective: if (C, ϕ, π) and (C, ϕ, π) are mapped to equivalent pairs (C, π), (C', π'), then let θ be a k-isomorphism such that $\pi'\theta = \pi$. Then we can apply the previous lemma to obtain $Q \in E[n]$ such that $\phi'\theta = \tau_Q\phi$, which implies that (C, ϕ, π) and (C', ϕ', π') are equivalent. Surjective: if we have a n-covering (C, π), then by definition we can find a $\overline{k}$-isomorphism $\phi : C \to E$ such that $[n]\phi = \pi$, so the triple (C, ϕ, π) is mapped to (C, π).

We recall that we have a bijective map from $\mathrm{WC}(E/k)$ to $H^1(k, E)$ which was obtained by sending the k-equivalence class of a homogeneous space C/k to the image of the 1-cocycle $\sigma \mapsto p_0^\sigma - p_0$ in $H^1(k, E)$ where p_0 is any point of C. Also, we recall that in order to prove that this map is bijective, we made

use of the bijection $\mathrm{Twist}(E/k) \to H^1(k, \mathrm{Isom}(E))$ where the bijection is given by mapping a twist $\varphi : C \to E$ to the image of the 1-cocycle $\sigma \mapsto \varphi^\sigma \varphi^{-1}$ in $H^1(k, \mathrm{Isom}(E))$. We will follow a similar procedure to prove that there is a bijection between the set of k-equivalence classes of n-coverings of E/k and $H^1(k, E[n])$:

1.2.8 Theorem Let (C, π) be a n-covering of E/k, and denote by $\{C/k\}$ its equivalence class. Fix a point $P \in \ker(\pi)$ and let $\{\sigma \mapsto P^\sigma - P\}$ be the image in $H^1(k, E[n])$ of the 1-cocycle $\sigma \mapsto P^\sigma - P$. Then there is a bijection between the set of k-equivalence classes of n-coverings for E/k and $H^1(k, E[n])$ given by the map $\{(C, \pi)\} \mapsto \{\sigma \mapsto P^\sigma - P\}$.

Proof: Let $\phi : C \to E$ be a $\overline{k}$-isomorphism such that $\pi = [n]\phi$. First we check that $P^\sigma - P \in E[n]$ and that $\sigma \mapsto P^\sigma - P$ is a 1-cocycle. Recall that (C, π) has a structure of homogeneous space for E/k by remark 1.2.2. By definition of this structure and by definition of the symbol $-$, we know that $P^\sigma - P$ is the unique point in E satisfying $P + (P^\sigma - P) = P^\sigma$, i.e. $\phi^{-1}(\phi(P) + (P^\sigma - P)) = P^\sigma$ which implies $P^\sigma - P = \phi(P^\sigma) - \phi(P)$. Then

$$\begin{aligned} [n](P^\sigma - P) &= [n](\phi(P^\sigma) - \phi(P)) \\ &= ([n]\phi)(P^\sigma) - ([n]\phi)(P) \\ &= \pi(P)^\sigma - \pi(P) \\ &= O \end{aligned}$$

where we use that $P \in \ker(\pi)$ and that π is defined over k, which implies that $P^\sigma - P \in E[n]$. Now, $\sigma \mapsto P^\sigma - P$ is a 1-cocycle because

$$\begin{aligned} P^{\sigma\tau} - P &= P^{\sigma\tau} - P^\tau + P^\tau - P \\ &= (P^\sigma - P)^\tau + (P^\tau - P) \end{aligned}$$

Well-defined: Suppose $(C, \pi), (C', \pi')$ are k-equivalent n-coverings and fix $P_0 \in \ker(\pi)$, $P_0' \in \ker(\pi')$. First we will show that this implies that (C, π) and (C', π') are k-equivalent as homogeneous spaces.

Take $\theta : C \to C'$ a k-isomorphism which makes (C, π) and (C', π') k-equivalent as n-coverings, i.e. $\pi'\theta = \pi$. By lemma 1.2.6 there exists $T \in E[n]$ such that the following diagram commutes

$$\begin{array}{ccc} C & \xrightarrow{\theta} & C' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ E & \xrightarrow{\tau_T} & E \end{array}$$

Since all the morphisms in this diagram are isomorphisms (in particular bijective), we obtain $\theta\phi^{-1} = \phi'^{-1}\tau_T$. Therefore, for any $p \in C$ and any $P \in E$ we have

$$\begin{aligned}\theta(\phi^{-1}(\phi(p)+P)) &= \phi'^{-1}(\tau_T(\phi(p)+P)) \\ &= \phi'^{-1}((\phi(p)+P)+T) \\ &= \phi'^{-1}(\phi'(\theta(p))+P)\end{aligned}$$

where in the last equality we use that E is abelian and also the equality $\phi'\theta = \tau_P\phi$ (because the diagram is commutative). So $\theta(\phi^{-1}(\phi(p)+P)) = \phi'^{-1}(\phi'(\theta(p))+P)$ which is precisely the definition of $\theta(p+P) = \theta(p) +' P$, i.e. θ respects the torsor structure of C and C'. As θ is already a k-isomorphism, it follows that (C,π) and (C',π') as k-equivalent as homogeneous spaces.

Now, to show that $\sigma \mapsto P_0^\sigma - P_0$ and $\sigma \mapsto P_0'^\sigma - P_0'$ are cohomologus, we will follow the same procedure as in the proof of theorem 1.1.5. Namely, we claim that the previous two cocycles differ by the 1-coboundary

$$\sigma \mapsto (\theta(P_0) -' P_0')^\sigma - (\theta(P_0) -' P_0')$$

where we note that $\theta(P_0) -' P_0' \in E[n]$. Indeed, this happens because $P_0' +' (\theta(P_0) -' P_0') = \theta(P_0)$, which implies $\phi'^{-1}(\phi'(P_0') + (\theta(P_0) -' P_0')) = \theta(P_0)$, or in other words, $\theta(P_0) -' P_0' = \phi'(\theta(P_0)) - \phi'(P_0')$. Composing with $[n]$ yields

$$\begin{aligned}[n](\theta(P_0) -' P_0') &= [n](\phi'(\theta(P_0)) - \phi'(P_0')) \\ &= ([n]\phi')(\theta(P_0)) - ([n]\phi')(P_0') \\ &= (\pi'\theta)(P_0) - \pi'(P_0') \\ &= \pi(P_0) - \pi'(P_0') \\ &= O - O \\ &= O\end{aligned}$$

It follows that $\theta(P_0) -' P_0' \in E[n]$ and the map

$$\sigma \mapsto (\theta(P_0) -' P_0')^\sigma - (\theta(P_0) -' P_0')$$

is a 1-coboundary. Finally, the fact that (C,π) and (C',π') are k-equivalent as homogeneous spaces together with lemma 1.1.1 and the fact that θ is defined over k imply

$$\begin{aligned}P_0^\sigma - P_0 &= \theta(P_0^\sigma) -' \theta(P_0) \\ &= \theta(P_0)^\sigma -' \theta(P_0) \\ &= \theta(P_0)^\sigma -' \theta(P_0) + (P_0'^\sigma -' P_0'^\sigma) + (P_0' -' P_0') \\ &= (P_0'^\sigma -' P_0') + ((\theta(P_0) -' P_0')^\sigma - (\theta(P_0) -' P_0'))\end{aligned}$$

and we conclude that our two 1-cocycles are cohomogous.

Injective: Suppose that we have two n-coverings (C,π), (C',π') and two fixed points $P \in \ker(\pi)$, $P' \in \ker(\pi')$, and suppose that there exists $T \in E[n]$ such that $P^\sigma - P = (P'^\sigma -' P') + (T^\sigma - T)$ for all $\sigma \in G_k$. Define $Q' := P' +' (Q - P) +' T \in C'$ and define the map $\theta : C \to C'$ as $Q \mapsto Q'$. We note that θ is a $\overline{k}$-isomorphism. Also, we have

$$\begin{aligned}
\theta(Q)^\sigma &= P'^\sigma +' (Q^\sigma - P^\sigma) +' T^\sigma \\
&= (P'^\sigma +' (Q^\sigma - P^\sigma) +' T^\sigma) + O \\
&= (P'^\sigma +' (Q^\sigma - P^\sigma) +' T^\sigma) + (P' -' P' + P - P + T - T) \\
&= (P' +' (Q^\sigma - P) +' T) + [(P'^\sigma -' P') + (T^\sigma - T) - (P^\sigma - P)] \\
&= (P' +' (Q^\sigma - P) +' T) + O \\
&= P' +' (Q^\sigma - P) +' T \\
&= \theta(Q^\sigma)
\end{aligned}$$

and so θ is defined over k. It remains to verify $\pi'\theta = \pi$. For any $Q \in C$ we have

$$\begin{aligned}
(\pi')(\theta(Q)) &= ([n]\phi')(\theta(Q)) \\
&= ([n]\phi')(P' +' ((Q - P) + T)) \\
&= ([n]\phi')\phi'^{-1}(\phi'(P') + (Q - P) + T) \\
&= [n](\phi'(P') + (Q - P) + T) \\
&= \pi'(P') + [n](Q - P) + [n]T \\
&= [n](Q - P) \\
&= [n](\phi(Q) - \phi(P)) \\
&= \pi(Q) - \pi(P) \\
&= \pi(Q) - O \\
&= \pi(Q)
\end{aligned}$$

where we used that $Q - P = \phi(Q) - \phi(P)$ which follows because $P + (Q - P) = Q$ and applying the definition of $+$. Therefore, $\pi'\theta = \pi$.

Surjective: Consider any element x in $H^1(k, E[n])$ given by a 1-cocycle $\xi : G_k \to E[n]$, and consider the 1-cocycle $-\xi$, i.e. the map given by $\sigma \mapsto -\xi_\sigma$. We apply theorem 0.5.4 to the 1-cocycle $-\xi$ in order to find a twist of E/k, say $\phi : C \to E$ where ϕ is a $\overline{k}$-isomorphism, such that $\{\sigma \mapsto \phi^\sigma\phi^{-1}\} = \{\sigma \mapsto -\xi_\sigma\}$ in $H^1(k, E[n])$. This means that there exists $T \in E[n]$ such that the two 1-cocycles $\sigma \mapsto \phi^\sigma\phi^{-1}$ and $-\xi$ differ by the 1-coboundary $\sigma \mapsto T^\sigma - T$ (recall that we can view any point $T \in E$ as an element of $\mathrm{Isom}(E)$ by means of the translation map τ_T, so $T^\sigma - T$ is identified with $\tau_T^\sigma \tau_T^{-1}$). It follows that $\phi^\sigma\phi^{-1} = (\tau_T^\sigma\tau_T^{-1})\tau_{-\xi_\sigma} = \tau_{-\xi_\sigma + T^\sigma - T}$. Note that $-\xi_\sigma + T^\sigma - T \in E[n]$. Define an n-covering of E/k as (C, π) where $\pi := [n]\phi$. To check that this is a n-covering, it remains to check that π is defined over k. Indeed: $([n]\phi)^\sigma = [n]\phi^\sigma = [n](\tau_{-\xi_\sigma + T^\sigma - T}\phi) = [n]\phi$ because $[n](-\xi_\sigma + T^\sigma - T) = O$. Therefore, $\pi^\sigma = \pi$. Choose $P := \phi^{-1}(O)$. We note that $\pi(P) = ([n]\phi)(\phi^{-1}(O)) = [n]O = O$, in particular $P \in \ker(\pi)$. To check surjectivity, it remains to check that $\{\sigma \mapsto P^\sigma - P\} = \{\xi\}$ in $H^1(k, E[n])$. We have

$$\begin{aligned} P^\sigma - P &= \phi^{-1}(O)^\sigma - \phi^{-1}(O) \\ &= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) \\ &= (\phi^{-1}\tau^{-1}_{-\xi_\sigma + T^\sigma - T})(O) - \phi^{-1}(O) \\ &= \phi^{-1}(\xi_\sigma - T^\sigma + T) - \phi^{-1}(O) \\ &= \xi_\sigma - T^\sigma + T \end{aligned}$$

where the last equality holds thanks again to the condition $\phi^{-1}(O)+(\phi^{-1}(-\xi_\sigma - T^\sigma + T) - \phi^{-1}(O)) = \phi^{-1}(-\xi_\sigma - T^\sigma + T)$ and the definition of $+$ together with the fact that ϕ (and hence ϕ^{-1}) is an isomorphism. Since $-T^\sigma = (-T)^\sigma$ and $-T \in E[n]$, it follows that $\sigma \mapsto P^\sigma - P$ and ξ differ by the 1-coboundary $\sigma \mapsto (-T)^\sigma - (-T)$. □

1.2.9 Definition Let C/k be a n-covering of E/k. We say that C/k is locally soluble if $C(k_v) \neq \emptyset$ for every place v of k

1.2.10 Corollary For an elliptic curve E/k, there is a bijection between k-isomorphism classes of locally soluble n-coverings of E/k and $\mathrm{Sel}_n(E/k)$.

Proof: By the previous theorem, there is already a bijection between k-isomorphism classes of n-coverings of E/k and $H^1(k, E[n])$. By definition, $\mathrm{Sel}_n(E/k)$ is the kernel of the map $H^1(k, E[n]) \to \prod_v H^1(\mathrm{Gal}(\overline{k_v}/k_v), E(\overline{k_v}))$, and we note that a n-covering $\{C/k\} \in H^1(k, E[n])$ belongs to the kernel of this map if and only if $\{C/k\}$ is the zero element in $H^1(\mathrm{Gal}(\overline{k_v}/k_v), E(\overline{k_v}))$ for every place v. By remark 1.2.2, we know that C/k is a homogeneous space for E/k, and so corollary 1.1.6 implies that $\{C/k\}$ is the zero element in $H^1(\mathrm{Gal}(\overline{k_v}/k_v), E(\overline{k_v}))$ for every place v if and only if $C(k_v) \neq \emptyset$ for every place v, and this is the definition of being locally soluble. □

1.3 $H^1(k, E[n])$ in terms of twists of $([E \to \mathbb{P}^{n-1}], \omega_E)$ and Brauer-Severi diagrams

We also want to consider a variation of the parametrization in theorem 1.2.8. This variation will allows us to understand in particular the case $n = 3$ for $\mathrm{Sel}_n(E/k)$ in the next chapter.

In definition 0.6.1 we already defined what a Brauer-Severi diagram of dimension $n-1$ is. Now we should say what we mean by a twist of $([E \to \mathbb{P}^{n-1}], \omega_E)$.

1.3.1 Definition (i) Let E/k an elliptic curve. Consider the pair $([E \to \mathbb{P}^{n-1}], \omega_E)$ consisting of the morphism $E \to \mathbb{P}^{n-1}$ given by the linear system $|nO|$ and the invariant differential ω_E of E. We define a twist of $([E \to \mathbb{P}^{n-1}], \omega_E)$ as a pair $([C \to S], \omega)$ consisting of a morphism $C \to S$ from a smooth genus

1 curve C over k to a Brauer-Severi variety S over k, a regular 1-form ω on C, and such that there exist $\overline{k}$-isomorphisms $\phi : C \to E$ and $\varphi : S \to \mathbb{P}^{n-1}$ with $\phi^*\omega_E = \omega$ and such that the following diagram commutes

$$\begin{array}{ccc} C & \longrightarrow & S \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} \\ E & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

(ii) We say that two such pairs $(C \to S, \omega)$, $(C' \to S', \omega')$ are k-isomorphic if there exist k-isomorphisms $\phi : C \to C'$ and $\varphi : S \to S'$ with $\phi^*\omega' = \omega$ and the following diagram commutes

$$\begin{array}{ccc} C & \longrightarrow & S \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} \\ C' & \longrightarrow & S' \end{array}$$

We will introduce some notation. In definition 1.3.1 (ii), consider the morphisms $\phi := \mathrm{Id}_E : E \to E$ and $\varphi := \mathrm{Id}_{\mathbb{P}^{n-1}} : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ The choice of these two morphisms implies that $([E \to \mathbb{P}^{n-1}], \omega_E)$ becomes k-isomorphic to itself in the sense of definition 1.3.1 (ii). Consider the set of pairs (ϕ, φ) where $\phi : E \to E$ and $\varphi : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ are k-isomorphisms such that $([E \to \mathbb{P}^{n-1}], \omega_E)$ becomes k-isomorphic to itself (for example, $(\mathrm{Id}_E, \mathrm{Id}_{\mathbb{P}^{n-1}})$ belongs to this set). Then we can define a group structure on this set: if (ϕ, φ) and (ϕ', φ') are two elements in this set, we define $(\phi, \varphi) \cdot (\phi', \varphi') = (\phi' \circ \phi, \varphi' \circ \varphi)$. The inverse of (ϕ, φ) is $(\phi^{-1}, \varphi^{-1})$ and the identity is $(\mathrm{Id}_E, \mathrm{Id}_{\mathbb{P}^{n-1}})$. This group is denoted by $\mathrm{Aut}([E \to \mathbb{P}^{n-1}], \omega_E)$.

1.3.2 Remark Consider a twist $([C \to S], \omega)$ as in the previous definition. We note that C is not necessarily a homogeneous space of E/k. Instead of this, we require the condition $\phi^*\omega_E = \omega$.

1.3.3 Lemma For E/k elliptic curve and $n \geq 2$ we have an isomorphism of groups $E[n] \cong \mathrm{Aut}([E \to \mathbb{P}^{n-1}], \omega_E)$.

Proof: We define the map $E[n] \to \mathrm{Aut}([E \to \mathbb{P}^{n-1}], \omega_E)$ by sending $P \in E[n]$ to the pair $\tau_P : E \to E$ (translation by P) and $\varphi : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ which is a k-isomorphism of $\mathbb{P}^{n-1}$ to itself extending τ_P thanks to the condition $\tau_P^*(nO)$ being linearly equivalent nO (which holds because $P \in E[n]$). Therefore, the diagram

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{P}^{n-1} \\ \downarrow{\scriptstyle \tau_P} & & \downarrow{\scriptstyle \varphi} \\ E & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

is commutative, and we note that the choice of φ makes it unique, so the map is well-defined.

Injectivity follows from the same definition (for $P, P' \in E[n]$ such that $(\tau_P, \varphi) = (\tau_{P'}, \varphi')$ we have $\tau_P = \tau_{P'}$ and so $P = P'$). For surjectivity, if we have a pair (ϕ, φ) of k-isomorphisms $\phi : E \to E$ and $\varphi : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ such that the diagram

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{P}^{n-1} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} \\ E & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

commutes and $\phi^*\omega_E = \omega_E$, then we know that the only automorphisms ϕ of E such that $\phi^*\omega_E = \omega_E$ are translations by $P \in E$, so for this P we have $\phi = \tau_P$. Since φ extends ϕ, we know that $\tau_P^*(nO)$ should be linearly equivalent to nO which implies that $P \in E[n]$. Therefore, $P \in E[n]$ and it's mapped to the pair (τ_P, φ) and we obtain surjectivity.

Finally, it is a group homomorphism because for $P, P' \in E[n]$ we have $\tau_{P+P'} = \tau_{P'} \circ \tau_P$, and if we denote by i the morphism $E \to \mathbb{P}^{n-1}$ defined by the linear system $|nO|$ and if φ satisfies $\varphi \circ i = i \circ \tau_P$ and similarly if φ' satisfies $\varphi' \circ i = i \circ \tau_{P'}$, then the composition $\varphi' \circ \varphi$ satisfies $(\varphi' \circ \varphi) \circ i = i \circ \tau_{P+P'}$. $\square$

1.3.4 Lemma There is a bijection between k-isomorphism classes of twists $([C \to S], \omega)$ of $([E \to \mathbb{P}^{n-1}], \omega_E)$ and k-isomorphisms classes of Brauer-Severi diagrams of dimension $n-1$.

Proof: We define the bijection by sending a twist $([C \to S], \omega)$ of $([E \to \mathbb{P}^{n-1}], \omega_E)$ to the Brauer-Severi diagram $[C \to S]$ of dimension $n-1$ where C has a structure of homogeneous space for E/k as follows. Let $\phi : C \to E$ be a $\overline{k}$-isomorphism such that $\phi^*\omega_E = \omega$ and $\varphi : S \to \mathbb{P}^{n-1}$ another $\overline{k}$-isomorphism, where we can choose such ϕ and φ from the definition of $([C \to S], \omega)$. If $P \in C$ and $Q \in E$, then define $P + Q := \phi^{-1}(\phi(P) + Q)$. This action of E on C depends only on ω and not on ϕ. To see this, suppose that $\phi' : C \to E$ is another $\overline{k}$-isomorphism such that $\phi'^*\omega_E = \omega$. Then we have to check

$$(\phi')^{-1}(\phi'(P) + Q) = \phi^{-1}(\phi(P) + Q)$$

This is equivalent to

$$(\phi\phi'^{-1})(\phi'(P) + Q) = (\phi\phi'^{-1})(\phi'(P)) + Q \tag{1}$$

But we have

$$\phi^*\omega_E = \omega = \phi'^*\omega_E$$

so that

$$(\phi'^*)^{-1}\phi^*\omega_E = (\phi\phi'^{-1})^*\omega_E = \omega_E$$

but this means that $\phi\phi'^{-1}$ should be a translation by some point $R \in E$. Therefore, (1) becomes

$$\tau_R(\phi'(P) + Q) = \tau_R(\phi'(P)) + Q$$

which is true because E is abelian. It follows that $[C \to E]$ is indeed a Brauer-Severi diagram of dimension $n-1$.

Well-defined: Suppose that $([C \to S], \omega)$ and $([C' \to S'], \omega')$ are k-isomorphic, and let $\alpha : C \to C'$ and $\beta : S \to S'$ be k-isomorphisms such that $\alpha^*\omega' = \omega$. In order to check that the corresponding images $[C \to S]$ and $[C' \to S']$ are k-isomorphic, it suffices to check that α respects the torsor structure on C and C', i.e. that $\alpha(P+Q) = \alpha(P) +' Q$. To check this, note that $\alpha^*\omega' = \omega$ implies $(\alpha^*\phi'^*)\omega_E = \phi^*\omega_E$ and this implies $((\phi^*)^{-1}\alpha^*\phi'^*)\omega_E = \omega_E$. It follows that $\phi'\alpha\phi^{-1}$ is a translation τ_R for some fixed point $R \in E$. Now we want to show that $\alpha(P+Q) = \alpha(P) +' Q$ and this means to show

$$\alpha(\phi^{-1}(\phi(P) + Q)) = \phi'^{-1}(\phi'(\alpha(P)) + Q)$$

which is equivalent to showing that

$$(\phi'\alpha\phi^{-1})(\phi(P) + Q) = (\phi'\alpha\phi^{-1})(\phi(P)) + Q$$

and this is equivalent to

$$\tau_R(\phi(P) + Q) = \tau_R(\phi(P)) + Q$$

and this equality holds for all $P \in C$ and $Q \in E$.

Injective: Suppose that $([C \to S], \omega)$ and $([C' \to S'], \omega')$ have images $[C \to S]$ and $[C' \to S']$ such that they are k-isomorphic. Let $\alpha : C \to C'$ and $\beta : S \to S'$ be k-isomorphisms such that α respects the torsor structure on C and C'. It suffices to check that $\alpha^*\omega' = \omega$. As always, let $\phi : C \to E$ be a $\overline{k}$-isomorphism such that $\phi^*\omega_E = \omega$ and similarly $\phi' : C' \to E$ such that $\phi'^*\omega_E = \omega'$. So we have to check that $\alpha^*\phi'^*\omega_E = \phi^*\omega_E$, or equivalently $((\phi^*)^{-1}\alpha^*\phi'^*)\omega_E = \omega_E$, and we will achieve this by showing that $\phi'\alpha\phi^{-1}$ is a translation τ_R for some fixed $R \in E$. However, α respects the torsor structure, so

$$\alpha(P+Q) = \alpha(P) +' Q$$

which is equivalent to

$$\alpha(\phi^{-1}(\phi(P) + Q)) = \phi'^{-1}(\phi'(\alpha(P)) + Q)$$

and this is equivalent to

$$(\phi'\alpha\phi^{-1})(\phi(P) + Q) = (\phi'\alpha\phi^{-1})(\phi(P)) + Q$$

and this is true for all $P \in C$ and all $Q \in E$. In particular, for $P := \phi^{-1}(O)$ and any $Q \in E$ it follows that

$$(\phi'\alpha\phi^{-1})(Q) = (\phi'\alpha\phi^{-1})(O) + Q$$

and so we conclude that $\phi'\alpha\phi^{-1}$ is a translation by $R := (\phi'\alpha\phi^{-1})(O) \in E$.

Surjective: Consider a Brauer-Severi diagram of dimension $n-1$, say $[C \to S]$ and let $\phi : C \to E$ be a $\overline{k}$-isomorphism respecting the torsor structure on C and E (we can take such ϕ by definition of $[C \to S]$). We take the twist $([C \to S], \phi^*\omega_E)$ and we claim that its image is k-isomorphic to $[C \to S]$. To see this, we define $\alpha : C \to C$ as $\alpha := \mathrm{Id}_C$ and note that we have two torsor structures on C: the first coming from the hypothesis and which we denote by $+$, and the second coming from ϕ and which we denote by $+'$. So we need to check that α satisfies $\alpha(P+Q) = \alpha(P) +' Q$ for all $P \in E$ and $Q \in E$. We have

$$\begin{aligned} \alpha(P) +' Q &= P +' Q \\ &= \phi^{-1}(\phi(P) + Q) \\ &= \phi^{-1}(\phi(P+Q)) \\ &= P + Q \end{aligned}$$

where the third equality holds because ϕ respects the torsor structure on C and E. By choosing $\beta : S \to S$ as $\beta := \mathrm{Id}_S$, it follows that the image of $([C \to S], \phi^*\omega_E)$ is k-isomorphic to $[C \to S]$. □

The previous lemma implies the following.

1.3.5 Lemma There is a group isomorphism $\mathrm{Aut}([E \to \mathbb{P}^{n-1}]) \cong E[n]$.

Proof: We already know that $E[n]$ is isomorphic to $\mathrm{Aut}([E \to \mathbb{P}^{n-1}], \omega_E)$ by lemma 1.3.3, so it suffices to check that there is an isomorphism between $\mathrm{Aut}([E \to \mathbb{P}^{n-1}])$ and $\mathrm{Aut}([E \to \mathbb{P}^{n-1}], \omega_E)$. We achieve this by mapping a pair $(\phi, \varphi) \in \mathrm{Aut}([E \to \mathbb{P}^{n-1}])$ to the same pair (ϕ, φ) and verifying that $\varphi^*\omega_E = \omega_E$. But a k-isomorphism $\phi : E \to E$ respects the torsor structure on E if and only ϕ is the translation map τ_P for some point $P \in E$, and we know that $\tau_P^*\omega_E = \omega_E$. The result follows from this. □

The previous two lemmas imply the following theorem.

1.3.6 Theorem For an elliptic curve E/k, the set of k-equivalence classes of Brauer-Severi diagrams of dimension $n-1$ is parametrized by $H^1(k, E[n])$.

Proof: We give a sketch of the proof which can be found in proposition 2.2 in [14]. The statement is a consequence of proving the following. Let $[C_0 \to S_0]$ be any fixed Brauer-Severi diagram. We may have $C_0(k) = \emptyset$, so choose a sufficiently large (finite) Galois extension L'/k such that $C_0(L') \neq \emptyset$. Let L/k be any finite Galois such that L' is an intermediate subfield of L/k (note that if $C_0(L') \neq \emptyset$, then $C_0(L) \neq \emptyset$). Then we want to prove that the set of k-isomorphism classes of Brauer-Severi diagrams $[C \to S]$ such that $C(L) \neq \emptyset$ is parametrized by $H^1(\mathrm{Gal}(L/k), E[n]^{\mathrm{Gal}(\overline{k}/L)})$.

To see this, let $[C \to S]$ be a Brauer-Severi diagram such that $C(L) \neq \emptyset$. The condition $C(L) \neq \emptyset$ implies that $C(L)$ is isomorphic to $E(L)$ under

some L-isomorphism of torsors $\phi : C \to E$. Since we may regard C/L as the elliptic curve E/L and the only isomorphisms of torsors from E/L to itself are translations, and since the translations τ_P with $P \in E[n](\overline{k})$ satisfy that $\tau_P^*(nO)$ is linearly equivalent to nO, it follows that ϕ extends to a L-isomorphism $\varphi : S(L) \to \mathbb{P}_L^{n-1}$, so that the following diagram commutes

$$\begin{array}{ccc} C(L) & \longrightarrow & S(L) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} \\ E(L) & \longrightarrow & \mathbb{P}_L^{n-1} \end{array}$$

But we also know that there is an isomorphism $E[n] \cong \mathrm{Aut}(E \to \mathbb{P}^{n-1})$ by lemma 1.3.5. It follows that $E[n](L) \cong \mathrm{Aut}([E \to \mathbb{P}^{n-1}])(L)$, and given an element $\sigma \in \mathrm{Gal}(L/k)$ we can construct $\phi^\sigma \phi^{-1}$ which is naturally identified with a pair $(\phi^\sigma \phi^{-1}, \psi)$ belonging to $\mathrm{Aut}([E \to \mathbb{P}^{n-1}])(L)$ where ψ is the extended automorphism of E induced by $\phi^\sigma \phi^{-1} = \tau_P$ for some $P \in E[n]$ (recall that we can extend it thanks to the condition $\tau_P^*(nO)$ linearly equivalent to nO). In this way, we have obtained an element, say ξ_σ, belonging to $E[n](L)$ and therefore an element in $H^1(\mathrm{Gal}(L/k), E[n]^{\mathrm{Gal}(\overline{k}/L)})$ given by the image of the 1-cocycle ξ mapping σ to ξ_σ. The map given by mapping the k-isomorphic class of $[C \to S]$ to the image of the 1-cocycle ξ will imply the desired bijection.

Now if we take the direct limit of the groups $H^1(\mathrm{Gal}(L/k), E[n]^{\mathrm{Gal}(\overline{k}/L)})$ where the direct limit is running over the finite Galois extensions L/k such that L' is an intermediate field extension of L/k, we obtain the statement of the proposition. □

The previous theorem implies the following.

1.3.7 Theorem For an elliptic curve E/k, there is a bijection between the k-isomorphism classes of twists of $([E \to \mathbb{P}^{n-1}], \omega_E)$ and the group $H^1(k, E[n])$.

Proof: This is because $H^1(k, E[n])$ is in bijective correspondence with k-isomorphism classes of Brauer-Severi diagrams by theorem 1.3.6, which in turn are in bijective correspondence with k-isomorphism classes of twists of $([E \to \mathbb{P}^{n-1}], \omega_E)$ by lemma 1.3.4. □

1.4 $H^1(k, E[n])$ in terms of torsor-divisor class pairs

First we need to know the definition of torsor-divisor class pair.

1.4.1 Definition (i) Consider an elliptic curve E/k and the map $E \to \mathbb{P}_k^{n-1}$ given by the linear system $|nO|$. A torsor-divisor class pair of degree n is a pair

$(C,[D])$ given by a homogeneous space C for E such that the $\overline{k}$-isomorphism between C and E respects the homogeneous space structures on C and E, together with a k-rational divisor class $[D]$ of some effective divisor D of degree n on C, where we define the class $[D]$ to be k-rational if D^σ is linearly equivalent to D for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

(ii) A k-isomorphism between two torsor-divisor class pairs $(C,[D])$ and $(C',[D'])$ of degree n is a k-isomorphism $\phi : C \to C'$ respecting the homogeneous space structure on C and C' such that $\phi^* D'$ is linearly equivalent to D. The set of k-isomorphisms from $(C,[D])$ to itself is denoted by $\mathrm{Aut}(C,[D])$.

The trivial torsor-divisor class pair of degree n is the pair $(E,[nO])$.

Now we can describe $H^1(k,E[n])$ in terms of torsor-divisor class pairs.

1.4.2 Theorem: There is a bijection between k-isomorphism classes of torsor-divisor class pairs $(C,[D])$ of degree n and $H^1(k,E[n])$.

Proof: Recall that $H^1(k,E[n])$ is parametrized by n-coverings (C,π) of E/k. If we initially start with a torsor-divisor class pair $(C,[D])$ of degree n, we take $\pi : C \to E = \mathrm{Pic}(C)$ given by $P \mapsto [nP - D]$. Note that π is k-rational because D is linearly equivalent to all its Galois conjugates. Conversely, if (C,π) is a n-covering, take a $\overline{k}$-isomorphism $\phi : C \to E$, and we give C a structure of torsor as before, namely $p + P = \phi^{-1}(\phi(p) + P)$, and we map our n-covering to the torsor divisor class pair $(C,[\phi^* nO])$. It suffices to check that $(C,[D])$ and $(C',[D'])$ are k-isomorphic if and only if the corresponding (C,π) and (C',π') are k-isomorphic.

If $\theta : C \to C'$ is a k-isomorphism such that $\theta^* D' = D$, then we have $(\phi'\theta\phi^{-1})^* nO = (\theta\phi^{-1})^*\phi'^* nO = (\phi^{-1})^*\theta^* D' = (\phi^{-1})^* D = nO$. Since ϕ', θ and ϕ respect the corresponding torsor structures, the same holds for $\alpha := \phi'\theta\phi^{-1} : E \to E$, and the only isomorphisms of E respecting the torsor structure are translations by some $P \in E$. In our case, $P \in E[n]$ because $\alpha^* nO$ is equal to nO (in particular, linearly equivalent).

If (C,π) and (C',π') are k-equivalent n-coverings, then take $\theta : C \to C'$ such that $\pi'\theta = \pi$, then θ respects the torsor structures (see proof of parametrization of $H^1(k,E[n])$ by n-coverings). It remains to check $\theta^*(\phi'^* nO) = \phi^* nO$. This happens because there exists $P \in E[n]$ such that $\phi'\theta = \tau_P\phi$, so $\theta^*\phi'^* nO = \phi^*\tau_P^* nO$ and since $\tau_P^* nO$ is linearly equivalent to nO (P is n-torsion) then $\phi^*\tau_P^* nO$ is linearly equivalent to $\phi^* nO$. □

1.4.3 Corollary Given an elliptic curve E/k, there is a bijection between torsor-divisor class pairs of degree n and Brauer-Severi diagrams of dimension $n-1$.

Proof: This follows from theorem 1.3.6 and theorem 1.4.2. □

1.4.4 Remark. In the previous corollary, the assignment is given as follows (see [7]). If we have a torsor-divisor class pair $(C,[D])$ of degree n, then we

identify the complete linear system $|D|$ with the dual of some Brauer-Severi variety S (see remark 1.20 in [7]) to obtain a morphism $C \to S$. Conversely, if $[C \to S]$ is a Brauer-Severi diagram of dimension $n-1$, then $S \cong \mathbb{P}_k^{n-1}$ over $\overline{k}$ and we take the pullback of a hyperplane on $\mathbb{P}_k^{n-1}$ to obtain a k-rational divisor class $[D]$ on C (see proposition 1.5.6).

1.5 The divisor of a locally soluble n-covering of E/k

Given a locally soluble n-covering (C, π) of E/k, we will sketch a proof which shows that we can always find a k-rational effective divisor of degree n on C. We mention this because besides its importance regarding the period-index problem for elements (of order n) in the Tate-Shafarevich group $Ш(E/k)$, it will be useful in Chapter 2 to prove the bijection between $\mathrm{Sel}_2(E/k)$ and binary quartic forms (or more accurately, k-equivalence classes of locally soluble binary quartic forms with invariants equal to the invariants of the elliptic curve). Indeed, we will only need the divisor in the case $n = 2$.

The construction of such a divisor will use two main ingredients: Hasse's theorem and Hilbert's Theorem 90, both stated in Chapter 0 - Preliminaries.

1.5.1 Lemma: Suppose that (C, π) is a locally soluble n-covering of E/k, and suppose that there exists a divisor D on C (in general defined over $\overline{k}$) such that D^σ is linearly equivalent to D for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Then D is linearly equivalent to a k-rational divisor on C.

Proof: We provide a sketch of this which can be found in [5]. Let ξ be a generic point of C. By hypothesis, for each $\sigma \in G_k$ there exists some $f_\sigma(\xi) \in \overline{k}(\xi) \subseteq \overline{k}(C)$ such that $D^\sigma - D = \mathrm{div}(f_\sigma(\xi))$. We note that G_k defines an action on $\overline{k}(\xi)^*$ as follows. For each $\sigma \in \mathrm{Gal}(\overline{k}/k)$, we can take the automorphism $\tilde{\sigma}$ which extends σ and satisfies $\tilde{\sigma}(\xi) = \xi$. Then for all $\sigma \in G_k$ and $f(\xi) \in \overline{k}(\xi)$, define $\sigma \cdot f(\xi) := f(\xi)^{\tilde{\sigma}}$, and it will make sense to consider $H^1(\mathrm{Gal}(\overline{k}/k), \overline{k}(\xi)^*)$.

For all $\sigma, \tau \in G_k$, define $f(\sigma, \tau) := \frac{f_\tau(\xi)^{\tilde{\sigma}} f_\sigma(\xi)}{f_{\sigma\tau}(\xi)}$. Since $\mathrm{div}(f_\sigma(\xi)) = D^\sigma - D$ for all σ and since $\mathrm{div}(f_\tau(\xi)^{\tilde{\sigma}}) = \mathrm{div}(f_\tau(\xi))^\sigma$, it follows that $\mathrm{div}(f(\sigma, \tau)) = 0$ which in turn implies that $f(\sigma, \tau) \in \overline{k}^*$. Next, define the map $f : G_k \times G_k \to \overline{k}^*$ as $(\sigma, \tau) \mapsto f(\sigma, \tau)$. Then we can quickly verify that f is a 2-cocycle.

Since (C, π) is a locally soluble n-covering of E/k, there exists some $P_v \in k_v$ which belongs to C. As we want to use Hasse's theorem, we note that not only the 2-cocycle f defines an element x in $H^2(G_k, \overline{k}^*)$ but also defines a 2-cocycle $f_v : G_{k_v} \times G_{k_v} \to \overline{k_v}^*$ which in turn defines an element x_v in $H^2(G_{k_v}, \overline{k_v}^*)$. On the one hand, we know that $\mathrm{Br}(k_v)$ is $H^2(G_{k_v}, \overline{k_v}^*)$. On the other hand, the locally soluble n-covering (C, π) corresponds to a Brauer-Severi diagram $[C \to S]$. The fact that $C(k_v) \neq \emptyset$ implies that $S(k_v) \neq \emptyset$, so $[S]$ corresponds to the zero element in $H^1(k_v, \mathrm{PGL}_n(\overline{k_v}))$. So proposition 0.3.5 implies that $[S]$ corresponds to the zero element in $\mathrm{Br}(k_v)$. From this, we obtain that the element x_v is the zero element in $H^2(G_{k_v}, \overline{k_v}^*)$. Therefore, the 2-cocycle f_v is

also a 2-coboundary. Since the image of x under the natural map $H^2(G_k, \overline{k}^*) \to \prod_v H^2(G_{k_v}, \overline{k_v}^*)$ is trivial, Hasse's theorem (theorem 0.5.10) implies that x is trivial in $H^2(G_k, \overline{k}^*)$. In particular, f is a 2-coboundary. Therefore, for all $\sigma \in G_k$ there exists some m_σ such that for all $\sigma, \tau \in G_k$ we have $f(\sigma, \tau) = \frac{m_\tau^\sigma m_\sigma}{m_{\sigma\tau}}$.

Now consider $\frac{f_\sigma(\xi)}{m_\sigma} \in \overline{k}(\xi)^*$ for each $\sigma \in G_k$. The map $\sigma \mapsto \frac{f_\sigma(\xi)}{m_\sigma}$ is a 1-cocycle $G_k \to \overline{k}(\xi)^*$ thanks to the equalities $\frac{m_\tau^\sigma m_\sigma}{m_{\sigma\tau}} = f(\sigma, \tau) = \frac{f_\sigma(\xi)}{m_\sigma}$. Therefore, this map defines an element in $H^1(\mathrm{Gal}(\overline{k}/k), \overline{k}(\xi)^*)$. However, Hilbert's Theorem 90 implies that $H^1(\mathrm{Gal}(\overline{k}(\xi)/k(\xi)), \overline{k}(\xi)^*) = 0$, which in turn implies that $H^1(\mathrm{Gal}(\overline{k}/k), \overline{k}(\xi)^*) = 0$ (here we use that $\mathrm{Gal}(\overline{k}/k) \cong \mathrm{Gal}(\overline{k}(\xi)/k(\xi))$ and so $H^1(\mathrm{Gal}(\overline{k}(\xi)/k(\xi)), \overline{k}(\xi)^*) \cong H^1(\mathrm{Gal}(\overline{k}/k), \overline{k}(\xi)^*)$). So the 1-cocycle $\sigma \mapsto \frac{f_\sigma(\xi)}{m_\sigma}$ is also a 1-coboundary. This means that there exists a function $g(\xi) \in \overline{k}(\xi)^*$ such that $\frac{f_\sigma(\xi)}{m_\sigma} = \frac{g(\xi)^\sigma}{g(\xi)}$ for all $\sigma \in G_k$. Then again using that $\mathrm{div}(g(\xi)^{\tilde{\sigma}}) = \mathrm{div}(g(\xi))^\sigma$ and $\mathrm{div}(f_\sigma(\xi)) = D^\sigma - D$, and also using that $\frac{f_\sigma(\xi)}{m_\sigma} = \frac{g(\xi)^\sigma}{g(\xi)}$, it follows that the divisor $D' := D - (g(\xi))$ satisfies $D'^\sigma - D' = 0$. In particular, D' is a k-rational divisor on C and this is the divisor that we wanted. □

1.5.2 Proposition: Suppose that (C, π) is a locally soluble n-covering of E/k. Then there exists a k-rational divisor D on C which is effective and has degree n.

Proof: Consider any point $P \in \pi^{-1}(O)$ and take the divisor nP on C. Let $\phi : C \to E$ be a $\overline{k}$-isomorphism such that $\pi = [n]\phi$. We note that if $P' \in \pi^{-1}(O)$ is another point, then the divisors nP and nP' are linearly equivalent. To see this, we may assume that E is the Jacobian of C by remark 1.2.3, and that $\phi : C \to E$ is defined by $P \mapsto [P - Q]$ for some fixed point $Q \in C$, again by remark 1.2.3. Then the elements nP and nP' are linearly equivalent if and only if $[nP - nQ] = [nP' - nQ]$, which is equivalent to $([n]\phi)(P) = ([n]\phi)(P')$, i.e. $\pi(P) = \pi(P')$ and this is true by hypothesis.

On the other hand, note that if $P \in \pi^{-1}(O)$ then $P^\sigma \in \pi^{-1}(O)$ because $\pi(P^\sigma) = \pi(P)^\sigma = O$ (where we use that π is defined over k). In particular, nP^σ is linearly equivalent to nP by last paragraph, so nP satisfies lemma 1.5.1 and then it is linearly equivalent to some k-rational divisor D. This divisor is effective and has degree n as well. □

1.5.3 Remark Consider an element $C \in H^1(k, E)$. Here recall that we identified this group with $\mathrm{WC}(E/k)$. We say that C has period n if the order of C in the torsion group $H^1(k, E)$ is equal to n. Also, we say that the index of C is d if d is the smallest positive integer for which there exists a k-rational divisor of degree d on C. So proposition 1.5.2 is telling us that when we assume that C belongs to the Tate-Shafarevich group $Ш(E/k)$, the condition $n = d$ holds. Here we are using the exact sequence in proposition 0.5.3, namely $0 \to E(k)/nE(k) \to \mathrm{Sel}_n(E/k) \to Ш(E/k)[n] \to 0$ where $E(k)/nE(k)$ is identified with soluble n-coverings and $\mathrm{Sel}_n(E/K)$ with locally soluble n-coverings, and

also remark 1.2.2 to see the n-covering C as a homogeneous space. This is called 'the period-index problem' and it holds for elements in Ш.

So in summary, we have obtained a k-rational effective divisor of degree n when we are dealing with locally soluble n-coverings (C, π) of E/k. There is, however, another way to obtain a k-rational effective divisor of degree n in the case when we are dealing with twists $([C \to S], \omega)$ of $([E \to \mathbb{P}^{n-1}], \omega_E)$ which belong to the kernel of the obstruction map, i.e. those twists satisfying that S is isomorphic to $\mathbb{P}^{n-1}_k$ over k (equivalently, those Brauer-Severi diagrams $C \to S$ which belong to the kernel of the obstruction map, i.e. those Brauer-Severi diagrams such that S is isomorphic to $\mathbb{P}^{n-1}_k$ over k). To achieve this, we need the parametrization of $H^1(k, E[n])$ as torsor-divisor class pairs and the obstruction map in terms of torsor-divisor class pairs, both as follows in the next lemma:

1.5.4 Lemma: Consider the obstruction map in terms of torsor-divisor class pairs of degree n, $\mathrm{Ob} : H^1(k, E[n]) \to \mathrm{Br}(k)$ given by $(C, [D]) \mapsto \delta_C([D])$ where we consider δ_C as in proposition 0.3.9. Then $\mathrm{Ob}(C, [D]) = 0$ if and only D is linearly equivalent to a k-rational divisor.

Proof: If $\mathrm{Ob}(C, [D]) = 0$ then the exactness of the sequence $\mathrm{Div}(\overline{C})^{G_k} \to \mathrm{Pic}(\overline{C})^{G_k} \xrightarrow{\delta_C} \mathrm{Br}(k)$ (proposition 0.3.9) implies that there exists $D' \in \mathrm{Div}(\overline{C})^{G_k}$ such that $[D'] = [D]$, i.e. D is linearly equivalent to D' which is k-rational. Conversely, if D is linearly equivalent to a k-rational divisor D', then $[D] = [D']$ in $\mathrm{Pic}(\overline{C})^{G_k}$ and the exactness of the sequence implies that $\delta_C([D']) = 0$, i.e. $\delta_C([D]) = 0$. □

1.5.5 Observation: Recall that in the definition of torsor-divisor class pair $(C, [D])$ of degree n we defined $[D]$ to be k-rational in the sense that D is linearly equivalent (not necessarily equal) to D^σ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$. In particular, when a torsor-divisor class pair $(C, [D])$ of degree n belongs to $\mathrm{Sel}_n(E/k)$, then we can view C as a locally soluble n-covering of E/k, in which case the fact that D is linearly equivalent to a k-rational follows from lemma 1.5.1. This makes sense because we actually have $\mathrm{Sel}_n(E/k) \subseteq \ker(\mathrm{Ob})$ (see the proof of theorem 2.2.6 of chapter 2) and in this case we can also apply the previous lemma to get the same result. In other words, whereas a torsor-divisor class pair $(C, [D])$ only satisfies that D is linearly equivalent to its Galois conjugates but not necessarily linearly equivalent to a k-rational divisor, the condition of belonging to the kernel implies that it is linearly equivalent to a k-rational divisor, in which case lemma 1.5.1 gives a proof when it belongs to $\mathrm{Sel}_n(E/k)$ and lemma 1.5.4 gives another (simpler) proof when it belongs not only to $\mathrm{Sel}_n(E/k)$ but also to $\ker(\mathrm{Ob}) \supseteq \mathrm{Sel}_n(E/k)$.

1.5.6 Proposition: If $\alpha : C \to S$ is a Brauer-Severi diagram belonging to $\ker(\mathrm{Ob})$, i.e. $S \cong \mathbb{P}^{n-1}_k$ over k and if H denotes any hyperplane of $\mathbb{P}^{n-1}_k$, then

the pullback divisor $\alpha^* H$ is the class of a k-rational effective divisor of degree n on C.

Proof: We provide a sketch of this. The commutativity of the diagram means that the morphism $E \to \mathbb{P}^2$ becomes isomorphic to the morphism $C \to S$ over $\overline{k}$. If we denote the morphism $E \to \mathbb{P}^2$ by β, then the pullback $\beta^* \mathcal{O}(1)$ is linearly equivalent to nO which is an effective divisor of degree n. Since the morphism α becomes isomorphic to the morphism β, it follows that the pullback $\alpha^* \mathcal{O}(1)$ is also linearly equivalent to an effective divisor of degree n. Finally, the k-rationality of this divisor follows from the fact that α is defined over k. $\square$

Finally, we conclude this chapter with the definition of the invariants of an elliptic curve E/k which we will need in the next chapter.

1.5.7 Definition The invariants of an elliptic curve $E : y^2 = x^3 + Ax + B$ defined over k are the values $I(E) = -3A$, $J = -27B$

Chapter 2 - Parametrizing the 2-Selmer group and the 3-Selmer group of E/k

In this chapter we explain, given an elliptic curve E/k, the bijection between (k-equivalence classes of) binary quartic forms with invariants $I(E), J(E)$ and $\mathrm{Sel}_2(E/k)$ and also the bijection between (k-equivalence classes of) ternary cubic forms with invariants $I(E), J(E)$ and $\mathrm{Sel}_3(E/k)$.

2.1 The case $n = 2$

2.1.1 Definition An element of the form $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ with coefficients in k is called a binary quartic form. The action of $\mathrm{GL}_2(k)$ on $f(x,y)$ is defined by $g \cdot f(x,y) := f((x,y)g)$ where $g \in \mathrm{GL}_2(k)$. Two binary quartic forms $f(x,y)$ and $f'(x,y)$ are equivalent if there exists $\gamma \in k^*$ and $g \in \mathrm{GL}_2(k)$ such that $f(x,y) = \gamma^2(g \cdot f'(x,y))$.

Every binary quartic form has two associated quantities:

2.1.2 Definition The invariants of a binary quartic form $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ over k are $I(f) := 12ae - 3bd + c^2$ and $J(f) := 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$

2.1.3 Observation In Example 0.4.9 we considered the affine equation $y^2 = g(x,1)$ where $g(x,z) = a_0x^4 + 4a_1x^3z + 6a_2x^2z^2 + 4a_3xz^3 + a_4z^4 \in k[x,z]$ and defined the values $I' = a_0a_4 - 4a_1a_3 + 3a_2^2$ and $J' = a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3$. Putting $a = a_0$, $b = 4a_1$, $c = 6a_2$, $d = 4a_3$ and $e = a_4$ in the previous definition, we obtain $I = 12I'$ and $J = 432J'$.

We already know from Chapter 1 that there is a bijection between locally soluble 2-coverings and the 2-Selmer group $\mathrm{Sel}_2(E/k)$ of an elliptic curve E/k, so first given a locally soluble 2-covering C we describe how to obtain a quartic from it. For this, we need the divisor that we constructed in section 1.5 of chapter 1. Conversely, given a binary quartic form we know how to construct a n-covering of some elliptic curve over k (example 1.2.5).

2.1.4 Lemma If (C, ϕ) is a locally soluble 2-covering of E/k, then we can find an effective degree 2 divisor D of C defined over k.

Let g be the genus of a smooth curve C. Recall that if the degree of a divisor D is greater than $2g - 2$, then the Riemann-Roch theorem becomes $l(D) = \deg(D) - g + 1$. In Chapter 0 we defined $l(D)$ as the dimension of the $\overline{k}$-vector space $\mathcal{L}(D) := \{f \in \overline{k}(C)^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$. However, the Riemann-Roch theorem is also true if we consider instead the k-vector space

$\mathcal{L}(D) := \{f \in k(C)^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$. Therefore, when $\deg(D) > 2g-2$ we have $l(D) = \deg(D) - g + 1$ where $l(D)$ is the dimension of the k-vector space $\mathcal{L}(D)$. We will use this in the next proposition.

2.1.5 Proposition To every locally soluble 2-covering (C, π) of E/k it corresponds a quartic $g(x) \in k[x]$ such that $C' : y^2 = g(x)$ is k-isomorphic to C.

Proof: Take D a divisor as in lemma 2.1.4. We note that the genus of C is 1 by definition of 2-covering of E/k, and and also we note that the degree of D is 2. By Riemann-Roch, it follows that the dimension of the k-vector space $\mathcal{L}(D)$ is equal to $\deg(D) - g + 1 = 2$. Now we observe that the k-vector space $\mathcal{L}(D)$ is naturally a k-vector subspace of k-vector space $\mathcal{L}(2D)$, which is in turn a k-vector subspace of $\mathcal{L}(4D)$. By applying the Riemann-Roch theorem to the k-vector spaces $\mathcal{L}(2D)$ and $\mathcal{L}(4D)$, it follows that the dimension of $\mathcal{L}(2D)$ is 4 and the dimension of $\mathcal{L}(4D)$ is 8. The idea is to choose a suitable $x \in k(C)^*$ inducing a linearly dependence relation in $\mathcal{L}(4D)$ so that it takes the form $y^2 = g(x)$ where $g(x) \in k[x]$ is a quartic.

We note that $\mathcal{L}(D)$ contains nonconstant elements because it has dimension 2, so we pick a nonconstant element x such that $1, x$ form a basis of $\mathcal{L}(D)$. In particular, we note that $x \in k(C)^*$. Also, we note that x induces a morphism $C \to \mathbb{P}^1$ of degree 2 because we can take the linear system $|D|$ which induces a morphism $C \stackrel{|D|}{\to} \mathbb{P}^1$, and the fact that D has degree 2 together with the Riemann-Roch theorem implies that the morphism induced by $|D|$ has degree 2 as well. Also, we observe that $k(x)$ is isomorphic to the field of rational functions in one variable because $1, x$ is a basis of $\mathcal{L}(D)$. Using that $K(C)/k(\mathbb{P}^1)$ has degree 2, it follows that the field extension $K(C)/k(x)$ has degree 2 as well.

Now we look at $1, x, x^2$ in $\mathcal{L}(2D)$. Since the dimension of $\mathcal{L}(2D)$ is $\deg(2D) - g + 1 = 4$, we can find an element $v \in \mathcal{L}(2D)$ (in particular, $v \in k(C)^*$) which is linearly independent from the previous three elements. Next, we produce nine elements in the k-vector space $\mathcal{L}(4D)$, namely $1, x, x^2, x^3, x^4, v, v^2, xv, x^2v$. The k-vector space $\mathcal{L}(4D)$ has dimension $\deg(4D) - g + 1 = 8$, which implies that our nine elements satisfy a linearly dependence relation, say $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + b_0v + b_1xv + b_2x^2v + c_0v^2 = 0$ where the coefficients belong to k and they're not equal to zero all at the same time. We should have $c_0 \neq 0$, otherwise we have $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 = -(b_0 + b_1x + b_2x^2)v$ which would imply that $v \in k(x)$ and therefore $1, x, v$ would satisfy a linearly dependence relation, which is impossible. So we have $c_0 \neq 0$ and after dividing the equality by c_0 we get, for some $l, m, n, \alpha, \beta, \gamma, \delta, \epsilon \in k$, a relation of the form $v^2 - 2v(lx^2+mx+n) = \alpha x^4+\beta x^3+\gamma x^2+\delta x+\epsilon$. Put $y := v - lx^2 - mx - n \in \mathcal{L}(4D)$ and we note that y is nonconstant, otherwise v would be a linear combination of $1, x, x^2$ which is not possible. We obtain

$$\begin{aligned} y^2 &= (v - lx^2 - mx - n)^2 \\ &= v^2 - 2v(lx^2 + mx + n) + (lx^2 + mx + n)^2 \\ &= (\alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + \epsilon) + (lx^2 + mx + n)^2 \end{aligned}$$

But $(lx^2+mx+n)^2$ is of the form $\alpha' x^4+\beta' x^3+\gamma' x^2+\delta' x+\epsilon'$ with $\alpha', \beta', \gamma', \delta', \epsilon' \in k$, so we obtain a relation of the form

$$\begin{aligned} y^2 &= (\alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + \epsilon) + (\alpha' x^4 + \beta' x^3 + \gamma' x^2 + \delta' x + \epsilon') \\ &= g(x) \end{aligned}$$

where $g(x) = ax^4+bx^3+cx^2+dx+e \in k[x]$ is such that $a = \alpha+\alpha'$, ..., $e = \epsilon+\epsilon'$ and has degree 4, as desired.

Finally, the equality $y^2 = g(x)$ implies that $k(x, y)/k(x)$ has degree 2. But we already know that $k(C)/k(x)$ has degree 2 as well. It follows that C should be k-isomorphic to the curve defined by $y^2 = g(x)$. □

2.1.6 Proposition There is a bijection between the equivalence classes of locally soluble 2-coverings of an elliptic curve E/k and the equivalence classes of binary quartic forms $g(x, z)$ such that the curve $y^2 = g(x, 1)$ is nonsingular, locally soluble, and its Jacobian is k-isomorphic to E.

Proof: If (C, π) is a locally soluble 2-covering of E/k, then from proposition 2.1.5 we obtain a quartic $g(x)$ such that $C' : y^2 = g(x)$ is k-isomorphic to C. Note that the fact that C' is k-isomorphic to C implies that $C' : y^2 = g(x)$ is locally soluble and nonsingular. Also, the fact that $C' : y^2 = g(x)$ is a 2-covering of its own Jacobian (by example 1.2.5) and again that C is k-isomorphic to C' implies that the Jacobian of $y^2 = g(x)$ is k-isomorphic to E. Denote the homogenization of $g(x)$ by $g(x, z)$. Then we map the equivalence class of (C, π) to the equivalence class of $g(x, z)$.

Well-defined: Suppose that (C, π) and (C', π') are two locally soluble 2-coverings which are equivalent and let $g(x, z)$ and $g'(x, z)$ be their images. Let $\theta : C \to C'$ be a k-isomorphism such that $\pi'\theta = \pi$ and let D and D' be the k-rational divisors of degree 2 on C and C', respectively, coming from lemma 2.1.4. Recall that the complete linear systems $|D|$ and $|D'|$ can be identified with maps $C \to \mathbb{P}^1$ and $C' \to \mathbb{P}^1$, respectively (section 0.2). We note that θ defines a k-isomorphism between the linear systems $|D|$ and $|D'|$. To see this, note that θ already defines a k-isomorphism between the n-covering (C, π) and the n-covering (C', π') and note that the divisor D is linearly equivalent to $2P$ for all $P \in \pi^{-1}\{O\}$ (see the proof of proposition 1.5.2) and similarly the divisor D' is linearly equivalent to $2P'$ for all $P' \in \pi'^{-1}\{O\}$, which implies that $\theta^* D'$ is linearly equivalent to D, and so θ induces an isomorphism between $|D|$ and $|D'|$.

As a consequence, we obtain a commutative diagram

$$\begin{array}{ccc} C & \longrightarrow & \mathbb{P}^1 \\ \downarrow{\scriptstyle \theta} & & \downarrow \\ C' & \longrightarrow & \mathbb{P}^1 \end{array}$$

such that $C \to \mathbb{P}^1$ is defined by $P \mapsto (x(P):1)$ where $1, x$ is a basis of $\mathcal{L}(D)$, $C' \to \mathbb{P}^1$ is defined by $P' \mapsto (x'(P'):1)$ where $1, x'$ is a basis of $\mathcal{L}(D')$, and $\mathbb{P}^1 \to \mathbb{P}^1$ is an k-automorphism of $\mathbb{P}^1$ such that $x' \circ \theta = \frac{\gamma_{11}x+\gamma_{12}}{\gamma_{21}x+\gamma_{22}}$ where $\gamma = \left(\begin{smallmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{smallmatrix}\right) \in \mathrm{GL}_2(k)$ defines such k-automorphism (the entries belong to k because θ is a k-isomorphism).

Now the fact that θ is a k-isomorphism satisfying $\pi'\theta = \pi$ implies that there exists $\mu \in k^*$ such that $g((x,z)\gamma) = \mu g'(x,z)$. To see this, note that if we take a root ξ of $g(x,1)$ then $(\xi, 0) \in \pi^{-1}\{O\}$ which follows from the definition of π (example 1.2.5). If we combine this with the equality $\pi'\theta = \pi$, we obtain that $\theta(\xi,0) \in \pi'^{-1}\{O\}$, i.e. $\theta(\xi,0)$ is of the form $(\xi',0)$ where ξ' is a root of $g'(x,1)$. It follows that when $y = 0$, θ maps bijectively the roots of $g(x,1)$ to the roots of $g'(x,1)$, and this implies that $g((x,z)\gamma)$ and $g'(x,z)$ are forms of degree 4 with the same roots in $\mathbb{P}^1$. Therefore, $g((x,z)\gamma) = \mu g'(x,z)$ for some $\mu \in k^*$.

In order to check that $g(x,z)$ and $g'(x,z)$ are equivalent, it remains to check that μ is of the form λ^2 for some $\lambda \in k^*$. For this, note that the equality $g((x,z)\gamma) = \mu g'(x,z)$ implies that $g'(\frac{\gamma_{11}x+\gamma_{12}}{\gamma_{21}x+\gamma_{22}}, 1) = \mu \frac{g(x,1)}{(\gamma_{21}x+\gamma_{22})^4}$ after dehomogenization. Let y and y' be functions on C and C', respectively, such that $y^2 = g(x,1)$ and $y'^2 = g'(x',1)$. We compose the equality $y'^2 = g'(x',1)$ with θ on both sides to obtain

$$(y' \circ \theta)^2 = g'(x' \circ \theta, 1) = g'(\frac{\gamma_{11}x+\gamma_{12}}{\gamma_{21}x+\gamma_{22}}, 1) = \mu \frac{g(x,1)}{(\gamma_{21}x+\gamma_{22})^4} = \mu \frac{y^2}{(\gamma_{21}x+\gamma_{22})^4}$$

It follows that μ is a square in k^* and so $\mu = \lambda^2$ for some $\lambda \in k^*$. Therefore, $g(x,z)$ and $g'(x,z)$ are equivalent.

Injective: Suppose that (C,π) and (C',π') satisfy that their images $g(x,z)$ and $g'(x,z)$ are equivalent. There exists $\lambda \in k^*$ and $\gamma \in \mathrm{GL}_2(k)$ where $\gamma = \left(\begin{smallmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{smallmatrix}\right)$ and such that $g(x,z) = \lambda^2 g'((x,z)\gamma)$, which after dehomogenizing becomes

$$g(x,1) = \lambda^2(\gamma_{21}x+\gamma_{22})^4 g'(\frac{\gamma_{11}x+\gamma_{12}}{\gamma_{21}x+\gamma_{22}}, 1) \tag{2}$$

Let $\gamma' \in \mathrm{GL}_2(k)$ the inverse matrix of γ, say $\gamma' = \left(\begin{smallmatrix} \gamma'_{11} & \gamma'_{12} \\ \gamma'_{21} & \gamma'_{22} \end{smallmatrix}\right)$ so that

$$\left(\begin{smallmatrix} \gamma'_{11} & \gamma'_{12} \\ \gamma'_{21} & \gamma'_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} \gamma'_{11} & \gamma'_{12} \\ \gamma'_{21} & \gamma'_{22} \end{smallmatrix}\right) \tag{3}$$

We define the morphism $\theta : C \to C'$ given by

$$(x,y) \mapsto (\frac{\gamma_{11}x+\gamma_{12}}{\gamma_{21}x+\gamma_{22}}, \frac{\lambda^{-1}y}{(\gamma_{21}x+\gamma_{22})^2})$$

Here we note that the image of θ is contained in C' thanks to (2) and the fact that $y^2 = g(x,1)$. This morphism has an inverse, namely $\theta' : C' \to C$ given by

$$(x,y) \mapsto (\frac{\gamma'_{11}x+\gamma'_{12}}{\gamma'_{21}x+\gamma'_{22}}, \frac{\lambda y}{(\gamma'_{21}x+\gamma'_{22})^2})$$

Using (3), we can verify that $\theta' \circ \theta = \mathrm{Id}_C$ and that $\theta \circ \theta' = \mathrm{Id}_{C'}$. Also, note that the coefficients of θ are in k. It follows that θ is a k-isomorphism and it remains to check that $\pi'\theta = \pi$. By example 1.2.5, we have $\pi = [2]\phi$ where $\phi(x,y) = [(x,y) - (\xi, 0)]$ and ξ is a root of $g(x,1)$, and similarly $\pi' = [2]\phi'$ where $\phi'(x,y) = [(x,y) - (\xi', 0)]$ and ξ' is a root of $g'(x,1)$. So we want to show

$$[2(x,y) - 2(\xi,0)] = [2(\frac{\gamma_{11}x + \gamma_{12}}{\gamma_{21}x + \gamma_{22}}, \frac{\lambda y}{(\gamma_{21}x + \gamma_{22})^2}) - 2(\xi', 0)] \qquad (4)$$

However, note that the fact that (C, π) and (C', π') are n-coverings of their corresponding Jacobians and the fact that such Jacobians are k-isomorphic imply that θ identifies C with C' in such a way that $\pi^{-1}\{O\}$ is identified with $\pi'^{-1}\{O\}$ under θ. In this identification, (x,y) is identified with $(\frac{\gamma_{11}x+\gamma_{12}}{\gamma_{21}x+\gamma_{22}}, \frac{\lambda y}{(\gamma_{21}x+\gamma_{22})^2})$, so in order to verify (4) it remains to check that $2(\xi, 0)$ is linearly equivalent to $2(\xi', 0)$ under such identification. This is true because the proof of proposition 1.5.2 implies that for any $P, Q \in \pi^{-1}\{O\}$ the divisors $2P$ and $2Q$ are linearly equivalent.

Surjective: If $g(x,z)$ is a binary quartic form such that $C : y^2 = g(x,1)$ is nonsingular and locally soluble with its Jacobian k-isomorphic to E, then example 1.2.5 implies that C is a 2-covering of its own Jacobian which is k-isomorphic to E. In particular, (C, π) as in example 1.2.5 is a 2-covering of E/k. □

2.1.7 Lemma Suppose that $g(x) \in k[x]$ is a quartic such that $C : y^2 = g(x)$ is a nonsingular curve of genus 1 and such that C is also locally soluble, and let I, J be the invariants of $g(x)$. Then the following hold:

(1) The curve C is a 2-covering of the elliptic curve $E : y^2 = x^3 - 27Ix - 27J$ and the invariants of E are $I(E) = 3^4 I, J(E) = 3^6 J$.

(2) If C' is another 2-covering of $y^2 = x^3 - 27Ix - 27J$ and if we let $g'(x) \in k[x]$ be a quartic such that $C : y^2 = g'(x)$ as in proposition 2.1.5, then the invariants of $g'(x)$ are $\lambda^4 I$ and $\lambda^6 J$ for some $\lambda \in k$.

Proof From Example 1.2.5 we know that C is a 2-covering of its Jacobian $E := \mathrm{Jac}(C)$ of C. And using Example 0.4.9 we know that E takes the form $Y^2 = 4X^3 - I'X - J'$ where we have $I' = a_0a_4 - 4a_1a_3 + 3a_2^2$, $J' = a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3$, $g(x) = a_0x^4 + 4a_1x^3 + 6a_2x^2 + 4a_3x + a_4$, $X = \frac{G(x,z)}{y^2z^2}$ and $Y = \frac{H(x,z)}{y^3z^3}$. Make the substitutions $a = a_0$, $b = 4a_1$, $c = 6a_2$, $d = 4a_3$ and $e = a_4$ to obtain $I = 12I'$ and $J = 432J'$ (observation 2.1.3) and so E takes the form $Y^2 = 4X^3 - \frac{I}{12}X - \frac{J}{432}$.

We know that an elliptic curve of the form $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$ can be taken to the form $y^2 = x^3 - 27c_4 - 54c_6$ under the transformation $(x,y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ with $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ (section 1 of chapter III in [17]). Applying this to our case, we have $b_2 = 0$, $b_4 = -\frac{I}{24}$, $b_6 = -\frac{J}{432}$ and $c_4 = I$, $c_6 = \frac{J}{2}$, hence E takes the form $Y^2 = X^3 - 27IX - 27J$ which has invariants $I(E) = -3(-27I) = 3^4 I$, $J(E) = -27(-27J) = 3^6 J$.

Conversely, if C is a 2-covering of $E : y^2 = x^3 - 27Ix - 27J$, take $g'(x)$ such that $C : y^2 = g'(x)$ (corollary 2.1.7) and let I', J' be the invariants of $g'(x)$. By the first implication, we know that $y^2 = g'(x)$ is a 2-covering of $E' : y^2 = x^3 - 27I'x - 27J'$. Finally, since the Jacobian $E = \mathrm{Jac}(C) : y^2 = x^3 - 27Ix - 27J$ is unique up to k-isomorphism, we should have $E \cong E'$ and we use lemma 0.4.7 to find some $\lambda \in k$ such that $-27I' = \lambda^4(-27I)$ and $-27J' = \lambda^6(-27J)$, implying $I' = \lambda^4 I$ and $J' = \lambda^6 J$. □

So we have the following. By corollary 1.2.10 there is a bijection between $\mathrm{Sel}_2(E/k)$ and the set of k-equivalence classes of locally soluble 2-coverings of E/k. Also, by proposition 2.1.6 there is a bijection between the equivalence classes of locally soluble 2-coverings of E/k and the equivalence classes of binary quartic forms $g(x, z)$ such that $y^2 = g(x, 1)$ is nonsingular, locally soluble, and its Jacobian is k-isomorphic to E. If we combine these two results with lemma 2.1.7, we obtain the following theorem.

2.1.8 Theorem For an elliptic curve E/k with invariants $I(E), J(E)$, there is a bijection between $\mathrm{Sel}_2(E/k)$ and the set of equivalence classes of binary quartic forms $g(x, z)$ having invariants $\lambda^4 I(E)$ and $\lambda^6 J(E)$ for some $\lambda \in k^*$ and such that $y^2 = g(x, 1)$ is locally soluble.

Proof: We identify $\mathrm{Sel}_2(E/k)$ with the set of k-equivalence classes of locally soluble 2-coverings of E/k. By proposition 2.1.6, the latter is identified with the set of equivalence classes of binary quartic forms $g(x, z)$ such that $C : y^2 = g(x, 1)$ is locally soluble and the Jacobian of C is k-isomorphic to E. We should identify this set with the set of equivalence classes of binary quartic forms $g(x, z)$ having invariants $\lambda^4 I(E)$ and $\lambda^6 J(E)$ for some $\lambda \in k^*$ and such that $y^2 = g(x, 1)$ is locally soluble. So it suffices to show if $g(x, z)$ is such that the Jacobian of $C : y^2 = g(x, 1)$ is k-isomorphic to E, then the invariants of $g(x, z)$ are $\lambda^4 I(E)$ and $\lambda^6 J(E)$ for some $\lambda \in k^*$, and conversely, if $g(x, z)$ has invariants $\lambda^4 I(E)$ and $\lambda^6 J(E)$ for some $\lambda \in k^*$, then the Jacobian of C is k-isomorphic to E.

Suppose that the Jacobian of $C : y^2 = g(x, 1)$ is k-isomorphic to E. By the proof of lemma 2.1.7, the Jacobian of C is given by $y^2 = x^3 - 27Ix - 27J$. Suppose that E is of the form $E : y^2 = x^3 + Ax + B$ for some $A, B \in k$ and let I, J be the invariants of $g(x, z)$. Since E and the Jacobian of C are k-isomorphic, lemma 0.4.7 implies that we can find some $s \in k$ such that $-27I = s^4 A$, $-27J = s^6 B$, and since $I(E) = -3A$, $J(E) = -27B$ we obtain $3^4 I = s^4 I(E)$ and $3^6 I = s^6 J(E)$. This yields $I = \lambda^4 I(E)$ and $J = \lambda^6 J(E)$ for some $\lambda \in k$.

Now suppose that $g(x, z)$ has invariants $I := \lambda^4 I(E)$ and $J := \lambda^6 J(E)$ for some $\lambda \in k$. By lemma 2.1.7 and its proof, we obtain in particular that $C : y^2 = g(x, 1)$ has Jacobian $E' : y^2 = x^3 - 27Ix - 27J$, i.e. $E' : y^2 = x^3 - 27\lambda^4 I(E)x - 27\lambda^6 J(E)$. On the other hand, E is of the form $E : y^2 = x^3 + Ax + B$ for some $A, B \in k$, which is equivalent to $E : y^2 = x^3 - \frac{I(E)}{3}x - \frac{J(E)}{27}$ because $I(E) = -3A$ and $J(E) = -27B$. The map from $E : y^2 = x^3 - \frac{I(E)}{3}x - \frac{J(E)}{27}$ to $E' : y^2 = x^3 - 27\lambda^4 I(E)x - 27\lambda^6 J(E)$ defined by $(x, y) \mapsto (3^2\lambda^2 x, 3^3\lambda^3 y)$ is a k-isomorphism, so the Jacobian of C and E are k-isomorphic. □

2.2 The case $n = 3$

Now we study the bijection in the case $n = 3$. Consider any ternary cubic form $U(x, y, z) = ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz$ with coefficients in k. We introduce the notion of equivalent and properly equivalent ternary cubic forms.

2.2.1 Definition If $U(x, y, z)$ is a ternary cubic form, the action of $\mathrm{GL}_3(k)$ on $U(x, y, z)$ is defined as $g \cdot U(x, y, z) := U((x, y, z) \cdot g)$ where $g \in \mathrm{GL}_3(k)$. Two ternary cubic forms $U_1(x, y, z)$ and $U_2(x, y, z)$ are equivalent if there exists $\gamma \in k^*$ and $g \in \mathrm{GL}_3(k)$ such that $U_2(x, y, z) = \gamma(gU_1(x, y, z))$. If we can choose $\gamma := \det(g)^{-1}$, then U_1 and U_2 are properly equivalent.

2.2.2 Definition (i) The Aronhold's invariants $S(U)$ and $T(U)$ of a ternary cubic form $U(x, y, z)$ of the form $ax^3 + by^3 + cz^3 + 3a_2x^2y + 3a_3x^2z + 3b_1xy^2 + 3b_3y^2z + 3c_1xz^2 + 3c_2yz^2 + 6mxyz \in k[x, y, z]$ are expressions defined in terms of the coefficients $a, b, c, a_2, a_3, b_1, b_3, c_1, c_2, m$. We define $S(U)$ as in (3.4), page 309 of [1]. Similarly, we define $T(U)$ as in (3.5), page 310 of [1].

(ii) The invariants $I(U)$ and $J(U)$ of a ternary cubic form $U(x, y, z)$ are defined as $I(U) := -81S(U)$ and $J(U) := \frac{729}{4}T(U)$, where $S(U)$ and $T(U)$ are the Aronhold's invariants.

(iii) The Hessian of a ternary cubic form $U(x, y, z)$ of the form $ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz$ is defined as another ternary cubic form given by $H(U)(x, y, z) := (-\frac{1}{2})\det \begin{pmatrix} U_{xx} & U_{xy} & U_{xz} \\ U_{xy} & U_{yy} & U_{yz} \\ U_{xz} & U_{yz} & U_{zz} \end{pmatrix}$. If we let $I := I(U)$, $J := J(U)$ be the invariants of the ternary cubic form $U(x, y, z)$ and if we consider any $\lambda, \mu \in k$, then the Hessian $H(U)(x, y, z)$ satisfies the relation $H(\lambda U + \mu H(U)) = 48(I\lambda^2\mu + 4J\lambda\mu^2 + 16I^2\mu^3)U + (\lambda^3 - 48I\lambda\mu^2 - 64J\mu^3)H(U)$.

The following lemma is also useful.

2.2.3 Lemma: If two ternary cubic forms with coefficients in k are properly equivalent, then they have the same invariants. If k is algebraically closed, then the converse is true.

Proof: See lemma 2.2 in [8]. □

Note that any nonsingular cubic form U with coefficients in k defines a morphism $C \to \mathbb{P}^2$ where C/k is given by $U(x, y, z) = 0$. Further, such a curve C/k is equipped with a regular 1-form, namely $\omega := \frac{z^2 d(\frac{y}{z})}{U_x}$ where U_x denotes the partial derivative of $U(x, y, z)$ with respect to x. We denote this pair by $([C \to \mathbb{P}^2], \omega)$. For the bijection in the case $n = 3$ the following lemma is important:

2.2.4 Lemma: Suppose U_1 and U_2 are nonsingular cubic forms such that there exists $g \in \mathrm{GL}_3(\bar{k})$ satisfying $g \cdot U_1 = U_2$, i.e. $U_1((x, y, z) \cdot g) = U_2(x, y, z))$.

Let $\phi : C_2 \to C_1$ be the $\overline{k}$-isomorphism defined by $\phi(x : y : z) = (x : y : z)g = (g_{11}x + g_{21}y + g_{31}z : g_{12}x + g_{22}y + g_{32}z : g_{13}x + g_{23}y + g_{33}z)$ where $g = \left(\begin{smallmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{smallmatrix}\right)$, and where the pair $([C_1 \to \mathbb{P}^2], \omega_1)$ corresponds to U_1 and the pair $([C_2 \to \mathbb{P}^2], \omega_2)$ corresponds to U_2. Then $\phi^*\omega_1 = \det(g)\omega_2$.

Proof: We look at matrices of the form $\left(\begin{smallmatrix} \gamma_1 & 0 & 0 \\ 0 & \gamma_2 & 0 \\ 0 & \mu & \gamma_3 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. These matrices generate $\mathrm{GL}_3(\overline{k})$.

If $\left(\begin{smallmatrix} \gamma_1 & 0 & 0 \\ 0 & \gamma_2 & 0 \\ 0 & \mu & \gamma_3 \end{smallmatrix}\right)U_1 = U_2$ then $U_1(\gamma_1 x, \gamma_2 y + \mu z, \gamma_3 z) = U_2(x, y, z)$, so by the chain rule we have $\frac{\partial U_2}{\partial x} = \frac{\partial U_1(\gamma_1 x, \gamma_2 y + \mu z, \gamma_3 z)}{\partial x} = \gamma_1 \frac{\partial U_1}{\partial x}(\gamma_1 x, \gamma_2 y + \mu z, \gamma_3 z)$. By following the definitions, we observe that $\phi^*(x) = \gamma_1 x$, $\phi^*(y) = \gamma_2 y + \mu z$ and $\phi^*(z) = \gamma_3 z$ and so $\phi^*(\frac{\partial U_1}{\partial x}) = \frac{\partial U_1}{\partial x}(\gamma_1 x, \gamma_2 y + \mu z, \gamma_3 z)$. Therefore, we have

$$\phi^*\omega = \phi^*\left(\frac{z^2 d(\frac{y}{z})}{\frac{\partial U_1}{\partial x}}\right) = \frac{\gamma_3^2 z^2 d(\frac{\gamma_2 y + \mu z}{\gamma_3 z})}{\frac{1}{\gamma_1}\frac{\partial U_2}{\partial x}} = \gamma_1\gamma_2\gamma_3 \frac{d(\frac{y}{z})}{\frac{\partial U_2}{\partial x}}$$

and $\gamma_1\gamma_2\gamma_3$ is the determinant of the matrix $\left(\begin{smallmatrix} \gamma_1 & 0 & 0 \\ 0 & \gamma_2 & 0 \\ 0 & \mu & \gamma_3 \end{smallmatrix}\right)$.

For the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$ we use the relation $\frac{y}{z}d(\frac{z}{y}) + \frac{z}{y}d(\frac{y}{z}) = 0$ which implies $y^2 d(\frac{z}{y}) = -z^2 d(\frac{y}{z})$. If $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)U_1 = U_2$ then $U_1(x, z, y) = U_2(x, y, z)$ and by the chain rule again we have $\frac{\partial U_2}{\partial x} = \frac{\partial U_1(x,z,y)}{\partial x}$. Also, we obtain $\phi^*(x) = x$, $\phi^*(y) = z$ and $\phi^*(z) = y$. So we have

$$\phi^*\omega = \phi^*\left(\frac{z^2 d(\frac{y}{z})}{\frac{\partial U_1}{\partial x}}\right) = \frac{y^2 d(\frac{z}{y})}{\frac{\partial U_1}{\partial x}(x, z, y)} = \frac{y^2 d(\frac{z}{y})}{\frac{\partial U_1(x,z,y)}{\partial x}} = -z^2 \frac{d(\frac{y}{z})}{\frac{\partial U_2}{\partial x}}$$

where we are using that $\frac{\partial U_1(x,z,y)}{\partial x} = \frac{\partial U_1}{\partial x}(x, z, y) = \phi^*(\frac{\partial U_1}{\partial}(x, y, z))$. Since the determinant of $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$ is -1 then we conclude this case.

For $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ we use the relation $\frac{1}{z^2}\frac{U}{\partial x}d(\frac{x}{z}) + \frac{1}{z^2}\frac{\partial U}{\partial y}d(\frac{y}{z}) = 0$. We note that the equality $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)U_1 = U_2$ implies $U_1(y, x, z) = U_2(x, y, z)$ and also note that $\phi^*(x) = y$, $\phi^*(y) = x$ and $\phi^*(z) = z$, so

$$\phi^*\left(z^2 \frac{d(\frac{y}{z})}{\frac{U_1(x,y,z)}{\partial x}}\right) = z^2 \frac{d(\frac{x}{z})}{\frac{\partial U_1}{\partial x}(y, x, z)}$$

But we want to prove that

$$z^2 \frac{d(\frac{x}{z})}{\frac{\partial U_1}{\partial x}(y, x, z)} = (-1)z^2 \frac{d(\frac{y}{z})}{\frac{\partial U_2(x,y,z)}{\partial x}}$$

because the determinant of the matrix is -1, and so we want

$$\frac{1}{z^2}\frac{\partial U_2}{\partial x}(y, x, z)d(\frac{x}{z}) + \frac{1}{z^2}\frac{\partial U_1(x, y, z)}{\partial y}d(\frac{y}{z}) = 0$$

However, we know that $U_1(y,x,z) = U_2(x,y,z)$ and so we want

$$\frac{1}{z^2}\frac{\partial U_1}{\partial x}(x,y,z)d(\frac{x}{z}) + \frac{1}{z^2}\frac{\partial U_1(x,y,z)}{\partial y}d(\frac{y}{z}) = 0$$

but this is true by example 0.1.1 of Chapter 0. □

Recall that in Chapter 1 we parametrized the set of k-equivalence classes of twists $([C \to S], \omega)$ of $([E \to \mathbb{P}^{n-1}], \omega_E)$ by $H^1(k, E[n])$. Now we will restrict this bijection to the kernel of the obstruction map which is contained in $H^1(k, E[n])$ and find out what it corresponds to. In order to do this, for convenience we denote by ω_U the differential 1-form $\frac{z^2 d(\frac{y}{z})}{\frac{\partial U}{\partial x}(x,y,z)}$ associated to a ternary cubic form $U(x,y,z)$. Now suppose that we are in the situation of lemma 2.2.4. Then we have

$$\begin{aligned}\phi^*\omega_{U_1} &= \det(g)\omega_{U_2} \\ &= \det(g)\omega_{g\cdot U_1}\end{aligned}$$

where the first equality is lemma 2.2.4 and the second equality holds because $U_2 = g \cdot U_1$ by hypothesis of lemma 2.2.4. So we have

$$\phi^*\omega_{U_1} = \det(g)\omega_{g\cdot U_1} \tag{5}$$

Next, for any $\lambda \in k$ and any ternary cubic form $U(x,y,z)$ with associated differential 1-form ω_U, we have

$$\omega_{\lambda U} = \lambda^{-1}\omega_U \tag{6}$$

which follows directly from the definition.

We will need (5) and (6) to prove the following bijection.

2.2.5 Proposition For an elliptic curve E/k with invariants $I(E), J(E)$, there is a bijection between the set of properly k-equivalence classes of ternary cubic forms with invariants equal to $I(E), J(E)$, and $\ker(\mathrm{Ob}) \subseteq H^1(k, E[3])$.

Proof: Given a ternary cubic form $U(x,y,z) = 0$, consider $C : U(x,y,z) = 0$ to obtain an embedding $C \to \mathbb{P}^2$. Next, we consider the differential 1-form ω_U on C to obtain the pair $([C \to \mathbb{P}^2], \omega_U)$. We have to show that the map $U \mapsto ([C \to \mathbb{P}^2], \omega_U)$ defines a bijection between the set of properly equivalent ternary cubic forms with invariants $I(E), J(E)$, and $\ker(\mathrm{Ob})$. Recall that the elements in $\ker(\mathrm{Ob})$ correspond to the k-isomorphism classes of twists $([C \to S], \omega_U)$ of $([E \to \mathbb{P}^2], \omega_{U_E})$ such that $S \cong \mathbb{P}^2$ over k, where U_E is the Weierstrass form of E and ω_{U_E} is the invariant differential of E.

Well-defined: First we should check that if U is a ternary cubic form with invariants $I(E)$ and $J(E)$, then the corresponding $([C \to \mathbb{P}^2], \omega_U)$ is indeed a twist of $([E \to \mathbb{P}^2], \omega_{U_E})$. By viewing U and U_E as ternary cubic forms with coefficients in $\overline{k}$ and using that U andU_E have the same invariants by hypothesis,

we can apply the converse of lemma 2.2.3 to obtain that U and U_E are properly equivalent. This means that there exists $g \in \mathrm{GL}_3(\overline{k})$ such that $U(x,y,z) = \det(g)^{-1} g \cdot U_E(x,y,z)$, or equivalently $\det(g)U(x,y,z) = g \cdot U_E(x,y,z)$. Using this and the fact that the $\overline{k}$-automorphisms of $\mathbb{P}^2$ are given by $\mathrm{PGL}_2(\overline{k})$, we obtain a $\overline{k}$-isomorphism $\phi : C \to E$ and a $\overline{k}$-automorphism $\mathbb{P}^2 \to \mathbb{P}^2$ induced by g such that $\phi(x:y:z) = (x:y:z)g$ and such that the following diagram

$$\begin{array}{ccc} C & \longrightarrow & \mathbb{P}^2 \\ \downarrow{\scriptstyle \phi} & & \downarrow \\ E & \longrightarrow & \mathbb{P}^2 \end{array}$$

is commutative. In particular, we are in the situation of lemma 2.2.4, and therefore we can apply (5).

From (5), the equality $\det(g)U(x,y,z) = g \cdot U_E(x,y,z)$, and (6) we obtain

$$\begin{aligned} \phi^* \omega_{U_E} &= \det(g)\omega_{g \cdot U_E} \\ &= \det(g)\omega_{\det(g)U} \\ &= \det(g)\det(g)^{-1}\omega_U \\ &= \omega_U \end{aligned}$$

It follows that $([C \to \mathbb{P}^2], \omega_U)$ is a twist of $([E \to \mathbb{P}^2], \omega_{U_E})$.

Now suppose that U_1, U_2 are properly equivalent ternary cubic forms (both with invariants $I(E), J(E)$), so that $U_2(x,y,z) = (\det(g))^{-1} g \cdot U_1(x,y,z)$ for some $g \in \mathrm{GL}_3(k)$, or equivalently $\det(g)U_2(x,y,z) = g \cdot U_1(x,y,z)$. We want to show that their corresponding images $([C_1 \to \mathbb{P}^2], \omega_1)$ and $([C_2 \to \mathbb{P}^2], \omega_2)$ are k-isomorphic. Note that the equality $\det(g)U_2(x,y,z) = g \cdot U_1(x,y,z)$ and the fact that the k-automorphisms of $\mathbb{P}^2$ are given by $\mathrm{PGL}_3(k)$ imply that we can find a k-isomorphism $\phi : C_2 \to C_1$ and a k-automorphism $\mathbb{P}^2 \to \mathbb{P}^2$ induced by g such that $\phi(x:y:z) = (x:y:z)g$ and the following diagram

$$\begin{array}{ccc} C_2 & \longrightarrow & \mathbb{P}^2 \\ \downarrow{\scriptstyle \phi} & & \downarrow \\ C_1 & \longrightarrow & \mathbb{P}^2 \end{array}$$

is commutative. In particular, we are in the situation of lemma 2.2.4 and therefore we can apply (5).

From (5), the equality $\det(g)U_2(x,y,z) = g \cdot U_1(x,y,z)$, and (6) we obtain

$$\begin{aligned} \phi^* \omega_{U_1} &= \det(g)\omega_{g \cdot U_1} \\ &= \det(g)\omega_{\det(g)U_2} \\ &= \det(g)\det(g)^{-1}\omega_{U_2} \\ &= \omega_{U_2} \end{aligned}$$

It follows that $([C_1 \to \mathbb{P}^2], \omega_1)$ and $([C_2 \to \mathbb{P}^2], \omega_2)$ are k-isomorphic.

Injective: Consider two ternary cubic forms $U_1(x, y, z)$, $U_2(x, y, z)$, both with invariants $I(E), J(E)$, such that their corresponding images $([C_1 \to \mathbb{P}^2], \omega_{U_1})$, $([C_2 \to \mathbb{P}^2], \omega_{U_2})$ are k-isomorphic. This means that there is a k-automorphism of $\mathbb{P}^2$ induced by some matrix $g \in \mathrm{GL}_n(k)$ and a k-isomorphism $\phi : C_2 \to C_1$ such that $\phi(x : y : z) = (x : y : z)g$ and such that the diagram

$$\begin{array}{ccc} C_2 & \longrightarrow & \mathbb{P}^2 \\ \downarrow{\scriptstyle \phi} & & \downarrow \\ C_1 & \longrightarrow & \mathbb{P}^2 \end{array}$$

is commutative. In particular, we are in the situation of lemma 2.2.4 and we can apply (5). Note that this diagram implies that there exists some $\lambda \in k$ such that

$$\lambda U_2 = g \cdot U_1 \tag{7}$$

.

By applying (5), (6), and (7) we obtain

$$\begin{aligned} \phi^* \omega_{U_1} &= \det(g) \omega_{g \cdot U_1} \\ &= \det(g) \omega_{\lambda U_2} \\ &= \det(g) \lambda^{-1} \omega_{U_2} \end{aligned}$$

But we know that $\phi^* \omega_{U_1} = \omega_{U_2}$ by hypothesis. This implies that $\det(g)\lambda^{-1} = 1$, or equivalently $\lambda = \det(g)$. By substituting this into (7), we obtain that U_1 and U_2 are properly equivalent.

Surjective: Suppose that $([C \to \mathbb{P}^2], \omega_U)$ is a twist of $([E \to \mathbb{P}^2], \omega_{U_E})$, where U is the ternary cubic form which defines C (note that C has genus 1, and this implies that it's defined by some cubic form U). We have a commutative diagram

$$\begin{array}{ccc} C & \longrightarrow & \mathbb{P}^2 \\ \downarrow{\scriptstyle \phi} & & \downarrow \\ E & \longrightarrow & \mathbb{P}^2 \end{array}$$

where $\mathbb{P}^2 \to \mathbb{P}^2$ is a $\overline{k}$-automorphism of $\mathbb{P}^2$ induced by some matrix $g \in \mathrm{GL}_3(\overline{k})$ and ϕ is a $\overline{k}$-isomorphism such that $\phi(x : y : z) = (x : y : z)g$. In particular, we are in the situation of lemma 2.2.4 and again we can apply (5). Also, note that the diagram implies that there exists some $\lambda \in \overline{k}$ such that

$$\lambda U = g \cdot U_E \tag{8}$$

By applying (5), (6), and (8) we obtain

$$\begin{aligned}\phi^*\omega_{U_E} &= \det(g)\omega_{g\cdot U_E}\\ &= \det(g)\omega_{\lambda U}\\ &= \det(g)\lambda^{-1}\omega_U\end{aligned}$$

But we know that $\phi^*\omega_{U_E} = \omega_U$ by hypothesis. This implies that $\det(g)\lambda^{-1} = 1$, or equivalently $\lambda = \det(g)$. After substituting this into (8), we obtain that U and U_E are properly equivalent. Now we apply lemma 2.2.3 to conclude that U and U_E have the same invariants. Then U is the ternary cubic form that we wanted. □

With the previous proposition we get the following diagram

$$\begin{array}{ccc}
\left\{\begin{array}{c}k\text{-isomorphism classes of twists}\\ [C \to S, \omega] \text{ of } [E \to \mathbb{P}^2, \omega_E]\\ \text{such that } S \text{ is locally soluble (hence } S \cong \mathbb{P}^2)\end{array}\right\} & \subseteq & \left\{\begin{array}{c}k\text{-isomorphism}\\ \text{classes of twists}\\ [C \to S, \omega] \text{ of } [E \to \mathbb{P}^2, \omega_E]\end{array}\right\}\\
\updownarrow & & \updownarrow\\
\ker(\mathrm{Ob}) & \subseteq & H^1(k, E[3])\\
\updownarrow & & \\
\left\{\begin{array}{c}k\text{-isomorphism classes of}\\ \text{ternary cubic forms having invariants } I(E), J(E)\end{array}\right\} & &
\end{array}$$

The final step is to prove that $\mathrm{Sel}_3(E/k) \subseteq \ker(\mathrm{Ob})$. If we prove this, then we obtain the following diagram

$$\begin{array}{ccc}
\mathrm{Sel}_3(E/k) & \subseteq & \ker(\mathrm{Ob})\\
\updownarrow & & \updownarrow\\
\left\{\begin{array}{c}k\text{-isomorphism classes of}\\ \text{locally soluble ternary cubic forms}\\ \text{having invariants } I(E), J(E)\end{array}\right\} & \subseteq & \left\{\begin{array}{c}k\text{-isomorphism classes of}\\ \text{ternary cubic forms}\\ \text{having invariants } I(E), J(E)\end{array}\right\}
\end{array}$$

Recall that $H^1(k, E[n])$ is parametrized by the set of k-equivalence classes of Brauer-Severi diagrams $[C \to S]$ of dimension $n-1$, and also recall that we defined the obstruction map $\mathrm{Ob} : H^1(k, E[n]) \to \mathrm{Br}(k)$, where $\mathrm{Br}(k)$ is the Brauer group of k, by $[C \to S] \mapsto [S]$. Thanks to lemma 1.3.4, the obstruction map coincides with the map which sends $([C \to S], \omega)$ to $[S]$.

Next, we note that the proof of theorem 1.4.2 and remark 1.4.4 imply that the k-equivalence class of a Brauer-Severi diagram $[C \to S]$ of dimension $n-1$ will correspond to the k-equivalence class of a n-covering of E/k of the form (C, π), i.e. the underlying smooth curve of genus 1 is still C. And it follows again from lemma 1.3.4 that the k-equivalence class of a twist $([C \to S], \omega)$ of $([E \to \mathbb{P}^{n-1}], \omega_E)$ will correspond to the same k-equivalence class of (C, π) (again, the underlying curve C is the same).

Using these observations, we obtain the following theorem.

2.2.6 Theorem: Given an elliptic curve E/k with invariants $I(E), J(E)$, there is a bijection between $\mathrm{Sel}_3(E/k)$ and the set of properly k-equivalence classes of locally soluble ternary cubic forms having invariants $I(E)$ and $J(E)$.

Proof: First we note that $\mathrm{Sel}_3(E/k) \subseteq \ker(\mathrm{Ob})$. To see this, we already know that $\mathrm{Sel}_3(E/k)$ is in bijection with the k-equivalence classes of locally soluble 3-coverings (C, π) of E/k. It follows that $\mathrm{Sel}_3(E/k)$ is also parametrized by the k-equivalence classes of Brauer-Severi diagrams $[C \to S]$ of dimension 2 such that C is locally soluble and by the k-equivalence classes of twists $([C \to S], \omega)$ of $([E \to \mathbb{P}^{n-1}], \omega_E)$ such that C is locally soluble. In both cases we have $C(k_v) \neq \emptyset$ for every place v which implies that $S(k_v) \neq \emptyset$ for every place v. But S is a Brauer-Severi variety, and so $S(k) \neq \emptyset$ which implies that S is k-isomorphic to $\mathbb{P}^{n-1}_k$. Therefore, the class of S in $\mathrm{Br}(k)$ is the zero element of this group.

Now, the previous paragraph implies that $\mathrm{Sel}_3(E/k)$ is parametrized by the k-equivalence classes of twists $([C \to S], \omega)$ with $S \cong \mathbb{P}^{n-1}$ over k and C locally soluble, whereas proposition 2.2.5 and its proof imply that we can identify $\ker(\mathrm{Ob})$ with the properly k-equivalence classes of ternary cubic forms with invariants $I(E), J(E)$. Since $\mathrm{Sel}_3(E/k) \subseteq \ker(\mathrm{Ob})$, it follows that $\mathrm{Sel}_3(E/k)$ is parametrized by the properly k-equivalence classes of *locally soluble* ternary cubic forms with invariants $I(E), J(E)$. □

References

[1] S. Y. An, S. Y. Kim, D.C. Marshall, S. H. Marshall, W. G. McCallum, and A. H. Perlis, *Jacobians of Genus One Curves*, J. Number Theory **90** (2001), no. 2, 304-315.

[2] M. Bhargava, A. Shankar, *Binary Quartic Forms Having Bounded Invariants, and the Boundedness of the Average Rank of Elliptic Curves*, http://arxiv.org/abs/1006.1002 (2010).

[3] M. Bhargava, A. Shankar, *Ternary Cubic Forms Having Bounded Invariants, and the Existence of a Positive Proportion of Elliptic Curves Having Rank 0*, http://arxiv.org/abs/1007.0052 (2003).

[4] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves I*, J. Reine Angew. Math. **212** (1963), 7-25.

[5] J. W. S. Cassels, *Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95-112.

[6] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Stud. Texts **24**, Cambridge University Press (1991).

[7] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-Descent on Elliptic Curves, I. Algebra*, J. Reine Angew. Math. **615** (2008), 121-155.

[8] T. Fisher, *Testing Equivalence of Ternary Cubics*, Algorithmic Number Theory, Lecture Notes in Comput. Sci. **4076**, Springer, (2006), 333-345.

[9] R. Hartshorne, *Algebraic Geometry*, GTM **52**, Springer-Verlag (1977).

[10] W. Hurlimann, *A Short Proof of the Albert-Brauer-Hasse-Noether Theorem*, Journées Arithmétiques de Genève, Astérisque **209** (1992), 215-220.

[11] J. Jahnel, *The Brauer-Severi Variety Associated With a Central Simple Algebra: A Survey*, Linear Algebraic Groups and Related Structures **52** (2000), 1-60.

[12] S. Lichtenbaum, *The Period-Index Problem for Elliptic Curves*, Amer. J. Math. **90** (1968), 1209-1223.

[13] P. Morandi, *Field and Galois Theory*, GTM **167**, Springer-Verlag (1996).

[14] C. O'Neil, *The Period-Index Obstruction for Elliptic Curves*, J. Number Theory **95** (2002), no. 2, 329-339.

[15] S. Schmitt, H. G. Zimmer, *Elliptic Curves: A Computational Approach*, de Gruyter Studies in Mathematics **31**, Walter de Gruyter & Co. (2003).

[16] J. P. Serre, *Local Fields*, GTM **67**, Springer-Verlag (1979).

[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag (1986).