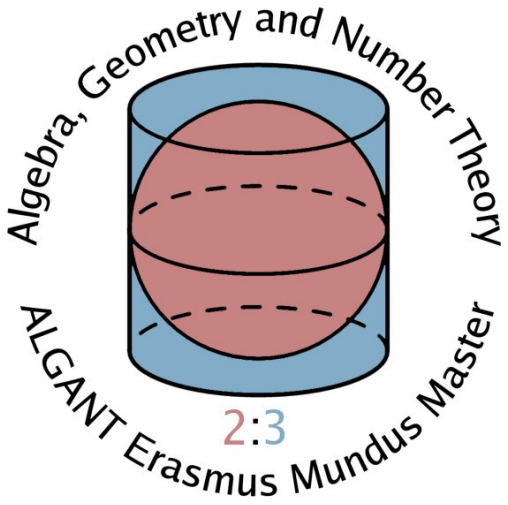


Master Thesis in Mathematics

Advisor: Prof. Ehud De Shalit

Arithmetic of Abelian Varieties over Number Fields:

A New Characterization of the Tate-Shafarevich Group

Menny Aka

June 2007

To Nili King

Acknowledgments

This thesis is the culmination of my studies in the framework of the ALGANT program. I would like to take this opportunity to thank all those who have helped me over the past two years. First, I would like to express my deepest gratitude to Professor Ehud De Shalit, for teaching me so many things, referring me to the ALGANT program and for the wonderful guidance he provided in preparing this thesis. I want to thank Professor Bas Edixhoven, for his office that is always open, for teaching me all the algebraic geometry I know and for all the help he gave me in the first year of the program in Leiden. I also want to thank Professor Boas Erez for the great help and flexibility along the way. With the help of these people, the last two years were especially enriching, in the mathematical aspect and in the other aspects of life.

Introduction

This thesis was prepared for the ALGANT program which focuses on the synthesis of **AL**gebra **G**eometry **A**nd **N**umber **T**heory. The subject of this thesis shows the various inter-relations between these fields. The Tate-Shafarevich group is a number theoretic object that is attached to a geometric object (an Abelian variety). Our new characterization is a geometric one, and its proof is mainly algebraic, using Galois cohomology and theorems from class field theory.

The Tate-Shafarevich group Ш arises in the study of rational points on Abelian varieties, namely the study of the finitely generated Mordell-Weil group $A(k)$ where A is an Abelian variety (Abelian varieties are the higher dimensional analog of elliptic curves), and k is a number field. The non-zero elements of Ш correspond to principal homogeneous spaces for A that have a rational point in any completion of k but not in k itself. In this sense, Ш measures the failure of the local-to-global principle for principal homogeneous spaces of A. Such arithmetic local-to-global questions are being researched since Kurt Hensel discovered the p-adic numbers.

Ш is conjectured to be finite for any Abelian variety, and turns out to be a difficult object to understand. This is not too surprising, as finding rational global points is a difficult Diophantine problem in general. As one can see, to decide whether a principal homogeneous space belongs to Ш, one checks the existence of a rational point in each localization of k, a problem of *local* nature. Our characterization gives an alternate way, of *global* nature, to decide when a principal homogeneous space belongs to Ш:

Theorem 1 (A new characterization of the Tate-Shafarevich group)**.** *Let A be an Abelian variety over a number field k, $\alpha \in H^1(k, A)$ and A_α be a principal homogeneous space for A that represent α. Then $\alpha \in Ш(k, A)$ if and only if for any finite field extensions l/k and for any group extension X of A_l by $\mathbb{G}_{m,l}$, i.e., any short exact sequence of the form*

$$0 \to \mathbb{G}_{m,l} \to X \to A_l \to 0,$$

one can find a principal homogeneous space X_α for X such that if we divide by the action of $\mathbb{G}_{m,l}$ on X_α we get a principal homogeneous space that is isomorphic to $(A_\alpha)_l$.

As this is a characterization of elements in Ш, one hopes that there would be a way to 'translate' certain constructions and notions that we have on Ш (e.g. the Cassels' pairing, visibility), and hopefully this new view would shed some light on the many unsolved questions on this mysterious group.

The proof of our characterization uses mainly two theorems on Galois cohomology of Abelian varieties over number fields, namely, the Tate local duality and the Brauer-Hasse-Noether theorem. This thesis should be accessible for anyone who know algebraic varieties to a level of being able to accept certain basic theorems on Abelian varieties and invertible sheaves on them, and is familiar with the basic theory of algebraic number fields (mainly about completions of a number field and decomposition of primes in global finite extensions). All the Galois cohomology techniques are explained in detail.

The first two chapters explain the necessary background from the theory of Abelian varieties and Galois cohomology. Chapter 3 and 4 explains the statements and the proofs of the deeper theorems, namely, the Tate local duality and the Brauer-Hasse-Noether theorem, and chapter 4 focuses on semi-Abelian varieties. Chapter 5 explain defines the Tate-Shafarevich group and its connection to the Mordell-Weil group. Chapter 6 explains an approximation theorem which allows us to make our characterization global, and in chapter 7 we formulate and prove our characterization.

Contents

Chapter 1

Abelian Varieties

1.1 Basic Properties and Facts

In this section we quickly review the most basic theorems regarding the geometric theory of Abelian varieties, and we give much more detailed discussion on the dual Abelian variety and the Weil-pairing in the rest of this chapter.
An *Abelian Variety* A over a field k is a geometrically integral, proper algebraic group. It turns out that the properness hypothesis is very strong and in particular we shall see that it implies that A is commutative, and even projective.
As any algebraic group, it is automatically smooth. This is true because it has a non-empty open smooth subvariety [5, lemma 4.2.21 and proposition 4.2.24] and its translations cover A.
We now show a first consequence of the properness assumption, the rigidity theorem, which gives a concrete description of morphisms between Abelian varieties and shows in particular that Abelian varieties are indeed Abelian, i.e., commutative.

Theorem 2 (Rigidity)**.** *Let $f : V \times W \to U$ morphism of varieties over k. If V is proper, $V \times W$ is geometrically connected, and*

$$f(v_0 \times W) = u_0 = f(V \times w_0)$$

for some $v_o \in V(k)$, $w_o \in W(k)$, $u_o \in U(k)$, then $f(V \times W) = u_o$. In plain words, rigidity here means that if f is constant on the 'coordinates axes', it is constant everywhere.

This theorem is plainly false without the properness assumption; for example, the map $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ defined by $(x, y) \to xy$ is constant on $0 \times \mathbb{A}^1$ and $\mathbb{A}^1 \times 0$ and it is not constant.
We use the rigidity theorem to analyze maps between Abelian varieties:

Corollary 3. *Any morphism $f : A \to B$ between two Abelian varieties is a composition of a translation and a homomorphism.*

Proof. By composing with the translation $x \mapsto x - f(e)$ for $x \in B(\bar{k})$ it is enough to show that if $f(e) = e$ then it is a homomorphism. Let

$$g : A \times A \to B, \quad g(a, b) = f(a + b) - f(a) - f(b).$$

We have that $g(A \times e) = e = g(e \times A)$ and therefore by the rigidity theorem, $g(A \times A) = e$, or in other words, f is a homomorphism. □

Corollary 4. *Abelian varieties are commutative algebraic groups.*

Proof. The map $x \to x^{-1}$ is a homomorphism since the identity element e is mapped to itself. □

Theorem 5. *Let $f : A \to B$ be a morphism of Abelian varieties. Then, the following are equivalent:*

1. *f is surjective and has finite kernel.*
2. *$dim(A) = dim(B)$ and f is surjective.*
3. *$dim(A) = dim(B)$ and f has finite kernel.*
4. *f is finite, flat and surjective.*

A very important example of an isogeny is the multiplication by n map. Thus, as abstract groups, Abelian varieties are divisible groups.

1.2 The Dual Abelian Variety

As Abelian varieties are proper, they have no global non-constant functions, and except for specific cases, working with the explicit equations that define the Abelian variety is no longer easy as in the study elliptic curves. Therefore, the study locally defined function on general Abelian variety, i.e. Cartier divisors/invertible sheaves/line bundles, is of main interest in the geometric theory of Abelian varieties. Most of the theorems in this subject are much easier to prove for elliptic curves, where we have equations to work with.

Let $a \in A(\bar{k})$, defined over a field l. The translation map t_a, which sends x to $x + a$, is denoted by t_a and is defined over l. The most important and basic theorem about line bundles over an Abelian variety is the theorem of the square which is due to A. Weil:

Theorem 6 (Theorem of the Square)**.** *Let A/k be an Abelian variety and $\mathcal{L}$ be a line bundle on the variety A. then*

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \cong t_a^*\mathcal{L} \otimes t_b^*\mathcal{L},$$

for arbitrary points $a, b \in A(\bar{k})$.

The original aim of this theorem was to prove that Abelian varieties are in fact projective varieties. For a proof we refer to [9, §6]. This theorem allows us to construct a homomorphism $A \to \mathrm{Pic}(A)$ in the following way: fix an invertible sheaf $\mathcal{L}$ on A and define a map

$$\varphi_{\mathcal{L}} : A \to \mathrm{Pic}(A),\ a \mapsto [t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}].$$

The theorem of the square implies that

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L}^{-1} \cong (t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}) \otimes (t_b^*\mathcal{L} \otimes \mathcal{L}^{-1}),$$

so $\varphi_{\mathcal{L}}$ is a homomorphism.

We are going now to endow a subgroup of $\mathrm{Pic}(A)$ which is denoted by $\mathrm{Pic}^0(A)$ and consist with the structure of an Abelian variety over k. We will call this variety $A^\vee$ the dual of A (or the Picard variety of A).

Let $m : A \times A \to A$ be the multiplication map, and let $p, q : A \times A \to A$ be the natural projections. Let $\mathcal{L}$ an invertible sheaf on A and consider the sheaf $m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1}$ on $A \times A$. We can regard it as a family of invertible sheaves on A (the second factor) which is parametrized by A (the first factor). In other words, for any $a \in A(\bar{k})$ we have a map

$$A_{k(a)} \cong \mathrm{Spec}(k(a)) \times_k A \overset{i\times \mathrm{Id}}{\to} A \times A$$

and the inverse image by this map of $m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1}$ is an invertible sheaf on A, which we denote by $(m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1})|_{a\times A}$. We define

$$K(\mathcal{L}) = \{a \in A(\bar{k}) | (m^*\mathcal{L} \otimes q^*\mathcal{L})^{-1}|_{a\times A} \text{ is trivial}\}. \tag{1.1}$$

Note that

$$(m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1})|_{a\times A} = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

thus

$$K(\mathcal{L})(k) = \{a \in A(k) | \varphi_{\mathcal{L}}(a) = 0\}.$$

Proposition 7. *Let A be an Abelian variety and $\mathcal{L}$ an invertible sheaf on it. The following are equivalent:*

1. $K(\mathcal{L}) = A$

2. $t_a^*\mathcal{L} \sim \mathcal{L}$, *for all* $a \in A(\bar{k})$

3. $m^*\mathcal{L} \sim p^*\mathcal{L} \otimes q^*\mathcal{L}$.

Proof. The equivalence of (1) and (2) follows from the remark above. (3) implies that $(m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1})|_{a\times A} \sim p^*\mathcal{L}|_{a\times A} = 0$, so (3) implies (1). (1) implies (3), is an easy consequence of the Seesaw principle (see [9, §8 page 74]). □

We define $\mathrm{Pic}^0(A)$ to be the group of isomorphism classes of invertible sheaves that satisfy the properties of proposition 7. It is indeed a subgroup as one can easily check using property (2). We write $\mathcal{L} \in \mathrm{Pic}^0(A)$ to mean the isomorphism class of $\mathcal{L}$ when no confusion arises. Let $f, g : V \to A$ be two maps from some variety V. Then, by applying $(f \times g)^*$ to condition (3) we see that for any $\mathcal{L} \in \mathrm{Pic}^0(A)$

$$(f+g)^*\mathcal{L} \sim f^*\mathcal{L} \otimes g^*\mathcal{L}.$$

in particular as $n_A = 1_A + \ldots + 1_A$, we have

$$n_A^*(\mathcal{L}) \sim \mathcal{L}^n. \tag{1.2}$$

Next, we will show that the image of $\varphi_{\mathcal{L}}$ is contained in the subgroup $\mathrm{Pic}^0(A)$. To check this, we take $a, b \in A(\bar{k})$ and we have

$$t_a^*(\varphi_{\mathcal{L}}(b)) = t_a^*(t_b^*\mathcal{L} \otimes \mathcal{L}^{-1}) = t_{a+b}^*\mathcal{L} \otimes (t_a^*\mathcal{L})^{-1} \sim t_b^*\mathcal{L} \otimes \mathcal{L}^{-1} = \varphi_{\mathcal{L}}(b),$$

Where the $\sim$ follows from the theorem of the square. Therefore, $[\varphi_{\mathcal{L}}(b)] \in \mathrm{Pic}^0(A)$.

Roughly speaking, we are going to endow $\mathrm{Pic}^0(A)$ with a structure of an Abelian variety which we denote by $A^\vee$. Suppose one has $A^\vee(\bar{k}) \cong \mathrm{Pic}^0(A_{\bar{k}})$ as abstract groups (see theorem 9 below). We would want an invertible sheaf $\mathcal{P}$ on $A \times A^\vee$, called the *Poincaré sheaf*, such that if we think of $\mathcal{P}$ as a family of sheaves $\mathcal{P}_\alpha := \mathcal{P}|_{A\times\alpha}$ on A parametrized by points in $\alpha \in A^\vee(\bar{k})$, then $\mathcal{P}_\alpha$ corresponds to α through the isomorphism to $A^\vee(\bar{k}) \cong \mathrm{Pic}^0(A_{\bar{k}})$. We now give a precise definition

Definition 8. *The dual (or Picard) variety is an Abelian variety* $A^\vee$*, together with an invertible sheaf* $\mathcal{P}$ *on* $A \times A^\vee$ *(called the Poincaré sheaf), such that*

1. $\mathcal{P}|_{\{0\}\times A^\vee}$ *is trivial and for each* $a \in A^\vee(\bar{k})$, $\mathcal{P}|_{A\times\{\alpha\}}$ *represents the element* α.

2. *For every* k*-scheme* T *and invertible sheaf* $\mathcal{L}$ *on* $A\times T$*, such that* $\mathcal{L}|_{\{0\}\times T}$ *is trivial and* $\mathcal{L}_t := \mathcal{L}_{A\times\{t\}}$ *lies in* $Pic^0(A_{k(t)})$ *for all* $t \in T(\bar{k})$*, there is a unique morphism* $f : T \to A^\vee$*, such that* $(1 \times f)^*\mathcal{P} \cong \mathcal{L}$.

Remarks:

1. It follows from the universal property in the definition that the pair $(A^\vee, \mathcal{P})$, if it exists, is unique up to a unique isomorphism.

2. If we put $T = \mathrm{Spec}(\bar{k})$, then we get $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$.

3. The unique morphism $f : T \to A^\vee$ above, maps a point $t \in T(\bar{k})$ to $\mathcal{L}_t \in A^\vee(\bar{k})$.

4. As expected, one has $A^{\vee\vee} \cong A$. See [9, §13 page 132]

To construct the dual Abelian variety $A^\vee$ we use the following theorem:

Theorem 9. *Let A/k be an Abelian variety over an algebraically closed field, and let $\mathcal{L}$ be an ample invertible sheaf on A (such a sheaf exists as Abelian varieties are projective.) Then, the map $\varphi_{\mathcal{L}} : A \to Pic^0(A)$ is surjective, i.e., for all $M \in Pic^0(A)$, there exist $a \in A(k)$ such that $M = [t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}]$.*

Proof. For a proof using spectral sequences, see [9, §8, page 77]. □

This theorem says that at least as abstract groups we have $A/K(\mathcal{L}) \cong \mathrm{Pic}^0(A)$, and now we only need to construct $\mathcal{P}$. Let

$$\Lambda(\mathcal{L}) := m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1} \otimes q^*\mathcal{L}^{-1}$$

where $\mathcal{L}$ is some ample line bundle. $\Lambda(\mathcal{L})$ is called the Mumford line bundle. It follows easily that $\Lambda(\mathcal{L})|_{\{0\}\times A} = \mathcal{L} \otimes \mathcal{L}^{-1}$, which is trivial. Moreover, $\Lambda(\mathcal{L})|_{A\times\{a\}} = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1} = \varphi_{\mathcal{L}}(a)$, which is an element of $\mathrm{Pic}^0(A_{\bar{k}})$. Thus, each element of $\mathrm{Pic}^0(A_{\bar{k}})$ is represented by $\Lambda(\mathcal{L})|_{A\times\{a\}}$ for a finitely many but at least one a. Thus, if $(A^\vee, \mathcal{P})$ exists, then there is a unique isogeny $\varphi : A \to A^\vee$, such that $(1 \times \varphi)^*\mathcal{P} = \Lambda(\mathcal{L})$. Furthermore, it follows from (2) of definition 8 that $\varphi = \varphi_{\mathcal{L}}$.

Now, to construct $A^\vee$ one uses general techniques for constructing quotients (the most adapted reference for this construction is naturally [9, §7 page 66], and a more basic reference is [5, Exercises 2.3.20-21]) to give the right structure of a variety (or a scheme) to $A/K(\mathcal{L})$. This construction is quite easy when the characteristic of k is zero, since the variety structure of $K(\mathcal{L})$ as a finite group subscheme of A is just the reduced subscheme structure. Therefore, in this case we have $A^\vee \cong A/K_{\mathcal{L}}$. To construct $\mathcal{P}$, note that $K(\mathcal{L})$ acts on $\Lambda(\mathcal{L})$ over $A \times A$ by lifting the action on the second factor. If we form the quotient of this action, we obtain a sheaf $\mathcal{P}$, such that $(1 \times \varphi_{\mathcal{L}})^*\mathcal{P} = \Lambda(\mathcal{L})$. A proof that this pair satisfies the conditions in definition 8 can be found in [9, §8]. The general case ($\mathrm{char}(k) \neq 0$) is proved also in [9, §13].

1.3 The Dual Isogeny and the Dual Exact Sequence

Let $f : A \to B$ be homomorphism of Abelian varieties. The fact that f is homomorphism implies that

$$t_a^* f^*(\mathcal{M}) = (f \circ t_a)^*(\mathcal{M}) = f^* t_{f(a)}^*(\mathcal{M}), \quad \forall \mathcal{M} \in \mathrm{Pic}(A)$$

If $\mathcal{L} \in \mathrm{Pic}^0(B)$ then for all $a \in A(\bar{k})$

$$t_a^*(f^*\mathcal{L}) \otimes (f^*\mathcal{L})^{-1} = f^* t_{f(a)}^*(\mathcal{L}) \otimes (f^*\mathcal{L})^{-1} = f^*(t_{f(a)}^*\mathcal{L} \otimes \mathcal{L}^{-1}) \sim f^*(\mathcal{O}_B) = \mathcal{O}_A.$$

Therefore $f^* : \mathrm{Pic}(B) \to \mathrm{Pic}(A)$ induces a map $f^* : \mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A)$. It follows from remark 3 to definition 8 that this is the map that we get from the following construction:
Let $\mathcal{P}_B$ be the Poincaré sheaf on $B^\vee \times B$. The line bundle $(\mathrm{Id} \times f)^*\mathcal{P}_B$ on $B^\vee \times A$ satisfies that

$$((\mathrm{Id} \times f)^*\mathcal{P}_B)_\beta = f^*(\beta) \in \mathrm{Pic}^0(A), \quad \forall \beta \in B^\vee(\bar{k})$$

so by the universal property of $(A^\vee, \mathcal{P}_A)$ we get a map, $f^\vee : B^\vee \to A^\vee$, such that $(f^\vee \times \mathrm{Id})^*\mathcal{P}_B = \mathcal{P}_A$. Thus, the natural map $f^* : \mathrm{Pic}^0(B)(\bar{k}) \to \mathrm{Pic}^0(A)(\bar{k})$ is in fact a morphism, i.e., it is the 'point' map of the morphism $f^\vee : B^\vee \to A^\vee$.

The next theorem provides a description of the dual homomorphisms to isogenies.

Theorem 10. *Let $f : A \to B$ be an isogeny with finite kernel N. Let $N^\vee$ be the Cartier dual of N. Then the kernel of the dual isogeny $f^\vee : B^\vee \to A^\vee$ is $N^\vee$, i.e., there is a short exact sequence*

$$0 \to N^\vee \to B^\vee \xrightarrow{f^\vee} A^\vee \to 0.$$

Proof. See [9, §15, page 143]. □

1.4 The Weil pairing

We remind the reader that when G is a group, a G- pairing

$$<,>: A \times B \to C,$$

where A,B and C are G-modules, is a bilinear map such that

$$< \sigma a, \sigma b >= \sigma < a, b >, \quad a \in A, b \in B, \sigma \in G.$$

We wish to construct a G_k-pairing

$$e_n : A_n(\bar{k}) \times A_n^\vee(\bar{k}) \to \mu_n.$$

One easy way to construct this pairing is to recall that A_n fits in the short exact sequence

$$0 \to A_n \to A \xrightarrow{\cdot n} A \to 0$$

and the dual of the multiplication by n is also multiplication by n, so the dual sequence is

$$0 \to A_n^\vee \to A^\vee \xrightarrow{\cdot n} A^\vee \to 0$$

and by theorem 10, $A_n^\vee$ is the Cartier dual of A_n, i.e., $A_n^\vee \cong \mathrm{Hom}(A, \mathbb{G}_m)$, and therefore we can get the desired pairing using this identification.(that is, if we take $\alpha \in \mathrm{Hom}(A, \mathbb{G}_m) \cong A_n^\vee$ we define $e_n(a, \alpha) = \alpha(a)$.)
We wish to have a more explicit construction, using Cartier divisors. Let $a \in A_n(\bar{k})$ and $a' \in A_n^\vee(\bar{k})$. We want to think of a' as an element of $\mathrm{Pic}^0(A)(\bar{k})$, so we denote it by $[D]$. We have that $n_A^* D \sim nD$ (by 1.2) and $nD \sim 0$ since $[D] \in A_n^\vee(\bar{k})$. Therefore nD and $n_A^* D$ are principal divisor and we choose functions g, h such that $nD = (h)$ and $n_A^* D = (g)$. We have

$$(h \circ n_A) = n_A^*((h)) = n_A^*(nD) = n \cdot n_A^*(D) = n \cdot (g) = (g^n)$$

so $g^n / h \circ n_A = c$ where c is some constant function. Then

$$(g \circ t_a)^n = g(x+a)^n = c \cdot h \circ n_A(x+a) = c \cdot h(nx+na) = c \cdot h(nx+0_A) = c \cdot h(nx) = g(x)^n$$

and therefore $\frac{g(x+a)^n}{g(x)^n} = (\frac{g(x+a)}{g(x)})^n = 1$. We define $e_n(a, a') = \frac{g(x)}{g(x+a)} \in \mu_n$.

Proposition 11 (Weil pairing)**.** *Let A/k be an Abelian variety, $A^\vee$ its dual and $n \in \mathbb{N}$ a positive integer not divisible by the characteristic of k. Then the construction above gives a non-degenerate G_k-pairing*

$$e_n : A_n(\bar{k}) \times A_n^\vee(\bar{k}) \to \mu_n.$$

The reader may have encountered this pairing in the context of elliptic curves, where one uses a polarization (i.e., a morphism from $A \to A^\vee$) to obtain a pairing

$$A_n(\bar{k}) \times A_n(\bar{k}) \to \mu_n.$$

Proof. A proof can be found in [9, §20, page 184] □

Chapter 2

Group Cohomology

2.1 Basic properties and facts

In this section we develop the basics of group cohomology in a very concrete way, which can look a bit artificial. The 'right' context in which this subject sits is Abelian categories and derived functors, which is a bit lengthy to develop here. We refer to [7] for a short,easy-going introduction.

The example to keep in mind in this section is the Galois group $\mathrm{Gal}(l/k)$ where l/k is a finite extension of number fields, that act on the $\mathrm{Gal}(l/k)$-module $A(l)$ where A is an Abelian variety.

2.1.1 Definitions

Given a group G, we define the *group ring* $\mathbb{Z}[G]$ to be the free Abelian group on the underlying set G. We extend the multiplication of G to a multiplication on $Z[G]$ by distributivity.
An Abelian group A is called a G-module if there exist a map

$$G \times A \to A \quad (g, a) \mapsto g \cdot a$$

such that, for all $a, b \in A$ and $g, h \in G$

1. $g \cdot (a + b) = g \cdot a + g \cdot b$
2. $1 \cdot a = a$
3. $g \cdot (h \cdot a) = (gh) \cdot a$

A morphism of G-modules $f : A \to B$ is a morphism of Abelian groups, s.t. $f(g \cdot a) = g \cdot f(a)$. In the sequel, where there is no danger of confusion, we will write ga for $g \cdot a$. It is easy to check that giving a G-module structure on A is equivalent to giving a $\mathbb{Z}[G]$-module structure on A which is equivalent

to giving a homomorphism of groups $G \to \mathrm{Aut}(A)$.
Given a G-module A we define the subgroup of invariants

$$A^G = \{a \in A | ga = a, \forall g \in G\}.$$

This is a functor from G-modules to Abelian groups. It is left exact and in the language of derived functors the cohomology groups $H^i(G, *)$ could be defined as the derived functors of $A \mapsto A^G$. We give below as much more concrete construction.

2.1.2 The bar resolution

Let A be a G-module. For each $n \in \mathbb{N}$, we define the group (with pointwise addition)

$$C^n(G, A) := \mathrm{Hom}_{\mathrm{Sets}}(G^n, A),$$

and the boundary map

$$\delta^n : C^{n-1}(G, A) \to C^n(G, A)$$

which is defined as $\delta^n := \sum_{i=0}^{n} (-1)^n \delta_i$ and

$$\delta_i = \begin{cases} g_1 f(g_2, \cdots, g_n) & i = 0 \\ f(g_1, \cdots, g_i g_{i+1}, g_{i+2}, \cdots, g_n) & i = 1, \cdots, n-1 \\ f(g_1, \cdots, g_{n-1}) & i = n \end{cases}$$

We have that for all $n \in \mathbb{N}$, $\delta^{n+1} \circ \delta^n = 0$ and we define the cohomology group of degree n, $H^n(G, A)$, to be the degree n cohomology group of the cochain complex $C^*(G, A)$, i.e., we define

$$H^n(G, A) = \mathrm{Ker}\delta^n / \mathrm{Im}\delta^{n-1}.$$

Elements of $C^n(G, A)$ are called n-cochains, elements of $\mathrm{Ker}\delta^n$ are called n-cocycles and elements of $\mathrm{Im}\delta^{n-1}$ are called n-coboundaries.

2.1.3 Examples

1. $H^0(G, A) = \mathrm{Ker}\delta^0 = A^G$ since $\delta^0(a) = ga - a$
2. $H^1(G, A) = \mathrm{Ker}\delta^1 / \mathrm{Im}\delta^0$. First we calculate $\mathrm{Ker}\delta^1$. $f : G \to A \in \mathrm{Ker}\delta^1$ satisfy $f(gh) = f(g) + gf(h)$ which is 'almost' a homomorphism and it is called 'crossed-homomorphism'. Now for an element $f : G \to A \in \mathrm{Im}\delta^0$ there exist $a \in A$ s.t. $f(g) = ga - a$. Note that it is also a crossed homomorphism, and it is called a *principal crossed-homomorphism*. Therefore

$$H^1(G, A) = \frac{\text{Crossed-homomorphisms}}{\text{Principal crossed-homomorphisms}}.$$

Note that if G acts trivially on A, the only principal homomorphism is the identity and the crossed homomorphisms are just ordinary homomorphisms. When $G = G_k$ and A the the group of geometric points of an Abelian variety, $H^1(G, A)$ has a very interesting and useful description and will return to investigate it in details later.

3. $H^2(G, A)$. 2-Cocycles satisfy that

$$gf(h, i) - f(gh, i) + f(g, hi) - f(g, h).$$

They are tradionally called 'factor sets' of 'factor systems'.
2-coboundaries are are maps $\phi : G \times G \to A$ such that there exist a map $\alpha : G \to A$ and

$$\phi(g, h) = \delta\alpha(g, h) := g\alpha(h) - \alpha(gh) + \alpha(g) = 0.$$

We will sketch a classical result that will show that $H^2(G, A)$ classifies group extensions of G by A.
Let A be a commutative group and G a group. First, we observe that an extension E of G by A, i.e., a short exact sequence

$$0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 0$$

defines a structure of a G-module on A by

$$g \cdot a := e_g i(a) e_g^{-1}$$

where e_g is some element of E mapping to g. One check that since A is commutative, this action does not depend on the choice of e_g.
Two extensions E, E' of G by A are said to be isomorphic if there is a homomorphism $f : E \to E'$ making the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0. \end{array}$$

One checks that isomorphic extensions induce the same G action on A. For a given structure of a G-module on A, We denote by Ext(G,A) the set of isomorphisms classes of extensions of G by A, which induce the given structure of a G-module on A. In section 4.1 we define a structure of a group on Ext(G,A).

Theorem 12. *There is a group isomorphism*

$$H^2(G, A) \cong Ext(G, A).$$

Proof. We will sketch the main ideas of the proof, making it easy to fill in the details. For each extension

$$0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 0$$

we define a 2-cocycle by choosing a section of π, i.e., a set-theoretic map $\sigma : G \to E$ such that $\pi \circ \sigma = \mathrm{Id}_G$ (like $g \mapsto e_g$ above), and using it to define

$$\alpha : G \times G \to A, \quad \alpha(g, g') = \sigma(gg')\sigma(g)^{-1}\sigma(g')^{-1} \in \mathrm{Ker}\pi = \mathrm{Im}(i) \cong A.$$

That is, α is measuring the deviation of σ from being a homomorphism. In particular, when there is a section that is a homomorphism (in this case one says that the extension *splits* or *trivial*), the corresponding cocycle is the trivial cocycle. After verifying that it is indeed a cocycle, one shows that choosing different section, or taking different representative in the extension isomorphism class, will change α by a coboundary at most. Therefore, this gives a well defined map

$$\mathrm{Ext}(G, A) \xrightarrow{\psi} H^2(G, A).$$

To define the inverse of ψ, one shows that in any cohomology class of $H^2(G, A)$ we can find a *normal* cocycle that represent it, which is a cocycle $\beta : G \times G \to A$ with the property that $\beta(1, g) = 0 = \beta(g, 1), \forall g \in G$. Then, we define on the set $A \times G$ the composition law

$$(a, g) * (a', g') = (a + a' + \beta(g, g'), gg').$$

The resulting extension is denoted by $A \rtimes_\beta G$. One verify that the map $\beta \to A \rtimes_\beta G$ is well-defined map from $H^2(G, A) \to \mathrm{Ext}(G, A)$ and that is double-sided inverse to ψ. □

For later use in the next chapter we note that if we look on $H^2(G, A)$ when G acts trivially on A, this corresponds to *central* extensions of G by A (i.e., $G \subset \mathrm{Center}(E)$). If we further assume that G is commutative and look only on symmetric cocycles, that is $\beta(g, g') = \beta(g', g)$, they will correspond to commutative extensions.

2.1.4 Characterization of $H^n(G, -)$

The following characterization is a basic theorem on derived functors, applied to our case:

Theorem 13. *For fixed group G,*

1. *$H^n(G,-)$ is a functor from **{G-modules}** to **{Abelian groups}**.*
2. *$H^0(G,A) = A^G$*
3. *Every short exact sequence of G-modules, $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, gives rise to 'connecting homomorphisms' δ_n, which fits in a long exact sequence*

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

   and the δ_n are also functorial with short exact sequences maps.

4. *if A is injective $\mathbb{Z}[G]$-module[1] then $H^n(G,A) = 0, \quad \forall n \neq 0$.*

   These properties define the functors $H^n(G,-)$ with the connecting homomorphisms δ_n uniquely, up to a unique isomorphism.

Proof. One construct the maps $H^i(f)$ for $f : A \to B$ by sending a i-cocycle $G^i \to A$ to the i-cocycle $G^i \to A \xrightarrow{f} B$. The construction of the coboundary maps δ_i is simple but more complicated. In the sequel we will only need δ_1 and δ_2 which are constructed as follows. If $c \in C^G$, we choose $b \in B$ such that $g(b) = c$. For any $\sigma \in G$, we have $g(\sigma b - b) = \sigma g(b) - g(b) = \sigma c - c = 0$ so $\sigma b - b$ is a well defined element of A. Therefore we define $\delta_1(c)$ to be the cohomology class of the 1-cocycle $\sigma \mapsto \sigma b - b$. Similarly, given cocycle $\alpha : G \to C$ that represent a class $[\alpha] \in H^1(G,C)$, for all $\sigma \in G$ we choose $\beta(\sigma)$ to be some preimage of $\alpha(\sigma)$ and define

$$\delta_2(\alpha)(\sigma,\tau) := \sigma(\beta(\tau)) - \beta(\sigma\tau) + \beta(\sigma).$$

One check directly that this is indeed a map from $G^2 \to A$, and that these maps are well defined (do not depend on the choices) and give rise to the long exact sequence above. □

2.1.5 Functoriallity in G

Consider a homomorphism of groups $G' \to G$. This induces a map from

$$\mathrm{Hom}_{\mathrm{Sets}}(G^n, A) \to \mathrm{Hom}_{\mathrm{Sets}}(G'^n, A)$$

and therefore a map from $H^n(G,A) \to H^n(G',A)$ which is called the restriction homomorphism (since it is mostly used when $G' < G$).

[1] The functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-,A)$ is exact.

2.1.6 Galois cohomology

Let k be a field and let $G_k := \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group. The above theory works very well for finite groups G. When we wish to consider a topological group G (like the profinite group G_k) , we consider 'continuous' cocyles. This means that for n-cochains we take continuous maps from G^n to A where we give A the discrete topology. Alternatively, in the profinite case, say, for $G = \varprojlim G_\alpha$ where G_α are finite group, we can use the finite group construction to define

$$H^n(G, A) = \varinjlim H^n(G_\alpha, A).$$

These constructions are equivalent.
When we have a continuous action of G_k on a abelian group A, we call A a *Galois module*. Given an Abelian group variety V over a field k, the Abelian group $V(\bar{k})$ is naturally a Galois module. Galois cohomology is the study of the group cohomology of these Galois modules. We write $H^n(k, V)$ for $H^n(G_k, V(\bar{k}))$.
Note that if l/k is an algebraic extension of fields, then $G_l < G_k$ and therefore we have the restriction homomorphism $H^n(k, V) \to H^n(l, V)$.

Example 14 (Hilbert theorem 90)**.** *Let F be a field. Then $H^1(k, \mathbb{G}_{m,k}) = 0$*

Proof. By definition

$$H^1(k, \mathbb{G}_{m,k}) = H^1(G_k, \bar{k}^*) = \varinjlim H^1(\mathrm{Gal}(l/k), l^*)$$

where the limit is over all finite extensions. Therefore it is enough to show that

$$H^1(\mathrm{Gal}(l/k), \bar{k}^*) = 0.$$

Let $a : \mathrm{Gal}(l/k) \to l^*$ be a cocycle and let $a_\sigma := a(\sigma)$. By Dedekind theorem on independence of automorphisms [1, §14.2] there exist $b \in l$, such that

$$c := \sum_{\sigma \in \mathrm{Gal}(l/k)} a_\sigma \sigma(b) \neq 0.$$

Now, for all $\tau \in \mathrm{Gal}(l/k)$ we have

$$\tau(c) = \sum_{\sigma \in \mathrm{Gal}(l/k)} \tau a_\sigma \tau\sigma(b) = \sum_{\sigma \in \mathrm{Gal}(l/k)} a_{\tau\sigma} \cdot a_\tau^{-1} \tau\sigma(b) =$$

$$= a_\tau^{-1} \cdot \sum_{\sigma \in \mathrm{Gal}(l/k)} a_{\tau\sigma} \cdot \tau\sigma(b) = a_\tau^{-1} \cdot c$$

where we used the equality $\tau a_\sigma = a_{\tau\sigma} \cdot a_\tau^{-1}$ which is the cocycle condition (written multiplicatively). Therefore, $a_\tau = \frac{c}{\tau c}$, so a is a coboundary and we are done. □

2.1.7 Cup products

Let G be a group. For two G-modules, A and B, define a G-module structure on $A \otimes B := A \otimes_{\mathbb{Z}} B$ by

$$g(a \otimes b) = ga \otimes gb, \quad g \in G, a \in A, b \in B.$$

Theorem 15. *Let G be a group. For any two G-modules, A and B, and two integers r and s, there is a unique family of bi-additive pairings*

$$H^r(G, A) \times H^r(G, B) \to H^r(G, A \otimes B), \quad (\alpha, \beta) \mapsto \alpha \cup \beta$$

such that

1. *When both sides are considered as covariant bifunctors on (M,N) these maps are morphism of such functors.*

2. *for r=s=0 this pairing is*

$$A^G \times B^G \to (A \otimes B)^G, \quad (a, b) \to a \otimes b$$

3. *If $0 \to A' \to A \to A'' \to 0$ is an exact sequence of G-modules such that*

$$0 \to A' \otimes B \to A \otimes B \to A'' \otimes B \to 0$$

is exact too, we have

$$\delta\alpha'' \cup \beta = \delta(\alpha'' \cup \beta), \quad \alpha'' \in H^r(G, A''), \beta \in H^s(G, B)$$

and by abuse of notation, the first δ is

$$\delta : H^r(G, A'') \to H^{r+1}(G, A')$$

and the second one is

$$\delta : H^{r+s}(G, A'' \otimes B) \to H^{r+s+1}(G, A' \otimes B)$$

4. *If $0 \to B' \to B \to B'' \to 0$ is an exact sequence of G-modules such that*

$$0 \to A \otimes B' \to A \otimes B \to A \otimes B'' \to 0$$

is exact too, we have

$$\alpha \cup \delta\beta'' = (-1)^r \delta(\alpha \cup \beta''), \quad \alpha \in H^r(G, A), \beta'' \in H^s(G, B'')$$

and by abuse of notation, the first δ is

$$\delta : H^r(G, B'') \to H^{r+1}(G, B')$$

and the second one is

$$\delta : H^{r+s}(G, A \otimes B'') \to H^{r+s+1}(G, A \otimes B')$$

Proof. If ϕ, ψ are cocycles representing $\alpha \in H^r(G, A), \beta \in H^s(G, B)$ respectively, one defines $\alpha \cup \beta$ to be the element represented by the cocycle

$$\phi \cup \psi(g_1, \ldots, g_{r+s}) = \phi(g_1, \ldots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \ldots, g_{r+s})$$

and check that it satisfy the above conditions. One can find a proof in [2, 3.4.8] □

A G-pairing, i.e. a bilinear map from $A \times B \xrightarrow{\Phi} P$ such that $\Phi(ga, gb) = g\Phi(a, b)$ and it induces a G-homomorphism $A \otimes B \to P$ and therefore a map

$$H^{r+s}(G, A \otimes B) \to H^{r+s}(G, P)$$

and by composing it with the cup product, we get a pairing

$$H^r(G, A) \times H^s(G, B) \to H^{r+s}(G, P).$$

We will use this with the Weil pairing which is a G_k-pairing. All of the above is still true when we consider profinite groups like G_k, where its cohomology groups are defined using direct limits of the cohomology groups of finite extensions or continuous cocycles and coboundaries.

2.2 The Weil-Chatelet Group

2.2.1 The geometric definition

Definition 16. *Let A/k be an Abelian variety defined over k. A* principal homogeneous space *of A/k is a variety X/k with a map $\mu : X \times A \to X$ (a simple transitive action of A) satisfying:*

1. $\mu(x, 0) = x$
2. $\mu(x, a + b) = \mu(\mu(x, a), b) \quad \forall x \in X \quad a, b \in A$
3. *For all $x \in X$ the map $a \mapsto \mu(x, a)$ is an isomorphism of A with X, which is defined over $k(x)$.*

It is obvious from condition 3, that X is isomorphic over k to A if and only if $X(k) \neq \emptyset$. Indeed, if $x \in X(k)$ then 3 defined a k-isomorphism, and if there is an isomorphism, 0_A is mapped to a k-rational point of X. Therefore, the triviality of a principal homogeneous space is a fundamental (usually difficult) Diophantine question, and the cohomology construction that will follow soon can be regarded as a tool to study such difficult questions.

Two homogeneous spaces of A, $(X, \mu), (X', \mu')$, are said to be isomorphic if there exist a k-isomorphism ϕ such that

$$\begin{array}{ccc} X \times A & \xrightarrow{\mu} & X \\ \downarrow{\scriptstyle \phi \times \mathrm{Id}} & & \downarrow{\scriptstyle \phi} \\ X' \times A & \xrightarrow{\mu'} & X' \end{array}$$

Note that that the same variety can represent different principal homogeneous space. For example, one can compose an automorphism of A on the action μ, that is, for $\alpha \in \mathrm{Aut}A$ one can consider the action $\mu^{\alpha}(x, a) := \mu(x, \alpha a)$ instead of μ. One can show that this is the only way that the same variety arises as different principal homogeneous space. See [13, exercise 10.4].
The set of isomorphisms classes of principal homogeneous spaces is called the **Weil-Chatelet group** and we denote it by $WC(k, A)$. Why is it a group? One way to see it is to construct a bijection from this set to $H^1(k, A)$ and pull back the group structure. We will do it in the next section and our main treatment of principal homogeneous spaces will be through Galois cohomology. A more geometric, *equivalent* way, is to define the a group law using the the Baer sum: Given two principal homogeneous spaces $(X_1, \mu_1), (X_2, \mu_2)$ we define the 'anti-diagonal' action $\mu_{+,-}$ on $X_1 \times X_2$ by $\mu_{+,-}(a, (x_1, x_2)) = (\mu_1(a, x_1), \mu_2([-1]a, x_2))$. Now we define $X_1 + X_2$ to be the quotient $X_1 \times X_2/\mu_{+,-}$, and A acts on it by the action that comes from letting A acts on the first term, X_1 in $X_1 \times X_2$.

Given field extension l/k we can extend the base of scalars to get map from

$$WC(k, A) \to WC(l, A_l) = WC(l, A)$$

. This map is in fact a homomorphism and it is clear by the discussion above that non-zero elements in its kernel are principal homogeneous spaces with no k-rational points but with some l-rational point. We denote this kernel as $WC(l/k, A)$.

2.2.2 The Galois cohomological definition

Classification of twists: One motivation for defining the first cohomology group H^1 is the classification of **twists**. When X_0 is an algebro-geometric object defined over a field k (in our case we consider Abelian varieties over k), we wish to classify the set of k-isomorphism classes of objects X with the property that X is isomorphic to X_0 over $\bar{k}$. Such an object is called a *twist* of X_0.
In [3, pages-283-285], there is a well-written discussion and development that shows that the set of twists of X_0 when X_0 is a quasi-projective variety is in bijection with $H^1(G_k, \mathrm{Aut}(X_0))$.

Note that any principal homogeneous spaces for A is a twist of A, as condition (3) in the definition 16 shows. We wish to show something similiar to the classification of twists but more specialized to our situation:

Theorem 17. *Let A/k be an Abelian variety. Then $WC(k,a) \cong H^1(k,A)$ as groups. Moreover, for any Galois extension l/k, $WC(l/k,A) \cong H^1(l/k,A)$.*

Proof. The first statement obviously follows from the second. Let $(X,\mu) \in WC(l/k,A)$ and we first define the subtraction map $\nu : V \times V \to A$ on X to be

$$\nu(x_1,x_2) = a \Leftrightarrow a + x_2 := \mu(a,x_2) = x_1.$$

Note the it is well defined by (3) of definition 16, and one can show that it is a k-morphism. We denote $x_1 - x_2 := \nu(x_1,x_2)$. Let P be a l-rational point of X and we define the map $a_P : G_k \to A(l)$ by $a_P(\sigma) = \sigma P - P$, which is easily checked to be a 1-cocycle. So $[a] \in H^1(l/k,A)$. The choice of different point P' will change a by the coboundary $\sigma \mapsto \sigma(P-P') - (P-P')$, so $[a_P] = [a_{P'}]$. If $(X',\mu') \cong (X,\mu)$, say, by isomorphism i, then defining the cocycle using the l-rational point $i(P) \in X'(l)$ will give rise to the *same* cocycle. So the assignment $X \mapsto a_P$ give rise to a well-defined map $WC(l/k,A) \to H^1(l/k,A)$. To show it is injective, suppose that $(X',\mu')$and (X,μ) give rise to cohomologous cocycles a_P and $a_{P'}$. If they differ by a coboundary $\sigma \mapsto \sigma a - a$ for $a \in A(k)$ then by choosing $P - a \in X(l)$ instead of P, we can assume that the cocycles are equal. Now the map

$$\phi : X(\bar{k}) \to X'(\bar{k}), v \mapsto (v - P) + P'$$

is an isomorphism defined over l, and using that the cocycles are identical we see that ϕ is $\mathrm{Gal}(l/k)$- invariant and therefore $(X',\mu') \cong (X,\mu)$, and our assignment is injective.
Now we will show it is surjective. Given a cocycle $a \in H^1(l/k,A)$ we define $f_\sigma : A/l \to A/l$ by $f_\sigma(P) = a(\sigma) + P$ (f_σ is defined over l as $a(\sigma) \in A(l)$). From the cocycle identity (i.e. $a(\sigma\tau) = \sigma a(\tau) + a(\sigma)$) we get the similar identity $f_\sigma \circ \sigma(f_\tau) = f_{\sigma\tau}$. By Weil descent conditions [15], this data defines uniquely a k-variety X such that $\sigma P - P = a(\sigma)$ for some $P \in X(\bar{k})$ as needed. □

2.2.3 Examples

When A/k is an elliptic curve, principal homogeneous spaces are smooth curves of genus one without rational points, that are isomorphic to A over $\bar{k}$. A general smooth curve of genus 1, is a principal homogeneous space over its jacobian, which is always an elliptic curve, see [13, Theorem 10.3.8] .

Kummer sequence

Theorem 18. *Let A/k be an Abelian variety, let $n \in \mathbb{N}$ such that n is coprime to char(k) and let $A[n]$ group of n-torsion points of $A(\bar{k})$. Then we have the* ***Kummer sequence:***

$$0 \to A(k)/nA(k) \to H^1(k, A[n]) \to H^1(k, A)[n] \to 0.$$

Proof. The Kummer Sequence follows easily from taking the cohomology (see theorem 13) of the short exact sequence that corresponds to multiplication by n:

$$0 \to A[n] \to A(\bar{k}) \xrightarrow{\cdot[n]} A(\bar{k}) \to 0.$$

Indeed, taking cohomology we get the *exact* sequence

$$0 \to A[n]^{G_k} \to A(\bar{k})^{G_k} \xrightarrow{\cdot[n]} A(\bar{k})^{G_k} \to H^1(k, A[n]) \to H^1(k, A) \xrightarrow{\cdot[n]} H^1(k, A) \to \dots$$

and since $A(\bar{k})^{G_k} = A(k)$ we get the desired sequence. □

2.2.4 Special fields

In this subsection, we state several theorems about $WC(k, A)$ for different fields k. These result will not be needed in the sequel.

1. $H^1(k, A) = 0$, for k algebraically closed. Indeed, using the geometric definition, every principal homogeneous space has a rational point, and using the cohomological definitions, G_k is the trivial group. The same is true for k separably closed, as any geometrically irreducible variety has a rational point.

2. $H^1(\mathbb{F}_q, A) = 0$ where $\mathbb{F}_q$ is the finite field with q-elements. When A is some elliptic curves, we can use Weil bounds [13, chapter V] , to get that any principal homogeneous space C, which is a curve of genus one, satisfies that
$$|C(\mathbb{F}_q)| \geq (\sqrt{q} - 1)^2 > 0$$
so C has a rational point and therefore it is trivial. For the general case there is a theorem of Lang and Weil [4] on the number of points of projective varieties over finite field, from which it follows that any principal homogeneous space of a connected algebraic variety $G/\mathbb{F}_q$ has a rational point.

3. The smooth curves
$$C_g : y^2 = -(x^{2g+2} + 1)$$
has no $\mathbb{R}$-rational points and of genus g. In particular C_1 is a non-trivial element of the Weil-Chatelet group of its Jacobian.

Chapter 3

The Brauer-Hasse-Nother theorem and Tate Local Duality

In this chapter, we explain the main theorems that are used in our characterization.

3.1 The Brauer-Hasse-Noether theorem

In many fields of mathematics one is concerned with deciding in with cases *local* data can give *global* data. This thesis in about the Tate-Shafarevich group which we will shortly define. Non-zero elements of Tate-Shafarevich group are varieties that have certain property $\mathcal{P}$ locally (having a rational point) but does not have the same property $\mathcal{P}$ globally. In such cases, we say that the local-to-global principle fails for this property $\mathcal{P}$. In the field of arithmetic, global properties are connected to a certain global field k and local properties are connected to its localizations , i.e., its completions. Being zero in $H^2(k, \mathbb{G}_m)$ is one instance of a property for which the local-to-global principle holds, and this is the part of the Brauer-Hasse-Noether theorem (we will refer to it as the BHN theorem) that we wish to prove in this section:

Theorem 19 (Brauer-Hasse-Noether)**.** *The map*

$$H^2(k, \mathbb{G}_m) \to \prod_{\nu} H^2(k_\nu, \mathbb{G}_m)$$

is injective.

There a new book in the history of mathematics, [11], which describe the collaboration of these three great mathematicians while proving the BHN theorem (it was published on January 6, 1932 in Crelle journal, in a special issue to honor the chief editor, Kurt Hensel, the mathematician who discovered the p-adic numbers. It was completed and handed to Hensel in his 70th

birthday, on December 29, 1931). The book also explains the interest in this theorem which in the form we stated it, does not look very appealing. We will follow the original proof as described in [11], but we strongly recommend to read it in the book, for a fascinating description of the genesis of one of the most famous articles in 20-th century number theory.
The proof is essentially done by several reductions to Hasse Norm theorem for cyclic extension which we will state now:

Theorem 20 (Hasse Norm Theorem)**.** *Let l/k be a cyclic extension of number fields. $0 \neq a \in k$ is a norm in l/k (i.e. it is a norm of some element in l) if and only if a is a norm in $l_{\mathfrak{p}}/k_{\mathfrak{p}}$.*

Proof. See [10, Chap VI, corollary 4.5]. □

Note that since cyclic extensions are Galois, all the extensions $l_{\mathfrak{P}}$, for primes $\mathfrak{P}$ above $\mathfrak{p}$ are isomorphic, and by $l_{\mathfrak{p}}$ we means that we choose one of them, and whether a is a norm in these fields, does not depend on our choice.
For quadratic extensions, this theorem was prove by Hilbert in 1897. For field extensions of prime degree, it was proved by Furtwängler, and Hasse generalized it for general cyclic extensions. As we will explain below, Noether showed that Hasse's generalization is not needed for the proof of the BHN theorem and that it is in fact a consequence of the BHN theorem .
As the BHN theorem was originally formulated for central simple algebras, we will describe now the relation to our formulation. A central simple algebra A over k a finite dimensional vector space over k which is also an algebra whose center is equal to k, and it contains no two-sided ideal except the whole algebra and the trivial ideal. Wedderburn's theorem (see [2, Theorem 2.1.3]) states that any such algebra A is isomorphic to the matrix algebra $M_n(D)$ where D is some uniquely defined (up to an isomorphism) division algebra over k. Two such algebras are said to be *similar* is their corresponding division algebras are isomorphic. We denote by $Br(k)$ the similarity classes of central simple algebras over k. One shows that if A and B are central simple algebras then so is $A \otimes_k B$ (see [2, Lemma 2.4.4]), and then shows that this induces a structure of a group on $Br(k)$ with the similarity class of $M_n(k)$ as a unit element (see [2, Proposition 2.4.8]). This group is called the *Brauer group of k*. As to each element of $Br(k)$ correspond a division algebra over k, one may think on $Br(k)$ as a way to give the division algebras over k a structure of a group.

Example 21. *For any algebraically closed field k, $Br(k) = 0$.*

Proof. Let D be a division algebra over k. Take an arbitrary $\alpha \in D$ and look at $k[\alpha]$. As D is a division algebra, $k[\alpha]$ is a (commutative) integral domain

of finite degree as a vector space and therefore a finite field extension. As k is algebraically closed, we have that $k = k[\alpha]$ so $\alpha \in k$. □

For any field extension l/k we have the maps $Br(k) \xrightarrow{r} Br(l)$ given by $[A] \mapsto [A_l]$ where $A_l := A \otimes_k l$. One shows that the map r does not depend on the representative A and that A_l is indeed central simple algebra over l (see [2, Lemma 2.2.2]), and that this is a group homomorphism. We say that l splits A, or that A is split in l, if A_l is similar to the identity element $[M_n(l)] \in Br(l)$. It turns out this these algebras a closely related to $H^2(k, \mathbb{G}_m)$:

Theorem 22. *$H^2(k, \mathbb{G}_m)$ is canonically isomorphic to $Br(k)$. Moreover, under this isomorphisms, the map r is exactly the restriction map res^l_k : $H^2(k, \mathbb{G}_m) \to H^2(l, \mathbb{G}_m)$.*

Proof. See [2, Theorem 4.4.7]. □

Note that given this theorem, example 21 is trivial. From example 21 it follows that for any central simple algebra A over k, $A_{\bar{k}}$ splits, and since the splitting occurs over finite extension of k, A_l splits for some finite Galois extension l/k. A formulation of theorem 19 in the terms of central simple algebras is that a central simple algebra A over k that splits in $k_\mathfrak{p}$ for all completions $k_\mathfrak{p}$ of k, splits already in k.
Let $H^2(l/k, \mathbb{G}_m) := \mathrm{Ker}(res^l_k)$. To relate these groups to Hasse norm theorem, one shows that for cyclic extension l/k,

$$H^2(l/k, \mathbb{G}_m) \cong k^*/\mathrm{Nm}(l^*) \tag{3.1}$$

and that the isomorphism sends $a \in k^*$ to the algebra $L[u]$ with the relations $u^n = a$ and $bu = ub^\sigma, \quad \forall b \in l$ where σ is a generator of the cyclic group $\mathrm{Gal}(l/k)$ (for a proof of this fact that uses only the basic techniques of group cohomology that we explained in chapter 2, see [2, Corollary 4.7.4]). We denote the algebra that correspond to a by $A(l/k, a, \sigma)$, and such algebras are called cyclic algebras. Thus $A(l/k, a, \sigma)$ splits if and only if a is a norm of l. Now, since l splits A, $l_\mathfrak{p}$ splits $A_\mathfrak{p} := A_{k_\mathfrak{p}}$ and we get a map

$$H^2(l/k, \mathbb{G}_m) \to \prod_\mathfrak{p} H^2(l_\mathfrak{p}/k_\mathfrak{p}, \mathbb{G}_m)$$

which the Hasse Norm theorem(theorem 20) claims to be injective. Indeed, 3.1 implies that being zero in the right hand side means that a is a norm in each extension $l_\mathfrak{p}/k_\mathfrak{p}$, which by Hasse norm theorem yields that a is a norm in the extension l/k, which by 3.1 shows that A splits in k. We will state again this result in a convinient form: A central simple cyclic algebra that splits everywhere locally, splits.
We shall use another fact that was developed by Brauer few years before the

proof of the BHN theorem, namely, that for any central simple algebra A over k, there exist an integer m called the index of A, such that the degree over k of any splitting field of A is divisible by m, and that there exist a splitting field of degree m. For a proof of this result, see [2, Proposition 4.5.4 and 4.5.8]

The proof of BHN theorem now follows by reduction to this case, using heavily the functorial properties of the Brauer group, i.e., the functoriallity of the restriction maps on $H^2(-, \mathbb{G}_m)$. We take a central simple algebra over k that splits everywhere locally and we want to show that it splits already in k. We assume that it doesn't, so its index m is greater that 1. We choose a prime p that divides m and take a Galois extension l that that splits A. Note that if l/k was cyclic we were done by the previous argument and we wish to make reductions to this case. Our first reduction, which was contributed by Brauer, is to the case when l/k is solvable. Let l_0 be the fixed field of some p-Sylow subgroup of $\mathrm{Gal}(l/k)$, and we have that A_{l_0} is a central simple algebra over l_0, that splits in a solvable extension l/l_0 (as its Galois group is the p-Sylow subgroup, which is of order p^n and therefore solvable) and that A_{l_0} splits everywhere locally. Now, the last reduction to cyclic extensions, was contributed by Noether, and goes as follows. As l/l_0 is solvable, where is a chain of fields

$$l_0 \subset l_1 \subset \cdots \subset l_k = l$$

such that l_i/l_{i-1} is cyclic of degree p. Now, $A_{l_{k-1}}$ splits in the cyclic extension l/l_{k-1} and everywhere locally and therefore A splits in l_{k-1}, and by the same argument, we see that A splits in l_{k-2} and so on, and therefore it splits in l_0. Thus m divides $[l_0 : k]$ which is a contradiction as p divides m and does not divide $[l_0 : k]$ by the choice of l_0.

Note that we didn't use Hasse's generalization of the Norm theorem for cyclic extensions, as our cyclic extensions where of prime degree. (this fact is interesting historically, as the second reduction was due to Noether, who immediately noticed that it bypass the need for Hasse's generalization (and prove his generalization as a consequence), and she had asked Hasse to mention it in their joint paper, which he did.)

3.2 Tate local duality

In this section F denotes be a locally compact field. Note that $H^1(F, A)$ is a discrete group and that $A^\vee(F)$ is compact group (since $A^\vee$ is projective and F is locally compact.) Tate local duality asserts that these groups are Pontraygin duals. To define a perfect pairing between them, consider the diagram that we get by considering the the Kummer sequences (see theorem

18) for A and $A^\vee$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(F)/nA(F) & \longrightarrow & H^1(F, A[n]) & \longrightarrow & H^1(F, A)[n] & \longrightarrow & 0 \\
 & & & & \times & & & & \\
0 & \longrightarrow & A^\vee(F)/nA^\vee(F) & \longrightarrow & H^1(F, A^\vee[n]) & \longrightarrow & H^1(F, A^\vee)[n] & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \text{cup-product}} & & & & \\
 & & & & H^2(F, A[n] \otimes A^\vee[n]) & & & & \\
 & & & & \downarrow{\scriptstyle \text{Weil-pairing}} & & & & \\
 & & & & H^2(F, \mu_n) & & & &
\end{array}$$

and we have that

$$H^2(F, \mu_n) \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{if } F \text{ is non-Archimedean} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } F = \mathbb{R} \text{ and } n = 2 \\ 0 & \textit{otherwise} \end{cases}$$

Theorem 23 (Tate)**.** *Under this pairing we have*

$$(A(F)/nA(F))^\perp = A^\vee(F)/nA^\vee(F)$$

and since the rows in the diagram above are exact, this induces a non-degenerate duality between $H^1(F, A)[n]$ and $A^\vee(F)/nA^\vee(F)$. We denote this pairing by $(,)_n$

Proof. We refer the reader to [6, chapter I §3]. □

Since $\cap_{n=1}^{\infty} nA^\vee(F) = 0$, then for fixed non-zero $a \in A^\vee(F)$, we can find n such that the image of a in $A^\vee(F)/nA^\vee(F)$ is non-zero. By theorem 23, there exist $\alpha \in H^1(F, A)[n]$ such that its pairing with a is non-zero. Similarly, as $H^1(F, A)$ is torsion, for given $0 \neq \alpha \in H^1(F, A)$, there exist $n \in \mathbb{N}$ such that $\alpha \in H^1(F, A)[n]$, and by 23, there exist $a \in A^\vee(F)/nA^\vee(F)$ such that its pairing with α is non-zero. One checks that by passing to the limit over n of diagrams as above, we get a non-degenerate pairing

$$(,) : A^\vee(F) \times H^1(F, A) \to \mathbb{Q}/\mathbb{Z}.$$

This gives

Theorem 24. *Let A/F be an Abelian variety over a local field F and let $A^\vee$ denote its dual. We have perfect pairing*

$$(,) : A^\vee(F) \times H^1(F, A) \to \mathbb{Q}/\mathbb{Z}.$$

Let's calculate it explicitly for $a \in A^\vee(F)/nA^\vee(F)$ and $\alpha \in H^1(F,A)[n]$. We take $\tilde{\alpha} \in H^1(F,A[n])$ that is mapped to α under

$$H^1(F,A[n]) \to H^1(F,A)[n].$$

Now, we know by the construction of the boundary maps that the image of $a \in A^\vee(F)/nA^\vee(F)$ in $H^1(F,A^\vee[n])$ is represented by the cocycle β sending $\sigma \to \sigma(a') - a'$ where $a' \in A^\vee(\bar{F})$ such that $na' = a$. As explained in subsection 2.1.7, we can pair $\tilde{\alpha}$ and β with the pairing induce by the Weil pairing and the cup-product, and we get the 2-cocycle that sends (σ,τ) to $e_n(\sigma(a') - a', \sigma\tilde{\alpha}(\tau))$.
In the sequel, we will show another calculation of this pairing, and in order to show that both calculations are equivalent, we need to calculate this pairing in terms of Cartier divisors. To this end, we choose D' such that $[D'] \in \mathrm{Pic}^0(A)(\bar{F})$ and $a' = [D']$ and define $D := nD'$. Therefore $[D] = a$. We denote $D'_\sigma = \sigma D' - D'$. Then $[D'_\sigma] = \beta(\sigma)$ and $\beta(\sigma) \in A^\vee[n]$. Indeed,

$$n[D'_\sigma] = [nD'_\sigma] = [\sigma D - D] = 0$$

since $[D] = a \in Pic^0(A)(F)$.
Now we use the construction of the Weil pairing (see section 1.4) to get functions $h_\sigma, g_\sigma \in \bar{F}(A)$ such that $(h_\sigma) = nD'_\sigma$ and $n_A^* D'_\sigma = (g_\sigma)$. As the class of D does not change by acting with translations on D, we can assume that $0_A \notin Supp(g_\sigma)$, so $g_\sigma(0)$ is not a zero nor a pole, and we can normalize it to $g_\sigma(0) = 1$. Since $g_\sigma^n = c \cdot h_\sigma \circ n_A$ and $n_A(0) = 0$, we see that $h_\sigma(0)$ is not a zero nor a pole, and we can put the constant c in h_σ in order to normalize $h_\sigma(0) = 1$. This gives

$$\zeta(\sigma,\tau) = e_n(\sigma(a') - a', \sigma\alpha(\tau)) := g_\sigma(x + \sigma\alpha(\tau))/g_\sigma(x) = g_\sigma(\sigma\alpha(\tau))$$

where the last equality in due to the normalization, putting $x = 0$.
Summing up, one way to calculate the pairing is

$$\boxed{\zeta(\sigma,\tau) = g_\sigma(\sigma\alpha(\tau))}$$

Chapter 4

Semi-Abelian varieties

Let A/k be and Abelian variety over k. In this chapter we want to establish an isomorphism of groups

$$\mathrm{Pic}^0(A) \cong \mathrm{Ext}^1(A, \mathbb{G}_m),$$

or more precisely, an isomorphism

$$\mathrm{Pic}^0(A)(l) \cong \mathrm{Ext}^1_l(A, \mathbb{G}_m).$$

An element of $\mathrm{Ext}^1(A, \mathbb{G}_m)$ is called a *semi-Abelian variety*. To formulate our characterization, we need to understand the structure of semi-Abelian varieties that correspond to elements of $\mathrm{Pic}^0(A)$ as a Galois modules.

4.1 Extension of algebraic groups

We shall describe the group structure on Ext^1. Let A, B be two commutative algebraic groups (toward the end of this chapter we will specialize to the case where A is an Abelian variety and B is some linear group). An extension L of A by B is a short exact sequence of algebraic groups and homomoprhisms

$$0 \to B \xrightarrow{i} L \xrightarrow{\pi} A \to 0$$

such that i is a closed immersion and π makes A the quotient of L by B. We state some properties of such extensions, leaving the algebraic verifications out (which are mostly done by considering the tangent spaces of these algebraic groups, See [12, chap VII §1, lemma 1].)
Two extensions of A by B, L and L', are said to be isomorphic if there exist a homomorphism $f : L \to L'$ making the following diagram commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & L & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 0 & \longrightarrow & B & \longrightarrow & L' & \longrightarrow & A & \longrightarrow & 0. \end{array}$$

In this case f is automatically an isomorphism.
We denote by $Ext^1(A,B)$, the set of isomorphism classes of extensions of A by B. Since all our manipulations with such classes of extensions will not depend on specific representatives, we will ignore the distinction between a specific extenstion L and its isomorphism class in $\mathrm{Ext}^1(A,B)$.
We claim that $\mathrm{Ext}^1(A,B)$ is a contravariant functor in A and a covariant functor in B. Indeed, given a homomorphism $\phi : B \to B'$ and $L \in \mathrm{Ext}^1(A,B)$, we define $\phi_*(L) \in \mathrm{Ext}^1(A,B')$ to be the quotient of $L \times B'$ by the subgroup $\{(-i(b), \phi(b)) | b \in B\}$ where i is the injection of B into L. The canonical map $B' \to L \times B'$ (resp. $L \times B' \to L$) composed (resp. induced by) the quotient map $L \times B' \to \phi_*(L)$, gives the desired extension

$$0 \to B' \to \phi_*(L) \to A \to 0.$$

$\phi_*(L)$ is also characterized as the unique extension $L' \in \mathrm{Ext}^1(A,B')$ such that there exist a homomorphism $\Phi : L \to L'$ making the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & L & \longrightarrow & A & \longrightarrow & 0\,. \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 0 & \longrightarrow & B' & \longrightarrow & L' = \phi_*(L) & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Similarly, given a homomorphism $\psi : A' \to A$ and $L \in \mathrm{Ext}^1(A,B)$, we define $\psi^*(L) \in \mathrm{Ext}^1(A',B)$ by the subgroup of $A' \times L$ defined $\{(g',l) | \psi(g') = \pi(l)\}$ where π is the projection of L onto A. This gives a sequence

$$0 \to B \to \psi^*(L) \to A' \to 0$$

using the canonical projections $\pi_{A'} : A' \times L \to A'$, $\pi_L : A' \times L \to L$.
$\psi^*(L)$ is also characterized as the unique extension $L' \in \mathrm{Ext}^1(A',B)$ such that there exist a homomorphism $\Psi : L' \to L$ making the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & L' = \psi^*(L) & \longrightarrow & A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & B & \longrightarrow & L & \longrightarrow & A & \longrightarrow & 0. \end{array}$$

One easily check that these definitions makes $\mathrm{Ext}^1(A,B)$ into a contravariant functor in A and a covariant functor in B. One also checks that $f^* g_* = g_* f^*$.
Now, it is easy to define a group law in $\mathrm{Ext}^1(A,B)$: given $L, L' \in \mathrm{Ext}^1(A,B)$, the product $L \times L'$ is an element of $\mathrm{Ext}^1(A \times A, B \times B)$. Let $d : A \to A \times A$ be the diagonal map and $s : B \times B \to B$ be the multiplication map. One defines

$$L + L' = d^* s_* (L \times L') \in \mathrm{Ext}^1(A,B).$$

For a proof that this is indeed a group law , we refer to [12, chap VII §Proposition 1].

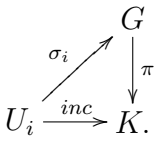
4.2 Theta groups

This section explains how semi-Abelian varieties arise in a bit broader point of view. In [9, §23] Mumford studies short exact sequences of group schemes [1]

$$1 \to \mathbb{G}_m \xrightarrow{i} G \xrightarrow{\pi} K \to 1$$

such that

1. K is commutative.
2. There exists an open covering $\{U_i\}$ of K and sections σ_i of π: i.e.



3. i is a closed immersion, which makes $\mathbb{G}_m$ into the kernel of π.
4. $\mathbb{G}_m$ is in the center of G.

Such a sequence is called a *theta group* or G is called a *theta group*.
This theorem explains how theta groups arise in the context of Abelian varieties:

Theorem 25. *Let $\mathcal{L}$ be a line bundle on an Abelian variety. Then there is a sequence of group schemes*

$$1 \to \mathbb{G}_m \xrightarrow{i} \mathcal{G}(\mathcal{L}) \xrightarrow{\pi} K(\mathcal{L}) \to 0$$

were $K(\mathcal{L})$ were defined in 1.1

Proof. We will get back to the construction of $\mathcal{G}(\mathcal{L})$, when $\mathcal{L} \in \mathrm{Pic}^0(A)$, later in this chapter. For a proof, see [9, page 225]. □

By definition, if $\mathcal{L} \in \mathrm{Pic}^0(A)$ then $K(\mathcal{L}) = A$, so an element $\mathcal{L}$ of $\mathrm{Pic}^0(A)$ gives rise to an extension of A by $\mathbb{G}_m$ i.e., a sequence of group schemes

$$1 \to \mathbb{G}_m \xrightarrow{i} \mathcal{G}(\mathcal{L}) \xrightarrow{\pi} A \to 0$$

[1] A group scheme is a group object in the category of schemes,i.e., It is a functor from **Schemes** to **Groups**. For a great introduction to the subject see [14]

In fact, in this case $\mathcal{G}(\mathcal{L})$ is commutative group (Since in general, one has a pairing

$$e^{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \to \mathbb{G}_m$$

that 'measures' the deviation of $\mathcal{G}(\mathcal{L})$ from being commutative, and in our case this pairing is trivial as $K(\mathcal{L}) = A$ so $e^{\mathcal{L}}$ is a map form a complete variety $A \times A$ to an affine one, and therefore trivial.), so theorem 25 give a map

$$\mathrm{Pic}^0(A) \to \mathrm{Ext}^1(A, \mathbb{G}_m), \quad \mathcal{L} \mapsto \mathcal{G}(\mathcal{L}) \tag{4.1}$$

which is in fact group isomorphism as we explain in the next section.

4.3 Serre view on the proof of the isomorphism (4.1).

In this section, A and B denote a connected, commutative algebraic groups. We review the several steps in a proof of the isomorphism 4.1 in [12, chap VII]. In that chapter, Serre studies $\mathrm{Ext}^1(A, B)$ for general algebraic group A and B, and we will review some results that are proved there and are used to prove the above isomorphism 4.1.
First, Serre generalizes theorem 12, to the case of commutative algebraic group (in this context, we will write group law additively). As explained after theorem 12, the commutative case corresponds to a trivial action of A and symmetric factors set. We recall the definitions in this for this case. $H^2(A, B)_s$ is the set of 'symmetric factor system' modulo 'trivial factor systems'. A factor system is a set map $f : A \times A \to B$ such that

$$f(y, z) - f(x + y, z) + f(x, y + z) - f(x, y) = 0, \quad \forall x, y, z \in A \tag{4.2}$$

and

$$f(x, y) = f(y, x) \forall x, y \in A.$$

a 'trivial factor systems' is of the form δg where $g : A \to B$ is any set map, and $\delta g(x, y) = g(x+y)-g(x)-g(y)$. Note that it is automatically symmetric. Now, Serre considers two groups:

1. $H^2_{\mathrm{rat}}(A, B)_s$, which consists of rational functions $f : A \times A \to B$ which are also symmetric factor systems, modulo such functions that are equal to δg, where $g : A \to B$ is some rational function.

2. $H^2_{\mathrm{reg}}(A, B)_s$, which consists of regular functions $f : A \times A \to B$ which are also symmetric factor systems, modulo such functions that are equal to δg, where $g : A \to B$ is some regular function.

Proposition 26. *With the above definitions we have that*

1. *$H^2_{reg}(A,B)_s$ is isomorphic to the subgroup of $Ext(A,B)$ given by extensions which admit a regular section.*

2. *$H^2_{rat}(A,B)_s$ is isomorphic to the subgroup of $Ext(A,B)$ given by extensions which admit a rational section.*

In particular, the canonical morphism $H^2_{reg}(A,B) \to H^2_{rat}(A,B)$ is injective.

Proof. The proof of the first statement follows the same lines as the proof of theorem 12. We recall them shortly: If $C \in \mathrm{Ext}(A,B)$ admits a regular section $s : A \to C$, then one defines the factor system $f(x,y) = s(x+y) - s(x) - s(y)$. One sees that it defines an element of $H^2_{\mathrm{reg}}(A,B)_s$. We denote by $\mathrm{Ext}(A,B)_*$ the set of extensions that have regular section,and one checks it is a subgroup of $\mathrm{Ext}(A,B)$. We defined a map $\theta : \mathrm{Ext}(A,B)_* \to H^2_{\mathrm{reg}}(A,B)_s$. If $\theta(C) = 0$ then it is an extension with a regular section that it is a homomorphism, so C is the trivial extension. So θ is injective. To see it is surjective, we take $[f] \in H^2_{\mathrm{reg}}(A,B)_s$ (i.e. f is a symmetric factor system) and define $A \rtimes_f B$ as in the proof of theorem 12. Since f is regular, one checks easily that $A \rtimes_f B$ is an algebraic group which is an extension of A by B and that $\theta(A \rtimes_f B) = [f]$.
The second statement follows the same line of proof but is a bit more subtle. Again, we denote by $\mathrm{Ext}(A,B)_{**}$ the set of extensions that have rational section, and one checks it is a subgroup of $\mathrm{Ext}(A,B)$. In the exact same way as above, ee define a map $\theta : \mathrm{Ext}(A,B)_{**} \to H^2_{\mathrm{rat}}(A,B)_s$. To see it is injective, we just need to notice that a rational section s which is a homomorphism is automatically regular (this is easy: if $s|_U$ is regular, then $s|_{x+U} = s(x) + s|_U$ since s is a homomorphism, so it is regular on $x+U$ too. Since the translate of U cover A, s is regular.),and therefore, injectivity follows as above. Now, to see surjectivity, one defines again $A \rtimes_f B$ but now, the composition law is only rational. According to results of Weil cited and explained in [12, chap V, §5], there is a connected algebraic group C, birationally equivalent by a map F to $A \rtimes_f B$ with the same composition law, this makes C commutative as f is symmetric. Using F one makes C into an extension of A by B, and surjectivity follows as above.
The last statement on the proposition is obvious, as we identified both terms as subgroups of $\mathrm{Ext}(A,B)$. □

As we are interested in the case that $B = \mathbb{G}_m$, we can go further:

Proposition 27. *If B is linear, then $H^2_{rat}(A,B)_s \cong Ext(A,B)$. This applies in particular when $B = \mathbb{G}_m$.*

Proof. By proposition 26, we only have to show that any extension $C \in \mathrm{Ext}(A,B)$ admits a rational section. Let ξ be the generic point of A. Its

inverse image in C, B_ξ, is a principal homogeneous space for B. If $B = \mathbb{G}_m$ it follows from Hilbert theorem 90 (example 14) that B_ξ is trivial and therefore contains a $k(\xi)$ rational point. So we have a morphism $\mathrm{Spec}(k(\xi)) \to B_\xi \subset C$, which is equivalent to having a rational section from $A \to C$. Serre proves the general case, i.e., for general linear group B instead of $\mathbb{G}_m$, with the same arguments, just by noting that any such B admits a composition series whose quotients are isomorphic to $\mathbb{G}_m$ or $\mathbb{G}_a$, so the result follows by showing that $H^1(k, \mathbb{G}_a) = 0$ for any field k (which is an easy theorem in Galois theory), and using the functoriality of H^1. (We need only the case $B = \mathbb{G}_m$ in the sequel.) □

Proposition 28. *Let B be a linear group and let $\mathcal{B}_A$ be the sheaf of germs of regular maps from A to B. We have a map*

$$\pi : Ext(A, B) \cong H^2_{rat}(A, B)_s \longrightarrow H^1(A, \mathcal{B}_A).$$

The kernel of π is $H^2_{reg}(A, B)_s$.
In particular, when $B = \mathbb{G}_m$, we have an map

$$\pi : Ext(A, \mathbb{G}_m) \cong H^2_{rat}(A, \mathbb{G}_m)_s \longrightarrow H^1(A, \mathcal{O}^*_A) \cong Pic(A).$$

Proof. Let $C \in \mathrm{Ext}(A, B)$ be an extension with rational section. Let U be the non-empty subset of A such that $s : U \to C$ is regular. As the translates of U cover A, we can find a cover $\{U_i\}$of A and sections $s_i : U_i \to C$ (composition of translation of A and s). Letting $b_{ij} := s_i - s_j$ we see that it is a map $U_i \cap U_j \to \ker(C \to A) = B$, and we easily check that it satisfies the cocycle identity and thus defines an element of $H^1(A, \mathcal{B}_A)$.

Elements of the kernel of π are ones that are isomorphic to an extension that has a regular section, and by proposition 26, these are exactly the elements of $H^2_{reg}(A, B)_s$. The last statement is obvious and will be explained again in the next theorem. □

We need to explain of element of $H^1(A, \mathcal{B}_A)$ corresponds to 'principal fiber spaces' with base A and structure group B (in Serre language), or in other language, B-torsors over A.
A *B-torsor over A* is a variety C with projection morphism $\pi : C \to A$, on which B acts transitively and faithfully on each fiber of π. Note that any extension of A by B is a B-torsor. One defines a natural equivalence of torsors (just by isomorphism that respect the action of B fiber-wise) and a basic fact in cohomology shows that equivalence classes of torsors are in fact a group with is isomorphic to $H^1(A, \mathcal{B}_A)$. We briefly describe how a cocycle $(f_i : U_i \to B)_{i \in I} \in H^1(A, \mathcal{B}_A)$ give rise to a B-torsor; one glue $\{U_i \times B\}_{i \in I}$ using the maps $f_i - f_j : U_i \cap U_j \to B$ (i.e., take the identity on $U_i \cap U_j$ and

twist the fibers by $f_i - f_j$). The cocycle identity is exactly the necessary information for gluing $U_i \times B$. If C is a B-torsor over A we write

$$0 \longrightarrow B \rightsquigarrow C \longrightarrow A \longrightarrow 0$$

where $0 \to B \rightsquigarrow C$ just means that B acts transitively and faithfully on C. In this notation, we can say that the pull-back and push-forward on $H^1(-,-)$ translates to maps on fiber spaces in the same way as we had for extensions in section 4.1, that is, given homomorphism $\phi : B \to B'$ and $L \in H^1(A, \mathcal{B}_A)$, $\phi_*(L) \in H^1(A, \mathcal{B}'_A)$ is characterized as the unique element $L' \in H^1(A, \mathcal{B}'_A)$ such that there exist a homomorphism $\Phi : L \to L'$ making the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \rightsquigarrow & L & \longrightarrow & A & \longrightarrow & 0\,. \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 0 & \longrightarrow & B' & \rightsquigarrow & L' = \phi_*(L) & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Similarly, given a homomorphism $\psi : A' \to A$ and $L \in H^1(A, \mathcal{B}_A)$, $\psi^*(L) \in H^1(A', \mathcal{B}_{A'})$ is characterized as the unique extension $L' \in H^1(A', \mathcal{B}_{A'})$ such that there exist a homomorphism $\Psi : L' \to L$ making the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \rightsquigarrow & L' = \psi^*(L) & \longrightarrow & A' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & B & \rightsquigarrow & L & \longrightarrow & A & \longrightarrow & 0. \end{array}$$

Commutativity of these diagrams means that the map in the diagram are compatible with the actions in the diagram.

We want to define the subgroup of primitive elements of $H^1(A, \mathcal{B}_A)$. We fix B and for brevity sake we denote by $T(X) := H^1(X, \mathcal{B}_X)$. The projections $p, q : A \times A \to A$ and the injections $i, j : A \to A \times A$ (defined by $i(a) = (a, 0_A)$ and $j(a) = (0_A, a)$) give rise to $p^*, q^* : T(A) \to T(A \times A)$ and $i^*, j^* : T(A \times A) \to T(A)$, that satisfy that $i^* \circ p^* = \mathrm{Id} = j^* \circ q^*$ and $j^* \circ p^* = 0 = i^* \circ q^*$. Therefore the map

$$(p^*, q^*) : T(A) \times T(A) \to T(A \times A)$$

admits a left inverse $i^* \times j^*$, and therefore $T(A) \times T(A)$ is a direct factor of $T(A \times A)$. Elements which belongs to this direct factor are called *decomposable*. Now taking $x \in T(A)$ we see that $(i^* \times j^*) \circ m_A^*(x) = (x, x)$ as $m_A \circ i = m_A \circ i = \mathrm{Id}$. We call $x \in T(A)$ *primitive* if $m_A^*(x) = (x, x)$, which is equivalent to saying that $m_A^*(x)$ is decomposable, by the last remark. Note that by writing $m_A^*(x) = (x, x)$ we identify $T(A) \times T(A)$ with its image in

$T(A \times A)$ via (p^*, q^*). When $B = \mathbb{G}_m$ the map $(p^*, q^*)(\mathcal{L}) = p^*\mathcal{L} \otimes q^*\mathcal{L}$ and therefore primitive elements are the ones for which $m_A^*\mathcal{L} \cong p^*\mathcal{L} \otimes q^*\mathcal{L}$, i.e., primitive elements of $H^1(A, \mathcal{O}_A^*) = \mathrm{Pic}(A)$ are exactly the elements in $\mathrm{Pic}^0(A)$.

We are now ready to state and prove the main result of this section:

Theorem 29. *When A is an Abelian variety, and B is a linear group, the above map*

$$\pi : Ext(A, B) \cong H^2_{rat}(A, B)_s \longrightarrow H^1(A, \mathcal{B}_A)$$

is injective and its image is exactly the subgroup of primitive elements.

Proof. By proposition 28 we know that the kernel of π is $H^2_{reg}(A, B)_s$, but since A is proper and B is affine, there are no non-constant morphisms $A \times A \to B$. Another, more direct argument goes as follows: if $C \in \mathrm{Ker}(\pi)$ then there is a regular section $s : A \to C$. We think of B as subgroup of C.Translating by element of B if needed, we can assume that $s(0) = 0$. Since A is proper, $s(A)$ is a proper subvariety of C and the subgroup generated by it, A', is also a complete subvariety of C.As B is affine, $A' \cap G_m$ is finite. We consider the projection map $A' \to A$. Since s is a section, it is surjective and its kernel is $A' \cap G_m$ and therefore finite. By theorem 5, we have that $\dim A' = \dim A = \dim(s(A))$, and as A' is irreducible, it follows that $A' = s(A)$, so s(A) is a subgroup of C, which implies that s is a homomorphism and therefore C is the trivial extension. So π is injective.

Let x be a primitive element of $H^1(A, \mathcal{B}_A)$. We wish to find $C \in \mathrm{Ext}^1(A, B)$ such that $\pi(C) = x$. Let C be the B-torsor that corresponds to x, and we denote

$$0 \longrightarrow B \rightsquigarrow C \xrightarrow{\pi} A \longrightarrow 0$$

Using the push-foward and the pull-back operators, $m_A : A \times A \to A$ induces:

$$\begin{array}{ccccccc} 0 & \longrightarrow & B & \rightsquigarrow & m_A^*(C) & \longrightarrow & A \times A \longrightarrow 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow & & \downarrow{\scriptstyle m_A} \\ 0 & \longrightarrow & B & \rightsquigarrow & C & \xrightarrow{\pi} & A \longrightarrow 0, \end{array}$$

and the multiplication morphism $m_B : B \times B \to B$ induces:

$$\begin{array}{ccccccc} 0 & \longrightarrow & B \times B & \rightsquigarrow & C \times C & \xrightarrow{\pi \times \pi} & A \times A \longrightarrow 0 \\ & & \downarrow{\scriptstyle m_B} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} \\ 0 & \longrightarrow & B & \rightsquigarrow & m_{B*}(C \times C) & \longrightarrow & A \times A \longrightarrow 0. \end{array}$$

As $p^* m_{B*}(C \times C) = C$ and $q^* m_{B*}(C \times C) = C$ it is clear, that $m_{B*}(C \times C) = (p^*, q^*)(x)$ and since x is primitive we get that

$$m_A^*(C) = m_{B*}(C \times C).$$

Putting both diagrams together we have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B\times B & \rightsquigarrow & C\times C & \xrightarrow{\pi\times\pi} & A\times A & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle m_B} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} & & \\
0 & \longrightarrow & B & \rightsquigarrow & m_{B*}(C\times C) & \longrightarrow & A\times A & \longrightarrow & 0\\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & B & \rightsquigarrow & m_A^*(C) & \longrightarrow & A\times A & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow & & \downarrow{\scriptstyle m_A} & & \\
0 & \longrightarrow & B & \rightsquigarrow & C & \xrightarrow{\pi} & A & \longrightarrow & 0.
\end{array}$$

This gives a map g fitting in the commutative diagram

$$\begin{array}{ccc}
C\times C & \xrightarrow{g} & C\\
\downarrow{\scriptstyle \pi\times\pi} & & \downarrow{\scriptstyle \pi}\\
A\times A & \xrightarrow{m_A} & A
\end{array} \tag{4.3}$$

such that

$$g(c+b,c'+b') = g(c,c') + b + b', \quad \forall b,b' \in B, \forall c,c' \in C. \tag{4.4}$$

We choose a point $e \in G$ that projects to 0_A, the identity element of A. By the commutativity of 4.3 and since $m_A(0_A,0_A) = 0_A$, $g(e,e) - e \in B$, so by translating e by element of B we can suppose that $g(e,e) = e$.
Using that A is proper, we will show now that g is in fact a group law on C making it a commutative algebraic group with e as an identity element.

1. Unit element: $g(e,c) = g(c,e) = c, \quad \forall c \in C$. By the commutativity of 4.3 and since $m_A(\pi(c),0_A) = m_A(0_A,\pi(c)) = \pi(c)$. So $g(c,e) - c \in B$ and therefore we have $h_1, h_2 : C \to B, \quad h_1(c) := g(c,e) - c, h_2(c) := g(e,c) - c$ gives a function from $C \to B$. Moreover, by 4.4, $h_1(c+b) = g(e,c+b) - (c+b) = g(e,c) + b - c - b = g(e,c) - c = h_1(c)$ so h_1 factors through A, and likewise h_2. Since A is proper all the maps from it to B are constants, and since $g(e,e) = e$ we have that $h_1(c) = h_2(c) = e, \forall c \in C$.

2. Commutativity: $g(c,c') = g(c',c), \quad \forall c,c' \in C$. In a similar way, we define $h(c,c') := g(c,c') - g(c',c)$ and we see that $g(c,c') - g(c',c) \in B$, by the commutativity of 4.3 and since $m_A(\pi(c),\pi(c')) = m_A(\pi(c'),\pi(c))$. Moreover, by 4.4, $h(c+b,c'+b') = g(c+b,c'+b') - g(c'+b',c+b) = g(c,c') + b + b' - (g(c',c) + b + b') = h(c,c')$, therefore h factors through the proper variety $A \times A$ so h is a constant. Since $g(e,e) = e$ we have that $h(c,c') = e, \forall c,c' \in C$.

3. Associativity: $g(c, g(c', c'')) = g(g(c, c'), c''), \quad \forall c, c', c'' \in C$. By the same arguments, the difference map

$$k(c, c', c'') := g(c, g(c', c'')) - g(g(c, c'), c'')$$

in to B and factors through $A \times A \times A$, and therefore a constant which equals $k(e, e, e) = e$.

4. Inverse map: there exist a regular map $i : C \to C$ such that $g(c, i(c)) = e$. One uses again the fact that x is primitive to construct a map i fitting in the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{i} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} \\ A & \xrightarrow{i_A} & A \end{array} \tag{4.5}$$

such that

$$i(c + b) = i(c) + b, \quad \forall b \in B, c \in C \tag{4.6}$$

where i_A is the inverse map of A, and one normalizes i, in the same way, to $i(e) = e$. Now, by the same argument as above, the difference map $l(c) := g(c, i(c)) - e$ is a map from C to B that factors through A, and therefore a constant which equals $l(e) = e$.

This complete the proof and show in particular, that for $B = \mathbb{G}_m$, one has $\mathrm{Ext}^1(A, B) \cong \mathrm{Pic}^0(A)$. Serre notes that the (representative) rational factor system that corresponds to and element $\mathcal{L} \in \mathrm{Pic}^0(A)$ is a function f whose divisor

$$(f) = \Lambda(\mathcal{L}) := m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1} \otimes q^*\mathcal{L}^{-1}.$$

We come back to this factor system in the next section. □

4.4 Explicit description $\mathcal{G}(\mathcal{L})$.

We explained in the proof of proposition 26 that given a variety V with *rational* multiplication and inverse morphism on it (Serre calls such a variety a 'birational group'), there exists a unique algebraic group (i.e. a variety with *regular* composition laws) with the the same composition laws, birationally isomorphic to V. Therefore, in the sequel we define group varieties by rational composition laws and we really mean that we take a 'true' algebraic group that has the same composition laws.
We return to our original situation. A/k denotes an Abelian variety over k, and $\mathcal{L} \in \mathrm{Pic}^0(A)(k)$. Let $f \in \bar{k}(A)$ such that

$$(f) = \Lambda(\mathcal{L}) := m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1} \otimes q^*\mathcal{L}^{-1},$$

and normalized by $f(0_A, 0_A) = 1$. As explained above we have the variety $\mathbb{G}_m \rtimes_f A$ which is the variety $\mathbb{G}_m \times A$ with the birational composition laws

$$(t, a) \cdot (t', a') = (tt' f(a, a'), a + a'), \quad a, a' \in A,\ t, t' \in \mathbb{G}_m.$$

This is an algebraic group over $\bar{k}$ and we denote it as $X_{\mathcal{L}}$.

As $f \in \bar{k}(A)$, for any $\sigma \in G_k$ we will have different group structure, namely, we use ${}^{\sigma}f := \sigma \circ f \circ \sigma^{-1}$ to add points and we denote this group variety as $X_{\sigma\mathcal{L}}$. We appeal to Weil's decent conditions [15] in order to define an extension of A by $\mathbb{G}_m$ over the base field k, using the varieties $X_{\sigma\mathcal{L}}, \sigma \in G_k$. We already use Cartier divisors instead of invertible sheaves. We denote by D the a Cartier divisor such that $[D] = [\mathcal{L}] \in \mathrm{Pic}^0(A)(k)$ and by h_σ a function that satisfy $(h_\sigma) = \sigma D - D$ with $h_\sigma(0_A) = 1$. Note that by comparing divisors we have that

$$\frac{{}^{\sigma}f}{f} = \frac{h_\sigma \circ m_A}{(h_\sigma \circ p)(h_\sigma \circ q)},$$

or

$$\frac{{}^{\sigma}f(x, y)}{f(x, y)} = \frac{h_\sigma(x + y)}{h_\sigma(x) h_\sigma(y)}, \quad \forall x, y \in A(\bar{k})$$

We define $\psi_\sigma : X_{\mathcal{L}} \to X_{\sigma\mathcal{L}}$ by $(t, x) \to (t h_\sigma(x), x)$.

Lemma 30. *For all $\sigma \in G_k$, ψ_σ is a group homomorphism, and these homomorphisms satisfies the identity*

$$\psi_\sigma \circ {}^{\sigma}\psi_\tau = \psi_{\sigma\tau},$$

for all $\sigma, \tau \in G_k$.

Proof. First we check that it is a homomorphism:

$$\psi_\sigma\left((t, x)(t', x')\right) = \psi_\sigma((tt' f(x, x'), x + x')) = (tt' f(x, x') h_\sigma(x + x'), x + x')$$

and

$$\psi_\sigma(t, x)\psi_\sigma(t', x') = (t h_\sigma(x), x)(t' h_\sigma(x'), x') = (tt' {}^{\sigma}f(x, x') h_\sigma(x) h_\sigma(x), x + x')$$

and equality follows from the equality above

$$\frac{{}^{\sigma}f(x, y)}{f(x, y)} = \frac{h_\sigma(x + y)}{h_\sigma(x) h_\sigma(y)}.$$

Now, we establish the identity above:

$$\psi_\sigma \circ {}^{\sigma}\psi_\tau(t, x) = \psi_\sigma \circ \sigma(\psi_\tau(\sigma^{-1}(t, x))) = \psi_\sigma \circ \sigma(\psi_\tau(\sigma^{-1}t, \sigma^{-1}x)) =$$

$$= \psi_\sigma \circ \sigma((\sigma^{-1}t h_\tau(\sigma^{-1}x), \sigma^{-1}x)) = \psi_\sigma \circ (t\sigma(h_\tau(\sigma^{-1}x)), x) =$$

$$= (t\sigma(h_\tau(\sigma^{-1}x))h_\sigma(x), x) = (t{}^{\sigma}h_\tau(x)h_\sigma(x), x)$$

The latter is equal to $\psi_{\sigma\tau}(t,x) = (th_{\sigma\tau}(x), x)$ iff

$$h_{\sigma\tau}(x) = {}^{\sigma}h_\tau(x)h_\sigma(x)$$

which is easily checked by looking at the divisor of both sides, using the fact $(h_\rho) = \rho D - D, \quad \forall \rho \in G_k$, and the normalization $h_\rho(0_A) = 1, \quad \forall \rho \in G_k$. Indeed,

$$\sigma\tau D - D = \sigma\tau D - \tau D + \tau D - D = \sigma(\tau D - D) + (\tau D - D).$$

□

In [15] Weil shows that the conditions on $\{\psi_\sigma\}_{\sigma\in G_k}$ that appear in lemma 30 are necessary and sufficient for the existence of a unique (up to birational isomorphism) variety X defined over k, such that $X_{\bar{k}} \cong X_{\mathcal{L}}$ and ψ_σ comes from the base change $\mathrm{Spec}(\bar{k}) \xrightarrow{\sigma} \mathrm{Spec}(\bar{k})$.
Therefore, we have that for $(t,a) \in X_{\mathcal{L}}$, $\sigma(t,a)$ is the image under ψ_σ^{-1} of $(\sigma t, \sigma a)$, which gives

$$\boxed{\sigma(t,a) = (\sigma t h_\sigma(\sigma a)^{-1}, \sigma a)}$$

For later use we calculate here the inverse of an element in $X_{\mathcal{L}}$; we need to solve x and y in the following equation:

$$(x,y)(t,a) = (1, 0_A).$$

One checks that $y = -a$ and $x = t^{-1}f(a,-a)^{-1}$ will work and therefore

$$\boxed{(t,a)^{-1} = (t^{-1}f(a,-a)^{-1}, -a)}$$

Chapter 5

The Mordell-Weil Theorem and the Tate-Shafarevich Group

5.1 The Mordell-Weil Theorem

The arithmetic side of Abelian varieties started, in some sense, in the Mordell-Weil theorem. Recall that the group law on an elliptic curve is a 'geometric' one, which is called the 'the tangent and chord process'. Mordell's original formulation of the theorem was

Theorem 31. *On an ellptic curve over $\mathbb{Q}$ there exist a finite set of rational points such that all rational points may be obtained from them by the tangent and chord process.*

André Weil, in his thesis, generilized this theorem to

Theorem 32. *Let A be an Abelian variety over a number field k. Then the group $A(l)$ where l/k is a finite extension, is a finitely generated Abelian group.*

Using similar techniques, Serge Lang generalized it to arbitrary Abelian varieties (in fact, Weil proved it for jacobians of curves), and for fields which are finitely generated over their prime field.

We approach this proof in more general settings than usual proofs, using Galois cohomology. We follow the exposition of [3, §C.4.]

The proof has three parts. First one proves the

Theorem 33 (Weak Mordell-Weil)**.** *Let A/k be an Abelian variety over a number field k. For any n, the group $A(k)/nA(k)$ is finite. The latter group is commonly called the weak Mordell Weil group.*

We will review the proof of the weak Mordell-Weil theorem in the next section, using it to introduce the Selmer group and the Tate-Shafarevich

group.
Now, the second part is Weil development of a very useful tool, called **height**, which is kind of measurement for the 'arithmetic size' or 'arithmetic complexity' of a point on a variety. We will not explain this subject, which turned-up to be a very fruitful one (many important theorems in Diophantine analysis uses it) and we refer to [3] an account about heights (and also about the Mordell-Weil theorem).
In the third part of the proof, Weil used this tool to manage to do Fermat's 'infinite descent', i.e., he showed that $A(k)$ is finitely generated by doing some iterative process using heights that take an arbitrary point and does an iterative process on it the sends it eventually to the the finite weak Mordell-Weil group.

Proposition 34. *Let $\alpha : A \to B$ be an isogeny of two Abelian varieties which are defined over k. Then the short exact sequence*

$$0 \to Ker(\alpha) \xrightarrow{i} A(\bar{k}) \xrightarrow{\alpha} B(\bar{k}) \to 0$$

induces a long exact sequence of cohomology groups

$$0 \to Ker(\alpha)(k) \xrightarrow{i} A(k) \xrightarrow{\alpha} B(k) \xrightarrow{\delta} H^1(G_k, Ker(\alpha)) \xrightarrow{i} H^1(G_k, A(\bar{k})) \xrightarrow{\alpha} H^1(G_k, B(\bar{k})).$$

This sequence yields

$$0 \to B(k)/\alpha A(k) \xrightarrow{\delta} H^1(G_k, Ker(\alpha)) \xrightarrow{i} H^1(G_k, A(\bar{k}))[\alpha] \to 0 \qquad (5.1)$$

Note that when we consider $\alpha = [n] : A \to A$ we last sequence is

$$0 \to A(k)/nA(k) \xrightarrow{\delta} H^1(G_k, A[n]) \xrightarrow{i} H^1(G_k, A(\bar{k}))[n] \to 0$$

where its first term is the weak Mordell-Weil group.

Proof. This easily follows from theorem 13. □

We wish to prove that $B(k)/\alpha A(k)$ is finite. We managed to embed it in $H^1(G_k, \mathrm{Ker}(\alpha))$ but the latter is usually infinite. In the next section we will 'cut it down' using localizations.

5.2 The Tate-Shafarevich and the Selmer groups

Let ν be a place of k and let k_ν be the corresponding completion. Let $G_\nu := G_{k_\nu} := Gal(\bar{k}_\nu/k_\nu)$ and we have $G_\nu \hookrightarrow G_k$ and therefore a functorial

restriction $res_\nu : H^r(G_k, A) \to H^r(G_\nu, A)$. There is a 'local' short exact sequence as above which fits in the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B(k)/\alpha A(k) & \xrightarrow{\delta} & H^1(G_k, \mathrm{Ker}(\alpha)) & \xrightarrow{i} & H^1(G_k, A(\bar{k}))[\alpha] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B(k_\nu)/\alpha A(k_\nu) & \xrightarrow{\delta_\nu} & H^1(G_\nu, \mathrm{Ker}(\alpha)) & \xrightarrow{i_\nu} & H^1(G_\nu, A(\bar{k}_\nu))[\alpha] & \longrightarrow & 0. \end{array}$$

We see that for all $x \in B(k)$, $\delta_v(x)$ is in the kernel of i_v. This motivates:

Definition 35. *Let $\alpha : A \to B$ be an isogeny of Abelian varieties defined over a number field k. The* Selmer group *of A with respect to α is the group*

$$Sel^{(\alpha)}(A/k) := \bigcap_\nu Ker\{H^1(G_k, Ker(\alpha)) \to H^1(G_\nu, A(\bar{k}_\nu))[\alpha]\}$$

and when $\alpha = [n]$ we denote $Sel^n(A/k) := Sel^{[n]}(A/k)$.
The Tate-Shafarevich group *of A is the group*

$$Ш(A/k) := \bigcap_\nu Ker\{H^1(G_k, A(\bar{k})) \to H^1(G_\nu, A(\bar{k}_\nu))\}$$

Where the intersection is taken over all the places of k.

Let's stop and think on the geometric side of these definitions. As explained above, elements of $H^1(k, A) := H^1(G_k, A(\bar{k}))$ corresponds to isomorphism class of principal homogeneous space for A. Since triviality of such a principal homogeneous space is determined by whether it possesses a rational point, elements in $Ш(A, k)$ are principal homogeneous spaces with k_ν-rational point for all the places of k. In particular, a non-zero element is a principal homogeneous space without a k-rational point (we say that it does not have global points) but with k_ν-rational point for all places ν of k (we say that it has points everywhere locally). On many arithmetic objects one studies this local-to-global principle. In particular, Hasse studied quadratic forms, and found that a quadratic form has a rational global point if and only if it has points everywhere locally. This is not longer true for principal homogeneous spaces of Abelian varieties, even not for elliptic curves, for which principal homogeneous spaces are curves of genus 1. In particular there are cubics that have points everywhere locally without global points. One of the first examples that where find of such curves was the curve $3X^3 + 4Y^3 + 5Z^3 = 0$ that has no $\mathbb{Q}$ rational points and has $\mathbb{Q}_p$-rational point for every p, and $\mathbb{R}$-rational point. It is therefore a non-trivial element of the Tate-Shafarevich group of its Jacobian.
The Tate-Shafarevich group measure the failure of the local-to-global principle.

Thinking of the image of $H^1(G_k, \mathrm{Ker}\alpha)$ in $H^1(G_k, A(\bar{k}))$, we see that (isomorphism classes of) principal homogeneous spaces that correspond to elements of the Selmer group possess k_ν-rational point for all the places ν. Note that as opposed to the geometric description of elements of $Ш(A,k)$, this description does not characterize elements of the Selmer group. One can easily give such geometric characterization as principal homogeneous spaces with some additional data.

With these definitions, the exact sequence 5.1 yields

$$0 \to B(k)/\alpha A(k) \to \mathrm{Sel}^{(\alpha)}(A/k) \to Ш(A/k)[\alpha] \to 0 \tag{5.2}$$

This exact sequence is very interesting. The middle term, the Selmer group, turns out to be finite (and if fact computable) which proves weak Mordell-Weil theorem, and that $Ш(A/k)[\alpha]$ if finite. In particular, we see that $Ш(A,k)[n]$ is finite. Taking an element in the Selmer group and trying to determine whether it belongs to the weak-Mordell group or to the Tate-Shafarevich group, turns out to be a very difficult task. This is not very surprising, as checking whether an element belongs to Ш is equivalent to checking whether its corresponding principal homogeneous space possess a k-rational point, a known difficult task.

5.3 Proof of the finiteness of the Selmer group.

We keep the notation from the previous section. We will need several preliminary results for the proof:

Proposition 36 (Inflation-restriction sequence)**.** *Let H be a normal subgroup of G, A a G-module, and let $H^1(G/H, A^H) \overset{inf}{\to} H^1(G,A)$ be the map deduced from the quotient map $G \to G/H$ and the inclusion $A \to A^H$ (this map is called the inflation map). Then one has that*

$$0 \to H^1(G/H, A^H) \overset{inf}{\to} H^1(G,A) \overset{res}{\to} H^1(H,A)$$

is exact.

Proof. See [13, Appendix B], or [2, Proposition 3.3.14] □

Theorem 37. *Let A be an Abelian variety over a number field k, let ν be a finite place of k at which A has a good reduction, let $\tilde{k}$ be the residue field of ν, and let p be the characteristic of $\tilde{k}$. Then for any $m \geq 1$, not divisible by p the reduction map $A_m(k) \longrightarrow \tilde{A}(\tilde{k})$ is injective, where $A_m(k)$ is the m-torsion subgroup of $A(k)$.*

Proof. See [3, §C.2]. □

The finiteness of the Selmer group follows from the following finiteness theorem:

Theorem 38. *Let k be a number field such that μ_m, the m-roots of unity, are contained in k, and let S a finite set of places of k such that it contains all the places that divide m, and the ring of S-integers is a principal ideal domain (from the finiteness of the class group, the latter condition can always be achieved by enlarging S). Let l be the maximal Abelian extension of exponent m which is unramified outside S. Then l/k is a finite Galois extension.*

Proof. See [3, Corollary C.1.8]. □

We want to define when a cohomology class is unramified:

Definition 39. *Let ν be a place of a number field k, and let $I_\nu \subset G_k$ be an inertia for ν. A cohomology class $\phi \in H^1(G_k, M)$ is said to be* unramified at ν *if its restriction to $H^1(I_\nu, M)$ is trivial.*

Note that although I_ν is defined up to conjugation, the triviality of the restriction of ϕ is independent of the choice of I_ν. When S is a set of places, we denote by $H^1_S(G_k, A)$ the group of cohomology classes that are unramified outside S.

Proposition 40. *Let k be a number field such that $\mu_m \subset k$, G_k its absolute Galois group, let M be an Abelian group of exponent m. Then elements of $Hom(G_k, M)$ correspond to Abelian extensions of k of exponent m. If we think of M as a G_k module with the trivial action, elements of $H^1_S(G_k, M)$ correspond to Abelian extensions of k which are unramified outside S.*

Proof. See [3, Example C.5.2.1]. □

We can give the proof of the finiteness of the Selmer group.

Theorem 41. *1. Let M be a finite G_k-module and let S be a finite set of places of k. Then $H^1_S(G_k, M)$ is a finite group.*

2. Let $\alpha : A \to B$ be an isogeny of Abelian varieties, and let S be a finite set of places of k that contains:

(a) all Archimedean places;

(b) all places of bad reduction of A and B;

(c) all places dividing $deg(\alpha)$.

Then the Selmer group $Sel^{(\alpha)}(A/k)$ is contained in $H^1_S(G_k, ker(\alpha))$. In particular, it is finite.

Proof. (a) Let m be the exponent of M. As G_k acts continuously on M, we can find a Galois extension l/k such that $\mu_m \subset l$ and G_l acts trivially on M. By the inflation-restriction sequence (proposition 36) we have

$$0 \to H^1(\mathrm{Gal}(l/k), M^{\mathrm{Gal}(l/k)}) \xrightarrow{inf} H^1(G_k, M) \xrightarrow{res} H^1(G_l, M)$$

and as $H^1(\mathrm{Gal}(l/k), M^{\mathrm{Gal}(l/k)})$ is obviously finite, it is enough to show that $H^1(G_l, M)$ is finite, so we are reduced to the case where G_k acts trivially on M and $\mu_m \subset k$. In this case $H^1(G_k, M) = \mathrm{Hom}(G_k, M)$ and by proposition 40, elements of $\mathrm{Hom}(G_k, M)$ corresponds to Abelian extensions of k of exponent m, and it is easily seen that $H^1_S(G_k, M)$ corresponds to Abelian extensions of k of exponent m that are unramified outside S. By theorem 38 the maximal Abelian extension of k of exponent m that is unramified outside S is of finite degree so $H^1_S(G_k, M)$ is finite.
(b) Let $\phi \in \mathrm{Sel}^{(\alpha)}(A/k)$, and fix ν a finite place not in S. There exist $y \in A(\bar{k}_\nu)$ such that $\phi(\sigma) = \sigma y - y, \quad \forall \sigma \in G_k$. For σ in the inertia group of ν, I_ν, we denote by $\bar{x}$ reduction modulo ν of x and we the compute the reduction modulo ν of $\sigma y - y$:

$$\overline{\sigma y - y} = \overline{\sigma y} - \overline{y} = \overline{0}$$

since $\sigma \in I_\nu$. As $\sigma y - y \in \ker(\alpha)$, it is a torsion point of order that divides $\deg(\alpha)$ and since ν is outside S, we have that ν is a finite place of good reduction not dividing $\deg(\alpha)$ so by theorem 37 we have that $\sigma y - y = 0$, which shows that $\phi(\sigma) = 0$ for all $\sigma \in I_\nu$, so ϕ is unramified at ν. □

Chapter 6

An Approximation Theorem

The global nature of our characterization, is achieved by finding a set of global points on a smooth variety V/k, which will be dense in $V(k_\nu)$ for any place ν. The set of global rational points, $V(k)$, would certainly not work as it can be even empty. We will explain below that a finite extension l of k can be injected to k_ν in certain cases that depends on the arithmetic properties of of ν in l. In turns out, that if we take all the global points in such extensions, we get a dense set in $V(k_\nu)$ for the ν-adic topology, for all places ν. We begin by explaining basic facts and theorems about extension of valuations. One can find proofs of all these claims in [10, chapter II §8]. Let l/k be extension on number fields, let $\alpha \in l$ be a primitive element i.e., $k(\alpha) = l$ and let $f(X)$ be its minimal polynomial. Let ν be a place of k and let

$$f(X) = f_1(X) \cdots f_n(X)$$

be the decomposition of f into irreducible factors over k_ν. Note that $f_i(X)$ are distinct as k and k_ν are separable. All the k-embeddings of l in $\bar{k}_\nu$ are of the form $\alpha \mapsto \beta$ where β is some root of f in $\bar{k}_\nu$. Note that since $\bar{k}_\nu$ has a valuation $\bar{\nu}$, any k-embedding of l induces a valuation on l and therefore a place of l. Two embedding induce the same place if and only if the arise by sending α to roots of the same irreducible factor $f_i(X)$. Therefore, for each irreducible factor f_i corresponds a place ω of l, and a completion l_ω. If f_i corresponds to ω, we have

$$l_\omega \cong k_\nu[X]/f_i(X).$$

Therefore if k_ν contains a root of $f(X)$ then we get a linear factor in the decomposition of f, and if ω is the place that corresponds to it, we have that $l_\omega \cong k_\nu$ and in particular we have an injection of l into k_ν. Such place ω is said to be a split place above ν.

We are now ready to formulate an approximation theorem:

Theorem 42. *Let A be an Abelian variety over k, and let ν be a place of k. We define T to be the union of $A(l)$ where l has some split place above ν (the proof will show that we can even assume that ν totally splits in l), and therefore an embedding of l in k_ν, which gives an embedding of $A(l)$ in $A(k_\nu)$. Using these embeddings we have a map from T to $A(k_\nu)$. The image of T in $A(k_\nu)$ is dense in the ν-adic topology.*

Proof. This result is proved in [8] where it is formulated in much more general settings which we explain shortly. Consider the following data:

1. A surjective separated map $f : X \to B := \mathrm{Spec}(R)$ where B is the ring of S-integer of a global field k, and S is finite, non-empty set of places of k that contains all the Archimedean ones.

2. A proper non-empty subset Σ of S (in particular, this theorem does not apply to the case when S has only one element), such that $\Sigma \cup \mathrm{Max}(R)$ is not all the places of k, where $\mathrm{Max}(R)$ is the set of the maximal ideals of B.

3. For all $\nu \in \Sigma$, we are given Galois extensions l_ν/k_ν and $\mathrm{Gal}(l_\nu/k_\nu)$-stable open subsets $\Omega_\nu \subset X_k(l_\nu)$ (in the ν-adic topology) of smooth points.

In [8], the data $(f : X \to \mathrm{Spec}(B), \Sigma, l_\nu/k_\nu, \Omega_\nu)$ is called Skolem Data. The main theorem of [8] claim that given Skolem data, there exist a closed subscheme $Y \to X$, finite over B, such that all the closed point of $Y_k \times_k l_\nu$ are l_ν-rational, and $Y(l_\nu) \subset \Omega_\nu$.
As an easy corollary, we apply this result to an Abelian variety A over k. We know that A is smooth and admits a model[1] over some ring of S-integers of k, where we can add places to S if needed (see [9, Appendix II lemma 1] for a proof of the existence of such model). We fix a set of places Σ, and choose S to properly contain Σ and all the Archimedean places and such that we have a model of A over the ring of S-integers. We set $l_\nu = k_\nu$ for all $\nu \in \Sigma$ and we get Skolem data for any open sets Ω_ν (as $\mathrm{Gal}(l_\nu/k_\nu)$ is a trivial extension). From the result stated above, we easily get that if we let k^Σ be the maximal extension of k in which all $\nu \in \Sigma$ are totally split, then $A(k^\Sigma)$ is dense in $A(k_\nu)$ for all $\nu \in \Sigma$. □

[1] A model of A, is a scheme $\mathcal{A}$ with a surjective map to $f : \mathcal{A} \to \mathrm{Spec(R)}$ where R is a ring of S-integers of k, such that the generic fiber of f, is isomorphic to A.

Chapter 7

A Characterization of the Tate-Shafarevich Group

7.1 A Geometric property of elements in Ш

As always, A denotes an Abelian variety over k. For each place ν of k, we denote by k_ν the corresponding completion, and let $G_\nu := G_{k_\nu} := Gal(\bar{k}_\nu/k_\nu)$. As we explained before, we have $G_\nu \hookrightarrow G_k$ and therefore a functorial restriction $res^i_\nu : H^r(G_k, A) \to H^r(G_\nu, A)$.
When one considers extension of A by $\mathbb{G}_m$ when trying to investigate a local-to-global problems, it is natural to apply the restriction maps to an extension X of A by $\mathbb{G}_m$,

$$0 \to \mathbb{G}_m \to X \xrightarrow{\pi} A \to 0.$$

We use Hilbert's theorem 90 (see example 14) and we take the product over all places ν of k to obtain:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(k,X) & \xrightarrow{\pi^1} & H^1(k,A) & \xrightarrow{\delta} & H^2(k,\mathbb{G}_m) \\ & & \downarrow{\scriptstyle \prod_\nu res^1_\nu} & & \downarrow{\scriptstyle \prod_\nu res^1_\nu} & & \downarrow{\scriptstyle \prod_\nu res^2_\nu} \\ 0 & \longrightarrow & \prod_\nu H^1(k_\nu,X) & \xrightarrow{\prod_\nu \pi^1_\nu} & \prod_\nu H^1(k_\nu,A) & \xrightarrow{\delta_\nu} & \prod_\nu H^2(k_\nu,\mathbb{G}_m). \end{array}$$

Examining this 'local-to-global' diagram we note few things: the first is that Brauer-Hasse-Noether theorem asserts that $\prod_\nu res^2_\nu$ satisfies the local-to-global principle, i.e., it is injective, and the second is that an element $\alpha \in H^1(k, A)$ belongs to $Ш(k, A)$ if and only if it is in the kernel of the middle arrow $\prod_\nu res^1_\nu$.
Using the exactness of the rows and the last two remarks, we see that if $\alpha \in H^1(k, A)$ belongs to $Ш(k, A)$ its image in $\prod_\nu H^2(k_\nu, \mathbb{G}_m)$ is necessarily

zero and therefore its image in $H^2(k,\mathbb{G}_m)$ is already zero, and by the exactness of the top row it is in the image of $H^1(k,X) \xrightarrow{\pi^1} H^1(k,A)$, which is a 'global' property that admits an interesting geometric description: given a principal homogeneous space A' for A, one can ask whether it can be lifted to a principal homogeneous space X' for X. This means that we look for a principal homogeneous space X' for X, on which $\mathbb{G}_m$ acts naturally (as it is a subgroup of X), and if we divide by this action of $\mathbb{G}_m$, we get a space on which $X/\mathbb{G}_m \overset{\Psi}{\cong} A$ acts, and we want this space to be isomorphic to A' as a principal homogeneous space for A (when one think of A via Ψ). We claim that

Proposition 43. *Given an extension* $0 \to \mathbb{G}_m \to X \xrightarrow{\pi} A \to 0$, *and a principal homogeneous space* A' *for* A *one can lift* A' *to a principal homogeneous space* X' *for* X *if and only if the class* $[A'] \in H^1(k,A)$ *is in the image of* $\pi^1 : H^1(k,X) \to H^1(k,A)$.

As a corollary we formulate again the result we showed before

Corollary 44. *Given an element* $\alpha \in Ш(k,A)$, *and principal homogeneous space for* A, A' *with* $[A'] = \alpha$, A' *can be lifted to a principal homogeneous space for* X' *for any extension* $0 \to \mathbb{G}_m \to X \xrightarrow{\pi} A \to 0$.

Note that the lifting property is for a global object and being in Ш is a property that is related to all the localizations. We wish to characterize elements of Ш with this lifting property and to keep its global nature. The problem that we are facing it that we have $\alpha \in H^1(k,A)$ and we wish to connect the lifting property to showing that $\alpha_\nu := res^1_\nu(\alpha)$ is trivial. As α_ν is over a locally compact field, we can use Tate-duality to show that it is trivial. It turns out that we can give a cohomological description of the Tate pairing which is closely linked to this lifting property and extensions of A by $\mathbb{G}_m$. This description will be the main ingredient in our characterization.

7.2 Cohomological expression of Tate's pairing

We recall the notation from chapter 3. F denotes some locally compact field and we wish to calculate the pairing of $a \in A^\vee(F)$ and $\alpha \in H^1(k,A)$. We took n such that $\alpha \in H^1(k,A)[n]$ and we chose $a' \in A(\bar{F})$ such that $na' = a$. We denoted by D' a Cartier divisor such that $a' = [D']$ and defined $D := nD'$. Therefore $[D] = a$. We denoted $D'_\sigma = \sigma D' - D'$, and we chose $h_\sigma, g_\sigma \in \bar{F}(A)$ such that $(h_\sigma) = nD'_\sigma$ and $n_A^* D'_\sigma = (g_\sigma)$(see section 1.4 for an explanation why these divisors are principal). We let

$$0 \to \mathbb{G}_m \to X_a \xrightarrow{\pi_a} A \to 0$$

be the extension of A by $\mathbb{G}_m$ that corresponds to a. Using the Galois cohomology of the this short exact sequence, we have another way to calculate the Tate pairing; Indeed, taking cohomology of this exact sequence we get a coboundary map

$$\delta_a : H^1(F, A) \to H^2(F, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$$

where the last isomorphism is the invariant map from local class field theory. If we denote the pairing we defined in chapter 3 by $(,)$, we have

Theorem 45. *With this notation,* $(a, \alpha) = \delta_a(\alpha)^{-1}$.

Proof. We've seen in section 4.4, that a generic (that is, on a dense open subset) explicit description of X_a as G_F-module is given by:

- $X_a(\bar{F}) = \mathbb{G}_m(F) \times A(F)$
- The multiplication rule on X_a is given by

  $$(t_1, u_1) * (t_2, u_2) = (t_1 t_2 f(u_1, u_2), u_1 + u_2)$$

  where $(f) = \Lambda(D)$ and we write the group law on A additively and on $\mathbb{G}_m$ multiplicatively.
- $(t, u)^{-1} = (t^{-1} f(u, -u)^{-1}, -u)$.
- If $\sigma \in G_F$ then

  $$\sigma(t, u) = (\sigma(t) h_\sigma(\sigma u)^{-1}, \sigma u)$$

We take the rational section for A to X_a by $p \mapsto (1, p)$, then by the definition of the coboundary maps we have that

$$\delta_a(\alpha)(\sigma, \tau) = \sigma(1, \alpha(\tau)) - (1, \alpha(\sigma\tau)) + (1, \alpha(\sigma))$$

where we used the fact that $(1, u) \in \pi_a^{-1}(u)$ and that we can choose any preimage for the calculation. Note that this should be an element of $\mathbb{G}_m$ as we will shortly see.
Denote $\gamma := \delta_a(\alpha)$ and we calculate :

$$\gamma(\sigma, \tau) = \sigma(1, \alpha(\tau)) - (1, \alpha(\sigma\tau)) + (1, \alpha(\sigma)) = (h_\sigma(\sigma\alpha(\tau))^{-1}, \sigma\alpha(\tau)) - (1, \alpha(\sigma\tau)) + (1, \alpha(\sigma))$$

To ease notation let $H := h_\sigma(\sigma\alpha(\tau))^{-1}$, $x := \sigma\alpha(\tau)$ and $y := \alpha(\sigma)$ and since α is a cocycle we have that $x + y = \sigma(\alpha(\tau)) + \alpha(\sigma) = \alpha(\sigma\tau)$. With these notations

$$\gamma(\sigma, \tau) = (H, x) - (1, x + y) + (1, y) = (H, x) + (1, y) - (1, x + y) =$$
$$= (Hf(x, y), x + y) + (f(x + y, -(x + y))^{-1}, -(x + y)) =$$
$$= \left(\frac{Hf(x, y) f(x + y, -(x + y))}{f(x + y, -(x + y))}, 0 \right)$$

Canceling alike terms and identifying $\mathbb{G}_m$ as a subgroup of X_a we get

$$\boxed{\gamma(\sigma,\tau) = Hf(x,y) = h_\sigma(\sigma\alpha(\tau))^{-1} f(\sigma\alpha(\tau),\alpha(\sigma))}$$

We will now show that $\gamma^{-1} \sim \zeta$ ($\sim$ means that they differ by a coboundary) where we showed that $\zeta(\sigma,\tau) = g_\sigma(\sigma\alpha(\tau))$ in section 3.2. In order to do that we need to compare f to g_σ and h_σ.
We choose $f' \in F(A \times A)$ such that $\Lambda(D') = (f')$ and $f'(0,0) = 1$ (we can normilize it as we already explain before why $0 \notin Supp(D')$ and therefore $(0,0) \notin Supp(\Lambda(D'))$). We let $f := (f')^n$. Note that $(f) = \Lambda(D)$ and if we denote ${}^\sigma f := \sigma \circ f \circ \sigma^{-1}$ we have $({}^\sigma f) = \sigma(f)$.
Comparing divisors and using our normalizations, we have

$$\frac{{}^\sigma f}{f} = \frac{h_\sigma \circ m_A}{(h_\sigma \circ p)(h_\sigma \circ q)}$$

or

$$\frac{{}^\sigma f(x,y)}{f(x,y)} = \frac{h_\sigma(x+y)}{h_\sigma(x)h_\sigma(y)}$$

Similiarly, since $n_A^*(\sigma D' - D') = (g_\sigma)$ we have

$$\frac{{}^\sigma f'}{f'} \circ n_A = \frac{g_\sigma(x+y)}{g_\sigma(x)g_\sigma(y)}$$

Now, since n_A is onto, we choose u such that $nu = \sigma\alpha(\tau)$. Note that

$$\prod_{i=1}^{n} \frac{g_\sigma(iu)}{g_\sigma((i-1)u)g_\sigma(u)} = \frac{g_\sigma(nu)}{g_\sigma(0_A)g_\sigma(u)^n} = \frac{g_\sigma(\sigma\alpha(\tau))}{h_\sigma(nu)} = \frac{g_\sigma(\sigma\alpha(\tau))}{h_\sigma(\sigma\alpha(\tau))}$$

Thus, using that $\zeta(\sigma,\tau) = g_\sigma(\sigma\alpha(\tau))$, we have

$$h_\sigma(\sigma\alpha(\tau))^{-1}\zeta(\sigma,\tau) = \prod_{i=1}^{n} \frac{g_\sigma(iu)}{g_\sigma((i-1)u)g_\sigma(u)} = \prod_{i=1}^{n} \frac{{}^\sigma f'((i-1)\sigma\alpha(\tau),\sigma\alpha(\tau))}{f'((i-1)\sigma\alpha(\tau),\sigma\alpha(\tau))}$$

$$= \prod_{i=1}^{n} \frac{\sigma f'((i-1)\alpha(\tau),\alpha(\tau))}{f'((i-1)\sigma\alpha(\tau),\sigma\alpha(\tau))}$$

and changing every term by the coboundary of $w_i(*) = f'((i-1)\alpha(*),\alpha(*))$ we see that the last line is cohomologous to

$$= \prod_{i=1}^{n} \frac{f'((i-1)\alpha(\sigma\tau),\alpha(\sigma\tau))}{f'((i-1)\alpha(\sigma),\alpha(\sigma))f'((i-1)\sigma\alpha(\tau),\sigma\alpha(\tau))} =$$

We now prove a lemma that will help us show that

$$= \frac{1}{f'(\sigma\alpha(\tau),\alpha(\sigma))^n}$$

Lemma 46. *Let $(A,+),(G,\cdot)$ be groups and if $\phi : A \times A \to G$ satisfy*

1. *$\phi(a,b) = \phi(b,a)$, for all $a,b \in A$,*
2. *$\phi(a,b)\phi(a+b,c) = \phi(a,b+c)\phi(b,c)$, for all $a,b,c \in A$,*
3. *$\phi(0,a) = 1$, for all $a \in A$,*

Then for all $x,y \in A$ and for all $m \in \mathbb{N}$ we have

$$\prod_{i=1}^{m} \frac{\phi((i-1)(x+y),x+y)\phi(x,y)}{\phi((i-1)x,x)\phi((i-1)y,y)} = \phi(mx,my)$$

Proof. We prove it by induction on m. We have

$$\prod_{i=1}^{m+1} \frac{\phi((i-1)(x+y),x+y)\phi(x,y)}{\phi((i-1)x,x)\phi((i-1)y,y)} =$$

$$= \prod_{i=1}^{m} \frac{\phi((i-1)(x+y),x+y)\phi(x,y)}{\phi((i-1)x,x)\phi((i-1)y,y)} \cdot \frac{\phi(mx+my,x+y)\phi(x,y)}{\phi(mx,x)\phi(my,y)} =$$

$$= \frac{\phi(mx,my)\phi(mx+my,x+y)\phi(x,y)}{\phi(mx,x)\phi(my,y)} =$$

where the last equality follows by induction. Now, using the second identity with $a = mx, b = my, c = x+y$ we get

$$\phi(mx,my)\phi(mx+my,x+y) = \phi(mx,x+(m+1)y)\phi(my,x+y)$$

and therefore

$$= \frac{\phi(mx,x+(m+1)y)\phi(my,x+y)\phi(x,y)}{\phi(mx,x)\phi(my,y)}$$

using again the second identity this time with $a = x, b = y, c = my$ we get

$$\phi(my,x+y)\phi(x,y) = \phi(x,(m+1)y)\phi(y,my)$$

and therefore

$$= \frac{\phi(mx,x+(m+1)y)\phi(x,(m+1)y)\phi(y,my)}{\phi(mx,x)\phi(my,y)}$$

using again the second identity this time with $a = (m+1)y, b = x, c = mx$ we get

$$\phi(mx,x+(m+1)y)\phi(x,(m+1)y) = \phi((m+1)y,(m+1)x)\phi(x,mx)$$

and therefore

$$= \frac{\phi((m+1)y,(m+1)x)\phi(x,mx)\phi(y,my)}{\phi(mx,x)\phi(my,y)} = \phi((m+1)y,(m+1)x).$$

□

We use this lemma with $\phi = f'$, $x := \sigma\alpha(\tau)$ and $y := \alpha(\sigma)$ and since α is a cocycle we have that $x + y = \sigma(\alpha(\tau)) + \alpha(\sigma) = \alpha(\sigma\tau)$. We already explained in the proof of theorem why f' satisfies the three identities of the lemma, and it is also very easy to see it directly using the facts both sides have the same divisor and they agree on $x = y = 0$. Thus, in this notation, we see the last term in the calculation above above is equal to

$$\prod_{i=1}^{n} \frac{f'((i-1)(x+y), x+y)}{f'((i-1)x, x)f'((i-1)y, y)}$$

and by the lemma is is equal to

$$= \frac{f'(nx, ny)}{f'(x, y)^n} = \frac{1}{f(x, y)^n}.$$

since in our case $nx = ny = 0$ and $(f')^n = f$.
We conclude that

$$\zeta(\sigma, \tau) = h_\sigma(\sigma\alpha(\tau))f(\sigma\alpha(\tau), \alpha(\sigma))^{-1} = \gamma(\sigma, \tau)^{-1}$$

Thus, as elements of $H^2(F, \mathbb{G}_m)$,

$$\boxed{[\zeta] = [\gamma]^{-1}}$$

□

7.3 The characterization

We fix element $\alpha \in H^1(k, A)$. Extensions of A by $\mathbb{G}_m$ corresponds to elements of $A^\vee(k)$, and we already showed that if α is in $Ш(k, A)$ then it can be lifted to any extension of A by $\mathbb{G}_m$ and in particular to the ones that corresponds to $A^\vee(k)$. It is obvious that this property will not suffice to characterize the fact that α belongs to Ш as $A^\vee(k)$ can be very small (it can consist only from $0_{A^\vee}$ which corresponds to the trivial extension). It is surprising, though, that if we check this lifting property for α against element of $A^\vee(l)$ where l is finite extensions of k, it *does* follows that α belongs to $Ш(k, A)$. Note that these are *global* conditions.
Before proving this characterization, we fix some notations and language. Note that elements in $A^\vee(l)$ corresponds to extensions of the base extension $A_l := A \times_{\mathrm{Spec}(k)} \mathrm{Spec}(l)$ by $\mathbb{G}_{m,l}$. For $b \in A^\vee(l)$ we say that $\alpha \in H^1(k, A)$ can be b-lifted if $res^l_k(\alpha)$ can be lifted with respect to the short exact sequence that corresponds to[1] b,

$$0 \longrightarrow \mathbb{G}_{m,l} \longrightarrow X_b \xrightarrow{\pi_b} A_l \longrightarrow 0.$$

[1] res^l_k comes from $G_l \subset G_k$

This still has the same geometric description: let A_α be a principal homogeneous space that satisfies $[A_\alpha] = \alpha$. Base extension to l of the action morphism $A \times A_\alpha \to A_\alpha$ gives $(A_\alpha)_l$ a structure of a principal homogeneous space of A_l and it satisfy that $[(A_\alpha)_l] = res^l_k(\alpha)$ (which may certainly by trivial). Having said this, geometric description of the b-lifting property is the same as before. We already showed that if α is in $Ш(k, A)$ then it can be lifted for any extension of A by $\mathbb{G}_m$ over k and we can do the same argument using $H^i(l, *)$ instead of $H^i(k, *)$ and we get that if $\alpha \in Ш(k, A)$ it can be b-lifted for any extensions over l, i.e., for $b \in A^\vee(l)$.

We now can formulate our criterion:

Theorem 47. *For $\alpha \in H^1(k, A)$ we have $\alpha \in Ш(k, A)$ if and only if for all finite extension l/k and for all element of $b \in Pic^0(A)(l)$, α can be b-lifted, where l/k is a finite field extension.*

Proof. Corollary 44 and the remark above shows that this criterion is necessary. For the converse, fix $\alpha \in H^1(k, A)$ that satisfies our condition. Fix some discrete valuation ν and let α_ν denote the restriction of α under $H^1(k, A) \to H^1(k_\nu, A)$. We wish to show that α_ν is zero. By Tate duality (theorem 24) we have

$$\alpha_\nu = 0 \Leftrightarrow (a', \alpha_\nu) = 0 \quad \forall a' \in A^\vee(k_\nu).$$

From the cohomological description of the pairing (theorem 45), we have the important observation that $(a', \alpha_\nu) = 0$ if and only if α_ν can be a'-lifted, which follows from the fact that the long sequence of cohomology is exact. From this it follows that $\alpha_v = 0$ if α_ν can be a'-lifted for all $a' \in A^\vee(k_\nu)$. If this lifting property would be true for the points in $A^\vee(k_\nu)$ for all places ν, then it will follows that $\alpha \in Ш(k, A)$. But this condition is of local nature as points $a \in A^\vee(k_\nu)$ are local objects. To make it a global criterion, we use the continuity of the Tate pairing to approximate local point by global points. In theorem 42 we found a set T that is dense in $A(k_\nu)$, and therefore we fix arbitrary $a' \in T$ and let l/k be a finite extension such that $a' \in A'(l)$. Look at the following diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(l, X_{a'}) & \xrightarrow{\pi} & H^1(l, A_l) & \xrightarrow{\delta} & H^2(l, \mathbb{G}_m) \\ & & \downarrow f & & \downarrow g & & \downarrow \\ 0 & \longrightarrow & H^1(k_\nu, X_{a'}) & \xrightarrow{\pi_v} & H^1(k_\nu, A) & \xrightarrow{\delta_\nu} & H^2(k_\nu, \mathbb{G}_m) \end{array}$$

where the vertical arrows are the restriction morphisms that come from the injection of $l \to k_\nu$ that corresponds to a prime of l that splits over ν. We denote them by f and g to ease notation.
Since the injection $k \to k_\nu$ factor as $k \to l \to k_\nu$, $H^1(k, A) \to H^1(k_\nu, A)$

factors through $H^1(l, A_l)$, and we let α_l denote the image of α in $H^1(l, A_l)$. By our assumption there exist $b \in H^1(l, X_{a'})$ such that $\pi(b) = \alpha_l$, and by the commutativity of the diagram $\pi_v(f(b)) = g(\alpha_l) = \alpha_\nu$ and by the exactness of the second row we get that $\delta_v(\alpha_\nu) = 0$. Therefore, $(a', \alpha_\nu) = 0$. As $a' \in T$ was arbitrary, and T is dense, we get by continuity that $\alpha_\nu = 0$. As this argument as true for all places ν, we have that $\alpha \in Ш(K, A)$. □

Bibliography

[1] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons Inc., Hoboken, NJ, 2004.

[2] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006.

[3] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction.

[4] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[5] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[6] J.S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, 2006.

[7] Ieke Moerdijk, *Notes on homological algebra*, Online notes, 2006.

[8] Laurent Moret-Bailly, *Groupes de Picard et problèmes de Skolem. II*, Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 2, 161–179, 181–194.

[9] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[10] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[11] Peter Roquette, *The Brauer-Hasse-Noether theorem in historical perspective*, Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences], vol. 15, Springer-Verlag, Berlin, 2005.

[12] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French.

[13] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[14] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979. MR MR547117 (82e:14003)

[15] André Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524.