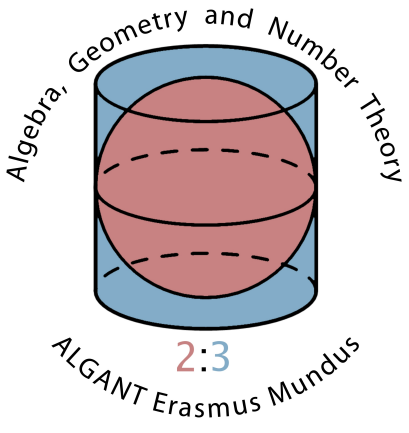

Torsor Dual Pairs

Carles Checa Nualart

Thesis advisor: Peter Bruin

Università degli Studi di Padova

Universiteit Leiden

Universittà degli Studi di Padova. Dipartamento di Matematica.
Universiteit Leiden. Mathematisch Instituut.
Academic year 2019-2020

Acknowledgements

The ALGANT experience was a short but very intense period of two years on which I could develop myself both as person and mathematician. This means that I feel very grateful to all the people that, in their way, have allowed me to live it.
Firstly, I would like to thank Oscar Rivero, who mentioned ALGANT to me, in the first place. His enthusiasm during the year 2017-18, showing me the beauty of algebra and number theory and tutorizing my Bachelor's thesis was of great importance on developing my passion for these topics. I would also like to thank Jordi Quer, for showing to me the elegance of maths in the courses of algebraic structures and Galois theory.
I would like to thank all the members of the ALGANT consistorium, which accepted me in the first place and helped me during these two years. The possibility of studying in two different universities abroad, meeting an amount of collegues from different countries and knowing the work of many researchers is the dream of any young mathematician.
I would like to thank the university of Padova for their compaion during the academic year 2018-19. The student ambient of the city is something every student around the world would like to enjoy
I would like to thank Leiden university teachers who have helped me during the last year and made my stay there very confortable. I would specially like to mention my thesis director Peter Bruin who, in times of coronavirus, has devoted all the time that he could to the best success of this work.
As every experience of this kind, it wouldn't have been the same without the people with which I shared maths and life in Padova and Leiden. I would like to mention Giacomo Negrisolo, Mael Denys, Margherita Pagano, Fabio Buccoliero, Pietro Capovilla, Kelvin Lian, Phrador Sanhiery, Njaka Andriamandratomanana and many others.
Thanks also to all my group of friends from Leiden and Padova which, in their diversity and desire to have a good time, made my stay in both cities an unforgettalbe experience.

Finalment, vull agrair a la meva família. Als meus pares, Andrés i Elisabet, que tot i les ansietats del moment i la distància, han sabut fer-me notar el seu amor i suport durant aquests dos anys. Al meu germà Martí, per fer de referent durant tant de temps. I als meus avis, especialment les meves dues avies Luisa i María Helena, que com ningú han sabut ferme veure lo magnífic que és disfrutar d'aquestes experiències, fent acte de presència tant a Itàlia com a Holanda.

Contents

0 Introduction and preliminaries of group schemes

The idea of associating dual pairs of algebras to finite commutative group schemes was introduced by Peter Bruin in [1] with the intention of making these structures more easily computed in the practical methods. The paper didn't only focus on group schemes, but made a broader picture of closer objects to which this construction could be helpful at the computational level such as Galois representations or modular forms.

Apart from that, he left a window open to future research when he thought of torsors over these group schemes, which are basically schemes on which these groups act in a geometrically interesting way. My initial ambitious idea was to be as general as possible, studying the first cohomology groups $H^1_\tau(S, \mathcal{G})$ that parametrize these torsors for a general group scheme over a base S in a suitable topology τ. With that information, I hoped to be able to construct some kind of dual pairs of algebras.

As it often happens in maths, bigger tasks cannot be understood if one does not give all the details of the smaller and easier cases. That is why this thesis focuses on two particular types of group schemes for which the task is easier to fulfill. These two objects are the finite commutative group schemes μ_n and $E[n]$ where E is an elliptic curve and $n > 0$. The reason these objects are the easier to understand is because their cohomologies come related to objects for which we know a lot about their structure. For instance, μ_n appears in the Kummer short exact sequence of sheaves:

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 1$$

and these allows us to relate $H^1(S, \mu_n)$ with other familiar objects by cutting the long exact sequence of cohomology to:

$$1 \to \mathbb{G}_m(S)/\mathbb{G}_m(S)^n \to H^1(S, \mu_n) \to \mathrm{Pic}(S)[n] \to 1.$$

We can relate the objects to the units and the class group of the base scheme and we will be closer to computing the torsors. For instance, suppose K is a number field and $S = \mathrm{Spec}(\mathcal{O}_{K,\mathcal{S}})$ where $\mathcal{S}$ is a finite set of prime ideals. Then, we can write a similar short exact sequence:

$$1 \to \mathcal{O}^\times_{K,\mathcal{S}}/\mathcal{O}^{\times n}_{K,\mathcal{S}} \to K_S(n) \to \mathrm{Cl}(K)[n] \to 1$$

where $K_S(n)$ is formed by elements of $K^\times$ up to powers, such that their valuation at the ideals not in $\mathcal{S}$ is an n-th power. This sequence appears in [3]. This suggests that we can find an isomorphism between $K_S(n)$ and $H^1(S, \mu_n)$, sending the elements $a \in K_S(n)$ to certain finite algebras $\mathcal{X}_a$ and with them, constructing the torsors $X_a = \mathrm{Spec}\,\mathcal{X}_a$. More generally, this will work for S any Dedekind scheme which are integral Noetherian normal schemes of dimension 1. In particular, we will relate these groups with the Selmer groups, seeing that these torsors become locally trivial when seen as $\mathbb{G}_m$-torsors.

In the case of elliptic curves over a field K, we also have an short exact sequence. Namely,

$$1 \to E[n] \to E \xrightarrow{n} E \to 1$$

which, together with the embeddings at each completion of K, gives us the short exact sequence:

$$1 \to E(K)/nE(K) \to \mathrm{Sel}^n(E, K) \to Ш(E, K)[n] \to 1.$$

The art of moving along this short exact sequence is the descent method. Our goal is to study explicitly these methods in the literature, specially in [6], [11] or [21]. They give a few characterizations of the objects in $H^1(K, E[n])$ and map them inside the group $R^\times/R^{\times n}$ where R is the algebra of Galois equivariant maps from $E[n]$ to $\overline{\mathbb{Q}}$, as well as the ring of coordinate functions. By explicit descent, the literature refers to finding the image of these maps by putting some conditions on the elements of R. The maps will be injective only when n is prime, and [8] uses other methods of explicit descent when n is not prime, which might also work for computing the dual pairs. However, all the examples added in this thesis deal with $n = 2, 3$.

There are many ways to add these conditions. The first is the one used in [20], which reduces to computing the norm on the elements of R and then adding some local conditions, which guarantee that our elements are

in the Selmer group. These computations are easier but only work for $n = 2$. The second ones, used in [21], also deal with norm conditions in a more sophisticated way and add restrictions on the elements of $E[n]$ as a G-module, where G is the absolute Galois group of K. Moreover, there is a big simplification added in [20] and [21], which reduces the local computations to a finite number of primes. In fact, there is no reason for the dual pairs that we intend to construct to be representing Selmer group elements, as we could just write down the elements on $H^1(K, E[n])$, representing curves that don't have to be locally solvable. The reason of the focus on the Selmer group is due to the fact it was easier to relate it to the already implemented methods, having a reference for comparing our results.

Once performed the descent, our goal is to use it in order to write the torsor dual pairs. By looking at the paper [6], we can define a new multiplication structure on R, which defines the algebra of maps on the torsor R_ρ. However, this multiplication does not help us visualizing the algebras as products of number fields. In [8], explicit equations for the curves C that represent these Selmer group elements are recovered, and help us see the previous algebras in more familiar terms.

In the case of $n = 2$, these curves take the form of a 2-covering map $C \to E$ where $C : y^2 = f(x)$ with $f(x)$ a quartic polynomial. The algorithm for doing that is implemented as **TwoDescent** in **Magma** and other software. We go through this algorithm, understand the algebra of our torsor as $A = \mathbb{Q}[x]/(f(x))$ and then try and compare it with the algebras R_ρ.

In the case of $n = 3$, the result of the process of recovering equations for C and the covering, gives much more complicated output, and we will use a much rudimentary method in order to understand R_ρ as an algebra of degree 9.

The end of this introduction and the first chapter are devoted to giving basic and necessary results on group schemes and torsors, as well as understanding the type of objects that we want to construct. The rest of the chapters, from 2 to 5 are devoted to giving all the details of the development I just explained. I added 2 appendix of collateral things that appear at some point of the explanation. The first one explains why the map from $H^1(K, E[n])$ to $R^\times/R^{\times n}$ is injective when n is prime. The other one compiles all the **Sage** and **Magma** commands that were used in the example computations in chapters 3, 4 and 5.

0.1 Group schemes

We first give a brief introduction to the concept of group scheme.

Definition 0.1. Let S be a scheme. A group scheme is a scheme G over S with a defining map $\pi : G \to S$ and three given morphisms:

- Multiplication: $m : G \times_S G \to G$.
- Identity: $e : S \to G$.
- Inverse: $i : G \to G$.

satisfying the following identities:

- $m \circ (m \times \mathrm{id}_G) = m \circ (\mathrm{id}_G \times m) : G \times_S G \times_S G \to G$.
- $m \circ (e \times \mathrm{id}_G) = j_1 : S \times_S G \xrightarrow{\cong} G$.
- $m \circ (\mathrm{id}_G \times e) = j_2 : G \times_S S \xrightarrow{\cong} G$.
- $e \circ \pi = m \circ (\mathrm{id}_G \times i) \circ \Delta_G = m \circ (i \times \mathrm{id}_G) \circ \Delta_G : G \to G$.

where $j_1 : S \times_S G \xrightarrow{\cong} G$ and $j_2 : G \times_S S \xrightarrow{\cong} G$ are the given canonical isomorphisms. A group scheme is commutative if multiplication is invariant under composition with with the morphism $s : G \times_S G \to G \times_S G$ switching both factors.

The category of group schemes over S can be defined by giving the suitable invariance property to the morphisms of group schemes. We usually represent the elements in a scheme X over S in terms of points over another given scheme T, which means giving an S-morphism $x : T \to X$. We usually denote the T-points as $G(T)$. Namely, we can also give a group scheme, in terms of a functor $G : \mathrm{Sch}_S \to \mathrm{Gr}$. More details can be found in [17]. Given a group scheme G over S, a subgroup scheme H is a subscheme such that for all schemes T over S, $H(T)$ is a subgroup of $G(T)$. We can also change the base of the group scheme G over S to another scheme S' and denote it by $G_{S'}$.

Definition 0.2. Let R be a ring and A be a unitary commutative R-algebra. A is called a R-Hopf algebra if it is endowed with three R-algebra maps:

- Comultiplication: $\overline{m} : A \to A \otimes_R A$.
- Counit: $\overline{e} : A \to R$.
- Coinverse: $\overline{i} : A \to A$.

satisfying dual identities from those in the group scheme category. The dual property of the commutativity property is called cocommutativity.

The coinverse is usually called the antipode in the theory of Hopf algebras. We can see a few examples of how to associate a Hopf algebra to an affine group scheme.

Example 0.1. Let $S = \operatorname{Spec} R$ be a scheme.

- The additive group $\mathbb{G}_a$ is the group scheme representing the functor $T \to \Gamma(T, \mathcal{O}_T)$, taking the additive group structure on the latter. The corresponding Hopf algebra is $R[x]$ with the comultiplication given by sending x to $1 \otimes x + x \otimes 1$ and counit and coinverse given by sending x to 0 and $-x$ respsectively.
- The multiplicative group $\mathbb{G}_m$ is the scheme representing the functor $T \to \Gamma(T, \mathcal{O}_T^\times)$, with the multiplicative structure on the latter. The corresponding Hopf algebra is $R[x, x^{-1}]$ with comultiplication given by $x \to x \otimes x$ and counit and coinverse given multiplicatively, as the maps sending x to 1 and x^{-1}.
- Let G be a group. We can construct the functor sending a scheme T over S to the locally constant functions with values in G, calling it $G_S(T)$. The group structure of G can be transfered to $G_S(T)$. The representative of this group is a constant group scheme called G_S. If S is not empty, it is isomorphic as scheme to a direct sum of copies of S indexed by G: $G_S \cong \coprod_{g \in G} S$, which is only an affine scheme if G is finite.
- Let $n > 0$. The group scheme of n-th roots of unity μ_n is given as the closed subgroup scheme of $\mathbb{G}_m$ formed by elements such that $f^n = 1$ in $\Gamma(T, \mathcal{O}_T^\times)$. The Hopf algebra in this case is $R[X]/(X^n - 1)$ with the same comultiplication and multiplication as for $\mathbb{G}_m$.
- Let R have characteristic $p > 0$ and $n > 0$. The group scheme of p^n-th roots of zero α_{p^n} to be the subgroup scheme of $\mathbb{G}_a$ consisting of elements such that $x^{p^n} = 0$ in $\Gamma(T, \mathcal{O}_T)$. The corresponding Hopf algebra is $R[X]/(X^{p^n})$.

In the case of the last two, they are finite and commutative, in the sense that the Hopf algebras are finite over R and cocommutative. The category on which we will work is the one of finite commutative locally free schemes over an affine base scheme $S = \operatorname{Spec} R$, and denote it by $\mathbf{GS}_S$. This category is anti-equivalent to the category of finite commutative cocommutative R-Hopf algebras, and denote it by $\mathbf{HA}_R$.

0.2 Cartier duality

Let S be a scheme and G a finite commutative locally free group scheme over it. For some purposes, we might want to define a dual of this group scheme. This is another group scheme that can be given in terms of the functor:

$$\mathrm{Sch}_S \to \mathrm{Gr}$$

$$T \to \mathrm{Hom}_{\mathrm{Gr}}(G_T, \mathbb{G}_{m,T})$$

which is representable and we call its representative G^D the Cartier dual of our group scheme. Nonetheless, this scheme can be also defined in terms of a Hopf algebra.

Let R be a ring and $a : R \to A$ be an algebra over it with multiplication defined by a map $\mu : A \otimes_R A \to A$. We endow it with the Hopf algebra structure given the three maps $\overline{m}, \overline{e}, \overline{i}$, and form the dual algebra $A^D = \mathrm{Hom}_R(A, R)$. By dualising, we are changing the structure maps of A. Namely,

- $a^D : A^D \to R$.
- $\mu^D : A^D \to A^D \otimes_R A^D$.
- $\overline{m}^D : A^D \otimes_R A^D \to A^D$.
- $\overline{e}^D : R \to A^D$.
- $\overline{i}^D : A^D \to A^D$.

and in this case $\overline{e}^D$ works as the structure map, $\overline{m}^D$ works as multiplication, and $\mu^D, a^D, \overline{i}^D$ give the Hopf algebra structure, with the corresponding identities appearing by the use of the ones on A. For instance, commutativity of the initial algebra, gives cocommutativity of the dual algebra. Now, we have to check that both duals coincide.

Theorem 0.1. Let R be a ring and A a cocommutative finite Hopf algebra over it. Take G the finite affine group scheme $\mathrm{Spec}(A)$ over $S = \mathrm{Spec}(R)$. Then, the group scheme $G^D = \mathrm{Spec}(A^D)$ is finite commutative and represents the functor $\mathrm{Sch}_S \to \mathrm{Gr}$ sending T to $\mathrm{Hom}_T(G_T, \mathbb{G}_{m,T})$.

Proof. The fact that it is finite comes from the finiteness of A. The cocommutativity of A^D comes from the commutativity of A. We just have to check an isomorphism between $\mathrm{Hom}_S(S, G^D)$ and $\mathrm{Hom}_S(G, \mathbb{G}_m)$. For instance, the second is given by homomorphisms of Hopf algebras $f : R[X, X^{-1}] \to A$ which are determined only by $b = f(x)$ for some $b \in A^\times$. The condition of it being a homomorphism is equivalent to the condition $m_A(b) = b \otimes b$. In fact, for it to be a homomorphism we need the commutativity of the diagram:

$$\begin{array}{ccc} R[X, X^{-1}] & \xrightarrow{\quad f \quad} & A \\ \downarrow{\scriptstyle m_R} & & \downarrow{\scriptstyle m_A} \\ R[X, X^{-1}] \otimes R[X, X^{-1}] & \xrightarrow{f \otimes f} & A \otimes A \end{array}$$

but at the same time, we just need to check the condition of morphism at b, therefore we require $m_A(b) = b \otimes b$. An element satisfying this, will also satisfy $e_A(b) = 1$ using the identity $m \circ (e_A, \mathrm{id}_A) = \mathrm{id}_A$. Therefore, we get:

$$\mathrm{Hom}_R(R[X, X^{-1}], A) \cong \{b \in A^\times \mid m_A(b) = b \otimes b, \quad e_A(b) = 1\}$$

but at the same time, the morphisms $A^D \to R$ are all determined by the evaluation at some unit b, and the fact that this evaluation is a morphism of R-algebras can be translated in terms of the two previous conditions put on b. Therefore, we have an isomorphism between the prevously mentioned groups of homomorphisms. □

Example 0.2. Let S be a scheme. The constant group scheme ove S associated to the group $(\mathbb{Z}/n\mathbb{Z})$ is the Cartier dual to the scheme of n-th roots of unity $\mu_{n,S}$. It can be checked by comparing the definition of the second with the group scheme $\mathrm{Hom}_S((\mathbb{Z}/n\mathbb{Z})_S, \mathbb{G}_{m,S})$.

0.3 Dual pairs

The category of dual pairs of algebras was first mentioned by Bruin in [1]. The purpose of construction of is that concrete group schemes can be made explicit in terms of algebras without needing to pass through the computation of its comultiplication that the category of Hopf algebras uses.

Let R be a ring and A, B two finite locally free algebras over it and $\Phi : A \times B \to R$ a perfect R-bilinear map. We can also define the map

$$\Phi^{(2)} : (A \otimes_R A) \times (B \otimes_R B) \to R$$

sending $(a \otimes a', b \otimes b')$ to $\Phi(a, b)\Phi(a', b')$ and the maps that serve as comultiplication:

$$\mu_1^\Phi : A \to A \otimes_R A$$

$$\mu_2^\Phi : B \to B \otimes_R B$$

appear as R-algebra maps such that the following identities hold for any $a, a' \in A$ and $b, b' \in B$.

$$\Phi(a, bb') = \Phi^{(2)}(\mu_1^\Phi(a), b \otimes b')$$

$$\Phi(aa', b) = \Phi^{(2)}(a \otimes a', \mu_2^\Phi(b))$$

The same way, we can define the maps $\epsilon_1^\Phi, \epsilon_2^\Phi : A \to R$ as:

$$\epsilon_1^\Phi(a) = \Phi(a, 1_B)$$

$$\epsilon_2^\Phi(b) = \Phi(1_A, b)$$

which will serve as counits.

Definition 0.3. A dual pair of algebras is a triple (A, B, Φ) where A, B are two finite locally free R-algebras and $\Phi : A \times B \to R$ is a perfect R-bilinear map satisfying the following identities:

- $\Phi(1_A, 1_B) = 1$.
- For all $a, a' \in A$, we have $\Phi(aa', 1_B) = \Phi(a, 1_B)\Phi(a', 1_B)$.
- For all $b, b' \in A$, we have $\Phi(1_A, bb') = \Phi(1_A, b)\Phi(1_A, b')$.
- For all $a, a' \in A$ and $b, b' \in B$, $\Phi^{(2)}(\mu_1^\Phi(a)\mu_1^\Phi(a'), b \otimes b') = \Phi(aa', bb') = \Phi^{(2)}(a \otimes a', \mu_2^\Phi(b)\mu_2^\Phi(b'))$

Morphisms between the objects $(A, B, \Phi), (A', B', \Phi')$ in this category can be defined as a pair of morphisms $f : A' \to A$ and $g : B \to B'$ such that:

$$\Phi(f(a'), b) = \Phi'(a', g(b))$$

for all $a \in A$, $a' \in A'$, $b \in B$ and $b' \in B'$.

We denote this category as $\mathbf{DP}_R$. We can now construct an equivalence of categories between $\mathbf{HA}_R$ and this new category of dual pairs of algebras over R. Therefore, the equivalence of categories between Hopf algebras and group schemes in the finite commutative locally free case gives a further equivalence with the category of dual pairs. We can represent Φ, at least locally, as a matrix after choosing bases of A and B. Together with the algebras, this matrix will encode all the information of our group scheme.

Remark 0.1. If we want to calculate the dual pair of the Cartier dual of the group scheme encoded in (A, B, Φ), we just have to look at the isomorphism $B \otimes A \cong A \otimes B$. If we have Φ as a matrix with given bases of A and B, the matrix of the Cartier dual is given by transposing the initial one.

Theorem 0.2. Let $\mathbf{HA}_R$ be the category of Hopf algebras and $\mathbf{DP}_R$ the category of dual pairs. There is a contravariant functor $F : \mathbf{DP}_R \to \mathbf{HA}_R$ sending the dual pair (A, B, Φ) to the Hopf algebra $(A, m_A, e_A, \mu_A^1, \epsilon_A^1)$. The inverse functor $G : \mathbf{HA} \to \mathbf{DP}$ sends $(A, m_A, e_A, \mu_A, \epsilon_A)$ to the dual pair (A, A^D, Φ_A) where this Φ is determined as the canonical duality pairing. The pair (F, G) forms an equivalence of categories.

Proof. The only isomorphism we have to check is the one formed by taking a dual pair (A, B, Φ) which is sent to (A, A^D, Φ_A). This comes from the pair of isomorphisms:

$$\mathrm{id} : A \to A$$

$$\phi : B \to A^D$$

where this last is defined as $\phi(b)(a) = \Phi(a, b)$. The rest of the ingredients of the equivalence are straightforward to check. □

Together with the previously mentioned equivalence between $\mathbf{HA}_R$ and $\mathbf{GS}_S$, we have the foretold equivalence between $\mathbf{GS}_S$ and $\mathbf{DA}_R$.

We have to specify how will we determine the map Φ for a given group scheme. Namely, let (A, B, Φ) form a dual pair of algebras. The isomorphism that appears on the previous proof:

$$B \xrightarrow{\cong} A^D$$

determines an element $\theta_\Phi \in A \otimes_R B$ after the isomorphism:

$$A \otimes_R B \xrightarrow{\cong} \mathrm{Hom}_R(A^D, B)$$

sending $a \otimes b$ to the morphism sending ϕ to $\phi(a)b$.

Proposition 0.1. The matrices of θ_Φ and Φ with values on R are inverse transpose of each other, with respect to a choice of bases of A and B.

Proof. Take e_i and f_j bases of A and B respectively and e_i^* and f_j^* their respective dual bases. The isomorphism $B \to A^D$ above mentioned is given in those bases by sending:

$$f_j \to \sum_i e_i^{*t} \Phi(e_i, f_j) = \sum_i \Phi^t(f_j, e_i) e_i^*$$

So its inverse can be given as:

$$e_i^* \to \sum_i (\Phi^t)^{-1}(e_i, f_j) f_j^*.$$

The other isomorphism

$$\mathrm{Hom}_R(A^D, B) \xrightarrow{\cong} A \otimes_K B.$$

sends the element $\phi \in \mathrm{Hom}_R(A^D, B)$ satisfying $\phi(e_i^*) = \sum_j \phi_i^j f_j$ to:

$$\sum_{i,j} \phi^{ij} e_i \otimes f_j$$

which for our case implies $\theta_\Phi = \sum_{i,j} (\Phi^t)^{-1}(e_i, f_j) e_i \otimes f_j$. This proves the proposition. □

Example 0.3. Let E be the elliptic curve over $\mathbb{Q}$ given by the equation:

$$y^2 = x^3 + 5x$$

and let $E[2]$ be its 2-torsion. The dual pair associated to this group scheme is the one given by the algebras:

$$A = B = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-5})$$

and the matrix:

$$\Phi = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & -5 \end{pmatrix}$$

on the basis $(1,0,0),(0,1,0),(0,0,1),(0,0,\sqrt{-5})$.

We know that the algebra corresponding to this finite commutative group scheme is given by the direct product of the zero element O in the elliptic curve (which lives in the projective completion) and the algebra of those elements generated by taking $y = 0$ (which is the condition for a point to be 2-torsion). Therefore:

$$A = \mathbb{Q} \times \mathbb{Q}[x]/(x^3 + 5x) \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-5})$$

which proves the first part of the statement. Fix L the splitting field for A, which in this case is $\mathbb{Q}(\sqrt{-5})$. As we will see in section 3, the torsion of an elliptic curve can be identified with its own Cartier dual through the Weil pairing, which in this case is given by the matrix:

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

The four points of $E[2]$ are given by the homomorphisms to the splitting field:

$$p_0, p_1, p_2, p_3 : A \otimes L \to L \quad p_i : (a, b, c + \sqrt{-5}d) \to \begin{cases} a & i = 0 \\ b & i = 1 \\ c + \sqrt{-5}d & i = 2 \\ c - \sqrt{-5}d & i = 3 \end{cases}$$

and the matrix $P = (p_0, p_1, p_2, p_3) : A \otimes L \to L^4$ on the previous bases is:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{-5} \\ 0 & 0 & 1 & -\sqrt{-5} \end{pmatrix}$$

$$P\theta_\Phi P^t = W$$

This calculation gives us:

$$\theta_\Phi = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{5} \end{pmatrix}$$

and the previous proposition gives us the result.

Remark 0.2. It is possible to recover the group law on G from this construction. Namely, as in this example, we interpret the R'-points of G as maps $p, q : A \to R'$ for any ring R' over R. From this, we use Φ to get elements in $B \otimes_R R'$, multiply them in this ring, and then recover a map $pq : A \to R$.

Example 0.4. Suppose now that the elliptic curve is:

$$y^2 = f(x)$$

where $f(x)$ splits in $\mathbb{Q}$. This implies that the pair of algebras is $A = B = \mathbb{Q}^4$ and we can choose the canonical bases of both these algebras, up to ordering the points. Then, the matrix of Φ in these bases corresponds to

the inverse matrix of the Weil pairing as given before:

$$\Phi = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

We might also be interested in an example where $f(x)$ is irreducible, completing all the possible cases that we will treat in section 4.

Example 0.5. Let $E : y^2 = x^3 - 2$ be an ellliptic curve over $\mathbb{Q}$. The dual pair of algebras for the group scheme $E[2]$ is given by the algebra $A = \mathbb{Q} \otimes \mathbb{Q}[x]/(x^3 - 2)$ and the matrix:

$$\Phi = \begin{pmatrix} \frac{1}{4} & \frac{3}{4} & 0 & 0 \\ \frac{3}{4} & -\frac{3}{4} & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

In this case, the inclusion of the points in $E[2]$ in $\overline{\mathbb{Q}}^4$ is the sending given by the matrix:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 0 & 1 & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{4} \\ 0 & 1 & \omega^2\sqrt[3]{2} & \omega\sqrt[3]{4} \end{pmatrix}$$

where ω is a primitive third root of unity, which gives an element $\theta_\Phi \in A \otimes B$ given by the matrix:

$$\theta_\Phi = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & \frac{1}{3} & 0 \end{pmatrix}$$

corresponding to the matrix previously stated.

Example 0.6. Finally, we might also add an example with $n = 3$, with which we will deal in section 5. The simplest example I could come up with is the curve $E : y^2 = x^3 + 1$. The previous algebra in this case is:

$$A = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3})$$

and the torsion points on $E[3]$ are:

$$\{O, (0,1), (0,-1), (-\sqrt[3]{4}, \sqrt{-3}), (-\sqrt[3]{4}, -\sqrt{-3}), (-\omega\sqrt[3]{4}, \sqrt{-3}), (-\omega\sqrt[3]{4}, -\sqrt{-3}), (-\omega^2\sqrt[3]{4}, \sqrt{-3}), (-\omega^2\sqrt[3]{4}, -\sqrt{-3})\}$$

and if we choose the bases given by $-\sqrt[3]{4}$ and $\sqrt{-3}$, i.e. $\{1, -\sqrt[3]{4}, \sqrt[3]{4^2}, \sqrt{-3}, -\sqrt[3]{4}, \sqrt[3]{4^2}\}$, then the homomorphisms $A \otimes \overline{Q} \to \overline{\mathbb{Q}}^9$ corresponding to each point give us a matrix of the form:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -\sqrt[3]{4} & 2\sqrt[3]{2} & \sqrt{-3} & -\sqrt{-3}\sqrt[3]{4} & 2\sqrt{-3}\sqrt[3]{2} \\ 0 & 0 & 0 & 1 & -\sqrt[3]{4} & 2\sqrt[3]{2} & -\sqrt{-3} & \sqrt{-3}\sqrt[3]{4} & -2\sqrt{-3}\sqrt[3]{2} \\ 0 & 0 & 0 & 1 & -\omega\sqrt[3]{4} & 2\omega^2\sqrt[3]{2} & \sqrt{-3} & -\omega\sqrt{-3}\sqrt[3]{4} & 2\omega\sqrt{-3}\sqrt[3]{2} \\ 0 & 0 & 0 & 1 & -\omega\sqrt[3]{4} & 2\omega^2\sqrt[3]{2} & -\sqrt{-3} & \omega\sqrt{-3}\sqrt[3]{4} & -2\omega\sqrt{-3}\sqrt[3]{2} \\ 0 & 0 & 0 & 1 & -\omega^2\sqrt[3]{4} & 2\omega\sqrt[3]{2} & \sqrt{-3} & -\omega^2\sqrt{-3}\sqrt[3]{4} & 2\omega\sqrt{-3}\sqrt[3]{2} \\ 0 & 0 & 0 & 1 & -\omega^2\sqrt[3]{4} & 2\omega\sqrt[3]{2} & -\sqrt{-3} & \omega^2\sqrt{-3}\sqrt[3]{4} & -2\omega\sqrt{-3}\sqrt[3]{2} \end{pmatrix}$$

where ω is a primitive third root of unity. The Weil pairing in this case is:

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \omega & \omega^2 & \omega & \omega^2 & \omega & \omega^2 \\ 1 & 1 & 1 & \omega^2 & \omega & \omega^2 & \omega & \omega^2 & \omega \\ 1 & \omega^2 & \omega & 1 & 1 & \omega^2 & \omega & \omega & \omega^2 \\ 1 & \omega & \omega^2 & 1 & 1 & \omega & \omega^2 & \omega^2 & \omega \\ 1 & \omega^2 & \omega & \omega & \omega^2 & 1 & 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & \omega & 1 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & \omega & \omega^2 & \omega^2 & \omega & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^2 & \omega & \omega & \omega^2 & 1 & 1 \end{pmatrix}$$

and they both together give an element θ_Φ of the form:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -\frac{1}{2} & 0 & 0 & -\frac{1}{2} & 0 & 0 \\ 1 & 1 & 1 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 1 & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{8} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{8} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{24} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{24} & 0 \end{pmatrix}$$

and therefore, the matrix of the dual pair is:

$$\Phi = \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & \frac{2}{3} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & -\frac{1}{3} & 0 & 0 & -1 & 0 & 0 \\ \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & -\frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -8 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 24 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -24 & 0 \end{pmatrix}$$

1 Torsors

The goal of this section is to prepare all the necessary objects to be able to compute torsors in terms of dual pairs. Nevertheless, we will need to use a few definitions of torsor at the same time, so we introduce a quite wide meaning of the definition of torsor. We also need to choose the right topology for taking torsors. Once this is done, we will be ready to give the definition of a torsor dual pair.

1.1 Two definitions of torsor

The first definition of torsors is given in terms of sheaves.

Definition 1.1. Let $\mathcal{G}$ be a sheaf of groups on a site $\mathfrak{C}$. A $\mathcal{G}$-torsor is a sheaf of sets $\mathcal{F}$, on $\mathfrak{C}$, with a given $\mathcal{G}$-action $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ satisfying the following conditions:

- For every $U \in \mathfrak{C}$ such that $\mathcal{F}(U) \neq \emptyset$, the group action:

$$\mathcal{G}(U) \times \mathcal{F}(U) \to \mathcal{F}(U)$$

  is free and has exactly one orbit.

- For every $\mathcal{U} \in \mathfrak{C}$ there is a cover $\{U_i \to U\}_{i \in I}$ such that $\mathcal{F}(U_i) \neq 0$ for every $i \in I$.

A $\mathcal{G}$-torsor is trivial if it is isomorphic to $\mathcal{G}$ as a $\mathcal{G}$-torsor, with the action given by translation.

Lemma 1.1. A torsor is trivial, if and only if, $\Gamma(\mathfrak{C}, \mathcal{F}) \neq \emptyset$.

Proof. Suppose first that there is a global section $s \in \Gamma(\mathfrak{C}, \mathcal{F})$, then the map $\mathcal{G} \to \mathcal{F}$ sending a local section $g \in \mathcal{G}(U)$ to $gs|_U \in \mathcal{F}(U)$ is an isomorphism of sheaves.
On the other direction, if there is an isomorphism of sheaves, the section $1 \in \Gamma(\mathfrak{C}, \mathcal{G})$ is sent to some other global section in $\Gamma(\mathfrak{C}, \mathcal{F})$, therefore this space is nonempty. □

This result also proves that a torsor comes with the given structure of an isomorphism of sheaves of $\mathcal{G}$-sets:

$$\mathcal{F} \to \mathrm{Iso}(\mathcal{F}, \mathcal{G})$$

We basically want to translate this to schemes, having the advantage that for the fpqc, and other topologies below it, all representable functors are sheaves. In other words, let S be a scheme and X another scheme over S. X will be a torsor over some group object G, if and only if, $\mathrm{Hom}_S(-, X)$ is a torsor as a sheaf over the sheaf of groups $\mathrm{Hom}_S(-, G)$. This leads to this other pair of definitions.

Definition 1.2. Let S be a scheme. Let X be a S-scheme, G a group scheme over S and $G \times_S X \to X$ an action of G on X. X will be called a pseudo-torsor if the morphism of schemes $G \times_S X \to X \times_S X$ over S sending (g, x) to (x, gx) is an isomorphism of schemes. The pseudo-torsor will be called trivial in the case that there is a section of the map $X \to S$.

Definition 1.3. Let X be a G-pseudo-torsor over a scheme S and let τ be a topology. Then, X is called a torsor if there is a cover in the τ topology $\{S_i \to S\}$ such that each $X \times_S S_i \to S_i$ has a section. [1]

Remark 1.1. In this thesis, we will only use covers formed by a single arrow $\{T \to S\}$.

We are using the notation G when dealing with group schemes in the way denoted in the previous section and $\mathcal{G}$ when dealing with sheaves. The equivalence between the two definitions of torsor is proved in the following proposition.

Proposition 1.1. Let S be a scheme and τ a topology. Let X be a scheme and G a group scheme, both over S, and $G \times_S X \to X$ an action of G on X. The following conditions are equivalent:

[1] Some references do not specify the topology when dealing with torsors for the fpqc topology. However, mentioning the topology is a key ingredient.

– X is a G-torsor for the topology τ.

– $\mathrm{Hom}_S(-, X)$ is a torsor as a sheaf in $\mathrm{Sch}_{\tau,S}$.

Proof. If the map $G \times_S X \to X \times_S X$ is an isomorphism, so it is taking the corresponding sheaves, and then for a pair $(x_1, x_2) \in X \times_S X$, there is a corressponding $(g, x_1) \in G \times_S X$, which implies that $gx_1 = x_2$ making the action transitive. On the other hand, the element (x, x) is mapped uniquely by $(1, x)$ implying the action is free. Conversely, we follow the same steps taking the functor of points. □

This result does not imply that all torsors for the fppf topology are representable.

1.2 Torsors and $H^1(S, G)$

Next, we have to prove that the cohomology object that represents isomorphism classes of torsors is $H^1(S, G)$. We prove this result in any category first and then motivate the necessity of the fppf topology. For our proof to work, we need the sheaf of groups to be abelian, but this is the case for finite commutative group schemes.

Proposition 1.2. Let $\mathfrak{C}$ be a site and $\mathcal{G}$ a sheaf of abelian groups on this site. The isomorphism classes of $\mathcal{G}$-torsors are parametrized by $H^1(\mathfrak{C}, \mathcal{G})$.

Proof. Let $\mathcal{F}$ be a $\mathcal{G}$-torsor and can construct the presheaf:

$$\mathbb{Z}[\mathcal{F}](U) = \Big\{ \sum_i n_i[s_i] \mid s_i \in \mathcal{F}(U) \Big\}$$

as a free $\mathbb{Z}$-module with basis $\mathcal{F}(U)$ and sheafify it to $\overline{Z}[\mathcal{F}]$. This sheaf comes with a given degree map $\deg : \overline{\mathbb{Z}}[\mathcal{F}] \to \overline{\mathbb{Z}}$, sending $\sum_i n_i[s_i]$ to $\sum_i n_i$, where the right sheaf is the constant sheaf generated by $\mathbb{Z}$. This leads to another sheaf $\mathrm{Ker}(\deg)$, which exists due to the fact that the categories of sheaves are abelian. This sheaf is generated by the sums $[s] - [s']$. We can send these elements to the sections $h \in \mathcal{G}$ such that $hs = s'$. This constructs a diagram of sheaves:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(\deg) & \longrightarrow & \overline{\mathbb{Z}}(\mathcal{F}) & \longrightarrow & \overline{\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{G} & \longrightarrow & \mathcal{E} & \longrightarrow & \overline{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

where $\mathcal{E}$ is generated by pushout. The arrows of the diagram are morphisms due to the fact that the sheaf of groups $\mathcal{G}$ is abelian. Using the long exact sequence of cohomology:

$$\ldots \to H^0(\mathfrak{C}, \overline{\mathbb{Z}}) \to H^1(\mathfrak{C}, \mathcal{G}) \to H^1(\mathfrak{C}, \mathcal{E}) \to \ldots$$

so there is an element $\xi \in H^1(\mathfrak{C}, \mathcal{G})$, which is the image of $1 \in H^0(\mathfrak{C}, \overline{\mathbb{Z}})$.
Conversely, we can choose an embedding of the abelian sheaf $\mathcal{G}$ into an injective abelian sheaf $\mathcal{I}$. Then, there is a short exact sequence:

$$0 \to \mathcal{G} \to \mathcal{I} \to \mathcal{Q} \to 0$$

Using the vanishing of the cohomology of an injective sheaf, we have a surjective arrow:

$$H^0(\mathfrak{C}, \mathcal{G}) \to H^1(\mathfrak{C}, \mathcal{G})$$

so if we take $\xi \in H^1(\mathfrak{C}, \mathcal{G})$, there is a global section $q \in H^0(\mathfrak{C}, \mathcal{Q})$. We can take $\mathcal{F} \subset \mathcal{I}$ the subsheaf of sections mapping to q. This is a torsor, with the action given by the injection of $\mathcal{G}$ in $\mathcal{I}$, well defined as the elements of $\mathcal{G}$ become trivial in $\mathcal{Q}$. It is free and transitive using this same fact. It is straightforward to see that this is the inverse of the previous map. □

In the case of abelian schemes, the group of G-torsors over a given scheme is called the Weil-Chatelet group and it is denoted by $\mathrm{WC}(G)$. This notation comes from the case of elliptic curves, with which we will deal in the last chapters. If E is an elliptic curve over a field K, the torsors in $\mathrm{WC}(E,K)$ are called twists, which means other curves with E-action that are isomorphic to E over $\overline{K}$.

We illustrate this with the following example why it is suitable to take the fppf topology instead of the etale topology.

Example 1.1. Let K be a field of characteristic p. We are going to take μ_p-torsors, and write this group scheme as:

$$\mu_p = \operatorname{Spec} K[X]/(X^p - 1)$$

which is evidently nonreduced as it coincides with $\operatorname{Spec} K[X]/(X-1)^p$. We could take some $a \in K^\times$ and our torsor take the form:

$$\operatorname{Spec} K[Y]/(Y^p - a)$$

as any root of unity acts freely on the solutions of $Y^p - a$, but we cannot do it on the etale topology as $K(\sqrt[p]{a})$ is not a separable extension in general, therefore not a cover on the etale topology. But still, it remains being a torsor for the fppf topology. Therefore, this is going to be the site in which we shall work usually.

From now on, we will say just torsor for the torsors on the fppf topology.

1.3 The Selmer and Tate-Shafarevich groups

Let $\mathcal{G}$ be a finite commutative group scheme over a number field K. Suppose it has a presentation in terms of two abelian varieties $\mathcal{A}, \mathcal{B}$:

$$1 \to \mathcal{G} \to \mathcal{A} \xrightarrow{f} \mathcal{B} \to 1$$

Taking the long exact sequence of cohomology we get:

$$1 \to \mathcal{G}(K) \to \mathcal{A}(K) \xrightarrow{n} \mathcal{B}(K) \to H^1_{\mathrm{fppf}}(K,\mathcal{G}) \to H^1_{\mathrm{fppf}}(K,\mathcal{A}) \to H^1_{\mathrm{fppf}}(K,\mathcal{B}) \to \dots.$$

We can cut the sequence to another short exact sequence

$$1 \to \mathcal{B}(K)/f(\mathcal{A}(K)) \to H^1_{\mathrm{fppf}}(K,\mathcal{G}) \to H^1_{\mathrm{fppf}}(K,\mathcal{A})[f] \to 1.$$

The inclusion $K \hookrightarrow K_v$ yields a diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{B}(K)/f(\mathcal{A}(K)) & \longrightarrow & H^1_{\mathrm{fppf}}(K,\mathcal{G}) & \longrightarrow & H^1_{\mathrm{fppf}}(K,\mathcal{A})[f] & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \prod_v \mathcal{B}(K_v)/f(\mathcal{A}(K_v)) & \longrightarrow & \prod_v H^1_{\mathrm{fppf}}(K_v,\mathcal{G}) & \longrightarrow & \prod_v H^1_{\mathrm{fppf}}(K_v,\mathcal{A})[f] & \longrightarrow & 1
\end{array}$$

Definition 1.4. In this case, we define the Selmer group to be:

$$\mathrm{Sel}^f(\mathcal{G},K) = \ker\{H^1_{\mathrm{fppf}}(K,\mathcal{G}) \to \prod_v H^1_{\mathrm{fppf}}(K_v,\mathcal{A})\}$$

We can also define the Tate-Shafarevich group to be:

$$Ш(\mathcal{A},K) = \ker\{H^1_{\mathrm{fppf}}(K,\mathcal{A}) \to \prod_v H^1_{\mathrm{fppf}}(K_v,\mathcal{A})\}$$

As during this thesis we show equivalences with some related objects, we can call these objects geometric.

This also yields an exact sequence

$$1 \to \mathcal{B}(K)/f(\mathcal{A}(K)) \to \mathrm{Sel}^f(\mathcal{G}, K) \to Ш(\mathcal{G}, K)[f] \to 1$$

The method of moving between these three terms is called descent, as it can be related to the classical infinite descent of Fermat. The most known case is the descent of elliptic curves, which allows us to prove the Mordell-Weil theorem of finiteness of the group of K-points of the curve.

For instance, if we take an elliptic curve E and f to be multiplication by n, the previous sequence will write as:

$$1 \to E(K)/nE(K) \to \mathrm{Sel}^n(E, K) \to Ш(E, K)[n] \to 1.$$

When determining the Selmer group, we will have elements coming from K-rational points in our curve, and others representing nontrivial elements on $Ш(E, K)$, namely those torsors will violate the Hasse principle (having points everywhere locally but not globally). However, the local condition will be one of our requirements on the process of descent.

In the case of μ_n-torsors, the presentation is not given in terms of abelian varieties but the torus $\mathbb{G}_m$. Still, a similar object to the Selmer group appears. Namely, we will work over schemes of the type $S = \mathrm{Spec}(\mathcal{O}_{K,\mathcal{S}})$, and the corresponding fields of functions K_S, which are be number fields. Then, the corresponding Selmer group is

$$\mathrm{Sel}^n(K_S) = \mathrm{Ker}\left(H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_S, \mu_n) \to \prod_{v \in s} H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_v, \mu_n)\right)$$

so this is our reference for comparing the results.

1.4 Torsor dual pairs

The goal of this thesis is to use these results for writing torsors over a given group scheme in terms of its dual pair of algebras. So, as well as we saw an equivalence of categories between group schemes and dual pairs of algebras, we should also give a similar statement for torsors.

Definition 1.5. Let R be a ring, A a R-Hopf algebra and T an R-algebra, both finite and locally free of positive rank. An A-torsor structure on T is an R-algebra morphism:

$$x : T \to T \otimes A$$

satisfying that, after the functor Spec, the map:

$$\mathrm{Spec}\, A \times \mathrm{Spec}\, T \to \mathrm{Spec}\, T$$

is a free and transitive group action. This means that x satisfies dual conditions to those of being a group action and that the map:

$$x' : T \otimes T \to T \otimes A$$
$$t \otimes t' \to (t \otimes 1)x(t')$$

is an isomorphism of R-algebras.

Proposition 1.3. Let $S = \mathrm{Spec}\, R$ be an affine scheme and $G = \mathrm{Spec}\, A$ be a finite commutative locally free group scheme with corresponding dual pair of algebras given by the triple (A, B, Φ). It is equivalent to give the following information:

- An isomorphism class of G-torsors, with representative X.
- A triple (T, U, Ψ) where T is an R-algebra, U is a locally free B-module of rank 1 and $\Psi : T \times U \to R$ is a perfect pairing satisfying that if:

$$B \otimes U \to U$$

is the map giving B-module structure, then the corresponding map:

$$T \to T \otimes A$$

using the duality given by Φ and Ψ is a R-algebra morphism and has A-torsor structure for T.

Proof. Let X be a G-torsor. Using that X has to be isomorphic to G over some cover, we can see that $X = \operatorname{Spec} T$ has to be given by some finite R-algebra T. the torsor structure is given by a morphism:

$$\operatorname{Spec} A \otimes \operatorname{Spec} T \to \operatorname{Spec} T$$

which, in terms of algebras, gives a morphism:

$$T \to T \otimes A$$

which is an A-torsor structure on A, by using the conditions on Definition 1.2. One uses this map to recover the B-module strucure on $\operatorname{Hom}_R(T, R)$, by erasing its multiplication and define the pairing Ψ. Conversely, we can take the spectrum of T and see that the resulting scheme is a G-torsor. □

Remark 1.2. We have no algebra structure on U, so we really have to take care that when we recover the map $T \to T \otimes A$, this structure is preserved. In the case of μ_n, we will give this map first instead of the module structure, and then the rest is recovered. On the other hand, in the case of $E[n]$, we will modify the multiplication on A in order to get T.

Definition 1.6. Let (T, U, Φ) be a triple satisfying the properties of the previous proposition, with respect to a group scheme G. We call it a torsor dual pair.

For the rest of this work, we will try to associate an object of this type to each torsor over a group scheme.

2 The case of μ_n-torsors

This section contains all all the details of the case of torsors over the group scheme μ_n. For sake of simplification, we will deal with a particular case of the base scheme S, but one could imagine simple ways to generalize this. During the whole section, the case of arithmetic schemes, meaning $\operatorname{Spec} A$ where A is a number ring, has a relevant role.

2.1 Dedekind schemes and μ_n-torsors

Definition 2.1. A Dedekind scheme is an integral Noetherian normal scheme of dimension 1.

Remark 2.1. We have mentioned why we are taking the fppf topology. However, on the practical examples that we are giving we can suppose n is coprime with the characteristics of the scheme. No examples of positive characteristics appear in this thesis.

We will deal with this type of base schemes. Let S be a Dedekind scheme with the fppf topology and $n \in \mathbb{Z}_{>1}$. There is a short exact sequence of group schemes:

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 1$$

which is called the Kummer sequence. It gives a long exact sequence of cohomology:

$$1 \to \mu_n(S) \to \mathbb{G}_m(S) \to \mathbb{G}_m(S) \to H^1(S, \mu_n) \to H^1(S, \mathbb{G}_m)$$

$$\to H^1(S, \mathbb{G}_m) \to \dots$$

as we already know that the 0-th cohomology groups parametrize the global sections.

Theorem 2.1. Over the Zariski topology

$$H^1_{\mathrm{Zar}}(S, \mathbb{G}_m) = \operatorname{Pic}(S)$$

Proof. See on [27, Theo 57.42.1]. □

This theorem also works for etale, fppf, fpqc and other topologies. We can cut the previous sequence to construct a short exact sequence:

$$0 \to \mathbb{G}_m(S)/\mathbb{G}_m(S)^n \to H^1(S, \mu_n) \to \operatorname{Pic}(S)[n] \to 0$$

This sequence can be exploited to get the good representatives of the torsor classes explicitly, but we need more tools to get a good explicit representative of these classes.

Remark 2.2. We don't require S to be affine, but the equivalence of categories between group schemes and Hopf algebras does require this fact. Therefore, all the computations have to be performed locally.

The following idea is taken from [10] and sets a similar short exact sequence, which encodes in a better way the information on the torsors. We set it in the most general framework and then we will see how this works for some example.

Let S be a Dedekind scheme. Let $\mathcal{O}_S$ be the sheaf of regular functions of this scheme and $\mathcal{K}_S$ be the sheaf of rational functions. Let O_S be the ring of global sections of the previous sheaf and K_S respectively. However, we understand this ring in terms of the valuations on the local rings of each point. We can write:

$$O_S = \{x \in K_S \mid \operatorname{ord}_v(x) \geq 0 \, \forall v \in S\}^2$$

$$O_S^\times = \{x \in K_S \mid \operatorname{ord}_v(x) = 0 \, \forall v \in S\}$$

[2] We are taking all the closed points

We also take $\mathrm{Pic}(S)$ to be the corresponding Picard group. Then, for all $m \in \mathbb{Z}_{>0}$ there is a group:

$$K_S(n) = \{x \in K_S^\times / K_S^{\times n} \mid \mathrm{ord}_v(x) = 0 \bmod n \, \forall v \text{ closed point in } S\}$$

which can be interpreted as the elements in K_S whose principal ideal is an n-th power. This object can be included inside the short exact sequence:

$$1 \to O_S^\times / O_S^{\times n} \to K_S(n) \to \mathrm{Pic}(S)[n] \to 1$$

We can write explicitly the arrows of the short exact sequence. The first is determined by the inclusion $O_S^\times \to K_S^\times$ and the second sends $a \in K_S(n)$ to a unique fractional ideal $\mathfrak{b}_a$ satisfying:

$$aO_S = \mathfrak{b}_a^n$$

If we show that this object $K_S(n)$ is equivalent to $H^1(S, \mu_n)$, we will have a quite good parametrization of it. Moreover, along the way, a nice way to write the torsors in terms of algebras will appear, and we will be able to derive the dual pair interpretation of these algebras. Namely, this equivalence theorem can be written as the following.

Theorem 2.2. Let S be a Dedekind scheme with function field K_S and $n > 0$. There are isomorphisms of groups:

$$K_S(n) \cong H^1_{\mathrm{fppf}}(S, \mu_n) \cong \mathrm{Sel}^n(K_S)$$

In order to prove the first isomorphism, we need to explicitly write down the central arrow and show the commutativity of the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & O_S^\times / O_S^{\times n} & \longrightarrow & K_S(n) & \longrightarrow & \mathrm{Pic}(S)[n] & \longrightarrow & 1 \\ & & \downarrow \mathrm{id} & & \downarrow & & \downarrow \mathrm{id} & & \\ 1 & \longrightarrow & O_S^\times / O_S^{\times n} & \longrightarrow & H^1_{\mathrm{fppf}}(S, \mu_n) & \longrightarrow & \mathrm{Pic}(S)[n] & \longrightarrow & 1 \end{array}$$

Take $a \in K_S(n)$ and the ideal $\mathfrak{b}_a \subset O_S$. This allows us to construct the following O_S-module :

$$\mathcal{X}_a = \oplus_{i=0}^{n-1} \mathfrak{b}_a^i$$

on which we can put a O_S-algebra structure with the natural product:

$$\mathfrak{b}_a^i \otimes \mathfrak{b}_a^j \to \mathfrak{b}_a^{i+j}$$

which needs to be projected back in the case that $i + j \geq n$ with the map

$$\mathfrak{b}_a^{i+j} \to \mathfrak{b}_a^{i+j-n}$$

sending x to xa^{-1}. Denote this product with a subscript dot. Now, we can give the torsor in terms of a morphism:

$$\Phi_a : \mathcal{X}_a \to \mathcal{X}_a \otimes_{O_S} O_S[X]/(X^n - 1)$$

by interpreting this last algebra as $\oplus_{i=0}^{n-1} \mathfrak{b}_a^i \otimes O_S[X]/(X^n - 1)$ and sending (a_i) to $(a_i X^i)$. The first thing to check is that this is an O_S-algebra morphism.

The fact that it is a O_S-module morphism can be directly shown in the coordinates. The only possible trouble to see that the product behaves well appears when $i + j \geq n$. Take $x \in \mathfrak{b}_a^i$ and $y \in \mathfrak{b}_a^j$, then:

$$\Phi_a(x.y) = \Phi_a(xya^{-1}) = xya^{-1}X^{i+j-n} =$$

$$xya^{-1}X^{i+j-n}X^n = xya^{-1}X^{i+j} = \Phi_a(x).\Phi_a(y)$$

This algebra morphism creates a torsor structure if the morphism

$$\mathcal{X}_a \otimes_{O_S} \mathcal{X}_a \to \mathcal{X}_a \otimes O_S[X]/(X^n - 1)$$

sending $x \otimes y$ to $x \otimes \Phi_a(y)$ is an isomorphism. We can write an inverse just by understanding both algebras in a different way. Namely,

$$\mathcal{X}_a \otimes_{O_S} \mathcal{X}_a \cong \oplus_{m=0}^{n-1} \oplus_{i=0}^{n-1} \mathfrak{b}_a^i \otimes_{O_S} \mathfrak{b}_a^{n-i}$$

where we already include in the notation that if $m < i$, we change $m - i$ by $m - i + n$. Therefore its elements are indexed as $(z_{m,i})_{m,i=0\ldots n-1}$. We also use the isomorphism:

$$\mathcal{X}_a \otimes_{O_S} O_S[X]/(X^m - 1) \cong \oplus_{n=0}^{m-1} \oplus_{i=0}^{m-1} O_S X^i \otimes_{O_S} \mathfrak{b}_a^{n-i}$$

The elements of this last algebra are indexed as $(z_{m,i}X^i)_{m,i=0\ldots n-1}$ and the inverse of the map is:

$$\mathcal{X}_a \otimes_{O_S} O_S[X]/(X^n - 1) \to \mathcal{X}_a \otimes_{O_S} \mathcal{X}_a$$

$$(z_{m,i}X^i)_{m,i=0\ldots n-1} \to (z_{m,i})_{m,i=0\ldots n-1}$$

Therefore, the affine scheme $X_a = \operatorname{Spec} \mathcal{X}_a$ defines a μ_n pseudo-torsor.

We also have to check the existence of a cover such that there are sections of this scheme. Over the fppf topology, this cover is the structural morphism itself $\{X_a \to S\}$. The section that we take has to match into the following base change diagram:

$$\begin{array}{ccc} X_a & \xleftarrow{\text{pr}_1} & X_a \times_S X_a \\ \downarrow{\scriptstyle \text{structural}} & & \downarrow{\scriptstyle \text{pr}_2} \\ S & \xleftarrow[\text{cover}]{} & X_a \end{array}$$

And a section for the second projection is the diagonal map $\Delta : X_a \to X_a \times_S X_a$, which corresponds to the identity map under the isomorphism $\operatorname{Hom}_S(X_a, X_a) \cong \operatorname{Hom}_S(X_a, X_a \times_S X_a)$, therefore it is fppf.

The next step is to check that the map that we just defined fits in the commutative square of both short exact sequences, and then our map will directly be an isomorphism (for instance, using the five lemma). First, we could see that our method also works for computing $\mathbb{G}_m$-torsors. Namely, if $\mathfrak{b}$ is a fractional ideal of O_S. We construct the O_S-algebra:

$$\mathcal{Y}_\mathfrak{b} = \oplus_{i \in \mathbb{Z}} \mathfrak{b}^i$$

with the natural product and define a torsor structure on it as:

$$\mathcal{Y}_\mathfrak{b} \to \mathcal{Y}_\mathfrak{b} \otimes O_S[X, X^{-1}]$$

$$(a_i)_{i \in \mathbb{Z}} \to (a_i X^i)_{i \in \mathbb{Z}}$$

which defines a torsor by an argument similar to the previous. This helps us seeing the explicit maps on the following commutative diagram:

$$\begin{array}{ccc} K_S(n) & \longrightarrow & \operatorname{Pic}(S)[n] \\ \downarrow & & \downarrow \\ H^1_{\text{fppf}}(S, \mu_n) & \longrightarrow & H^1_{\text{fppf}}(S, \mathbb{G}_m)[n]. \end{array}$$

The top arrow sends a to $[\mathfrak{b}_a]$, the left one sends a to the $\mathbb{G}_m$-torsor class of X_a, the bottom arrow sends X as a μ_m-torsor to its pushforward to $\mathbb{G}_m$, and the right arrow sends any invertible module $\mathfrak{b}$ to $Y_\mathfrak{b}$.

In order to prove this it, we need to explicitly compute a theory for pushing torsors forward, also in terms of their algebras. We add this general construction ad hoc for this situation. In this case, we are interested in the map:

$$H^1_{\text{fppf}}(S, \mu_n) \to H^1_{\text{fppf}}(S, \mathbb{G}_m)$$

for the case of computing μ_n-torsors.

In general, let S be a scheme and $\phi : G \to G'$ be a morphism of group schemes over S. We have an induced map on cohomology:

$$\begin{array}{ccc} H^1_{\text{fppf}}(S,G) & \xrightarrow{\quad\phi^*\quad} & H^1_{\text{fppf}}(S,G') \\ \downarrow & & \downarrow \\ \{\text{isomorphism classes of } G\text{-torsors}\} & \longrightarrow & \{\text{isomorphism classes of } G'\text{-torsors}\} \end{array}$$

We can compute the map only over torsors the following way. Imagine we have a G-torsor, represented by a S-scheme T. Then, we have the following diagram:

$$\begin{array}{ccc} G & \longrightarrow & G' \\ \downarrow & \searrow & \downarrow \\ T & \longrightarrow & S \end{array}$$

and we want to construct a G'-torsor. We take the scheme $G' \times_S T$ and the G-action given by:

$$g(g', t) \to (\phi(g^{-1})g', gt)$$

At this point, the action has a quotient that we could call $G' *_G T := G \setminus (G' \times_S T)$ has a G'-torsor structure. The action is:

$$G' \times_X (G' *_G T) \to (G' *_G T)$$
$$(g', (h, t)) \to (g'h, t)$$

For this, we have to prove that:

$$G' \times_X (G' *_G T) \to (G' *_G T) \times_X (G' *_g T)$$
$$(g', (h, t)) \to ((h, t), (gh, t))$$

is an isomorphism. We take two elements $(h_1, t_1), (h_2, t_2)$ and find an element $h \in \mathcal{G}$ such that $h(h_1, t_1) = (h_2, t_2)$. I claim that this element is $h = \phi(g)h_2g_1^{-1}$ where g an element such that $gt_1 = t_2$, which exists and is unique as T is a $\mathcal{G}$-torsor. Therefore,

$$h(h_1, t_1) = h(\phi(g)^{-1}h_1, gt_1) = h(\phi(g)^{-1}h_1, t_2) = (h_2, t_2)$$

Then, the inverse of the map is given by $((h_1, t_1), (h_2, t_2)) \to (h, (h_1, t_1))$. This finishes all the details on how to push torsors forward along with group scheme morphisms. On the other, we also need to reproduce this construction in terms of algebras.

Lemma 2.1. Let $G = \operatorname{Spec} A$ be an affine group scheme acting on an affine scheme $X = \operatorname{Spec} R$. Then, we know that the action is given by a morphism:

$$R \to A \otimes R$$

The scheme representing the quotient of tbe action of G on X is given as a spectrum of a certain subring R'. The subring is given as the coequalizer of this map and the natural injection:

$$R' \to R \rightrightarrows A \otimes R$$

Proof. Take the spectrums on the last diagram and get:

$$G \times X \rightrightarrows X \to Y$$

where the last arrow is the equalizer map of the group action and the projection. This means that if two elements are in the same orbit, they map to the same element in Y. □

We apply this to the morphism of group schemes:

$$\mu_n \to \mathbb{G}_m$$

In order to prove the commutativity of the diagram, we need the identity:

$$[X_a *_{\mu_n} \mathbb{G}_m] = [Y_{\mathfrak{b}_a}]$$

We first have an action of μ_n on the product $\mathbb{G}_m \times_{\mu_n} X_a$ which, in terms of algebras is given by a morphism:

$$\mathcal{X}_a \otimes O_S[X, X^{-1}] \to \mathcal{X}_a \otimes O_S[X, X^{-1}] \otimes O_S[Y]/(Y^m - 1)$$

sending $\sum_{i=0,\dots,m-1 j\in\mathbb{Z}} a_i \otimes X^j$ to $\sum_{i=0,\dots,m-1 j\in\mathbb{Z}} a_i \otimes X^j \otimes Y^{i-j}$. By the previous lemma, we are taking the coequalizer of the previous map and the inclusion, which means identifying the elements $a_i \otimes X^j$ and $a_i \otimes X^j \otimes Y^{i-j}$. Eventually, the elements of our quotient ring R' take the form:

$$\sum_{i=0,\dots,n-1 \ j-i\in n\mathbb{Z}} a_i \otimes X^j$$

The only thing left in order to have the torsor is the action of $\mathbb{G}_m$ on it which is given by the map:

$$R' \to R' \otimes_{O_S} O_S[Z, Z^{-1}]$$

sending $\sum_{i=0,\dots,m-1 j-i\in m\mathbb{Z}} a_i \otimes X^j$ to $\sum_{i=0,\dots,m-1 \ j-i\in m\mathbb{Z}} a_i \otimes X^j \otimes Z^j$. Now, we need an isomorphism of torsors. This means that we need a map $R' \to \mathcal{Y}_{\mathfrak{b}_a}$ that is $\mathbb{G}_m$-equivariant, which means that it gives a commutative diagram:

$$\begin{array}{ccc} R' & \longrightarrow & R' \otimes_{O_S} O_S[Z, Z^{-1}] \\ \downarrow & & \downarrow \mathrm{id} \\ \mathcal{Y}_{\mathfrak{b}_a} & \longrightarrow & \mathcal{Y}_{\mathfrak{b}_a} \otimes_{O_S} O_S[Z, Z^{-1}]. \end{array}$$

This map is given by sending $a_i \otimes X^j$ to the element that has a_i in the j component and extending by linearity. It is an isomporphism as it is injective and the degrees of the algebras are the same. In terms of schemes, this implies $X_a *_{\mu_n} \mathbb{G}_m \cong \operatorname{Spec} R' \cong Y_{\mathfrak{b}_a}$.

Remark 2.3. So far, we have taken concrete natural choices of all the given structures (the torsor class, the way to give an μ_n-torsor, the representative of each class in $K_S(n)$...) that make the square commutative. This naturality does not imply that this is the only correct choice. Nevertheless, it served our purpose and other choices would eventually give us the same torsor class.

Remark 2.4. In terms of sheaves, the group $H^1_{\mathrm{fppf}}(S, \mu_n)$ has also the following interpretation:

$$H^1_{\mathrm{fppf}}(S, \mu_n) = \{(\mathcal{L}, \alpha) \mid \mathcal{L} \in \operatorname{Pic}(S)\ \alpha : \mathcal{L}^n \xrightarrow{\cong} \mathcal{O}_S\}/\{ \text{ up to isomorphism of sheaves } \}$$

which allows us to see the map from $H^1_{\mathrm{fppf}}(S, \mu_n) \to H^1_{\mathrm{fppf}}(S, \mathbb{G}_m)$ in a simpler way. However, in this work we are more interested in algebras than sheaves. Remember that $\mathbb{L}$ has an equivalent Weil divisor.

On the other hand, we also have to prove the commutativity of the other square of the diagram.

$$\begin{array}{ccc} O_S^\times/O_S^{\times n} & \longrightarrow & K_S(n) \\ \downarrow \mathrm{id} & & \downarrow \\ O_S^\times/O_S^{\times n} & \longrightarrow & H^1_{\mathrm{fppf}}(S, \mu_n) \end{array}$$

For that, we have to know where the long exact sequence of cohomology sends an element $a \in O_S^\times$, and check that it coincides with the constructed torsor X_a.

Lemma 2.2. The torsor constructed by the connecting map on cohomology $\mathbb{G}_m(S) \to H^1_{\text{fppf}}(\mu_n, S)$ is precisely the one sending $a \in \mathbb{G}_m(S)$ to the fiber of a in the map $\mathbb{G}_m(S) \xrightarrow{n} \mathbb{G}_m(\text{S})$.

Proof. (Sketch) There are ways to prove this in terms of Cech cohomology. However, it is easier to think of the global section $a : S \to \mathbb{G}_m$ as a map for which applying the fibered product $\mathbb{G}_m \times_{\mathbb{G}_{m,a}} S$. One could check on the construction of the cohomological connecting map that this is precisely the way it moves this objects. □

This gives a diagram:

$$\begin{array}{ccc} \mathbb{G}_m \times_{\mathbb{G}_m} S & \longrightarrow & S \\ \downarrow & & \downarrow a \\ \mathbb{G}_m & \xrightarrow{n} & \mathbb{G}_m \end{array}$$

where we are seeing a as a section $S \to \mathbb{G}_m$. In terms of algebras, this is given by a pushout diagram.

$$\begin{array}{ccc} O_S[T,T^{-1}] \otimes_{O_S[T,T^{-1}]} O_S & \longleftarrow & O_S \\ \uparrow & & \uparrow T \to a \\ O_S[T,T^{-1}] & \xleftarrow[T \to T^n]{} & O_S[T,T^{-1}] \end{array}$$

We just need a better way to write the tensor pushout of algebras which is the following:

$$O_S[T,T^{-1}] \otimes_{O_S[T,T^{-1}]} O_S = \Big\{ \sum_i (p(x), b) \mid p(x) \in O_S[T,T^{-1}], b \in O_S \Big\} \Big/ \big\{ (q(x^n)p(x), b) - (p(x), q(a)a) \big\}$$

In particular, this ideal that we are taking as quotient is the product $T^n O_S[T,T^{-1}] \otimes O_S$. This helps us construct a morphism the following way:

$$O_S[T,T^{-1}] \otimes_{O_S[T,T^{-1}]} O_S \to \oplus_{i=0}^{n-1} O_S^i \quad T^j \otimes 1 \to 1 \in O_S^{\overline{j}}$$

where $\overline{j}$ is j taken modulo n and we extend by linearity. We also need to know where to send X^n.

$$(T^n, 1) = (T^n, 1) - (T^n, 1) + (1, a) = a(1, 1) = (a, 1)$$

This implies that every time that we get an exponent bigger than n, we have to project it back to our ring and divide by a. Finally, the algebra structure is the same in both rings implying that the previous map is an isomorphism, counting the ranks in both sides.

The action of μ_n can be defined now the same way as we defined it for $\mathcal{X}_a$, getting also a commutative diagram of the form:

$$\begin{array}{ccc} \mu_n \times \mathbb{G}_m \times_{\mathbb{G}_m,a} S & \longrightarrow & \mathbb{G}_m \times_{\mathbb{G}_m,a} S \\ \downarrow & & \downarrow \\ \mu_n \times X_a & \longrightarrow & X_a \end{array}$$

Once this is done, the central arrow has to be an isomorphism by the 5 lemma and we have two different definitions of the Selmer group. The following examples illustrate what we have proved so far.

Example 2.1. Let $S = \text{Spec}(\mathbb{Z}[\sqrt{-5}])$, $n = 2$ with field of rational functions is $\mathbb{Q}(\sqrt{-5})$. The group of units is $\{\pm 1\}$. The Picard group, in this case, is the class group and is formed by the ideals $\{O_S, 2O_S + (1+\sqrt{-5})O_S\}$. Therefore, we can deduce that:

$$K_S(n) = \{\pm 1, \pm 2\}$$

and the torsors algebras would take the form:

$$\mathcal{X}_a = O_S \oplus \mathfrak{b}_a$$

where $\mathfrak{b}_a^2 = aO_S$. For the purpose of keeping the normalitiy and integrality of the Dedekind scheme, we can take away a finite number of points $\mathcal{S}$, and repeat the construction for $S = \text{Spec}(\mathbb{Z}[\sqrt{-5}]_{\mathcal{S}})$.

Example 2.2. Let S be the affine part of an elliptic curve with the Weierstrass equation $S = \mathrm{Spec}(\mathbb{C}[X,Y]/(Y^2 - X^3 - aX - b))$. It is a smooth irreducible curve. We want to know how the short exact sequence writes for $n = 2$. We can see that the units are the constants, therefore squares in $\mathbb{C}$. Therefore our short exact sequence gives the isomorphism:

$$H^1(S, \mu_2) \cong \mathrm{Pic}(S)[2]$$

As we are dealing with an elliptic curve, we can identify the latter with $E[2] \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^2$ adding the divisor that corresponds to the missing point on the projective space. Therefore, we can identify the torsors space with the rational functions with the tangent at these points. The 3 nontrivial 2-torsion points are of the form $P_i = (\alpha_i, 0)$ where α_i are the zeros of the polynomial $X^3 + aX + b$. Namely,

$$H^1(S, \mu_2) \cong \{0, [P_1], [P_2], [P_3]\} \cong \{1, X - \alpha_1, X - \alpha_2, X - \alpha_3\}$$

On the other hand, we can take the torsor algebras of the form:

$$\mathcal{X}_f = \Gamma(S, O_S) \oplus \Gamma(S, O_S(-D))$$

where D is Weil divisor such that $2D$ is principal and corresponds to the rational function f.

Remark 2.5. During this construction, we have supposed S was affine and used the equivalence between group schemes and dual pairs over an affine base. For a general scheme, one can thing on gluing the schemes corresponding to these torsors. However, in the following section we will make an inverstigation on what happens to this construction when we remove or add closed points.

2.2 The relation with the Selmer group

The final part of Theorem 2.2 consists on matching these spaces with the Selmer group and complete all the characterizations of the Selmer group for this case.

Theorem 2.3. Let S be an affine Dedekind scheme, O_S its ring of global sections and K_S be its field of functions. We denote by K_v the completion of the field to each closed point v of the scheme. Then,

$$H^1_{\mathrm{fppf}}(S, \mu_n) \xrightarrow{\cong} \mathrm{Ker}\left(H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_S, \mu_n) \to \prod_{v \in S} H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_v, \mu_n)\right)$$

In order to do that, we begin with the Kummer sequence and take the long exact sequence of cohomology, for O_S, K_S and $\prod_{v\in S} K_v$, which have natural injective maps between them. This gives us a diagram of the form:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_n(O_S) & \longrightarrow & O_S^\times & \xrightarrow{n} & O_S^\times & \longrightarrow & H^1_{\mathrm{fppf}}(S, \mu_n) \longrightarrow \mathrm{Pic}(S) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mu_n(K_S) & \longrightarrow & K_S^\times & \xrightarrow{n} & K_S^\times & \longrightarrow & H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_S, \mu_n) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \prod_{v\in S} \mu_n(K_v) & \longrightarrow & \prod_{v\in S} K_v^\times & \xrightarrow{n} & \prod_{v\in S} K_v^\times & \longrightarrow & \prod_{v\in S} H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_v, \mu_n) \longrightarrow 1
\end{array}$$

where only the rows are exact, and we used that the Picard group of the fields is trivial (Hilbert 90). Therefore, this gives us:

$$H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_S, \mu_n) = K^\times / K^{\times n}$$

$$\prod_{v\in S} H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K_v, \mu_n) = \prod_{v\in S} K_v^\times / K_v^{\times n}$$

Lemma 2.3. Let A be an integrally closed domain and K its fraction field. The map $H^1_{\mathrm{fppf}}(\mathrm{Spec}\, A, \mu_n) \to H^1_{\mathrm{fppf}}(\mathrm{Spec}\, K, \mu_n)$ is injective.

Proof. As we are dealing with finite commutative group schemes, these maps are also group homomorphisms, so we are reduced to prove that the kernel is trivial. Suppose we have a torsor $\operatorname{Spec} X$ over $\operatorname{Spec} A$ with a section on the ring of fractions, which is given in terms of K-algebras by a section:

$$X \otimes_A K \to K$$

This map has a corresponding map of A-algebras given by a homomorphism $X \to K$, through the isomorphism $\operatorname{Hom}_K(X \otimes_A K, K) \cong \operatorname{Hom}_A(X, K)$. So, we have to find a section $X \to A$ which fits in the following diagram:

$$\begin{array}{ccccc} A & \longrightarrow & X & \xrightarrow{?} & A \\ & \searrow & \downarrow f & \swarrow & \\ & & K & & \end{array}$$

Therefore, we have to see that if $x \in X$, then $f(x) \in A$. As X is finite over A, it is a fact of commutative algebra that X is integral over A and therefore there is a monic polynomial $g \in A[X]$ such that $g(x) = 0$. Therefore $g(f(x)) = 0 \in K$ and therefore, as A is integrally closed, $f(x) \in A$. Therefore, the image of f can be sent back to A, constructing the section. □

The next step is to show that the following diagram:

$$\begin{array}{ccc} H^1_{\text{fppf}}(\operatorname{Spec} O_S, \mu_n) & \longrightarrow & H^1_{\text{fppf}}(\operatorname{Spec} K, \mu_n) \\ \downarrow & & \downarrow \\ \prod_{v \in S} H^1_{\text{fppf}}(\operatorname{Spec} O_v, \mu_n) & \longrightarrow & \prod_{v \in S} H^1_{\text{fppf}}(\operatorname{Spec} K_v, \mu_n) \end{array}$$

is cartesian, where O_v is the complete localization. We do have the maps in terms of the multiplicative groups, using Hilbert 90 and the diagram of the beginning of the section:

$$\begin{array}{ccc} K_S(n) & \xrightarrow{i} & K^\times / K^{\times n} \\ \downarrow & & \downarrow c_K \\ \prod_{v \in S} O_v^\times / O_v^{\times n} & \xrightarrow{j_K} & \prod_{v \in S} K_v^\times / K_v^{\times n} \end{array}$$

where both horizontal arrows are injective. Using the previous isomorphism between $K_S(n)$ and $H^1_{\text{fppf}}(S, \mu_n)$, we are reduced to prove that:

$$K_S(n) = \{x \in K_S^\times / K_S^{\times n} \mid c_K(x) \in \operatorname{Im}(j_K)\}$$

Proof. (of this equality) For the first inclusion, the point is that we can take the elements of $K_S(n)$ to be represented by integral elements. This is true because we can represent the classes on the Picard group by ideals generated by integral elements as well. For the other inclusion, take a place $v \in S$ and c_v, j_v the maps restricted to the factor of this place. We use the following short exact sequence on this place

$$1 \to O_v^\times / O_v^{\times n} \to K_v^\times / K_v^{\times n} \to \mathbb{Z}/n\mathbb{Z} \to 1$$

which is induced by the valuation map. From here, we can see that if an element comes from $O_v^\times / O_v^{\times n}$, then it has trivial valuation modulo n. □

One can find in [3] a more general result.

2.3 Morphisms of Picard groups

It could be interesting to know how torsors move along a morphism of schemes $Y \to X$. In particular, for Dedekind schemes, we could think of $Y = X - \mathcal{S}$, being $\mathcal{S}$ a a finite number of points. Then our short exact sequence should generalize into a diagram of the following type.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & O_X^\times/O_X^{\times n} & \longrightarrow & K_X(n) & \longrightarrow & \mathrm{Pic}(X)[n] & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & O_Y^\times/O_Y^{\times n} & \longrightarrow & K_Y(n) & \longrightarrow & \mathrm{Pic}(Y)[n] & \longrightarrow & 1 \end{array}$$

The first investigation is whether the morphism of the Selmer groups is injective. We could prove the injectivity of the left and right arrows, but using the isomorphism of the function fields $K_X \cong K_Y$ we can conclude that they are both subgroups of a common group $K_Y^\times/K_Y^{\times n}$, having Y a less restrictive property. That implies that our diagram can extend to:

$$\begin{array}{ccccccccc} & & 1 & & 1 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & O_X^\times/O_X^{\times n} & \longrightarrow & K_X(m) & \longrightarrow & \mathrm{Pic}(X)[n] & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & O_Y^\times/O_Y^{\times n} & \longrightarrow & K_Y(m) & \longrightarrow & \mathrm{Pic}(Y)[n] & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & O_Y^\times/\langle O_Y^{\times n}, O_X^\times\rangle & \longrightarrow & Q & \longrightarrow & L/nL & \longrightarrow & 1 \end{array}$$

where L is the lattice in the cokernel of $\mathrm{Pic}(X) \to \mathrm{Pic}(Y)$ and Q is the quotient of the groups. The map on the Picard groups is quite far from being injective too.

Example 2.3. On our number theoretic example, $X = \mathrm{Spec}(\mathbb{Z}[\sqrt{-5}])$. We can think of eliminating the prime ideal $(2, 1+\sqrt{-5})$. Consider now the scheme $Y = \mathrm{Spec}(\mathbb{Z}[\sqrt{-5}][\frac{1}{6}])$ where we are taking this ideal away. We see that now the Picard group becomes trivial. Let's take $\mathfrak{p}$ be an ideal in $\mathrm{Pic}(X)$ and we see that this group is $\big(\mathbb{Z}/2\mathbb{Z}\big)$ and therefore it takes the form:

$$\mathfrak{p} = (2, 1+\sqrt{-5})^k(x)$$

for some $k \in \mathbb{Z}$ and $x \in \mathbb{Z}[\sqrt{-5}]$. As we are now skipping the ideals above (2), we see that $\mathfrak{p}$, as an ideal in Y is principal. Therefore, $\mathrm{Pic}(Y) = 1$ and the map cannot be injective.

Nevertheless, there is quite bad news about the possibility of giving $K_Y(n)$ explicitly in terms of $K_X(n)$ and the number of eliminated points.

Theorem 2.4. Every abelian group arises as a class group of some Dedekind domain.

Proof. [26] is a whole article discussing this result. □

This result reduces a lot our capacity to calculate the lattice L and consequently to calculate $K_Y(n)$ in terms of $K_X(n)$. In fact, we don't even have a reference group like $\mathbb{Z}/n\mathbb{Z}$, for which we know that our Selmer group is some direct sum of it, as in the previously mentioned examples. Nonetheless, we have results for the case of the of irreducible smooth curves. For instance, if we have X a smooth affine curve of genus g, we can look at the projectivization, where we know that $H^1_{\mathrm{fppf}}(X, \mu_n) \cong \big(\mathbb{Z}/n\mathbb{Z}\big)^{2g}$.

Theorem 2.5. Let X be a smooth affine curve of genus g, then $H^1_{\mathrm{fppf}}(X, \mu_n) = (\mathbb{Z}/n\mathbb{Z})^{2g+r-1}$ where r is the number of points on $\overline{X} - X$ for some smooth compactification.

Proof. Let $X = \overline{X} - \{p_1, \ldots, p_r\}$. We know that the Picard group now satisfies $\mathrm{Pic}(X) = \mathrm{Pic}(\overline{X})/R$, where R is the subgroup generated by the elements $\mathcal{O}_{\overline{X}}(p_i)$. We see that the map $\mathrm{Pic}^0(\overline{X}) \to \mathrm{Pic}(\overline{X})$ is surjective in this case and therefore the group $\mathrm{Pic}(X)$ is divisible. We write the cohomology as in the remark 2.4 with $\mathcal{L} \in \mathrm{Pic}^0(\overline{X})$, $\overline{D}$ is a Weil divisor supported in $\{p_1, \ldots, p_r\}$, $\overline{\alpha} : \mathcal{O}_S(\overline{D}) \xrightarrow{\cong} \overline{\mathcal{L}}$ and $\overline{R}$ is the subgroup of $H^1_{\mathrm{fppf}}(\overline{X}, \mu_n)$ generated by the triples of the type $(\mathcal{O}_{\overline{X}}(D'), nD', 1^{\otimes n})$. This gives an exact sequence:

$$1 \to H^1_{\mathrm{et}}(\overline{X}, \mu_n) \to H^1_{\mathrm{et}}(X, \mu_n) \to \oplus_{i=1}^r \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1$$

where the last arrow is the degree and the second sends $D = \sum_{i=1}^r a_i p_i$ to the coefficient a_i at the component corresponding to p_i. The computation of ranks gives the desired result. □

It can be interesting to have this last sequence in terms of $K_S(n)$.

$$1 \to K_{\overline{X}}(n) \to K_X(n) \to \oplus_{i=1}^r \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1$$

The first arrow we have seen it before, the second sends a function (up to n-th power) to the valuations of its extension to $\overline{X}$ in the points $\overline{X} - X$ modulo n at each component. By definition, the functions in $K_{\overline{X}}(n)$ exactly those that are zero modulo m on those excluded points. The last map is the degree on divisors. On $\overline{X}$, we can suppose that we take a representative of a divisor modulo n that has degree 0. Those divisors of degree 0 can be represented by a rational function with possible poles or zeroes in the eliminated points. However, a different choice of the representative would change the valuations only up to multiples of n, therefore, if we suppose that this rational function is invertible in X, then its class belongs to $K_X(n)$.

2.4 Dual pair interpretation

How can this be interpreted in terms of dual pairs? We first need to write the corresponding dual pair of μ_n over a given scheme S. We know from group scheme theory that the corresponding Hopf algebra can be given as $A = O_S[Z]/(Z^n - 1)$ with the usual algebra structure, but also the coalgebra structure given by the comultiplication

$$\Delta : O_S[Z]/(Z^n - 1) \to O_S[Z]/(Z^n - 1) \otimes O_S[Z]/(Z^n - 1) \quad Z \to Z \otimes Z$$

and the counit and coinverse similarly defined, and taking $\{1, \ldots, Z^{n-1}\}$. We can also write $B = \mathrm{Hom}_{O_S}(A, O_S) \cong O_S^n$ for the dual algebra with the isomorphism given by taking the dual bases $\{1^*, \ldots, Z^{n-1*}\}$. The dual pair arises with this duality with the matrix

$$\Phi = \mathrm{Id}$$

with respect to the mentioned bases. Let T be an algebra representing a torsor over A. We take U to be its dual, as O_S-module. We can only choose an isomorphism between T and U if they are free modules, but in this case they are only locally free. Then, our procedure endows T with a torsor structure:

$$\Phi_a : T \to T \otimes A$$

Suppose that Ψ is also given by the duality between T and U. Namely we just have to dualise the previous map using Φ and Ψ in order to get:

$$B \otimes U = \mathrm{Hom}_{O_S}(T, B) \cong \mathrm{Hom}_{O_S}(T \otimes A, O_S) \to \mathrm{Hom}_{O_S}(T, O_S) = U$$

gives the structure of locally free B-module of rank 1 in U.

For our case, $T = \oplus_{i=0}^{n-1} \mathfrak{b}_a^i$ is the algebra corresponding to the torsor given by $a \in K_S(n)$, which is given by a locally free module over A. Then, we choose $U = \mathrm{Hom}_{O_S}(\oplus_{i=0}^{n-1} \mathfrak{b}_a^i, O_S)$ and we know which is the map $\Phi_a : T \to T \otimes A$ by the previous sections and the B-module structure is given by:

$$\prod_{i=0\ldots n-1} O_S \otimes \mathrm{Hom}_{O_S}(\oplus_{i=0}^{n-1} \mathfrak{b}_a^i, O_S) \xrightarrow{\cong} \mathrm{Hom}_{O_S}(\oplus_{i=0}^{n-1} \mathfrak{b}_a^i \otimes O_S[Z]/(Z^n - 1), O_S)$$

$$\xrightarrow{\text{using } T \to T \otimes A} \mathrm{Hom}_{O_S}(\oplus_{i=0}^{n-1} \mathfrak{b}_a^i, O_S)$$

which forms componentwise multiplication in of each O_S in $\mathrm{Hom}_{O_S}(\mathfrak{b}_a^i, O_S)$

Example 2.4. Let $S = \mathrm{Spec}(\mathbb{Z}[\sqrt{-5}])$ and $A = O_S[Z]/(Z^2 - 1)$. Let T be corresponding to the element $2 \in K_S(2)$, therefore $T = O_S \oplus (2, 1 + \sqrt{-5})$ and $U = \mathrm{Hom}_{O_S}(O_S \oplus (2, 1 + \sqrt{-5}), O_S)$ as O_S-modules. The B-module structure is given by the composition of the maps:

$$\prod_{i=0,1} O_S \otimes \mathrm{Hom}_{O_S}(O_S \oplus (2, 1 + \sqrt{-5}), O_S) \xrightarrow{\cong} \mathrm{Hom}_{O_S}((O_S \oplus (2, 1 + \sqrt{-5}) \otimes O_S[Z]/(Z^2 - 1), O_S)$$

$$(x, \phi) \to \Phi(-, x) \otimes \phi$$

and

$$\mathrm{Hom}_{O_S}((O_S \oplus (2, 1 + \sqrt{-5}) \otimes O_S[Z]/(Z^2 - 1), O_S) \to \mathrm{Hom}_{O_S}(O_S \oplus (2, 1 + \sqrt{-5}), O_S)$$

$$\psi \to \psi \circ \Phi_a$$

3 The case of $E[n]$-torsors

The goal of this chapter is to understand the Selmer group of an elliptic curve in terms of dual pairs of algebras. In order to do that, part of the chapter will be devoted to understanding the process of descent of elliptic curves, specifically the methods used in [6], [11] or [21].

3.1 Review on elliptic curves

Definition 3.1. An elliptic curve over a field K is a proper smooth genus 1 curve with a distinguished point K-rational point O. It can be shown that it is projective and it has a group scheme structure for which O is the neutral point.

The curve can be given in terms of a Weierstrass equation in the projective plane $\mathbb{P}^2_K$:

$$Y^2Z + a_1YXZ + a_2YZ^2 = X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3$$

where the point O corresponds to the point $[0:1:0]$. In case the characteristic of our base field K is not 2 or 3 we can write the curve as:

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

using a suitable change of coordinates. A relevant invariant for an elliptic curve is the discriminant $\Delta = -16(4a^3 + 27b^2)$. We will need to study the behaviour over the completions of the field K so for sake of simplicity, we suppose that K is a number field.

Definition 3.2. Let E be an elliptic curve and E_v its reduction in the valuation v for a minimal Weierstrass equation. Then, we say:

- E is said to have good reduction if E_v is nonsingular.
- E is said to have multiplicative reduction (or semistable) if E_v has a node.
- E is said to have additive (or unstable) reduction if E_v has a cusp.

The last two are also called bad reduction. The reason for the name of the last two is that the group structures of $E_v(\overline{k})$ coincide with $\overline{k}^\times$ and $\overline{k}$ respectively, after removing the singular points.

The type of reduction at each valuation v can be calculated in terms of invariants of the curve. Namely, the discriminant Δ and the value $12a$ in the previous form of the curve.

Proposition 3.1. Let E be an elliptic curve over a number field K and v a place of K.

- E has good reduction at v if and only if $v(\Delta) = 0$.
- E has multiplicative reduction at v if and only if $v(\Delta) \neq 0$ and $v(12a) = 0$.
- E has additive reduction at v if $v(\Delta) \neq 0$ and $v(12a) \neq 0$.

This also implies that the number of places with bad reduction is finite.

Proof. The proof can be found in [24, VII, Prop 5.1]. □

One can also find in [24] and other introductory references on elliptic curves the definition of the conductor, which is an invariant that encodes all the information on the reduction type at every prime. However, the invariants that we will use in our construction are the Tamagawa numbers.

Definition 3.3. Let E be an elliptic curve over a number field K and let K_v be its completion at the valuation v.

$$E_0^v = \left\{ P \in E(K_v) \mid \overline{P} \in E^{\text{ns}}(k_v) \right\}$$

where $E^{\text{ns}}(k_v)$ are the nonsingular points in the reduction. It is a subgroup of $E(k_v)$, in the sense that if you take two points in E_0^v, their sum is still in E_0. The Tamagawa number at v is the index:

$$c_v = [E(K_v) : E_0^v(K_v)]$$

and the global Tamagawa number is:

$$c_E = \prod_{v \text{ place in } K} c_v$$

For the case of elliptic curves, we will be interested in the following short exact sequence of group schemes.

$$1 \to E[n] \to E \xrightarrow{n} E \to 1$$

and parametrize the torsors by $H^1(K, E[n])$. We will use the Weil pairing in order to inject $H^1(K, E[n])$ inside another group. Firstly, we need to recall the group structure of $E[n]$ is $\left(\mathbb{Z}/n\mathbb{Z}\right)^2$. Secondly, recall that the Weil divisors $\sum_i m_i[P_i]$ on an elliptic curve are principal, if and only if, they satisfy

$$\sum_i m_i = 0 \text{ and } \sum_i m_i P_i = O$$

where the last sum uses the group law of the curve.

Taking this into account, if we take $T \in E[n]$, it is sure that there is a rational function f_T such that:

$$\text{div}(f_T) = n[T] - n[O].$$

We take $T' \in E$ such that $[n]T' = T$ (which exists by surjectivity). There is also a rational function g_T such that:

$$\text{div}(g_T) = [n]^*[T] - [n]^*[O]$$

Then, take $S \in E[n]$ and for any other point $X \in E$, we have:

$$g_T(X+S)^n = f_T([n]X + [n]S) = f_T([n]X) = g_T(X)^n$$

Therefore, the quotient $\frac{g_T(X+S)}{g_T(X)}$ takes only n-th roots of unity as values.

Definition 3.4. We define:

$$e_n : E[n] \times E[n] \to \mu_m$$
$$e_n(S,T) = \frac{g(X+S)}{g(X)}$$

where X is any point such that both $g(X+S)$ and $g(X)$ are defined. This map is called the Weil pairing.

Proposition 3.2. The Weil pairing satisfies the following properties:

- The value does not depend on the chosen g.
- It is bilinear:

  $$e_n(S+S',T) = e_n(S,T)e_n(S',T)$$
  $$e_n(S,T+T') = e_n(S,T)e_n(S,T')$$

  This implies that fixing a component, the Weil pairing acts as a character.
- It is alternating:

  $$e_n(T,T) = 1$$

  for all $T \in E[n]$. This also implies that $e_n(S,T) = e_n(T,S)^{-1}$ for all $T, S \in E[n]$.

– It is Galois invariant:

$$e_n(S,T)^\sigma = e_n(S^\sigma, T^\sigma)$$

for all $\sigma \in G_{\overline{K}/K}$.

– It is compatible with composition:

$$e_{nn'}(S,T) = e_m([n']S, T)$$

for all $S \in E[nn']$ and $T \in E[n]$.

– Taking S, T to be generators of $E[n]$, then $e_n(S,T)$ is a primitive n-th root of unity.

Proof. One can find these properties in [24, III, Prop 8.1]. □

3.2 Interpretation of the cohomology group $H^1(K, E[n])$

Let E be an elliptic curve over a number field K. Take $n > 0$ and consider the finite commutative group scheme $E[n]$. We know that $H^1(K, E[n])$ parametrizes $E[n]$-torsors and that it has Galois cohomology interpretation [27] and that we are working over the fppf topology. .

We might as well interpret this group as central $\mathbb{G}_m$-extensions of $E[n]$, namely the group $\mathrm{Ext}^1_K(E[n], \mathbb{G}_m)$. Remember that we have identified $E[n]$ with its own Cartier dual through the Weil pairing, which using the exponent of the group, takes values in μ_n.

Definition 3.5. A central $\mathbb{G}_m$-extension of $E[n]$ is a group scheme Λ and a short exact sequence of group schemes:

$$0 \to \mathbb{G}_m \xrightarrow{\alpha} \Lambda \xrightarrow{\beta} E[n] \to 0$$

with the condition that $\mathbb{G}_m$ is contained in the center of Λ.

The trivial extension is given by the product $\mathbb{G}_m \times E[n]$. An isomorphism of central extensions is given by a diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Lambda_1 & \longrightarrow & E[n] & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Lambda_2 & \longrightarrow & E[n] & \longrightarrow & 1 \end{array}$$

where the right and left vertical arrows are the identities.

Lemma 3.1. All central A-extensions

$$0 \to A \to G \to J \to 0$$

where A is a divisible group, split.

Proof. We have to construct a map that extends the identity $\mathrm{id} : A \to A$, to a retraction $r : G \to A$. We call $\mathcal{R}$ the set of all pairs (C, g) where C is a subgroup $A \subset C \subset G$ and morphisms $g : C \to A$ such that $g|_A = \mathrm{id}$. We endow this set with the order defined by restriction of morphisms, and use the Zorn lemma.

– The set $\mathcal{R}$ is nonempty as it contains (A, id).

– Every partially ordered set of pairs (C_α, g_α) has an upper bound. Namely, $(\cup_\alpha C_\alpha, g)$ can be generated by defining g in all the subgroups.

Therefore, there is some maximal extension (H, r). We have to prove that $H = G$. Suppose otherwise and take $x \notin H$.

If xH has finite order in G/H, and take n such that $x^n \in H$. By divisibility, there has to be some $z \in A$ such that $z^n = r(x^n)$, so we can define $r(x) = z$ and get a new extension that contradicts the maximality. If the order is infinite, the sum of H and the subgroup generated by x is direct, therefore we can extend the map sending x to whichever element we want, and extending linearly. □

Lemma 3.2. Every commutative $\mathbb{G}_m$-extension of $E[n]$ is isomorphic to the trivial extension over $\overline{K}$.

Proof. As the field $\overline{K}$ is algebraically closed, the polynomial $X^n - a$ has a root for all $a \in \overline{K}^\times$, therefore the multiplicative group is divisible. □

We can also prove that $\mathrm{Aut}(\Lambda) \cong E[n]$, by seeing that all automorphisms are given by the composition with some $\pi : E[n] \to \mathbb{G}_m$. In particular, we can find in [22] a result in Galois cohomology that tells us that for general G-modules M, N:

$$H^r(G, \mathrm{Hom}(M, N)) = \mathrm{Ext}^r_G(M, N)$$

In particular, for $r = 1$, $M = E[n]$ and $N = \mathbb{G}_m$, we get

$$H^1(K, E[n]) = H^1(K, \mathrm{Hom}(E[n], \mathbb{G}_m)) = \mathrm{Ext}^1_K(E[n], \mathbb{G}_m)$$

We will also use other objects that $H^1(K, E[n])$ is parametrizing.

Definition 3.6. An n-covering is a pair (C, π) where C is a twist of the elliptic curve E with isomorphism ϕ over $\overline{K}$ and $\pi : C \to E$ over $\overline{K}$ fits in the diagram:

$$\begin{array}{ccc} E_{\overline{K}} & \xrightarrow{n} & E_{\overline{K}} \\ {\scriptstyle \phi_K}\uparrow & \nearrow_{\pi} & \\ C_{\overline{K}} & & \end{array}$$

Example 3.1. The trivial example is the pair $(E, [n])$ and $\phi = \mathrm{id}$.

Recall from Galois cohomology [22] that for any G-module M, $H^1(G, M)$ parametrizes crossed homomorphisms, which are maps:

$$e : G \to M$$

satisfying:

$$e(\sigma\tau) = e(\sigma)\sigma(e(\tau))$$

up to principal crossed homomorphisms which are those for which there is an element $m \in M$ satisfying:

$$e(\sigma) = \frac{\sigma(m)}{m}$$

Theorem 3.1. The cohomology group $H^1(K, E[n])$ parametrizes n-coverings of E.

Proof. The full proof can be found in [2]. The basic idea, using Galois cohomology, is to take an n-covering (C, π) and a point $P \in \ker(\pi)$ and send it to the cocycle $\sigma \to P - P^\sigma$. This construction is well-defined and bijective. □

3.3 The algebra of equivariant maps

Definition 3.7. Let G_K be the absolute Galois group of K. We can define the algebra $R = \mathrm{Map}_K(E[n], \overline{K})$ to be the algebra of Galois equivariant maps on $E[n]$. We will also see the algebra $\overline{R} = \mathrm{Map}(E[n], \overline{K}) = R \otimes_K \overline{K}$, which is the extension of R to an algebaic closure of K. In this case, we know that $\overline{R}$ is isomorphic to $(\overline{K})^{n^2}$.

Let e be a crossed homomorphism on $H^1(K, E[n])$, then there is a corresponding curve that can be given in terms of the algebra:

$$\overline{R}^{G_K}$$

of fixed elements on $\overline{R}$ by a certain action of G_K which is given as:

$$^\sigma(f)(P_i) = f(\sigma(P_i) + e_\sigma)$$

where + is the group law in $E[n]$. Then, this new algebra of fixed elements H comes with a corresponding isomorphism over $\overline{K}$ to R. This can be interpreted in terms of curves as an isomorphism $\phi : C_{\overline{K}} \to E_{\overline{K}}$., where C is a curve we can extract from the new algebra. One can check [24, X, Ex 4.8] for but we will giv some examples of this curves in the following section.

Composing it with the $[n]$ product we get a map:

$$\pi = [n] \circ \phi : C \to E$$

which is the n-covering that we wanted to construct. Only for the trivial elements on $H^1(K, E[n])$, we will get a curve with a K-point, which will be isomorphic to E over K. For those elements of $H^1(K, E[n])$ coming from $P \in E(K)$, this gives us the algebra of points in $[n]^{-1}(P)$.

This is parallel to what we have said about torsors in the provious section. However, this is closer to the theory of twists over E and we would be parametrizing $H^1(K, E)$, which means walking away from our discussion. We also can see in [24] that these curves have Jacobian E. There is a further interpretation of this group that will help us, that deals with K-rational divisors, but as many of our curves don't have K-rational points, we need to define what they are.

Definition 3.8. A K-rational divisor on a curve C over K is a Weil divisor D such that for every $\sigma \in G$, ${}^{\sigma}D = D$.

Definition 3.9. A torsor-divisor class pair is a pair $(C, [D])$ where C is a twisted curve of E and D a K-rational divisor of degree n on C representing a class of linear equivalence on $\mathrm{Pic}(C)$.

Example 3.2. The trivial torsor-divisor class pair is given by $(E, [nO])$

Theorem 3.2. The cohomology group $H^1(K, E[n])$ parametrizes torsor-divisor class pairs.

Proof. From a torsor-divisor class pair, we construct an n-covering with the map:

$$\pi : C \to E = \mathrm{Pic}^0(C)$$

$$P \to [D - nP]$$

Conversely, from a covering $\pi : C \to E$ we construct the pairing $(C, [\phi^*(nO)])$. We have to prove that $\phi^*(nO)$ is really a K-rational divisor. This comes from the fact that ϕ is an isomorphism over $\overline{K}$. These two maps are well defined and inverse from each other. Namely, if we take two isomorphic n-coverings C and C' over $\overline{K}$, they lift to the isomorphism ϕ so they move the same way n-coverings and torsor-divisor class pairs. □

Let G_K be the absolute Galois group of K and $R = \mathrm{Map}_K(E[n], \overline{K})$, the étale algebra that we have defined before. Now, we have to map $H^1(K, E[n])$ to some groups related to R.

Lemma 3.3. If the characteristic of K is zero, then any finite commutative group scheme over it is étale.

Proof. The proof can be found in [18, Theo 13.2]. The result can be generalized by saying that any finite group scheme of order an invertible element in the base field is etale. □

The Weil pairing gives us a map:

$$w : E[n] \hookrightarrow \overline{R}^{\times}$$

defined sending $P \in E[n]$ to the function $e_n(P, -)$. We can also define $\partial : \overline{R}^{\times} \to (\overline{R} \otimes \overline{R})^{\times}$ as:

$$\partial\alpha(T_1, T_2) = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)}.$$

As the map w is a homomorphism of groups, this gives a short exact sequence:

$$0 \to E[n] \to \overline{R}^{\times} \to (\overline{R} \otimes \overline{R})^{\times}$$

whose exactness can be proved using the properties of the Weil pairing. This sequence helps us define the maps:

$$w_1 : H^1(K, E[n]) \to R^\times / R^{\times n}$$

$$w_2 : H^1(K, E[n]) \to (R \otimes R)^\times / \partial R^\times$$

In order to define them, we apply Hilbert 90 also to $R^\times$ as G_K-module, and see that if we have $\psi \in H^1(K, E[n])$ such that it maps to $H^1(K, R^\times)$ to a coboundary so:

$$w(\psi_\sigma) = \frac{\sigma(\gamma)}{\gamma}$$

for some $\gamma \in \overline{R}^\times$ and all $\sigma \in G_K$. At this point, take $\alpha = \gamma^n$ and $\rho = \partial\gamma$ and define $w_1(\psi) = \alpha(R^{\times n})$ and $w_2(\psi) = \rho(\partial R^\times)$. The only choices we have made are those of ψ and γ.

- ψ can only be changed by a coboundary ξ, which is written as $\xi = \sigma(P) - P$ for some $T \in E[n]$. That choice would multiply γ by $w(T)$ but we have $\partial(w(T)) = 1$ in the exact sequence and $nT = O$ so $w(T)^n = 1$. They don't change the choices of α and ρ;
- γ can be changed by multiplying it by some Galois invariant element, namely $\gamma' \in R^\times$. Therefore, it would change α and ρ by multiplying them by some elements in $R^{\times n}$ and $\partial R^\times$ respectively.

Remark 3.1. One can check that by the way that we have defined the map w_1, it coincides with the composition of the map induced on cohomology by $\overline{w}$ and the Kummer isomorphism:

$$H^1(K, E[n]) \xrightarrow{\overline{w}} H^1(K, \mu_n(\bar{R})) \to R^\times / R^{\times n}$$

A good reference for the details of this last isomorphism is [16].

Our goal is to study $H^1(K, E[n])$ as the image of these maps. For that, we would like to have injectivity.

Lemma 3.4. If n is prime, then w_1 is injective.

Proof. Appendix 1. □

Lemma 3.5. The map w_2 is injective.

Proof. Let ψ belong to the kernel of w_2. Then, $w(\psi_\sigma) = \frac{\sigma(\phi)}{\phi}$ for some $\phi \in R^\times$. Multiplying ϕ by an element of $R^\times$ we may suppose that $\partial\phi = 1$. Then, we get $\phi = w(T)$ for some $T \in E[n]$. Since w is injective it follows that $\psi_\sigma = \sigma(T) - T$. Hence ψ is a coboundary. □

We may also relate the central extensions to this map. As we saw in the lemma 3.2, all extensions split over $\overline{K}^\times$. Therefore, we have some section $\phi : E[n] \to \Lambda$ over $\overline{K}$ whose n-th power is a section in $R^\times$:

$$\phi(T)^n = \alpha(T)$$

whose choice depends on ϕ only up to multiplication to some element of $R^{\times n}$, so we can associate to Λ an invariant $\mathrm{inv}_1(\Lambda) = \alpha R^{\times n}$. Identically, we associate a second invariant $\rho \in (R \otimes R)^\times$ that satisfies:

$$\phi(T_1)\phi(T_2) = \rho(T_1, T_2)\phi(T_1 + T_2)$$

whose choice only depends on some coboundary $\partial\gamma(T)$, so $\mathrm{inv}_2(\Lambda) = \rho(\partial R^\times)$. We see that both invariants coincide with the maps previously defined.

Lemma 3.6. Let Λ be the $\mathbb{G}_m$-extension corresponding to the cocycle $\xi \in H^1(K, E[n])$. Then we have $\mathrm{inv}_1(\Lambda) = w_1(\psi)$ and $\mathrm{inv}_2(\Lambda) = w_2(\psi)$.

Proof. It can be found in [6, Lemma 3.3]. □

In order to help us find the image of w_2, we need to continue the previous short exact sequence for the group scheme $E[n]$. For that, we define a new map ∂^2 to be:

$$\partial^2 : \overline{R \otimes R}^\times \to \overline{R \otimes R \otimes R}$$
$$\rho \to \partial^2\rho(T_1, T_2, T_3) = \frac{\rho(T_1, T_2)\rho(T_1 + T_2, T_3)}{\rho(T_1, T_2 + T_3)\rho(T_2, T_3)}.$$

When we have two elements, we can define $\rho^{\mathrm{op}}(T_1, T_2) = \rho(T_2, T_1)$. That help us on the determination of the image.

Lemma 3.7. The image of w_2 is:

$$H = \{\rho \in (R \otimes R)^\times \mid \rho^{\mathrm{op}} = \rho \text{ and } \partial^2\rho = 1\}/\partial R^\times$$

Proof. We have to prove that our conditions express associativity and commutativity on the section defined section $\phi : E[n] \to \Lambda$ are precisely those on ρ.

– Associativity:

$$\big(\phi(T_1)\phi(T_2)\big)\phi(T_3) = \rho(T_1, T_2)\phi(T_1 + T_2)\phi(T_3) = \rho(T_1, T_2)\rho(T_1 + T_2, T_3)\phi(T_1 + T_2 + T_3) =$$
$$\rho(T_2, T_3)\rho(T_1, T_2 + T_3)\phi(T_1 + T_2 + T_3) = \phi(T_1)\rho(T_2, T_3)\phi(T_2 + T_3) = \phi(T_1)\big(\phi(T_2)\phi(T_3)\big)$$

– Commutativity:

$$\phi(T_1)\phi(T_2) = \rho(T_1, T_2)\phi(T_1 + T_2) = \rho(T_2, T_1)\phi(T_2 + T_1) = \phi(T_2)\phi(T_1)$$

Conversely, if we are given a cocycle with those conditions we can define a new extension as $\mathbb{G}_m \times E[n]$ with the group law.

$$(\lambda_1, T_1)(\lambda_2, T_2) = (\lambda_1\lambda_2\rho(T_1, T_2), T_1 + T_2)$$

which defines a new extension. □

Nonetheless, it seems too tedious to have to compute representatives of H, so we will determine $H^1(K, E[n])$ through computing first the image of w_1 and then tracing it back to H using the diagram:

$$\begin{array}{ccc} H^1(K, E[n]) & \xrightarrow{w_2} & H \\ & \searrow^{w_1} & \downarrow k \\ & & R^\times/R^{\times n} \end{array}.$$

We have to determine how to go from $R^\times/R^{\times n}$ to H. The definition itself is suggesting that if from a cocycle ψ we constructed $\alpha \in R^\times/R^{\times n}$ and $\rho \in H$, we should have $k(\rho\partial R^\times) = \alpha R^{\times n}$. However, we have hidden in this map the choice of an element $\gamma \in \overline{R}^\times$ such that $\alpha = \gamma^n$ and $\rho = \partial\gamma$.

Lemma 3.8. Let $\alpha \in R^\times/R^{\times n}$ belong to the image of w_1. Then, there is $\rho \in H$ satisfying:

$$\alpha(T) = \prod_{i=0}^{n-1} \rho(T, iT)$$

and $\partial^2\rho = 1$. If the conditions are satisfied we can say $k(\rho\partial R^\times) = \alpha R^{\times n}$.

Proof. As in $\overline{R}^\times$ is an algebra over an algebraically closed field, we can take the root γ. Then we can prove:

$$\partial\rho(T) = \prod_{i=0}^{n} \frac{\gamma(T)\gamma(iT)}{\gamma((i+1)T)} = \gamma(T)^n = \alpha(T)$$

and also that,

$$\partial^2\rho(T_1, T_2, T_2) = \frac{\rho(T_1, T_2)\rho(T_1 + T_2, T_3)}{\rho(T_1, T_2 + T_3)\rho(T_2, T_3)} = \frac{\gamma(T_1)\gamma(T_2)\gamma(T_1 + T_2)\gamma(T_3)\gamma(T_1 + T_2 + T_3)\gamma(T_2 + T_3)}{\gamma(T_1 + T_2)\gamma(T_1 + T_2 + T_3)\gamma(T_1)\gamma(T_2 + T_3)\gamma(T_2)\gamma(T_3)} = 1$$

□

Remark 3.2. The importance of this lemma is due to the fact that if any of the constituent fields of R contains the n-th roots of unity, it is not sure that all the choices of γ give the correct ρ. In the practical examples, I checked that the ρ satisfies these conditions, but this could be a big computational problem as checking the condition $\partial\rho = 1$ is less efficient as it has to check n^6 equations.

Example 3.3. Think of the example $E : y^2 = x^3 + 5x$ with $p = 2$. We have seen previously that the splitting algebra is $\mathbb{Q}(\sqrt{-5})$ which has two rational points and two conjugate points over this field. Therefore, $R = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-5})$. One might think that all the field extensions forming this algebra need to be Galois extensions.

Nevertheless, one might interpret the nontrivial points in $E[2]$ as maps of $\overline{R}$ in $\overline{\mathbb{Q}}$. The trivial point is always there contributing with a factor $\mathbb{Q}$, and a nontrivial part formed by other embeddings. We might need to use this in non-Galois examples. For instance, the curve $E' : y^2 = x^3 - 2$, where the field $\mathbb{Q}[X]/(X^3 - 2)$ is not Galois. Still, there are 3 different embeddings of this field in $\overline{\mathbb{Q}}$, namely:

$$p_1, p_2, p_3 : \mathbb{Q}[X]/(X^3 - 2) \to \overline{\mathbb{Q}}$$

$$\sqrt[3]{2} \to \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$$

respectively, where ω is a primitive third root of unity. We interpret each element $c \in \mathbb{Q}[X]/(X^3 - 2)$ as a map in $\mathrm{Map}_{\mathbb{Q}}(E[2], \overline{\mathbb{Q}})$ sending each point in $E[2]$ to the image of c after the corresponding embedding.

3.4 Determining the map F

From here on, we need w_1 to be injective so we will suppose that $n = p$ is prime. We know that in order to get elements of the Selmer group, we will have to impose some condition that has to be satisfied everywhere locally. Once the map w_1 is injecting $H^1(K, E[p])$ inside $R^\times/R^{\times p}$, some diagram of the type:

$$\begin{array}{ccc} E(K)/pE(K) & \longrightarrow & R^\times/R^{\times p} \\ \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} \\ \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod R_v^\times/R_v^{\times p} \end{array}$$

will appear, where $R_v = R \otimes_K K_v$ and the restriction is defined through the injection and the restrictions can be defined by the inclusion $K \hookrightarrow K_v$. We want to define some functions $F : E(K) \to R^\times/R^{\times p}$. For defining it, we recall of the functions f_T that we used previously to define the Weil pairing. They can help us to define the map as:

$$F(P) = \{T \to f_T(P)\} \in R^\times$$

for all $P \in E(K) - E[p]$. These functions extend to divisors on the whole E, and therefore to the group $\mathrm{Pic}^0(E)$, where we can always pick representative with support outside $E[p]$ (these are sometimes called good divisors). This extension takes the form:

$$\overline{F} : E(K) = \mathrm{Pic}^0_K(E) \to R^\times/R^{\times p}$$

leading to the following result.

Theorem 3.3. The map $\overline{F}$ coincides with the composition $w_1 \circ \delta$, where δ is the connecting map from $E(K)$ to $R^\times/R^{\times p}$.

Proof. [20, Theo 2.3] □

These maps can also be lifted to the completions at each place v, $A_v = R \otimes_K K_v$, by giving new maps:

$$\overline{F}_v : E(K_v) \to R_v^\times/R_v^{\times p}$$

Therefore, the kind of condition that we have to check if we want to know where there is a local point for all $\alpha \in R^\times/R^{\times p}$ is:

$$\mathrm{res}_v(\alpha) \in F_v(E(K_v)/nE(K_v))$$

We will use the conditions in the paper [21] to determine the image of w_1, where it is explicitly seen why this condition can be added to the elements of $H^1(E[p], K)$ in order to find Selmer group elements. They also simplify the situation by showing that it is enough to check these conditions in a finite set of primes $\mathcal{S}$, namely those above p and those primes whose Tamagawa number is divisible by p. In the case that $p = 2$, we may have to add the places at infinity. This fact is related to the structure of the set of real points of the elliptic curve $E(\mathbb{R})$. This is a compact Lie group of dimension 1 of 1 or 2 components depending on whether $f(x)$ has 1 or 3 real roots. Therefore, by the classification of these Lie groups [19]:

$$E(\mathbb{R}) = \begin{cases} \mathbb{R}/\mathbb{Z} & f(x) \text{ has one real root} \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & f(x) \text{ has three real roots} \end{cases}$$

and therefore $E(\mathbb{R})/pE(\mathbb{R})$ is trivial unless $p = 2$ and $f(x)$ has three real roots, we might only need to check the infinite places in this case.

Remark 3.3. The F is taking a point $T \in E[p](\overline{K})$ and a point $P \in E(K)$, therefore it can be seen as a pairing:

$$\tau : E(K)/pE(K) \times E[p](K) \to K^\times/K^{\times p}$$

$$\tau(T, P) \to f_T(P) \mod K^{\times p}$$

which is called the Tate-Lichtenbaum pairing. It is well defined and one can see that using the definitions of F and the Weil pairing, it has an equivalent definition in:

$$\tau(T, P) = e_p(Q^\sigma - Q, T)$$

where Q satisfies $[p]Q = P$. This fact also solves the small uncertainty definition that we had when $P \in E[p]$. For more details, one can check [24, Section XI.9]. This construction is also well defined when n is not prime.

We will deal only with examples where $p = 2, 3$, therefore we would need to see how this map F looks explicitly for these cases but first we study the image of w_1 for all $H^1(E[p], K)$.

3.5 Determining the image of w_1

We take $\mathcal{S}$ to be the finite set of places containing the primes above p and those primes such that the Tamagawa number is divisible by p. We write $R = K \times A$ where K represents the 0 section of our group scheme and A a finite field extension of degree $m - 1$ where m is the order of $E[n]$, or a product of such extensions summing total degree $m - 1$. For the calculation of the Selmer group we need to compute a certain subgroup $A(\mathcal{S}, p) \subset A^\times/A^{\times p}$ defined as:

$$A(\mathcal{S}, p) = \{\alpha \in R^\times/R^{\times p} \mid \alpha \text{ is unramified outside} \mathcal{S}\}.$$

Being unramified means that the extensions $A_i(\sqrt[p]{\alpha_i})$ are unramified where $A = \prod_i A_i$ and A_i is a field and $\alpha = (\alpha_1, \ldots, \alpha_i)$. This group can be computed only by knowing the $\mathcal{S}$-units and the $\mathcal{S}$-class group of each of the A_i. Namely, if A is a field we have:

$$0 \to O_{A,\mathcal{S}}^\times/O_{A,\mathcal{S}}^{\times p} \to A(\mathcal{S}, p) \to \mathrm{Cl}(O_{A,\mathcal{S}}) \to 0$$

If $A(\mathcal{S}, p)$ has decomposition into a direct sum of fields, then the sequence writes as:

$$0 \to \prod_{i=1}^m O_{A_i,\mathcal{S}}^\times/O_{A_i,\mathcal{S}}^{\times p} \to A(\mathcal{S}, p) \cong \prod_{i=1}^m A_i(\mathcal{S}, p) \to \prod_{i=1} \mathrm{Pic}(O_{A_i,\mathcal{S}}) \to 0$$

This group $A(\mathcal{S},p)$ is the image of a particular subgroup of $H^1(K,E[p])$. Namely, the subgroup $H^1(K,E[2],\mathcal{S})$ which can be interpreted as the subgroup of cocycles which are unramified outside $\mathcal{S}$. In terms of Galois cohomology, being unramified as cocycle means mapping to the trivial cocycle in $H^1(K_{\mathcal{S}},E[p])$ where $K_{\mathcal{S}}$ is the maximal extension unramified outside $\mathcal{S}$. This subgroup contains the Selmer group.

Lemma 3.9. Suppose that v does not lie in our set $\mathcal{S}$. Then, the image of the map $E(K_v)/pE(K_v) \to H^1(K_v,E[p])$ is equal to the unramified subgroup.

Proof. See [21, Lemma 4.5]. □

Therefore, we first compute $A(\mathcal{S},p)$ and then impose conditions on the image of w_1 to their elements, getting representatives of $H^1(K,E[p],\mathcal{S})$, and finally we add some more local conditions, arriving to representatives of the Selmer group. We differentiate between the case of p even and odd.

Theorem 3.4. There is an isomorphism:

$$H^1(K,E[2]) \cong \mathrm{Ker}(\mathrm{Nm}_{A/K} : A^\times/A^{\times 2} \to K^\times/K^{\times 2})$$

If A decomposes as $\prod_{i=0}^{r} A_i$ where A_i are finite field extensions summing the necessary degree over K, then:

$$\mathrm{Nm}_{A/K}(x) = \prod_{i=0}^{r} \mathrm{Nm}_{A_i/K}(x_i).$$

Proof. We firstly use that the map $w : E[2](\overline{K}) \to \mu_2(A)$ is injective, due to the nondegeneracy of the Weil pairing. This gives us a short exact sequence over $\overline{K}$:

$$1 \to E[2](\overline{K}) \to \mu_2(\overline{A}) \to \mu_2(\overline{K}) \to 1$$

We know that the begining of the sequence is injective and the ending is surjective. By counting the order of $E[2](\overline{K})$, one can check that its image in $\mu_2(\overline{A})$ coincides with the kernel of the norm map. This gives us a long exact sequence of cohomology:

$$1 \to E[2](K) \to \mu_2(A) \to \mu_2(K) \to H^1(K,E[2]) \to H^1(K,\mu_2(\overline{A})) \cong A^\times/A^{\times 2} \to H^1(K,\mu_2(\overline{K})) \cong K^\times/K^{\times 2} \to \dots$$

and now we just have to prove that $\mu_2(A) \to \mu_2(K)$ is surjective, which in fact means proving that there is an element with norm -1 in A. This element can be chosen as $-1 \in A$. □

This result also proves the injectivity of the map w_1 for $p = 2$, which is not treated in the proof given in the appendix. Once we finish this process, we will have an output of elements in A, but to construct the dual pairs, we will need the elements to be in R. In [8], we can find arguments that corroborate that the value of this extension in O has to be a square. In the last part of this chapter, we will see that the best possible choice is extending it to the value 1.

Example 3.4. Take the elliptic curve $E : y^2 = x^3 + 5x$, whose 2 torsion is parametrized by:

$$A = \mathbb{Q} \times \mathbb{Q}(\sqrt{-5})$$

In this case, $S = \{2,5\}$ and the class group is trivial as we erased the non principal ideal over 2. By calculating the units we get:

$$A(S,2) = \{\pm 2^m 5^n \; m,n \in \mathbb{Z}\} \times \{\pm 2^m \sqrt{-5}^n \; m,n \in \mathbb{Z}\}.$$

We can see these elements up to squares, therefore we take $m,n \in \mathbb{Z}/2\mathbb{Z}$.
In order to take the norm we write the element in A as $\alpha = (\alpha_1, \alpha_2 + \alpha_3\sqrt{-5})$, the norm is:

$$\mathrm{Nm}_{A/\mathbb{Q}}(\alpha) = \alpha_1 \,\mathrm{Nm}_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(\alpha_2 + \alpha_3\sqrt{-5}) = \alpha_1(\alpha_2^2 + 5\alpha_3^2)$$

Therefore we get the group:

$$H^1(K,E[2],\mathcal{S}) \cong \{(1,1),(1,-1),(1,2)(1,-2),(5,\sqrt{-5}),(5,-\sqrt{-5}),(5,2\sqrt{-5}),(5,-2\sqrt{-5})\}$$

Suppose now that p is odd. We could still use the condition of the kernel of the norm.

Lemma 3.10. The image of $H^1(K, E[p])$ under w_1 is still contained in

$$\mathrm{Ker}\{\mathrm{Nm}_{A/K} : A^\times/A^{\times p} \to K^\times/K^{\times p}\}$$

However, this is not enough in order to get the image as the map:

$$\mu_p(\overline{A}) \to \mu_p(\overline{K})$$

is no longer surjective and we cannot split the sequence in a proper manner as we did in the Theorem 3.4. The paper [21] changes the point of view and imposes now other conditions. We know that the group $E[p](\overline{K})$ is of the form $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ after the choice of a basis.

Firstly, we need to define 3 different algebras. The first is the same algebra A, but this time interpreted as:

$$A = \mathrm{Map}_K(E[p] - \{0\}, \overline{K}).$$

The second algebra is

$$B = \mathrm{Map}_K(E[p]^D - \{0\}, \overline{K})$$

where $E[p]^D$ is the dual of $E[p]$ as $\mathbb{F}_p$-vector spaces. This set also parametrizes the lines in $E[p]$.

Lemma 3.11. The Galois invariant subset $E[p]^D - \{0\}$ parametrizes the lines in the configuration of points of $E[p]$ that do not pass through zero.

Proof. We send each map $\phi : \left(\mathbb{Z}/p\mathbb{Z}\right)^2 \to \left(\mathbb{Z}/p\mathbb{Z}\right)$ in $E[p]^D - \{0\}$ to the line configured by the points $\{P \in E[p] \mid \phi(P) = 1\}$. As we know that in this configuration, a given set is a line if and only if their points sum to 0, and ϕ is a morphism, these points form a line. Conversely, we can form a morphism from a line by giving the value 1 at the points of the line and extending linearly. □

Finally, we also define:

$$D = \mathrm{Map}_K(Y, \overline{K})$$

where

$$Y = \left\{(P, l) \in (E[p] - \{0\}) \times (E[p]^D - \{0\}) \mid P \in l\right\}$$

We can describe D as an extension of degree p of A. Take a point $P \in E[p]$ and consider $E[p]$ as a set of p^2 points. We avoid the p points in the line through O and P, and we count the rest of lines which have $p-1$ points different than P. Therefore, given a point we have $\frac{p^2-p}{p-1} = p$ lines through it.

Example 3.5. Let E be the elliptic curve $E : y^2 = x^3 + 5x$ and $p = 2$. Then,

$$A = B = \mathbb{Q} \times \mathbb{Q}(\sqrt{-5})$$

We call P_1, P_2, P_3 for the points on $E[2] - \{0\}$. We call l_1, l_2, l_3 the lines describing $E[2]^D - \{0\}$, where l_i is the line that does not pass through P_i. We describe also the Galois action on these points:

$$\sigma(P_1) = P_1$$

$$\sigma(P_2) = P_3$$

$$\sigma(P_3) = P_2$$

where σ is the only nontrivial automorphism. The same kind of action appears for the lines. We can also describe the functions on D. The space Y of domain of these functions is parametrized by the pairs (P_i, l_j) where $P_i \in l_j$ which means that $i \neq j$. The Galois action on these pairs is:

$$\sigma((P_1, l_2)) = (P_1, l_3) \quad \sigma((P_1, l_3)) = (P_1, l_2) \quad \sigma((P_2, l_1)) = (P_3, l_1)$$

$$\sigma((P_3, l_1)) = (P_2, l_1) \quad \sigma((P_2, l_3)) = (P_3, l_2) \quad \sigma((P_3, l_2)) = (P_2, l_3)$$

where σ is the nontrivial automorphism. This suggests that:

$$D = \mathbb{Q}(\sqrt{-5}) \times \mathbb{Q}(\sqrt{-5}) \times \mathbb{Q}(\sqrt{-5})$$

This example illustrates how a configuration of this type can be calculated, but we will never use it when performing a 2-descent.

We already know that $H^1(K, E[p]) \subset A^\times / A^{\times p}$. The new conditions are the following:

- The elements have to be in the kernel of a certain map $\overline{u} : A^\times / A^{\times p} \to B^\times / B^{\times p}$. This map is formed by using the composition of the inclusion of A inside D and the norm to B

  $$u = \mathrm{Nm}_{D/B} \circ i_{D/A} : A \to B$$

  and then taking quotient to the multiplicative p-th powers. If α is a generator of A, it can also be described as $\overline{u}(h(\alpha)) = \det(h(M_\alpha))$ where M_α is the matrix induced by the multiplication by α in D and $h(\alpha)$ is the polynomial expression of any element in A.

- The elements have to be in the kernel of the map $g - \sigma_g$ where g is a primitive root of unity modulo p, which means that it is a generator of $\mathbb{F}_p^\times$. Then the action of g is given by its multiplication on $A^\times / A^{p*}$ as $\mathbb{F}_p^\times$-vector space, namely:

  $$g\phi(P) = \phi^g(P)$$

  The second action is given on functions as $\sigma_g \phi(P) = \phi(gP)$. Therefore, we impose:

  $$\phi(gP) = \phi^g(P)$$

Remark 3.4. This last condition can be simplified in both of the cases that we will deal with in this thesis. Namely, if $p = 2$ both actions coincide with the action of -1 on the functions. On the other hand, if $p = 3$, we can restate this last condition by means of a simpler statement. This is defining D_+ the etale subalgebra corresponding to the orbits in $Y = \{(P, l) \in E[3] \times E[3]^D \; P \in l\}$ of the center $Z = \mathbb{F}_p^\times \mathrm{Id}$ and then changing the condition by imposing that the an element is in the image if it belongs to the kernel of the norm map:

$$\mathrm{Nm}_{D/D_+} : D^\times / D^{\times 3} \to D_+^\times / D_+^{\times 3}$$

All the details can be found in [21]. Now, we add the local conditions and we get:

$$\mathrm{Sel}^p(E, K) \cong \mathrm{im}(w_1) \cap \{a \in A^\times / A^{\times n} \mid \mathrm{res}_v(a) \in F_v(E(K_v)/nE(K_v))\} \cap A(S, p)$$

In any case, the calculations with the norms between A and B are quite tedious so a shortcut could be to use the norm conditions and afterwards measure the difference between the result and the expected size of the Selmer group. We can compare the order of $H^1(K, E[p], S)$ with the expected order of the Selmer group. One can take advantage of the known order of the Mordell-Weil and the Tate-Shafarevich group, refering to the L-functions and modular forms database, to investigate the expected orders these groups. The order of the $Ш(K, E)[p]$ can be calculated analytically using the values of the L-function associated to the curve and other invariants, by using the Birch and Swinnerton-Dyer conjecture. This database is large and powerful enough to satisfy all the examples that we want. This is a method for computing the analytic order of $Ш(K, E)[p]$, but using the structure of the Mordell-Weil group could lead to circular arguments, as this is calculated as result of the same descent procedure we are using. However, this is not the usual case, and we have to deal with p-adic points and their images after F. We first add an example where we can easily visualize the Mordell-Weil group.

Example 3.6. Let $E : y^2 = x^3 - x$ and $p = 2$. We have to consider $\mathcal{S} = \{2, \infty\}$ and we know that the algebra A corresponds to $\mathbb{Q}^3$ as $E[2] = \{O, (0,0), (1,0), (-1,0)\}$. The class group is trivial and the O_S-units are $\{\pm 1, \pm 2\}$. Therefore, we have to check the norm condition, which in this case is just taking the products and we get:

$$\mathrm{im}(w_1) \cap A(\mathcal{S}, 2) = \{(1,1,1), (1,-1,-1), (1,2,2), (1,-2,-2), (-1,1,-1), (2,1,2), (-2,1,-2), (-1,-1,1), (2,2,1),$$
$$(-2,-2,1), (-1,2,-2), (-1,-2,2), (2,-1,-2), (2,-2,-1), (-2,-1,2), (-2,2,-1)\}$$

supposing, as usual, that the values at O of these functions are 1.

In this case, the Mordell-Weil group is:

$$E(\mathbb{Q}) = \{O, (0,0), (1,0), (-1,0)\}$$

and the map $F : E(\mathbb{Q})/2E(\mathbb{Q}) \to A^\times/A^{\times 2}$ follows the formula:

$$F(P) = \begin{cases} 1 & P = O \\ x - X & P = (x,y) \notin E[2] \\ x_1 - X + (x_2 - X)(x_3 - X) & P = (x_1, 0) \in E[2] \quad x_2, x_3 \text{ the other roots} \end{cases}$$

by finding good divisors representing each point. We try to see which of the previous elements are in the image of a class in $E(\mathbb{Q})/2E(\mathbb{Q})$, which will mean that it has this point in the completion to each valuation. In this case we have $E(\mathbb{Q})/2E(\mathbb{Q}) = E[2]$ and those points in the image are:

$$\mathrm{im}(w_i) \cap F(E(\mathbb{Q})/2E(\mathbb{Q})) = \{(1,1,1), (1,2,2), (-1,-1,1), (-1,-2,2)\}$$

and it fits to the expected size of the Selmer group.

Now, we compare this example with an explicit way of finding p-adic points and calculating their images.

3.6 How to deal with p-adic points

The study of the structure of the groups of p-adic points is usually related to finding the non-singular points on the reduction to $\mathbb{F}_p$ and then studying the following short exact sequence:

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \overline{E}_{\mathrm{ns}}(\mathbb{F}_p) \to 0$$

where $E_1(\mathbb{Q}_p) = \{P \in E_0(\mathbb{Q}_p) \mid \overline{P} = \overline{O}\}$. When the reduction is good, we can see that $E(\mathbb{Q}_p) = E_0(\mathbb{Q}_p)$. Also, when p is odd, we can prove the existence of an isomorphism $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$. In this thesis, we have been dealing with primes where these conditions are not satisfied, for instance, having nontrivial Tamagawa numbers or $p = 2$. Nonetheless, we can take advantage of the filtration on this group given by:

$$E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_\text{ı}) \supset E_2(\mathbb{Q}_p) \supset \dots E_n(\mathbb{Q}_p)$$

where this subgroups are given as $E_n(\mathbb{Q}_p) = \{P \in E_0(\mathbb{Q}_p) \mid P \equiv O \mod p^n\mathbb{Z}_p\}$. The same theorem that proves the isomorphism $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$ using formal groups [24], claims the existence of $n > 0$ such that $E_n(\mathbb{Q}_p) \cong \mathbb{Z}_p$ when $p = 2$. This allows us to determine the order of the group $E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$.

Proposition 3.3. The order of the group $E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$ is $p^r|E(\mathbb{Q}_p)[n]|$ where $r = v_p(n)$.

This result could be generalized to any abelian variety and any finite extension of $\mathbb{Q}_p$ by multiplying the exponent of p by the dimension of the variety and the degree of the field.

Proof. Take $n > 0$ such that $E_n(\mathbb{Q}_p) \cong \mathbb{Z}_p$. Then, we can construct a diagram of short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_n(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p)/E_n(\mathbb{Q}_p) & \longrightarrow & 0 \\ & & \downarrow n & & \downarrow n & & \downarrow n & & \\ 0 & \longrightarrow & E_n(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p)/E_n(\mathbb{Q}_p) & \longrightarrow & 0 \end{array}$$

which gives us an exact sequence using the snake lemma of the form:

$$0 \to E(\mathbb{Q}_p)[n] \to H_1 \to E_m(\mathbb{Q}_p)/nE_m(\mathbb{Q}_p) \to E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) \to H_2 \to 0$$

where H_1 and H_2 are the kernel and cokernel of the last column and therefore have the same order. Using the isomorphism we can say that $|E_m(\mathbb{Q}_p)/nE_m(\mathbb{Q}_p)| = p^r$. □

Previously, we showed that $\overline{F} = w_1 \circ \delta$ which, in this case, is a composition of injective maps. Therefore, if we know the order of $E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$, we know the order of the image inside A_v, so we can start computing the image of different points, until we have generated a subgroup of the correct order. But once we have determined these images, we will need some instrument to determine whether these images are p-th powers or not. In fact, we will need to do that in any finite extension $L_{\mathfrak{p}}$ of $\mathbb{Q}_p$.

Lemma 3.12. Let $\alpha \in L_{\mathfrak{p}}$ be such that $v_{\mathfrak{p}}(\alpha) = 0$ and $e_{\mathfrak{p}} = v_{\mathfrak{p}}(n)$. Let r be:

$$\begin{cases} 1 & \text{if } v_{\mathfrak{p}}(n) = 0 \\ \left\lfloor \frac{e_{\mathfrak{p}}}{p-1} \right\rfloor + e_{\mathfrak{p}} + 1 & \text{if } v_{\mathfrak{p}}(n) \neq 0 \end{cases}$$

Then α is an n-th power in $L_{\mathfrak{p}}$, if and only if, α is an n-th power modulo $\mathfrak{p}^r$

Proof. The proof can be found in Lemma 13 of [11]. □

It is also deduced from this lemma that if α is an n-th power in $L_{\mathfrak{p}}$, then we can reduce to an n-th power modulo $r' > r$. Why could possibly we need that? Eventually, we are trying to calculate the classes of elements in $E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)$, so we will need to lift points of the elliptic curve modulo $p^{r'}$ with r' big enough so that we have as many points to lift as the size of the image (in fact it is enough for generators of this image). We recover the previous example and now compute the local images. As usual with local fields, the basic tool for lifting these points is Hensel's lemma. We state the version that we need to use.

Lemma 3.13. (Hensel) If $f(X_1, \ldots, X_d) \in \mathbb{Z}_p[X_1, \ldots, X_d]$ and some $a \in \mathbb{Z}_p^d$ satisfying:

$$\frac{v_p(f(a))}{2} > \min_i v_p(\nabla_i f(a))$$

then there is an $b \in \mathbb{Z}_p^d$ such that $f(b) = 0$ and $v_p(b - a) > \min_i v_p(\nabla_i f(a))$. In particular, if $v_p(a) = d$ and $\min_i v_p(\nabla_i f(a)) = 0$, then there is $b \in \mathbb{Z}_p^d$ such that $f(b) = 0$ and $b = ap^d$.

Proof. [5] □

It can be seen that these liftings dont have to be unique.

Example 3.7. Let $E : y^2 = x^3 - x$ and $n = 2$. We have to consider $S = \{2, \infty\}$. For $p = \infty$, we have $E(\mathbb{R})/2E(\mathbb{R}) = 2$ and we take as generators O and $(0, 0)$ with images:

$$F_\infty(E(\mathbb{R})/2E(\mathbb{R})) = \{(1, 1, 1), (-1, -1, 1)\}$$

therefore, this reduces the image to $\{(1, 1, 1), (-1, -1, 1), (1, 2, 2), (-1, -2, 2), (2, 2, 1), (-2, -2, 1), (-2, -1, 2), (2, 1, 2)\}$ by noting that they are, up to taking real square roots, one of the previous elements. In other words, they have the signs in the same order. In the case of $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$, we know that the order is 8, using the previous proposition. We take $r = 3$ and find points on the curve mod 8, otherwise we would not get enough points to lift or they would be nonsingular, and we would not be able to apply Hensel's lemma. These set of points could be written as:

$$E(\mathbb{Z}_2/8\mathbb{Z}_2) \supset \{O, (0, 0), (1, 0), (3, 0), (4, 2), (6, 2), (5, 0) \ldots\}$$

They all satisfy some of the ∇f conditions on Hensel's lemma. We calculate their images after $\overline{F}$.

$$F(\{O, (0, 0), (1, 0), (3, 0), (4, 2), (6, 2), (5, 0) \ldots\}) =$$

$$\{(1,1,1),(-1,-1,1),(1,2,2),(-1,-2,2),(4+o(2^3),3+o(2^3),5+o(2^3)),$$
$$(4+o(2^3),3+o(2^3),5+o(2^3)),(5+o(2^3),4+o(2^3),6+o(2^3)),(7+o(2^3),6+o(2^3),o(2^3))\}$$

In this case, the four first points already generate a group of the expected size.

Example 3.8. We could also calculate the example with $E : y^2 = x^3 - 1$. The expected size of the Selmer group is 2 and the primes that we have to check are $\mathcal{S} = \{2, 3\}$. The group $A(S, 2)$ coincides with:

$$\{\pm 1, \pm 2, \pm 3\} \times \{2, -2\omega - 1, \omega + 1, -4\omega - 2, 2\omega + 2, -\omega + 1\}$$

of which are squares only the pairs $\{(1,1),(1,-1),(1,2),(1,-1),(3,-2\omega+1),(3,2\omega-1),(3,4\omega 2),(3,-4\omega+2)\}$ which form the classes in $H^1(K, E[2], \mathcal{S})$. Take the prime 3, and consider the 3-adic points and the images of the points $O, (1, 0)$ are $\{(1, 1, 1), (3, -2\omega + 1)\}$.

3.7 The enveloping algebras

Up until here, we have performed the descent process, meaning that we have found the image of w_1, and we have which elements on $R^\times/R^{\times n}$ correspond to classes of torsors. Finally, we need to use this information, in order to construct an algebra representing the torsor. The main ideas for doing that keep coming from [6].

We drop the assumption that n is prime and suppose we completed the descent for any n. Let R be the etale algebra of $E[n]$ and $\overline{R}$ its base change to $\overline{K}$. Firstly, take an extension:

$$1 \to \mathbb{G}_m \to \Lambda \to E[n] \to 1$$

representing a given class in $H^1(K, E[n])$. We have to show how to construct an algebra from this extension. We saw that it has an equivariant section $\phi : E[n] \to \Lambda$. We can define the following map from Λ to $\overline{R}$ defined by sending:

$$\lambda\phi(T) \to \lambda\delta_T$$

where the latter is the function:

$$\delta_T(S) = \begin{cases} 1 & \text{if } T = S \\ 0 & \text{otherwise} \end{cases}$$

and the set of δ_T for all $T \in E[n]$ forms a basis of $\overline{R}$. This map defines a new multiplication on $\overline{R}$ using the group law on Λ. At the same time, this descends to an inclusion inside R, using Galois equivariance, and therefore we have constructed from Λ a different K-algebra structure, which is refered in [6] as an enveloping algebra. However, we have no explicit information about this new multiplication. Firstly, we remember that the group law on $E[n]$ gives a certain morphism for R. Namely:

$$m : E[n] \times E[n] \to E[n]$$

gives the diagonal map on R

$$\Delta : R \to R \otimes R$$

defined as $\Delta(\alpha)(S, T) = \alpha(S + T)$. This makes $R \otimes R$ an R-algebra, and therefore there is a trace map as:

$$\mathrm{tr} : R \otimes R \to R$$

defined as:

$$\mathrm{tr}(\rho)(T) = \sum_{S \in E[n]} \rho(S, T - S)$$

With this we can define a new multiplication on R, which will coincide with the one given by the extension. Let $\rho \in R \otimes R$ be representing an element on the Selmer group under the map w_2. Then there is a multiplication map:

$$z_1 *_\rho z_2 = \mathrm{tr}(\rho(z_1 \otimes z_2))$$

Lemma 3.14. This multiplication defines the algebra $(R, +, *_\rho)$ where the extension Λ corresponding to ρ.

Proof. The multiplication in Λ can be understood in terms of ρ as:

$$\phi(S)\phi(T) = \rho(S,T)\phi(S+T)$$

This implies that the multiplication in $\overline{R}$ is given, in the elements of the bases by:

$$\delta_S *_\rho \delta_T = \rho(S,T)\delta_{S+T}$$

which descends to the functions of R as:

$$\alpha *_\rho \beta = \big(\sum_T \alpha(T)\delta_T\big) *_\rho \big(\sum_T \beta(T')\delta_{T'}\big) = \sum_T (\sum_{T'} \rho(T', T-T')\alpha(T')\beta(T-T'))\delta_T$$

which gives the group law. □

Now we see that we made a good choice by fixing the value 1 in O, when extending from A to R, as the element $(1,0)$ is the neutral for this multiplication.

Theorem 3.5. The previous algebra is the etale algebra of the $E[n]$-torsor corresponding to $\rho \in H$.

Proof. The discussion above serves as sketch of a proof of this result. □

We can simplify its notation to R_ρ. The first thing we should prove is that we recover the group law on $E[n]$ in the case that we take the trivial ρ. Nonetheless, we have to use the Fourier transform to go from this multiplication to the usual one in R.

Definition 3.10. The Fourier transform sends $\alpha \in R$ to the function,

$$\widehat{\alpha}(S) = \sum_T e_n(S,T)\alpha(T)$$

It is called Fourier transform due to the similarity between the Weil pairing and $e^{\pi i x}$.

In order to prove the previous claim, we first need to prove some things on this Fourier transform.

Lemma 3.15. Let $\alpha \in R$. The Fourier transform satisfies:

$$\widehat{\widehat{\alpha}} = n^2\alpha$$

Proof. Take $S \in E[n]$ and:

$$\widehat{\widehat{\alpha}}(S) = \sum_T \widehat{e_n(S,T)}\alpha(T) = \sum_{T,T'} e_n(S,T)e_n(T,T')\alpha(T')$$

Now, we fix T' and we have to prove that:

$$\sum_T e_n(S,T)e_n(T,T') = \begin{cases} n^2 & S = T' \\ 0 & S \neq T' \end{cases}$$

We can prove this fact by saying that $e_n(-,T)$ is a character on $E[n]$ and $e_n(T,-)$ is its conjugate and recall the formula for conjugate sums of characters. □

Lemma 3.16. Take $1 \in R \otimes R$ be the trivial element, then the Fourier transform gives an isomorphism between $(R, +, \cdot)$ and $(R, +, *_1)$.

Proof. The only thing we have to prove is that it moves multiplication the right way. Therefore, take $\alpha, \beta \in R$ we need:

$$\hat{\alpha} \cdot \hat{\beta} = \widehat{\alpha *_1 \beta}$$

which explicitly in an element S is:

$$\hat{\alpha} \cdot \hat{\beta}(S) = \big(\sum_T e_n(S,T)\alpha(T)\big)\big(\sum_{T'} e_n(S,T')\beta(T')\big) = \sum_{T,T'} e_n(S,T)e_n(S,T')\alpha(T)\beta(T) =$$

$$\sum_{T,T'} e_n(S,T+T')\alpha(T)\beta(T') = \sum_{T,T'} e_n(S,T)\alpha(T')\beta(T-T') = \big(\sum_T \widehat{\alpha(T)\beta(S-T)}\big) = \big(\widehat{\alpha *_1 \beta}\big)(S)$$

and with the previous lemma, the given map is an isomorphism. □

4 Case $n = 2$: comparing with quartic algebras

In the previous section, we constructed algebras of the form R_ρ, representing the etale algebra of a class of $E[n]$-torsors. However, we know that its multiplication is twisted and it would be more useful to have a componentwise multiplication instead. In order to get that, we would like to classify the torsors in terms of other algebras of dimension p^2. We take advantage of the work done in [2] classifying these algebras for $n = 2$ and $n = 3$.

4.1 Quartic algebras

Fix $n = 2$. We expect to associate to each 2-covering a finite scheme of 4 points. Using the same arguments as in Lemma 2.2, we know that these torsors can be constructed as the preimages of the rational points by the multiplication by 2 map. The algebras that we are looking for are those appearing as coordinate rings of these schemes.

Proposition 4.1. For every locally soluble 2-covering (C, π), we get a corresponding quartic curve $C' : y^2 = g(x)$, which is K-isomorphic to C.

Proof. All the details of the proof can be found in [2, Prop 2.1.5]. As a sketch, we can say the argument relies on the existence of a K-rational divisor D on the curve to which we can apply Riemann-Roch theorem, in order to find relations between the generators of $H^0(K, \mathcal{O}_C(2D))$ and $H^0(K, \mathcal{O}_C(4D))$. □

These curves can be homogenized in the weighted projective space $\mathbb{P}^2(1, 2, 1)$ as $y^2 = g(x, z)$ and then we can talk about the rational maps to E forming the 2-covering. This way, we can consider $g(x, z)$ as a binary quartic form, which means homogeneous polynomial of degree 4 in two variables.

The paper [9] determines these maps to E, in terms of some invariants of the quartic. In general, this isogeny will only be a change of multiplicative constants so [9] proves that the generic form of these maps is the projective map:

$$\pi : C \to E$$

$$[X : Y : Z] \to [c_1 Y Z g_4(X, Z) : c_2 g_6(X, Z) : c_3 Y^3 Z^3]$$

where g_4, g_6 are homogeneous polynomials determined from the coefficients of the quartic, and c_1, c_2, c_3 are constants. One can see that this map has degree 4, and that precisely those points mapping to trivial in E are those of the form $[x_i : 0 : 1]$ where x_i are the 4 roots of $g(x, 1)$. This fact indicates that we can send the four points $[x_i : 0 : 1]$ to the 2 torsion points in E.

$$\begin{array}{ccc} E_{\overline{\mathbb{Q}}} & \xrightarrow{2} & E_{\overline{\mathbb{Q}}} \\ {\scriptstyle\theta}\uparrow & \nearrow_{\pi} & \\ C_{\overline{\mathbb{Q}}} & & \end{array}$$

We can fix a root x_1 of $g(x, 1)$ and send it to the trivial point in E with a given isomorphism θ_1 over the field $\mathbb{Q}(x_1)$ which sends the other three roots to the three nontrivial points on $E[2]$. This determines all the possible choices of θ up to composing with some automorphism, as we could define similar maps θ_i for the other roots x_i. [3] In fact, we can relate the number of zeroes of $g(x, 1)$ and the number of division points on a fixed extension K.

Lemma 4.1. There is an isomorphism of schemes over $\operatorname{Spec} K$ between $\pi^{-1}(O)$ and $\operatorname{Spec} K[x]/g(x)$.

Proof. The proof can be found in [9, Prop 4.3] □

At this point, we want to compare the extension over which the map θ is defined with the extension defining γ in the previous sections.

[3] Using the construction of the Weierstrass equation, and assuming we are in characteristic $\neq 2, 3$, we can see that the group $\operatorname{Aut}(E)$ will be of order $6, 4$ or 2 depending on wherther the j invariant is $0, 1728$ or any other value.

Theorem 4.1. The splitting fields of $g(x)$ and γ are the same.

Before proving this result, we can to point an example that makes us confident that we are in the right direction, using the output on **Magma**.

Example 4.1. In the example $E : y^2 = x^3 - x$, the quartics that we can calculate are the following:

$$\{x^4 + 4, x^4 - 6x^2 + 1, 2x^4 + 2\}$$

with splitting fields

$$\{\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}, i)\}$$

and the non trivial γ elements are $\{(1, i, i, 1), (1, 1, \sqrt{2}, \sqrt{2}), (1, i, \sqrt{-2}, \sqrt{2})\}$which are precisely defined over the same fields. We can take some of these quartics and try to define the map θ. For instance, the roots of $x^4 + 4$ are $\{\lambda, -\lambda, i\lambda, -i\lambda\}$ where $\lambda = (1 + i)$. The map θ could be defined as:

$$\theta([X : Y : Z]) = [X + \lambda Z : Y : \frac{X - \lambda Z}{\lambda}]$$

Remark 4.1. These field extensions are the covers of the fppf topology that give the torsor strucrure.

This serves as evidence that we are in the right direction. Nonetheless, if we want to prove the theorem we have to understand how the quartics $g(x, z)$ are constructed, starting from a Selmer group element α. This is precisely the kind of algorithms implemented in **Magma**. The explanation of these algorithms is given in [8] and works both starting with $\alpha \in R^\times$ or $\rho \in (R \otimes R)^\times$. For the case of 2-descent, we start with α a Selmer group element.

The first approach to writing equations for the curve is the set:

$$C = \{(P, z) \in E \times \mathbb{A}(R) \mid F(P) = \alpha z^2\}$$

where A(R) is the affine space corresponding to R. We can claim that the solutions z are the points of the covering curve due to the fact that the image of $P \in E(K)$ after the map F is the image of the curve $C \in H^1(K, E[n])$ by the connecting map. The covering map is given by the projection to the first component.

We write these equations in a generic form, for the 2-descent. Suppose the curve E is given by the equation $y^2 = f(x)$, and that e is a generic zero of f. The element $\alpha \in R^\times$ result of the descent can be written in terms of e as:

$$\alpha = \alpha_0 + \alpha_1 e + \alpha_2 e^2$$

as well as the variable z

$$z = z_0 + z_1 e + z_2 e^2.$$

We will use the coefficients z_i as our projective variables. The homogenized equation for C this case is written as:

$$x - e z_3^2 = \alpha z^2$$

We can equate the coefficients of each e and eliminate the x. What we get after this process are two equations of degree 2 in $\mathbb{P}(z_0, z_1, z_2, z_3)$. One of them does not contain any z_3 coefficient, so it defines a conic S in the projective plane. Moreover, as S appears as the projection of a curve representing a Selmer group element, it has points everywhere locally. Therefore, the local-global principle in degree 2 applies. We can find a rational point on S and we can throw lines from this point that will intersect the conic on only one other point, forming an isomorphism $S \cong \mathbb{P}^1$. This gives a parametrization of z_0, z_1, z_2 as polynomials of degree 2 in two variables a, b. If we substitute these polynomials in the other equation, we finally get $z_3^2 = g(a, zb)$. Let's apply this first to a particular example:

Example 4.2. Let $E : y^2 = x^3 - x$ and $\alpha \in R^\times / R^{\times 2}$ be the element with values $(-1, -1, 1)$ in the points of $E[2]$. The isomorphism:

$$\mathbb{Q}[x]/(x^3 - x) \xrightarrow{\cong} \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \quad x \to (0, 1, -1)$$

allows us to write α in the bases $\{1, e, e^2\} \cong \{(1,1,1),(0,1,-1),(0,1,1)\}$ as $\alpha = -1 - e + e^2$. Then we take $z = z_0 + z_1 e + z_2 e^2$ and we expand the equation:

$$x - ez_3^2 = \alpha z^2 = -z_0^2 - (z_1^2 + (z_0 + z_2)^2)e - (2z_1(z_0 + z_2) - z_0^2)$$

We construct the equations from equalizing the coefficients of e. The last equation is the one representing the conic S. We notice that one rational point on this conic is $[0:0:1]$. All the lines around this point are of the form:

$$z_0 = ua$$

$$z_1 = ub$$

$$z_2 = t$$

where $[a:b] \in \mathbb{P}^1$ is the element determining the line and u, t are the parameters. We have to unravel the parameters inside the equation.

$$u^2a^2 = 2abu^2 + 2btu$$

The case $u = 0$ is the point that we already have so the parameters of the other point are:

$$u = 2b$$

$$t = a^2 - 2ab$$

Therefore, we can write the isomorphism:

$$\mathbb{P}^1 \cong S \; [a:b] \to [2ab : 2b^2 : a^2 - 2ab]$$

Puting these values in the other equation we get:

$$z_3^2 = a^4 + 4b^2$$

However, if we attempt to make this procedure as general as possible for any α, the equations become too complicated and when we get to the point of choosing a rational point, we are already facing too many computational difficulties. Instead, [7] uses a similar method starting with the elements ρ. This is the theoretical background that will give us the proof of theorem 4.1.

4.2 Determining the map g_C

The following construction does not restrict to the case $n = 2$, but proves a similar statement to Theorem 4.1 for any n. The goal is to embed the curve C inside a projective space of the type $\mathbb{P}(A)$ where A is the etale algebra of $E[n]$. As well as in the construction of $\overline{F}$, we could start with the maps that appear in the definition of the Weil pairing. This time, we pick the function g_T satisfying:

$$\mathrm{div}(g_T) = [n]^*T - [n]^*T$$

The same role that in this case, the map $[n]$ plays, can be transfered to the covering $\pi : C \to E$, so we claim the existence of another function $g_{T,C}$ satisfying:

$$\mathrm{div}(g_{T,C}) = \pi^*T - \pi^*O$$

We can pack up all the properties of these functions.

Lemma 4.2. Let $\pi : C \to E$ be an n-covering and ρ, γ the corresponding descent elements of it as in section 3.3. The functions previously defined satisfy:

- If θ satisfies $\pi = [n] \circ \phi$, then:

$$g_{T,C}(P) = \gamma(T)^{-1} g_T(\theta(T)),$$

- The map $T \to g_{T,C}$ is Galois equivariant.
- Let r_{T_1,T_2} be the rational function with the formula:

$$r_{T_1,T_2}(P) = \begin{cases} 1 & T_1, T_2 = O \\ x(P) - x(T_1) & T_1 + T_2 = O \; T_1 = O \\ \frac{y(P)+y(T_1+T_2)}{x(P)-x(T_1+T_2)} - \lambda(T_1, T_2) & \text{otherwise} \end{cases}$$

then we have the formula:

$$r_{T_1,T_2}(\pi(P)) = \rho(T_1, T_2)\frac{g_{T_1,C}(P)g_{T_2,C}(P)}{g_{T_1+T_2,C}(P)}$$

Proof.
- Using the equality $\pi = [n] \circ \phi$, we can see that both functions have the same divisor. If we want the Galois equivariance, we will see that the right constant to multiply is $\gamma(T)$.
- The proof of the Galois equivariance uses several of the interpretations of the cohomology that we defined in section 3.2. Initially, it uses the Galois cohomology cocycle e_σ associated to ρ and the definition of the Weil pairng to see that for $\sigma \in G_K$:

$$\sigma(g_T(\theta(P))) = g_{\sigma(T)}(\theta(\sigma P) + \xi_\sigma) = e_n(\xi_\sigma, \sigma(T))g_{\sigma(T)}(\theta(\sigma P))$$

Also, for $\gamma \in \overline{R}$, the action of G_K is:

$$\sigma(\gamma(T)) = w(\xi_\sigma)(\sigma T)\gamma(\sigma T) = e_n(\xi_\sigma, \sigma T)\gamma(\sigma T)$$

Joining these two facts, we get the desired equation.
- For the last equation, we first need to prove this fact for $r_{T_1,T_2}(nP)$, which one can find in [7] and then the fact for $r_{T_1,T_2}(\pi P)$ arises as:

$$r_{T_1,T_2}(\pi P) = r_{T_1,T_2}(n\theta P) = \frac{g_{T_1}(\theta(P))g_{T_2}(\theta(P))}{g_{T_1+T_2}(\theta(P))} = \rho(T_1, T_2)\frac{g_{T_1,C}(\theta(P))g_{T_2,C}(\theta(P))}{g_{T_1+T_2,C}(\theta(P))}$$

□

These functions pack up to morphisms of schemes:

$$g_C : C \to \mathbb{P}(R)$$
$$g_C(P) = \{T \to g_{T,C}(P)\}.$$

Corollary 4.1. There is a commutative square:

$$\begin{array}{ccc} C & \xrightarrow{g_C} & \mathbb{P}(R) \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \cdot\gamma} \\ E & \xrightarrow{g_E} & \mathbb{P}(R) \end{array}$$

This serves as proof of Theorem 4.1, in the case $n = 2$, as the maps θ and the multiplication by γ are defined over the same number field. [7] also gives equations of the images of the maps g_C. In particular, there is a set of $\frac{n^2(n^2-3)}{2}$ equations defined with the variables z_T of the coordinate functions in $\mathbb{P}(R)$. Some of the equations take the form:

$$(x(T_1) - x(T_2))z_O^2 + \rho(T_1, -T_1)z_{T_1}z_{-T_1} - \rho(T_2, -T_2)z_{T_2}z_{-T_2}$$

for $T_1, T_2 \neq 0$ and some others take the form:

$$(\lambda(T_{11}, T_{12}) - \lambda(T_{21}, T_{22}))z_O z_{T_{11}+T_{12}} - \rho(T_{11}, T_{12})z_{T_{11}}z_{T_{12}} + \rho(T_{21}, T_{22})z_{T_{21}}z_{T_{22}}$$

where $T_{11}, T_{12}, T_{21}, T_{22} \neq O$ satisfying $T_{11} + T_{12} = T_{21} + T_{22} \neq O$. In the case $n = 2$, only the first type of equations appears and one can use the same methods as before in order to recover the quartic equations. For more details on how these equations are constructed, one can check [8]. However, in order to write down the dual pair with the quartic algebras, we need to make the diagram of Corollary 4.1 explicit.

4.3 Dual pair interpretation

Once we have all the tools, the point is to be able to rewrite the dual pairs of algebras, from the information we have got from the descent process and the quartic equations.

Initially, we have the group scheme $E[2]$ with the corresponding dual pair of algebras (A, B, Φ). We claim that the dual pair is the same triple (A, B, Φ), but with the multiplication on A twisted as previously. In this case, we are only regarding B as a module over the corresponding number field.

Then, we use the base change of A_ρ in order to construct a new pairing (T, U, Ψ). In order to determine the particular base change, we could try to construct the isomorphism from T to A_ρ as the composition of maps:

$$T \xrightarrow{\theta^*} A \xrightarrow{\text{Fourier transform}} A_1 \xrightarrow{\overline{\gamma}} A_\rho$$

where θ is determined by factoring the coverings 2 and π, and $\overline{\gamma}$ is the multiplication by γ isomorphism over $\overline{\mathbb{Q}}$. However, this method is not quite feasible as the first and last arrows are not defined over $\mathbb{Q}$ and one should find the correct bases on which the whole composition is well-defined over $\mathbb{Q}$. Instead, the most reasonable idea is to try to realise A_ρ as an algebra isomorphic to T by finding the minimal polynomial of one of their elements, and then constructing the change of bases.

On T, we can fix $\{1, x, x^2, x^3\}$ if the algebra forms a field of degree 4 and $\{1, x, y, xy\}$ if it splits as two quadratic fields. Once we have P the matrix of change of bases, we compute $(P^{-1})^T$ as the dual matrix of change of bases. On the other hand, B remains with the twisted comultiplication as it is isomorphic to the dual of A, so we have to multiply the fourier transfrom matrix on the left. Therefore, the matrix of the dual pair Ψ on this bases of T is:

$$\Psi = P^T \Phi$$

The choice of the element of which we try to find the minimal polynomial is random. We have to make sure that this point has the required degree and we check that its minimal polynomial spans an isomorphic algebra to T.

Remark 4.2. It can happen that the polynomial that we find is not the same as the one we have as reference from the descent implemented in **Magma**, but they still generate the same algebra. If the one given in **Magma** is substantially more simple than the one we get, we can compose the change of bases with the corresponding isomorphism of fields. We use **Sage** to find these isomorphisms.

We put one example and use the same strategy for the rest of computations.

Example 4.3. Take the elliptic curve $y^2 = x^3 - x$ and the quartic curve $y^2 = x^4 + 4$ which spans the same algebra as the element $\gamma = (1, i, i, 1)$. We saw in example 3.6 that the corresponding ρ element is given by:

$$\rho = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Take $X = (0, 0, 1, 1)$, then all its powers using the twisted multiplication are given by:

$$1 = (1, 0, 0, 0) \quad X = (0, 0, 1, 1) \quad X^2 = (0, 2, 0, 0) \quad X^3 = (0, 0, 2, -2) \quad X^4 = (-4, 0, 0, 0)$$

Therefore, the matrix of the change of bases from A_ρ to T is:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & -2 \end{pmatrix}$$

Using the dual pair matrix Φ calculated in the initial section, we calculate:

$$\Psi = P^T \Phi F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 4 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 8 & -8 \end{pmatrix}$$

Finally, I put a summary of all the 2-descent process for the different cases of splitting of the polynomial $f(x)$ defining $y^2 = f(x)$. These are characterized by whether $f(x)$ has 0, 1 or 3 rational roots.

Example 4.4. Example of an elliptic curve with $f(x)$ having 3 rational roots.

Elliptic curve	$y^2 = x^3 - x$
(A, B)	$\mathbb{Q}^4$
Φ	$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$
S	$\{2\}$
$E(\mathbb{Q})/2E(\mathbb{Q})$	$\{O, (0,0), (1,0), (-1,0)\}$
Analytic order of Ш	1
Order of the Selmer group	4
$\operatorname{im} w_1 \subset H^1(K, E[n], S)$	Order 16
Non-trivial Selmer group elements α	{(1,-1,-1,1), (1,1,2,2), (1,-1,-2,2)}
Quartics defining T	$\{\mathrm{x}^4 + 4, x^4 - 6x^2 + 1, 2x^4 + 2\}$
Matrices Ψ of the dual pairs	(-1,-1,1) $\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & -2 \end{pmatrix}$ (1,2,2) $\to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ (-1,-2,2) $\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

Example 4.5. An example of a curve with $f(x)$ having 1 rational root.

Elliptic curve	$y^2 = x^3 - 1$
(A, B)	$\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\omega)$ [4]
Φ	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & -\frac{1}{3} & \frac{2}{3} \\ 0 & 0 & \frac{2}{3} & -\frac{4}{3} \end{pmatrix}$
S	{2,3}
$E(\mathbb{Q})/2E(\mathbb{Q})$	{O, (1,2)}
Analytic order of Ш	1
Order of the Selmer group	2
$\operatorname{im} w_1 \subset H^1(K, E[n], S)$	Order 8
Non-trivial Selmer group elements α	$\{(1, 3, -2\omega - 1)\}$
Quartics defining T	$\{x^4 - 6x^2 - 3\}$
Matrices Ψ of the dual pairs	$\begin{pmatrix} 2 & 2 & -2 & -10 \\ \frac{2}{3} & -\frac{2}{3} & 2 & 6 \\ \frac{4}{3} & -\frac{4}{3} & -4 & 4 \\ \frac{13}{3} & -\frac{1}{3} & -11 & 11 \end{pmatrix}$

Example 4.6. Example of an elliptic curve with $f(x)$ being irreducible over $\mathbb{Q}$.

Elliptic curve	$\mathrm{y}^2 = x^3 - 2$
(A, B)	$\mathbb{Q} \times \mathbb{Q}(\sqrt[3]{2})$
Φ	$\begin{pmatrix} \frac{1}{4} & \frac{3}{4} & 0 & 0 \\ \frac{3}{4} & -\frac{3}{4} & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 3 & 0 \end{pmatrix}$
S	{2}
$E(\mathbb{Q})/2E(\mathbb{Q})$	{(3,5)}
Analytic order of Ш	1
Order of the Selmer group	2
$\operatorname{im} w_1 \subset H^1(K, E[n], S)$	Order 2
Non-trivial Selmer group elements	$\{(1, \sqrt[3]{2} - 1)\}$
Quartics defining T	$\{\mathrm{x}^4 - 12x^3 - 16x^2 - 12\}$
Matrices Ψ of the dual pairs	$(\sqrt[3]{2} - 1, \omega\sqrt[3]{2} - 1, \omega^2\sqrt[3]{2} - 1) \to \begin{pmatrix} 55 & -53 & \frac{35}{2} & -\frac{37}{2} \\ 6 & -6 & -6 & 6 \\ 48 & -48 & \frac{51}{2} & -\frac{45}{2} \\ 24 & -24 & 0 & 0 \end{pmatrix}$

Finally, we need to perform some calculation that proves that these is not some random output, but Ψ encodes the information of a torsor. This means giving some evidence that after taking points on the algebra, the matrices describe the aciton of $E[2](L)$ on $X(L)$ for X a torsor and L a suitable number field. In order to do this, we have to interpret the L-points of $E[2]$ and X as maps $A, T \to L$, then use Φ and Ψ to get elements of $B \otimes L$ and $U \otimes L$, and finally use the module structure on them to perform the action.

Example 4.7. Let E be the elliptic curve $E : y^2 = x^3 - x$ and let X be the torsor correponding to the element $\alpha = (1, -1, -1, 1)$ result of the descent, with quartic algebra $T = \mathbb{Q}[x]/(x^4 + 4)$. We know from Example 4.5 that the dual pair of $E[2]$ is given by:

$$A = B = \mathbb{Q}^4$$

and the matrix of Φ in the canonical bases is:

$$\Phi = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

On the other hand, the torsor dual pair is given by the triple (T, U, Ψ) is given by T the quartic algebra, $U = B$ and Ψ is given in the basis $\{1, x, x^2, x^3\}$ of T and the natural basis for U as the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & -2 \end{pmatrix}$$

The four $\overline{\mathbb{Q}}$-points of $E[2]$ can be seen as morphisms $p_i : A \to \overline{\mathbb{Q}}$ that send:

$$p_0, p_1, p_2, p_3 : A \otimes L \to L \quad p_i : (a, b, c, d) \to \begin{cases} a & i = 0 \\ b & i = 1 \\ c & i = 2 \\ d & i = 3 \end{cases}$$

and, in order to translate them to elements $v_i \in B \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$, we have to solve:

$$(a, b, c, d)\Phi v_i = p_i((a, b, c, d))$$

which in this case, means:

$$v_i = \Phi^{-1} e_i$$

where e_i is the canonical basis of $\mathbb{Q}^4$. The points that we get are:

$$v_0 = (1, 1, 1, 1)$$

$$v_1 = (1, 1, -1, -1)$$

$$v_2 = (1, -1, 1, -1)$$

$$v_3 = (1, 1, -1, -1)$$

In the case of the torsor X, we have four morphisms $q_i : T \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, which are sending x to each of the roots λ_i of $x^4 + 4$, which we can order as $\{\lambda_0 = (1 + i), \lambda_1 = -(1 + i), \lambda_2 = (1 - i), \lambda_3 = -(1 - i)\}$, so translate to elements $w_i \in U \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ by solving the equation:

$$(a, b, c, d)\Psi w_i = a + b\lambda_i + c\lambda_i^2 + d\lambda_i^3$$

in the basis $\{1, x, x^2, x^3\}$ of T. If we do that we get:

$$w_0 = \big(1, i, i, 1\big)$$

$$w_1 = \big(1, i, -i, -1\big)$$

$$w_2 = \big(1, -i, -i, 1\big)$$

$$w_3 = \big(1, -i, i, -1\big)$$

At this moment, the action:

$$B \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \times U \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to U \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$$

is given by componentwise multiplication and and moves the points of U free and transitively. We can respresent the action in the following table:

U/B	(1, i, i, 1)	(1, i, -i, -1)	(1, -i, i, -1)	(1, -i, -i, 1)
(1, 1, 1, 1)	(1, i, i, 1)	(1, i, -i, -1)	(1, -i, i, -1)	(1, -i, -i, 1)
(1, 1, -1, -1)	(1, i, -i, -1)	(1, i, i, 1)	(1, -i, -i, 1)	(1, -i, i, -1)
(1, -1, 1, -1)	(1, -i, i, -1)	(1, -i, -i, 1)	(1, i, i, 1)	(1, i, -i, -1)
(1, -1, -1, 1)	(1, -i, -i, 1)	(1, -i, i, -1)	(1, i, -i, -1)	(1, i, i, 1)

This serves as proof that the torsor dual pairs do really encode all the information of the torsors over this group schemes.

5 Case $n = 3$

Finally, we give a sketch of how the procedure should be constructed for $n = 3$. In many examples, we have trivial $\mathrm{Sel}^3(K, E)$, so we start by finding in **Magma**, an elliptic curve, for which the command **ThreeDescent** gives non-trivial output.

On the other hand, we have to find the algebraic structure of $E[3]$. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. We usually impose equations on the x-coordinate of a point on the curve by noting that if $P = (x, y)$ is a non-zero 3-torsion point, then it satisfies the condition $-P = [2]P$. These condition can be written in terms of a polynomial as:

$$3x^4 + 6ax^2 + 12bxa^2$$

Therefore, the algebra with which we are dealing is:

$$A = \mathbb{Q} \times \mathbb{Q}[x, y]/(y^2 - x^3 - ax - b, 3x^4 + 6ax^2 + 12bxa^2)$$

Example 5.1. Let E be the elliptic curve $y^2 = x^3 - 1$. The complex points on $E[3]$ are:

$$\{O, (0,1), (0,-1), (-\sqrt[3]{4}, \sqrt{-3}), (-\sqrt[3]{4}, -\sqrt{-3}), (-\omega\sqrt[3]{4}, \sqrt{-3}), (-\omega\sqrt[3]{4}, -\sqrt{-3})(-\omega^2\sqrt[3]{4}, \sqrt{-3}), ((-\omega^2\sqrt[3]{4}, -\sqrt{-3})\}$$

and the etale algebra $R = \mathbb{Q} \times A$ has the non-trivial component as:

$$A = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3}) = A_1 \times A_2$$

where A_1 is formed by the first two factors and A_2 by the other number field. We proved that the matrix of the dual pairing is:

$$\Phi = \begin{pmatrix} 1/9 & 1/9 & 1/9 & \frac{2}{3} & 0 & 0 & 0 & 0 & 0 \\ 1/9 & 1/9 & 1/9 & -\frac{1}{3} & 0 & 0 & -1 & 0 & 0 \\ 1/9 & 1/9 & 1/9 & -\frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -8 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{9}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{9}{8} & 0 \end{pmatrix}.$$

We start by using A as the etale algebra. Firstly, we need to realize A as a polynomial algebra. In order to do that, we find the minimal polynomial of the element $\sqrt{-3} - \sqrt[3]{4}$, which is:

$$f(x) = x^6 + 9x^4 + 8x^3 + 27x^2 - 72x + 43.$$

Then, calculate $A(\mathcal{S}, 3)$ where $S = \{3\}$ is formed by the elements:

$$\{\pm 1, \pm 3\} \times \{\pm 1, \pm 3\} \times \Big\{ \big(-\sqrt{1 - \sqrt[3]{4}}\big)^{i_1}, \big(\frac{1}{2} + \frac{\sqrt{-3}}{2}\big)^{i_2}, \big(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt{-3}}{3} + \frac{\sqrt[3]{2}\sqrt{-3}}{6} + \frac{\sqrt[3]{4}\sqrt{-3}}{3}\big)^{i_3}, \big(\frac{\sqrt[3]{4}}{2} + \sqrt{\frac{\sqrt[3]{4}}{2} - 1}\big)^{i_4}$$

$$i_1, i_2, i_3, i_4 \in \mathbb{Z}/3\mathbb{Z} \Big\}$$

The next step is to understand how to deal with the norm conditions coming from $A = \mathrm{Map}_{\mathbb{Q}}(E[3] - \{0\}, \overline{\mathbb{Q}})$, $B = \mathrm{Map}_{\mathbb{Q}}(E[3]^D - \{0\}, \overline{\mathbb{Q}})$ and $D = \mathrm{Map}_{\mathbb{Q}}(Y, \overline{\mathbb{Q}})$ as in section 3.5.

One can write down all the possible lines on the $E[3]$ configuration not passing through $\{0\}$ and one arrives to the conclusion that:

$$B = \mathbb{Q}(\sqrt{-3}) \times \mathbb{Q}(\sqrt[3]{4}) \times \mathbb{Q}(\sqrt[3]{4}) = B_1 \times B_2$$

where $B_1 = \mathbb{Q}(\sqrt{-3})$ and $B_2 = \mathbb{Q}(\sqrt[3]{4}) \times \mathbb{Q}(\sqrt[3]{4})$. The algebra D coincides is:

$$D = \mathbb{Q}(\sqrt[3]{4}) \times \mathbb{Q}(\sqrt[3]{4}) \times \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3}) \times \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3}) \times \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3}) = D_1 \times D_2 \times D_3$$

where $D_1 = \mathbb{Q}(\sqrt[3]{4}) \times \mathbb{Q}(\sqrt[3]{4})$, $D_2 = \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3})$ and $D_3 = \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3}) \times \mathbb{Q}(\sqrt[3]{4}, \sqrt{-3})$. After applying the norm conditions on the image, we get that the embedding of $\alpha = (\alpha_1, \alpha_2) \in A$ inside D as $(\alpha_1, \alpha_2, \alpha_2)$ and the norm to B corresponds to:

$$(N_{A_2/B_1}(\alpha_2), \alpha_1 \operatorname{Nm}_{D_3/B_2}(\alpha_2^\rho))$$

where ρ is the automorphism of D_3 sending $\sqrt[3]{4}$ to $\omega^{-1}\sqrt[3]{4}$ with ω is a third root of unity. Therefore, the conditions on the elements of A to be in the image of $H^1(K, E[3])$ are:

$$\big\{(\alpha_1, \alpha_2) \in A_1^\times/A_1^{\times 3} \times A_2^\times/A_2^{\times 3} \mid \operatorname{Nm}_{A1/K}(\alpha_1) \in K^{\times 3},\ \operatorname{Nm} A_2/A_{+2}(\alpha_2) \in A_{+2}^{\times 3}$$

$$i_{B_2/A_1}(\alpha_1) \operatorname{Nm}_{D_3/B_2}(\alpha_2^\rho) \in B_2^{\times 3},\ \operatorname{Nm}_{A_2/B_1}(\alpha_2) \in B_1^{\times 3}\big\}$$

which translated to our curve over $\mathbb{Q}$ is:

$$\big\{(a_1, a_2, a_3 - a_4\sqrt[3]{4} + 2a_5\sqrt[3]{2} + a_6\sqrt{-3} - a_7\sqrt[3]{4}\sqrt{-3} + 2a_8\sqrt[3]{2}\sqrt{-3}) \in A_1^\times/A_1^{\times 3} \times A_2^\times/A_2^{\times 3} \mid a_1a_2 \in \mathbb{Q}^3$$

$$(a_3 - a_4\sqrt[3]{4} + 2a_5\sqrt[3]{2})^2 + 3(a_6 - a_7\sqrt[3]{4} + 2a_8\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{4})^{\times 3}$$

$$-(a_3+\sqrt{-3}a_6)^3-24(a_3+\sqrt{-3}a_6)(a_4+\sqrt{-3}a_7)(a_5+\sqrt{-3}a_8)-4(a_4+\sqrt{-3}a_7)^3+128(a_5+\sqrt{-3}a_8)^3 \in \mathbb{Q}(\sqrt{-3})^{\times 3}\big\}$$

Instead of finding which of the elements on $A(\mathcal{S}, 3)$ satisfy these conditions. We pick one of them which is simple enough. For sake of simplicity, we can also skip the computation of the local conditions. Therefore, the dual pair that we will construct will correspond to an element in $H^1(K, E[3], \mathcal{S})$.

Once this is done, it is possible to prove that the image of the curve C in $\mathbb{P}^8$ is contained in the image of the Segre embedding $\mathbb{P}^2 \times \mathbb{P}^2 \to \mathbb{P}^8$. This allows the projection to one of the components in order to get a curve in $\mathbb{P}^2$. [2] arrives to the same parametrization of the selmer group using another path, in this case, proving a similar result to Theorem 4.1. In this case, instead of quartic curves, we get ternary cubics, which are given by equations of the form:

$$ax^3 + by^3 + cz^3 + dxy^2 + ex^2y + fxz^2 + gx^2z + hy^2z + iyz^2 + lxyz$$

However, in order to get an algebra of degree 9 representing the torsor, we would also need to find which points of these ternary cubics map to the trivial point in E, after the 3-covering.

In this particular case, the equations for these points are not as simple as in the case of $p = 2$, so it is quite more difficult to give an elegant example for these curves for instance, in the case of our example, the result of three descent implemented in **Magma** is the ternary cubic curve:

$$x^2y + xy^2 - xz^2 + y^2z + yz^2 + z^3$$

in $\mathbb{P}^2$ and the covering map is given in the appendix and one easily see a big number of equations.

Once performed the descent, one can derive equations for the curve using the construction in the section 4.2, and get 27 equations in $\mathbb{P}^8$. Concerning the methods of descent, many of the papers stated in the literature focus on the fact of needing to trivialize the algebras A_ρ in order to construct the Selmer group, which means constructing an isomorphism $A_\rho \cong \operatorname{Mat}_n(K)$. In [7] and [8] a "black box" is used at this point, meaning that he presupposes known and claims the existence of this isomorphism and decomposes the algebra as $A_\rho \cong \{\mathrm{id}\} \oplus \{\mathrm{tr} = 0\}$.

However, we can try to follow a similar method as before, without the given reference of **Magma**. Namely, taking an element and computing its minimal polynomial using the twisted multiplication.

Example 5.2. (end of example 5.1) For sake of simplicity, I pick the element $\alpha = (1, 1, \frac{1}{2} + \frac{\sqrt{-3}}{2})$, which represents a torsor class not necessarily locally trivial, and try to write an algebra of degree 9 for the

corresponding torsor structure. The element ρ corresponding to it is the matrix:

$$\rho = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & e^{\frac{\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} & 1 \\ 1 & 1 & 1 & 1 & e^{-\frac{\pi i}{3}} & 1 & e^{-\frac{\pi i}{3}} & 1 & e^{-\frac{\pi i}{3}} \\ 1 & 1 & 1 & e^{\frac{\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} & 1 \\ 1 & 1 & 1 & 1 & e^{-\frac{\pi i}{3}} & 1 & e^{-\frac{\pi i}{3}} & 1 & e^{-\frac{\pi i}{3}} \\ 1 & 1 & 1 & e^{\frac{\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} & 1 \\ 1 & 1 & 1 & 1 & e^{-\frac{\pi i}{3}} & 1 & e^{-\frac{\pi i}{3}} & 1 & e^{-\frac{\pi i}{3}} \end{pmatrix}$$

In order to write this matrix, I have needed to choose a basis of $E[3] \cong \big(\mathbb{Z}/3\mathbb{Z})^2$. Namely, we choose the points $(0,1)$ and $(-\sqrt[3]{4}, \sqrt{-3})$. Then, the rest of the elements on the list of points of $E[3]$ correspond to a particular element of $\big(\mathbb{Z}/3\mathbb{Z})^2$. The rows and columns of the matrix are ordered in the same way as the previous list of points.

Remark 5.1. We have checked the conditions $\partial\rho = 1$ and $\alpha(T) = \prod_{i=0}^{2} \rho(T, iT)$, noting the computational difficulty that we have when the 3rd roots of unity belong to A, which is the case.

Remark 5.2. I have had difficulties on writing the twisted multiplication in this case explicitly, but one should pick up an element of the ring and calculate its minimal polynomial in order to get an algebra T and use all its powers in order to get the base change and getting a dual pair matrix Ψ.

6 Future work

The thesis has covered the two cases that were expected initially, applying the descent for the low cases of $n = 2, 3$. The methods of explicit descent were already covered in the literature, as well as similar things to the representation of the μ_n torsors in terms of algebras. The most relevant contribution of this work is the realization of this group schemes as algebras and the connection of these with the already stated methods. Note that the representations for these two examples are in terms of a torus ($\mathbb{G}_m$) and an abelian variety (E), which gives the ideas for the possible future generalization. For instance, if we can construct a presentation of any finite commutative group scheme $\mathcal{G}$ in terms of abelian varieties over a field K as:

$$0 \to \mathcal{G} \to \mathcal{A} \to \mathcal{B} \to 0$$

one could try to derive similar methods than the one of descent, trying to understand the cohomological objects with which we have dealt, like $H^1_{\text{fppf}}(K, \mathcal{A})$ and the K-points of $\mathcal{B}(K)$. A similar generalization could be deduced for the case of algebraic tori, however, the objects in discussion are not as known as the ones we have treated during this thesis.

On another order of things, we have not dealt during this thesis with examples of positive characteristics.

The other relevant thing to do is finish the computational implementation of these torsors in **Sage**.

Finally, as mentioned on the previous chapter, this thesis does not deal with the obstruction maps on the algebras R_ρ, and their presentation as matrix algebras. In [6], a part from all the explicit descent arguments that we used, the authors deal with this situation for a method changing the role of the central extension Λ by theta groups Θ, and the role of their sections γ by sections sending T to a particular matrix M_T. It is possible that using these objects, we can construct a shortcut for the computation of the dual pairs. However, it is too soon to claim what would be a shortcut, because the torsor dual pairs are still pending to be implemented in **Sage**.

7 Appendix 1: the injectivity of w_1

The goal of this section is to present the proof of the injectivity of the map w_1, which has been central on the second part of all our discussion. I could perfectly give the right reference to it, as I have done with many other results. Nonetheless, I believe that for what I have learnt in my years of study, maths are grounded on the originality of giving methods of proof, instead of in the depth of the results. Therefore, showing the core of this proof seems interesting on itself to me.
The only injectivity that we have to prove is the one of the map $H^1(K, E[p]) \to H^1(K, \mu_p(\bar{R}))$ as the other component of the map w_1 is the Kummer isomorphism. The case $p = 2$ has already been treated in Theorem 3.4, so we suppose p is odd. The proof of the injectivity is firstly grounded in seeing $E[p] \cong \mathbb{F}_p^2$ and therefore interpreting:

$$\mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

which has order $p(p+1)^2(p-1)$. One also knows that there is a subgroup which corresponds to the Galois group $\mathrm{Gal}(L/K)$, where $L = K(E[p])$. From now, on we will be dividing the cases. Firstly, on checking whether p divides the order of $\mathrm{Gal}(L/K)$.

Lemma 7.1. If p does not divide the order of the Galois group, then $H^1(\mathrm{Gal}(L/K), E[p]) = 0$.

Proof. It is well known from Galois cohomology that if the orders of the group and the module are coprime, the cohomology vanishes. □

Therefore, in this case, there would be nothing to prove about injectivity. On the other hand, if p divides the order of $\mathrm{Gal}(L/K)$, we know about the existence of a p-Sylow subgroup S, of $\mathrm{Gal}(L/K)$.

Lemma 7.2. If S is not normal in $\mathrm{Gal}(L/K)$, then $\mathrm{Gal}(L/K) \subset \mathrm{GL}_2(\mathbb{F}_p)$ contains $\mathrm{SL}_2(\mathbb{F}_p)$.

Proof. There are some particular subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, the Borel subgroups, which, in some bases, can be written in the matrix form:

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{F}_p^\times,\ b \in \mathbb{F}_p \right\} \subset \mathrm{GL}_2(\mathbb{F}_p)$$

which have order $p(p-1)^2$ and necessarily have to fix a line l in $\mathbb{F}_p^2$. Then, the elements of order p in $\mathrm{Gal}(L/K)$ can always be represented in the form of a matrix:

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

which necessarily fix one line in $\mathbb{F}_p^2$. If all the lines fixed by this elements are the same, then $\mathrm{Gal}(L/K)$ fixes this line too, therefore it is contained in the Borel subgroup defined by this line. But, in this case, once fixed the bases, the group generated by the matrix x is the only possible p-subgroup of the Borel subgroup, therefore, it is normal.
Them, we have to suppose that there are different lines fixed by different order p elements of $\mathrm{Gal}(L/K)$ and we could write two of these elements as:

$$x = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad y = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

where $a, b \neq 0$. These subgroups generate $\mathrm{SL}_2(\mathbb{F}_p)$. □

We base many of the proofs on the classical Galois cohomology inflation-restriction sequence, which says that given a group G, a G-module M and a normal subgroup H, there is an exact sequence:

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M)$$

Lemma 7.3. Let p be an odd prime, then $H^1(\mathrm{SL}_2(\mathbb{F}_p), E[p]) = 0$.

Proof. We apply the sequence to the subgroup generated by $-\mathrm{id}$ in $\mathrm{SL}_2(\mathbb{F}_p)$, having a quotient J. Therefore the sequence writes as:

$$0 \to H^1(J, E[p]^{-\mathrm{id}}) \to H^1(\mathrm{SL}_2(\mathbb{F}_p), E[p]) \to H^1((-\mathrm{id}), E[p])$$

where the first is trivial as $E[p]^{-\mathrm{id}} = 0$ and the last is trivial by coprimality of $E[p]$ and $(-\mathrm{id})$. □

Lemma 7.4. If S is not normal in $\mathrm{Gal}(L/K)$, then w_1 is injective.

Proof. In this case, $\mathrm{SL}_2(\mathbb{F}_p)$ is normal in $\mathrm{Gal}(L/K)$ as it arises as the kernel of the determinant. Let J be the quotient, and we can use again the inflation-restriction sequence:

$$0 \to H^1(J, E[p]^{\mathrm{SL}_2(\mathbb{F}_p)}) \to H^1(\mathrm{Gal}(L/K), E[p]) \to H^1(\mathrm{SL}_2(\mathbb{F}_p), E[p])$$

and again $E[p]^{\mathrm{SL}_2(\mathbb{F}_p)}$ is trivial and the last cohomology group is trivial by lemma 7.3, therefore $H^1(K, E[p]) = 0$. □

Lemma 7.5. If $S = \mathrm{Gal}(L/K)$, then w_1 is injective.

Proof. In this case, S is cyclic generated by an element g. Take $E[p]$ as a S-module. We can use results of Galois cohomology to see that $H^1(S, E[p])$ is isomorphic to the quotient of the norm $\mathrm{Nm} : E[p] \to E[p]$:

$$\mathrm{Ker}(\mathrm{Nm}) / \mathrm{im}(g - 1)$$

The first is isomorphic to the whole $E[p]$ and the second coincides with the invariants $E[p]^S = E[p]^{\mathrm{Gal}(L/K)}$. Therefore, a nontrivial element in $H^1(K, E[p])$, corresponds to an element which is not fixed by $\mathrm{Gal}(L/K)$, and therefore maps to a nontrivial element in $H^1(K, \mu_p(R))$. □

This lemma also proves the injectivity of the map $H^1(S, E[p]) \to H^1(S, \mu_p(R))$, with S being a p-Sylow subgroup for any $\mathrm{Gal}(L/K)$, but we have to extend it to the whole $H^1(K, E[p])$.

Lemma 7.6. If S is normal in $\mathrm{Gal}(L/K)$, then w_1 is injective.

Proof. Take J the quotient of $\mathrm{Gal}(L/K)$ by S. We can extend the inflation-restriction sequence to:

$$0 \to H^1(J, E[p]^S) \to H^1(K, E[p]) \to H^1(S, E[p])^J \to H^2(J, E[p]^S)$$

and the fact that p does not divide the order of J gives $H^i(J, E[p]^S) = 0$ for $i > 0$, implying $H^1(K, E[p]) \cong H^1(S, E[p])^J$. The previously mentioned injectivity for $H^1(S, E[p])$ implies the injectivity for $H^1(S, E[p])^J$, and therefore the result. □

At this point, all the possible cases have already been treated.

8 Appendix 2: List of Sage and Magma commands used

The example computations from chapters 2 to 5 have used many commands of **Sage** and **Magma**. For matrix multiplications, I also used **Pari/GP**, but no further implemented command.

In chapter 2, I did not use any specific command, due to the simplicity of the examples with which I did deal. However, it can be mentioned that the command **K.selmer_group()** of **Sage** computes generators of the group $K_S(n)$ for the scheme $\mathrm{Spec}(\mathcal{O}_{K,\mathcal{S}})$ given a number field K. The input are a finite set of primes S and the number n. For example, let $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{S} = \emptyset$ and $n = 2$, which is an example we used.

```
K.<a> = NumberField(x^2 + 5)
S = K.primes_above(1)
K.selmer_group(S,2)
    [-1,2]
```

These are the same commands used in chapter 3 to compute $A(S,2)$ but in this case, it is required to get generators of each number field component. In some cases, I also used the commands S-units and S-class group of these fields like **K.S_class_group(S)** or **UnitGroup(K,S=tuple(S))**. In any case, once computed the generators of $A(S,2)$, I have needed to calculate the norms of these elements, and seeing whether they are squares (or n-th powers on higher descents). There are many ways to calculate these norms, like calculating the minimal polynomials of these elements and taking $(-1)^r a_0$ where a_0 is the constant coefficient and r is the degree of the field.

```
K.<a> = NumberField(x^3 - 2)
S = K.primes_avobe(6)
Sel = K.selmer_group(S,2)
    [a, a + 1, -1, a - 1]
[(x).norm() for x in Sel]
    [2,3,-1,1]
```

Therefore, the only way to generate a nontrivial element in x^3-2 with square norm would be taking $\sqrt[3]{2}-1$.

There are basic commands for finding invariants of an elliptic curve such as the conductor or the Tamagawa numbers. Take the elliptic curve $E : y^2 = x^3 + 5x$.

```
E = EllipticCurve([5,0])
E.conductor()
    1600
E.tamagawa_numbers()
    [1,2]
```

Initially, I thought of the torsors coming from rational points as the preimages of these points by the multiplication by n map, and I used the following commands to get the algebra on which the x-coordinate of these points taking values. That's why I used the following **Sage** commands.

```
E = EllipticCurve([5,0])
P = E([20,90])
P.division_points(2,poly=true)
    x^4 - 80*x^3 - 10*x^2 - 400*x + 25
```

But then, I realised that the thesis was going to focus on how to recover the curves representing Selmer group elements from $\alpha \in R^\times/R^{\times n}$, which is implemented in **Magma** as the command **TwoDescent**. This gives you also the mapping from the curve to E, that defines the covering. **Magma** represents the projective variables X, Y, Z as \$.1, \$.2, \$.3,

```
E = EllipticCurve([5,0])
TwoDescent(E)
```

```
Hyperelliptic Curve defined by y^2 = x^4 - 20 over Rational Field,
Hyperelliptic Curve defined by y^2 = x^4 - x^3 - x - 1 over Rational Field,
Hyperelliptic Curve defined by y^2 = -x^4 + 20 over Rational Field

Mapping from: Hyperelliptic Curve defined by y^2 = x^4 - 20 over Rational
Field to Elliptic Curve defined by y^2 = x^3 + 5*x over Rational Field
with equations :
20*$.1^2*$.2*$.3^2
-10*$.1^5*$.3 - 200*$.1*$.3^5
$.2^3,

Mapping from: Hyperelliptic Curve defined by y^2 = x^4 - x^3 - x - 1 over
Rational Field to Elliptic Curve defined by y^2 = x^3 + 5*x over Rational
Field
with equations :
1/4*$.1^4*$.2 + 2*$.1^3*$.2*$.3 + 7/2*$.1^2*$.2*$.3^2 - 2*$.1*$.2*$.3^3 +
    1/4*$.2*$.3^4
-9/8*$.1^6 - 7/2*$.1^5*$.3 + 35/8*$.1^4*$.3^2 - 5*$.1^3*$.3^3 -
    35/8*$.1^2*$.3^4 - 7/2*$.1*$.3^5 + 9/8*$.3^6
$.2^3,

Mapping from: Hyperelliptic Curve defined by y^2 = -x^4 + 20 over Rational
Field to Elliptic Curve defined by y^2 = x^3 + 5*x over Rational Field
with equations :
20*$.1^2*$.2*$.3^2
10*$.1^5*$.3 + 200*$.1*$.3^5
$.2^3
```

There are also **Magma** commands for 3-descent and higher descent, but some of them are not calculated through the same algorithms we mentioned before. For instance, for n-descent with n not prime, we remarked that the algorithm with $\alpha \in R^\times/R^{\times n}$ does not work, and there are similar methods using $\rho \in (R \otimes R)^\times/\partial R^\times$.

In the case of the charts in the fifth chapter, we checked the existence of isomorphisms between the algebras spanning the two polynomials using **Sage**.

```
(x^4 - 64).factor()
    (x^2 + 8)*(x^2 - 8)
(x^4 - 6*x^2 + 1).factor()
    (x^2 + 2*x - 1)*(x^2 - 2*x - 1)
L.<b> = NumberField(x^2 - 2*x - 1)
K.<a> = NumberField(x^2 - 8)
K.is_isomorphic(L)
    True
```

A part from the existence of this isomorphism, one might also want to find explicit isomorphisms.

```
list(K.Hom(L))
    [Ring morphism:
   From: Number Field in a with defining polynomial x^2 - 8
   To:   Number Field in b with defining polynomial x^2 - 2*x - 1
   Defn: a |--> 2*b - 2, Ring morphism:
   From: Number Field in a with defining polynomial x^2 - 8
```

```
To:   Number Field in b with defining polynomial x^2 - 2*x - 1
Defn: a |--> -2*b + 2]
```

References

[1] Bruin P. *Dual pairs of algebras and finite commutative group schemes*, Leiden Universiteit, (2017).

[2] Campos Rodríguez A. *Parametrizing the 2-Selmer group and the 3-Selmeg group of an elliptic curve*, Leiden Universiteit, (2016).

[3] Česnavičius K. *Selmer groups as flat cohomology groups*. J. Ramanujan Math. Soc. 31 (2016), no. 1, 31–61.

[4] Česnavičius K. *Selmer groups and class groups*. Compos. Math. 151 (2015), no. 3, 416–434.

[5] Conrad K. *A multivariate Hensel's lemma*. (2010).

[6] Cremona J. E., Fisher T. A., O'Neil C., Simon D., Stoll M. *Explicit n-descent on elliptic curves. I. Algebra.* J. Reine Angew. Math. 615 (2008), 121–155.

[7] Cremona J. E., Fisher T. A., O'Neil C., Simon D., Stoll M. *Explicit n-descent on elliptic curves. II. Geometry.* J. Reine Angew. Math. 632 (2009), 63–84.

[8] Cremona J. E., Fisher T. A., O'Neil C., Simon D., Stoll M. *Explicit n-descent on elliptic curves III. Algorithms.* Math. Comp. 84 (2015), no. 292, 895–922.

[9] Cremona, J. E. *Classical invariants and 2-descent on elliptic curves.* Computational algebra and number theory (Milwaukee, WI, 1996). J. Symbolic Comput. 31 (2001), no. 1-2, 71–87.

[10] Cremona, J. E., Lingham M. P. *Finding all elliptic curves with good reduction outside a given set of primes.* Experiment. Math. 16 (2007), no. 3, 303–312.

[11] Djabri Z., Schaefer E. F., Smart N. P. *Computing the p-Selmer group of an elliptic curve.* Trans. Amer. Math. Soc. 352 (2000), no. 12, 5583–5597.

[12] de Jong J. *Etale cohomology.* Columbia University, (2008).

[13] Hartshorne R. *Algebraic Geometry.* Graduate Texts in Mathematics 52, Springer-Verlag, NewYork, (1977).

[14] Milne J. S. *Arithmetic duality theorems*, Stanford university, (2006).

[15] Milne, J. S. *Elliptic curves.* BookSurge Publishers. (2006).

[16] Milne, J. S. *Fields and Galois Theory.* (v4.40), (2013).

[17] Moonen B., Edixhoven B., Van der Geer G. *Abelian Varieties* , Leiden Universitey, (2014).

[18] Pink R. *Lectures on finite group schemes*, ETH Zürich, (2005).

[19] Poonen, B. *Elliptic curves*, MIT. (2006).

[20] Schaefer E. F. *Computing a Selmer group of a Jacobian using functions on the curve.* Math. Ann. 339 (2007), no. 1.

[21] Schaefer E. F., Stoll M. *How to do a p-descent on an elliptic curve.* Trans. Amer. Math. Soc. 356 (2004), no. 3, 1209–1231.

[22] Serre, J. P. *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, (2002).

[23] Serre, J. P. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* (French) Invent. Math. 15 (1972), no. 4, 259–331.

[24] Silverman, J. H. *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, (2009).

[25] Silverman, J. H., Tate J. *Rational points on elliptic curves.* Second edition. Undergraduate Texts in Mathematics. Springer, Cham, (2015).

[26] Smertnig, D. *Every abelian group is the class group of a simple Dedekind domain.* Trans. Amer. Math. Soc. 369 (2017), no. 4, 2477–2491.

[27] Stacks Project's Authors *The stacks project*, (2008).