MINISTRY OF EDUCATION AND TRAINING

VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY

GRADUATE UNIVERSITY OF SCIENCE AND TECHNLOGY

Nguyen Quang Khai

ON THE ORDER OF REDUCTION OF RATIONAL POINTS ON ALGEBRAIC GROUPS

MASTER THESIS IN MATHEMATICS

Ha Noi - 2022

MINISTRY OF EDUCATION AND TRAINING

VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY

GRADUATE UNIVERSITY OF SCIENCE AND TECHNLOGY

Nguyen Quang Khai

ON THE ORDER OF REDUCTION OF RATIONAL POINTS ON ALGEBRAIC GROUPS

Major : Algebra and Number Theory
Code : 8 46 01 04

MASTER THESIS IN MATHEMATICS

SUPERVISOR :
Prof. Dr. Nguyen Quoc Thang

Ha Noi - 2022

Declaration

I declare that this thesis titled "On The Order Of The Reduction Of Rational Points On Algebraic Groups" has been composed solely by myself and it has not been previously included in a thesis or dissertation submitted for a degree or any other qualification at this graduate university or any other institution. Wherever the works of others are involved, every effort is made to indicate this clearly, with due reference to the literature. I will take responsibility for the above declaration.

Hanoi, 30th September 2022

Signature of Student

Nguyen Quang Khai

Acknowledgements

First and foremost, I would like to express my deepest gratitude to Professor Nguyen Quoc Thang for his support and encouragement throughout the two past years, and his advice and guidance on the topic of my thesis. My fascination with number theory, and its interaction with algebraic groups, has been expanded by him.

I am grateful to Professor Phung Ho Hai for his help and guidance, especially in my early years learning algebraic geometry. His lectures and seminars on algebraic geometry play a key role in my algebraic geometry knowledge.

I am thankful to the Graduate University of Science and Technology and the Institute of Mathematics for giving me a chance to study and work here. Learning mathematics there helps me to meet more mathematicians and friends who share the same interests. Participating in seminars and lectures there always motivates me to understand and study more mathematics.

I would like to express my gratitude towards mathematicians in the Institute of Mathematics who always do not hesitate to answer my silly questions and encourage me to pursue advanced mathematics.

I would like to thank my roommates, Vo Quoc Bao and Nguyen Khanh Hung, for the many fun discussions on every aspect of mathematics and life. Exchanging mathematics ideas with them always amazes me and helps me a lot in understanding mathematics.

Finally, I am indebted to my family, for their support throughout my academic study.

This work is funded by International Center for Research and Postgraduate Training in Mathematics Under the auspices of Unesco, grant ICRTM03_2020.06, and supported by the Domestic Master Scholarship Programme of Vingroup Innovation Foundation, Vingroup Big Data Institute, grant VINIF.2021.ThS.05.

Contents

List of Tables

Introduction

The present thesis is motivated by the following classical result of Schinzel and Postnikova in 1968, see the main theorem in [1].

Theorem 0.0.1. *Let a and b be relatively prime nonzero integers of a number field K for which $\frac{a}{b}$ is not a root of unity. Then there exists a constant $n(a,b)$ such that for all $n > n(a,b)$, the number $a^n - b^n$ has a primitive divisor.*

Here, a primitive divisor of $a^n - b^n$ is a prime ideal $\mathfrak{p}$ such that n is the smallest integer in the set of positive integers h satisfying $\mathfrak{p}|a^h - b^h$. In other words, n is the order of the reduction modulo $\mathfrak{p}$ of the non-torsion point $\frac{a}{b} \in \mathbb{G}_m(K)$. The proof is based on some estimates of the orders of $a^n - b^n$ modulo prime ideals and an approximation theorem of Gel'fond. This theorem gives us some information about the reduction of non-torsion rational points on the multiplicative group $\mathbb{G}_m$ over K. Passing to elliptic curves, S. Hahn and J. Cheon also obtained a similar result (see [2])

Theorem 0.0.2. *Let $P \in E(K)$ be a point of infinite order on an elliptic curve E over a number field K. Then there exists an integer N such that for every $n > N$, there exists a prime $\mathfrak{p}$ of good reduction of E so that the order of P modulo $\mathfrak{p}$ is equal to n. Moreover, for all P, except finitely many points, there exists such a prime $\mathfrak{p}$ for all positive integer n.*

As usual, when working with rational points on elliptic curves, one needs height function machinery. Using height functions, the idea of the elliptic curve proof is similar to the classical case. In this thesis, we prove a global function field version for above theorems for one-dimensional tori and elliptic curves. In the case of the one-dimensional tori over global function fields, we first give proof of the case of multiplicative groups, and, using reductions, we deduce the one-dimensional torus case. In the case of elliptic curves over number fields, height functions work well; however, we need some auxiliary results when passing to the function field cases. Therefore, we need to treat carefully calculations involving the characteristic of the base field. Precisely, we need some estimates for height functions over function fields of H. Zimmer in [3] and Roth's theorem in positive characteristics which is proven in [4] by J.V.Armitage. In addition, A. Perucca in her thesis [5] has proven the following theorem

Theorem 0.0.3. *Let G be a product of a torus and an abelian variety over a number field K, and L a finite extension of K. Let $P \in G(L)$ be such that G_P is connected,*

and m is some fixed non-zero integer. Then there exists a set of primes $\mathfrak{p}$ of K whose Dirichlet density is positive satisfying the following: any prime $\mathfrak{q}$ of L over $\mathfrak{p}$ satisfies the order of P modulo $\mathfrak{q}$ is prime to m.

Here, G_P is the Zariski closure of $\mathbb{Z}P$, the group generated by P, in $G_L := G \times_K L$. When $L = K$ and G is a product of an elliptic curve and $\mathbb{G}_m$, we note that Theorems 0.0.1 and 0.0.2 give us infinitely many places $\mathfrak{p}$ satisfying the order of P modulo $\mathfrak{p}$ is prime to m, but this theorem tells us more, the Dirichlet density of such places is positive. At the end of the thesis, we recall the Kummer theory after Ribet and apply it to give proof of this result due to A. Perucca. Finally, we propose some open questions.

Chapter 1

Algebraic Groups and Reductions

The main references for this chapter are [5], [6], [7], [8], and [9]. This chapter contains five following sections

1. Global Fields.
2. Algebraic Groups.
3. Integral Models of Algebraic Groups.
4. Reduction of Algebraic Groups.
5. Formal Groups.

1.1 Global Fields

Because we will work with global fields most of the time, I start the thesis with some properties of global fields.

Definition 1.1.1. By **global field** we mean a number field (i.e., a finite extension of the field of rational numbers $\mathbb{Q}$), or a global function field (i.e., a finite extension of the field $\mathbb{F}_q(t)$ for a variable t and a finite field $\mathbb{F}_q$).

We denote $\mathbb{F}$ the base field $\mathbb{Q}$ or $\mathbb{F}_q(t)$. For a field K, denote by K^s its separable extension and $\Gamma := \mathrm{Gal}(K^s/K)$ its absolute Galois group.

Example 1.1. $\mathbb{F}_4(t)$ and $\mathbb{Q}(\sqrt{2})$ are global fields.

- $M_{\mathbb{Q}} = \{\text{primes } p\} \cup |\cdot|$ where $|\cdot|$ is the usual absolute value.
- $M_{\mathbb{F}_q(t)}$ is the set of irreducible monic polynomials and $\frac{1}{t}$. In addition, those places induce normalized absolute values as follows:
  (a) $|x|_p := p^{-\operatorname{ord}_p(x)}$ for $x \in \mathbb{Q}^\times$ and prime number p, and
  (b) $|x|_f := q^{-\operatorname{ord}_f(x).\deg f}$ for $x \in \mathbb{F}_q(t)^\times$ and $f \in M_{\mathbb{F}_q(t)}$.

These two kinds of global fields share a lot of common behaviours. A global field K admits a set of non-trivial non-equivalent normalized places (absolute values) M_K. We let $\mathcal{O}_K$ to be the **ring of integers** in K, i.e., the integral closure of $\mathbb{Z}$ or $\mathbb{F}_q[t]$ in K. Now, for S a set of finitely many places in K (we always assume that S contains all Archimedean places), we denote $\mathcal{O}_{K,S} := \mathcal{O}_S := \{x \in K : v(x) \geqslant 0, \forall x \notin S\}$ the **ring of $S-$integer**, $\mathcal{O}_{K,S}^\times := \mathcal{O}_S^\times = \{x \in K : v(x) = 0, \forall x \notin S\}$ the **group of $S-$units**, and $\mathcal{O}_{K,v} := \mathcal{O}_v := \{x \in K^\times : v(x) \geqslant 0\}$ the valuation ring correspond to non-Archimedean place v . We denote $\mathfrak{p}_v$ the maximal ideal in $\mathcal{O}_v$, and $\mathrm{ord}_v(x) := \mathrm{ord}_{\mathfrak{p}_v}(x)$. For a place v of K over p of $\mathbb{Q}$ (or f of $\mathbb{F}_q(t)$), we denote K_v the completion of K at v and $N_v := [K_v : \mathbb{Q}_p]$ (or $[K_v : \mathbb{F}_q(t)_f]$). The number N_v is called the **local degree** at v.

To simplify, we work with normalized absolute values, i.e., we have (see [10] Proposition 2.1)

- $|x|_v = |x|^{N_v}$ if v is Archimedean,
- $|x|_v = (1/\mathbb{N}v)^{\mathrm{ord}_v x}$ for every non-Archimedean place v of a number field, where $\mathbb{N}v := \#\mathcal{O}_v/\mathfrak{p}_v$, and
- $|x|_v = (1/q)^{\mathrm{ord}_v x. \deg v}$ for every place v of a global function field. Here, the degree of v, $\deg(v)$ is defined to be the degree $[\mathcal{O}_v/\mathfrak{p}_v : \mathbb{F}_q]$ when K is a global function field.

We note that those normalized absolute values satisfy

- (P) The product formula: for any $x \in K \setminus \{0\}$

$$\prod_{v \in M_K} |x|_v = 1;$$

- (F) The finiteness property: for any $x \in K \setminus \{0\}$, for all but finitely many v, $|x|_v = 1$.

For $v \in M_K$ a non-Archimedean place, its associated valuation $v(.)$ on $K^\times$ is defined to be $-\log|.|_v$ in the number field case, and $-\log_q|.|_v = \mathrm{ord}_v(.).\deg v$ in the global function field case.

Definition 1.1.2. We denote $\mathrm{Div}(K)$ the **divisor group** that is the free abelian group generated by places of K. It means that a divisor is a formal sum

$$D = \sum_v n_v.v \text{ with } n_v \in \mathbb{Z}, \text{ and almost } n_v = 0.$$

Such D is called a **prime divisor** if D is of the form $D = v$ for some $v \in M_K$. D is **principal** if it is of the form

$$(x) = \sum_v \mathrm{ord}_v(x).v \text{ for some } x \in K^\times.$$

Similarly, for the set S as above, the **group of $S-$divisors**, $\mathrm{Div}_S(K)$, is the subgroup of $\mathrm{Div}(K)$ generated by primes not in S. A divisor is called $S-$principal if it is of the form

$$(x)_S := \sum_{v \notin S} \mathrm{ord}_v(x).v \text{ for some } x \in K^\times.$$

We denote $\mathrm{Prin}(K)$ (resp. $\mathrm{Prin}_S(K)$) the **group of principal divisors** (resp. **$S-$principal divisors**). The quotients $\mathrm{Cl}(K) := \mathrm{Div}(K)/\mathrm{Prin}(K)$, and $\mathrm{Cl}_S(K) := \mathrm{Div}_S(K)/\mathrm{Prin}_S(K)$ are called the **class group**, and **$S-$class group** respectively.

For L a Galois extension of K, and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$, we let $\mathfrak{q}$ be a prime ideal of L above $\mathfrak{p}$, then we define the **decomposition group**

$$D(\mathfrak{q}|\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

and the **inertia group**

$$I(\mathfrak{q}|\mathfrak{p}) := \{\sigma \in D(\mathfrak{q}|\mathfrak{p}) : \sigma(x) \equiv x \bmod \mathfrak{q}, \forall x \in \mathcal{O}_L\}.$$

Definition 1.1.3. The prime $\mathfrak{p}$ is **unramified** over L if $I(\mathfrak{q}|\mathfrak{p}) = 1$ for some $\mathfrak{q}|\mathfrak{p}$ (and hence for all $\mathfrak{q}$).

The following important theorem will be used later.

Theorem 1.1.4. *(Chebotarev's density theorem) Let K be a global field, L a finite Galois extension of K, and $\mathcal{C}$ a conjugacy class in $\mathrm{Gal}(L/K)$. Then the Dirichlet density of the set of unramified (in L) primes $\mathfrak{p}$ of K whose Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right) = \mathcal{C}$ equals $\frac{|\mathcal{C}|}{[L:K]}$.*

Proof. We refer to [11] Theorem 6.3.1. □

Number Fields

For number fields K, there are some well known finiteness theorems, see [12] Theorem 7.4, Corollary 11.7 and 11.8.

Theorem 1.1.5. *1. (Dirichlet unit theorem) The group $\mathcal{O}_K^\times$ is isomorphic to $\mu(K) \times \mathbb{Z}^{r_1+r_2-1}$ where $\mu(K)$ is the group of roots of unity in K, r_1 and $2r_2$ are the number of real places, and complex places of K, respectively. In particular, $\mathcal{O}_K^\times$ is finitely generated.*

2. *(Dirichlet $S-$unit theorem) The group of S-units is finitely generated, with rank equal to $r+s$, where r is the rank of the unit group and $s=|S|$.*

3. *The groups* $\mathrm{Cl}(K)$ *and* $\mathrm{Cl}_S(K)$ *are finite.*

Global Function Fields

For more details on global function fields, we refer to books [13] and [6]. From now on, we always assume that global function fields K are the fields whose constant fields are $\mathbb{F}_q$. One has the similar results for global function fields K over $\mathbb{F}_q$.

First, we have the degree maps

$$\deg : \mathrm{Div}(K) \to \mathbb{Z}, \sum_v n_v.v \mapsto \sum_v n_v.\deg(v), \text{ and}$$

$$\deg_S : \mathrm{Div}_S(K) \to \mathbb{Z}, \sum_{v\notin S} n_v.v \mapsto \sum_{v\notin S} n_v.\deg(v).$$

Their kernels are denoted by $\mathrm{Div}^0(K)$, and $\mathrm{Div}^0_S(K)$ respectively.

Proposition 1.1.6. *Let $x\in K^\times$. Then $(x)=0$, the zero divisor, if and only if $x\in\mathbb{F}_q^\times$, the ring of constant functions. Furthermore, $\deg(x)=0$ for all $x\in K^\times$ (equivalently, K satisfies the product formula).*

Proof. See [6] Proposition 5.1. □

Thanks to this result, we let $\mathrm{Cl}^0(K) := \mathrm{Div}^0(K)/\mathrm{Prin}(K)$.

Theorem 1.1.7. *(F.K. Schmidt) The image $\deg(\mathrm{Div}(K))$ is equal to $\mathbb{Z}$. In other words, the $\gcd(\deg v : v\in M_K)=1$.*

Proof. We refer to [13] Corollary 5.1.11. □

Now we recall the proof of Dirichlet $S-$unit theorem for global function fields. Let $d\mathbb{Z}$ be the image of $\mathrm{Div}_S(K)$ via the degree map. Then we have

Proposition 1.1.8. *The following sequences are exact:*

- $0\to\mathbb{F}_q^\times\to\mathcal{O}_S^\times\to\mathrm{Prin}_S(K)\to 0$;
- $0\to\mathrm{Div}^0_S(K)/\mathrm{Prin}_S(K)\to\mathrm{Cl}^(K)\to\mathrm{Cl}_S(K)\to\mathbb{Z}/d\mathbb{Z}\to 0$.

Proof. The exactness of the first sequence is by definition. To address the second one, we define a map $\tau:\mathrm{Div}(K)\to\mathrm{Div}_S(K)$ as follows:

$$\tau(D)=\sum_{v\notin S}\mathrm{ord}_v(D)v.$$

This map is surjective with kernel $\mathrm{Div}_S(K)$, and $\tau(\mathrm{Prin}(K)) = \mathrm{Prin}_S(K)$. Thus, τ induces a homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}_S(K)$ with kernel $(\mathrm{Div}_S(K)+\mathrm{Prin}(K))/\mathrm{Prin}(K) \cong \mathrm{Div}_S(K)/\mathrm{Prin}_S(K)$. So we get an exact sequence

$$0 \to \mathrm{Div}_S^0(K)/\mathrm{Prin}_S(K) \to \mathrm{Cl}^0 \to \mathrm{Cl}_S\,.$$

We need to prove that the cokernel of the last map is $\mathbb{Z}/d\mathbb{Z}$. Since $\mathrm{Cl}_S(K) \cong \dfrac{\mathrm{Div}(K)}{\mathrm{Prin}(K)+\mathrm{Div}_S(K)}$, and $\mathrm{Cl}^0(K) = \dfrac{\mathrm{Div}^0(K)}{\mathrm{Prin}(K)}$, this cokernel equals the cokernel of the natural map

$$\frac{\mathrm{Div}^0(K)}{\mathrm{Prin}(K)} \to \frac{\mathrm{Div}(K)}{\mathrm{Prin}(K)+\mathrm{Div}_S(K)},$$

which is $\dfrac{\mathrm{Div}(K)}{\mathrm{Div}^0(K)+\mathrm{Div}_S(K)}$. Via the degree map, it is isomorphic to $\mathbb{Z}/d\mathbb{Z}$. □

Corollary 1.1.9. *$\mathcal{O}_S^\times/\mathbb{F}_q^\times$ is finitely generated of rank at most $|S|-1$. In particular, $\mathcal{O}_S^\times$ is finitely generated.*

Proof. Since $\mathcal{O}_S^\times/\mathbb{F}_q^\times \cong \mathrm{Prin}_S(K)$, and the latter is a subgroup the free group $\mathrm{Div}_S(K)$ of rank $|S|-1$, we obtain the desired result. □

Even more, one can show that

Theorem 1.1.10. *$\mathrm{Cl}_S(K)$ is finite and $\mathcal{O}_S^\times/\mathbb{F}_q^\times$ is a free group of rank $|S|-1$.*

Proof. We refer to [6] Proposition 14.2. □

We recall (cf. [14], Remark 2.5) that there is an equivalence of categories between

- The category of smooth curves over $\mathbb{F}_q$:
  - Objects: smooth projective geometrically integral curves over $\mathbb{F}_q$,
  - Maps: non-constant rational maps over $\mathbb{F}_q$;
- The category of function fields whose constant field is $\mathbb{F}_q$
  - Objects: finitely generated field extensions $K/\mathbb{F}_q$ with $\mathrm{tr.deg}_{\mathbb{F}_q} K = 1$ and $K \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$,
  - Maps: non-trivial homomorphisms over $\mathbb{F}_q$.

Furthermore, one has

Proposition 1.1.11. *Let C be a smooth projective geometrically integral curve over $\mathbb{F}_q$. There is a bijection between the closed points of C and the set of places of $K := K(C)$.*

Proof. Since for every closed point p, $\mathcal{O}_{C,p}$ is a discrete valuation ring, it induces a place on K. Conversely, let v be a place on K, it then induce a discrete valuation subring $\mathcal{O}_v$ on K. Since $v(\mathbb{F}_q^\times) = 0$, the diagram

$$\begin{array}{ccc} \operatorname{Spec}(K) & \xhookrightarrow{\iota} & C \\ \downarrow & & \downarrow \\ \operatorname{Spec}(\mathcal{O}_v) & \longrightarrow & \operatorname{Spec}\mathbb{F}_q \end{array}$$

commutes. By the valuative criteria for properness, ι can lift to a morphism $\operatorname{Spec}\mathcal{O}_v \to C$ which map the unique closed point of $\mathcal{O}_v$ to some closed point x of C. It then induces a local map (and hence an injective map) $\mathcal{O}_{C,x} \to \mathcal{O}_v$, and since every valuation ring $\mathcal{O}$ of $K/\mathbb{F}_q$ is a maximal proper subring of K (cf. [13] Theorem 1.1.13), we have $\mathcal{O}_{C,x} = \mathcal{O}_v$. □

Example 1.2. By direct computations, closed points of $\mathbb{P}_1$ over $\mathbb{F}_q$ are in bijection with the set of irreducible monic polynomials with coefficients in $\mathbb{F}_q$ and the polynomial $\frac{1}{t}$, which is exactly $M_{\mathbb{F}_q(t)}$.

Example 1.3. Thanks to these correspondences, and thanks to the fact, that prime divisors on a smooth projective geometrically integral curve over a field are just closed points, notions relating to divisors of $K = K(C)$ is also in an 1-1 correspondence to those of C. In particular, those definitions of absolute values on $K = K(C)$ correspond to those on C defined in [10] Chapter 2, section 3.

1.2 Algebraic Groups

Now we turn the the geometric side of the thesis. First, we need some definitions.

Definition 1.2.1. A scheme G over a field K is called a **group scheme** if it is equipped with $K-$morphisms $m : G \times G \to G$, $i : G \to G$, and $e : \operatorname{Spec} K \to G$ satisfying the usual group axioms, i.e., the following diagrams commute

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m\times \mathrm{id}_G} & G \times G \\ {\scriptstyle \mathrm{id}_G\times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{(\mathrm{id}_G,e)} & G \times G \\ {\scriptstyle (e,\mathrm{id}_G)}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array}$$

$$\begin{array}{ccccc} G & & \xrightarrow{(\mathrm{id}_G,i)} & & G \times G \\ & \searrow & & & \\ {\scriptstyle (i,\mathrm{id}_G)}\downarrow & & \operatorname{Spec} K & & \downarrow{\scriptstyle m} \\ & & & \searrow^{e} & \\ G \times G & & \xrightarrow[m]{} & & G \end{array}$$

Further, G is said to be commutative if the diagram below commutes (τ is the interchaging map)

$$\begin{array}{ccc} G \times G & \xrightarrow{\tau} & G \times G \\ & \searrow^{m} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

The morphisms between $K-$group schemes can be defined in an evident way.

Definition 1.2.2. Let (G, m_G, i_G, e_G) be a group scheme over a field K. We define a K**-subgroup** H of G to be a closed subscheme such that there exist e_H, m_H, i_H satisfying the following diagrams commute

$$\begin{array}{ccc} \operatorname{Spec} K & & \\ {\scriptstyle e_H}\downarrow & \searrow^{e_G} & \\ H & \hookrightarrow & G \end{array} \qquad \begin{array}{ccc} H \times H & \xrightarrow{m_H} & H \times H \\ \downarrow & & \downarrow \\ G \times G & \xrightarrow[m_G]{} & G \times G \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{i_H} & H \\ \downarrow & & \downarrow \\ G & \xrightarrow[i_G]{} & G \end{array}$$

In other words, for every K-algebra R, $H(R)$ is a subgroup of $G(R)$. Further, H is is said to be normal in G if $H(R)$ is normal in $G(R)$ for each R.

Proposition 1.2.3. *(Existence of kernel) Let $f : G \to G'$ be morphism of group schemes. Then, there exists a unique normal subgroup $H \triangleleft G$ such that*

$$H(R) = \ker(G(R) \to G'(R))$$

functorially in R. This group scheme H is called the ***kernel*** *of ϕ.*

Proof. H is the fiber product $\operatorname{Spec} K \times_H G$

$$\begin{array}{ccc} H & \longrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle \phi} \\ \operatorname{Spec} K & \xrightarrow[e']{} & G' \end{array}$$

□

Definition 1.2.4. Let $1 \to G' \xrightarrow{i} G \xrightarrow{s} G''$ be a sequence of morphisms of group schemes. It is called **exact** if i is an isomorphism of G' onto $\ker s$. The sequence $1 \to G' \xrightarrow{i} G \xrightarrow{s} G'' \to 1$ is called exact if in addition, s is surjective and flat, i.e., faithfully flat.

In this thesis, we only focus on algebraic groups.

Definition 1.2.5. A group scheme over a field K is called an **algebraic group** if it is of finite type over K.

Proposition 1.2.6 (Existence of quotient algebraic groups, see [8] Theorem 5.2.5)**.** *Let H be a subgroup of an algebraic group G over a field K.*

1. *Then there exists a faithfully flat quotient map $q : G \to Q$ onto a $K-$scheme Q of finite type that is initial among K-morphisms $G \to G'$ that are invariant with respect to the right action of H on G. We call Q the **quotient** of G by H and denote by G/H. The formation of this quotient commutes with base field extension. Further, Q is smooth if G and H are smooth.*

2. *If in addition H is normal in G, then Q admits a unique K-group scheme structure such that q is a homomorphism, and $\ker q = H$. If moreover G is affine then Q is affine.*

Proposition 1.2.7 (Homomorphism theorem, see [8] Theorem 5.2.9)**.** *Let $f : G \to G'$ homomorphism of algebraic groups. Then it factors uniquely through homomorphisms $G \twoheadrightarrow I \hookrightarrow G'$ with $G \twoheadrightarrow I$ faithfully flat, and $I \to G'$ a closed immersion. We then call I the **image** of ϕ.*

Corollary 1.2.8. *With the above notation, we have that $\ker f = 0$ if and only if f is a closed immersion. In particular, if f is a monomorphism then it is a closed immersion and we denote its image by $f(G)$. If in addition, G and G' are smooth, then $f(G)$ is smooth and the map $G'/\ker f \to f(G)$ is an isomorphism. Particularly, when f is surjective, G and G' are smooth, then f is a quotient map.*

Proof. If $\ker f = 0$, then $f = i$ in the above proposition. Conversely, if f is a closed immersion, then $f : G(S) \to G'(S)$ is injective for every $K-$scheme, so $\ker f = 0$. □

Definition 1.2.9. Let G and H be two algebraic groups. A homomorphism $f : G \to H$ is called an **isogeny** if α is faithfullt flat and has finite kernel (i.e., $\ker \phi \to \operatorname{Spec} K$ is finite). Thanks to the generic flatness and the homogeneity of algebraic groups, it is equivalent to that f is surjective and $\dim G = \dim H$. We then define the degree of ϕ to be $\deg \phi := \# \ker \phi := \dim_K \Gamma(\ker \phi)$, where Γ is the global section functor.

Example 1.4. The following are algebraic groups.

(a) The additive group $\mathbb{G}_a = \operatorname{Spec} K[T] = \mathbb{A}^1_K$.

(b) The multiplicative group $\mathbb{G}_m = \operatorname{Spec} K[T, T^{-1}] = \mathbb{A}^1_K \setminus \{0\} \subset \mathbb{A}^1_K$.

(c) The general linear group $\mathrm{GL}_n = \operatorname{Spec} K[T_{ij} : 1 \leqslant i, j \leqslant n][\det(T_{ij})^{-1}] \subset \mathbb{A}^{n\times n}_K$.

(d) Similarly, we have the general sympletic group scheme GSp_{2n} which is defined by

$$\{g \in \mathrm{GL}_n :< gv, gw >= \mu(g) < v, w > \text{ for some } \mu(g) \in K^\times, \forall v, w \in V\}$$

associated to a given non-degenerate skew-symmetric form $<,>: V \times V \to K$ over a field K.

(e) Elliptic curves over K are also algebraic groups, but they are projective while the above examples are affine.

We note that the absolute Galois group $\Gamma = \mathrm{Gal}(K^s/K)$ acts continuously on $G(K^s)$ (here we need G to be of finite type) and the fixed points of this group under $\mathrm{Gal}(K^s/K)$ is $G(K)$. We denote $G[n] := G(\bar{K})[n] := \{x \in G(\bar{K}) : n.x = 0\}$ the $n-$torsion group for every positive integer n.

Definition 1.2.10 (see [15])**.** Let G be an algebraic group over a field K. For any prime l, the ($l-$adic) **Tate module** associating to G is

$$T_l(G) := \varprojlim G(K^s)[l^n],$$

where $G(K^s)[l^n] := \{x \in G(K^s) : l^n.x = e_G\}$, and the transitive maps are multiplication by l. We denote $V_l(G) := T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. We then have a natural Galois action on $T_l(G)$, and hence on $V_l(G)$

$$\rho_l : \mathrm{Gal}(K^s/K) \to \mathrm{Aut}_{\mathbb{Q}_l}(V_l(G)).$$

We denote by G_l the image of ρ_l. We will see later that in some circumstances, namely when G is semi-abelian, $G[n] = G(K^s)[n]$ when n is prime to char.K.

Example 1.5. We have $T_l(\mathbb{G}_m) = \varprojlim_m \mu_{l^m} =: \mathbb{Z}_l(1)$ is a free $\mathbb{Z}_l$ module of rank 1 where $\mathrm{Gal}(K^s/K)$ acts via the cyclotomic character $\chi_l : \mathrm{Gal}(K^s/K) \to \mathbb{Z}_l^\times$ (here, char.$K \nmid l$).

Definition 1.2.11. For G an algebraic group over K, and a subgroup $\Sigma \subset G(K)$, we define its **Zariski closure** to be the smallest reduced closed subscheme Σ^{zar} of G whose $K-$points contain Σ.

Remark. When G is a smooth algebraic $K-$group, Σ^{zar} is also smooth. Further, its formation commutes with base field extensions, i.e., if L is a field extension of K, then the closed subgroup $(\Sigma^{\mathrm{zar}})_L := \Sigma^{\mathrm{zar}} \times_K L \subset G_L$ is also the Zariski closure of $\Sigma \subset G(L) = G_L(L)$, see [7] Theorem 3.2.1.

Definition 1.2.12. We have two important types of algebraic groups.

- A **linear algebraic group** over K is a smooth algebraic group scheme with the underlying affine scheme defined over K.
- An **abelian variety** over a field K is a smooth, connected, proper algebraic group over K.

Then we have

Theorem 1.2.13 (Chevalley's theorem, see [7] Theorem 2.5.1)**.** *If K is perfect, then every smooth connected K-algebraic group fits into a unique short exact sequence of algebraic groups over K*

$$1 \longrightarrow G^{aff} \longrightarrow G \longrightarrow A \longrightarrow 1$$

where G^{aff} is a linear algebraic group and A is an abelian variety.

We then call G^{aff} and A the affine part and the abelian part of G respectively. Furthermore, the decomposition behaves well under surjective homomorphisms.

Proposition 1.2.14. *Let $f : G \to G'$ be a surjective homomorphism (resp. isogeny) between smooth connected K-groups where K is perfect, then $G^{aff} \to G'^{aff}$ is surjective (resp. an isogeny) and similarly for the induced map $G/G^{aff} \to G/G^{aff}$ between the abelian parts.*

So, to study algebraic groups amounts to study linear algebraic groups and abelian varieties separately.

1.2.1 Linear Algebraic Groups

The main reference for the section is [9].

Definition 1.2.15. A $K-$linear algebraic group G is called **unipotent** if $G_{\bar{K}}$ admits a composition series in which each successive quotient is isomorphic to a closed subgroup of $\mathbb{G}_{a,\bar{K}}$. G is called **solvable** if its nth derived subgroups is trivial for some n. Here, $G^0 := G$, $G^1 := [G^0, G^0]$ its commutator subgroup, etc.

Lemma 1.2.16. *There are no non-trivial homomorphisms between a torus T and an unipotent group U (in either direction).*

Definition 1.2.17. A K-**torus** is a algebraic group T over K such that $T_{K^s} \cong \mathbb{G}_m^n$ for some n. We define the **rank** of T to be n. Then, T is a commutative, connected, and affine $K-$group.

By definition, T is splitted by some finite extension L/K, i.e., $T_L \cong \mathbb{G}_m^n$. The smallest such L is called the **splitting field** of T.

Remark. Thanks to Jordan decomposition, one can show that a torus is a connected commutative group all of whose K^s-points are semisimple, and vice versa.

Not surprisingly, under some conditions, we can describe an algebraic group via its torus part and unipotent part as follows.

Proposition 1.2.18. *For a smooth connected commutative affine K-group G, we have the following.*

1. *There is a unique maximal K-torus T in G containing all K-tori of G, and $U = G/T$ is unipotent.*
2. *Such extension is split, i.e., $G = T \times U$, if K is perfect.*
3. *The formations of T and U are functorial in G. Furthermore, every surjective homomorphism (resp. isogeny) $G \to G'$ between commutative affine K-groups which are smooth and connected induces surjective homomorphisms (resp. isogenies) $T' \to T$ and $U' \to U$. Particularly, G' is a torus if and only if G is a torus, and similarly for unipotence.*

Proof. See [9] Proposition 2.16. □

Corollary 1.2.19. *A connected algebraic subgroup and a quotient of a torus are tori.*

Proof. For the subgroup, it must not contain any unipotent elements. This can also be proved as follows. Since the K^s-points of this subgroup must also are semisimple, the result follows from above remark. For the quotient, its unipotent part is a quotient of the unipotent part of the torus which is trivial. □

Definition 1.2.20. The **character group** and **cocharacter group** of an algebraic group G is defined to be $X(G) := \mathrm{Hom}_{\bar{K}}(G_{\bar{K}}, \mathbb{G}_m)$, and $X^\vee(G) := \mathrm{Hom}_{\bar{K}}(\mathbb{G}_m, G_{\bar{K}})$ respectively.

Example 1.6. For T a torus of dimension m over K, and l a prime satisfying $\mathrm{char}.K \nmid l$, one has

$$X^\vee(T) \otimes_{\mathbb{Z}} \mathbb{Z}_l(1) \cong T_l(T)$$

as $\mathrm{Gal}(K^s/K)$-modules. Indeed, each $\bar{K}-$homomorphism $\mathbb{G}_m \xrightarrow{\phi} T_{\bar{K}}$ induces a homomorphism

$$\phi[l^n] : \mu_{l^n} \to T[l^n], \xi_{l^n} \mapsto g_{l^n}$$

where ξ_{l^n} is a fixed primitive root of unity for each n. Let n go to the infinity, we have a Galois equivariant homomorphism

$$\phi_l : \mathbb{Z}_l(1) \to T[l^n].$$

We then have a map

$$X^\vee(T) \otimes_{\mathbb{Z}} \mathbb{Z}_l(1) \to T_l(T), \phi_l \otimes 1 \mapsto \phi_l((\xi_{l^n})) = (g_{l^n}).$$

Because both sides are isomorphic (as groups) to $\mathbb{Z}_l^m$, it remains to show that this map is injective. If $\phi_l((\xi_{l^n})) = 1$, then $\phi[l] = 1$, i.e. $\mathrm{Im}(\phi)[l] = 1$. Since $\mathrm{Im}(\phi)$ is a connected subgroup of T (since $\mathbb{G}_m$ is connected), it is a torus. Therefore, $\mathrm{Im}(\phi)[l]$ is of dimension $\dim \mathrm{Im}(\phi)$, and hence, $\mathrm{Im}(\phi)$ is trivial . It means that ϕ is trivial. We note that for a smooth connected unipotent group, their character group, cocharacter group, and Tate module are all trivial (since it does not have any non-trivial $l-$torsion points).

Remark. Thanks to the Dirichlet's unit theorem, see Theorem 1.1.5 and corollary 1.1.5, the group $T(\mathcal{O}_{K,S})$ is finitely generated for any torus T over a global field K. Consequently, the number of torsion K-points of a torus is finite. We note that in general, the number of torsion points of a linear algebraic group is not finite.

1.2.2 Abelian Varieties

The main reference for this section is [16]. First, we list here some important properties of abelian varieties.

- Abelian varieties are commutative.
- They are also projective.
- Over $\mathbb{C}$, they are 1-1 corresponding to polarizable complex tori (i.e., complex tori admitting a Hermitian form).

First we have the following result due to A. Weil, see [16] Chapter 3.

Proposition 1.2.21. *Let $\alpha : X \dashrightarrow A$ be a rational map from a smooth variety X over K to an abelian variety. Then α is a morphism.*

Corollary 1.2.22. *Every rational map $\mathbb{A}^1 \dashrightarrow A$ or $\mathbb{P}^1 \dashrightarrow A$ is constant.*

We note that every morphism from a proper connected K-scheme to an affine K-scheme of finite type is also a constant. For instance, there are no non-trivial K-homomorphisms from an abelian variety A to a connected linear algebraic group G. In addition, there are also no non-trivial $K-$homomorphisms from G to A.

Lemma 1.2.23. *A connected algebraic subgroup H and a connected quotient Q of an abelian variety G are abelian varieties.*

Proof. Because over $\bar{K}$, the affine part $H^{aff}_{\bar{K}}$ is a subgroup of $G^{aff}_{\bar{K}}$, $Q^{aff}_{\bar{K}}$ is a quotient of $G^{aff}_{\bar{K}}$, and $H^{aff}_{\bar{K}}$ is trivial, then the lemma follows. □

We also note that for abelian varieties A, the multiplication-by-n map $[n] : A \to A$ is an isogeny. In fact one can show that

Proposition 1.2.24 (see [16] Theorem 7.2)**.** *Suppose A has dimension g, then*

1. $\deg[n] = n^{2g}$, *and*
2. $[n]$ *is separable if and only if* $\mathrm{char}.K \nmid n$.

In particular, $A(K^s)[n] = A(\bar{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ *when* $\mathrm{char}.K \nmid n$.

Remark. If $f : A \to B$ is an isogeny of degree n between abelian varieties, then there exists an isogeny $f' : B \to A$ with $f' \circ f = [n]_A$ and $f \circ f' = [n]_B$. Indeed, since f is an isogeny, we have an isomorphism

$$f : A/\ker f \to B.$$

Now let $h : B \to A/\ker f$ be its inverse. Then the map $[n] : A \to A$ factors through $[n] : A/\ker f \to A$, since $[n]$ kills $\ker f$. Next we define $f' : B \to A$ as $f' := [n] \circ h : B \to A$ and it is straightfoward to check that $f' \circ f = [n]_A$ and $f \circ f' = [n]_B$.

Next, we will construct the Weil pairing on abelian varieties. We first need to construct dual abelian varieties. For an abelian variety $A \xrightarrow{f} \operatorname{Spec} K$, we introduced the **relative Picard functor**, see [8] Remark 5.7.12,

$$\mathrm{Pic}_{A/K} : (\mathbf{Sch}_{/K}) \to (\mathbf{Set}), T \mapsto \mathrm{Pic}(A_T)/f_T^*\mathrm{Pic}(T).$$

Here $A_T = A \times_K T$ and $f_T : A_T \to T$. Grothendieck proved that this functor is representable (he actually did for a more general situation).

Theorem 1.2.25 (see [8] Remark 5.7.12)**.**

1. $\mathrm{Pic}_{A/K}$ *is represented by a locally of finite type scheme over K (hence a group scheme).*
2. *The connected component* $\mathrm{Pic}^0_{A/K}$ *is projective and smooth. We define* $\hat{A} := \mathrm{Pic}^0_{A/K}$ *the* ***dual abelian variety*** *of A. In addition, the set* $\hat{A}(K)$ *equals* $\mathrm{Pic}^0(A) := \{\mathcal{L} \in \mathrm{Pic}(A) : T_x^*\mathcal{L} = \mathcal{L}\ \forall x \in A(\bar{K})\}$, *the group of translation invariant line bundles.*

We note that for any line bundle $\mathcal{L}$ on A, we have

$$\phi_{\mathcal{L}} : A \to \mathrm{Pic}^0(A), x \mapsto T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}.$$

When $\mathcal{L}$ is ample, this map is surjective with finite kernel, and hence an isogeny. Since A always admits an ample line bundle (due to the projectivity of A), we have $\dim A = \dim \hat{A}$.

Definition 1.2.26 ([16] section 11)**.** With the above notation, a **polarization** of A is an isogeny $\lambda : A \to \hat{A}$ satisfying $\lambda_{\bar{K}} = \phi_{\mathcal{L},\bar{K}}$ for some ample line bundle $\mathcal{L}$ on A. If in addition, λ is an isomorphism (i.e., $\deg \lambda = 1$), then λ is said to be **principal**.

Now, for char.$K \nmid m$, we will construct a pairing

$$e_m : A(\bar{K})[m] \times \hat{A}(\bar{K})[m] \to \mu_m(\bar{K}).$$

We follows the construction in [16]. First we assume $K = \bar{K}$ for simplicity. Let $a \in A(K)[m]$ and $\mathcal{L} \in \hat{A}(K)[m] \subset \mathrm{Pic}^0(A)$, then $\mathcal{L}$ can be represented by the divisor D on A. We denote $\sim$ the linear equivalent.

Then $[m]^*D \sim mD$ because for $\mathcal{L} \in \mathrm{Pic}^0(A)$, $(\alpha+\beta)^*(\mathcal{L}) \sim \alpha^*(\mathcal{L}) \otimes \beta^*(\mathcal{L})$ for all regular morphisms α, β: $X \to A$ from some variety $X \to A$. Therefore, $[m]^*D \sim 0$, i.e., there are $f, g \in K(A)$ satisfying $mD = \mathrm{div}(f)$ and $[m]^*D = \mathrm{div}(g)$. We then have

$$\mathrm{div}(f \circ [m]) = \mathrm{div}([m]^*(f)) = [m]^*(mD) = m([m]^*D) = \mathrm{div}(g^m)$$

because div commutes with pull back via separable morphism. Thus $g^m/(f \circ [m])$ is also a rational function on A. Further, it does not contain ant zeros or poles, so it must be constant and we denote it by c. Thus we have

$$g(x+a)^m = cf(mx+ma) = cf(mx) = g(x)^m,$$

i.e., the values of the funtion $g/(g \circ T_a)$ are in $\mu_m(K)$. Since A is connected, it is an constant function $\in \mu_m(K)$. So we define

$$e_m(a, \mathcal{L}) := g/(g \circ T_a).$$

Lemma 1.2.27. *For integers $m, n > 0$ prime to* char.K*, and $a \in A(\bar{K})[mn]$, $\mathcal{L} \in \hat{A}(\bar{K})[mn]$, we have*

$$e_{mn}(a, \mathcal{L})^n = e_m(na, n\mathcal{L}).$$

Proof. As above, $\mathcal{L}$ corresponds to some divisor D, and there exists rational functions f, g, h such that

$$m(nD) = mnD = \mathrm{div}(f), [mn]^*D = \mathrm{div}(g), [m]^*(nD) = \mathrm{div}(h).$$

Then there exist constant functions c and d satisfying $g^{mn} = c.(f \circ [mn]), h^m = d.(f \circ [n])$. So

$$g(x+a)^{mn} = c.f(mnx) = g(x)^{mn}, h(x+na)^m = d.f(mx) = h(x)^m.$$

Thus $g(x)^n/h(nx)$ is a $\mu_m(K)-$valued function anh hence is constant. Therefore

$$e_{mn}(a, \mathcal{L})^n = \Big[g(0)/g(a)\Big]^n = h(0)/h(na) = e_m(na, n\mathcal{L}).$$

□

From this we have a **(Weil) pairing** (also denote by e_l)

$$e_l : T_l(A) \times T_l(\hat{A}) \to \mathbb{Z}_l(1), ((a_n)(\mathcal{L}_n)) \mapsto (e_{l^n}(a_n, \mathcal{L}_n)).$$

For a polarization $\lambda : A \to \hat{A}$ (which always exists), we have an associated pairing

$$e_l^\lambda : T_l(A) \times T_l(A) \to \mathbb{Z}_l(1), (a, \mathcal{L}) \mapsto e_l(a, T_l(\lambda)\mathcal{L}).$$

One can show that

Proposition 1.2.28. *The pairings e_m, and e_l are* $\mathrm{Gal}(\bar{K}/K)-$*equivariant, and symplectic, i.e., they are skew-symmetric and non-degenerate, for any $m > 0$ prime to* $\mathrm{char}.K$ *and any primes l coprime to* $\mathrm{char}.K$*. Similar properties also hold for e_l^λ, except the non-degenerate one.*

Proposition 1.2.29. *Let $\phi : A \to B$ be an isogeny between abelian varieties over a field K. Then for primes $l > \deg \phi$, we have an isomorphism of* $\mathrm{Gal}(\bar{K}/K)-$*modules*

$$\phi[l] : A[l] \cong B[l].$$

Proof. The sequence

$$0 \to \ker(\phi) \to A \to B \to 0$$

induces an exact sequence

$$0 \to \ker(\phi)(\bar{K}) \to A(\bar{K}) \to B(\bar{K}) \to 0.$$

It is straightforward to check that by taking $l-$torsion points, we have an exact sequence

$$0 \to \ker(\phi)[l] \to A[l] \to B[l].$$

By choosing $l > \#\ker(\phi)(\bar{K})$, we have $\ker(\phi)[l] = 0$, and hence, $A[l] \hookrightarrow B[l]$. In addition, these two groups have the same cardinality when $l > \mathrm{char}.K$ because A and B have the same dimension. Thus the proposition follows. □

Corollary 1.2.30. *For almost all primes l, the division field $K(A[l])$ contains μ_l, the group of lth roots of unity in $\bar{K}$. Here, and from now on, by "**almost all**" we mean "for all but finitely many".*

Proof. First we choose a polarization $\lambda : A \to \hat{A}$. because the pairing $e_l : A[l] \times \hat{A}[l] \to \mu_l$ is $\mathrm{Gal}(\bar{K}/K)-$equivariant and non-degenerate, and for l large, $A[l] \cong \hat{A}[l]$ as Galois modules, the pairing $e_l^{\lambda} : A[l] \times A[l] \to \mu_l$ is also $\mathrm{Gal}(\bar{K}/K)-$equivariant and non-degenerate. Therefore, since $A[m] \times A[m]$ is fixed by $\mathrm{Gal}(\bar{K}/K(A[m]))$, μ_m is also fixed by $\mathrm{Gal}(\bar{K}/K(A[m]))$, i.e., $\mu_m \subset K(A[m])$. □

In fact, we have more, see [17].

Proposition 1.2.31. *For every $n > 0$ prime to* char.K*, the division field $K(A[n])$, i.e., the smallest field L over K such that $A[n] \subset A(L)$, contains μ_n.*

Proof. We can assume that $n = l^m$ for some prime l, and we denote $L := K(A[l^m])$. We take a $K-$polarization $\lambda : A \to \hat{A}$ of smallest possible degree. Then $\ker(\lambda)$ does not contain $A[l]$, otherwise the isogeny λ would factor via the multiplication-by-l map (see [16] Remark 8.12 and the diagram below) and an isogeny $\beta : A \to \hat{A}$ of degree $\deg(\lambda)/l$, a contradiction.

$$\begin{array}{ccccc} A & & \xrightarrow{\quad\lambda\quad} & & \hat{A} \\ {\scriptstyle [l]}\downarrow & & \overset{\beta}{\nearrow} & & \| \\ A & = & A/A[l] & \longrightarrow & A/\ker(\lambda) \end{array}$$

We then observe that $\lambda(A[l^m]) \subset \hat{A}[l^m]$ contains a point of order l^m, say P. Otherwise, $\lambda(A[l^m]) \subset \hat{A}[l^{m-1}]$, and hence, $A[l] = l^{m-1}A[l^m]$ is contained in $\ker(\lambda)$, a contradiction. Furthermore, since $A[l^m] \subset A(L)$, $\lambda(A[l^m])$ lies in $\hat{A}(L)$. Now, we claim that there is a point $Q \in A[l^m]$ such that $\xi := e_{l^m}(Q, P)$ is a l^m-primitive root of unity. Otherwise,

$$e_{l^m}(A[l^m], P) \subset \mu_{l^{m-1}},$$

and so the non-zero element $l^{m-1}P$ is orthogonal to $A[l^m]$, which is a contradiction. Since P and Q are defined over L, ξ also lies in L, and so $\mu_{l^m} \subset L = K(A[l^m])$. □

Remark. We will see later that (Mordell-Weil theorem 2.2.1) that $A(K)$ is finitely generated for any abelian variety A over any global field K. As a consequence, the number of its K-torsion points is finite.

1.2.3 Elliptic Curves

We follow [14].

Definition 1.2.32. . An **elliptic curve** E over a field K is

1. an irreducible smooth projective curve over K of genus one with a marked point O, or equivalently,

2. a plane projective curve defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K,$$

with non-zero discriminant. When K has the charateristics different from 2 and 3, changing variables gives us the simplified Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3, g_2, g_3 \in K.$$

Elliptic curves have rich structures. The group of ($\bar{K}$-) homomorphisms from an elliptic curve E_1 to another E_2 is denoted by $\mathrm{Hom}(E_1, E_2)$. For each elliptic curve E, we have the **endomorphism ring** $\mathrm{End}(E)$, which contains $\mathbb{Z}$.

Remark. 1. Elliptic curves are one-dimensional abelian varieties. Over $\mathbb{C}$, the category of elliptic curves are equivalent to the category of lattices in $\mathbb{C}$, thanks to the Weierstrass functions. One way to see this is that one-dimensional tori always admit a Hermitian form, while higher-dimensional complex tori may not in general. In addition, morphisms between elliptic curves over $\mathbb{C}$ correspond to homotheties between lattices.

2. Because there is the canonical principal polarization given by $\mathcal{L} = \mathcal{O}(O)$ on elliptic curves, elliptic curves are canonically isomorphic to its dual. In general, abelian varieties may not admit any principal polarization, but there is a way called Zarhin's trick to embed an abelian variety to a principally polarized one.

3. Because E_1 and E_2 are elliptic curves, non-trivial $\bar{K}-$homomorphisms between them are isogenies. However, this property is not true for general abelian varieties.

One can describes the endomorphism ring as follows.

Theorem 1.2.33 (see [14] Corollary 9.4)**.** *With the above notation, the ring* $\mathrm{End}(E)$ *is either* $\mathbb{Z}$*, an order in an imaginary quadratic extension of* $\mathbb{Q}$*, or an order in a quaternion algebra over* $\mathbb{Q}$*. Moreover, only the first two cases are possible when* $\mathrm{char}(K) = 0$.

Thanks to this result, we then have the following terminologies.

Definition 1.2.34. If char.$K = 0$, then we say that an elliptic curve E/K has **complex multiplication** if $\mathrm{End}(E) \neq \mathbb{Z}$. If char.$K > 0$, E/K is said to be **supersingular** if $\mathrm{End}(E)$ is an order in a rational quaternion algebra, otherwise E is said to be **ordinary**.

In certain circumstances, Serre (see [18] Theorem 7) proved that $G_l \subset \mathrm{GSp}_2 = \mathrm{GL}_2$ can be as large as possible for almost l.

Theorem 1.2.35. *Let E be an elliptic curve over a number field K without complex multiplication, the image G_l of the representation ρ_l is open in $\mathrm{GL}_2(\mathbb{Q}_l)$, i.e., the Lie algebra g_l is $\mathrm{End}(V_l(E))$ for all primes l. In addition, ρ_l is surjective for all but finitely many $l's$.*

1.2.4 Semi-Abelian Varieties

The main reference for this section is [9].

Definition 1.2.36. An algebraic group G over a field K is called a **semi-abelian variety** if it fits into an exact sequence

$$1 \longrightarrow T \longrightarrow G \longrightarrow A \longrightarrow 1$$

where T is a torus, and A is an abelian variety over K.

Equivalently, G^{aff} is a torus because although $\bar{K}/K$ may not be Galois due to the imperfectness of K, one can still descend the affine part to K as in [9] Theorem 3.1. In addition, semi-abelian varieties are commutative, see [9] Theorem 3.1. Therefore, thanks to the behaviour of Chevalley decomposition under isogeny, it follows that for an isogeny $G \to G'$, G is semi-abelian if and only if G' is.

Lemma 1.2.37 (see [9] Corollary 3.2)**.** *Let $1 \to G' \to G \to G'' \to 1$ be an exact sequence of smooth connected groups over K. Then G is semi-abelian if and only if G' and G'' are semi-abelian. In particular, connected subgroup of semi-abelian varieties are semi-abelian.*

Proof. Indeed, we may assume that $K = \bar{K}$ thanks to [9] Theorem 3.1. If G is semi-abelian, then G'^{aff}, a smooth connected subgroup of G^{aff}, and G''^{aff}, a quotient of G^{aff}, are tori. Conversely, we need to show thar a unipotent smooth connected subgroup U in G^{aff} is trivial. Because its image in G''^{aff} is trivial, U must be a subgroup of G' and hence is trivial since G'^{aff} is a torus. □

Corollary 1.2.38. *A subgroup of a product of a torus and an abelian variety is also a product of a (sub)torus and an (sub)abelian variety.*

We note that if $G = T \rtimes A$, we have $G[l] = T[l] \rtimes A[l]$ and $T_l(G) = T_l(T) \rtimes T_l(A)$. Therefore, we have

Corollary 1.2.39. *Let H be a K-subgroup of a semi-abelian variety G over K. If $H[l]$ vanishes for l, then H is finite.*

Proof. If H is connected. It follows from the assumption that H is semi-abelian. Hence, $0 = H^{aff}[l]$ is of order $l^{\dim H^{aff}}$, so $H^{aff} = 0$, i.e. H is an abelian variety. Then $0 = H[l]$ is of order $l^{2\dim H}$, i.e. $H = 0$. For H non-connected, the result follows from the finiteness of H/H^o. □

We know that the groups of geometric points of tori and abelian varieties over K are divisible when char.K = 0. Therefore, we have

Lemma 1.2.40. *If* char.$K = 0$*, and G is a semi-abelian variety over K, then the group $G(\bar{K})$ is divisible.*

Proof. Indeed, by definition we have an exact sequence

$$1 \to T \xrightarrow{f} G \xrightarrow{g} A \to 1.$$

It yields an exact sequence

$$1 \to T(\bar{K}) \xrightarrow{f} G(\bar{K}) \xrightarrow{g} A(\bar{K}) \to 1.$$

Take $R \in G(\bar{K})$, then there exists $P \in T(\bar{K})$ such that $nP = g(R)$. Let $Q \in g^{-1}(P)$, then $nQ - R \in \ker(g) = T(\bar{K})$. So there exists $S \in T(\bar{K})$ such that $nS = nQ - R$ and then $R = n(Q - S)$. □

Similarly, when char.$K = p > 0$, the group $G(\bar{K})$ is divisible by any n prime to p.

Remark. For every semi-abelian variety $G = TA$ over a global field K, we have $G(K) \subset T(K)A(K)$. We have its group of torsion elements $G(K)^{\text{tors}}$ is finite, because from the exact sequence

$$1 \to T(K) \xrightarrow{f} G(K) \xrightarrow{g} A(K),$$

$g(G(K)^{\text{tors}}) \subset A(K)^{\text{tors}}$. In addition, if $P, R \in G(K)^{\text{tors}}$ has the same image in $A(K)$, then there is some $Q \in T(K)^{\text{tors}}$ such that $f(Q) = P - R \in G(K)^{\text{tors}}$, then $Q \in T(K)^{\text{tors}}$ since f is injective. Thus $G(K)^{\text{tors}} \subset T(K)^{\text{tors}}A(K)^{\text{tors}}$ and it is also finite.

1.3 Integral Models of Algebraic Groups

The main reference for this section is [5]. We are mostly interested in algebraic groups over a global field K. In particular, we sometimes want to understand the $(S-)$integral points and their reductions. To do this process, we need to lift the objects to integral bases. First, we have a definition.

Definition 1.3.1. 1. Let X be a scheme over a global field K, and let R be an integral domain whose fraction field equals K. Then an R-scheme $\mathcal{X}$ is a R-**model** for X if its generic fiber is X, i.e. $\mathcal{X} \times_{\operatorname{Spec} R} \operatorname{Spec} K \cong X$.

2. If $\mathcal{X}$ and $\mathcal{X}'$ are $R-$models of X and X' over K, and $f : X \to X'$ is a $K-$morphism. Then $F : \mathcal{X} \to \mathcal{X}'$ is called a **lift** of f to R if $F_K = f$.

For an algebraic scheme X over K, there may not exist a model over $\mathcal{O}_K$. However, if we distract finitely many points in $\operatorname{Spec} \mathcal{O}_K$, X will admits a model over the smaller base. In fact, this is true for any finitely presented scheme over K, and roughly speaking, this process called **spreading out** can be described as follows (see [8]). We first note that X can be given by solutions of finitely many polynomials in finitely many variables with coefficients in K. We then write each coefficient of those polynomials as a fraction of elements in $\mathcal{O}_K$, and we let S be places dividing those denominators that appear, then S is finite. Discarding those primes, we obtain an open subscheme $U := \operatorname{Spec} \mathcal{O}_{K,S}$ of $\mathcal{O}_K$ (by localizing at those primes). By gluing affine pieces, we obtain to a scheme $\mathcal{X}$ over U, this is what we want. We can also use Grothendieck's general theory to show the existence of integral models. Grothendieck shows the following (see [19] Theorem 3.4).

Theorem 1.3.2. *Let A be the direct limit $\varinjlim A_i$ over a directed system of rings A_i, and X a finitely presented scheme over A. Then*

1. *There exists some i_0 and a finitely presented scheme X_{i_0} over A_{i_0} such that*

$$X_{i_0} \times_{A_{i_0}} A \cong X.$$

In addition, if X_{i_0} and Y_{i_0} are finitely presented over A_{i_0} for some i_0, then there is a natural bijection

$$\varinjlim \operatorname{Hom}_{A_i}(X_i, Y_i) \to \operatorname{Hom}_A(X, Y)$$

where $X_i := X_{i_0} \times_{A_{i_0}} A_i$, $Y_i := Y_{i_0} \times_{A_{i_0}} A_i$, $X := X_{i_0} \times_{A_{i_0}} A$, and $X := Y \times_{A_{i_0}} A$.

2. *The map $f_{i_0} : X_{i_0} \to Y_{i_0}$ is $\boldsymbol{P}$ if and only if its base change $f : X \to Y$ over A is $\boldsymbol{P}$. Here $\boldsymbol{P}$ can be any of the following: closed immersion, separated, proper, smooth, affine, flat, faithfully flat, open immersion, finite. This also means that this property also holds for $i \geqslant i_0$.*

3. *(The unicity of integral models) The formation of a lift X_{i_0} over A_{i_0} from X over A is unique in the following sense: for any finitely presented A_{i_0}-schemes X_{i_0} and X'_{i_0} whose base changes over A are identified with X, there exists some $i \geqslant i_0$ and an isomorphism $h_i : X_i \cong X'_i$ over A_i which is compatible with the identification with X after base changing to A, and further if h_i and h'_i are two such isomorphisms, then for some $j \geqslant i$ the induced morphisms h_j and h'_j are equal over A_j.*

We note that $K = \varinjlim_S \mathcal{O}_{K,S}$ where S runs over the set of finitely many non-Archimedean places of K. Therefore, as a direct consequence, we have

Theorem 1.3.3. *(see [8] Theorem 3.2.1)*

1. *Let X be a finitely presented scheme over K. Then there exists an open subscheme U of $\operatorname{Spec} \mathcal{O}_K$ such that X can be lifted to an U-scheme $\mathcal{X}$.*

2. *Let $\mathcal{X}$ be a finitely presented $\mathcal{O}_{K,S}-$scheme for some S as above. If $\mathcal{X}_K \to K$ is $\boldsymbol{P}$, then there exists an open subscheme $U \subset \operatorname{Spec} \mathcal{O}_{K,S}$ such that $X_U \to U$ is $\boldsymbol{P}$.*

3. *Let $\mathcal{X}$ and $\mathcal{X}'$ are finitely presented schemes over $\mathcal{O}_{K,S}$, and $f : \mathcal{X}_K \to \mathcal{X}'_K$. Then f can be lifted to a $U-$morphism from $\mathcal{X}_U \to \mathcal{X}'_U$ for some open dense subscheme $U \subset \mathcal{O}_{K,S}$.*

4. *For $f : \mathcal{X} \to \mathcal{X}'$ an morphism between finitely presented schemes over $\mathcal{O}_{K,S}$ satisfying $f_K : \mathcal{X}_K \to \mathcal{X}'_K$ is $\boldsymbol{P}$, there always exists an open subscheme $U \subset \mathcal{O}_{K,S}$ such that $f_U : \mathcal{X}_U \to \mathcal{X}'_U$ is $\boldsymbol{P}$.*

So this theorem says that one can spread out schemes and morphism between them without losing any properties.

Corollary 1.3.4. *By discarding finitely many points, the lift of the composition (resp. fiber products) of two morphisms over K is the composition (resp. fiber products) of their lifts.*

Proof. This follows from the unicity of the lift. □

This is straightforward to check that spreading out "commutes" with exact sequences, fiber products, and extending the base after ruling out finitely many points. Now, let G be an (commutative) algebraic group. We note that because schemes of finite type over fields are finitely presented, so we can apply the spreading out principle to G with the maps m, i, e. Then there exists an open dense subscheme $U \subset \mathcal{O}_K$ such that G and those morphisms can be lifted to U. Then by 1.3.4, these lifted morphisms satisfy the usual commutative diagrams which means that the lifted scheme is also an (commutative) algebraic group over U. Here algebraic groups over a scheme U are scheme of finite types with multiplication and inverse map satisfying usual commutative diagram, in other words, each fiber is an algebraic group as in the absolute sense. In addition, those properties above also hold in the algebraic group case.

Example 1.7. (a) (Models of linear algebraic groups) Because spreading out preserves affiness property of morphisms, models for affine schemes (resp. linear algebraic groups) of finite presentation over K are also affine schemes (resp. linear algebraic groups). In addition, for a linear algebraic group G, we consider a embedding $G \to \mathrm{GL}_n(K)$. It induces a $K-$morphism of $K-$Hopf algebras $\varphi : K[\mathrm{GL}_n] \to K[G]$. We note that $K[\mathrm{GL}_n] = K[x_{11}, ..., x_{nn}, \det(x_{ij})^{-1}]$ is defined by polynomials over $\mathcal{O}_K$, then the $\mathcal{O}_K$-algebra

$$\mathcal{O}_K[x_{11}, ..., x_{nn}, \det(x_{ij})^{-1}]$$

defines an algebraic group $\mathrm{GL}_n(\mathcal{O}_K)$, and $\varphi(\mathcal{O}_K[x_{11}, ..., x_{nn}, \det(x_{ij})^{-1}])$ is a Hopf $\mathcal{O}_K-$algebra which is a model for G.

(b) $G = \mathbb{G}_{m,K}$ over K admits $\mathbb{G}_{m,\mathcal{O}_K}$ as its $\mathcal{O}_K$-model.

Further, one needs the notion of abelian schemes, which is a relative version of abelian varieties.

Definition 1.3.5 (Abelian scheme)**.** Let U be a scheme (we are mostly interested in the case $U = \mathcal{O}_{K,S}$ for some set of finitely many non-Archimedean places S of K). A g-dimensional **abelian scheme** over U is a group scheme $A \to U$ of finite presentation, proper, smooth, with all fibers geometrically connected and of dimension g.

Remark. From the spreading out principal, any abelian varieties over a global field K can be always lifted to an abelian scheme over $\mathcal{O}_{K,S}$ for some set of finitely many non-Archimedean places S.

Abelian schemes also admit similar properties of abelian varieties. We note that there may not exists an abelian scheme over an arbitrary base. For instance, over $\mathbb{Z}$,

Tate, and Fontaine have shown that there is no elliptic curve, and abelian variety over $\mathbb{Z}$. It is similar to the theorem of Minkowski which says that $\mathbb{Q}$ does not admit any finite extension which is unramified everywhere. In arithmetic situation, if $\mathcal{A}$ is an abelian scheme over $\mathcal{O}_K$, then its $\mathcal{O}_K$ points are $A(K)$ where $A = \mathcal{A}_K = \mathcal{A} \times_K \mathcal{O}_K$.

1.4 Reduction of Algebraic Groups

First we discuss the reduction of algebraic groups G over a global field K. Any such G can be lifted to an algebraic group $\mathcal{G}$ over $\mathcal{O}_{K,S}$ for some set of finitely many non-Archimedean places S. Then for $\mathfrak{p} \notin S$, we denote $G_\mathfrak{p} := \mathcal{G} \times_{\mathcal{O}_{K,S}} k(\mathfrak{p})$ its special fiber at $\mathfrak{p}$, where $k(\mathfrak{p})$ denotes the **residue field** at $\mathfrak{p}$. We note that for all but finitely many $\mathfrak{p}$, $G_\mathfrak{p}$ is again an algebraic group over $k(\mathfrak{p})$, and hence, its set of $k(\mathfrak{p})-$points is finite. When G is an abelian variety, we have the notion of bad, good, and stable reduction.

Definition 1.4.1. For an abelian variety A over a global field K, and a place $\mathfrak{p}$ of K, we say that A has **good reduction** at $\mathfrak{p}$ if A can be lifted to an abelian scheme $\mathcal{A}$ over $\mathcal{O}_{K,\mathfrak{p}}$, otherwise we say that A has **bad reduction** at $\mathfrak{p}$.

Thanks to the spreading out principle (and its properties), we have

Proposition 1.4.2. *Abelian varieties over global fields have good reduction at almost all places.*

Reduction of Points

Now, we want to define the **reduction** of the $K-$points of an algebraic group G over a global field K. For a $K-$point $R : \operatorname{Spec} K \to G$, it can be lifted to $R : U \to \mathcal{G}$ where U is some open subscheme of $\mathcal{O}_K$ and $\mathcal{G}$ is the model of G over U. For a point $\mathfrak{p} \in U$, by tensoring with $k(\mathfrak{p})$ we obtain $R \bmod \mathfrak{p} : \operatorname{Spec} k(\mathfrak{p}) \to G_\mathfrak{p}$. In other words, the notion of reduction mod $\mathfrak{p}$ depends on whether the point R can be lifted to a morphism over $\mathcal{O}_\mathfrak{p}$. If it is the case, we can take the reduction mod $\mathfrak{p}$ of R. In addition, if R and R' are two K-points that can be extended to $\mathcal{O}_\mathfrak{p}$-points of some model $\mathcal{G}$ (by discarding finitely many places, we can assume that their models are the same). Then we obtain $R \times R' : \operatorname{Spec} \mathcal{O}_\mathfrak{p} \to \mathcal{G} \times \mathcal{G}'$, composing with the multiplication map $m : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$, we obtain $m(R, R') : \operatorname{Spec} \mathcal{O}_\mathfrak{p} \to \mathcal{G}$ which is exactly a lift of $m(R, R')$, the product of R and R' in G by the unicity of lifting. Similarly for the inverse of those points; therefore, we have a group homomorphism from (the set of $K-$points of G that can be lifted to $\mathcal{O}_\mathfrak{p}$) to (the set of $k(\mathfrak{p})-$points of $G_\mathfrak{p} = \mathcal{G} \times k(\mathfrak{p})$). Particularly, e_G is mapped to $e_{G_\mathfrak{p}}$ for almost all $\mathfrak{p}$.

Example 1.8. (a) When G is a linear algebraic group, there is a closed embedding $G \hookrightarrow \mathbb{A}_n$ and the point $R \in G(K)$ is a point in $\mathbb{A}_n(K)$. Therefore, $R = (a_1, ..., a_n)$ and we can take reduction mod $\mathfrak{p}$ for any prime $\mathfrak{p}$ not containing a_1,..., a_n. The unicity of integral model guarantees that this process does not depend on the embedding.

(b) When G is an abelian variety, there is a closed embedding $G \hookrightarrow \mathbb{P}^n$ and then the point $R \in G(K)$ is a point in $\mathbb{P}^n(K)$. Now to take reduction mod $\mathfrak{p}$, the point K must be lifted to a $\mathcal{O}_\mathfrak{p}$-point of some abelian scheme $\mathcal{A}$ over $\mathcal{O}_\mathfrak{p} \subset \mathbb{P}_n(\mathcal{O}_\mathfrak{p})$. It is well-known (see Exercise III-43. [20]) that for a ring A, there is a bijection between the set of $(n+1)$-tuples of elements of A that generate A and the set of $A-$points of $\mathbb{P}_n$. Therefore, an $\mathcal{O}_\mathfrak{p}-$point R of $\mathbb{P}^n$ corresponds to a tuple $(a_0, ..., a_n)$ where $a_0, ..., a_n \in \mathcal{O}_\mathfrak{p}$ generate $\mathcal{O}_\mathfrak{p}$, and then taking reduction gives us a $k(\mathfrak{p})$-point correspond to $(a_1 + \mod \mathfrak{p}, ..., a_n + \mod \mathfrak{p})$. We note that one of a_i's does not lie in $\mathfrak{m}_\mathfrak{p}$, and hence this tuple correspond to a $k(\mathfrak{p})-$point in $\mathbb{P}^n$ lying in $\mathcal{A}_\mathfrak{p}$.

(c) The two above examples show that the reduction can be described in concrete terms when the variety can be described by equations, so integral models are very useful to give a geometric framework for the notion of reduction. When $G = E$ is an elliptic curve, one can describe the reduction as follows. Because $\mathcal{O}_\mathfrak{p}$ is a DVR, we can find a minimal Weierstrass equation for E with respect to $\mathrm{ord}_\mathfrak{p}$, i.e., the equation with coefficients in $\mathcal{O}_\mathfrak{p}$ such that the $\mathrm{ord}_\mathfrak{p}$ of discriminant $\Delta(E)$ is the smallest non-negative integer:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Now we take reduction mod $\mathfrak{p}$ for every coefficient, we then get the reduction $E_\mathfrak{p}$ of E mod $\mathfrak{p}$, for any $\mathfrak{p}$. When $\mathrm{ord}_\mathfrak{p}(\Delta(E)) = 0$, we obtain the reduction mod $\mathfrak{p}$ of E as we described above. In this case, E has good reduction at $\mathfrak{p}$. Now for a point $R \in E(K) \subset \mathbb{P}^2(K)$, we can write $R = [a_0 : a_1 : a_2]$ such that $a_0, a_1, a_2 \in \mathcal{O}_\mathfrak{p}$ and one of a_0, a_1, a_2 in $\mathcal{O}_\mathfrak{p}^\times$. Taking reduction mod $\mathfrak{p}$ at each coordinate of R, we obtain a point R mod $\mathfrak{p}$ in $E_\mathfrak{p}$.

Extending The Base Field

We want to understand how reduction behaves under a finite field extensions L over a global field K. For G an algebraic group over K, we have $G(K) \subset G_L(L)$ where $G_L = G \times_K L$. Now G admits an integral model $\mathcal{G}$ over $\mathrm{Spec}\,\mathcal{O}_{K,S}$ for some S. Let

$\mathfrak{p} \notin S$ and $\mathfrak{q}$ is a place lying above $\mathfrak{p}$ in L. Consider the $\mathcal{O}_\mathfrak{p}$-model $\mathcal{G} \times_{\mathcal{O}_{K,S}} \mathcal{O}_\mathfrak{p}$ of G and look at its set of $\mathcal{O}_\mathfrak{p}$-points, denote $G(\mathcal{O}_\mathfrak{p})$. Then G_L also admits an $\mathcal{O}_\mathfrak{q}$-model $(\mathcal{G} \times_{\mathcal{O}_{K,S}} \mathcal{O}_\mathfrak{p})_{\mathcal{O}_\mathfrak{p}} \mathcal{O}_\mathfrak{q}$, and denote its set of $\mathcal{O}_\mathfrak{q}$-points $G(\mathcal{O}_\mathfrak{q})$. In addition, taking reduction of those models gives us algebraic groups $G_\mathfrak{p}$ over $k(\mathfrak{p})$ and $G_\mathfrak{q}$ over $k(\mathfrak{q})$. Furthermore, we have

$$G_\mathfrak{q} = G_\mathfrak{p} \times_{k(\mathfrak{p})} k(\mathfrak{q}).$$

Therefore we have a commutative diagram

$$\begin{array}{ccc} G_L(L) \supset G(\mathcal{O}_\mathfrak{q}) & \xrightarrow{\text{red mod } \mathfrak{q}} & G_\mathfrak{q}(k(\mathfrak{q})) \\ \uparrow & & \uparrow \\ G(K) \supset G(\mathcal{O}_\mathfrak{p}) & \xrightarrow{\text{red mod } \mathfrak{p}} & G_\mathfrak{p}(k(\mathfrak{p})) \end{array}$$

We note that for almost all $\mathfrak{p}$, all the maps are group homomorphisms. Thanks to this construction, we have

Lemma 1.4.3. *With above notation, let P be a $K-$point of G. Then for almost all primes $\mathfrak{p}$ of K, we have the order of P modulo $\mathfrak{q}$ is equal to the order of P modulo $\mathfrak{p}$.*

Proof. See [5] Lemma 1.2.3. □

Reduction of Morphisms

From the above discussion, we see that the map $[n]$ (of multiplication by n) commutes with taking reduction for almost all places $\mathfrak{p}$. In fact, it is true for any morphisms (resp. homomorphisms).

Proposition 1.4.4. *Let G and H be algebraic groups over a global field K, $f : G \to H$ over K and a morphism (resp. homomorphism). Then f induces a $k(\mathfrak{p})-$morphism (resp. homomorphism) $f_\mathfrak{p} : G_\mathfrak{p} \to H_\mathfrak{p}$ for almost all $\mathfrak{p}$.*

Proof. We lift f from K to some $\mathcal{O}_{K,S}$ by spreading out principal and then taking special fiber at $\mathfrak{p}$. □

It is then straightforward to check that

Corollary 1.4.5. *With the notation as above, let $R \in G(K)$. Then for almost all $\mathfrak{p}$, the order of $\phi(R)$ modulo $\mathfrak{p}$ in $H_\mathfrak{p}$ divides that of R modulo $\mathfrak{p}$ in $G_\mathfrak{p}$. In particular, when ϕ is an isomorphism, those orders are equal.*

Reductions of Torsion Points

Now we want to understand how reductions behave with torsion points. First we have

Proposition 1.4.6. *Let G be an extension of an abelian variety by a linear algebraic group over a global field K, and $R \in G(K)$ a non-zero point. Then for almost all $\mathfrak{p}$, R modulo $\mathfrak{p}$ is non-zero. In particular, this holds for semi-abelian varieties.*

Proof. First we see that it is true for linear algebraic groups because when a K-point $R = (a_1, ..., a_n)$ can be embedded in $\mathbb{A}^n$. Therefore the elements $a_1 - e_1, ..., a_n - e_n$, where $e = (e_1, ..., e_n)$, lie in only finitely many prime ideals. When G is an abelian vatiety, a $K-$point R (and e) can be lifted to a $\mathcal{O}_{K,S}$ for some S and then it corresponds to an $(n+1)-$tuple $[a_0 : ... : a_n]$ (and $[e_0 : ... : e_n]$) where $a_0, ..., a_n, e_0, ..., e_n \in \mathcal{O}_{K,S}$ and $a_0, ..., a_n$ (and $e_0, ..., e_n$) generate $\mathcal{O}_{K,S}$, and the result follows again because each of $a_1 - e_1, ..., a_n - e_n$ lies in only finitely many prime ideals. Now for general G, by assumption we have an exact sequence

$$1 \to G^{aff} \xrightarrow{f} G \xrightarrow{g} A \to 1.$$

Taking K-points induces an exact sequence

$$1 \to G^{aff}(K) \xrightarrow{f} G(K) \xrightarrow{g} A(K).$$

Now we suppose that there are infinitely many $\mathfrak{p}$ satisfying R modulo $\mathfrak{p}$ is trivial, then there are also infinitely many $\mathfrak{p}$ satisfying $g(R)$ modulo $\mathfrak{p}$ is zero. Thus, $g(R)$ is zero, and hence, R is a $K-$point in the affine part G^{aff}, which gives us a contradiction. □

Corollary 1.4.7. *For G as above, let Q and R be distinct $K-$points of G. Then there are only finitely many $\mathfrak{p}$ satisfying Q modulo $\mathfrak{p}$ equals R modulo $\mathfrak{p}$.*

Proof. We can take reduction of Q, R, $Q - R$, and e mod $\mathfrak{p}$. The result follows from the above proposition. □

Corollary 1.4.8. *For G as above, let $Q \in G(K)$ be non-torsion. Then for any $m > 0$, there are only finitely many $\mathfrak{p}$ such that R modulo $\mathfrak{p}$ has order m.*

Proof. If mR mod $\mathfrak{p} = 0$ for infinitely many $\mathfrak{p}$, then $mR = 0$, which is a contradiction. □

Corollary 1.4.9. *Let G be a semi-abelian variety over a global field K, then for almost all $\mathfrak{p}$, the map*

$$G(K)^{\text{tors}} \xrightarrow{\text{red}} G_{\mathfrak{p}}(k(\mathfrak{p}))$$

is injective. As a consequence, the order of a torsion point is equal to the order of its reduction mod $\mathfrak{p}$ *for almost all* $\mathfrak{p}$.

Proof. For the first claim, recall that there are only finitely many torsion points in $G(K)$, and then by discarding finitely many $\mathfrak{p}$, we have P and R have different orders when taking mod $\mathfrak{p}$ for any distinct points P, $R \in G(K)^{\text{tors}}$. For the second one, let n be the order of R, then nR modulo $\mathfrak{p} = 0$ for almost all $\mathfrak{p}$. If there exist $0 < m < n$ satisfying the order of R mod $\mathfrak{p}$ is m for infinitely many $\mathfrak{p}$, then $mR = 0$, a contradiction. From this we obtain the claim. □

Remark. In general, the map

$$G(K) \xrightarrow{\text{red}} G_{\mathfrak{p}}(k(\mathfrak{p}))$$

is not surjective. For example, consider an elliptic curve E over $\mathbb{Q}$ of rank 0, i.e., $E(\mathbb{Q})$ is finite. For instance, one can take E to be of the form $E : y^2 = x^3 + px$ where p is a prime such that $p \equiv 7$ or $11 \bmod 16$ as in [14] Chapter X, Corollary 6.2.1. The Hasse-Weil bound for elliptic curves give us the estimate

$$|E_q(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}$$

for almost all primes q. In particular, $|E_q(\mathbb{F}_q)|$ tends to infinity when q goes to infinity. Therefore, for sufficiently large q, the reduction map $E(\mathbb{Q}) \to E_q(\mathbb{F}_q)$ is not surjective. However, if we look at geometric points (not only rational points), the reduction maps are bijective at almost every place as follows.

Proposition 1.4.10. *With* G/K *as in Corollary 1.4.9 and any* $m > 0$*, the map*

$$G[m] \xrightarrow{\text{red}} G_{\mathfrak{p}}[m]$$

is an isomorphism for almost all $\mathfrak{p}$.

Proof. See [21] Lemma 4.4. □

1.5 Formal Groups

In this last section, we define the formal group associated to an algebraic group G over a field K. First we recall the notion of formal groups over a complete valuation ring R (i.e, a valuation ring which is complete with respect to the $\mathfrak{m}$-adic topology defined by the unique maximal ideal $\mathfrak{m}$). The references for this section are [22] Chapter III section 5, and [23] section C.2.

Definition 1.5.1. A commutative $R-$algebra A is called **profinite** if $A = \varprojlim A/\mathfrak{I}$ over a family of ideals $\mathfrak{I}$ such that $A/\mathfrak{I}$ is a finitely generated $R-$module.

Example 1.9. The power series $R[[X_1, ..., X_n]]$ is a profinite R-algebra and it is not finitely generated over R.

Definition 1.5.2. A **formal (group) scheme** is a representable functor on the category of profinite $R-$algebras to the category of sets (groups).

So for a profinite $R-$algebra A, we have a formal scheme $\mathrm{Spf}(A)$, the formal spectrum of A. If it is a formal group, then the group operations give rise to a comultiplication and an inversion

$$m^* : A \to A\hat{\otimes}A, i : A \to A.$$

Definition 1.5.3. A formal group G over R is said to be **smooth** if its connected component G^o is the formal spectrum of a power series ring over R. If in addition it is connected, it is called a **formal Lie group**. In other word, it is of the form $\mathrm{Spf}(R[[X_1, ..., X_n]])$, and n is called the dimension of this group.

We note that

$$R[[X_1, ..., X_n]]\hat{\otimes}_R R[[Y_1, ..., Y_m]] \cong R[[X_1, ..., X_n, Y_1, ..., Y_m]].$$

Therefore, to give $\mathrm{Spf}(R[[X_1, ..., X_n]])$ the structure of formal group, it amounts to giving n power series in $2n$ variables satisfying some conditions. Suppose that we have $F_1, ..., F_n \in R[[X_1, ..., X_n, Y_1, ..., Y_n]]$ and write $F = (F_1, ..., F_n)$, then the rules we require are

1. $F(X, F(Y, Z)) = F(F(X, Y), Z)$,
2. $F(X, 0) = F(0, X) = X$,
3. There exists a unique $i(X) = (i_1(X), ..., i_n(X))$ such that $F(X, i(X)) = F(i(X), X) = 0$.
4. $F(X, Y) = F(Y, X)$ if the group is commutative.

Here $X = (X_1, ..., X_n)$, similarly for Y and Z. In addition, the first two relations imply

$$F(X, Y) = X + Y + (\text{higher order terms}).$$

Therefore for each formal Lie group G, there exists a unique function F as above which gives rise to the group law on the coordinate ring of G, and vice versa, each function F satisfying those relations also gives rise to a formal Lie group. We call F a formal group law of dimension n on R.

Example 1.10. (a) The additive group $\mathbb{G}_a$ corresponds to $F(X,Y) = X + Y$.

(b) The multiplicative group $\mathbb{G}_m$ corresponds to $F(X,Y) = X + Y + XY$.

From this description, a $R-$homomorphism f between formal Lie group schemes G and G' of dimension n and n' respectively corresponds to a $n'-$tuple of formal power series without constant terms $f = (f_1, ..., f_{n'}), f_i \in R[[X_1, ..., X_n]]$ such that

$$F'(f(X), f(Y)) = f(F(X,Y)).$$

Additionally, f is an isomorphism if there is $f' = (f'_1, ..., f'_n), f'_i \in R[[X_1, ..., X_{n'}]]$ such that

$$f \circ f' = \mathrm{id}, f' \circ f = \mathrm{id}.$$

As in the case of group schemes, we have a endomorphism $[m]$ on G which is the multiplication-by-m map.

Lemma 1.5.4. *The homomorphism $[m]$ on G is an isomorphism if and only if m is a unit in R.*

Now we want to associate to algebraic groups G over a field K a formal Lie group F. Let $\hat{\mathcal{O}}_{G,e}$ denote the completion of the local ring $\mathcal{O}_{G,e}$ at the identity e with respect to its maximal ideal $\mathfrak{m}_e$. Sinve G is smooth and of finite type, it admits local parameters $x_1, ..., x_n$ ($n = \dim G$) and we have an isomorphism

$$\hat{\mathcal{O}}_{G,e} \cong K[[x_1, ..., x_n]].$$

In addition, the maps m and i on G give rise to maps of local rings

$$m^* : \mathcal{O}_{G,e} \to \mathcal{O}_{G\times G,(e,e)}, i^* : \mathcal{O}_{G,e} \to \mathcal{O}_{G,e}.$$

Taking completion both sides, we then have

$$F : K[[x_1, ..., x_n]] \to K[[x_1, ..., x_n, y_1, ..., y_n]], i : K[[x_1, ..., x_n]] \to K[[x_1, ..., x_n]].$$

Then we have a formal Lie group assciated to G at e, and the map F and i give us a formal group law over K, also denote by F. Now let $G = A$ be an abelian variety over the fraction field $K = \mathrm{Frac}(R)$ of a complete valuation ring $(R, \mathfrak{m})$ with its residue field k of characteristic p. In this case, the formal group is useful to understand the reduction map of abelian varieties. First we have

Lemma 1.5.5. *If A have good reduction at $\mathfrak{m}$ (i.e., A can be lifted to an abelian scheme $\mathcal{A}$ over R), then the associated formal group F is defined over R. Here, the formal group F is said to be defined over R if its coefficients are in R*

Proof. Because A has good reduction at $\mathfrak{m}$, its reduction abelian variety $\tilde{A}$ is an abelian variety. We let $x_1, ..., x_n$ be local parameters at e such that their reductions $\tilde{x}_1, ..., \tilde{x}_n$ are also local parameters of $\tilde{A}$ at $\tilde{e}$. Then the power series giving the group law on the formal Lie group associated to $\tilde{A}$ must be the reduction module $\mathfrak{m}$ of the power series corresponding to the formal Lie group associated to A. Therefore, the coefficients of the latter power series must lie in R. □

Definition 1.5.6. Let F be a formal group law of dimension n over a complete valuation ring $(R, \mathfrak{m})$. We denote $F(\mathfrak{m})$ the **group associated to** F, i.e., the set of n-tuples $\mathfrak{m}^n$ with the group law, in the usual sense,

$$\mathfrak{m}^n \times \mathfrak{m}^n \xrightarrow{+_F} \mathfrak{m}, (X, Y) \mapsto F(X, Y).$$

Because of the completeness of R, the series $F(X, Y)$ converges in $\mathfrak{m}$ for $X, Y \in \mathfrak{m}$.

Proposition 1.5.7. *With these above notations, the group $F(\mathfrak{m})$ has no prime-to-p torsion.*

Proof. For an integer m prime to p, $[m]X = mX + ...$ has an inverse $m^{-1}X + ...$ since $m \in R^\times$. When applying to $\mathfrak{m}^g$ where $g = \dim F$, we have an automorphism of $F(\mathfrak{m})$, and hence, the multiplication-by-m map has trivial kernel. □

Proposition 1.5.8. *Let A/K be an abelian variety having good reduction at $\mathfrak{m}$, and we let*

$$A_1(K) := \ker(A(R) \xrightarrow{\text{red}} A_{\mathfrak{m}}(k)).$$

Here $A_{\mathfrak{m}}$ is the reduction of A at $\mathfrak{m}$. Let F be a formal group of A at e, then

$$F(\mathfrak{m}) \cong A_1(K).$$

Proof. We refer to [23] Theorem C.2.6 for the proof. □

Because the reduction map $A(R) \to A_{\mathfrak{m}}(k)$ is surjective (since the complete valuation ring is henselian and A is smooth, so one can lift maps from $\operatorname{Spec} k \to A$ to maps from $\operatorname{Spec} R \to A$ via Hensel's lemma), we have an exact sequence

$$0 \to A_1(K) \to A(R) \to A_{\mathfrak{m}}(k) \to 0.$$

If K is a local field with R its ring of integer and $\mathfrak{m}$ its unique maximal ideal, we note that the group $A(K)$ is profinite because

$$A(K) = A(R) = A(\varprojlim R/\mathfrak{m}^i) = \varprojlim A(R/\mathfrak{m}^i)$$

With those results, we have a quite stronger claim compared to Corollary 1.4.9

Corollary 1.5.9. *Let A be an abelian variety over a global field K. Suppose that A has good reduction at some finite place v. Let k_v be the residue field at v whose characteristic is p. Then for any $m > 1$ prime to p, the reduction map on the $m-$torsion $K-$points of A*

$$A(K)[m] \xrightarrow{\text{red}} A_{\mathfrak{m}}(k_v)$$

is injective.

Proof. Because $F(\mathfrak{m})$ has no prime-to-p torsion, $A_1(K)[m] = F(\mathfrak{m})[m] = 0$. □

When $A = E$ is an elliptic curve over the fraction field of a complete valuation ring $(R, \mathfrak{m})$, we can describe the map in Proposition 1.5.8 explicitly as follows (see [14] Chapter VII.2). Assume E satisfies a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and we want to investigate the structure of E close to the origin and its addition law around the origin. So we let $z = -\dfrac{x}{y}$ (so z is a local coordinate, and also a uniformizer at O because O is its zero of order 1), and $w = -\dfrac{1}{y}$, then we have

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3$$

and keep substituting this equation into itself, we have

$$w = z^3(1 + A_1z + A_2z^2 + ...),$$

where $A_i \in \mathbb{Z}[a_1, ..., a_6]$. This procedure must converge due to Hensel's lemma. So we have just seek a solution $(z, w(z))$ to the Weierstrass equation where $w(z) \in \mathbb{Z}[a_1, ..., a_6][[z]]$. We then have

$$x(z) = \frac{z}{w(z)}, y(z) = -\frac{1}{w(z)}.$$

In addition, to get the formal group law F on E at O, we formally compute the w-coordinate of $(x_1, y_1) + (x_2, y_2)$ using these above power series, and similarly for the inversion. We then have

$$F(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) + ...$$

In this case, Proposition 1.5.8 can be described as follows.

Proposition 1.5.10. *Let the notation be as above. Suppose that E have good reduction at $\mathfrak{m}$, then*

$$F(\mathfrak{m}) \to E_1(K), z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right),$$

is isomorphic. Here, the map sends $z = 0$ to O.

Chapter 2

Height Functions and Diophantine Geometry

The main references for this chapter are [14] and [24]. In the chapter, we present

1. Height functions,

2. Some applications of heights in Diophantine Geometry.

2.1 Height Functions

Height functions are tools to determine the size of a point. It, in some sense, reflects both local and global behaviors of the point. We will define height function over arbitrarily global fields. The main reference is [14] Chapter III. Although this book only deal with number fields, the results below also hold for global function fields. First, we recall that for a tower of number fields $L/K/\mathbb{F}$, and $v \in M_K$ we have the extension formula

$$\sum_{w \in M_L, w|v} N_w = [L : K] N_v.$$

(Here $w|v$ means that w is an extension of v to L.)

Definition 2.1.1. Let K be a global field, and $P \in \mathbb{P}^n(K)$ be a point with

$$P = [x_0 : ... : x_n], \ x_0, ..., x_n \in K.$$

The (relative to K) **height** of P is

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, ..., |x_n|_v\}.$$

Proposition 2.1.2. *For $P \in \mathbb{P}^n(K)$, we have*

1. *$H_K(P) \geqslant 1$.*

2. *Let L/K be a finite extension. Then*

$$H_L(P) = H_K(P)^{1/[L:K]}.$$

Proof. It is a direct corollary of the extension formula and the product formula. □

This result motivates us to define an absolute height, which does not depend on the field.

Definition 2.1.3. Let $P \in \mathbb{P}^n(\bar{\mathbb{F}})$. We choose a global field K such that $P \in \mathbb{P}^n(K)$. Then the **absolute height** of P is

$$H(P) := H_K(P)^{1/[K:\mathbb{F}]},$$

and the **logarithmic height** (or **Weil height**) of P is

$$h(P) := \log H(P).$$

Theorem 2.1.4. *(Northcott) Let C and d be constants. Then the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{F}}) : H(P) \leqslant C \text{ and } [\mathbb{F}(P) : \mathbb{F}] \leqslant d\}$$

is finite.

Proof. We remark that the proof in the global function field case is harder due to the non-separability of field extensions. We refer to [24] Theorem 10.1.6 for the proof. □

2.1.1 Heights on Elliptic Curves

Definition 2.1.5. Let E be an elliptic curve ove a global field K, and $f \in \bar{K}(E)$. The **height** of E (relative to f) is defined to be

$$h_f : E(\bar{K}) \to \mathbb{R}, h_f(Q) := h(f(Q)),$$

where h is the Weil height.

We have the following results about heights (see [14] VIII.6). Although those results are stated for number fields there, their proofs still hold in global function fields.

Proposition 2.1.6. *Let $f \in \bar{K}(E)$ be non-constant. Then for any C*

$$\{Q \in E(K) : h_f(Q) \leqslant C\}$$

is finite.

We recall that a function $f \in E(K)$ is **even** if $f \circ [-1] = f$.

Proposition 2.1.7. *For $f \in E(K)$ an even function, and for all $Q, R \in E(\bar{K})$ we have*

$$h_f(Q+R) + h_f(Q-R) = 2h_f(Q) + 2h_f(R) + O(1).$$

Here $O(1)$ depends only on E/K and f.

Lemma 2.1.8. *For $f, g \in K(E)$ even*

$$(\deg g)h_f = (\deg f)h_g + O(1).$$

Corollary 2.1.9. *Let $f \in K(E)$ be even.*

1. *Let $Q \in E(\bar{K})$. Then*

$$h_f(Q+R) \leqslant 2h_f(R) + O(1), \forall R \in E(\bar{K}).$$

Here $O(1)$ depends only on $E, f,$ and Q.

2. *Let $m \in \mathbb{Z}$. Then*

$$h_f([m]Q) = m^2 h_f(Q) + O(1), \forall Q \in E(\bar{K}).$$

Here $O(1)$ depends only on $E, f,$ and m.

Example 2.1. Let us experiment with two examples.

(a) Consider a $\mathbb{Q}-$point $Q = (3, 5)$ on $E/\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 - 2$, see [25] section 7.

Table 2.1: Heights of Points on $y^2 = x^3 - 2$ over $\mathbb{Q}$.

n	$h_x(nQ)$ (to nearest .1)
1	1.1
2	4.9
3	12.0
4	21.6
5	33.4
6	48.1
7	66.1
8	86.3

(b) Consider a $\mathbb{F}_5(t)-$point $Q = (t+2, 3t+3)$ on $E/\mathbb{F}_5(t)$ with Weierstrass equation $y^2 = x^3 - t^2x + (t+1)$.

Table 2.2: Heights of Points on $y^2 = x^3 - t^2x + (t+1)$ over $\mathbb{F}_t(t)$.

n	$h_x(nQ)$
1	1
2	4
3	9
4	14
5	25
6	36
7	49
8	64

Evidently, $h_x(nQ)$ grows roughly quadratically in n. So one hopes that by letting n tend to ∞, we obtain a "more canonical" height function. More precisely, we have the following results (for the proofs of those results for number fields, we refer to [14] Chapter VIII.9, and we note that those proofs work well for the global function fields).

Proposition 2.1.10 (Tate's theorem)**.** *Let f be a non-constant even function on an elliptic curve E/K, and $Q \in E(\bar{K})$. Then the limit*

$$\frac{1}{\deg f} \lim_{N\to\infty} \frac{h_f([2^N]Q)}{4^N}$$

exists and is independent of f.

Definition 2.1.11. The **canonical height** on E, denoted $\hat{\mathbf{h}}$, is the function

$$\hat{\mathbf{h}} : E(\bar{K}) \to \mathbb{R}, Q \mapsto \frac{1}{\deg f} \lim_{N\to\infty} \frac{1}{4^{-N}} h_f([2^N]Q)$$

for some f non-constant even (e.g. the function x when E is given by the normal form).

Theorem 2.1.12 (Néron-Tate, see [14] Theorem 9.3)**.** *With above notations, we have*

1. *For all $Q, R \in E(\bar{K})$ we have*

$$\hat{\mathbf{h}}(Q+R) + \hat{\mathbf{h}}(Q-R) = 2\hat{\mathbf{h}}(Q) + 2\hat{\mathbf{h}}(R)$$

2. *For all $Q \in E(\bar{K})$ and all $n \in \mathbb{Z}$,*

$$\hat{\mathbf{h}}([n]Q) = n^2\hat{\mathbf{h}}(Q).$$

3. $\hat{\mathbf{h}}$ *is a quadratic form on* $E(\bar{K})$.

4. *Let* $Q \in E(\bar{K})$. *Then* $\hat{\mathbf{h}}(Q) \geqslant 0$, *and*

$$\hat{\mathbf{h}}(Q) = 0 \text{ if and only if } Q \text{ torsion.}$$

5. *For even* $f \in K(E)$

$$(\deg f)\hat{\mathbf{h}} = h_f + O(1).$$

Here $O(1)$ *depends only on* E *and* f.

´

Corollary 2.1.13. *The canonical height* $\hat{\mathbf{h}}$ *induces a symmetric bilinear form* $<,>$: $E(K) \times E(K) \to \mathbb{R}$

$$< Q, R >= \hat{\mathbf{h}}(Q + R) - \hat{\mathbf{h}}(Q) - \hat{\mathbf{h}}(R)$$

such that

1. $< Q, Q > \geqslant 0$ *for all* $Q \in E(K)$, *and*

2. $\{Q \in E(K) :< Q, Q >< C\}$ *is finite for all* $C > 0$.

2.1.2 Roth's Theorem

Roth's theorem plays an important role in Diophantine approximation. Over number fields, it is stated as follows, see [14] Chapter IX, Theorem 1.4.

Theorem 2.1.14. *Let* K *be a number field. Let* $\epsilon > 0$, *let* $\alpha \in \bar{K}$, *and let* $v \in M_K$ *that extend to* $K(\alpha)$ *in some way. Then for any constant* C, *there exist only finitely many* $x \in K$ *satisfying*

$$|x - \alpha|_v < C.H_K(x)^{-2-\epsilon}. \tag{2.1}$$

Remark. Even more, Lang has established a general version of Roth's theorem.

Theorem 2.1.15. *Let* K *be a number field, and* S *be a finite set of non-Archimedean places of* K. *For each* $v \in S$, *let* $\alpha_v \in K_v$ *be algebraic over* K. *We fix a real number* $\kappa > 2$. *Then there are only finitely many* $x \in K$ *satisfying*

$$\prod_{v \in S} \min(1, |x - \alpha_v|_v) \leqslant H_K(x)^{-\kappa}.$$

Proof. We refer to [26] Chapter 6. □

Remark. Over function fields, there is a counter example showing that Theorem 2.1.15 does not hold, which is due to Mahler (see [26] example 6.2.8). The obstruction in this counter example is α_v lying in an extension of K of degree p. So, to obtain a version of 2.1.15 for global function fields, one has to discard elements lying in a cyclic extension of K of degree a power of p. In fact, by slightly modifying the proof of Theorem 2.1.15, J. V. Armitage proved the following theorem, see [4].

Theorem 2.1.16. *Let K be a global function field of characteristic p, and S a finite subset of M_K. For each $v \in S$, let α_v be K-algebraic and assume that v is extended in some way to the algebraic closure $\overline{K}$. Let ϵ be any positive number. Then if none of the α_v lies in a cyclic extension of degree a power of p over K, the elements $x \in K$ satisfying the approximation condition*

$$\prod_{v \in S} \inf(1, |\alpha_v - x|_v) < H_K(x)^{-2-\epsilon},$$

have bounded height. In particular, there are only finitely many of them.

Remark. Thanks to this theorem, now we are able to obtain the classical result of Roth for global function fields

Corollary 2.1.17. *Let K be a global function field of characteristic p. Let $\epsilon > 0$, and $\alpha \in \bar{K}$ which does not lie in any cyclic extension of degree a power of p, and let $v \in M_K$. Then for any $C > 0$, there exist only finitely many $x \in K$ satisfying the approximation condition*

$$|x - \alpha|_v < C.H_K(x)^{-2-\epsilon}. \tag{2.2}$$

Proof. We first fix a positive number $\epsilon_1 \in (0, \epsilon)$ and let $\epsilon_2 := \epsilon - \epsilon_1$. Let x be an element satisfying (2.2). If $C.H_K(x)^{-\epsilon_1} > 1$ then

$$H_K(x) < C^{1/\epsilon_1}$$

which is bounded. Otherwise, x then satisfies

$$|x - \alpha|_v < H_K(x)^{-2-\epsilon_2}.$$

- If $|x - \alpha|_v \geqslant 1$, then $1 < H_K(x)^{-2-\epsilon_2}$ and hence

  $$H_K(x) < 1.$$

- If $|x - \alpha|_v \leqslant 1$, then

  $$\inf(1, |\alpha - x|_v) < H_K(\beta)^{-2-\epsilon_2}$$

  Apply the above theorem for $S = \{v\}$ and $\alpha_v = \alpha$, we deduce that the height of x must be bounded.

Thus, these elements x's satisfying (2.2) have bounded height, and hence we conclude the corollary. □

2.2 Some Applications in Diophantine Geometry

2.2.1 Mordell-Weil Theorem

We follows [14] Chapter XIII and [24] Lecture 10. We aim to prove

Theorem 2.2.1 (Mordell–Weil theorem)**.** *Let E/K be an elliptic curve over a global field K. Then $E(K)$ is finitely generated.*

To prove this theorem, we need a weaker version, Weak Morell-Weil Theorem, and the Descent Theorem which is based on the height function h_f. The Mordell-Weil theorem also holds for abelian varieties over global fields. While Weak Morell-Weil Theorem for abelian varieties are proven similarly, height functions on abelian varieties are hard to construct, so we will not give details here. In fact, the construction is the main goal of A. Weil's thesis, and we refer to [24] Lecture 10 for more details.

Weak Mordell-Weil Theorem

Theorem 2.2.2 (Weak Mordell–Weil theorem)**.** *Let A/K be an abelian variety over a global field K. Then the group $A(K)/m.A(K)$ is finite for all integers m coprime to p. In particular, the group $E(K)/m.E(K)$ is finite for all integer m coprime to p.*

Remark. The main idea is to realize $A[m]$ as a subgroup of an appropriate cohomology group which is finite. First we have an exact sequence $K-$group scheme

$$0 \to A[m] \to A \xrightarrow{.m} A \to 0.$$

Here we consider $A[m]$ as a finite group scheme. We claim that taking K^s-points we obtain a short exact sequence of discrete $\Gamma = \mathrm{Gal}(K^s/K)$-modules

$$0 \to A[m](K^s) \to A(K^s) \xrightarrow{.m} A(K^s) \to 0.$$

The only non-trivial point here is the surjectiveness of the last arrow. Let $a \in A(K^s)$, we have a pullback diagram

$$\begin{array}{ccc} E & \longrightarrow & \operatorname{Spec} K^s \\ \downarrow & & \downarrow a \\ A & \xrightarrow{m} & A \end{array}$$

Since $m \in K^\times$, $[n]$ is a finite étale cover. Therefore, the morphism $E \to \operatorname{Spec} K^s$ is a finite étale cover too, and hence split since K^s is separable. So E admits a K^s-point, i.e., the last morphism is surjective. Applying Galois cohomology $H^*(\Gamma, \cdot)$, we obtain a long exact sequence

$$0 \longrightarrow A[m](K) \longrightarrow A(K) \xrightarrow{m} A(K) \longrightarrow H^1(\Gamma, A[m])$$

Thus $A(K)/mA(K)$ injects to $H^1(\Gamma, A[m])$, but the latter group is not finite. The main reason is that the group $K^\times$ is very large. To obtain the finiteness, we will need an "integral version" of K like $\mathcal{O}_S^\times$. Thus, we need to lift A to an abelian scheme $\mathcal{A}$ over $\mathcal{O}_S$, and because the base is no longer a field, so we need a more general version of Galois cohomology for schemes over any base, which is étale cohomology. For more details on etale cohomology, we refer to [8] section 6.4.

Proof of Theorem 2.2.2. First we spread out $A \to \operatorname{Spec} K$ to get an abelian scheme $\mathcal{A} \to U$, where $U := \operatorname{Spec} \mathcal{O}_S$ for some finite set $S \subset M_K$ containing all the Archimedean places m and $|A[m](K^s)|$ are S-units. Because $\mathcal{O}_S$ is Dedekind, the valuative criterion (see [8] Theorem 3.2.13) gives us $\mathcal{A}(K) = \mathcal{A}(U)$, and hence $A(K)/mA(K) = \mathcal{A}(U)/m\mathcal{A}(U)$. One has a similar exact sequence in étale topology on U

$$0 \to \mathcal{A}[m] \to \mathcal{A} \xrightarrow{\cdot m} \mathcal{A} \to 0.$$

(Since m is invertible in U, $[m]$ is an étale surjection on every geometric fiber, it then is an etale surjection). So we have a long exact sequence

$$0 \longrightarrow \mathcal{A}[m](U) \longrightarrow \mathcal{A}(U) \xrightarrow{m} \mathcal{A}(U) \longrightarrow H^1_{\text{et}}(U, \mathcal{A}[m])$$

which yields an injection

$$\mathcal{A}(U)/m\mathcal{A}(U) \hookrightarrow H^1_{\text{et}}(U, \mathcal{A}[m]).$$

Further, the diagram

$$\begin{array}{ccc} \mathcal{A}(U)/m & \hookrightarrow & H^1_{\text{et}}(U, \mathcal{A}[m]) \\ \| & & \downarrow \\ A(K)/m & \hookrightarrow & H^1(\Gamma, A[m]) \end{array}$$

is commutative, where the right arrow is induced by $\operatorname{Spec} K \to U$.

Claim. The image of $A(K)/mA(K)$ in $H^1(\Gamma, A[m])$ is contained in the subgroup of ξ unramified outside S; i.e., $\xi|_{I_u} \in H^1(I_u, A[m])$ is trivial for all $u \notin S$.

Here, for such u, the inertia group I_u is defined as follows. The first approach is to view I_u as $\mathrm{Gal}(K_u^s/K_u^{\mathrm{unr}})$ where K_u is the completion of K at u and K_u^{unr} is the maximal unramified extension. This group injects into $\mathrm{Gal}(K_u^s/K)$ and hence Γ by restriction. One has another way to define I_u is to view it as as the absolute Galois group of $F_u := \mathrm{Frac}(\mathcal{O}_{U,u}^{\mathrm{sh}})$, where $\mathcal{O}_{U,u}^{\mathrm{sh}}$ is the strict henselization of $\mathcal{O}_{U,u}$. Here we note that the equivalence between these approaches follows from the contruction of $\mathcal{O}_{U,u}^{\mathrm{sh}}$ which is henselian with the residue field $\kappa(u)^s$ satisfying universally strictly henselian property. So the diagram

$$\begin{array}{ccc} \mathcal{A}(U)/m & \hookrightarrow & H^1_{\mathrm{et}}(U, \mathcal{A}[m]) \\ \| & & \downarrow \\ A(K)/m & \hookrightarrow & H^1(\Gamma, A[m]) \\ \downarrow & & \downarrow \mathrm{Res} \\ \mathcal{A}(F_u)/m & \longrightarrow & H^1(I_u, A[m]) \end{array}$$

commutes. So it suffices to show that $[m] : \mathcal{A}(F_u) \to \mathcal{A}(F_u)$ is surjective. Via the identification $\mathcal{A}(F_u) = \mathcal{A}(\mathcal{O}_{U,u}^{\mathrm{sh}})$, we can prove this in a similar way as above (note that since $\mathrm{Spec}\, \mathcal{O}_{U,u}^{\mathrm{sh}}$ is strictly henselian, any finite étale cover is split over $\mathrm{Spec}\, \mathcal{O}_{U,u}^{\mathrm{sh}}$. Then we obtain the claim.

Now we note that

Claim. The $\Gamma-$module $A[n](K^s)$ is unramified at all $u \notin S$, i.e., the action of the inertia group I_u is trivial, since A has good reduction at such u.

Therefore, we have reduced the proof of the finiteness to the following claim

Claim. Let K be a global field, and $S \subset M_K$ a finite set containing all the Archimedean places. Let M be a finite Γ-module such that $m := |M| \in \mathcal{O}_S^\times$. We suppose further that M is unramified outside S. Then

$$H^1_S(K, M) := \{\xi \in H^1(K, M) : \xi \text{ is unramified outside } S\}$$

is finite.

We first note that one may assume that $\mu_m \subset K$, $M = \mu_d$ as $\Gamma-$modules for some $d|m$, and the places of K which divide m are contained in S. Indeed, there exists a finite Galois extension K' of K containing μ_m such that $\Gamma' := \mathrm{Gal}(K^s/K')$ acts trivially on M. By the hypothesis of m, the $m-$th root of unities are unramified outside places dividing m. Since enlarging S increases the size of $H^1_S(K, M)$, we may assume that S contains those places of K which divide m. We denote S' the set of places of K' above places in S. Then we have the inflation-restriction sequence

$$0 \longrightarrow H^1(K'/K, M) \xrightarrow{\text{Inf}} H^1(K, M) \xrightarrow{\text{Res}} H^1(K', M)$$

satisfying $\text{Res}(H^1_S(K, M)) \subset H^1_{S'}(K', M)$ (since for each $u \notin S$, $u'|u$, if the element $\xi_u \in H^1(I_u, M) = \text{Hom}(I_u, M)$ is 0, then $\xi_u|_{I_{u'}} : I_{u'} \hookrightarrow I_u \to M$ is 0 too). Because $H^1(K'/K, M)$ is finite, we want that $H^1_{S'}(K', M)$ is finite. Since we have isomorphisms between Γ'-modules

$$M \cong \prod(\mathbb{Z}/d_i\mathbb{Z}) \cong \prod \mu_{d_i}$$

for various integers $d_i|n$, we need to prove that $H^1_{S'}(K', \mu_d)$ is finite. So we can assume $K = K'$, $S = S'$, and $M = \mu_d$. We increase S more so that $h_{K,S} = |\text{Pic}_S(K)| = 1$ (we can do this since $\text{Pic}_S(K)$ is finite). In addition, Kummer theory gives us an isomorphism

$$K^\times/(K^\times)^d \xrightarrow{\sim} H^1(K, \mu_d) = \text{Hom}(\Gamma, \mu_d), [c] \mapsto \xi_c := \left(\xi_c(\sigma) = \frac{\sigma(c)}{c}\right).$$

We note that ξ_c is unramified at $u \notin S$ iff $\sigma(c) = c\ \forall \sigma \in I_u$, i.e., $K(\sqrt[d]{c})/K$ is unramified at u which is equivalent to $d|\,\text{ord}_u(c)$ (by considering the equation $X^d - c$ over K_u with discriminant $\pm d^d.c^{d-1}$). So the set $H^1_S(K, \mu_d)$ is in a bijective correspondence to

$$T_S := \{c \in K^\times/(K^\times)^d : \text{ord}_u(c) \equiv 0 \bmod m, \forall u \notin S\}.$$

Furthermore, we have an isomorphism

$$\mathcal{O}^\times_{K,S}/(\mathcal{O}^\times_{K,S})^d \to T_S$$

which is induced from a natural map

$$\iota : \mathcal{O}^\times_{K,S} \to T_S.$$

Indeed, suppose $c \in K^\times$ represents an element of T_S. Then $c\mathcal{O}_{K,S}$ is the dth power of an ideal in $\mathcal{O}^\times_{K,S}$. Since $\mathcal{O}_{K,S}$ is a PID, there exists $b \in K^\times$ satisfying $c\mathcal{O}_{K,S} = b^d\mathcal{O}_{K,S}$. Hence $\exists a \in \mathcal{O}^\times_{K,S}$ satisfying

$$c = a.b^d,$$

i.e., $a = c$ in T_S, which means ι is surjective. Clearly $\ker \iota$ contains $(\mathcal{O}^\times_{K,S})^d$. Using the above argument and comparing ord_u of both sides, it is evident that $\ker \iota = (\mathcal{O}^\times_{K,S})^d$. So we have the desired isomorphism. Since $\mathcal{O}^\times_{K,S}/(\mathcal{O}^\times_{K,S})^d$ is finite by Theorem 1.1.5 and Corollary 1.1.9, we obtain the finiteness of T_S, and hence of $H^1_S(K, \mu_d)$. Therefore, the finiteness of $A(K)/mA(K)$ follows.

□

Descent Theorem

Next, we need the descent theorem, see [24] Lemma 9.2.1 and [14] Chapter VIII Theorem 3.1.

Theorem 2.2.3. *Let A be an abelian group such that A/mA is finite for some $m > 1$. Suppose that there exists a symmetric bilinear form $<,>: A \times A \to \mathbb{R}$ satisfying*

1. $< a, a > \geqslant 0$ *for all* $a \in A$, *and*
2. $\{a \in A :< a, a >< C\}$ *is finite for all* $C > 0$

Then A is finitely generated.

Proof. We define $||a|| = \sqrt{< a, a >}$ and call it the radius of a, and let $\{a_1, .., a_n\}$ be representatives of A/mA. We choose $C > \max_i ||a_i||$.

Claim. If $||a|| \leqslant 2C$, then $||a - a_i|| \leqslant (3/2)$ for all i.

Indeed, we have

$$||a - a_i||^2 =< a - a_i, a - a_i >=< a, a > -2 < a, a_i > + < a_i, a_i > .$$

The Cauchy-Schwarz inequality gives us $| < a, a_i > | \leqslant ||a||.||a_i||$. So we have

$$||a - a_i||^2 \leqslant ||a||^2 + ||a_j||.(2||a|| + ||a_j||).$$

Since $||a_i|| \leqslant C \leqslant \frac{1}{2}||a||$, so we have the desired result

$$||a - a_i||^2 \leqslant ||a||^2 + \frac{1}{2}||a||\left(2||a|| + \frac{1}{2}||a||\right) = \frac{9}{4}||a||^2.$$

Now we will prove that A is generated by a_i and elements of A of radius less than $2C$. Let $a \in A$ such that $||a|| \geqslant 2C$. There exists some a_i such that $a - a_i = ma'$ for some $a' \in A$. Then

$$m.||a'|| = ||a - a_i|| \leqslant \frac{3}{2}||a||.$$

Hence,

$$||a'|| \leqslant \frac{3}{2m}||a||.$$

So we keep discarding a_i's until reaching a point lying in the ball of radius $2C$. Since this ball contains only finitely many points, A must be finitely generated. □

Combining Corollary 2.1.13, Theorem 2.2.2, and Theorem 2.2.3, $E(K)$ is finitely generated. In fact, $A(K)$ is also finitely generated for any abelian variety A over a global field K. We note that $T(\mathcal{O}_{K,S})$ is also finitely generated for any torus T over K due to the Dirichlet's finiteness theorem. Therefore, we obtain

Corollary 2.2.4. *Let $\mathcal{G}$ be an algebraic group over $U = \operatorname{Spec} \mathcal{O}_{K,S}$ (for some set of finitely many non-Archimedean places S) whose generic fiber $\mathcal{G}_K$ is semi-abelian. Then $\mathcal{G}(U)$ is finitely generated.*

Proof. We can lift the exact sequence associating to $\mathcal{G}_K$ to an exact sequence of group scheme over some small enough open subscheme $V \subset U$, i.e., we have

$$1 \to \mathcal{T} \to \mathcal{G}_{|V} \to \mathcal{A} \to 1$$

for some torus $\mathcal{T}$ and abelian scheme $\mathcal{A}$ over V. Taking V-points yields an exact sequence

$$1 \to \mathcal{T}(V) \to \mathcal{G}_{|V}(V) \to \mathcal{A}(V)$$

Since $\mathcal{T}(V)$ is finitely generated, and by the valuative criterion, $\mathcal{A}(V) = \mathcal{A}(K)$ is also finitely generated. Therefore, $\mathcal{G}(V) = \mathcal{G}_{|V}(V)$ is finitely generated. In addition, since

$$\mathcal{G}(U) \subset \mathcal{G}(V) \bigcup_{\mathfrak{p} \in V \setminus U} \mathcal{G}(k(\mathfrak{p})),$$

we need to show that $\mathcal{G}(k(\mathfrak{p}))$ is finitely generated. Indeed, we first cover $\mathcal{G}$ by finitely many affine opens $\mathcal{G}_i$. Since each point $\mathcal{G}(k(\mathfrak{p}))$ lies in only one of $\mathcal{G}_i$'s, we need that $\mathcal{G}_i(k(\mathfrak{p}))$ be finitely generated. Since $\mathcal{G}_i$ is of finite type over U, it is of the form $\mathcal{G}_i = \operatorname{Spec} \mathcal{O}_{K,S}[x_1, ..., x_n]/I$. Then $\mathcal{G}_i(k(\mathfrak{p}))$ is the set of ring homomorphisms $\mathcal{O}_{K,S}[x_1, ..., x_n]/I \to k(\mathfrak{p})$ compatible with the projection $\mathcal{O}_{K,S} \twoheadrightarrow k(\mathfrak{p})$, which is clearly finite. We then obtain the result.

□

2.2.2 Distance Function

In this section, we follow [14] Chapter IX. Here K is a global field of characteristic p.

Definition 2.2.5. Let C be a smooth projective curve over K. For P and Q in $C(K_v)$, we choose $t_Q \in K_v(C)$ which has a zero of order e, for some positive integer e, at Q and no other zeros. The **v-adic distance from P to Q** is then defined to be

$$d_v(P, Q) = \min \left\{ |t_Q(P)|_v^{1/e}, 1 \right\}.$$

Here, if t_Q has a pole at P, we let $|t_Q(P)| = \infty$, and so $d_v(P, Q) = 1$. In addition, P is called to be $v-$adically convergent to Q if $d_v(P, Q) \to 0$.

Remark. 1. We note that t_Q exists due to the Riemann-Roch theorem over K_v. Indeed, if g is the genus of C, and $e \geqslant g+1$, the $K_v-$the vector spaces $\mathcal{L}(e(Q)) :=$

$\{f \in K_v(C)^\times : \mathrm{div}(f) \geqslant -e(Q)\} \cup \{0\}$ has dimension at least $\deg(e(Q)) + 1 = 2$. Therefore, there is a non-constant function $f \in K_v(C)$ whose only pole is Q, and we take $t_Q = \dfrac{1}{f}$.

2. This distance function does not give rise to a topology on $C(K_v)$, it works in the sense that it measures $v-$adically the distance from P to the fixed point Q.

3. When $C = \mathbb{P}^1$, it is given by

$$d_v([x_0 : x_1], [y_0 : y_1]) = \frac{\max\{|x_i y_j - x_j y_i|_v\}}{(\max_i\{|x_i|_v\} \max_j\{|y_j|_v\})}.$$

4. For more geometric interpretations on distance functions, we refer to [27] section 2.

The following results are proved exactly in the same way as in [14], although in this book, the author only deals with number fields.

Proposition 2.2.6 (see [14], Proposition IX.2.2.)**.** *Let $Q \in C(K_v)$, and $f \in K_v(C)$ a function vanishing at Q. Then*

$$\lim_{\substack{P \in C(K_v) \\ P \xrightarrow{v} Q}} \frac{\log |f(P)|_v}{\log d_v(P, Q)} = \mathrm{ord}_Q(f)$$

exists.

Proposition 2.2.7. *Let $\phi : C_1 \to C_2$ be a finite map between smooth projective curves over K. Let $Q \in C_1(K_v)$. Then*

$$\lim_{\substack{P \in C_1(K_v) \\ P \xrightarrow{v} Q}} \frac{\log d_v(\phi(P), \phi(Q))}{\log d_v(P, Q)} = e_\phi(Q),$$

the ramification index of ϕ at Q.

Corollary 2.2.8. *Let $v \in M_K$, let $f \in K(C)$ be non-constant, and $Q \in C(\bar{K})$ such that $f(Q)$ does not lie in any cyclic extension of degree power of p. Then*

$$\liminf_{\substack{P \in C(K_v) \\ P \xrightarrow{v} Q}} \frac{\log d_v(P, Q)}{\log H_K(f(P))} \geqslant -2.$$

Proof. We can assume that $f(Q) \neq \infty$ (otherwise, replace f by $\dfrac{1}{f}$, the height does not change). So Q is a zero of $f - f(Q)$ of order $e \geqslant 1$. So we have

$$\lim_{\substack{P \in C(K_v) \\ P \xrightarrow{v} Q}} \frac{\log |f(P) - f(Q)|_v}{\log d_v(P, Q)} = e.$$

Therefore

$$\liminf_{\substack{P\in C(K_v)\\ P\xrightarrow{v}Q}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} = \liminf_{\substack{P\in C(K_v)\\ P\xrightarrow{v}Q}} \frac{\log |f(P)-f(Q)|_v}{e\log H_K(f(P))}.$$

For arbitrary $\epsilon > 0$, Proposition 2.1.17 gives us

$$|f(P)-f(Q)|_v \geqslant H_K(f(P))^{-2-\epsilon}$$

for almost all $P \in C(K)$. Hence

$$\frac{\log |f(P)-f(Q)|_v}{e\log H_K(f(P))} \geqslant \frac{-2-\epsilon}{e} > -2.$$

From this we obtain the claim. □

Now we prove a version of an important theorem of Siegel. We need to modify the proof for number fields as in [14] Theorem IX.3.1 a little bit. First we consider $f = x \in K(E)$ which is an even non-constant function.

Proposition 2.2.9. *Let E/K be an elliptic curve with $\#E(K) = \infty$, $Q \in E(K)$, and a valuation $v \in M_K$. Then*

$$\lim_{\substack{P\in E(K)\\ h_f(P)\to\infty}} \frac{\log d_v(P,Q)}{h_f(P)} = 0.$$

Proof. First we there exists a sequence of $K-$points $P_1, P_2, \ldots$ of E such that

$$\lim_{i\to\infty} \frac{d_v(P_i,Q)}{h_f(P_i)} = \lim_{\substack{P\in E(K)\\ h_f(P)\to\infty}} \frac{\log d_v(P,Q)}{h_f(P)} = L.$$

Since $d_v(P,Q) \leqslant 1$ and $h_f(P) \geqslant 0$, we have $L \leqslant 0$. So now we need $L \geqslant 0$. Indeed, let m be a sufficient large prime number larger than $p = \mathrm{char}.K$ such that $p \nmid m-1$ and K does not contain any mth primitive roots of unity. Since $E(K)/mE(K)$ is finite, it implies that there is a coset containing infinitely many P_i. We then replace P_i's by its subset, and there exists $U_i, R \in E(K)$ satisfying

$$P_i = [m]U_i + R.$$

Properties of height functions give us

$$m^2 h_f(U_i) \leqslant 2h_f(P_i) + O(1).$$

If there does not exist a subsequence P_j of P_i such that $P_j \xrightarrow{v} Q$, then $d_v(P_j,Q)$ is bounded and then $L = 0$. Therefore, by replacing P_i by its subsequence, we may

suppose that $P_i \xrightarrow{v} Q$, then $[m]U_i \xrightarrow{v} Q - R$. Because there are m^2 quantities of mth-roots of $Q - R$, there must be a subsequence of U_i which converges to one of the roots. Therefore, there exists $V \in E(K^s)$ such that

$$U_i \xrightarrow{v} V \text{ and } Q = [m]V + R.$$

Because the multiplication-by-m map and the translation map are unramified, their composition $E \to E, P \mapsto [m]P + R$ is also unramified. Therefore

$$\lim_{i\to\infty} \frac{d_v(P_i, Q)}{d_v(U_i, V)} = 1.$$

Thus

$$L = \lim_{i\to\infty} \frac{\log d_v(P_i, Q)}{h_f(P_i)} \geqslant \lim_{i\to\infty} \frac{\log d_v(U_i, V)}{1/2m^2 h_f(U_i) + O(1)}.$$

Because $U_i \xrightarrow{v} V$, to apply the previous corollary, we will show that $f(V)$ does not lie in any cyclic extension of degree power of $p = \text{char}.K$ in the case K is of characteristic $p > 0$ (in the number field case, there is no condition for $f(V)$). Indeed, if $x(V)$ lies in an extension of degree a power of p of K, then so are $x(U)$ for any $W \in \frac{1}{m}Q$ because they are $\text{Gal}(K^s/K)$-conjugate. Therefore $x\left(\frac{1}{m}Q\right)$ also lies in an extension of degree a power of p of K. Because of the equation defining E, $y\left(\frac{1}{m}Q\right)$ must lie in an extension of degree 2 times a power of p of K. So $K\left(E\left(\frac{1}{m}Q\right)\right)$ also lies in an extension of degree 2 times a power of p of K. On the other hand, $K\left(E\left(\frac{1}{m}Q\right)\right)$ contains $K(E[m])$, and hence $K(\mu_m)$. Therefore, $[K(\mu_m) : K]$ is a common divisor of $m - 1$ and $2p^s$ for some s, and by the assumption of m, it implies that $[K(\mu_m) : K] = 1$ or 2, a contradiction since K does not contain any mth primitive roots of unity. Therefore, the previous corollary gives us

$$\liminf_{i\to\infty} \frac{d_v(U_i, V)}{[K : \mathbb{F}]h_f(U_i)} \geqslant -2.$$

Then the last two inequalities yields

$$L \geqslant -\frac{4[K : \mathbb{F}]}{m^2}.$$

Because there are infinitely many such m, therefore we have $L \geqslant 0$ and the result follows. □

We note that y is not an even function, so we can not apply the proof of this theorem for y. However, when E is given by

$$y^2 = x^3 + ax + b$$

then y^2 is an even function. Therefore, we have

Proposition 2.2.10. *Let E be an elliptic curve over K given by $y^2 = x^3 + ax + b$ with $\#E(K) = \infty$, and $f = y^2 \in E(K)$. Let $Q \in E(K)$, and $v \in M_K$ a valuation. Then*

$$\lim_{\substack{P \in E(K) \\ h_f(P) \to \infty}} \frac{\log d_v(P, Q)}{h_f(P)} = 0.$$

Remark. When K is a number field, Proposition 2.2.9 holds for any non-constant even functions, it is known as Siegel's Theorem, see [14] Theorem IX.3.1. In fact, it holds for any non-constant functions, see [14] Exercise 9.14d.

2.2.3 Siegel's Theorem and S-Units Equation

In this section, we will follow the strategy of [14] Chapter IX.3 in proving some classical theorems for integral points on affine curves over global fields. Again, we denote K a global field of characteristic p.

S-Units Equation

Theorem 2.2.11. *Let S be a set of finitely many places of K, and $a, b \in K^\times$. Then the set*

$$\{(x, y) \in (\mathcal{O}_{K,S}^\times)^2 : ax + by = 1\}$$

is finite.

Proof. Let m be a large prime number such that $m > p$, then $\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times m}$ is finite, i.e., we can choose a finite set of elements $c_1, ..., c_r$ representing $\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times m}$. Then any solution (x, y) is written as

$$x = c_i X^m, y = c_j Y^m$$

for some $X, Y \in \mathcal{O}_{K,S}$ and some c_i and c_j. In other words, (X, Y) satisfies

$$ac_i X^m + bc_j Y^m = 1.$$

Therefore it remains to show

Claim. For any $a, b \in K^\times$, the equation

$$aX^m + bY^m = 1$$

has only finitely many $S-$integral solutions.

To prove this, we first suppose that this equation has infinitely many solutions (X, Y). Since Y is $S-$integral,

$$H_K(Y) = \prod_{v \in S} \max\{1, |Y|_v\}.$$

Therefore, there exists $v \in S$ such that there are infinitely many (X, Y) satisfying

$$|Y|_v \geqslant H_K(Y)^{1/\#S}$$

Let $\gamma \in \bar{K}$ be an mth root of $-b/a$. We note that by the assumption of m, γ does not lie in any cyclic extension of degree a power of p over K. From the equation $aX^m + bY^m = 1$ we have

$$\prod_{\xi \in \mu_m} \left(\frac{X}{Y} - \xi\gamma\right) = \frac{1}{aY^m}.$$

Thus

$$\prod_{\xi \in \mu_m} \left|\frac{X}{Y} - \xi\gamma\right| = \frac{1}{aY^m}.$$

Because there are infinitely many solutions, $H_K(Y)$ can be very large, and hence, $|Y|_v$ is large. Therefore, X/Y is $v-$adically close to some $\xi\gamma$, and by the infiniteness of solutions, there exists a ξ such that infinitely many solutions (X, Y) are $v-$adically close to $\xi\gamma$. By replacing γ by $\xi\gamma$, we then have that X/Y is $v-$adically closed to γ, i.e., $|X/Y - \gamma|_v$ closed to 0. Then $|X/Y - \xi\gamma|_v$ is bounded below for $\xi \neq 1$ since

$$\left|\frac{X}{Y} - \xi\gamma\right|_v \geqslant |\gamma(1-\xi)|_v - \left|\frac{X}{Y} - \gamma\right|_v.$$

Therefore, there exists a constant C_1, independent of X and Y, satisfying

$$\left|\frac{X}{Y} - \gamma\right| \leqslant \frac{C_1}{|Y|_v^m}.$$

In addition, because

$$a\left(\frac{X}{Y}\right)^m = \left(\frac{1}{Y}\right)^m - b,$$

there exists a sufficiently large constant C_2, independent of X and Y, such that

$$H_K\left(\frac{X}{Y}\right) \leqslant C_2 H_K(Y).$$

Those above inequalities imply that for some constant C independent of X and Y, we have

$$\left|\frac{X}{Y} - \gamma\right|_v \leqslant C H_K\left(\frac{X}{Y}\right)^{-m/\#S}.$$

Because m is very large, Proposition 2.1.17 implies that there are only finitely many possibilities for X/Y. Further, since

$$Y^m = \left(a\left(\frac{X}{Y}\right) + b\right)^{-1},$$

there are also finitely many (X, Y), a contradiction.

□

Siegel's Theorem

Theorem 2.2.12. *Let $f(x) \in K[x]$ be a polynomial of degree $d \geqslant 3$ and separable over $\bar{K}$. Then the set*

$$\{(x, y) \in (\mathcal{O}_{K,S})^2 : y^2 = f(x)\}$$

is finite.

Proof. We note that if this theorem is true for a finite extension of K and a larger set S, this clearly holds also for the original K and S. Therefore we many assume that f is of the form

$$f(x) = a(x - \alpha_1)...(x - \alpha_d)$$

where $\alpha_1, ..., \alpha_d \in K$ and $a \in \mathcal{O}_{K,S}^{\times}$, $\alpha_i - \alpha_j \in \mathcal{O}_{K,S}^{\times}$ for all $i \neq j$, and $\mathcal{O}_{K,S}$ is a PID. Let $x, y \in \mathcal{O}_{K,S}$ such that $y^2 = f(x)$, and let $\mathfrak{p} \notin S$. Then $\mathfrak{p} \nmid a$, and $\mathfrak{p}$ divides at most one $x - \alpha_i$ since $\mathfrak{p} \nmid \alpha_i - \alpha_j$. In addition, since $\mathrm{ord}_{\mathfrak{p}}(y^2)$ is even, $\mathrm{ord}_{\mathfrak{p}}(x - \alpha_i)$ must be even. In addition, if $x - \alpha_i \notin \mathcal{O}_{K,S}$, then for some $\mathfrak{q} \notin S$, $\mathrm{ord}_{\mathfrak{q}}(x - \alpha_i) < 0$, and hence $\mathrm{ord}_{\mathfrak{q}}(x - \alpha_j) > 0$ for some j, a contradiction since $\mathrm{ord}_{\mathfrak{q}}(\alpha_i - \alpha_j) = 0$. Therefore, $(x - \alpha_i)\mathcal{O}_{K,S}$ is a square of an ideal in $\mathcal{O}_{K,S}$, hence, there exist $z_i \in \mathcal{O}_{K,S}$ and $b_i \in \mathcal{O}_{K,S}^{\times}$ such that

$$x - \alpha_i = b_i.z_i^2 \text{ for } i = 1, ..., d.$$

We denote $L := K(\sqrt{a} : a \in \mathcal{O}_{K,S}^{\times})$, then L is a finite extension of K since $\mathcal{O}_{K,S}/\mathcal{O}_{K,S}^2$ is finite. We denote $T \subset M_L$ the set of places of L above S. Since each $b_i = \beta_i^2$ for some $\beta_i \in \mathcal{O}_{T,L}$, we have $x - \alpha_i = (\beta_i z_i)^2$. Therefore for $i \neq j$

$$\alpha_j - \alpha_i = (\beta_i z_i - \beta_i z_i)(\beta_i z_i + \beta_i z_i).$$

Because $\alpha_j - \alpha_i \in \mathcal{O}_{L,T}$ and $\beta_i z_i \pm \beta_j z_j \in \mathcal{O}_{L,T}$, it follows that

$$\beta_i z_i \pm \beta_j z_j \in \mathcal{O}_{L,T}^{\times}.$$

Because

$$\frac{\beta_1 z_1 \pm \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \mp \frac{\beta_2 z_2 \pm \beta_3 z_3}{\beta_1 z_1 - \beta_3 z_3} = 1,$$

and each term is in $\mathcal{O}_{L,T}^{\times}$. Therefore Theorem 2.2.11 implies that there are only finitely many possibilities for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \text{ and } \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3}.$$

Thus there are also only finitely many choices for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} . \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} = \frac{\alpha_2 - \alpha_1}{(\beta_1 z_1 - \beta_3 z_3)^2}.$$

So there are only finitely many choices for $\beta_1 z_1 - \beta_3 z_3$, and hence only finitely many for

$$\beta_1 z_1 = \frac{1}{2}\Big((\beta_1 z_1 - \beta_3 z_3) + \frac{\alpha_3 - \alpha_1}{\beta_1 z_1 - \beta_3 z_3}\Big).$$

Therefore there are only finitely many possible values for $x = \alpha_1 + (\beta_1 z_1)^2$. Thus the number of such pair (x, y) is finite. □

Some Relevant Results

We state here two landmarks of arithmetic geometry, for more details, we refer to [22] Chapter 1.

Theorem 2.2.13 (Mordell's conjecture, proved by Manin and Grauert for complex function fields, and by Falting for number fields)**.** *Let C be a smooth projective curve of genus g over a global field K. If $g > 1$, then $C(K)$ is finite.*

Theorem 2.2.14 (Siegel's theorem, see [22] Chapter 1 section 2)**.** *Let C be a smooth projective curve of genus g over a global field K, and let S be a finite set of places containing all the Archimedean places. Let Z be non-empty zero dimensional subscheme over K of C, and $U := C \setminus Z$. Let*

$$\chi(U) := 2 - 2g - r$$

where $r := \#Z(\bar{K})$. Let $\mathcal{U}$ be a finite type $\mathcal{O}_{K,S}-$scheme such that $\mathcal{U}_K = U$. If $\chi(U) < 0$, then $\mathcal{U}(\mathcal{O}_{K,S})$ is finite.

Remark. $\chi(U) < 0$ means

1. $g = 0$ and $r \geqslant 3$,
2. $g \geqslant 1$ and $r \geqslant 1$.

Example 2.2. 1. Consider a projective curve excluding three distinct points $C = \mathbb{P}^1$, $Z := \{0, 1, \infty\}$, and $U := \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Then

$$\mathcal{U} = \operatorname{Spec} \mathcal{O}_{K,S}\Big[x, \frac{1}{x}, \frac{1}{1-x}\Big].$$

So its integral points

$$\mathcal{U}(\mathcal{O}_{K,S}) = \{(x, y) \in \mathcal{O}_{K,S}^2 : x + y = 1\}.$$

In addition, when $r = 0, 1, 2$ we obtain $U = \mathbb{P}^1, \mathbb{G}_a, \mathbb{G}_m$ respectively, and hence the set of integral points of U in those cases is infinite.

2. Consider $U : y^2 = f(x)$ where $f \in \mathcal{O}_{K,S}[x]$ of degree $d \geqslant 3$ that is separable over $\bar{K}$. Its smooth projective model C has genus $\left\lfloor \frac{d-1}{2} \right\rfloor$. When $d = 3$, U is an elliptic curve minus the unique point at infinity. When $d = 4$, U is an elliptic curve minus the two points at infinity. When $d \geqslant 5$, U is a hyperelliptic curve minus one points (resp. two points) at infinity when d is odd (resp. d is even).

Chapter 3

The Orders of The Reductions of Rational Points on Algebraic Groups

Following Theorem 0.0.1, one can ask the following general question:

Question (1)**.** Let G be an algebraic group over a global field K of characteristic $p \geqslant 0$, and P a non-torsion $K-$point of G. How big is the set

$$O(P) := \{n \in \mathbb{N} : \text{ there exists a place } v \text{ of } K \text{ satisfying } n = \text{ord}(P \bmod \mathfrak{p}_v)\}?$$

This chapter contains the main results of the thesis which gives an answer to above question on the order of the reduction of points. It contains three main following contents:

1. An answer for tori ,
2. An answer for elliptic curves, and
3. An answer for a similar question for semi-abelian varieties.

In this chapter, we show that $\mathbb{N} \setminus (O(P) \cup p\mathbb{N})$ is finite when G is a torus over a global field, and when G is an elliptic curve over a global field of characteristic $p \neq 2, 3$.

3.1 Algebraic Tori

Number Fields

When $G = \mathbb{G}_m$ over a number field K, the answer to this question is given by Theorem 0.0.1, which is proven by Schinzel and Postnikova. We will give a detailed proof of Theorem 0.0.1 after Schinzel and Postnikova [1]. Let K be a number field of degree l over $\mathbb{Q}$. First we need some lemmas.

Lemma 3.1.1 (Some properties of Möbius function μ)**.**
For $n > 0$

- $\displaystyle\sum_{m|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$

- $\sum_{m|n} \mu\left(\frac{n}{m}\right) m = \phi(n)$, *where* $\phi(n)$ *is the Euler's totient function.*
- *For* $0 < \lambda < n$

$$\sum_{\lambda|m|n} \mu\left(\frac{n}{m}\right) = 0,$$

where m *runs over the set* $\{m > 0 : \lambda|m \text{ and } m|n\}$.

- *Let* $\Phi_n(x, y)$ *be the nth cyclotomic homogeneous polynomial, then*

$$\Phi_n(x, y) = \prod_{m|n} (x^m - y^m)^{\mu\left(\frac{n}{m}\right)}.$$

Proof. We prove the third and the fourth formula. Other formulas are well-known.

- If $\lambda \nmid n$, then there is no $m > 0$ satisfying $\lambda|m$ and $m|n$. Thus the formula holds. If $\lambda|n$, we have

$$\begin{aligned}\sum_{\lambda|m|n} \mu\left(\frac{n}{m}\right) &= \sum_{\lambda|m|n} \mu\left(\frac{n/\lambda}{m/\lambda}\right) \\ &= \sum_{d|(n/\lambda)} \mu\left(\frac{n/\lambda}{d}\right) = 0 \text{ since } \frac{n}{\lambda} > 1.\end{aligned}$$

- Since

$$x^n - y^n = \prod_{m|n} \Phi_m(x, y),$$

using the Möbius inversion formula we obtain

$$\Phi_n(x, y) = \prod_{m|n} (x^m - y^m)^{\mu\left(\frac{n}{m}\right)}.$$

□

Lemma 3.1.2 (Kronecker's theorem)**.**
Let f *be a monic polynomial with integers coefficients whose complex roots are non-zero and lie in the unit disk. Then then the roots of* f *are roots of unity.*

Proof. See [26, Theorem 1.5.9] □

Lemma 3.1.3 (Gel'fond's theorem)**.**
For a *and* b *as in Theorem 0.0.1, there exists a constant* $c(a, b)$ *depending on* a *and* b *such that* $\forall m > 0$*, we have*

$$\left|\left(\frac{a}{b}\right)^m - 1\right| > \exp\left\{\max\left(m.\ln\left|\frac{a}{b}\right|, 0\right) - c(a, b)\ln^4 m\right\}.$$

Proof. See [28]. □

Lemma 3.1.4 (Euler's totient function for ideals)**.** *For any ideal I in $\mathcal{O}_K$, let $\phi(I)$ be the number of invertible elements in $\mathcal{O}_K/I$. As in the usual Euler's totient function, we have:*

- *For $z+I \in (\mathcal{O}_K/I)^\times$, $I|z^{\phi(I)}-1$.*
- *For $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ and $k>0$, $\phi(\mathfrak{p}^k) = N(\mathfrak{p})^{k-1}(N(\mathfrak{p})-1)$. (Here denote $N(I) := \#\mathcal{O}_K/I$ the norm of an ideal I of $\mathcal{O}_K$.)*

Proof.

- Since $z+I \in (\mathcal{O}_K/I)^\times$, $z^{N(I)}+I = 1+I$. Thus $I|z^{\phi(I)}-1$.
- We have a surjective homomorphism between local rings

$$\mathcal{O}_K/\mathfrak{p}^k \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}$$

such that the preimage of $(\mathcal{O}_K/\mathfrak{p})^\times = \{a+\mathfrak{p} : a \in \mathcal{O}_K \setminus \mathfrak{p}\}$ is $\{a+\mathfrak{p}^k : a \in \mathcal{O}_K \setminus \mathfrak{p}^k\} = (\mathcal{O}_K/\mathfrak{p}^k)^\times$ since $\mathcal{O}_K/\mathfrak{p}^k$ is local with maximal ideal $\mathfrak{p}/\mathfrak{p}^k$. Thus

$$\phi(\mathfrak{p}^k) = \frac{|\mathcal{O}_K/\mathfrak{p}^k|}{|\mathcal{O}_K/\mathfrak{p}|}.|(\mathcal{O}_K/\mathfrak{p})^\times| = \frac{N(\mathfrak{p}^k)}{N(\mathfrak{p})}(N(\mathfrak{p})-1) = N(\mathfrak{p})^{k-1}(N(\mathfrak{p})-1).$$

□

Lemma 3.1.5. *Let $\mathfrak{p} \in M_K$ above a rational prime p. Denote $e := e(\mathfrak{p}|p) := \operatorname{ord}_\mathfrak{p} p$. Let $A, B \in K$ such that*

$$\operatorname{ord}_\mathfrak{p} B = 0 \text{ and } \operatorname{ord}_\mathfrak{p}(A-B) > \frac{e}{p-1},$$

then

$$\operatorname{ord}_\mathfrak{p}(A^n - B^n) = \operatorname{ord}_\mathfrak{p}(A-B) + \operatorname{ord}_\mathfrak{p} n.$$

Proof. There are three cases.

1. $(n,p)=1$. We see that

$$\frac{A^n-B^n}{A-B} = (A-B).Q(A,B) + nB^{n-1},$$

for some $Q \in \mathbb{Z}[x,y]$. Since $\operatorname{ord}_\mathfrak{p}(A-B) > 0, \operatorname{ord}_\mathfrak{p} B = 0$ and $(p,n)=1$, we have

$$\operatorname{ord}_\mathfrak{p}(A^n-B^n) = \operatorname{ord}_\mathfrak{p}(A-B).$$

2. $n = p^s$ for some $s>0$. We prove by induction on s.

(a) When $s = 1$, since

$$A^p - B^p = \sum_{k=1}^{p} C_p^k B^{p-k}(A-B)^k,$$

$\mathrm{ord}_{\mathfrak{p}}(A-B) + e < p.\,\mathrm{ord}_{\mathfrak{p}}(A-B)$, and since $\mathrm{ord}_p\, C_p^k = 1$ for $1 \leqslant k < p$, we have

$$\mathrm{ord}_{\mathfrak{p}}\left(C_p^1.B^{p-1}(A-B)\right) = e + \mathrm{ord}_{\mathfrak{p}}(A-B) < \mathrm{ord}_{\mathfrak{p}}\left(C_p^k B^{p-k}(A-B)^k\right)$$

for $1 < k \leqslant p$. Hence

$$\mathrm{ord}_{\mathfrak{p}}(A^p - B^p) = \mathrm{ord}_{\mathfrak{p}}(A-B) + \mathrm{ord}_{\mathfrak{p}}\, p = \mathrm{ord}_{\mathfrak{p}}(A-B) + e.$$

(b) If

$$\mathrm{ord}_{\mathfrak{p}}(A^{p^s} - B^{p^s}) = \mathrm{ord}_{\mathfrak{p}}(A-B) + s.e,$$

then we have

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}}\left(A^{p^{s+1}} - B^{p^{s+1}}\right) &= \mathrm{ord}_{\mathfrak{p}}\left(\frac{A^{p^{s+1}} - B^{p^{s+1}}}{A^{p^s} - B^{p^s}}.\frac{A^{p^s} - B^{p^s}}{A-B}\right) \\
&= \mathrm{ord}_{\mathfrak{p}}\left(\frac{A^{p^{s+1}} - B^{p^{s+1}}}{A^{p^s} - B^{p^s}}\right) + s.e \\
&= e + s.e = (s+1).e \text{ (by (a))}.
\end{aligned}$$

3. When $p|n$, we write $n = p^s.m$ with $(m,p) = 1$. We have

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}}\left(\frac{A^n - B^n}{A-B}\right) &= \mathrm{ord}_{\mathfrak{p}}\left(\frac{(A^m)^{p^s} - (B^m)^{p^s}}{A^m - B^m}.\frac{A^m - B^m}{A-B}\right) \\
&= s.e = s.\,\mathrm{ord}_{\mathfrak{p}}\, n \text{ (by cases 1 and 2)}.
\end{aligned}$$

Hence,

$$\mathrm{ord}_{\mathfrak{p}}(A^n - B^n) = \mathrm{ord}_{\mathfrak{p}}(A-B) + \mathrm{ord}_{\mathfrak{p}}\, n.$$

□

The following lemma allows us to detect whether a prime ideal is primitive or not.

Lemma 3.1.6. *Let $\mathfrak{p} \in M_K$. For a and b as in Theorem 0.0.1, if*

$$n > 2^l(2^l - 1), \mathfrak{p}|\Phi_n(a,b)$$

and if $\mathfrak{p}$ is not a primitive divisor of the number $a^n - b^n$, then

$$\mathrm{ord}_{\mathfrak{p}}\, \Phi_n(a,b) \leqslant \mathrm{ord}_{\mathfrak{p}}\, n.$$

Proof. For every $i \geqslant 1$, let λ_i be the least exponent $\lambda > 0$ such that

$$\mathfrak{p}^i | a^\lambda - b^\lambda.$$

We note that $\mathfrak{p}^i | a^\lambda - b^\lambda$ is equivalent to $\lambda_i | \lambda$. Since $\mathfrak{p} | \Phi_n(a,b) | a^n - b^n$, a and b are not contained in $\mathfrak{p}$. Indeed, if $a \in \mathfrak{p}$, then b is also in $\mathfrak{p}$, which is a contradiction as a and b are relatively primitive. Thus $\mathfrak{p} | a^n - 1$ and $\mathfrak{p} | b^n - 1$, therefore $\mathfrak{p} | a^n - b^n$. As a consequence, $\lambda_i | \phi(\mathfrak{p}^i)$. Further, by Lemma 3.1.1, we have

$$\Phi_n(a,b) = \prod_{m|n} (a^m - b^m)^{\mu\left(\frac{n}{m}\right)}.$$

Hence,

$$\operatorname{ord}_{\mathfrak{p}} \Phi_n(a,b) = \sum_{m|n} \mu\left(\frac{n}{m}\right) \operatorname{ord}_{\mathfrak{p}}(a^m - b^m).$$

In view of Lemma 3.1.5, the number λ_k is important when we calculate $\operatorname{ord}_{\mathfrak{p}}$, here $k := \left\lfloor \frac{e}{p-1} \right\rfloor$. For every i, if $\lambda_i | m$, but $\lambda_{i+1} \nmid m$, then $\operatorname{ord}_{\mathfrak{p}}(a^m - b^m) = i$ by the definition of λ_i. If $\lambda_{k+1} | m$, then (by Lemma 3.1.5)

$$\operatorname{ord}_{\mathfrak{p}}(a^m - b^m) = \operatorname{ord}_{\mathfrak{p}}(a^{\lambda_{k+1}} - b^{\lambda_k}) + \operatorname{ord}_{\mathfrak{p}}\left(\frac{m}{\lambda_{k+1}}\right).$$

From these observations, we get

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}} \Phi_n(a,b) = &\sum_{i=1}^{k} \sum_{\lambda_i | m | n} \mu\left(\frac{n}{m}\right) + \sum_{\lambda_{k+1} | m | n} \mu\left(\frac{n}{m}\right) (\operatorname{ord}_{\mathfrak{p}}(a^{\lambda_{k+1}} - b^{\lambda_{k+1}}) - k) \\ &+ \sum_{\lambda_{k+1} | m | n} \mu\left(\frac{n}{m}\right) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}}. \end{aligned}$$

We note that $\lambda_{k+1} < n$. Indeed, if $k = 0$, λ_1 is the least exponent λ such that $\mathfrak{p} | a^\lambda - b^\lambda$. Since $\mathfrak{p} | a^n - b^n$ is not a primitive divisor of $a^n - b^n$, there exists some d with $d | n$ and $0 < d < n$ such that $\mathfrak{p} | a^d - b^d$. Hence, $\lambda_1 \leqslant d < n$. If $k > 0$, then $e + 1 \geqslant p$, and since $N(\mathfrak{p}^e) \leqslant N(p) = p^l$, it follows that

$$\lambda_{k+1} \leqslant \Phi(\mathfrak{p}^{k+1}) = N(\mathfrak{p}^k)(N(\mathfrak{p}) - 1) \leqslant p^{\frac{k.l}{e}}(p^{\frac{l}{e}} - 1) \leqslant p^{\frac{l}{p-1}}((e+1)^{\frac{l}{e}} - 1) \leqslant 2^l(2^l - 1) < n.$$

Here we use Lemma 3.1.4 and the fact that $u^{\frac{1}{u-1}} \leqslant 2$ for all real numbers $u \geqslant 2$. Thus, using Lemma 3.1.1, we obtain

$$\sum_{\lambda_i | m | n} \mu\left(\frac{n}{m}\right) = 0, \ i = 1, 2, ..., k+1.$$

We consider the following two cases

1. If $\lambda_{k+1} \nmid n$ or $\lambda_{k+1}|n$ and $p \nmid \dfrac{n}{\lambda_{k+1}}$, then $\operatorname{ord} \dfrac{m}{\lambda_{k+1}} = 0$ for $\lambda_{k+1}|m|n$. Hence, $\operatorname{ord} \phi_n(a,b) = 0$.

2. If $\lambda_{k+1}|n$ and $p|\dfrac{n}{\lambda_{k+1}}$, then

$$
\begin{aligned}
\operatorname{ord}_{\mathfrak{p}} \Phi_n(a,b) &= \sum_{\lambda_{k+1}|m|n} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} \\
&= \sum_{\substack{\lambda_{k+1}|m|n \\ \operatorname{ord}_p(n/m)=0}} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} \\
&\quad + \sum_{\substack{\lambda_{k+1}|m|n \\ \operatorname{ord}_p(n/m)=1}} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} \\
&= \sum_{\substack{\lambda_{k+1}|m|n \\ \operatorname{ord}_p(n/m)=1}} \Big(\mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{mp}{\lambda_{k+1}} + \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}}\Big) \\
&= \sum_{\substack{\lambda_{k+1}|m|n \\ \operatorname{ord}_p(n/m)=1}} \Big(\mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} p + \mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} \\
&\quad + \mu(p)\mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}}\Big) \\
&= \sum_{\substack{\lambda_{k+1}|m|n \\ \operatorname{ord}_p(n/m)=1}} \mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} p \\
&= \sum_{r|d} \mu\Big(\frac{d}{r}\Big) \operatorname{ord}_{\mathfrak{p}} p, \text{ where } \frac{n}{\lambda_{k+1}} = p^t.d \text{ and } (d,p) = 1 \\
&= \begin{cases} \operatorname{ord}_{\mathfrak{p}} p & \text{if } d = 1, \\ 0 & \text{otherwise} \end{cases} \\
&\leqslant \operatorname{ord}_{\mathfrak{p}} n
\end{aligned}
$$

and therefore Lemma 3.1.6 is proven.

□

Now we have enough ingredients for the proof of Theorem 0.0.1.

Proof of Theorem 0.0.1. By Lemma 3.1.3, there exists a number $c(a,b)$ satisfying for all natural number m

$$\left|\left(\frac{a}{b}\right)^m - 1\right| > \exp\left\{m.\ln\max\left(\left|\frac{a}{b}\right|, 1\right) - c(a,b)\ln^4 m\right\}.$$

By considering $|a| \leqslant |b|$ and $|a| > |b|$, we get

$$\left|\left(\frac{a}{b}\right)^m - 1)\right| \leqslant \exp\left\{m.\ln\max\left(\left|\frac{a}{b}\right|, 1\right) + \ln 2\right\}.$$

For $n > 0$, from these evaluations and Lemma 3.1.1 we obtain

$$\begin{aligned}
\ln|\Phi_n(a,b)| &= \sum_{m|n}\mu\Big(\frac{n}{m}\Big)\ln|a^m - b^m| \\
&= \sum_{m|n}\mu\Big(\frac{n}{m}\Big)\Big(m\ln|b| + \ln\left|\left(\frac{a}{b}\right)^m - 1\right|\Big) \\
&> \phi(n)\ln|b| + \sum_{m|n}\mu\Big(\frac{n}{m}\Big)m\ln\max\left(\left|\frac{a}{b}\right|, 1\right) \\
&- \sum_{m|n}\left|\mu\Big(\frac{a}{b}\Big)\right|(\ln 2 + c(a,b)\ln^4 n) \\
&> \phi(n)\Big(\ln|b| + \ln\max\left(\left|\frac{a}{b}\right|, 1\right)\Big) - 2^{\omega(n)}(\ln 2 + c(a,b)\ln^4 n).
\end{aligned}$$

Here $\omega(n)$ is an arithmetic function which counts the number of divisors of n. In a similar way, $\forall\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ we have

$$\begin{aligned}
\ln|\sigma(\Phi_n(a,b))| &= \ln|\Phi_n(\sigma a, \sigma b)| \\
&> \phi(n)\Big(\ln|\sigma b| + \ln\max\left(\left|\frac{\sigma a}{\sigma b}\right|, 1\right)\Big) - 2^{\omega(n)}(\ln 2 + c(\sigma a, \sigma b)\ln^4 n).
\end{aligned}$$

Thus

$$\begin{aligned}
\ln|N(\Phi_n(a,b))| >& \phi(n)\Big(\ln|N(b)| + \sum_{\sigma}\ln\max\left(\left|\frac{\sigma a}{\sigma b}, 1\right|\right)\Big) \\
&- l.2^{\omega(n)}\ln 2 - 2^{\omega(n)}\ln^4 n\sum_{\sigma}c(\sigma a, \sigma b).
\end{aligned}$$

We note that

$$c := \ln|N(b)| + \sum_{\sigma}\ln\max\left(\left|\frac{\sigma a}{\sigma b}, 1\right|\right) > 0.$$

Indeed, if $|N(b)| \geqslant 2$, then $c > 0$. If $|N(b)| = 1$, then

$$f(x) := \prod_{\sigma}(\sigma b.x - \sigma a) = \pm\prod_{\sigma}\Big(x - \frac{\sigma a}{\sigma b}\Big).$$

Since $a, b \in \mathcal{O}_K$, it implies that $f(x) \in \mathbb{Z}[x]$, and, since $\dfrac{a}{b}$ is not a root of unity, it follows by Lemma 3.1.2 that there is a root of f, say $\left|\dfrac{\sigma a}{\sigma b}\right|$, which is larger than 1. Thus $c > 0$. Further, we need the following estimates

1. [29, Theorem 317] There exists a constant $C > 0$ satisfying

$$2^{\omega(n)} \leqslant e^{C\frac{\ln n}{\ln\ln n}} < e^{\frac{1}{2}\ln n} = \sqrt{n}$$

for all n large enough.

2. [29, Theorem 328] There exists a constant $D > 0$ satisfying

$$\frac{\phi(n)}{n} \geqslant \frac{D}{\ln\ln n}$$

for all n large enough.

Hence, for n sufficiently large we have

$$\ln|N(\Phi_n(a,b))| > n.\frac{D}{\ln\ln n}c - \sqrt{n}\Big(l\ln 2 + \ln^4 n.\sum_{\sigma} c(\sigma a, \sigma b)\Big) > \sqrt{n}$$

and therefore

$$|N(\Phi_n(a,n))| > e^{\sqrt{n}} > n^l. \tag{3.1}$$

So, for n large enough, there is a primitive divisor of $\Phi_n(a,b)$. Indeed, let's suppose that $\Phi_n(a,b)$ doesn't admit any primitive divisor. By Lemma 3.1.6, for $\mathfrak{p}|\Phi_n(a,b)$ we have

$$\operatorname{ord}\Phi_n(a,b) \leqslant \operatorname{ord}_{\mathfrak{p}} n.$$

It follows that

$$|N(\Phi_n(a,b))| = \prod_{\mathfrak{p}} N(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}}\Phi_n(a,b)} \leqslant \prod_{\mathfrak{p}} N(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}} n} = N(n) = n^l,$$

contradicts (3.1). In other words, for all n large enough, $a^n - b^n$ admits some primitive divisor. □

Remark. In their paper, L. Postnikova and A. Schinzel also proved that if K is purely real fields (i.e. all of whose conjugate fields are real), the number $n_0(a,b)$ is independent of a and b. In 1974, A. Schinzel showed that the number $n_0(a,b)$ depends only on the degree of $\frac{a}{b}$ over $\mathbb{Q}$ (see [30, Theorem 1, page 1090]).

When $G = T$ is a one-dimensional torus over a number field, Question 3 is affirmative due to Mikdad who proved it in his master thesis [31].

Theorem 3.1.7. *Let T be a one-dimensional torus over a number field K, and P a non-torsion $K-$point of T. Then the set*

$$\{n \in \mathbb{N} : \nexists \mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K \text{ such that } n = \operatorname{ord}(P \bmod \mathfrak{p})\}$$

is finite.

Proof. See [31] Theorem 3.1. It is also can by proved by using Lemma 1.4.3 and Theorem 0.0.1, as in the proof of Theorem 3.1.9 below. □

Global Function Fields

Similarly, I will show that Theorem 0.0.1 and 3.1.7, after discarding those $n's$ which is not prime to the characteristic of the base field, also hold in the global function field case. As usual, one of the advantages of global function fields is that global function field does not admit any Archimedean place. In addition, as in the proof of Theorem 0.0.1, the key idea is how to detect primitive divisors.

Proposition 3.1.8. *Let K be a global function field over $\mathbb{F}_q$ of charateristic p, and let $x \in K \setminus \{0\}$ be not a root of unity. Then for every $n > 1$ coprime to p, there exists $v \in M_K$ such that* $\mathrm{ord}(x \bmod \mathfrak{p}_v)$ *in $\mathbb{G}_m(\mathcal{O}_v/\mathfrak{p}_v)$ is equal to n.*

Proof. We denote $P := \{v \in M_K : v(x^n - 1) > 0\}$. We consider four following cases.

1. v in P such that n is not the order of x modulo $\mathfrak{p}_v$, we call this order by n_0. Then $n = n_0.k$ for some $k > 0$ and

$$x^n - 1 = (x^{n_0} - 1)(x^{n_0(k-1)} + x^{n_0(k-2)} + ... + x^{n_0} + 1).$$

Since $x^{n_0(k-1)} + x^{n_0(k-2)} + ... + x^{n_0} + 1 \equiv k \not\equiv 0 \bmod \mathfrak{p}_v$ $((k,p) = 1)$, we have $v(x^n - 1) = v(x^{n_0} - 1)$. Thus

$$\begin{aligned} v(\Phi_n(x)) &= \sum_{m|n} \mu\Big(\frac{n}{m}\Big) v(x^m - 1) \\ &= \sum_{n_0|m|n} \mu\Big(\frac{n}{m}\Big) v(x^m - 1) \\ &= \sum_{n_0|m|n} \mu\Big(\frac{n}{m}\Big) v(x^{n_0} - 1) \\ &= 0 \text{ since } n_0 < n. \end{aligned} \tag{3.2}$$

(Here $\Phi_n(x)$ is the nth cyclotomic polynomial.)

2. $v \in M_K$ satisfying $v(x) > 0$. Then $v(x^m - 1) = 0$ for all positive integer m. It implies that $v(\Phi_n(x)) = 0$.

3. $v \in M_K$ satisfying $v(x) < 0$. Then $v(x^m - 1) = v(1 - x^{-m}) + v(x^m) = mv(x)$. Hence

$$\begin{aligned} v(\Phi_n(x)) &= \sum_{m|n} \mu\Big(\frac{n}{m}\Big) v(x^m - 1) \\ &= \sum_{m|n} \mu\Big(\frac{n}{m}\Big) mv(x) \\ &= \phi(n).v(x). \end{aligned}$$

4. $v \in M_K$ satisfying $v(x) = 0$ and $v \notin P$. Then $v(x^m - 1) = 0$ for all $m|n$, and hence $v(\Phi_n(x)) = 0$.

Combining these equalities, we obtain that if for every $v \in P$, n is not the order of x modulo $\mathfrak{p}_v$, then

$$\begin{aligned} 0 &= \sum_{v \in M_K} v(\Phi_n(x)) \\ &= \sum_{v \in M_K : v(x) < 0} v(\Phi_n(x)) \\ &= \sum_{v \in M_K : v(x) < 0} \phi(n).v(x). \end{aligned}$$

This equality holds if and only if there is no place v such that $v(x) < 0$, which means that x must lie in the constant field $\mathbb{F}_q$, a contradiction. Thus, there exists some v in P such that $n = \operatorname{ord} x \bmod \mathfrak{p}_v$, this is what we want. □

For non-split tori, we have (see [32])

Theorem 3.1.9. *Let G be a one-dimensional torus over a global function field K of characteristic p, and let $x \in G(K)$ be non-torsion. Then for every sufficiently large n prime to p, there exists a place $v \in M_K$ such that at there, we can take the reduction of x modulo $\mathfrak{p}_v$, and the order of x modulo $\mathfrak{p}_v$ is n.*

Proof. This theorem can be proven using the behaviour of reduction under field extensions as in 1.4. Firstly, after discarding a finite set $S \subset M_K$, we see that the coefficients of x are in $\mathcal{O}_{K,S}$. After discarding finitely many more places (still denote this set by S), we can assume that G admits an integral model $\mathcal{G}$ over $\mathcal{O}_{K,S}$ and $x \in \mathcal{G}(\mathcal{O}_{K,S})$. Further, there exists a finite Galois extension K' of K such that $G \times_K K' = \mathbb{G}_{m,K'}$. After discarding finitely many more places (still denote this set of places by S), one can assume that $\mathbb{G}_{m,K'}$ admits an integral model $\mathbb{G}_{m,\mathcal{O}_{K',S'}}$ (S' is the set of places in $M_{K'}$ above S) which is an extension $\mathcal{G}$, i.e., $\mathbb{G}_{m,\mathcal{O}_{K',S'}} = \mathcal{G} \times_{\mathcal{O}_{K,S}} \mathcal{O}_{K,S'}$ (thanks to the uniqueness of integral models). Now for any $v \notin S$ and $w \notin S'$ above v, let P be an $\mathcal{O}_v-$point of $\mathcal{G}$. Then P is also an $\mathcal{O}_v-$point of G, and it can be lifted to a point $\mathcal{O}_w-$point P' of $\mathbb{G}_{m,K'}$, since $\mathcal{O}_v \otimes_K K' \cong \prod_{w|v} \mathcal{O}_w$. Since $\mathcal{O}_{K,S'} \subset \mathcal{O}_w$, the point P is also an $\mathcal{O}_w-$point of $\mathbb{G}_{m,S'}$, i.e., we have the commutative diagram

$$\begin{array}{ccccc} \operatorname{Spec} \mathcal{O}_w & \xrightarrow{P'} & \mathbb{G}_{m,\mathcal{O}_{K',S'}} & \longrightarrow & \mathbb{G}_{m,K'} \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Spec} \mathcal{O}_v & \xrightarrow{P} & \mathcal{G} & \longrightarrow & G \end{array}$$

In other words, $\mathcal{G}(\mathcal{O}_v) \subset \mathbb{G}_{m,\mathcal{O}_{K',S'}}(\mathcal{O}_w)$. Taking reduction, we see that the group of reduction points modulo $\mathfrak{p}_v$ in $\mathcal{G}$ is injected in the group of reduction points modulo $\mathfrak{p}_w$ in $\mathbb{G}_{m,\mathcal{O}_{K',S'}}$, and hence the order of P modulo $\mathfrak{p}_v$ is equal to the order of P' modulo $\mathfrak{p}_w$ for every $w|v$ and every $P \in \mathcal{G}(\mathcal{O}_v)$. Now we take P to be $x \in \mathcal{G}(\mathcal{O}_{K,S})$, then x lifts to $x' \in \mathbb{G}_{m,\mathcal{O}_{K',S'}}(\mathcal{O}_{K',S'}) = \mathcal{O}_{K',S'}^{\times}$, and we have the following commutative diagram

$$\begin{array}{ccccc} \operatorname{Spec}\mathcal{O}_w & \longrightarrow & \operatorname{Spec}\mathcal{O}_{K',S'} & \xrightarrow{x'} & \mathbb{G}_{m,\mathcal{O}_{K',S'}} \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Spec}\mathcal{O}_v & \longrightarrow & \operatorname{Spec}\mathcal{O}_{K,S} & \xrightarrow{x} & \mathcal{G} \end{array}$$

Applying Proposition 3.1.8, for every sufficiently large integer n prime to p, since S' is finite, there is a place $w_0 \notin S'$ such that $\operatorname{ord} x' \bmod \mathfrak{p}_{w_0}$ equals n. Thus $\operatorname{ord} x \bmod \mathfrak{p}_{v_0}$ also equals n for $v_0 \notin S$ the place that lies under w_0.

□

3.2 Elliptic Curves

The question (1) also has an affirmative answer for elliptic curves over global function fields as follows (see [32]).

Theorem 3.2.1. *Let E be an elliptic curve over a global function field K of characteristic $p \neq 2, 3$ and $P \in E(K)$ a non-torsion point. Then for every sufficiently large integer n prime to p, there exists $\mathfrak{p} \in M_K$ of good reduction so that the order of P modulo $\mathfrak{p}$ equals n. Moreover, for almost all P there exists such $\mathfrak{p}$ for all $n > 0$ prime to p.*

The main tools is the comparision between Weil height and Néron-Tate height, and versions of Siegel's Theorem, see Proposition 2.2.9 and Proposition 2.2.10. We note that every elliptic curve E over a global field K of characteristic $p \neq 2, 3$ can be given in the normal form

$$y^2 = x^3 + ax + b \ (a, b \in K)$$

with the identity element O. We fix an embedding $E \hookrightarrow \mathbb{P}^2$, and let S be a finite set containing all the places at which E has bad reduction, and all places at which either a or b has the non-zero valuation, i.e.,

$$S = \{v \in M_K : E \text{ has bad reduction at } v\} \cup \{v \in M_K : v(a) \neq 0 \text{ or } v(b) \neq 0\}.$$

For $P = (x, y) \in E(K)$, the **local height function** h_v at P is defined as follows:

$$h_v(P) := \begin{cases} -\dfrac{1}{[K : \mathbb{F}]} \min\{0, v(x), v(y)\} & \text{if } P \neq O \\ 0 & \text{if } P = O \end{cases}$$

We remark that $h(P) = \sum_{v \in M_K} h_v(P)$ at $P = [x : y : 1] \in \mathbb{P}^3(K)$, the projective closure of $E(K)$. We note that $h_v(P) \geqslant 0$ for all $v \in M_K$ and $P \in E(K)$. In addition, we will use the Néron-Tate height, due to H. Zimmer [3], because we need to compare the Weil height and the Néron-Tate height over global function fields. We need an auxiliary function d. The real-valued function d is defined by

$$d(P) := \frac{1}{[K : \mathbb{F}]} \sum_{v \in M_K} d_v(P),$$

where

$$d_v(P) := \begin{cases} -\frac{1}{[K : \mathbb{F}]} \cdot \frac{3}{2} \min\left\{\frac{1}{2}v(a), \frac{1}{3}v(b), v(x)\right\} & \text{if } P \neq O \\ -\frac{1}{[K : \mathbb{F}]} \cdot \frac{3}{2} \min\left\{\frac{1}{2}v(a), \frac{1}{3}v(b)\right\} & \text{if } P = O \end{cases}$$

The **Néron-Tate** height $\hat{h}$ now can be defined by

$$\hat{h}(P) := \lim_{t \to \infty} \frac{d(2^t P)}{2^{2t}},$$

where the limit is taken over all positive integers t.
We note that $\hat{\mathbf{h}}$ and $\hat{h}$ are defined differently. As in [3], the Néron-Tate height behaves similarly as the usual canonical height.

Proposition 3.2.2 (see [3], §2)**.**

- *The Néron-Tate height $\hat{h}$ is well-defined on $E(K)$ and is a quadratic form on $E(K)$.*
- *There exists a constant C satisfying*

$$|\hat{h}(P) - h(P)| < C \text{ for all } P \in E(K).$$

Proposition 3.2.3 (see [3], Property 5, §4)**.** *Let $P \in E(K)$. Then $\hat{h}(P) \geqslant 0$, and*

$$\hat{h}(P) = 0 \text{ if and only if } P \text{ is a torsion point.}$$

We note that

Proposition 3.2.4 (Northcott-type finiteness theorem)**.** *For any $B > 0$, the set*

$$\{P \in E(K) : h(P) < B\}$$

is finite.

Proof. It follows directly from 2.1.4. For elliptic curves (and also abelian varieties), it also can be proved by using K/k-trace theory, which is used by Lang and Néron to prove the Mordell-Weil theorem for finitely generated fields, as follows. Since E is an abelian variety over K, E admits a K/k-trace (A, τ) (see [33] section 3, Chapter VIII, Theorem 8), where k is the constant subfield of K. It means that A is an abelian variety over k and τ is a $K-$homomorphism

$$A \times_k K \to E$$

satisfying the usual universal property in the set of pairs of this form. Because $\dim_K E = 1$, A is also of dimension 1 over k, and hence, A is an elliptic curve over k. Applying Theorem 5.3 of Chapter 6, §5 in [10], the set $\{P \in E(K) : h(P) < B\}$ lies in a finite number of cosets of $A(k)$. Since k is finite, $A(k)$ is finite. Hence the proposition follows. □

Proposition 3.2.5. *Let P be a point of infinite order on E. Then for any place v, we have*

$$\lim_{n\to\infty} \frac{h_v(nP)}{h(nP)} = 0.$$

Proof. Applying Proposition 2.2.9 for $Q = O$, and $t_O = \dfrac{1}{x}$ (O is the only one zero of x and $\mathrm{ord}_O x = 2$), we have

$$\lim_{\substack{R\in E(K)\\ h_x(R)\to\infty}} \frac{\log \min\{|x(R)|^{-1/2}, 1\}}{h_x(R)} = 0$$

since $d_v(R, O) = \min\{|x(R)|^{-1/2}, 1\}$. Thus we obtain

$$\lim_{\substack{R\in E(K)\\ h_x(R)\to\infty}} \frac{-\min\{v(x(R)), 0\}}{h_x(R)} = 0.$$

In addition, because $\min\{w(x(R)), 0\} \geqslant \min\{w(x(R)), w(y(R)), 0\}$ for all $w \in M_K$, we have $0 \leqslant h_x(R) \leqslant h(R)$. Consequently,

$$\frac{-\min\{v(x(R)), 0\}}{h_x(R)} \geqslant \frac{-\min\{v(x(R)), 0\}}{h(R)} \geqslant 0.$$

Therefore

$$\lim_{\substack{R\in E(K)\\ h_x(R)\to\infty}} \frac{-\min\{v(x(R)), 0\}}{h(R)} = 0.$$

Similarly, we have

$$\lim_{\substack{R\in E(K)\\ h_y(R)\to\infty}} \frac{-\min\{v(y(R)), 0\}}{h(R)} = \frac{1}{2}\cdot \lim_{\substack{R\in E(K)\\ h_{y^2}(R)\to\infty}} \frac{-\min\{v(y^2(R)), 0\}}{h(R)} = 0.$$

Here we note that in this case, x, y^2 are even functions, and $h_{y^2}(R) = 2h_y(R)$.

Claim. We have $h_x(nP)$ tends to ∞ as n tends to ∞.

Indeed, suppose that there exists $N > 0$ and positive integers $n_1 < n_2 < ...$ such that $h_x(n_iP) < N$ for all n_i, i.e., $h(x(n_iP)) < N\ \forall i \in \mathbb{N}$. Hence $\{x(n_iP)|i \in \mathbb{N}\} \subset K$ takes only finitely many values by Proposition 3.2.4, and then so does $\{y(n_iP)|i \in \mathbb{N}\}$ thanks to the equation defining E. It follows that the set $\{n_iP|i \in \mathbb{N}\}$ is finite, whilst P is non-torsion, a contradiction. This concludes the claim.

Similarly, $h_y(nP)$ also tends to ∞ as $n \to \infty$. Let R run over the set $\{nP|n \in \mathbb{N}\}$, then the two above limits give

$$\lim_{n\to\infty} \frac{-\min\{v(x(nP)), 0\}}{h(nP)} = \lim_{n\to\infty} \frac{-\min\{v(y(nP)), 0\}}{h(nP)} = 0.$$

Since

$$-\min\{v(x(nP)), 0\} - \min\{v(y(nP)), 0)\} \geqslant -\min\{v(x(nP)), v(y(nP)), 0\},$$

we obtain

$$\lim_{n\to\infty} \frac{-\min\{v(x(nP)), v(y(nP)), 0\}}{h(nP)} = 0, \text{ i.e., } \lim_{n\to\infty} \frac{h_v(nP)}{h(nP)} = 0.$$

□

We need a result that helps us indicate whether a non-torsion point is trivial after taking reduction or not.

Lemma 3.2.6. *Let $v \in M_K \setminus S$, and $P \in E(K)$ be non-torsion. Then*

- *If P modulo $\mathfrak{p}_v \neq O$, we have $h_v(P) = 0$.*
- *If P modulo $\mathfrak{p}_v = O$, we have*

$$h_v(nP) = h_v(P) > 0$$

for any $n > 0$ prime to p.

Proof. We may write $P = (x, y)$ and $P = [X : Y : Z]$ in the corresponding projective closure of E ($X, Y, Z \in \mathcal{O}_{K,v}$). The condition P modulo $\mathfrak{p}_v = O$ means that $v(X) > v(Y)$, $v(Z) > v(Y)$, and hence $v(y) < 0$. Therefore, the condition P modulo $\mathfrak{p}_v \neq O$ is equivalent to either $v(X) \leqslant v(Y)$ or $v(Z) \leqslant v(Y)$. If $v(Z) \leqslant v(Y)$, then $v(y) \geqslant 0$, and from $y^2 = x^3 + ax + b$ we obtain $v(x) \geqslant 0$ (since if $v(x) < 0$, then $2v(y) = v(x^3 + ax + b) = 3v(x) < 0$, a contradiction), i.e., $h_v(P) = 0$. If $v(X) \leqslant v(Y)$ and $v(Y) < v(Z)$, then $v(X) < v(Z)$. But then from the homogeneous Weierstrass equation $Y^2Z = X^3 + aXZ^2 + bZ^3$ we obtain

$$2v(Y) + v(Z) = 3v(X),$$

a contradiction. Therefore the first statement is proven. For the second one, from the Weierstrass equation $y^2 = x^3 + ax + b$, we have

$$3v(x) = 2v(y) < 0,$$

and then $h_v(P) = -n_v.v(y) > 0$. Moreover, recall that if we let

$$E_1(K_v) := \{M \in E(K_v) : M \bmod \mathfrak{p}_v = O\},$$

we then have an isomorphism of groups, see Proposition 1.5.10,

$$E_1(K_v) \to F(\mathfrak{p}_v),\ M = (x(M), y(M)) \mapsto z(M) = \frac{-x(M)}{y(M)}.$$

Further, this isomorphism gives us the formula

$$v(y(M)) = -3v(z(M)).$$

Thus via this isomorphism, nP maps to

$$[n].\left(\frac{-x}{y}\right) = n.\left(\frac{-x}{y}\right) + (\text{higher-order terms}),$$

here $[n].\left(\frac{-x}{y}\right)$ is $\left(\frac{-x}{y}\right) + \left(\frac{-x}{y}\right) + ... + \left(\frac{-x}{y}\right)$ (n times) in $F(\mathfrak{p}_v)$. Since $v(x) > v(y)$, $v(n) = 0$ and F is defined over $\mathcal{O}_v$, we obtain

$$v(z(nP)) = v\left([n].\left(\frac{-x}{y}\right)\right) = v\left(\frac{-x}{y}\right) = v(x) - v(y).$$

Consequently, we get

$$v(y(nP)) = -3v(z([n].P)) = 3v(y) - 3v(x) = 3v(y) - 2v(y) = v(y) < 0.$$

Similar to these above arguments, we obtain

$$h_v(nP) = -v(y(nP)), \text{ and hence } h_v(nP) = h_v(P) > 0.$$

□

Now, to prove the main theorem, we will give estimates for places in S (as in Proposition 3.2.5) and places in $M_K \setminus S$ (as in the above lemma) and combine them together to deduce a contradition.

Proof of Theorem 3.2.1. Assume that for any sufficiently large $n > 1$ not divisible by p, $\mathrm{ord}(P \bmod \mathfrak{p}_v)$ does not equal n for any $v \in M_K$. In other words, if nP modulo $\mathfrak{p}_v = O$, then there exists some prime divisor r of n satisfying $\frac{n}{r}P$ modulo $\mathfrak{p}_v = O$. In this case, Lemma 3.2.6 give us

$$h_v(nP) = h_v\left(\frac{n}{r}P\right) \text{ for } v \in M_K \setminus S.$$

It follows that

$$h_v(nP) \leqslant \sum_r h_v\Big(\frac{n}{r}P\Big) \text{ for } v \in M_K \setminus S,$$

where r runs over the set of prime divisors of n.

For $v \in S$, Proposition 3.2.5 give us

$$\lim_{n\to\infty} \frac{h_v(nP)}{h(nP)} = 0.$$

Since $\#S$ is finite, it follows that for any $\epsilon > 0$,

$$h_v(nP) \leqslant \epsilon h(nP)$$

for all large enough integers n. Combining these estimates, we get

$$\begin{aligned} h(nP) = \sum_v h_v(nP) &\leqslant \sum_{v\notin S}\sum_{r|n} h_v\Big(\frac{n}{r}P\Big) + \sum_{v\in S} \epsilon.h(nP) \\ &\leqslant \sum_{r|n} h\Big(\frac{n}{r}P\Big) + \#S.\epsilon.h(nP). \end{aligned}$$

So

$$(1 - \#S.\epsilon)h(nP) \leqslant \sum_{r|n} h\Big(\frac{n}{r}P\Big). \tag{3.3}$$

Now by Proposition 3.2.2, there exists $C > 0$ satisfying

$$\hat{h}(Q) - C < h(Q) < \hat{h}(Q) + C, \forall Q \in E(K).$$

Combining with (3.3) implies

$$(1 - \#S.\epsilon)(\hat{h}(nP) - C) < \sum_{r|n} \hat{h}\Big(\frac{n}{r}P\Big) + C.n$$

since $\#\{\text{prime divisors of } n\} \leqslant n$. Because of the quadraticity of $\hat{h}$, it follows that

$$(1 - \#S.\epsilon)(n^2.\hat{h}(P) - C) < \sum_{r|n} \frac{n^2}{r^2}\hat{h}(P) + C.n < \frac{n^2}{2}\hat{h}(P) + Cn$$

since $\displaystyle\sum_{r|n} \frac{1}{r^2} < \frac{1}{2}$. Therefore

$$\Big(\frac{1}{2} - \#S.\epsilon\Big)n^2.\hat{h}(P) < (n + 1 - \#S.\epsilon).C$$

We choose $\epsilon < \dfrac{1}{2\#S}$ and let n tend to ∞, we obtain $\hat{h}(P) = 0$, which contradicts Proposition 3.2.3 since P is non-torsion. It remains to prove the second claim. Thanks to finiteness theorems and Proposition 3.2.3, it suffices to consider points P such that

$h(P)$ and $\hat{h}(P)$ is very large. Therefore $h_v(nP) = h_v(P)$ for any $n > 0$ prime to p by Proposition 3.2.6 and P is non-torsion since $E(K)^{\text{tors}}$ is finite. Therefore, similarly to the previous arguments, we have for $0 < \epsilon < \dfrac{1}{2\#S}$,

$$h_v(nP) \leqslant \epsilon h(nP)$$

for all positive integer n prime to p. Thus, as above, if for any $v \in M_K$, $\text{ord}(P \bmod \mathfrak{p}_v)$ does not equal some n prime to p, we then have

$$\left(\frac{1}{2} - \#S.\epsilon\right) n^2.\hat{h}(P) < (n + 1 - \#S.\epsilon)C,$$

i.e., $\hat{h}(P)$ is bounded, a contradiction.

□

Remark. We note that the condition $\gcd(n, p) = 1$ is necessary. For example, consider a supersingular elliptic curve E over K (for instance, we take E to be the base change to K of a supersingular elliptic curve over $\mathbb{F}_q$). Then $[p]$ is an isomorphism, and so for almost all $v \in M_K$

$$E_{\mathfrak{p}_v} \xrightarrow{[p]} E_{\mathfrak{p}_v}$$

is also an isomorphism, where E_v is the reduction modulo $\mathfrak{p}_v$ of E (see [5] Proposition 1.3.1 for the number field case and we note that the proof also works for global function fields). Hence, for almost all v, $E_{\mathfrak{p}_v}$ is a supersingular elliptic curve, and then $E_{\mathfrak{p}_v}[n] = E_{\mathfrak{p}_v}[np]$ for all integer n. Therefore, for almost all v, $\text{ord}\, P \bmod \mathfrak{p}_v$ must be prime to p.

When E is ordinary, we have (see [32])

Theorem 3.2.7. *Let E be an ordinary elliptic curve over some global function field K of characteristic $p \neq 2, 3$ and let $P \in E(K)$ be a non-torsion point. We fix a positive integer t. Then for every sufficiently large n prime to p, there exists $\mathfrak{p} \in M_K$ of good reduction so that $\text{ord}(P \bmod \mathfrak{p})$ is equal to np^t.*

Proof. Because E is ordinary, there exists $Q \in E(\bar{K})$ of order p^t. Set $L := K(E[p^t])$ the p^t-division field of E, and denote E_L the base change of E to L. Then $P - Q \in E_L(L)$ is also a non-torsion point. We recall the following properties of the reduction of points.

1. For almost all $\mathfrak{p} \in M_K$, we have for any $\mathfrak{q} \in M_l$ above $\mathfrak{p}$, the order of P (as an $L-$point of E_L) modulo $\mathfrak{q}$ equals the order of P modulo $\mathfrak{p}$.

2. Since Q is torsion, the order of Q modulo $\mathfrak{q}$ equals the order of Q, which is p^t, for almost all $\mathfrak{q} \in M_L$.

We call V the set of *exceptional primes* of K in (1) and call U the set of *exceptional primes* of L in (2) and primes of L lying above primes in V. Then both V and U are finite. Now we apply Theorem 3.2.1 for $P-Q \in E_L(L)$, we have for every sufficiently large integer n prime to p, there exists $\mathfrak{q} \in M_L$ of good reduction so that $P-Q$ modulo $\mathfrak{q}$ is of order n. Since U is finite, $\mathfrak{q} \notin U$ n sufficiently large. Since $np^tP = np^t(P-Q) + np^tQ = np^t(P-Q)$, the point np^tP modulo $\mathfrak{q}$ equals O. So P modulo $\mathfrak{q}$ has the order of the form mp^s where $m|n$ and $s \leqslant t$. Then

$$O = mp^tP \bmod \mathfrak{q} = mp^tQ + mp^t(P-Q) \bmod \mathfrak{q} = mp^t(P-Q) \bmod \mathfrak{q},$$

and hence, $n|mp^t$ which implies that $m = n$. Similarly we have

$$O = np^sP \bmod \mathfrak{q} = np^sQ + np^s(P-Q) \bmod \mathfrak{q} = np^sQ \bmod \mathfrak{q}.$$

Thus $p^t|np^s$ which means that $s = t$. Therefore the order of P modulo $\mathfrak{q}$ is np^t. Since $\mathfrak{p}$, the prime of K lying under $\mathfrak{q}$, does not lie in V, the order of P modulo $\mathfrak{p}$ also equals np^t. The theorem is then proven. □

3.3 Semi-Abelian Varieties

In this section, we summarize the Kummer theory for abelian varieties after Ribet [34]. We also assume that K is always a number field. The reason why we need this condition is that we need a theorem of Serre on the homotheties of the group G_l associated to an abelian variety, see the discussion in 3.3.2. Then we apply this theory to give a proof of Theorem 0.0.3 in Section 3.3.2.

3.3.1 Kummer Theory

Classical Kummer theory aims to describe the Galois group of a field extension of K obtained by adjoining mth roots elements of some elements in K (also called the m-**division field**) of a torus $\mathbb{G}_m$. Similar questions arises when one considers the division fields of abelian varieties and semi-abelian varieties. A lot of amazing results were established by J. Serre, D. Bertrand, K. Ribet, etc. Here, we summarize some results of K. Ribet that we need. The main references are his paper [34] and Bertrand's paper [35]. Let G be a semi-abelian variety over K with the affine part T and the abelian part A. For $t, l \geqslant 1$ and $P_1, ..., P_t \in G(K)$, we want to understand the Galois group of the extension

$$K\Big(G[l], \frac{1}{l}P_1, ..., \frac{1}{l}P_t\Big)/K(G[l]).$$

Ribet showed that in some certain circumstances, this group can be as large as possible. From now on, l will always be a prime number. First we have some observations. The group $G[l]$ is isomorphic to $(\mathbb{Z}/b\mathbb{Z})^b$ where b is the first Betti number of G (dimension of its first étale cohomology): when G is a split torus $\mathbb{G}_m^g$ (resp. an abelian variety), b is equal to $\dim G$ (resp. $2\dim G$). Recall that we $\mathrm{Gal}(\bar{K}/K)$ acts on $G[l]$ via

$$\rho_l : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(G[l]) = \mathrm{GL}_b(\mathbb{Z}/l\mathbb{Z}).$$

Its kernel is $\mathrm{Gal}(\bar{K}/K(G[l]))$, and its image $G_l \cong \mathrm{Gal}(K(G[l])/K)$. For a point $P \in G(K)$, and for any $l-$th division points $Q \in \frac{1}{l}P$, we have the map (so-called Kummer map)

$$\xi(P) : \ker(\rho_l) \to G[l], \sigma \mapsto \sigma(Q) - Q.$$

We then obtain a map

$$\xi : G(K)/lG(K) \to H^1(\ker(\rho_l), G[l]), P \mapsto \xi(P).$$

In fact, Galois cohomology theory tells us that this map is the composition of the coboundary map

$$G(K)/lG(K) \hookrightarrow H^1(\mathrm{Gal}(\bar{K}/K), G[l])$$

and the restriction map

$$H^1(\mathrm{Gal}(\bar{K}/K), G[l]) \to H^1(\ker(\rho_l), G[l]).$$

For $P_1, ..., P_n \in G(K)$, let

$$\varphi : \ker(\rho_l) \to G[l]^n$$

be the product of $\xi(P_i)$. Then the kernel of φ is

$$\mathrm{Gal}\Big(\bar{K}/K\Big(G[l], \frac{1}{l}P_1, ..., \frac{1}{l}P_n\Big)\Big).$$

Now we state the main result in the paper of Ribet, see [34] Theorem 1.2.

Theorem 3.3.1. *Let t be an integer with $0 \leqslant t \leqslant n$. Assume that the points $P_1, ..., P_t$ are linearly independent over $\mathrm{End}_K(G)$, modulo the points $P_{t+1}, ..., P_n$. Further, suppose that G satisfies four axioms B_1, B_2, B_3, B_4 stated below. Then for almost all primes l, the image of φ contains*

$$G[l]^t \times 0^{n-t} = (G[l] \times ... \times G[l]) \times (0 \times ... \times 0).$$

In other words, the Galois group of the field extension

$$K\Big(G[l], \frac{1}{l}P_1, ..., \frac{1}{l}P_n\Big)/K\Big(G[l], \frac{1}{l}P_{t+1}, ..., \frac{1}{l}P_n\Big),$$

which is the subgroup of $G[l]^t$ obtained by intersecting $\mathrm{Im}(\varphi)$ with $G[l]^t \times 0^{n-t}$, is as large as possible for almost all l.

Now we will explain that what the assumption in this theorem means.

Definition 3.3.2. Let M be a left module over a (not necessarily commutative) ring R, and let $m_1, ..., m_t$ be elements in M. These elements are said to be **linearly independent** (over R) if the equation

$$r_1 m_1 + ... + r_t m_t = 0$$

implies that the $r_i = 0, \forall i$. In addition, when N is an R-submodule of M, we say that the m_i are **linearly independent** mod N if their images in M/N are linearly independent. In particular, when N is generated over R by elements $\{n_j\}$ of M, we then say that m_i's are independent mod n_j's.

In out situation, the ring $\mathrm{End}_K(G)$ acts on the points $P_1, ..., P_n$.

Definition 3.3.3. For a point $P \in G(K)$, let $G_P := (\mathbb{Z}P)^{\mathrm{zar}}$ and we denote G_P^o its connected component. Then P is said to be **independent** in G if $G_P = G$. Here, one can show that P is independent in G if and only if the left $\mathrm{End}_K(G)$-submodule of $G(K)$ generated by P is free, see [5] Remark 3.3.2.

Now we describe Ribet's four axioms mentioned in Theorem 3.3.1.

- Axiom B_1: For almost all primes l, $\mathrm{End}_K(G)/l\,\mathrm{End}_K(G)$ equals the commutant of $G[l]$ in $\mathrm{End}(G[l])$.
- Axiom B_2: For almost all primes l, the $\mathrm{Gal}(K(G[l])/K)-$module $G[l]$ is semisimple.
- Axiom B_3: For almost all primes l, $H^1(\mathrm{Gal}(K(G[l])/K), G[l])$ vanishes.
- Axiom B_4: For each finitely generated subgroup Γ of $G(K)$, the group

  $$\Gamma' = \{Q \in G(K) | mQ \in \Gamma \text{ for some } m \geqslant 1\}$$

  satisfies Γ'/Γ has finite exponent.

The key insight in the proof of this theorem is that $G_l = \mathrm{Gal}(K(G[l])/K)$ has a natural action on $\mathrm{Gal}\Big(K\Big(G[l], \frac{1}{l}P\Big)/K(G[l])\Big)$ (resp. $\mathrm{Im}(\xi(P))$) via conjugation (resp. ρ_l). In other words, we have

$$\xi(P)(\tau\sigma\tau^{-1}) = \tau\Big[\xi(P)(\sigma)\Big]$$

for $\sigma \in \ker(\rho_l)$ and $\tau \in \mathrm{Gal}(\bar{K}/K)$. Note that when $G = A$ is an abelian variety, we have

- Axiom B_1 holds, see [36] Property (b) p.400.
- Axiom B_2 holds. It is a direct consequence of Falting's Theorem (Tate conjecture) which says that $\rho : \mathrm{Gal}(\bar{K}/K) \to V_l(A) = T_l(A) \otimes \mathbb{Q}_l$ is semisimple, see [22] Chapter 2 Theorem 4. Indeed, let W be a $\mathrm{Gal}(\bar{K}/K)$-stable subgroup of $A[l]$. Then its preimage V under the projection $T_l(A) \twoheadrightarrow T_l(A)/lT_l(A) = A[l]$ is a $\mathrm{Gal}(\bar{K}/K)$-stable submodule of $T_l(A)$. Therefore its complement V' projects down to $W' \subset A[l]$ which is stable under $\mathrm{Gal}(\bar{K}/K)$.
- Axiom B_3 holds, thanks to the vanishing of $H^i(\mathrm{Gal}(K(A[l^\infty])/K), T_l(A))$ for almost all l and for all $i \geqslant 0$, see [37] Theorem 2.4, and the injectivity of the inflation map

$$H^1(\mathrm{Gal}(K(A[l])/K), A[l]) \hookrightarrow H^1(\mathrm{Gal}(K(A[l^\infty])/K), T_l(A)).$$

- Axiom B_4 holds because it is a direct consequence of the Mordell-Weil theorem.

Therefore, this theorem can by applied for abelian varieties. However, we want to know whether those axioms are satisfied by semi-abelian varieties. To deal with it, we need an extra axiom (for A).

- Axiom B_3^+: A satisfies axiom B_3 and for almost all l, we have

$$H^1(\mathrm{Gal}(K(A[l])/K), \mu_l) = 0.$$

Here, we recall that (see Corollary 1.2.30) the division field $K(A[l])$ contains μ_l. Therefore $\ker(\rho_l) = \mathrm{Gal}(\bar{K}/K(A[l]))$ acts trivially on μ_l, and hence, we have an action of $G_l = \mathrm{Gal}(K(A[l])/K) = \mathrm{Gal}((\bar{K}/K)/\ker(\rho_l))$ on μ_l. Furthermore, we have

- Axiom B_3^+ holds for all abelian varieties. Indeed, it follows from the two following lemmas.

Lemma 3.3.4 (Sah's theorem, see [38] Theorem 5.1)**.** *Let H be a group and let M be a H-module. Let $\alpha \in Z(H)$, the center of H. Then $H^1(H, M)$ is annihilated by the map*

$$x \mapsto \alpha.x - x$$

on M. Particularly, if this map is an automorphism of M, then $H^1(H, M) = 0$.

From this lemma, we see that axiom B_3^+ is a consequence of

Lemma 3.3.5. *G_l contains a homothety $[d] \in \mathbb{F}_l^\times$ of $\mathrm{Aut}(A[l])$ such that $d \not\equiv \pm 1 \bmod l$ for almost all l.*

Now for l very large, we choose $\alpha \in G_l$ correspond to $[d] \in \mathbb{F}_l^\times \subset G_l$. We choose a polarization $\lambda : A \to \hat{A}$. It then induces a homomorphism between Galois modules $\lambda[l] : A[l] \to \hat{A}[l]$ which is an isomorphim since l is large. Therefore $e_l^\lambda : A[l] \times A[l] \to \mu_l$ is non-degenerate. Thus, there exists $a, b \in A[l]$ such that $e_l(a,b) = \xi_l$, an $l-$primitive root of unity. Then

$$\xi_l^{\alpha^2} = e_l(a,b)^{\alpha^2} = e_l(\alpha.a, \alpha.b) = \alpha.e_l(a,b) = \alpha.\xi_l,$$

and hence $\dfrac{\alpha.\xi_l}{\xi_l} = \xi_l^{d^2-1}$ which is another $l-$primitive root of unity because $d^2 - 1$ is coprime to l. So the map $\mu_l \to \mu_l, x \mapsto \alpha.x - x$ is an automorphism. Therefore $H^1(G_l, \mu_l) = 0$.

Proof of the lemma. Serre proved in the $l-$ adic situation that the group of homotheties C_l of $\mathrm{Im}(\rho_l)$, where $\rho_l : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_l(A))$ (also denote by ρ_l), has bounded index c (independently of l) in $\mathbb{Z}_l^\times$, see [39] section 2. Suppose that for some l very large, C_l, the group of homotheties (mod l) in G_l, is contained in J_l the group of homoteties congruent to ± 1 mod l. So $c > \#Z_l^\times/C_l \geqslant \#Z_l^\times/J_l = \dfrac{l-1}{2}$, it can not happen when l is sufficiently large. □

Now we turn to the case $G = T \times A$ for a torus T and an abelian variety A. As above, G satisfies Axiom B_4. For other axioms, we have

Proposition 3.3.6. *Suppose that axioms B_1, B_2, and B_3^+ hold for all abelian varieties over all number fields. Then the axioms B_1, B_2, B_3, B_4 hold for G.*

Proof. See [34] Theorem 2.6. □

Therefore, we can apply Theorem 3.3.1 for $G = T \times A$. We then have

Proposition 3.3.7. *Let $G = T \times A$, and $P \in G(K)$. Then for almost all primes l, $\mathrm{Gal}\Big(K\Big(G[l], \frac{1}{l}P\Big)/K(G[l])\Big) \cong G_P^o[l]$. In particular, there exists $c = c(G,P) > 0$ such that for all primes l, the group*

$$\mathrm{Gal}\Big(K\Big(G[l], \frac{1}{l}P\Big)/K(G[l])\Big)$$

is isomorphic to a subgroup $\mathrm{Im}(\xi(P))$ of $G_P^o[l]$ of index bounded by c.

Proof. Because P is independent in G_P, we can apply Theorem 3.3.1. Thus for almost all primes l, the image of $\xi(P)$, $\mathrm{Gal}\Big(K\Big(G[l], \frac{1}{l}P\Big)/K(G[l])\Big)$, contains $G[l]$. Therefore $\mathrm{Gal}\Big(K\Big(G[l], \frac{1}{l}P\Big)/K(G[l])\Big) = G[l]$. It remains to show that $\mathrm{Im}(\xi(P))$ lies in the group $G_P^o[l]$. First, we show that it lies in $G_P[l]$ (which is a subgroup of $G[l]$). We pick

$Q \in \frac{1}{l}P \subset G_P(\bar{K})$ (exists since G_P is also a semi-abelian variety and so $G_P[l]$ is non-empty) and then for $\sigma \in \ker(\rho_l) = \mathrm{Gal}(\bar{K}/K(G[l])) \subset \mathrm{Gal}(\bar{K}/K(G_P[l]))$, $\sigma(Q) - Q$ lies in $G_P(\bar{K})$, and hence in $G_P[l]$. Therefore, $\mathrm{Im}(\xi(P)) \subset G_P[l]$. In addition, for $l > \#G_P/G_P^o$, the number of connected components of G_P, the exact sequence

$$0 \to G_P^o[l] \hookrightarrow G_P[l] \to \frac{G_P}{G_P^o}[l] = 0$$

implies that $G_P[l] = G_P^o[l]$. The proposition is then proven. □

Remark. The procedure above also holds for a power of a prime l. In other words, we can replace $G[l]$ by $G[l^s]$, μ_l by μ_{l^s}, etc. Similarly, we have

Proposition 3.3.8. *Let $G = T \times A$, and $P \in G(K)$. Then for almost all primes l and all $s \geqslant 0$, $\mathrm{Gal}\Big(K\Big(G[l^s], \frac{1}{l^s}P\Big)/K(G[l^s])\Big)$ is isomorphic to $G_P^o[l^s]$.*

For arbitrarily l (not necessarily prime), we can not have the similar result for almost all l. Instead, we have a quite stronger (in some sense) result involving uniformly bounded constant.

Theorem 3.3.9 (see [35] Theorem 1)**.** *Let $G = T \times A$, and assume that G_P is connected for some $P \in G(K)$. Then there exists $c = c(G, P) > 0$ such that for all positive integers n, $\mathrm{Gal}\Big(K\Big(G[n], \frac{1}{n}P\Big)/K(G[n])\Big)$ is isomorphic to a subgroup $\mathrm{Im}(\xi(P))$ of $G_P[n]$ of index bounded by c.*

Remark. Proposition 3.3.8 and Theorem 3.3.9 implies that $\mathrm{Gal}(K_{P,\infty}/K_\infty)$ is isomorphic to an open subgroup of $T_\infty(G_P)$ where $K_\infty = K(G^{\mathrm{tors}}) = K(\cup_{n>0} G[n])$, $K_{P,\infty} = \bigcup_{n>0} K_\infty\Big(\frac{1}{n}P\Big)$, and $T_\infty = \prod_{l \text{ prime}} T_l$.

3.3.2 A Proof of Theorem 0.0.3

In this section, we will prove Theorem 0.0.3 by using Kummer theory. We will need some auxiliary results. First, we need a

Lemma 3.3.10. *Let G be a semi-abelian variety over K, a prime number l such that that $G[l] \subset G(K)$. Then $[K(G[l^n]) : K]$ and $\Big[K\Big(\frac{1}{l^n}P\Big) : K\Big]$ are powers of l for all $n > 0$ and $P \in G(K)$.*

Remark. $K\Big(\frac{1}{m}P\Big) = K\Big(G[m], \frac{1}{m}P\Big), \forall m > 0.$

Proof. Since $G[l] \subset G(K)$, we have an injective homomorphism

$$\mathrm{Gal}(K(G[l^n])/K) \hookrightarrow \mathrm{End}_{G[l]}(G[l^n]), \sigma \mapsto (\sigma : Q \mapsto \sigma(Q)).$$

Since $G[l^n] \cong (\mathbb{Z}/l\mathbb{Z})^{2\dim G}$, we obtain the first claim. In addition, since $\left[K\left(\frac{1}{l^n}P\right) : K\right] = \left[K\left(\frac{1}{l^n}P\right) : K(G[l^n])\right].[K(G[l^n]) : K]$, we need that $\left[K\left(\frac{1}{l^n}P\right)/K(G[l^n])\right]$ is a power of l. We have the Kummer map

$$\phi_n : \mathrm{Gal}\left(K\left(\frac{1}{l^n}P\right)/K(G[l^n])\right) \to G[l^n] \cong (\mathbb{Z}/l\mathbb{Z})^{2\dim G}; \sigma \mapsto \sigma\left(\frac{1}{l^n}Q\right) - \frac{1}{l^n}Q,$$

where Q is a fixed nth root of P (when $n = 1$, we obtain $\xi(P)$). It is straightforward to check that ϕ_n is injective. The claim follows. □

Lemma 3.3.11. *Let G be a product of a torus and an abelian variety over K, and $P \in G(K)$ is an independent point. The for n sufficiently large, we have*

$$K\left(\frac{1}{l^n}P\right) \cap K(G[l^{n+1}]) = K(G[l^n]).$$

Proof. We need to show that the restriction map

$$\alpha_n : \mathrm{Gal}\left(K\left(\frac{1}{l^{n+1}}P\right)/K(G[l^{n+1}])\right) \to \mathrm{Gal}\left(K\left(\frac{1}{l^n}P\right)/K(G[l^n])\right)$$

is surjective for n large enough since this map factors as

$$\begin{aligned}\mathrm{Gal}\left(K\left(\frac{1}{l^{n+1}}P\right)/K(G[l^{n+1}])\right) &\to \mathrm{Gal}\left(K\left(\frac{1}{l^{n+1}}P\right)/\left(K(G[l^{n+1}]) \cap K\left(\frac{1}{l^n}P\right)\right)\right) \\ &\to \mathrm{Gal}\left(K\left(\frac{1}{l^n}P\right)/K(G[l^n])\right).\end{aligned}$$

Next, diagram chasing gives us a surjective map $\beta_n : \mathrm{Coker}\,\phi_{n+1} \twoheadrightarrow \mathrm{Coker}\,\phi_n$ satisfies the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Gal}\left(K\left(\frac{1}{l^{n+1}}P\right)/K(G[l^{n+1}])\right) & \xrightarrow{\phi_{n+1}} & G[l^{n+1}] & \longrightarrow & \mathrm{Coker}\,\phi_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle [l]} & & \downarrow{\scriptstyle \beta_n} & & \\ 0 & \longrightarrow & \mathrm{Gal}\left(K\left(\frac{1}{l^n}P\right)/K(G[l^n])\right) & \xrightarrow{\phi_n} & G[l^n] & \longrightarrow & \mathrm{Coker}\,\phi_n & \longrightarrow & 0 \end{array}$$

Note that α_n is surjective if and only if β_n is injective. In addition, since β_n is surjective, it remains to show that the two groups $\mathrm{Coker}\,\phi_{n+1}$ and $\mathrm{Coker}\,\phi_n$ have the same order for n large. Since P is independent, Theorem 3.3.9 implies that $\mathrm{Coker}\,\phi_n$ is bounded by c which does not depend on n. So the lemma follows. □

Lemma 3.3.12. *Again, let $G = T \times A$ be a product of a split torus and an abelian variety over K, and l is an arbitrary prime. Then*

1. *If T is zero or A is zero or $l > 2$, then n large enough, there exists $h_l \in \mathrm{Gal}(\bar{K}/K)$ which acts as an automorphism of $G[l^\infty]$ whose set of fixed points is $G[l^n]$.*

2. *If T and A are non-zero and $l = 2$, the for n sufficiently large, there exists $h_2 \in \mathrm{Gal}(\bar{K}/K)$ acting on $G[2^\infty]$ whose fixed points are $T[2^{n+1}] \times A[2^n]$.*

Proof. 1. When $T = 0$, because $\mathrm{Gal}(K[l^\infty]/K)$ is a subgroup of finite index in $\mathbb{Z}_l^\times$, it is open. So it must contains a ball B_n of radius l^{-n} around 1, and hence, a homothety h_l such that $h_l \equiv 1 \bmod l^n$ and $h_l \not\equiv 1 \bmod l^{n+1}$. Therefore, the set of fixed points of h_l is $A[l^n]$.

2. When $A = 0$, we note that when n large enough, $K(\mu_{l^{n+1}})/K(\mu_{l^n})$ is an non-trivial Galois extension, and we take h_l to any non-trivial element in the Galois group.

3. When T and A are non-zero and l is odd, then $A \times \hat{A}$ is also non-zero. So there is $h_l \in \mathrm{Gal}(\bar{K}/K)$ such that h_l acts as a homothety on $(A \times \hat{A})[l^\infty]$ and $h_l \equiv 1 \bmod l^n$, $h \not\equiv 1 \bmod l^{n+1}$. As usual, the Weil pairing gives us $a \in A[l^n]$ and $\mathcal{L} \in \hat{A}[l^n]$ such that

$$e_{l^n}(a, \mathcal{L}) = \xi_{l^n}, \text{ an } l^n\text{th primitive root of unity.}$$

So we have

$$h_l(\xi_{l^n}) = h_l(e_{l^n}(a, \mathcal{L})) = e_{l^n}(h_l(a), h_l(\mathcal{L})) = e_{l^n}(h_l.a, h_l.\mathcal{L}) = \xi_{l^n}^{h_l^2}.$$

Therefore, h_l also acts on μ_{l^n} as a homothety with factor h_l^2. Since l is odd, we have $h_l^2 \equiv 1 \bmod l^n$ and $h_l^2 \not\equiv 1 \bmod l^{n+1}$, and so for n large enough, the homothety h_l satisfies the claim.

4. When T and A are non-zero and $l = 2$, the proof in of case is similar. Note that in this cae, $h_2^2 \equiv 1 \bmod 2^{n+1}$ and $h_2 \not\equiv 1 \bmod 2^{n+2}$, so its set of fixed points of G is $T[2^{n+1}] \times A[2^n]$.

□

Proof of Theorem 0.0.3. We note that G_P is also a product of a torus T and an abelian variety A over F, and P is an independent point on G_P. Let $R \in \frac{1}{2}P$, then R is also independent in G_P. Let S be the set of prime divisors of m, and E be a finite extension of F such that $R \in G_P(E)$, T is split over E, and $G_P[l]$ is defined over E for every $l \in S$. We then have

$$K'\left(\frac{1}{l^n}R\right) \cap K'(G[l^{n+1}]) = K'(G[l^n])$$

for n sufficiently large. Furthermore, there exists h_l for each $l \in S$ as in the previous lemma. Now, let L be the compositum of all $E\left(\frac{1}{l^n}R\right)$ and $E(G[l^{n+1}])$ for $l \in S$.

Thanks to Lemma 3.3.10, the fields $E\Big(\frac{1}{l^n}R, G[l^{n+1}]\Big)$, $l \in S$, are linearly disjoint over K'. By Galois theory, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\forall\ l \in S$, the restriction of σ to $|K'\Big(\frac{1}{l^n}R\Big)$ is the identity, and the restriction of σ to $|K'(G[l^{n+1}])$ is equal to the restriction of h_l to $|K'(G[l^{n+1}])$. Now by Theorem 1.1.4, there exists a set of primes $\mathfrak{p}$ of K unramified in L whose Dirichlet density is positive such that

$$\Big(\frac{L/K}{\mathfrak{p}}\Big) = \mathcal{C}^\sigma,$$

the conjugacy class of $\sigma \in \mathrm{Gal}(L/K)$. Therefore, for such $\mathfrak{p}$, there exists $\mathfrak{m} \in M_L$ above $\mathfrak{p}$ such that $\mathrm{Frob}_{L/K}\,\mathfrak{m} = \sigma$, and then we let $\mathfrak{q}$ be a prime of F below $\mathfrak{m}$.

$$\begin{array}{ccc} L & \text{———} & \mathfrak{m} \\ | & & | \\ F & \text{———} & \mathfrak{q} \\ | & & | \\ K & \text{———} & \mathfrak{p} \end{array}$$

Now for $l \in S$, suppose that l divides $\mathrm{ord}(R \bmod \mathfrak{q})$. After excluding finitely many $\mathfrak{p}$, $\mathrm{ord}(R \bmod \mathfrak{m})$ is also divisible by l. Now let $Z \in G_P(L)$ such that $l^n Z = R$. Then $\mathrm{ord}(Z \bmod \mathfrak{m})$ is divisible by l^{n+1} (resp. 2^{n+2} when $l = 2$). Then there exists $a \geqslant 1$ such that $\mathrm{ord}(aZ \bmod \mathfrak{m}) = l^{n+1}$ (resp. 2^{n+2} when $l = 2$). Therefore, by Proposition 1.4.10, there exists $X \in G_P(L)$ of order l^{n+1} (resp. 2^{n+2} when $l = 2$) subjects to

$$(aZ \bmod \mathfrak{m}) = (X \bmod \mathfrak{m}).$$

Now, because $\mathrm{Frob}_{L/K}\,\mathfrak{m}$ commute with red mod $\mathfrak{m}$ for almost all $\mathfrak{p}$ Therefore, after excluding finitely many $\mathfrak{p}$, we have that $(aZ \bmod \mathfrak{m})$ is fixed by $\mathrm{Frob}_{L/K}\,\mathfrak{m}$ (because $\sigma = \mathrm{id}$ on $|K'\Big(\frac{1}{l^n}R\Big)$), while $(X \bmod \mathfrak{m})$ is not fixed by $\mathrm{Frob}_{L/K}\,\mathfrak{m}$ (since the set of fixed points of σ in $G_P[l^{n+1}]$ is $G_P[l^n]$), we obtain a contradiction. In other words, after ruling out finitely many $\mathfrak{p} \in M_K$ (the Dirichlet density of this set is 0), $\mathrm{ord}\, R \bmod \mathfrak{q}$ is prime to m. Since the remaining set of primes still has positive Dirichlet density, the theorem is then proven. □

Other questions

Now, K is an arbitrarily field. First we note the followings well-known classification result.

Proposition 3.3.13. *Let G be a one-dimensional connected smooth algebraic group over K. Then, one of the following holds:*

- $G_{\bar{K}} \cong \mathbb{G}_{a,\bar{K}}$
- $G_{\bar{K}} \cong \mathbb{G}_{m,\bar{K}}$
- *G is an elliptic curve.*

For the additive group, it is clearly that the set in Question 3 is infinite, while for the other cases, it is finite as we see above. For higher dimensions, it is still not known whether this set is finite or infinite. For instance, when $G = (\mathbb{G}_m)^2$ over $K = \mathbb{Q}$, and $(a, b) \in G$ is an independent point (i.e., $\mathbb{Z}(a, b)$ is Zariski-dense, and in this case, it means that a and b are multiplicatively independent) and suppose that $\gcd(a-1, b-1) = 1$, then the set

$$\{n \in \mathbb{N} : \nexists \text{a prime number } p \text{ such that } n = \mathrm{ord}((a, b) \bmod p)\}$$

is infinite iff there are infinitely many $n \geqslant 1$ satisfying

$$\gcd(a^n - 1, b^n - 1) = 1.$$

The latter claim that there are infinitely many $n \geqslant 1$ such that $\gcd(a^n - 1, b^n - 1) = 1$ is a conjecture of Ailon and Rudnick, see [40] Conjecture A.

One also could ask whether Theorem 0.0.3 holds for global function fields. As we see in the proof, the number field case follows from the following results:

- Kummer theory for product of tori and abelian varieties
- Serre's theorem on homotheties (the openness of the subgroup of homotheties in $\mathbb{Z}_l^\times$ is due to Bogomolov)
- Chebotarev's density theorem

The Kummer theory is based the Mordell-Weil theorem and the Dirichlet's $S-$unit theorem, Serre's theorem on homotheties, Falting's theorem on the semisimplicity of the representation of Tate modules. The result of Falting also holds for global function fields of characteristic greater than 2 due to Zarhin, see [22] Chapter 1 section 7. For Serre's theorem on homotheties, it seems that there does not exist similar theorem for global function field. We note that the theorem is motivated by Serre's open image theorem, see Theorem 1.2.35, and in global function field case, we have

Theorem 3.3.14 (Igusa's theorem, see [41] Theorem 1.4)**.** *Considering an isotrivial elliptic curve E over a global function field $K/\mathbb{F}_q$. Here, E is said to be* ***isotrivial*** *if*

its $j-$invariant $\mathrm{j}(E) \notin \bar{\mathbb{F}}_q$. *Let* $n > 0$ *be prime to* p, *and let* Γ_n *be the inverse image of* $H_n :=< p >\subset (\mathbb{Z}/n\mathbb{Z})^\times$ *under the determinant map in the short exact sequence*

$$1 \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times \to 1.$$

In other words, we have a short exact sequence

$$1 \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \Gamma_n \xrightarrow{\det} H_n \to 1.$$

Then one can deduce from the Weil pairing for E *that* $\mathrm{Gal}(K(E[n])/K) \subset \Gamma_n$. *Furthermore, if for a prime* l *coprime to* q, *if* $\hat{\Gamma}_l$ *is the inverse limit of* $\{\Gamma_{l^s}\}_{s>0}$, *then* $\mathrm{Gal}(K(E[l^\infty]/K))$ *is open in* $\hat{\Gamma}_l$ *for all* l *coprime to* p, *and equals* $\hat{\Gamma}_l$ *for almost all* l.

Although it is not clear whether Serre's theorem on homotheties hold in the case in Theorem, we can still prove Theorem 0.0.3 for elliptic curves over global function fields because we only need to choose homotheties involving some congruence conditions which are still statisfied thanks to Isuga's theorem.

Lastly, we can ask similar questions for Drinfeld modules (which are well-known objects to work with global function fields).

Definition 3.3.15. Let $K := K(C)$ be the function field of a smooth projective geometrically integral curve C over $\mathbb{F}_q$. We fix a closed point ∞ and let A be the ring of regular functions outside ∞.

1. An $A-$**field** $\mathcal{F}$ is a field equipped with a fixed morphism $\iota : A \to \mathcal{F}$.

2. A **Drinfeld module** over $\mathcal{F}$ is a homomorphism of $\mathbb{F}_q-$algebras $\phi : A \to \mathcal{F}\{\tau\}$ such that
$$\phi_a = \iota(a)\tau^0 + (\text{higher order terms in } \tau), \forall a \in A$$
and $\phi_a \neq \iota(a)$ for some $a \in A$.

Drinfeld modules admit a lot of similar objects like abelian varieties, such as Tate modules and Galois representations (e.g. by Pink and his students), Reductions (e.g. by Takahasi), Height machinery (e.g. by Denis and Poonen). For example, one has a Mordell-Weil type theorem for Drinfeld modules due to Poonen, see [42] Theorem 1.

Theorem 3.3.16. *Let* ϕ *be a Drinfeld* A*-module over a finite extension* L *of* K. *Then the* $A-$*module* $\phi(L)$ *(i.e, the additive group* L *with an action of* A *via* $a \mapsto \phi_a$*) is the direct sum of a finite torsion module and a free* $A-$*module of countably infinite rank.*

So, for example, we have the following question

Question (2)**.** Let ϕ be a Drinfeld A-module over K and consider the $A-$module $\phi(K)$. One can take reduction modulo $\mathfrak{p}$ of ϕ for almost all $\mathfrak{p}$ to get a Drinfeld module $\phi_{\mathfrak{p}} : A/\mathfrak{p} \to K\{\tau\}$. Let $x \in K$ be a point that is not annihilated by $\phi(A)$. Is the following set

$$\{n \in \mathbb{N} : \gcd(n, q) = 1 \text{ and } \nexists \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K \text{ such that } n \text{ is the smallest positive integer satisfying } \phi_{\mathfrak{p}}(n)x = 0\}$$

finite? Here, since $A/\mathfrak{p}$ is a finite field extension of $\mathbb{F}_q$, we can consider n as an invertible element in $A/\mathfrak{p}$.

In the future, we want to find similar results of Schinzel - Postnikova for Drinfeld modules, and similar result of Perucca for elliptic curves (product with tori) over global function fields and for Drinfeld modules, and for other geometric objects.

Conclusion

In this thesis, we have presented the following.

1. On the arithmetic side, we presented some properties of global fields, especially some finiteness theorems for global function fields.

2. On the geometric side, we gave some properties of algebraic groups, especially linear algebraic groups (including tori), and abelian varieties (including elliptic curves), and semi-abelian varieties that we need. We also describe the notion of integral models, formal groups, and the reductions of points on those geometric objects which are used to prove the main results.

3. We gave constructions of height functions on elliptic curves over global fields. As a consequence of height machinery, we prove the Mordell-Weil theorem for elliptic curves, and some finiteness theorems for integral points on some affine curves over global function fields.

4. Finally, we describe the problems concerning the order of the reduction of a rational point on tori, elliptic curves, and semi-abelian varieties and gave some partial results extending Schinzel-Postnikova and Cheon-Hahn to global function fields. We also sketch the Kummer theory for abelian varieties over number fields due to Ribet. Relating to those problems, we propose some questions to study in the future.

Bibliography

[1] L. P. Postnikova and A. Schinzel, "Primitive divisors of the expression $a^n - b^n$ in algebraic number fields," *Math. USSR Sb.*, vol. 4, no. 153, p. 153–159, 1968.

[2] J. Cheon and S. Hahn, "The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve," *Acta Arithmetica*, vol. **88**, no. 3, pp. 219–111, 1999.

[3] H. G. Zimmer, "On the difference of the Weil height and the Néron-Tate height," *Mathematische Zeitschrift*, vol. **147**, pp. 35–52, 1976.

[4] J. V. Armitage, "The Thue-Siegel-Roth theorem in characteristic p," *Journal of Algebra*, vol. **9**, no. 2, pp. 183–189, 1999.

[5] A. Perucca, *On the order of the reductions of points on abelian varieties and tori.* PhD thesis, Universita di Roma La Sapienza, 2008.

[6] M. Rosen, *Number Theory in Function Fields*, vol. **210** of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2002.

[7] B. Conrad, "Linear Algebraic Groups I," *available at virtualmath1.stanford.edu/∼ conrad/252Page/handouts/alggroups.pdf*, 2020.

[8] B. Poonen, *Rational Points on Varieties*, vol. **186** of *Graduate Studies In Mathematics*. American Mathematical Society, 2017.

[9] B. Conrad, "Semistable reduction for abelian varieties," *available at virtualmath1.stanford.edu/ conrad/mordellsem/Notes/L13.pdf*, 2011.

[10] S. Lang, *Fundamentals of Diophantine Geometry*. Springer-Verlag New York, 1983.

[11] M. Fried and M. Jarden, *Field Arithmetic*, vol. **11** of *A Series of Modern Surveys in Mathematics*. Springer-Verlag Berlin Heidelberg, third ed., revised and enlarged edition, 2008.

[12] J. Neukirch, *Algebraic Number Theory, Translated from the German by Norbert Schappacher* , vol. **322** of *A Series of Comprehensive Studies in Mathematics*. Springer, 1999.

[13] H. Stichtenoth, *Algebraic Function Fields and Codes*, vol. **254** of *Graduate Texts in Mathematics*. Springer-Verlag Berlin Heidelberg, second ed., 2009.

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. **106** of *Graduate Texts in Mathematics*. Springer-Verlag, second ed., 1986.

[15] Wikipedia, "https://en.wikipedia.org/wiki/tate_module," 2022.

[16] J. Milne, "Abelian varieties," *available at jmilne.org/math/CourseNotes/AV.pdf*, 2008.

[17] Mathoverflow, "http://mathoverflow.net/questions/208386/n-th-root-of-unity-in-n-th-division-field-of-abelian-variety?noredirect=1&lq=1," 2015.

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

[19] B. Conrad, "Weil and Grothendieck approaches to adelic points," *L'Enseignement mathématique*, vol. **58**, no. 1/2, p. 61–97, 2012.

[20] D. Eisenbud and J. Harris, *The Geometry of Schemes*, vol. **197** of *Graduate Texts in Mathematics*. Springer New York, NY, second ed., 2000.

[21] E. Kowalski, "Some local-global applications of Kummer theory," *Manuscripta Math.*, vol. **111**, p. 105–139, 2003.

[22] G. Cornell and J. Silverman (edited), *Arithmetic Geometry*. Springer-Verlag New York, 1986.

[23] M. Hindry and J. Silverman, *Diophantine Geometry*, vol. **201** of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2000.

[24] B. Conrad, "Abelian varieties," *available at virtualmath1.stanford.edu/∼conrad/249CS15Page/handouts/abvarnotes.pdf*, 2015.

[25] J. Weinstein, "Faltings' Theorem Seminar Lecture Notes," *available at math.bu.edu/people/jsweinst/Teaching/MA842Spring21/FaltingsLectureNotes.pdf*, 2021.

[26] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, vol. **4** of *New Mathematical Monographs*. Cambridge University Press, 2006.

[27] D. McKinnon and M. Roth, "Seshadri constants, diophantine approximation, and Roth's theorem for arbitrary varieties," *Inventiones mathematicae*, vol. **200**, no. 2, 2015.

[28] A. O. Gel'fond, "Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier," *Matematiceskij sbornik*, vol. **49**, no. 1, pp. 7–25, 1940.

[29] G. Hardy and M. Wright, *An Introduction to the Theory of Numbers, revised by R. Heath-Brown and J. H. Silverman*, vol. **39** of *Oxford Mathematics*. Oxford University Press, sixth ed., 2009.

[30] A. Schinzel, *Selecta*, vol. **I**+**II** of *Heritage of European Mathematics*. American Mathematical Society, 2007.

[31] D. Mikdad, "Integral models of tori," Master's thesis, Mathematisch Instituut, Universiteit Leiden, 2007.

[32] N. Khai, "On some variants of Schinzel's Theorem for Global function fields," *Preprint*, 2022 (submitted).

[33] S. Lang, *Abelian Varieties*, vol. **9** of *Interscience Tracts in Pure and Applied Mathematics*. Interscience Publisher LTD London, 1983.

[34] K. Ribet, "Kummer theory on extensions of abelian varieties by tori," *Duke Math. J*, vol. **46**, no. 4, pp. 745–761, 1979.

[35] D. Bertrand, *Galois representations and transcendental numbers*. in: New Advances in Transcendence Theory (Durham, 1986) (A. Baker, ed.), Cambridge University Press, Cambridge, 1988, pp. 37-55.

[36] M. Larsen, "The support problem for abelian varieties," *Journal of Number Theory*, vol. **101**, no. 2, pp. 398–403, 2003.

[37] M. Larsen, "A Mordell-Weil theorem for abelian varieties over fields generated by torsion points," *Preprint arXiv:math/0503378*, 2005.

[38] S. Lang, *Elliptic Curves: Diophantine Analysis*, vol. **231** of *Grundlehren der mathematischen Wissenschaften*. Springer, 1978.

[39] J.-P. Serre, *Lettre à Ken Ribet du 7/3/1986*. in: volume **IV** 1985–1998 of Oeuvres Collected Papers, Springer-Verlag, Berlin, 2000.

[40] N. Ailon and Z. Rudnick, "Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$," *Acta Arithmetica*, vol. **113**, no. 1, pp. 31–38, 2004.

[41] I. Bandini, A. Longhi and S. Vigni, "Torsion points on elliptic curves over function fields and a theorem of Igusa," *Expositiones Mathematicae*, vol. **27**, no. 3, pp. 175–209, 2009.

[42] B. Poonen, "Local height functions and the Mordell-Weil theorem for Drinfeld modules," *Compositio Mathematica*, vol. **97**, no. 3, pp. 349–368, 1995.