N° d'ordre : 60/2022-C/MT

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumedienne

Faculté des Mathématiques

Thèse de Doctorat
présentée pour l'obtention du grade de Docteur
En: Mathématiques
Spécialité : Mathématiques et Applications

Par : Nabila BELHAMRA

THÈME

SOME RESULTS ON SUPERSINGULAR ELLIPTIC CURVES

Soutenue publiquement, le 11/06/2022 devant le jury composé de

M.	D. BEHLOUL	Professeur	à l'USTHB	Président
M.	M. MIHOUBI	Professeur	à l'USTHB	Directeur de thèse
M.	F. BENCHRIF	Professeur	à l'USTHB	Examinateur
M.	R. BOUCHENNA	Maître de Conférence/A	à l'USTHB	Examinateur
M.	R.BOUMEHDI	Maître de Conférence/A	à l'ESI	Examinateur

ACKNOWLEDGMENTS

First of all, thank God for giving me the courage and patience to go all the way and succeed in my doctorate. Thank you ALLAH for guiding me.

I would like to thank Mr M. MIHOUBI for being my thesis director and for his comments that helped me to improve my thesis redaction.

I would like to thank the jury members M. MIHOUBI, D. BEHLOUL, F. BENCHRIF, R. BOUCHENNA, R.BOUMEHDI for accepting to read my thesis and providing corrections and comments for improving my thesis redaction.

I would like to express a special thank to my dear parents for their patience and understanding the turbulence I have been through while preparing my doctorate. I thank them for having supported me during these years and for having always made life easy to me and my sisters to be able to devote our time to our studies and succeed.

I would like to thank my dear sisters and my dear friend Safia for their moral support and encouragement throughout the preparation of my doctorate.

Abstract

Let K be a perfect field of positive characteristic p. There are a finite number of isomorphism classes of supersingular elliptic curves on $\overline{K}$ and they are all defined on $\mathbb{F}_{p^2}$. The determination of these isomorphism classes constitues an interesting research question since several studies have carried out around it. Special cases $p = 2$ and $p = 3$ have been investigated separately in the literature. However, the general case $p \geq 5$ attracted numerous researchers and solved in different ways. The references of these proofs are mentionned. The original aim of this study is to bring an original explicit proof for the special case $p = 5$. we present an overview of the theorical background, then the necessary tools required for our proof.

Keywords: elliptic curve, supersingular elliptic curve, division polynomials of elliptic curves, group law of elliptic curves

Contents

Chapter 1

Introduction

The commutative ring theory provides the essential tool in the study of algebraic geometry. In algebraic geometry area the rings studied are the rings of polynomials in several variables over a field K since these rings are nœtherians and so theirs ideals are finitely generated, which allow to define the zero set of an idea and then define the notion of algebraic sets which are considered the first basic object constructed in this theory. Prime ideals are also a very important notions in commutative ring theory because they are used to define a central notion on which the algebraic geometry theory is based, that is algebraic varieties which are described by the zero set of a prime ideal. These objects define with their own a theory called the theory of algebraic varieties from which we derivative another vast theory, called the algebraic curves theory that is known by it richness in theory and their interesting applications in different area of algebra. In this work we will not go far in our study, we need only elementary commutative ring theory, but farther studied in this subject require a large background in commutative ring theory. We propose [40] and [42], these books contain all the necessary material to proceed in this theory.

Perfect fields have interesting arithmetic properties which don't hold over non perfect fields. Finite fields and their algebraic closures are perfect fields of positive characteristic, number fields and their algebraic closures are perfect fields of zero characteristic. Among the results needed for our aim in the last chapter we have those that only hold over perfect fields of finite characteristic.

This work is organized as follows:

Chapters two and three present the introductory facts for defining the concepts and stating the results that we will apply in chapter five for our proof. In the second chapter we give a revision from the field extension theory. In section one we give a review on the irreducible polynomials in one variable over a field since the construction of the field extensions of any field require the determination of irreducible polynomials over that field. In section two we define some basics in this theory; degree of an extension, algebraic closure of a field and its construction, simple extensions of a field and their constructions. In section four we state some few properties of perfect fields. Finite fields are an important example of perfect fields, we will state some basic properties of these fields in the last section and their construction and we give also effective examples can be found else where: $\mathbb{F}_4$, $\mathbb{F}_9$, $\mathbb{F}_{25}$.

Chapter three consists on many sections. In section one we give some review on polynomials in several variables; irreducible polynomials, homogeneous polynomials and some properties of them. In section two we make deal with the definitions of the main objects in the algebraic varieties theory. We define the affine and projective spaces over a field K and algebraic sets in these spaces with their ideals in the ring of polynomials over K. We define then the algebraic varieties and we give the characterization of these objects by their ideals. In section two we define a cover by affine spaces of the whole projective space. We define then the affine peaces of a projective algebraic set with their corresponding ideals and we define the set of its points at

infinity. We define also the projective closure of an affine algebraic set with its corresponding ideal. In section three we define the coordinate ring of an algebraic set and the field of rational functions of a variety that is the rational field of its coordinate ring and we describe the elements of these fields in the projective case. In section four we define rational maps between algebraic varieties, we define the regular functions on a variety and then we define regular maps between algebraic varieties, called also morphisms of varieties. There is an important distinction between singular points and nonsingular points on an algebraic variety. Nonsingular varieties are varieties whose all points are nonsingular, these objects are very important to study, in section five we will only give a characterization of these objects using their Jacobian matrix because we will work later by algebraic curves which are nonsingular. In section five we define the dimension of a variety and give the connection between the dimension of a projective variety and the dimension of its affine peace. Finally we come to define algebraic curves in section six and we discuss briefly the genus of a nonsingular projective curve that is an important invariant since it classifies non singular algebraic curves by isomorphism. Nonsingular projective curves of genus one are called elliptic curves. These curves define with their own a beautiful and vast theory combining between number theory and algebraic geometry theory.

In chapter four we recall some basics in the theory of elliptic curves and we state without proofs the results that will be apply for our aim in the last chapter. At first, we state that every elliptic curve has a structure of abelian group. Notice that the structure of this group is induced from the group structure of its Jacobian variety. Then we define isogenies of elliptic curves and particularly the multiplication by an integer N- isogeny. Its kernel is called the N- torsion group, we discuss without proof its structure according to the values of N and the characteristic of the field on which this curve is defined. Every elliptic curve can be described explicitly by a cubic equation

called a Weierstrass equation. There are a lot of results provided by this explicit equation. In section two we discus the Weierstrass equation of an elliptic curve and some results provided from this equation; explicit formulas of the abelian group of an elliptic curve, the $\jmath$-invariant of an elliptic curve defined by its Weierstrass equation, division polynomials of elliptic curves and the explicit expression of the multiplication by an integer N-isogeny of an elliptic curve. The set of esogenies from an elliptic curve to itself defines a ring called the endomorphism ring of this curve. There are much studies done for studying the structure of the endomorphism rings of elliptic curves, in this work we will only give the general structure of these rings and give the connection between the structure of the endomorphism ring and the structure of the p- torsion group of an elliptic curve defined over a perfect field of finite characteristic p. We define the supersingular elliptic curves over these fields and state that there are only finitely many supersingular elliptic curves up to isomorphism and they are all defined over the finite field $\mathbb{F}_{p^2}$. Many mathematicians were interested to determine the number of these classes or farther determine these classes and we have various demonstrations provided for the general case $p \geq 5$. Chapter five is the original part of this work. We will investigate the results reviewed in chapter four to give an explicit proof for the particular case $p = 5$.

Notice that elliptic curves are introduced for resolving different theoretical questions such that Diophantine equations and studying arithmetic progressions defined by squares over number fields. In practices area these curves are also introduced such that elliptic curve cryptography, [15] gives a brief discussion with extensive references in this subject.

Chapter 2

Revision from field extension theory

In this chapter we recall some facts and results in the field extension theory: degree of an extension, algebraic extensions, simple extensions and their constructions, Algebraic closure of a field and their constructions, perfect fields and their characterizations and finally finite fields and their constructions. For general references on fields and their extensions we propose [1, 28, 34, 54].

A field K is a commutative ring in which every nonzero element is a unit and a subfield K of a field F is a subring closed under passage to the inverse.

From the definition, it is obvious that every field is an integral domain.

From the definition, the only ideals in any field are (1) and (0).

Since every field K is an integral domain, it is obvious that the characteristic of K must be either 0 or a prime number. Notice that fields of positive characteristic are also said to be fields of finite characteristic.

If A is a ring and $\mathfrak{m}$ is a maximal ideal in A, then the quotient ring $A\backslash\mathfrak{m}$ is a field.

A ring homomorphism between two fields is called a field homomorphism. Notice that every non zero field homomorphism $f : K \to F$ is injective since its kernel is an ideal of K and can not be equal to (1).

The most known fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and the ring of integers modulo prime integer p that is denoted by $\mathbb{F}_p$.

Let $f : \mathbb{Z} \to K$, $n \mapsto n.1 = 1 + \ldots + 1$ (n times) be a ring homomorphism. $\ker(f)$ is an ideal of $\mathbb{Z}$ generated by an integer m and obviously this integer is the smallest integer in $\ker(f)$, which implies that m must be equal to $char(K)$. Then $im(f) \simeq \frac{\mathbb{Z}}{(char(K))}$. Thus if $char(K) = 0$, then $im(f) \simeq \mathbb{Z}$ and if $char(K)$ is a prime number p, then $im(f) \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$. This implies that K contains a field isomorphic to $\mathbb{Q}$ if $char(K) = 0$ and K contains a field isomorphic to $\frac{\mathbb{Z}}{p\mathbb{Z}}$ if $char(K) = p$.

2.1 Irreducible polynomials in one variable

Let K be a field and $K[X]$ is the ring of polynomials in one variable over K. Then $K[X]$ is an Euclidean domain.

Definition 2.1.1. A polynomial $f(X) \in K[X]$ is said to be irreducible over K if $f(X)$ is nonconstant and the only divisors of $f(X)$ in $K[X]$ are the constant polynomials. Otherwise, $f(X)$ is said to be reducible over K.

Example 2.1.2. The polynomial $X^2 - 3$ is reducible over $\mathbb{R}$ but it is irreducible over $\mathbb{Q}$, and the polynomial $X^2 + 1$ is reducible over $\mathbb{C}$ but it is irreducible over $\mathbb{R}$.

Example 2.1.3. $X^2 + X + 1$ is irreducible over $\mathbb{F}_2$.

Recall that a degree d polynomial $f(X) \in K[X]$ is called monic polynomial if the coefficient of x^d in the expression of $f(X)$ is equal to 1. The following theorem gives an estimation of the number of monic irreducible polynomials over $\mathbb{F}_p$ for a given prime number p. For the proof, see [37] or [50].

Theorem 2.1.4. *Let p be a prime number. Let $N_{d,p}$ denotes the number of the monic irreducible polynomials of degree d over $\mathbb{F}_p$. Then*

$$\frac{p^d}{2d} \leq N_{d,p} \leq \frac{p^d}{d}.$$

For testing if a given polynomial in one variable is irreducible we have the following knows results. For more studies and criterions provided on the irreducibility of polynomials in one variable we refer to [9, 12, 17, 30, 62].

Lemma 2.1.5 (Gauss Lemma)**.** *If A is a unique factorization domain and K is its quotient field. Then a polynomial in $A[X]$ whose the coefficients are relatively prime is irreducible if and only if it is irreducible in $K[X]$.*

Theorem 2.1.6 (Eisenstein 's Criterion)**.** *Let A be a unique factorization domain and K is its fractions field. Let $f(X) = a_nX^n + \ldots + a_1X + a_0$ be a polynomial in $A[X]$. Let p be a prime element in A satisfying the following*
1. p divides a_i for each $i = 0, \ldots, n-1$.
2. p does not divide a_n.
3. p^2 does not divide a_0.
Then $f(X)$ is irreducible in $A[X]$ and so irreducible in $K[X]$.

Example 2.1.7. Let $f(X) = 5X^4 + 15X^3 + 6X^2 + 3$. We apply the above theorem by taking $p = 3$. Then we deduce that $f(X)$ is irreducible over $\mathbb{Q}$.

Theorem 2.1.8. *Let $f(X)$ be a polynomial in $K[X]$ of degree two or three. Then $f(X)$ is irreducible over K if and only if it has no zeros.*

Example 2.1.9. $X^3 + 3X + 2$ is irreducible over $\mathbb{F}_5$.

Remark. An ideal that is generated by one irreducible polynomial over K is a maximal ideal in $K[X]$.

2.2 Algebraic extensions

Since the only ideals of any field K are (0) and (1), then any non zero field homomorphism from K to any other field L is injective.

Let L and K be two fields. If there exists a non zero field homomorphism $\pi : K \hookrightarrow L$, then we identify $\pi(K)$ by K in L and we say that L is an extension of K. We denote by L/K or $K \subset L$ to mean that L is a field extension of K.

Let L/K be an extension and $S = \{\alpha_1, \ldots, \alpha_n\}$ is a subset of L. We denote by $K(\alpha_1, \ldots, \alpha_n)$ the smallest extension of K containing S.

Notice that a field K is called prime field if it has no proper subfield. $\mathbb{F}_p$ and $\mathbb{Q}$ are prime fields. Prime fields of characteristic 0 are isomorphic to $\mathbb{Q}$ and prime fields of finite characteristic p are isomorphic to $\mathbb{F}_p$.

Theorem 2.2.1. *Let L/K be a field extension. Then L has a structure of K-vector space and its dimension as a K-vector space is denoted by $[L : K]$ and called the degree of the extension L/K.*

Example 2.2.2. $\mathbb{C}/\mathbb{R}$ is an extension of degree 2 and $\{1, \imath\}$ is a $\mathbb{R}$-basis of $\mathbb{C}$.

Remark. If $[L : K]$ is a finite integer n, then we say that L/K is a finite extension. It is clear $|L| = |K|^n$ since every K-vector space of dimension n is isomorphic to K^n.

Remark. If K is an extension of $\mathbb{Q}$, then K is called a number field.

number fields containing imaginary numbers are called imaginary number fields and number fields containing only real numbers are called real number fields.

Definition 2.2.3. Let L/K be a field extension. An element α in L is said to be algebraic over K if α is a zero of a non constant polynomial in $K[X]$. The extension L/K is called algebraic extension of K if every element in L is algebraic over K.

Definition 2.2.4. Let L/K be a field extension. Let $\alpha \in L$ be an algebraic element over K. Then the extension $K(\alpha)$ is called simple extension of K. The monic polynomial of the smallest degree in the set of polynomials in $K[X]$ vanishing at α is called the minimal polynomial of α. It is clear that the minimal polynomial of α is irreducible and unique. $K(\alpha)$ is called the root field of this polynomial.

Theorem 2.2.5. *Let K be a field and α is an algebraic element over K. Then the degree of the extension $K(\alpha)/K$ is equal to the degree of the minimal polynomial of α.*

Construction of simple extensions

We summarize the construction of simple extensions as follows: Let L/K be a field extension. Let α/inL be an algebraic element over K and f_α denotes its minimal polynomial in $K[X]$. Since $f_\alpha(X)$ is irreducible, then the ideal generated by $f_\alpha(X)$ is maximal in $K[X]$, so the quotient ring $\frac{K[X]}{(f_\alpha(X))}$ is a field. Let π denotes the projection map

$$\begin{aligned} \pi : K[X] &\rightarrow \frac{K[X]}{(f_\alpha(X))} \\ f_\alpha(X)Q(X) + R(X) &\mapsto \overline{R(X)} = R(\overline{X}) \end{aligned}$$

Let us set $\pi(X) = \alpha$ and define a map

$$\begin{aligned} \phi_\alpha : \frac{K[X]}{(f_\alpha(X))} &\rightarrow K(\alpha) \\ \overline{R(X)} &\mapsto R(\alpha) \end{aligned}$$

ϕ_α is bijective. This implies that $K(\alpha)$ is isomorphic to $\frac{K[X]}{(f_\alpha(X))}$. Therefore, we define $K(\alpha)$ by the set

$$\begin{aligned} K(\alpha) &= \{R(\alpha): \quad \overline{R(X)} \in \frac{K[X]}{(f_\alpha(X))}\} \\ &= \{R(\alpha): \quad R(X) \in K[X] \text{ and } \deg R(X) < \deg f_\alpha(X)\} \end{aligned}$$

Example 2.2.6. For all positive square free integer D, $\sqrt{D}$ is algebraic over $\mathbb{Q}$ and its minimal polynomial in $\mathbb{Q}[X]$ is $X^2 - D$. Then $\mathbb{Q}(\sqrt(D))$ is a simple extension of degree 2 over $\mathbb{Q}$, called a real quadratic field.

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D}: \quad a, b \in \mathbb{Q}\}.$$

Example 2.2.7. For all positive square free integer D, $\imath\sqrt{D}$ is algebraic over $\mathbb{Q}$ and its minimal polynomial in $\mathbb{Q}[X]$ is $X^2 + D$. Then $\mathbb{Q}(\imath\sqrt{D})$ is a simple extension of degree 2 over $\mathbb{Q}$, called imaginary quadratic field.

$$\mathbb{Q}(\imath\sqrt{D}) = \{a + \imath b\sqrt{D}: \quad a, b \in \mathbb{Q}\}.$$

Definition 2.2.8. Let L/K be a field extension. Let f be a non constant polynomial in $K[X]$. We say that f splits completely into linear factors over L if we have

$$f(X) = c(X - \alpha_1)\dots(X - \alpha_n) \qquad c \in K, \quad \alpha_1, \dots, \alpha_n \in L.$$

Definition 2.2.9. Let K be a field. K is said to be algebraically closed if every non constant polynomial in $K[X]$ has a zero (or root) in K. In other words, every nonconstant polynomial in $K[X]$ splits completely into linear factors over K.

Example 2.2.10. $\mathbb{Q}$, $\mathbb{R}$ and the ring of integers modulo prime number are not algebraically closed. $\mathbb{C}$ is algebraically closed.

Definition 2.2.11. Let L/K be a field extension. L is said to be an algebraic closure of K if L/K is an algebraic extension and every non constant polynomial in $K[X]$ has a zero in L. In other words, every nonconstant polynomial in $K[X]$ splits completely into linear factors over L.

Theorem 2.2.12. *[40] [Artin's construction] The algebraic closure of any field K exists and it is unique up to isomorphism, denoted by $\overline{K}$ and constructed as follows: Let Σ denotes the set of all irreducible monic polynomials in $K[X]$ and A denote the polynomial ring over K generated by the indeterminates $\{X_f\}_{f\in\Sigma}$. Let $\mathfrak{a}$ be the ideal generated by the polynomials $\{f(X_f)\}_{f\in\Sigma}$. Let $\mathfrak{m}$ be a maximal ideal in A containing $\mathfrak{a}$. Let $K_1 = \frac{A}{\mathfrak{m}}$. Then K_1 is a field extension of K in which every polynomial $f \in \Sigma$ has a root. We repeat the same construction with K_1 in place of K and then we obtain a field K_2. We repeat the same construction with K_2 and so on.....Let $L = \bigcup_{n=1}^{\infty} K_n$. Then L is a field extension of K over which each polynomial $f \in \Sigma$ splits completely into linear factors. We define $\overline{K}$ to be the set of all elements of L which are algebraic over K. Then $\overline{K}$ is an algebraic closure of K .*

2.3 Perfect fields

Definition 2.3.1. Let K be a field. Let f be a non constant polynomial in $K[X]$. Let $\alpha_1, \ldots, \alpha_s$ be all the zeros of f in $\overline{K}$ (not necessary simple). Then $K(\alpha_1, \ldots, \alpha_s)$ is called the splitting field of $f(X)$. In other words, the splitting field of f is the smallest extension of K over which $f(X)$ splits completely into linear factors.

Definition 2.3.2. Let K be a field. An irreducible polynomial $f(X)$ of degree n in $K[X]$ is said to be separable if it has only simple zeros in its splitting field.

Definition 2.3.3. Let L/K be a field extension. An element $\alpha \in L$ is called separable over K if it is algebraic over K and its minimal polynomial in $K[X]$ is separable. The extension L/K is called a separable extension of K if it is an algebraic extension of K and every element in L is separable.

Definition 2.3.4. A field K is called perfect if every algebraic extension of K is separable.

Remark. Every field K having characteristic 0 is perfect. Indeed, if $f(X)$ is an irreducible polynomial in $K[X]$, then f has no comun zeros with its derivative f', which implies that it has no repeated zero and so it is separable over K.

Let us give an example of a non perfect field of positive characteristic.

Example 2.3.5. Let p be a prime number. Let t be an element in $\mathbb{F}_p$. Then we have the field of rational functions $\mathbb{F}_p(t)$. The polynomial $X^p - t$ is irreducible in $\mathbb{F}_p(t)[X]$. Let F be a field extension of $\mathbb{F}_p(t)$ containing a zero θ of $X^p - t$. Then $\theta^p = t$, which implies that $X^p - \theta^p = 0$. Since $char(F) = p$, then $X^p - \theta^p = (X - \theta)^p$. This implies that θ is not a simple zero of $X^p - t$. Therefore, F is not a separable extension of $\mathbb{F}_p(t)$ and thus $\mathbb{F}_p(t)$ is not perfect.

The following theorem characterizes perfect fields of positive characteristic and it is very helpful to check if a field of positive characteristic is perfect or not.

Theorem 2.3.6. *Let K be a field of characteristic $p > 0$. Then K is perfect if and only if $K^p = K$, where K^p denotes the subfield defined by*

$$K^p = \{\alpha^p : \quad \alpha \in K\}.$$

Example 2.3.7. It is obvious that $\mathbb{F}_p$ is perfect for any prime number p.

Among the most important properties holding only over perfect fields is the following. The application of this theorem will not appear in all the statements of the next chapters but the reader have to make in mind that this property was used to get the basic facts of algebraic varieties theory. For the proof we refer to [28] or [34].

Theorem 2.3.8. *If K is a perfect field, then every finite extension of K is simple.*

2.4 Finite fields

We summarize the basic properties of finite fields in the following theorem

Theorem 2.4.1. *(a) Every finite field is an extension of some prime field $\mathbb{F}_p$ and thus it is a $\mathbb{F}_p$-vector space and its cardinal is a power of p.*

(b) The multiplicative group of every finite field is cyclic.

(c) For every prime number p and positive integer n, there exists a unique finite field up to isomorphism. This field is the root field of the minimal polynomial of the generator of its multiplicative group. It is denoted $\mathbb{F}_{p^n}$.

(d) Let p be a prime number and $n \in \mathbb{N}$. A finite field $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $m|n$.

(e) Let q be a power of prime number. The algebraic closure of the finite field $\mathbb{F}_q$ is given by $E = \bigcup_{k\in\mathbb{N}} \mathbb{F}_{q^k}$.

(f) Every finite field is perfect [1]

Proof. See. [28], [37], [38] and [50] □

Remark. Its obvious that for every prime number p and positive integer n, the finite field $\mathbb{F}_{p^n}$ is the splitting field of the polynomial $X^{p^n} - X$.

[1] There exists a field homomorphism of $\mathbb{F}_{p^n}$ defined by $\phi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^p$. Since ϕ_p is injective and $\mathbb{F}_{p^n}$ is finite, then ϕ_p is surjective, which implies that $\mathbb{F}_{p^n}^p = \mathbb{F}_{p^n}$. Therefore $\mathbb{F}_{p^n}$ is a perfect field.

Notice that there are more extensive studies on the finite fields theory and their applications, see [3, 36, 46, 50]. There are many algorithms for constructing finite fields larger than prime finite fields, see [23, 39, 59].

Remark. Let q be a power of a prime number. A generator of $\mathbb{F}_q^*$ is called a primitive element and its minimal polynomial is called primitive polynomial. There are $\varphi(q-1)$ generators of $\mathbb{F}_q^*$.

Construction of finite fields

We summarize the construction of finite fields larger than finite prime fields as follows: let p be a prime number and $n \in \mathbb{N}$. There are many monic irreducible polynomials in $\mathbb{F}_p[X]$, to construct $\mathbb{F}_{p^n}$ we have to choose the one whose the root $\omega = \pi(X)$ is primitive in $\mathbb{F}_{p^n}^*$. Let $f(X)$ be the good choice. Then

$$\mathbb{F}_{p^n} = \{P(\omega) : \quad P(X) \in \mathbb{F}_p[X] \quad \text{and} \quad \deg P(X) \leq n-1\}.$$

Since ω is a generator of $\mathbb{F}_{p^n}^*$, then every non zero element in $\mathbb{F}_{p^n}$ is of the form ω^s for some $0 \leq s \leq p^n - 2$. This writing is called the logarithmic writing and it is very helpful for doing calculus in finite fields.

Example 2.4.2. Let us give the construction of $\mathbb{F}_4$, $\mathbb{F}_9$, $\mathbb{F}_{25}$.

1. **Construction of $\mathbb{F}_4$:**

   The only irreducible polynomial of degree 2 in $\mathbb{F}_2[X]$ is the following

   $$f(X) = X^2 + X + 1.$$

   We set

   $$\omega = X \mod (f(X)).$$

This implies that we have

$$\omega^2 + \omega + 1 = 0$$

$\mathbb{F}_4$ is defined to be the simple extension $\mathbb{F}_2(\omega)$. The elements of $\mathbb{F}_4$ are the following

$$\begin{aligned} 0 &= 0 \\ \omega^0 &= 1 \\ \omega &= \omega \\ \omega^2 &= \omega + 1 \end{aligned}$$

2. **Construction of $\mathbb{F}_9$:** There are three monic irreducible polynomials of degree 2 over $\mathbb{F}_3$.

$$\begin{aligned} f_1(X) &= X^2 + 1, \\ f_2(X) &= X^2 + X - 1, \\ f_3(X) &= X^2 - X - 1 \end{aligned}$$

The primitive polynomial between them is $f_3(X)$. We set

$$\omega = X \mod (f_3(X)).$$

Then we have

$$\omega^2 - \omega - 1 = 0.$$

Then F_9 is defined to be the simple extension $\mathbb{F}_3(\omega)$. Since ω is a generator of F_9^*, every element in F_9^* can be written as ω^s with $0 \leq s \leq 7$. To find the s corresponding to each element in F_9^* we use the

formula $\omega^2 = \omega + 1$. Then the elements of $\mathbb{F}_9$ are the following

$$\begin{aligned} 0 &= 0 \\ \omega^0 &= 1 \\ \omega &= \omega \\ \omega^2 &= \omega + 1 \\ \omega^3 &= 2\omega + 1 \\ \omega^4 &= 2 \\ \omega^5 &= 2\omega \\ \omega^6 &= 2\omega + 2 \\ \omega^7 &= \omega + 2 \end{aligned}$$

3. **Construction of $\mathbb{F}_{25}$:**

There are many monic irreducible polynomials of degree 2 in $\mathbb{F}_5[X]$.

$$\begin{aligned} f_1(X) &= X^2 + 2, \\ f_2(X) &= X^2 - 2, \\ f_3(X) &= X^2 + X + 2, \\ f_4(X) &= X^2 + 2X - 2, \\ f_5(X) &= X^2 + 2X - 1, \\ f_6(X) &= X^2 + -2X - 1, \\ f_7(X) &= X^2 + -2X - 2. \end{aligned}$$

$f_3(X)$ is a primitive polynomials in $F_5[X]$. We set

$$\omega = X \mod (f_3(X)).$$

Then we have

$$\omega^2 + \omega + 2 = 0.$$

Then F_{25} is defined to be the simple extension $F_5(\omega)$. Since ω is the generator of the multiplicative group $\mathbb{F}_{25}^*$, then every non zero element in $\mathbb{F}_{25}$ is equal to ω^s for some $0 \leq s \leq 23$. To find the s corresponding to every element we use the formula $\omega^2 = -\omega - 2$. Then the elements of $\mathbb{F}_{25}$ are the following

$$
\begin{array}{lcl}
0 & = & 0 \\
\omega^0 & = & 1 \\
\omega & = & \omega \\
\omega^2 & = & -\omega - 2 \\
\omega^3 & = & -\omega + 2 \\
\omega^4 & = & 2\omega + 2 \\
\omega^5 & = & -\omega - 1 \\
\omega^6 & = & 2 \\
\omega^7 & = & 2\omega \\
\omega^8 & = & -2\omega + 1 \\
\omega^9 & = & -2\omega - 1 \\
\omega^{10} & = & \omega - 1 \\
\omega^{11} & = & -2\omega - 2
\end{array}
\qquad
\begin{array}{lcl}
\omega^{12} & = & -1 \\
\omega^{13} & = & -\omega \\
\omega^{14} & = & \omega + 2 \\
\omega^{15} & = & \omega - 2 \\
\omega^{16} & = & 2\omega - 2 \\
\omega^{17} & = & \omega + 1 \\
\omega^{18} & = & -2 \\
\omega^{19} & = & -2\omega \\
\omega^{20} & = & 2\omega - 1 \\
\omega^{21} & = & 2\omega + 1 \\
\omega^{22} & = & -\omega + 1 \\
\omega^{23} & = & 2\omega + 2
\end{array}
$$

Chapter 3

Recall on algebraic varieties

In this chapter we give a review on some basics in the theory of algebraic varieties: affine and projective spaces and algebraic sets in these spaces, algebraic varieties and their dimensions, coordinate rings of algebraic sets and function fields of algebraic varieties, characterization of nonsingular varieties, rational maps, regular functions and regular maps and finally we define algebraic curves without farther discussions. Notice that there are many other basic concepts in this theory but we will not discuss. for more basics in the theory of algebraic varieties we refer to [26, 22, 52, 51].

3.1 Some review on Polynomials

Let $n < \infty$ be a positive integer. From now and on the ring of polynomials in n variables over a field K is denoted by $K[x, y]$ if $n = 2$ and by $K[x, y, z]$ if $n = 3$ and by $K[x, y, z, w]$ if $n = 4$ and by $K[x_1, \ldots, x_n]$ if $n > 4$. And, the notation $K[x_0, \ldots, x_n]$ means the ring of polynomials in $n + 1$ variables.

Notice that the rings of polynomials in n variables over a U.F.D is a U.F.D. This implies that the polynomial rings $K[x_1, \ldots, x_n]$ and $K[x_0, \ldots, x_n]$ are U.F.D.

Definition 3.1.1. A polynomial $f(x_1, \ldots, x_n)$ in $K[x_1, \ldots, x_n]$ is said to be irreducible over K if f is non constant and f can not be factored into product of two non constant polynomials in $K[x_1, \ldots, x_n]$. Otherwise, f is said to be reducible over K.

Notice that there are some criterions for testing the irreducibility of polynomials with two or three variables. We refer to [4, 20, 48, 56].

Example 3.1.2. $x^2 + y^2$ is irreducible over $\mathbb{R}$ but it is reducible over $\mathbb{C}$.

Example 3.1.3. $y^2 - x^3 - x^2$ and $y^2 - x^3$ are irreducible over K.

Remark. A principal ideal in $K[x_1, \ldots, x_n]$ is a prime ideal in $K[x_1, \ldots, x_n]$ if and only if it is generated by an irreducible polynomial over K.

Definition 3.1.4. A homogeneous polynomial in $K[x_0, \ldots, x_n]$ is defined to be a non constant polynomial whose all the monomials have the same degree.

Example 3.1.5. xy and $xy + z^2$ are homogeneous polynomials in $K[x, y, z]$.

Example 3.1.6. $xy + z^2 + w^3$ and $x^2 + y$ are not homogeneous polynomials in $K[x, y, z, w]$.

There are many properties of homogeneous polynomials given in [34] and [22] which are introduced for providing properties of projective sets and varieties should be reviewed by the reader. The construction of the zeros of homogeneous polynomials in the projective space requires the following: a non consonant polynomial $f(x_0, \ldots, x_n)$ in $K[x_0, \ldots, x_n]$ is homogeneous if and only if we have

$$\forall \lambda \in K^*, \quad f(\lambda x_0, \ldots, \lambda x_n) = \lambda^{\deg(f)} f(x_0, \ldots, x_n).$$

Remark. The ring of polynomials in finite number of variables over a nœtherian ring is a nœtherian ring, which implies that $K[x_0, \ldots, x_n]$ is nœtherian. Therefore, every ideal in $K[x_0, \ldots, x_n]$ is finitely generated.

An ideal in $K[x_0, \ldots, x_n]$ may have many sets of generators. Homogeneous ideals are characterized by the following property

Proposition 3.1.7. *An ideal in $K[x_0, \ldots, x_n]$ is an homogeneous ideal if and only if it has homogeneous generators in $K[x_0, \ldots, x_n]$.*

Example 3.1.8. $(xz^2 + y^3, y, z^2)$ is an homogeneous ideal in $K[x, y, z]$.

Notice that it is not necessary that every set of generators of an homogeneous ideal must be defined by only homogeneous polynomials. The above proposition requires to find only one set of generators that contains only homogeneous polynomials.

Definition 3.1.9 (homogenization and de-homogenization maps)**.** For all integer $1 \leq i \leq n$, we define the homogenization map from $K[x_1, \ldots, x_n]$ to $K[x_0, \ldots, x_n]$ to be the map corresponding to any non constant polynomial $f(x_0, \ldots, x_n)$ the homogeneous polynomial

$$f^*(x_1, \ldots, x_n) = x_i^{\deg(f)} f(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}).$$

For each $i = 0, \ldots, x_n$, we define the de-homogenization map from $K[x_0, \ldots, x_n]$ to $K[x_0, \ldots, x_n]$ to be the map corresponding to any non constant homogeneous polynomial $f(x_1, \ldots, x_n)$ the polynomial

$$f_*(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = f(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

3.2 Definitions

In this section we make deal with definitions and notations of the principal objects in the theory of algebraic varieties.

Let K be a field and $\overline{K}$ is a fixed algebraic closure of K. Let n be a positive integer. The affine n-space (over K) is the set

$$\mathbb{A}^n_{\overline{K}} = \{P = (x_1, \ldots, x_n) : \quad x_i \in \overline{K}\}.$$

$x_1, \ldots, x_n$ are called the affine coordinates of the point $(x_1, \ldots, x_n)$.

Notice that the affine 2-space $\mathbb{A}^2_{\overline{K}}$ is called the affine plane over K.

We define an equivalence relation on $\mathbb{A}^{n+1}_{\overline{K}} \backslash (0, \ldots, 0)$ as follows:

$$(x_0, \ldots, x_{n+1}) \sim (y_0, \ldots, y_{n+1}) \Leftrightarrow \exists \lambda \in \overline{K} \text{ such that } x_i = \lambda y_i.$$

The projective n-space (over K), denoted by $\mathbb{P}^n_{\overline{K}}$, is defined to be the quotient set

$$\frac{\mathbb{A}^{n+1}_{\overline{K}} \backslash\ (0, \ldots, 0)}{\sim}.$$

The equivalence class of $(x_0, \ldots, x_n)$ is defined by

$$\overline{(x_0, \ldots, x_n)} = \{(\lambda x_0, \ldots, \lambda x_n) : \quad \lambda \in \overline{K}\}.$$

This class is denoted by $[x_0, \ldots, x_n]$ and called a projective point in $\mathbb{P}^n_{\overline{K}}$. $x_0, \ldots, x_n$ are called the projective (or homogeneous) coordinates of $[x_0, \ldots, x_n]$.

Notice that the projective 2-space $\mathbb{P}^2_{\overline{K}}$ is called the projective plane over K.

Let I be an ideal in $\overline{K}[x_1, \ldots, x_n]$ generated by polynomials $f_1, \ldots, f_m$. Then we define the zero set of I in $\mathbb{A}^n_{\overline{K}}$, denoted by $Z(I)$, to be the set of all the points $P \in \mathbb{A}^n_{\overline{K}}$ satisfying

$$f_1(P) = \cdots = f_m(P) = 0.$$

A subset W in $\mathbb{A}^n_{\overline{K}}$ is called affine algebraic set if it is equal to the zero set of an ideal $I \subseteq K[x_1, \ldots, x_n]$. The ideal I is called the ideal of W and denoted by $I(W)$. If $I(W)$ is generated by polynomials which are defined over K, then we say that W is an affine algebraic set defined over K. We denote by W/K to mean that W is defined over K.

Let f be a non constant homogeneous polynomial in $\overline{K}[x_0, \ldots, x_n]$. For all $(x_0, \ldots, x_n)$ in $\mathbb{A}^{n+1} \backslash (0, \ldots, 0)$, we have

$$f(x_0, \ldots, x_n) = 0 \Leftrightarrow \quad \text{for all} \quad \lambda \in \overline{K}^*, \quad f(\lambda x_0, \ldots, \lambda x_n) = 0.$$

This implies that every element in the equivalence class $[x_0, \ldots, x_n]$ is a zero of f. Therefore we define the zero of f in $\mathbb{P}^n_{\overline{K}}$ as follows

$$[x_0, \ldots, x_n] \ \text{ is a zero of } f \text{ if and only if } \ f(x_0, \ldots, x_n) = 0.$$

Let I be an homogeneous ideal in $\overline{K}[x_0, \ldots, x_n]$ generated by homogeneous polynomials $f_1, \ldots, f_m$. Then we define the zero set of I in $\mathbb{P}^n_{\overline{K}}$, denoted by $Z(I)$, to be the set of all the projective points P in $\mathbb{P}^n_{\overline{K}}$ satisfying

$$f_1(P) = \cdots = f_m(P) = 0.$$

A subset W in $\mathbb{P}^n_{\overline{K}}$ is called projective algebraic set in $\mathbb{P}^n_{\overline{K}}$ if it is equal to the zero set of an homogeneous ideal I in $K[x_0, \ldots, x_n]$. I is called the ideal of W and denoted by $I(W)$. If the generators of $I(W)$ are defined over K, then we say that W is an algebraic set defined over K. We denote by W/K to mean that W is defined over K.

An affine algebraic set V/K is called affine variety if V can not be expressed as union of two proper algebraic subsets of V. Similarly, we define a projective algebraic set.

Affine varieties are characterized as follows

Theorem 3.2.1. *An affine algebraic set V/K is an affine variety if and only if its ideal is a prime ideal in $\overline{K}[x_1, \ldots, x_n]$.*

Projective varieties are characterized as follows

Theorem 3.2.2. *A projective algebraic set V/K is a projective variety if and only if its ideal is a prime homogeneous ideal in $\overline{K}[x_0, \ldots, x_n]$.*

Example 3.2.3. $Z(x^2 + y^2)$ is defined over $\mathbb{R}$. This projective set is not a projective variety since $(x^2 + y^2)$ is not irreducible in $\mathbb{C}[x, y]$.

Example 3.2.4. $Z(y - x^2)$ and $Z(x - y^2)$ are affine varieties in $\mathbb{A}^2_{\overline{K}}$.

Notice that by an algebraic variety we mean an affine variety or a projective variety, and by an algebraic set we mean an affine algebraic set or a projective algebraic set.

A subvariety of an algebraic variety V is a subset of V that is also an algebraic variety over K.

3.3 Affine peaces, Projective closure, Points at infinity

The projective n-space $\mathbb{P}^n_{\overline{K}}$ has a covering by affine n-spaces. Indeed, we set

$$H_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n_{\overline{K}} : \quad x_i = 0\} \quad \text{for all i=0, \ldots,n.}$$

H_i is a projective algebraic set in $\mathbb{P}^n_{\overline{K}}$ since its the zero set of the ideal (x_i). We set

$$U_i = \mathbb{P}^n_{\overline{K}} \backslash H_i \quad \text{for all } i = 0, \ldots, n.$$

Every point $P = [x_0, \ldots, x_0] \in \mathbb{P}^n_{\overline{K}}$ has at least one coordinate $x_i \neq 0$, then P is in some U_i. Therefore, $\mathbb{P}^n_{\overline{K}}$ is covered by $\{U_i\}_{0 \leq i \leq n}$.

For all $i = 0, \ldots, n$, we define a bijection [1]

$$\begin{aligned} \phi_i \quad : \quad & U_i \to \mathbb{A}^n \\ & [x_0, \ldots, x_n] \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}) \end{aligned}$$

Its inverse map is ϕ_i^{-1} defined as follows

$$\begin{aligned} \phi_i^{-1} \quad : \quad & \mathbb{A}^n \to U_i \\ & (y_1, \ldots, y_n) \mapsto [y_1, \ldots, y_i, 1, y_{i+1}, \ldots, y_n] \end{aligned}$$

We identify each U_i by $\mathbb{A}^n_{\overline{K}}$ and thus we have an affine cover of $\mathbb{P}^n_{\overline{K}}$.

Definition 3.3.1. If W/K is a projective algebraic set, then W is covered by $\{W \cap U_i\}_{0 \leq i \leq n}$. If $W \cap U_i \neq \emptyset$, then $W_i = \phi_i(W \cap U_i)$ is called an affine peace of W with respect to i and its points are called the affine points of W. Notice that all the W_is are isomorphic since each U_i is isomorphic to $\mathbb{A}^n_{\overline{K}}$. W_i is defined by the zero set of the following ideal

$$I(W_i) = \{(f_*(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) : f(x_0, \ldots, x_n) \in I(W)\}.$$

The set $W \backslash W_i = W \cap H_i$ is called the set of points at infinity on W and defined by the points $[x_0, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n]$ satisfying

$$f(x_0, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = 0 \quad \text{for every generator } f \text{ of } I(W).$$

Example 3.3.2. Let $W = Z(y^2 - x^2 - z^2)$ be a projective algebraic set over K. An affine peace of W is $W_0 = Z(y^2 - 1 - z^2)$. The points at infinity of W are

$$\{[0, y, z] \in \mathbb{P}^2_{\overline{K}} : \quad y^2 - z^2 = 0\} = \{[0, 1, 1], [0, 1 - 1]\}.$$

[1] ϕ_i is well defined since the ratio $\frac{x_j}{x_i}$ are independent of the choice of the homogeneous coordinates.

Example 3.3.3. $W = Z(y^2 + z^2 - x^2)$ is a projective set over $\mathbb{C}$. Its affine peace is a circle $W_0 = Z(y^2 + z^2 - 1)$. The points at infinity of W are

$$\{[0, y, z] \in \mathbb{P}^2_{\overline{K}} : \quad y^2 + z^2 = 0\} = \{[0, \imath, 1], [0, -\imath, 1]\}.$$

Definition 3.3.4. If W/K is an affine algebraic set, then the projective closure of W in $\mathbb{P}^n_{\overline{K}}$ is denoted by $\overline{W}$ and defined to be the projective set whose the homogeneous ideal in $K[x_0, \ldots, x_n]$ is generated by

$$\{f^*(x_0, \ldots, x_n) : \quad f(x_1, \ldots, x_n) \in I(W)\}.$$

Example 3.3.5. The projective closure of the affine algebraic set $Z(xy - 1)$ is the projective algebraic set $Z(xy - z^2)$.

Example 3.3.6. the projective closure of the affine algebraic set $Z(y^2 - z^3 - x - 1)$ is the projective algebraic set $Z(wy^2 - z^3 - xw^2 - w^3)$.

3.4 Function field

Let W/K be an affine algebraic set. We define the affine coordinate ring of W, denoted by $\overline{K}[W]$, to be the quotient ring

$$\frac{\overline{K}[x_1, \ldots, x_n]}{I(W)}.$$

If V/K is an affine variety, then the affine coordinate ring of V is an integral domain since its ideal is prime in $\overline{K}[x_1, \ldots, x_n]$. Therefore, we can construct its fraction field. For the construction of fraction fields of integral domains we refer to [35] or [40].

Definition 3.4.1. Let V/K be an affine variety. The filed of fractions of the affine coordinate ring of V is called the field of rational functions on V or the function field of V. It is denoted by $\overline{K}(V)$.

Example 3.4.2. $V = Z(y - x^2)$ is an affine variety over K. The affine coordinate ring of V is $\frac{\overline{K}[x,y]}{(y-x^2)}$. This integral domain is isomorphic to $\overline{K}[x]$ via the ring isomorphism $y \mapsto x^2$. This implies that the function field of V is isomorphic to $\overline{K}(x)$.

Example 3.4.3. It is obvious that the function field of the hole affine space $\mathbb{A}^n_{\overline{K}}$ is $\overline{K}(x_1, \ldots, x_n)$ since its ideal is (0).

Let W/K be a projective algebraic set. We define the homogeneous coordinate ring of W, denoted by $\overline{K}[W]$, to be the quotient ring

$$\frac{\overline{K}[x_0, \ldots, x_n]}{I(W)}.$$

If V/K is a projective variety, then for the same argument us in the case of an affine variety we can define the function field of a projective variety.

Definition 3.4.4. Let V/K be a projective variety. The field of fractions of the homogeneous coordinate ring of V is denoted by $\overline{K}(V)$ and called the function field of V or the field of rational functions on V.

In the following proposition we describe the elements of the function field of a projective variety. For the proof, see [26].

Theorem 3.4.5. *Let V be a projective variety in $\mathbb{P}^n_{\overline{K}}$. Then $\overline{K}(V)$ is isomorphic to the set of rational functions $f = \frac{h}{g}$ such that h, g are homogeneous polynomials of the same degree in $\overline{K}[x_0, \ldots, x_n]$ and $g \notin I(V)$.*

We have also the following theorem

Theorem 3.4.6. *[52] Let V be an affine variety in $\mathbb{A}^n_{\overline{K}}$. Then $\overline{K}(\overline{V})$ is isomorphic to $\overline{K}(V)$.*

Example 3.4.7. the function field of the hole projective space $\mathbb{P}^2_{\overline{K}}$ is isomorphic to $\overline{K}[x, y]$.

3.5 Rational maps and morphisms

In this section we define the regular functions on an algebraic variety and then we define morphisms of varieties. The properties of these maps are studied in details in [26, 51, 52].

Definition 3.5.1. Let V/K be an affine variety. A function $f : V \to \overline{K}$ is said to be regular or defined at a point $P \in V$ if there are polynomials $h, g \in \overline{K}[x_1, \ldots, x_n]$ such that $f(p) = \frac{h(p)}{g(p)}$ and $g(P) \neq 0$. f is said to be regular on V if f is regular at every point on V.

Let $V_1 \subseteq \mathbb{A}^n_{\overline{K}}$ and $V_2 \subseteq \mathbb{A}^m_{\overline{K}}$ be two affine varieties. A rational map ϕ from V_1 to V_2 is a map defined by $(f_1, \ldots, f_m)$ such that $f_1, \ldots, f_m$ are rational functions on V_1 and $im(\phi) \subseteq V_2$.

$$im(\phi) = \{(f_1(P), \ldots, f_m(P)) : \quad P \in V_1 \text{ and } f_1, \ldots, f_m \text{ are defined at } P \}.$$

Definition 3.5.2. Let $V_1 \subseteq \mathbb{A}^n_{\overline{K}}$ and $V_2 \subseteq \mathbb{A}^m_{\overline{K}}$ be two affine varieties. Let $\varphi = (f_1, \ldots, f_m)$ be a rational map from V_1 to V_2. Let P be a point on V_1. We say that φ is regular or defined at P if $f_1, \ldots, f_m$ are all defined at P. We say that φ is a regular map or a morphism of affine varities if it is regular at every point $P \in V$.

Example 3.5.3. Let $V = Z(y^2 - x^3)$. The rational map $\phi : V \to \mathbb{A}^1_{\overline{K}}$ defined by $(x, y) \mapsto \frac{y}{x}$ is not a regular map at $(0, 0)$.

Example 3.5.4. Let $V = Z(y - x^3)$. The rational map $\phi : \mathbb{A}^1_{\overline{K}} \to V$ defined by $x \mapsto (x, x^3)$ is a morphism since it is regular at every point in $\mathbb{A}^1_{\overline{K}}$.

Definition 3.5.5. Let V/K be a projective variety. A function $f : V \to \overline{K}$ is said to be regular or defined at $P \in V$ if there are two homogeneous polynomials g, h in $\overline{K}[x_0, \ldots, x_n]$ of the same degree such that $f(P) = \frac{h(P)}{g(P)}$ and $g(P) \neq 0$. We say that f is regular on V if it is regular at every point $P \in V$.

Let V_1/K and V_2/K be two projective varieties with $V_2 \subseteq \mathbb{P}^m_K$. A rational map $\varphi : V_1 \to V_2$ is a map defined by $[f_0, \ldots, f_m]$ such that $f_0, \ldots, f_m$ are rational functions on V_1 and $im\varphi \subseteq V_2$.

$im\varphi = \{[f_0(P), \ldots, f_m(P)] : P \in V_1,\ f_0, \ldots, f_m$ are defined at P and not all zeros at $P\}$.

Definition 3.5.6. Let V_1 and V_2 be two projective varieties such that $V_2 \subseteq \mathbb{P}^m_K$. Let $\phi : V_1 \to V_2$ be a rational map given by $[f_0, \ldots, f_m]$. Let P be a point on V_1. We say that φ is regular (or defined) at P if we are in one of the following two cases:

Case 1: all the functions f_i are regular at P and are not all zeros at P.

Case 2: all the $f_i s$ vanish at P or there exists some i for which f_i is not defined at P, but we can find a function g on V_1 such that gf_i is defined at P for all $i = 0, \ldots, m$ and there exists some $0 \leq i_0 \leq m$ such that $gf_{i_0}(P) \neq 0$. In this case we set $G_i = gf_i$ for all $i = 0, \ldots, m$ and we write $\varphi(P) = [G_0(P), \ldots, G_m(P)]$.

We say that φ is a regular map or a morphism of projective varieties if φ is regular at every point $P \in V_1$.

Example 3.5.7. Let $V = Z(xy - z^2)$. Let $\phi : V \to \mathbb{P}^1_K$ be a rational map defined by $[1, \frac{z}{x}]$. Then ϕ is defined by the rational functions on V, $f_0(x, y, z) = 1$, that is defined every where at V and $f_1(x, y, z) = \frac{z}{x}$, that is not defined at $[0, 1, 0]$. We have every point $[x, y, z]$ on V satisfies $xy = z^2$ and so $\frac{z}{y} = \frac{x}{z}$. We define on V the function $g = \frac{x}{z}$. Then g makes ϕ defined at $[0, 1, 0]$ and $\phi([0, 1, 0]) = [0, 1]$. Since ϕ is defined at every point on V_1, then ϕ is a morphism of varieties.

Example 3.5.8. Let $V = Z(y^2z - x^3 - x^2z)$. Let $\phi : V \to \mathbb{P}^1_K$ defined by $[x, y]$. Then ϕ is not a morphism since it is not regular at the point $[0, 0, 1]$.

Definition 3.5.9. Two algebraic varieties V_1/K and V_2/K are said to be isomorphic over $\overline{K}$ or $\overline{K}$-isomorphic if there exists two morphisms of varieties $\varphi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\varphi \circ \psi = id_{V_2}$ and $\psi \circ \varphi = id_{V_1}$. In this case, we write $V_1 \simeq V_2$.

Example 3.5.10. Let $V = Z(y^2 - x^3)$. The rational map $\phi : \mathbb{A}^1 \to V$ defined by $x \mapsto (x^2, x^3)$ is a morphism. The inverse map of ψ is the rational map $\phi : V \to \mathbb{A}^1_{\overline{K}}$ defined by $(x, y) \mapsto \frac{y}{x}$. Since ϕ is not a morphism, then ψ is not an isomorphism of varieties.

Example 3.5.11. Let $V = Z(y^2 - x^3)$. Let $\psi : V \to \mathbb{A}^1_{\overline{K}}$ be a rational map defined by $(x, y) \mapsto x$. Then ψ is a morphism. The inverse map of ψ is the rational map $\phi : \mathbb{A}^1_{\overline{K}} \to V$ defied by $x \mapsto (x^2, x^3)$. Since ψ is a morphism and its inverse map is also a morphism, then ψ is an isomorphism of varieties.

Example 3.5.12. Let $V = Z(xy - z^2)$. Let $\psi : \mathbb{P}^1_{\overline{K}} \to V$ defined by $[\frac{x}{y}, \frac{y}{x}, 1]$. Then ψ is a morphism. The inverse map of ψ is the rational map $\phi : V \to \mathbb{P}^1_{\overline{K}}$ defined by $[x, y, z] \mapsto [1, \frac{z}{x}]$. Then ψ is an isomorphism of projective varieties since its inverse map is also a morphism.

3.6 Dimension

One of the important notions in the theory of algebraic varieties theory is the dimension of an algebraic variety.

Definition 3.6.1. [51] The dimension of an algebraic variety V, denoted by $\dim V$, is the maximal integer r for which there exists a strictly decreasing chain of length r of distinct sub-varieties $V_i \subseteq V$.

$$V_0 \supset V_1 \supset \ldots \supset V_r \supseteq \emptyset.$$

Notice that there is another equivalent definition of the dimension of an algebraic variety using the transcendence degree of its function field and it is practice for providing proofs of a lot of results in this theory. We refer to any reference cited in this chapter.

We have the following proposition [26].

Proposition 3.6.2. *A variety V in $\mathbb{A}^n_{\overline{K}}$ has dimension $n-1$ if and only if it is the zero set of an ideal generated by one irreducible polynomial in $\overline{K}[x_1, \ldots, x_n]$.*

In the following theorem we relate the dimension of a projective variety with the dimension of its affine peace. For the proof, see [52] or [26].

Theorem 3.6.3. *Let V/K be a projective variety and V_i is an affine peace of V. Then we have $dimV = dimV_i$.*

3.7 Nonsingularity

The following theorem gives a characterization of nonsingular algebraic varieties.

Theorem 3.7.1. *Let $V \subseteq \mathbb{P}^n_{\overline{K}}$ be a projective variety. Let $f_1, \ldots, f_m$ be the generators of its ideal $I(V)$. We say that V is nonsingular (or smooth) at a point $P \in V$ if its Jacobian matrix at P*

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{1 \leq i \leq m, 0 \leq j \leq n}$$

has rank equal to $n - dimV$. We say that V is a nonsingular variety if it is nonsingular at every point $P \in V$. Similarly, we characterize a nonsingular affine variety.

The particular case of a nonsingular variety given by one irreducible polynomial is given as follows.

Proposition 3.7.2. *An affine variety V that is defined over K by only one irreducible polynomial $f(x_1, \ldots, x_n)$ is nonsingular at a point $P \in V$ if and only if the partials $\frac{\partial f}{\partial x_i}$ vanish at P. It is the same in the case of a projective variety defined by one irreducible polynomial.*

Example 3.7.3. The affine variety $Z(x^3 + y^3 - 3xy)$ is singular at $(0, 0)$.

Example 3.7.4. The projective variety $Z = (x^3z + x^2yz + y^3z + x^4 + y^4)$ is singular at $[0, 0, 1]$.

3.8 Algebraic curves

In this section we define algebraic curves and we discuss briefly the genus of nonsingular projective curves. General references on the algebraic curves theory and morphisms between them are [22, 24, 26, 32, 44, 51, 52].

Definition 3.8.1. An algebraic curve C/K is defined to be an algebraic variety of dimension one.

Example 3.8.2. $Z(x^2 - xz - yw, yz - xw - zw)$ is a projective curve in $\mathbb{P}^3_{\overline{K}}$ called the elliptic quartic curve in $\mathbb{P}^3_{\overline{K}}$. See [22].

Notice that if C is defined by the zero set of one irreducible polynomial in $K[x, y]$, then C is called an affine plane curve. If C is defined by the zero set of one homogeneous irreducible polynomial in $K[x, y, z]$, then C is called a projective plane curve. We write $\mathcal{C} : f(x, y, z) = 0$ to mean that $\mathcal{C}$ is described by the zero set of the polynomial $f(x, y, z)$. Similarly, in the affine case.

The following result about rational maps between nonsingular projective curves will not be used in our proofs but we state this result because it has a central role in providing a lot of results in the theory of nonsingular algebraic curves and maps between them and in particular the elliptic curves theory. For the proof, see [26] and [52].

Theorem 3.8.3. *Every non constant rational map ϕ from a nonsingular projective curve C_1 to any projective curve C_2 is a morphism. Further, if C_2 is also nonsingular then ϕ is surjective.*

Let C/K be a projective curve and $P \in C$. Let $\mathcal{O}_{P,\overline{K}}(C)$ denotes the subset of $\overline{K}(C)$ defined by all the rational functions $f \in \overline{K}(C)$ such that f is regular at P. Then the local ring of C at P is defined to be $\mathcal{O}_{P,\overline{K}}(C)$ and its maximal ideal is denoted by $\mathfrak{m}_{P,\overline{K}}(C)$ and defined by the rational functions $f \in \mathcal{O}_{P,\overline{K}}(C)$ such that $f(P) = 0$ [15]. Notice that for the construction of local rings and further discussions about their structures and properties we refer to [40].

Theorem 3.8.4. *[15] Let C/K be a nonsingular projective curve and $P \in C$. Then $\mathfrak{m}_{P,\overline{K}}(C)$ is a principal ideal of $\mathcal{O}_{P,\overline{K}}(C)$.*

Notice that more properties about $\mathcal{O}_{P,\overline{K}}(C)$ and $\mathfrak{m}_{P,\overline{K}}(C)$ of any nonsingular projective curve should be reviewed [15, 52].

Let C/K be a nonsingular projective curve and $P \in C$. Let t_P be a generator of $\mathfrak{m}_{P,\overline{K}}(C)$. Let $h \in \mathcal{O}_{P,\overline{K}}(C)$.The order of h at P is defined to be

$$ord_P(h) = \max\{d \in \mathbb{Z}_{\geq 0} : h \in (t_P^d)\}.$$

We define the order of a rational function on V, $f = \frac{h}{g}$, at a point $P \in V$ to be $ord_P(f) = ord_P(g) - ord_P(h)$. If $ord_P(f) < 0$, then we say that f has a pole at P and if $ord_P f > 0$, then we say that f has a zero at P. We have

any non constant rational function on C has a finitely many poles and zeros [15].

Let C/K be a nonsingular projective curve. A finite sum of the form

$$D = n_{_{P_1}}(P_1)+, \ldots, n_{P_r}(P_r), \quad n_{P_1}, \ldots, n_{P_r} \in \mathbb{Z}, \quad P_1, \ldots, P_r \in C$$

is called a divisor on C. The sum $n_{P_1} + \ldots + n_{P_r}$ is called the degree of D and denoted by $\deg(D)$. The following set

$$\mathcal{L}_{\overline{K}}(D) = \{f \in \overline{K}(C)^* : \quad ord_{P_i}(f) \geq n_{P_i} \text{ for all } i = 1, \ldots, r\} \cup \{0\}$$

has a structure of finite dimensional $\overline{K}$-vector space and it is called the Riemann Roch space of D [26]. There exists a minimal integer g such that for all divisor D on C we have $\ell_{\overline{K}}(D) \geq \deg(D)+1-g$, where $\ell_{\overline{K}}(D)$ denotes the dimension of $\mathcal{L}_{\overline{K}}(D)$ over $\overline{K}$ [22, 44].

We define the genus of a nonsingular projective curve as follows [15, 22].

Definition 3.8.5. Let C/K be a nonsingular projective curve. The genus of C is denoted by g_C and defined to be the minimal integer for which we have $\ell_{\overline{K}}(D) \geq \deg(D) + 1 - g_C$ for all divisor D on C.

Notice that there are many other equivalent definitions of the genus of a nonsingular projective curve, see [26, 51, 52].

Definition 3.8.6. An elliptic curve is defined to be a nonsingular projective curve of genus one.

Notice that there are many other equivalent definitions of elliptic curves which flow from the properties provided from their definition given above.

Chapter 4

Elliptic curves

In this chapter we give a review on some basic facts in the elliptic curves theory and state the requirement results for our aim of the next chapter. All the basic concepts and results provided in this theory can be found in [13, 52, 60].

The following theorem states that the set of points of any elliptic curve defines an abelian group. For the proof, see [15] or [52].

Theorem 4.0.1. *Let E/K be an elliptic curve. Let $\mathcal{O}_E$ be a fixed point on E. Then the set of points of E defines a structure of additive group whose the identity element is $\mathcal{O}_E$.*

Notice that the point chosen to be the identity element of the additive group law defined by the set of points of E is called the base point of E or the identity point of E.

A morphism of elliptic curves $\phi : E_1 \to E_2$ is defined to be a morphism of algebraic varieties since every elliptic curve is by definition an algebraic variety.

A group homomorphism of elliptic curves $\phi : E_1 \to E_2$ is a morphism of elliptic curves satisfying the properties of a group homomorphism:

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \quad \text{for all} \quad P_1, P_2 \in E_1 \quad \text{and} \quad \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}.$$

Group homomorphisms of elliptic curves are called isogenies of elliptic curves. They are called isogenies because they are morphisms of varieties and morphisms of groups at the same time.

Theorem 4.0.2. *[15] Let E_1/K and E_2/K be two elliptic curves. Let $\phi : E_1 \to E_2$ be a morphism of elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. Then ϕ is a group homomorphism.*

The above theorem makes sens to the following definition

Definition 4.0.3 (Isogeny of elliptic curves)**.** An isogeny of elliptic curves $\phi : E_1 \to E_2$ is a morphism of elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$.

If E_1/K and E_2/K are elliptic curves, then every rational map $\phi : E_1 \to E_2$ is a morphism of elliptic curves since every elliptic curve is by definition a nonsingular projective curve.

Two elliptic curves are said to be isomorphic if they are isomorphic as algebraic varieties and isomorphic as additive groups, so the following definition make sens

Definition 4.0.4 (Isomorphic elliptic curves)**.** Let E_1/K and E_2/K be two elliptic curves. E_1 and E_2 are said to be isomorphic over $\overline{K}$ or $\overline{K}$-isomorphic if there exists an isogeny $\varphi : E_1 \to E_2$ and an isogeny $\psi : E_2 \to E_1$ such that $\psi \circ \varphi = id_{E_1}$ and $\varphi \circ \psi = id_{E_2}$.

4.1 Points of finite order

Definition 4.1.1 (The multiplication by N-isogeny)**.** Let E/K be an elliptic curve and $\mathcal{O}_E$ is its identity point. The multiplication by N-isogeny of E is denoted by $[N]$ and defined to be the rational map $[N] : E \to E$ sending a point $P \in E$ to the point $[N]P$ defined as follows: $[0]P = \mathcal{O}_E$ and

$$[N]P = \overbrace{P + \ldots + P}^{N \text{ times}} \text{ if } N > 0, \quad [N]P = -[-N]P \text{ if } N < 0.$$

Since the multiplication by N-isogeny is a group homomorphism the following definition make sens

Definition 4.1.2. Let E/K be an elliptic curve and $N \in \mathbb{N}$. Let $[N]$ be the multiplication by N-isogeny of E. Then the kernel of $[N]$ is denoted by $E[N]$ or $E[N]_{\overline{K}}$ and called the N-torsion group of E or the group of points of order N on E. A point in $E[N]$ is called a N-torsion point on E.

$$E[N] = \{P \in E : \quad [N]P = \mathcal{O}_E\}.$$

Notice that $E[N](K)$ denotes the subgroup of $E[N]$ defined by only the points in $E[N]$ whose the coordinates are in K.

The most important fact about the multiplication by N-isogeny of an elliptic curve is the structure of its kernel from which a lot of powerful results are provided. The following theorem describes the structure of $E[N]$. for the proof, see [52]

Theorem 4.1.3. *Let E/K be an elliptic curve such that K is a perfect field of characteristic p. Then*

(a) $\forall N \in \mathbb{Z}_{\geq 2}$ such that $N \neq p$, we have $E[N] \simeq \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}$.

(b) If $p > 0$, then $E[p^r] = \mathcal{O}_E \ \ \forall r \in \mathbb{Z}_{\geq 0}$ or $E[p^r] \simeq \frac{\mathbb{Z}}{p^r\mathbb{Z}} \ \ \forall r \in \mathbb{Z}_{\geq 0}$.

4.1.1 Explicit equation

Let $F(x, y, z)$ be an irreducible homogeneous polynomial in $K[x, y, z]$ defined as follows

$$F(x, y, z) = y^2z + a_1xyz + a_3y^2z - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

The zero set of the polynomial $F(x, y, z)$ defines a projective plane curve in $\mathbb{P}^2_K$ called the projective Weierstrass curve. This curve has only one point at infinity, that is $[0, 1, 0]$ and its affine curve is called the affine curve of Weierstrass and defined by $Z\left(f(x, y)\right)$ such that

$$f(x, y) = F_*(x, y) = y^2 + a_1xy + a_3y^2 - x^3 - a_2x^2 - a_4x - a_6. \tag{4.1}$$

The equations $f(x, y) = 0$ and $F(x, y, z) = 0$ are called Weierstrass equations. The polynomials $f(x, y)$ and $F(x, y, z)$ are called Weierstrass polynomials.

Since we have $\frac{\partial F}{\partial x}(0, 1, 0) = 1 \neq 0$, then every Weierstrass curve is nonsingular at its point at infinity $[0, 1, 0]$. This implies that any projective Weierstrass curve is nonsingular if and only if its affine curve is nonsingular.

Example 4.1.4. $\mathcal{C} : y^2 - x^3 - x = 0$ is nonsingular, which implies that its projective curve $\overline{\mathcal{C}} : y^2z - x^3 - xz^2 = 0$ is nonsingular.

Example 4.1.5. $\mathcal{C} : y^2 - x^3 - x^2 = 0$ is singular at $(0, 0)$, which implies that its projective curve $\overline{C} : y^2z - x^3 - x^2z = 0$ is singular at $[0, 0, 1]$.

The following quantities are defined in [52] for simplifying notations.

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6.$$

$$b_8 = \frac{1}{4}(b_2b_6 - b_4^2), \qquad c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Definition 4.1.6. The discriminant of the Weierstrass curve $\mathcal{C}$ given by the equation (4.1) is denoted by $\Delta_{\mathcal{C}}$ and defined to be the quantity

$$\Delta_{\mathcal{C}} = \frac{C_4^3 - C_6^2}{1728}.$$

The discriminant of $\mathcal{C}$ is the quantity from which we know if a given Weierstrass curve is nonsingular or not as the following proposition states

Proposition 4.1.7. *[52] A Weierstrass curve is nonsingular if and only if its discriminant is not vanish in K.*

Remark. There is an explicit formulas given in [22, 26]. for calculating the genus of a nonsingular projective plane curve of degree d. This formulas is $\frac{(d-1)(d-2)}{2}$. From this formulas we see that every nonsingular Weierstrass curve is an elliptic curve.

In the following theorem we see that every elliptic curve is isomorphic to a nonsingular Weierstrass curve. For the proof, see [26].

Theorem 4.1.8. *Let E be an elliptic curve defined over K and $\mathcal{O}_E$ is the identity point of E. Then there exists rational functions f_E, g_E in $K(E)$ such that $ord_{\mathcal{O}_E}(f_E) = -2$ and $ord_{\mathcal{O}_E}(g_E) = -3$ and defined at every other point on E and a_1, a_3, a_2, a_4, a_6 in K satisfying the following equation*

$$g_E^2 + a_1 f_E g_E + a_3 g_E = f_E^3 + a_2 f_E^2 + a_4 f_E + a_6. \tag{4.2}$$

Obviously, the equation (4.2) allows to define an isomorphism of algebraic curves ϕ_E from E to a Weierstrass curve $\mathcal{C} \cup \{[0,1,0]\}$ such that $\mathcal{C}$ is the affine curve defined from the equation (4.2) as follows.

$$\mathcal{C} : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{4.3}$$

and the isomorphism ϕ_E is defined as follows

$$\phi_E(\mathcal{O}_E) = [0,1,0] \quad \text{and} \quad \phi_E(P) = (f_E(P), g_E(P)) \ \text{ for all } \ P \in E.$$

The curve $\mathcal{C}$ is called the Weierstrass model of E and its equation is called the Weierstrass equation of E. Notice that the Weierstrass model is not the only model but there are other models of every elliptic curve E which are not treated in this work [5, 6, 18, 27, 43, 53].

4.1.2 $\jmath$-invariant

Definition 4.1.9 ($\jmath$-invariant)**.** Let E/K be an elliptic curve defined by its Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_3, a_2, a_4, a_6 \in K. \tag{4.4}$$

with its points at infinity $[0, 1, 0]$. The $\jmath$-invariant of E, denoted by $\jmath(E)$, is defined to be the following quantity:

$$\jmath(E) = \frac{C_4^2}{\Delta(E)}.$$

Tow Weierstrass equations are said to be isomorphic if there exists an isomorphism between the Weierstrass curves described by these equations and sending $[0, 1, 0]$ to $[0, 1, 0]$. In the following proposition we see that a such isomorphism exists in the case of elliptic curves if and only if these curves have the same $\jmath$-invariant.

Proposition 4.1.10. *[52]*

(a) Two elliptic curves E_1/K and E_2/K are isomorphic over $\overline{K}$ if and only if $\jmath(E_1) = \jmath(E_2)$.

(b) Let $\jmath \in \overline{K}$. Then there exists an elliptic curve defined over $K(\jmath)$ whose

$\jmath$-invariant is equal to $\jmath$, denoted by $E_\jmath$ and defined as follows:

$$\begin{aligned} E_\jmath &: y^2+xy = x^3 + \frac{36}{1728-\jmath}x + \frac{1}{1728-\jmath} \qquad \text{if} \quad \jmath \notin \{0, 1728\}, \\ E_{1728} &: y^2 = x^3 + x, \\ E_0 &: y^2 + y = x^3. \end{aligned}$$

4.1.3 Explicit formulas of the group law

Let E/K be an elliptic curve. The Weierstrass equation of E allows to provide the explicit formulas of the additive group law defined by the points of E. For the proof, see [52].

Theorem 4.1.11. *Let E/K be an elliptic curve defined by its Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_3, a_2, a_4, a_6 \in K.$$

with its point at infinity $[0, 1, 0]$. The point $[0, 1, 0]$ will be the identity point of the group law defined on E from its Weierstrass equation. This group law is defined as follows: let $P = (x, y)$, $Q = (x', y')$ be two points on E. Then we have

1) $-P = (x, -y - a_1x - a_3)$.

2) If $Q = -P$, then $P + Q = [0, 1, 0]$.

3) If $Q \neq -P$, then $P + Q = (x'', y'')$ such that

$$x'' = \lambda^2 + a_1\lambda - a_2 - x - x' \quad \text{and} \quad y'' = (-\lambda + a_1)x'' - \nu - a_3 \ ,$$

where,

$$\begin{cases} (\lambda, \nu) = \left(\frac{y'-y}{x'-x}, \frac{yx'-y'x}{x'-x}\right) & \text{if} \quad x \neq x' \\ (\lambda, \nu) = \left(\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}, \frac{-x^3+a_4x+2a_6-a_3y}{2y+a_1x+a_3}\right) & \text{if} \quad x = x' \end{cases}$$

Example 4.1.12. [52] Let $E/\mathbb{Q}$ be the elliptic curve defined by its Weierstrass equation

$$E : y^2 = x^3 + 17$$

and its point at infinity $[0, 1, 0]$. Let $P_1 = (-2.3)$ and $P_2 = (2, 5)$ be two points on E. Then $[-2]P_1 = (8, 23)$ and $[3]P_1 - P_2 = (52, 375)$.

4.2 Division polynomials

In the following theorem we see that the multiplication by N-isogeny of an elliptic curve E can be defined by explicit rational functions coming up from the explicit group law of E defined from its Weierstrass equation. For the proof, see [10, 31].

Theorem 4.2.1. *Assume that $charK \neq 2$. Let E/K be an elliptic curve defined by its Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_3, a_2, a_4, a_6 \in K. \tag{4.5}$$

with its point at infinity $[0, 1, 0]$. For all poisitive integer N, there exist rational functions ψ_N, ϕ_N and $\omega_N \in K[x, y]$ such that

$$[N]P = \left(\frac{\phi_N(P)}{\psi_N^2(P)}, \frac{\omega_N(P)}{\psi_N^3(P)} \right).$$

ψ_N *are defined recursively via:*

$$\begin{aligned}
\psi_0 &= 0, \\
\psi_1 &= 1, \\
\psi_2 &= 2y + a_1x + a_3, && (4.6)\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, && (4.7)\\
\psi_4 &= \psi_2\left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\right), && (4.8)\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad m \geq 2, && (4.9)\\
\psi_{2m} &= \psi_m\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+2}^2\right)/\psi_2 \qquad m > 2, && (4.10)
\end{aligned}$$

ϕ_N *are defined recursively via:*

$$\phi_0 = 1, \quad \phi_1 = x, \quad \phi_N = x\psi_N^2 - \psi_{N+1}\psi_{N-1}.$$

ω_N *are defined recursively via:*

$$\begin{aligned}
\omega_0 &= 1 \\
\omega_1 &= y \\
\omega_2 &= -\left(3x^2 + 2a_2x + a_4 - a_1y\right)\phi_2 - \left(-x^3 + a_4x + 2a_6 - a_3y\right)\psi_2^2 - (a_1\phi_2 + a_3\phi_2^2)\psi_2 \\
\omega_{2m+1} &= \omega_m\psi_{3m+2} - \omega_{m+1}\psi_{3m+1} - \left(a_1\phi_{2m+1} + a_3\psi_{2m+1}^2\right)\psi_{2m+1} \qquad m \geq 1, \\
\omega_{2m} &= (\omega_{m-1}\psi_{3m+1} - \omega_{m+1}\psi_{3m-1})/\psi_2 - (a_1\phi_{2m} + a_3\psi_{2m}^2)\psi_{2m} \qquad m \geq 2.
\end{aligned}$$

ω_N *can be defined also by the following relation:*

$$\omega_N = [(\psi_{N+2}\psi_{N-1}^2 - \psi_{N-2}\psi_{N+1}^2)/\psi_2 - (a_1\phi_N + a_3\psi_N^2)\psi_N]/2 \qquad (4.11)$$

ψ_N *and* ϕ_N *satisfay the following relation:*

$$\phi_r\psi_m^2 - \phi_m\psi_r^2 = \psi_{m-r}\psi_{m+r}, \qquad 1 \leq r \leq m \qquad (4.12)$$

Definition 4.2.2. Let E/K be an elliptic curve defined by its Weierstrass equation (4.5) with its point at infinity. The rational functions defined in Theorem 4.2.1 are called the N^{th} division polynomials on E. Notice that division polynomials for elliptic curves over field of characteristic 2 are defined in [2].

4.3 The Endomorphism ring

The set of isogenies of an elliptic curve E to itself endowed by the addition of isogenies and the composition of isogenies

$$\forall P \in E, \quad (\psi + \varphi)(P) = \psi(P) + \varphi(P) \quad \text{and} \quad (\psi \circ \varphi)(P) = \psi\left(\varphi(P)\right)$$

defines a ring called the endomorphism ring of E and denoted by $End(E)$.

The general classification of the endomorphism ring of an elliptic curve is given in the following theorem. For farther studies about the structure of the endomorphism rings of these curves we refer to [31, 61].

Theorem 4.3.1. *[52] Let E be an elliptic curve. The endomorphism ring $End(E)$ of an elliptic curve E is either $\mathbb{Z}$, or an order in an imaginary quadratic field[1], or an order in a definite quaternion algebra over $\mathbb{Q}$[2]. If $char(K) = 0$, then only the first two cases are possible.*

Remark. If $char(K) = 0$, then from the above Theorem $End(E)$ is equal to $\mathbb{Z}$ or an order in an imaginary quadratic field, which implies that $End(E)$ is always commutative. We say that E has complex multiplication or **CM** for short if its $End(E)$ is an order in an imaginary quadratic field. We refer to [33, 60] for more details.

[1]There are many references studying imaginary quadratic fields and orders in these number fields, we propose [41]

[2]for the study of the Arithmetic of quaternion algebra over $\mathbb{Q}$ we propose [57]

Remark. The endomorphism ring of an elliptic curve E defined over $\overline{\mathbb{F}}_p$ is larger than $\mathbb{Z}$. See [16] or [52].

Definition 4.3.2. [52] Let K be perfect field of finite characteristic and E/K is an elliptic curve. E is called supersingular if its endomorphism ring is an order in a quaternion algebra. Otherwise, we say that E is ordinary.

For further studies on supersingular elliptic curves see [47, 55, 58]. Notice that supersingular elliptic curves are exploited in anti-symmetric cryptography that is based on hash functions [14, 15, 21].

The following theorem connects between the structure of the endomorphism ring of any elliptic curve E and the structure of its p-torsion group when E is defined over a perfect field of finite characteristic p. For the proof, see [16] or [52].

Theorem 4.3.3. *[16] Let K be a perfect field of positive characteristic $p > 0$ and E/K is an elliptic curve. Then E is supersingular over $\overline{K}$ if and only if $E[p]$ is reduced to $\{\mathcal{O}_E\}$.*

Theorem 4.3.4. *If E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, then $\jmath(E) \in \mathbb{F}_{p^2}$.*

Proof. See. [16] or [33] or [52]. □

From this necessary condition given in the above theorem we see that there are only finitely many supersingular elliptic curves up to isomorphism over $\overline{\mathbb{F}}_p$ and they are all defined over $\mathbb{F}_{p^2}$, which motivated many known mathematiciens to find the number of the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, or farther determine these classes. See [8, 11, 19, 29, 49, 52, 60].

Chapter 5

Supersingular elliptic curves over $\overline{\mathbb{F}}_5$

As has been said in the previous chapter, the determination of the supersingular elliptic curves over finite characteristic p is considered by many mathematicians. The case $p = 2$ was treated by Washington [60] and the case $p = 3$ was treated by Silverman [52] and for the general case $p \geq 5$ we have several demonstrations [8, 19, 29]. In this chapter we give an explicit proof for the particular case $p = 5$, that is stated in the following theorem

Theorem 5.0.1. *There is a unique supersingular elliptic curve up to isomorphism over $\overline{\mathbb{F}}_5$, and its $\jmath$-invariant is equal to zero.*

Our tools for this proof are reviewed in the previous chapter: Theorem 4.2.1, Theorem 4.3.3, Theorem 4.1.3 and Proposition 4.1.10.

Proof of Theorem 5.0.1

From Proposition 4.1.10 we have for all $\jmath \in \overline{\mathbb{F}}_5$, an elliptic curve $E_\jmath$ of $\jmath$-invariant equal to $\jmath$ is defined over $\overline{\mathbb{F}}_5$ as follows:

$$E_\jmath \ : \ y^2 + xy = x^3 + \frac{1}{3-j}x + \frac{1}{3-j} \ \text{ if } \ j \neq 0 \text{ and } \jmath \neq 3, \tag{5.1}$$

$$E_0 \ : \ y^2 + y = x^3, \tag{5.2}$$

$$E_3 \ : \ y^2 = x^3 + x. \tag{5.3}$$

The following change of variables $(x, y) \mapsto (x + 2, y + 2x - 1)$ transforms the equation (5.1) into the following

$$y^2 = x^3 + \frac{2\jmath}{3-\jmath}x + \frac{\jmath}{3-\jmath}, \tag{5.4}$$

and the following change of variables $(x, y) \mapsto (x, y + 2)$ transforms the equation (5.2) into the following

$$y^2 = x^3 - 1. \tag{5.5}$$

Now we require the following proposition

Proposition 5.0.2. *Let $\jmath \in \overline{\mathbb{F}}_5$. Let P be a point on $E_\jmath$. Then we have*

$$[5]P = \mathcal{O} \Leftrightarrow \psi_5(P) = 0.$$

Proof. From (5.4), (5.3) and (5.5) we have for all $\jmath \in \overline{\mathbb{F}}_5$, the elliptic curve $E_\jmath$ is defined by an equation of the form

$$y^2 = x^3 + A_\jmath x + B_\jmath.$$

Let P be a point on $E_\jmath$. Then we have

$$[5]P = \mathcal{O} \Leftrightarrow [3]P = -[2]P \Leftrightarrow \frac{\phi_3(P)}{\psi_3(P)^2} = \frac{\phi_2(P)}{\psi_2(P)^2} \text{ and } \frac{\omega_3(P)}{\psi_3(P)^3} = -\frac{\omega_2(P)}{\psi_2(P)^3}. \tag{5.6}$$

From (4.12) we have

$$\frac{\phi_3(P)}{\psi_3(P)^2} = \frac{\phi_2(P)}{\psi_2(P)^2} \Leftrightarrow \phi_3(P)\psi_2(P)^2 - \phi_2(P)\psi_3(P)^2 = 0 \Leftrightarrow \psi_5(P) = 0,$$

and from (4.9) we have

$$\psi_5(P) = 0 \Leftrightarrow \psi_4(P)\psi_2(P)^3 - \psi_3(P)^3 = 0 \Leftrightarrow \frac{1}{\psi_2^3(P)} = \frac{\psi_4(P)}{\psi_3(P)^3}.$$

Therefore, from (4.11) we obtain

$$\frac{\omega_3(P)}{\psi_3(P)^3} = \frac{\psi_5(P)\psi_2(P)^2 - \psi_4(P)^2}{2\psi_2(P)\psi_3(P)^3} = \frac{-\psi_4(P)^2}{2\psi_2(P)\psi_3(P)^3} = \frac{-\omega_2(P)}{\psi_2(P)^3}.$$

Then the system given by (5.6) holds for $\psi_5(P) = 0$, which completes the proof. □

In the following theorem we prove that every non zero $\jmath$-invariant defines a non supersingular elliptic curve over $\overline{\mathbb{F}}_5$.

Theorem 5.0.3. *Every elliptic curve over $\overline{\mathbb{F}}_5$ of non zero $\jmath$-invariant is not supersingular.*

Proof. In view of Proposition 4.1.10 all the $\overline{\mathbb{F}}_5$ -isomorphic elliptic curves have the same $\jmath$-invariant. Then it suffices to study the supersingularity of the elliptic curve $E_\jmath$ defined by the equation (5.4) if $\jmath \in \overline{\mathbb{F}}_5^*\backslash\{3\}$, and by the equation (5.3) if $\jmath = 3$. Let $P = (x, y)$ be a point in $\mathbb{A}^2_{\overline{\mathbb{F}}_5}$. We have $P \in E_\jmath[5]$ if and only if $P \in E_\jmath$ and $[5]P = \mathcal{O}$. From Proposition 5.0.2, we have $\psi_5(x, y) = 0$. Therefore, we obtain

$$P \in E_\jmath[5] \Leftrightarrow \begin{cases} y^2 = x^3 + \frac{2\jmath}{3-\jmath}x + \frac{\jmath}{3-\jmath}, \\ \psi_2^3(x,y)\psi_4(x,y) - \psi_3^3(x,y) = 0. \end{cases} \quad \text{if} \quad \jmath \in \overline{\mathbb{F}}_5^*\backslash\{3\}, \tag{5.7}$$

$$P \in E_3[5] \Leftrightarrow \begin{cases} y^2 = x^3 + x, \\ \psi_2^3(x,y)\psi_4(x,y) - \psi_3^3(x,y) = 0. \end{cases} \tag{5.8}$$

From (4.6), (4.7) and (4.8) we get

$$(5.7) \Leftrightarrow \begin{cases} \frac{\jmath}{3-\jmath}x^{10} + \frac{\jmath}{3-\jmath}x^9 + \frac{4\jmath^3}{(3-\jmath)^3}x^5 + \frac{\jmath^4}{(3-\jmath)^4}x^2 + \left(\frac{\jmath^6}{(3-\jmath)^6} - \frac{2\jmath^4}{(3-\jmath)^5}\right) = 0, \\ y^2 = x^3 + \frac{2\jmath}{3-\jmath}x + \frac{\jmath}{3-\jmath}. \end{cases} \tag{5.9}$$

$$(5.8) \Leftrightarrow \begin{cases} 3x^{10} + 4 = 0, \\ y^2 = x^3 + x. \end{cases} \tag{5.10}$$

Since $\overline{\mathbb{F}}_5$ is an algebraically closed field, we see that the two systems given by (5.7) and (5.8) have solutions over $\overline{\mathbb{F}}_5$. Therefore, for all $\jmath \in \overline{\mathbb{F}}_5^*$, $E_\jmath[5]$ is larger than $\mathcal{O}$, which implies, by Theorem 4.3.3 that $E_\jmath$ is not supersingular over $\overline{\mathbb{F}}_5$. Thus we get the result. □

In the following theorem we prove that the zero $\jmath$-invariant defines a supersingular elliptic curve over $\overline{\mathbb{F}}_5$.

Theorem 5.0.4. *Let E_0 be the elliptic curve defined by the equation (5.5). Then E_0 is supersingular over $\overline{\mathbb{F}}_5$.*

Proof. Assume that E_0 is not supersingular over $\overline{\mathbb{F}}_5$. Then by Theorem 4.3.3 and Theorem 4.1.3, there exists a 5-torsion point $P = (x, y)$ on E_0. This implies that (x, y) satisfies the equation (5.5) and by Proposition 5.0.2 (x, y) satisfies also the following equation

$$\psi_5(x, y) = \psi_2^3(x, y)\psi_4(x, y) - \psi_3(x, y)^3 = 0.$$

From (4.6), (4.7), (4.8) and (5.5) we find that

$$\psi_2^3(x, y)\psi_4(x, y) - \psi_3(x, y)^3 = 0 \Leftrightarrow -1 = 0,$$

which is impossible. Then the group $E_0[5]$ must be reduced to $\{\mathcal{O}\}$. Thus by Theorem 4.1.3 E_0 is supersingular over $\overline{\mathbb{F}}_5$. □

In view of Theorem 5.0.3 every $\overline{\mathbb{F}}_5$-isomorphism class defined by a nonzero $\jmath$-invariant is not supersingular, and by Theorem 5.0.4 the zero $\jmath$-invariant defines a supersingular $\overline{\mathbb{F}}_5$-isomorphism class of elliptic curves. Then, there exists a unique supersinular elliptic curve up to isomorphism over $\overline{\mathbb{F}}_5$ and its $\jmath$-invariant is equal to zero. Thus We get the proof.

Remark. The systems given by (5.9) and (5.10) (for the cas $\jmath = 3$) allow to determine the 5-torsion group of any elliptic curve E defined over $\overline{\mathbb{F}}_5^*$. For example, from the system given by (5.9) we find that the elliptic curve defined over $\overline{\mathbb{F}}_5^*$ given by its Weierstrass equation

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

with its point at infinity $\mathcal{O} = [0, 1, 0]$ and whose the $\jmath$-invariant is 1 has the 5-torsion group defined over $\mathbb{F}_{25}$,

$$E[5] = \{\mathcal{O}, (\omega^9, \omega^{22}), (\omega^9, \omega^{10}), (\omega^{21}, \omega^4), (\omega^{21}, \omega^{16})\}.$$

Conclusion

Explicit proofs are generally provided for particular cases of a given general case and the object of these proofs is to get a simple and clear vision that helped us to understand the problematic and its resolution in short or simple ways.

In this work we have provided an explicit proof for determining supersingular elliptic curves in finite characteristic p for the particular case $p = 5$ that is the object of our paper [7]. For our object we have studied extension field theory for understanding some facts in this theory: algebraic closure of a field, perfect fields and finite fields which are arithmetically important for studying algebraic curves and in particular elliptic curves. Also we have needed to acquire some basics in the theory of algebraic geometry for understanding some arithmetic properties of elliptic curves and then find the results needed in this theory for our proof.

Notice that the cases $p = 2$ and $p = 3$ have been proved separately in [60] ($p = 2$) and [52] ($p = 3$). We can investigate the results that we have apply for the case $p = 5$ to give new proofs for these two cases. These proofs can be done in two ways, the first avoids the division polynomials and needs only to use the explicit formulas of the group law of elliptic curves and the second way uses the division polynomials. In the two ways the calculus is short and quick. However, the case $p = 5$ can not be treated with only the

explicit group law of elliptic curves, we have had to introduce the division polynomials on elliptic curves for getting the object.

From the recurrent formulas of the division polynomials on elliptic curves, we speculate that we may provide an explicit proof for the case $p = 7$ but the calculus will be more complicated and longer than the case $p = 5$, so we have to think to introduced some other properties or techniques for madding the calculus simple or a bit short. Also from the recurrent formulas of these polynomials, we can see that the work for any case p greater than 7 can not be completed and if one thinks to provide an explicit proof for any case p greater than 7, then he has to think to introduce other properties or results in this theory.

Bibliography

[1] Adamson, I. T., Introduction to Field Theory, Cambridge University Press, 1982.

[2] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, Handbook of elliptic and hyperelliptic cryptography, Chapman and Hall/CRC, 2006.

[3] E. Bach and J. Shallit, Algorithmic number theory, MIT press, 1996.

[4] S. Bhatia and S. K. Khanduja, Difference polynomials and their generalizations, Mathematika, 293-299, 2001.

[5] D.J. Bernstein, P. Birkner, M. Joye, T. Lange, C.P. Peter,Twisted Edwards curves, Progress in Cryptology - Africacrypt 2008, 389-405.

[6] D. J. Bernstein, T. Lange, and R. R. Farashahi, Binary Edwards curves, C.H.E.S 2008, 244-265.

[7] N. Belhamra, Supersingular elliptic curves over $\overline{\mathbb{F}}_5$, Indian J Pure Appl Math, Springer, 2021.

[8] J. B. Birch, W. Kuyk, Modular functions of one variable IV, Lecture Notes in Mathematics, Springer-Verlag, 1975.

[9] A. Bishnoi and S. K. Khanduja, On Eisenstein-Dumas and Generalized Schönemann polynomials., Comm. Algebra, 3163-3173, 2010.

[10] I. F. Blake, G. Seroussi, and N. P. Smart, Advances in elliptic curve cryptography, Cambridge, 2005.

[11] R. Bröker, Constructing supersingular elliptic curves, J. Comb. Number Theory 1 (2009), no. 3, 269-273.

[12] R. Brown, Roots of Schönemann Polynomials in Henselian extension fields, Indian J. Pure and Applied Mathematics, 403-410, 2008.

[13] J. W. S. Cassels, Lectures on elliptic curves, Cambridge, 1991.

[14] D. Charles, E. Goren and K.E. Lauter, Cryptographic hash functions from expander graphs, Journal of Cryptology, 93-113, 2009.

[15] S. Galbraith, Mathematics of Public Key Cryptography, Cambridge University, 2012.

[16] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abhandlungen aus dem Mathematischen Seminar der University Hamburg, 197-272, 1941.

[17] G. Dumas, Sur quelques cas d´irreductibilite des polynomes á coefficients rationnels, Journal de Math. Pures et Appliqus, 191-258, 1906.

[18] H. M. Edwards, A normal form for elliptic curves, Bulletin of the A.M.S, 393-422, 2007.

[19] N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over Q, Inventiones Mathematicae, 561-567, 1987.

[20] A. J. Engler and S. K. Khanduja, On Irreducible factors of the polynomial f(x)-g(y), International Journal of Mathematics, 407-418, 2010.

[21] L. De Feo, D. Jao and J. Plut, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Journal of Mathematical Cryptology, 209-247, 2014.

[22] W. Fulton, Algebraic curves, Addison-Wesley, 2008.

[23] S. Gao, Normal bases over finite fields, Ph.D. thesis, Waterloo, 1993.

[24] P. Griffiths and J. Harris. Principles of algebraic geometry. Wiley Classics Library. John Wiley and Sons Inc., New York, 1994.

[25] J. Harris, Algebraic geometry, Springer-Verlag, New York, 1992.

[26] R. Hartshorne.Algebraic geometry, Springer-Verlag, 1977.

[27] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, Jacobi quartic curves revisited, Australasian Conference on Information Security and Privacy, 452-468, 2009.

[28] T. W. Hungerford, Algebra, GTM 73, Springer, 1974.

[29] J. I. Igusa. Class number of a definite quaternion with prime discriminant. Proc Natl Acad Sci U S A., 312-314, 1958.

[30] R. Khassa and S. K. Khanduja, A generalization of Eisenstein-Schönemann Irreducibility Criterion, Manuscripta Mathematica, 215-224, 2011.

[31] D. R. Kohel. Endomorphism rings of elliptic curves over finite fields. PhD thesis, University of California, Berkeley, 1996.

[32] E. Kunz, Introduction to plane algebraic curves. Birkhäuser, 2005.

[33] S. Lang, Elliptic functions, Springer, 1987.

[34] S. Lang, Algebra, Addison-Wesley, 1993.

[35] S. Lang , Algebraic number theory, Springer, 1986.

[36] A. K. Lenstra, Factorization of polynomials, Computational methods in number theory, Mathematisch Centrum Amsterdam, 169-198, 1984.

[37] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge, 1994.

[38] R. Lidl and H. Niederreiter, Finite fields, Cambridge, 1997.

[39] H. Lüneburg, On a little but useful algorithm, Lecture Notes in Computer Science, 296-301, 1985.

[40] M.F. Atiyah and I.G. Macdonald. Introduction to commutative algebra. Addison-Wesley, 1969.

[41] D. A. Marcus. Number Fields. Springer, 2018.

[42] H. Matsumura. Commutative ring theory. Cambridge University Press, 1986.

[43] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, Mathematics of computation, 243-264, 1987.

[44] C. J. Moreno, Algebraic curves over finite fields, Cambridge, 1991.

[45] J. Neukirch, Algebraic Number Theory, Springer-Verlag, New York, 1999.

[46] H. Niederreiter, A new efficient factorization algorithm for polynomials over small finite fields, Applicable Algebra in Engineering, Communication and Computing 4 (1993), no. 2, 81- 87.

[47] H. G. Rück, A note on elliptic curves over finite fields, Mathematics of computation, 49, 301-304, 1987.

[48] A. Schinzel, Reducibility of polynomials in several variables II. Pacific J. Math., 531-563, 1985.

[49] R. Schoof, Nonsingular plane cubic curves over finite fields, Journal of Combinatorial Theory, 183-211, 1987.

[50] V. Shoup , A computational introduction to number theory and algebra, Cambridge, 2005.

[51] I. R. Shafarevich, Basic algebraic geometry, Springer, 2013.

[52] J. H. Silverman. The arithmetic of elliptic curves, Springer Science and Business Media, 2009.

[53] M. Stam, On Montgomery-like representations of elliptic curves over GF(2^k), Lecture Notes in Computer Science, 240-253, 2003.

[54] Stewart, I.A, Galois Theory, Chapman and Hall/CRC, 2014.

[55] M. A. Tsfasman, Group of points of an elliptic curve over a finite field, Theory of numbers and its applications, 286-287, 1985.

[56] H. Tverberg, On the irreducibility of polynomials $f(x) + g(y) + h(z)$, Quart. J. Math., 364-366, 1966.

[57] M.F. Vignèras, Arithmétique des algébres de quaternions, Lecture Notes in Mathematics, Springer, 1980.

[58] J. F. Voloch, A note on elliptic curves over finite fields, Bulletin de la S.M.F, 455-458, 1988.

[59] J. von zur Gathen and M. Giesbrecht, Constructing normal bases in finite fields, J. Symb. Comput. 10 (1990), no. 6, 547-570.

[60] L. C. Washington. Elliptic Curves: Number Theory and Cryptography, Second Edition. New York, 2003.

[61] E. Waterhouse, Abelian varieties over finite fields, Annale Scientifique De l'É.N.S., 521-560, 1969.

[62] S. H. Weintraub, A mild generalization of Eisensteins criterion, Proc. A.M.S, 1159-1160, 2013.