PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

# Equations over finite fields: the Zeta function and Weil Conjectures

Santiago Neira

A thesis presented for the degree of Bachelor in Mathematics

Advisor:
Jesus Alonso Ochoa Arango, Ph.D.

Bogotá - Colombia
November 24, 2022

# Equations over finite fields: Zeta function and Weil Conjectures

Santiago Neira

Department of Mathematics
Faculty of Sciences
Pontificia Universidad Javeriana

**Abstract**

This work is a review of the congruent zeta function and the Weil conjectures for non-singular curves. We derive an equation to obtain the number of solutions of equations over finite fields using Jacobi sums in order to compute the Zeta function for specific equations. Also, we introduce the necessary algebraic concepts to prove the rationality and functionality of the zeta function.

**Key Words: Weil Conjectures, Congruent Zeta function, Equations over finite fields, Gauss sum, Jacobi sum, Nonsingular Complete Curves, Divisors, Riemann-Roch Theorem**

# Contents

# Acknowledgements

Este trabajo y todo mi esfuerzo esta dedicado a mi mamá, Yolima. Quiero agradecerle por todo el amor que me ha brindado en mi vida. Su apoyo y sacrificio ha sido esencial para mi desarrollo como persona y matemático. Las palabras no me alcanzar para agradecerle por todo lo que me hado en la vida. También, quiero agradecer a mis tios: Rafael y Patricia, por el apoyo que me han dado a mi madre y a mi.

Quiero agradecer a mi tutor, Jesus Ochoa, por su tiempo y dedicación en la realización de este trabajo, y a mi formación como matemático. Sus consejos y conocimiento a lo largo de la carrera han sido valiosos. Quiero agradecer a los profesores Jorge Plazas y Rafael Gonzáles, por el conocimiento, el apoyo, y los consejos que me han dado. También, quiero agradecer a todos los profesores de la Universidad Javeriana que fueron participes en mi educación y en mi formación como matemático.

Finalemente quiero agradecer a los amigos que hecho en la universidad. Por ser mi acompañamiento durante estos cuatro años. Por los buenos momentos y la felicidad que me han dado.

¡Gracias Totales!

# Introduction

Mathematicians have been interested in polynomial equations with integer solutions since ancient times. These equations are called Diophantine equations. The most famous example of this type of equation is

$$X^n + Y^n = Z^n, \qquad n > 2. \tag{1}$$

Fermat conjectured that this equation does not have nonzero integer solution. It was until the end of 20th century that Andrew Wiles solved this problem.
To solve (1) is equivalent to find the solution of

$$x^n + y^n = 1, \qquad n > 2 \tag{2}$$

in $\mathbb{Q}$. However, it is still hard to find a solution in $\mathbb{Q}$. Instead, we can consider the equation (2) in a finite field $\mathbb{F}_{p^m}$. The reason, as Koblitz says in his paper [Kob82] from which we base ourselves for this introduction, is that it's easier! Just count the number of solutions. The first chapter of this work is devoted to finding a method to count the number of solutions of a polynomial equation over a finite field denoted by $N_m$; or at least, try to find a bound.
In general, given a prime number $p$ and an equation $f(x, y) = 0$ with $f \in \mathbb{F}_{q^m}[x, y]$, where $q = p^n$. We can encode the sequence $\{N_m\}_{m=1}^{\infty}$ into the generating series

$$\mathbf{Z}(T) = \exp(\sum_{m=1}^{\infty} \frac{N_m T^m}{m}),$$

called the Congruence Zeta function. The form of $\mathbf{Z}(T)$ may appear strange at first, but it has interesting properties, known as the Weil Conjectures due to the French mathematician André Weil, who stated the conjectures in [Wei49]. In chapter 3, we derive the zeta function and compare it with the Riemann and Dedekind $\zeta$ function. Also, we compute several examples of the congruence zeta function and prove two of the Weil conjectures for the case of nonsingular curves. Chapter 2 is devoted to presenting the necessary tools to comprehend chapter 3. We introduce Dedekind domains, ideal class groups, divisors, and the Riemann-Roch theorem.

It is worth to mention another two reasons to consider equations over finite fields, although we do not delve deeper about these topics in this work. The first conjecture states that the zeta function is a rational function, and for curves, the degree of the numerator is twice the Betti number of the corresponding complex Riemann surface. If we consider the set of complex numbers $(x, y)$ that satisfy the equation (2), we obtain a surface having $g = (N-1)(N-2)/2$ "handles". Thus there is a relationship between the number-theoretic properties of the equation considered mod $p$ and its "physical" properties when it is considered complex-analytically. Another parallel between this two branches, is that, in classical theory of algebraic curves over the complex numbers, one

associates to them certain definite integrals, called "periods". In the case of equation (2), these integrals are of the form

$$\int_0^1 x^{j/N}(1-x)^{k/N}\frac{dx}{x(1-x)}.$$

In chapter 1, we introduce Jacobi sum, which is analogous to the expression above. So another reasons for studying equations over finite fields is that deep analogies exist between finite-field theoretic and complex analytic properties of equations.

The second reason for studying over finite fields is that sometimes such information can be pieced together to tell us something about the set of solutions in the field $\mathbb{Q}$ of rational numbers. The best example is the conjecture on elliptic curves formulated by Birch and Swinnerton-Dyer in the early 1960's. Let $y^2 = f(x)$, where $f(x)$ is a cubic polynomial with integer coefficients and distinct roots. This is called an "ellitic curve". The complex Riemann surface corresponding to this equation has one "handle", i.e., the Betti number $g$ is equal to 1.

If we now consider the equation $y^2 = f(x)$ mod a prime $p$ and count all the solutions $(x, y) \in \mathbb{F}_{p^m}$, for each $m$, then we can consider the zeta function

$$\mathbf{Z}_p(T) = \exp\sum_{m=1}^{\infty}\frac{N_{p,m}T^m}{m}.$$

Sine $g = 1$, the numerator of $\mathbf{Z}_p(T)$ has dimension 2. Moreover, the Weil conjectures says that

$$\mathbf{Z}_p(T) = \frac{1 - a_pT + pT^2}{(1-T)(1-pT)}.$$

Taking log in both expressions of $\mathbf{Z}_p(T)$ and equate coefficients of $T$ in the two power series expansion, we obtain the formula

$$a_p = p + 1 - N_{1,p}.$$

We just need to find the value of $N_{1,p}$ and substituting in the equation to obtain $a_p$. Thus, finding the exact expression for $\mathbf{Z}_p(T)$. Since $\mathbf{Z}_p(T)$ determines all of the $N_{m,p}$, once we know $N_{1,p}$, all the $N_{m,p}$ can be found.

Once we know $\mathbf{Z}_p(T)$ for each prime $p$, we can combine all of this information into a single function. This function, called the Hasse-Weil zeta function, is defined as follows for $s$ a complex number:

$$\mathbf{Z}(s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Using well-known estimates for $a_p$, the infinite product converges when $\mathrm{Re}(s) > 3/2$. Moreover, for a broad class of elliptic curves, $Z(s)$ is known to extend by analytic continuation to a meromorphic function on the entire complex $s$-plane; and this is conjectured to be the case for all elliptic curves. Assuming that this extendibility conjecture is true, Birch and Swinnerton-Dyer make the following statement

**Conjecture 0.0.1.** $\mathbf{Z}(1) = 0$ if and only if the equation $y^2 = f(x)$ has infinitely many rational solutions $x, y \in \mathbb{Q}$.

As the reader can see, the connections between information about finite field solutions to equations, and information about $\mathbb{Q}$-solutions are very subtle, indirect, and difficult. Intensive efforts by number theorist have been, and for a long time will continue to be, directed toward understanding such connections.

# Chapter 1

# Counting Solutions of Polynomial Equations.

In this chapter, we want to introduce a method for counting the number of solutions of polynomial equations defined over a finite field. This method is constructed using Gauss and Jacobi sums. The behavior of these sums provides a connection with the number of solutions. Through all the sections we consider the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with $p$ a prime number, and the field $\mathbb{F}_q$ with $q$ elements, where $q = p^n$ for some $n > 0$.

## 1.1 Multiplicative Characters

**Definition 1.1.1.** Let $\mathbb{F}_q$ be a finite field, a multiplicative character on $\mathbb{F}_q$ is a map $\chi$ from $\mathbb{F}_q^*$ to the nonzero complex numbers that satisfies

$$\chi(ab) = \chi(a)\chi(b) \quad \text{for all } a, b \in \mathbb{F}_q^*$$

**Example 1.1.1.** The trivial multiplicative character is the map $\varepsilon : \mathbb{F}_q^* \to \mathbb{C}$ defined by $\varepsilon(a) = 1$ for all $a \in \mathbb{F}_q^*$.

It is possible to extend the notion of multiplicative character over all $\mathbb{F}_q$ as follows:

1. If $\chi \neq \varepsilon$, we define $\chi(0) = 0$.
2. if $\chi = \varepsilon$, we take $\varepsilon(0) = 1$.

The next theorem exposes some basic properties of the multiplicative characters.

**Theorem 1.1.2.** Let $\chi$ be a multiplicative character and $a \in \mathbb{F}_q^*$. Then

1. $\chi(1) = 1$
2. $\chi(a)$ is a $q-1$ th root of unity.
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

*Proof.* The proof of items 1. and 3. can be found in [IR90, Proposition 8.1.1]. In this reference, the proof of item 2. is made for $q = p$, we will prove for $q = p^n$ for any $n > 0$.
We know that $a^{q-1} = 1$, for all $a \in \mathbb{F}_q^*$, which implies that $1 = \chi(1) = \chi(a^{q-1}) = \chi(a)^{q-1}$, i.e., $\chi(a)$ is a $q-1$ th root of unity.

□

The next example presents the Legendre and Jacobi symbol, which are a special kind of character. If the reader wants to know more about these symbols, like the quadratic reciprocity law, refer to [Apo76] and [IR90].

**Example 1.1.3.** Consider $a, m \in \mathbb{Z}$ with $(a, m) = 1$, then $a$ is called a quadratic residue mod $m$ if the congruence $x^2 \equiv a(m)$ has a solution. Otherwise $a$ is called a quadratic nonresidue mod $m$. Associated with this concept, Legendre in 1798 introduced the Legendre symbol $(a/p)$ where $p$ is a prime number. We define the Legendre symbol by 1 if $a$ is a quadratic residue mod $p$, $-1$ if $a$ is a quadratic nonresidue mod $p$, and zero if $p|a$. The Legendre symbol considered as a function of the coset of $a$ modulo $p$ is a multiplicative character. In [IR90, Chapter 5, Theorem 1] is proved that $(-1/p) = (-1)^{(p-1)/2}$.

To determine if a number is a quadratic residue or nonresidue module of a composite number $m$ it is necessary to consider several cases depending on the quadratic character of the factors.

Suppose $m$ a positive odd integer with prime factorization

$$m = \prod_{i=1}^{r} p_i^{a^i}.$$

The Jacobi symbol (n/m) is defined for all integers $n$ by the equation

$$(n/m) = \prod_{i=1}^{r} (n/p_i)^{a^i},$$

where $(n/p_i)$ is the Legendre symbol. Set $(n/1) = 1$.

The congruence

$$x^2 \equiv n\,(m)$$

has a solution if and only if $(n|p_i) = 1$ for all prime $p_i$ of the factorization of $m$.

Again, the Jacobi symbol $(-1/m)$ is given by $(-1)^{(m-1)/2}$, the proof can be consulted in [Apo76, Theorem 9.10]

**Theorem 1.1.4.** Let $\chi$ be a multiplicative character. If $\chi \neq \varepsilon$, then $\sum_t \chi(t) = 0$, where the sum is over all $t \in \mathbb{F}_q$. If $\chi = \varepsilon$ the value of the sum is $q$.

*Proof.* The last assertion is obvious, so we may assume that $\chi \neq \varepsilon$. There exists an $a \in \mathbb{F}_q^*$ such that $\chi(a) \neq 1$. Let $T = \sum_{t \in \mathbb{F}_q} \chi(t)$, then

$$\chi(a)T = \sum_{t \in \mathbb{F}_q} \chi(a)\chi(t) = \sum_{t \in \mathbb{F}_q} \chi(at) = \sum_{\hat{t} \in \mathbb{F}_q} \chi(\hat{t}) = T.$$

Since $\chi(a)T = T$ and $\chi(a) \neq 1$, therefore $T = 0$. □

**Remark 1.1.5.** The multiplicative characters form a group with composition and inverse defined as follows:

1. If $\chi$ and $\lambda$ are characters, then $\chi\lambda$ is the map that takes $a \in \mathbb{F}_q^*$ to $\chi(a)\lambda(a)$.
2. If $\chi$ is a character, $\chi^{-1}$ is the map that takes $a \in \mathbb{F}_q^*$ to $\chi(a)^{-1}$.
3. $\varepsilon$ is the identity of the group.

**Theorem 1.1.6.** The group of multiplicative characters is a cyclic group of order $q-1$.

*Proof.* We know that $\mathbb{F}_q^*$ is cyclic since the multiplicative group of a finite field is cyclic. Let $g \in \mathbb{F}_q^*$ be a generator. Then every $a \in \mathbb{F}_q^*$ has the form $a = g^l$ for $l \in \{1, 2, \ldots, q-1\}$. If $\chi$ is a character, then $\chi(a) = \chi(g)^l$. This shows that $\chi$ is completely determined by the value of $\chi(g)$. Since $\chi(g)$ is a $q-1$ th root of unity, it follows that the character group has order at most $q-1$.

Now define a function $\lambda$ by the equation $\lambda(g^k) = e^{2\pi i(k/(q-1))}$. By the properties of the exponential, $\lambda$ is a multiplicative character. Suppose $n$ is the smallest integer such that $\lambda^n = \varepsilon$, then $\lambda^n(g) = \varepsilon(g) = 1$. However, $\lambda^n(g) = e^{2\pi i(n/(q-1))} = 1$. It follows that $q-1$ divides $n$. Since $\lambda^{q-1}(a) = \lambda(a^{q-1}) = \lambda(1) = 1$ we have $\lambda^{q-1} = \varepsilon$ so $n = q-1$, and all the character $\varepsilon, \lambda, \lambda^2, \ldots, \lambda^{q-2}$ are distinct. We have proved that there are exactly $q-1$ characters and $\lambda$ is a generator. □

**Corolary 1.1.1.** If $a \in \mathbb{F}_q^*$ and $a \neq 1$, then there is a character $\chi$ such that $\chi(a) \neq 1$. Moreover, $\sum_{\chi} \chi(a) = 0$, where the summation is over all characters.

*Proof.* We have $a = g^l$ with $q-1 \nmid l$, then $\lambda(a) = \lambda(g)^l = e^{2\pi i(l/(q-1))} \neq 1$. Let $S = \sum_{\chi} \chi(a)$. Since $a \neq 1$, there is a character $\lambda$ such that $\lambda(a) \neq 1$. Then

$$\lambda(a)S = \sum_{\chi} \lambda(a)\chi(a) = \sum_{\chi} \lambda\chi(a) = \sum_{\hat{\chi}} \hat{\chi}(a) = S$$

The sums are over all the characters. It follows that $(\lambda(a) - 1)S = 0$, thus $S = 0$. □

Now we will state some theorems that will lead us to a method to determine the number of solution of $x^n = a$.

**Theorem 1.1.7.** Let $\alpha \in \mathbb{F}_q^*$. The equation $x^n = \alpha$ is solvable iff $\alpha^{(q-1)/d} = 1$ where $d = (n, q-1)$. In addition, $d$ is the number of solutions.

For the proof we need the following result:

**Theorem 1.1.8.** Let $a, m \in \mathbb{Z}$ and $d = (a, m)$. The congruence $ax \equiv b\,(m)$ has solutions iff $d|b$. If $d|b$, then there are exactly $d$ solutions.

*Proof.* The proof is stated and proved in [IR90, Theorem 3.3.1]. □

Now we continue with the proof of the Theorem 1.1.7.

*Proof.* Let $\gamma$ be a generator of $\mathbb{F}_q^*$ and set $\alpha = \gamma^a$ and $x = \gamma^y$. Then

$$x^n = \alpha \;\Leftrightarrow\; \gamma^{ny} = \gamma^a \;\Leftrightarrow\; \gamma^{ny-a} = 1 \;\Leftrightarrow\; (q-1)|(ny-a) \;\Leftrightarrow\; ny \equiv a\,(q-1)$$

Then $d$ must divide $a$ as consequence of Theorem 1.1.8.

$$\alpha^{(q-1)/d} = (\gamma^a)^{(q-1)/d} = (\gamma^{dk})^{(q-1)/d} = \gamma^{k(q-1)} = 1.$$

Moreover, by the same theorem, the equation has $d$ solutions.

Now suppose $\alpha^{(q-1)/d} = 1$, then $\gamma^{a(q-1)/d} = 1$. This means that $d|a$ or $q-1$ divides $a(q-1)/d$ . In the first case, we get $ny \equiv a\ (q-1)$ is solvable, and we obtain the result consequently of the first

part of the proof. Now, assume that $q-1$ divides $a(q-1)/d$. Set $(q-1) = dk_1$ for some $k_1$, notice that

$$a(q-1)/d = (q-1)k_2 \;\Leftrightarrow\; ak_1 = (q-1)k_2 \;\Leftrightarrow\; a(q-1) = d(q-1)k_2$$

$$\Leftrightarrow\; 0 = d(q-1)k_2 - a(q-1) \;\Leftrightarrow\; 0 = (q-1)(dk_2 - a) \;\Leftrightarrow\; dk_2 = a.$$

Hence $d|a$, and we obtain the first case. In both cases $x^n = a$ has a solution.

□

For simplicity, we will assume that $n|q-1$ and $d = (n, q-1)$, the reason will be given in Theorem 1.1.11.

The next theorems provide a connection between the characters and the solutions of $x^n = a$ with $a \in \mathbb{F}_q$.

**Theorem 1.1.9.** If $a \in \mathbb{F}_q^*$ and $x^n = a$ is not solvable, then there is a character $\chi$ such that

1. $\chi^n = \varepsilon$
2. $\chi(a) \neq 1$

*Proof.* Let $g$ and $\lambda$ be as in theorem 1.1.6 and set $\chi = \lambda^{(q-1)/n}$. Then $\chi(g) = \lambda(g)^{(q-1)/n} = e^{2\pi i/n}$. Now let $a = g^l$ for some $l$, and since $x^n = a$ is not solvable, we must have that $n$ does not divide $l$. Then $\chi(a) = \chi(g)^l = e^{2\pi i(l/n)} \neq 1$. Finally, $\chi^n = \lambda^{q-1} = \varepsilon$. □

**Theorem 1.1.10.** For $a \in \mathbb{F}_q$, let $N(x^n = a)$ denote the number of solutions of the equation $x^n = a$, then we have

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a),$$

where the sum is over all characters of order dividing $n$.

*Proof.* First we prove that there are exactly $n$ character of order dividing $n$. If $g$ is a generator of $\mathbb{F}_q^*$ then the value of $\chi(g)$ for such a character must be an $n$th root of unity, there are at most $n$ such characters. In the proof of theorem 1.1.9, we found a character $\chi$ such that $\chi(g) = e^{2\pi i/n}$. It follows that $\varepsilon, \chi, \chi^2, \ldots, \chi^{n-1}$ are $n$ distinct characters of order dividing $n$.
To prove the formula, notice that $x = 0$ is the only solution of $x^n = 0$ and $\sum_{\chi^n=\varepsilon} \chi(0) = 1$.
Now suppose that $a \neq 0$ and that $x^n = a$ is solvable; i.e., there is an element $b$ such that $b^n = a$. Remember that by theorem 1.1.7, there are $n$ solutions of $x^n = a$. If $\chi^n = \varepsilon$, then $\chi(a) = \chi(b^n) = \chi(b)^n = \varepsilon(b) = 1$. Thus $\sum_{\chi^n=\varepsilon} \chi(a) = n = N(x^n = a)$.
Finally, suppose that $x^n = a$ is not solvable. Let $T = \sum_{\chi^n=\varepsilon} \chi(a)$. By theorem 1.1.9, there is a character $\rho$ such that $\rho(a) \neq 1$ and $\rho^n = \varepsilon$. Now

$$\rho(a)T = \sum_{\chi^n=\varepsilon} \rho(a)\chi(a) = \sum_{\chi^n=\varepsilon} \rho\chi(a) = \sum_{\hat{\chi}^n=\varepsilon} \hat{\chi}(a) = T.$$

Thus $(\rho(a) - 1)T = 0$ and $T = 0$, i.e., $\sum_{\chi^n=\varepsilon} \chi(a) = 0$. □

What happen if we put aside the assumption that $d = (n, q-1) = n$? The answer is the next theorem that assures us that we can still compute the number of solution.

**Theorem 1.1.11.** Let $q = p^n$, where $p$ is a prime number. Suppose $d = (m, q-1)$, then $N(x^m = a) = \sum_{\chi^d=\varepsilon} \chi(a)$. Moreover, $N(x^m = a) = N(x^d = a)$.

*Proof.* We use the results obtained in the proof theorem 1.1.10, since $d = (d, q-1)$ we have that $N(x^d = a) = \sum_{\chi^d=\varepsilon} \chi(a)$.

Assume that $a = 0$, then $x^m = 0$. The unique solution is $x = 0$, so $N(x^d = 0) = \sum_{\chi^d=\varepsilon} \chi(0) = 1 = N(x^m = 0)$.

If $a \neq 0$. Case 1: $x^m = a$ has a solution, then by theorem 1.1.7 there are $d$ solutions, i.e., $N(x^m = a) = d$. Hence $N(x^d = a) = \sum_{\chi^d=\varepsilon} \chi(a) = d = N(x^m = a)$.

Case 2. Suppose $x^m = a$ is not solvable, then $a^{(q-1)/d} \neq 1$. Assume that $x^d = a$ is solvable, then $a^{(q-1)/d} = 1$ which is a contradiction so $x^d = a$ is not solvable. Therefore

$$N(x^d = a) = \sum_{\chi^d=\varepsilon} \chi(a) = 0 = N(x^m = a).$$

□

**Example 1.1.12.** Suppose that $p$ is odd and that $n = 2$. Using Theorem 1.1.10, we obtain $N(x^2 = a) = 1 + (a/p)$ , where $(a/p)$ is the Legendre symbol.

## 1.2 Gauss Sums

**Definition 1.2.1.** Suppose that $\mathbb{F}_q$ has $q = p^n$ elements for some $n > 0$. For $\alpha \in \mathbb{F}_q$, we define the trace of $\alpha$, denoted by $\mathrm{tr}(\alpha)$, as the sums $\alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{n-1}}$.

Some properties of the trace are cited below, the proof of the items that are not proved here can be found in [IR90, Theorem 10.3.1].

**Theorem 1.2.1.** If $\alpha, \beta \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$, then

1. $\mathrm{tr}(\alpha) \in \mathbb{F}_p$.
2. $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$.
3. $\mathrm{tr}(a\alpha) = a\mathrm{tr}(\alpha)$.
4. tr maps $\mathbb{F}_q$ onto $\mathbb{F}_p$.

*Proof.* 4. The polynomial $x + x^p + \ldots + x^{p^{n-1}}$ has at most $p^{n-1}$ roots in $\mathbb{F}_q$. Since $\mathbb{F}_q$ has $p^n$ elements there is an $\alpha \in \mathbb{F}_q$ such that $\mathrm{tr}(\alpha) = c \neq 0$. If $b \in \mathbb{F}_p$, then using property 3. we obtain that $\mathrm{tr}((b/c)\alpha) = (b/c)\mathrm{tr}(\alpha) = b$. Therefore, the trace is onto. □

**Definition 1.2.2.** Let $\zeta_p = e^{2\pi i/p}$. We define $\psi : \mathbb{F}_q \to \mathbb{C}$ by $\psi(\alpha) = \zeta_p^{\mathrm{tr}(\alpha)}$.

**Theorem 1.2.2.** The function $\psi$ has the following properties:

1. $\psi(\alpha + \beta) = \psi(\alpha)\psi(\beta)$
2. There is an $\alpha \in F$ such that $\psi(\alpha) \neq 1$.

3. $\sum_{\alpha \in F} \psi(\alpha) = 0$

*Proof.* 1. Let $\alpha, \beta \in \mathbb{F}$, then

$$\psi(\alpha+\beta) = \zeta_p^{\mathrm{tr}(\alpha+\beta)} = \zeta_p^{\mathrm{tr}(\alpha)} \zeta_p^{\mathrm{tr}(\beta)} = \psi(\alpha)\psi(\beta).$$

2. tr is onto, so there is an $\alpha \in \mathbb{F}_q$ such that tr($\alpha$) =1. Then $\psi(\alpha) = \zeta_p \neq 1$.

3. Let $S = \sum_{\alpha \in F} \psi(\alpha)$, choose $\beta$ such that $\psi(\beta) \neq 1$. Then $\psi(\beta)S = \sum_{\alpha \in F} \psi(\beta)\psi(\alpha) = \sum_{\alpha \in F} \psi(\beta+\alpha) = S$. It follows that $S = 0$.

□

The next result is taken from [IR90, Theorem 10.3.3], it will help to prove some results involving Gauss sums. The proof can be consulted there.

**Theorem 1.2.3.** Let $\alpha, x, y \in \mathbb{F}_q$. Then

$$\frac{1}{q} \sum_{\alpha \in \mathbb{F}_q} \psi(\alpha(x-y)) = \delta(x,y)$$

where $\delta(x,y) = 1$ if $x = y$ and zero otherwise.

*Proof.* If $x = y$, then $\sum_{\alpha \in \mathbb{F}_q} (\psi(\alpha(x-y)) = \sum_{\alpha \in \mathbb{F}_q} \psi(0) = q$.

If $x \neq y$, then $x - y \neq 0$ and $\alpha(x-y)$ ranges over all of $F$ as $\alpha$ ranges over all of $F$. Thus $\sum_{\alpha \in \mathbb{F}_q} \psi(\alpha(x-y)) = \sum_{\beta \in \mathbb{F}_q} \psi(\beta) = 0$ by property 3. of theorem 1.2.2. □

**Definition 1.2.3.** Let $\chi$ be a character of $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q^*$. The Gauss Sum on $\mathbb{F}_q$ belonging to the character $\chi$ is defined by the expression $g_\alpha(\chi) = \sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t)$. We shall denote $g_1(\chi)$ by $g(\chi)$.

Some properties of the Gauss sums attached to $\chi$ are:

**Theorem 1.2.4.** If $g_\alpha(\chi)$ is a Gauss sum on $\mathbb{F}_q$, where $\chi \neq \varepsilon$. Then

1. $g_\alpha(\chi) = \overline{\chi(\alpha)} g(\chi)$.
2. $g_\alpha(\chi^{-1}) = g_\alpha(\overline{\chi}) = \chi(-1)\overline{g_\alpha(\chi)}$
3. $|g_\alpha(\chi)| = q^{1/2}$
4. $g_\alpha(\chi) g_\alpha(\chi^{-1}) = \chi(-1)q$

*Proof.* 1. If $\chi$ is a character and $\alpha \in \mathbb{F}_q^*$, then

$$\chi(\alpha) g_\alpha(\chi) = \chi(\alpha) \sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t) = \sum_{t \in \mathbb{F}_q} \chi(\alpha t)\psi(\alpha t).$$

Let $s = \alpha t$, since $t$ runs over all $t \in \mathbb{F}$, so $s$ does. Hence

$$\chi(\alpha) g_\alpha(\chi) = \sum_{s \in \mathbb{F}_q} \chi(s)\psi(s) = g(\chi) \;\Rightarrow\; g_\alpha(\chi) = \overline{\chi(\alpha)}\chi(\alpha) g_\alpha(\chi) = \overline{\chi(\alpha)} g(\chi).$$

2. This can be verified by a straightforward computation.

$$\overline{g_\alpha(\chi)} = \sum_{t\in\mathbb{F}_q} \overline{\chi(t)}\psi(-\alpha t) = \sum_{t\in\mathbb{F}_q} \overline{\chi(-1(-t))}\psi(-\alpha t) = \sum_{t\in\mathbb{F}_q} \overline{\chi(-1)}\,\overline{\chi(-t)}\psi(-\alpha t).$$

Notice that $\overline{\chi(-1)} = \chi(-1) = \pm 1$. Let $s = -t$ and

$$\overline{g_\alpha(\chi)} = \chi(-1)\sum_{s\in\mathbb{F}_q} \overline{\chi(s)}\psi(\alpha s) = \chi(-1)g_\alpha(\overline{\chi}) \;\Rightarrow\; g_\alpha(\chi^{-1}) = g_\alpha(\overline{\chi}) = \chi(-1)\overline{g_\alpha(\chi)}.$$

3. Using item 1.

$$\overline{g_\alpha(\chi)} = \chi(\alpha)\overline{g(\chi)} \quad \text{and} \quad g_\alpha(\chi) = \chi(\alpha^{-1})g(\chi)$$

thus

$$|g_\alpha(\chi)|^2 = \chi(\alpha)\chi(\alpha^{-1})\overline{g(\chi)}g(\chi) = |g(\chi)|^2.$$

If we sum over all $\alpha \in \mathbb{F}_q$ we get

$$\sum_{\alpha\in\mathbb{F}_q} |g_\alpha(\chi)|^2 = (q-1)|g(\chi)|^2.$$

On the other hand

$$g_\alpha(\chi)\overline{g_\alpha(\chi)} = (\sum_{x\in\mathbb{F}_q} \chi(x)\psi(\alpha x))(\sum_{y\in\mathbb{F}_q} \overline{\chi(x)}\psi(-\alpha y)) = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(\alpha(x-y)).$$

Again, summing over all $\alpha \in \mathbb{F}_q$ and using theorem 1.2.3 we obtain

$$\sum_{\alpha\in\mathbb{F}_q} |g_\alpha(\chi)|^2 = \sum_{\alpha\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(\alpha(x-y))$$

$$= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} q\delta(x,y)\chi(x)\overline{\chi(y)} = \sum_{x\in\mathbb{F}_q} \chi(x)\overline{\chi(x)}q = \sum_{x\in\mathbb{F}_q^*} q = q(q-1).$$

Combining both results we conclude that

$$(q-1)|g(\chi)|^2 = q(q-1) \;\Rightarrow\; |g(\chi)|^2 = q \;\Rightarrow\; |g_\alpha(\chi)| = |g(\chi)| = q^{1/2}.$$

4. From item 2. we get

$$g_\alpha(\chi)g_\alpha(\chi^{-1}) = \chi(-1)|g_\alpha(\chi)|^2 = \chi(-1)q.$$

□

## 1.3 Jacobi Sums

To introduce Jacobi Sums, we give a motivation about how these sums are necessary when we are counting the number of solution of equations of the form $x^n + y^n = 1$ in $\mathbb{F}_q$ (even for more general polynomial equations with coefficients in a finite field.) First we are going to analyze the case for $n = 2$ and $n = 3$ in the fields $\mathbb{F}_p$ and $\mathbb{F}_q$, respectively.

Since $\mathbb{F}_p$ is finite, the equation $x^2+y^2=1$ has only finitely many solutions, say $N(x^2+y^2=1)$. Observe that

$$N(x^2+y^2=1)=\sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_p}} N(x^2=a)N(y^2=b).$$

As consequence of example 1.1.12, we get that

$$N(x^2+y^2=1)=p+\sum_a\left(\frac{a}{p}\right)+\sum_b\left(\frac{b}{p}\right)+\sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

In the sums, we omit that $a,b\in\mathbb{F}_p$. By theorem 1.1.4, we have that $N(x^2+y^2=1)=p+\sum_{a+b=1}(\frac{a}{p})(\frac{b}{p})$. This is the best result we can obtain for the moment.

To evaluate the number of solution of $x^3+y^3=1$ in $\mathbb{F}_q$, we reason in the same way

$$N(x^3+y^3=1)=\sum_{a+b=1}N(x^3=a)N(y^3=b),$$

but in this case we analize two cases. If $q\equiv 2(3)$, as consequence of Theorem 1.1.7, $N(x^3=a)=1$ for all $a$ due $(3,q-1)=1$. It follows that $N(x^3+y^3=1)=q$. Now assume $q\equiv 1(3)$. Let $\chi\neq\varepsilon$ be a character of order 3, so by Theorem 1.1.4, we have that $N(x^3=a)=1+\chi(a)+\chi^2(a)$. Thus

$$N(x^3+y^3=1)=\sum_{a+b=1}(\sum_{i=0}^{2}\chi^i(a))(\sum_{j=0}^{2}\chi^j(b))=\sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{a+b=1}\chi^i(a)\chi^j(b).$$

With the purpose of simplify the expression for number of solutions of the equations $x^2+y^2=1$ and $x^3+y^3=1$ we introduce the Jacobi Sums.

**Definition 1.3.1.** Let $\chi$ and $\lambda$ be characters of $\mathbb{F}_q$ and set $J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b)$. $J(\chi,\lambda)$ is called a Jacobi sum.

**Theorem 1.3.1.** Let $\chi$ and $\lambda$ be nontrivial characters. Then

1. $J(\varepsilon,\varepsilon)=q$.
2. $J(\varepsilon,\chi)=0$.
3. $J(\chi,\chi^{-1})=-\chi(-1)$.
4. If $\chi\lambda\neq\varepsilon$, then
$$J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$
Moreover $|J(\chi,\lambda)|=q^{1/2}$.

*Proof.* The proofs of 1. and 2. follow from the properties of Gauss sums and characters. The proof of 3. and 4. are in [BEW98, Theorem 2.1.1 and Theorem 2.1.3]. □

We now return to the analysis of $N(x^2+y^2=1)$. We need to compute the value of $\sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. By item 3. of Theorem 1.3.1, we obtain $J(\chi,\chi)=-\left(\frac{-1}{p}\right)=-(-1)^{(p-1)/2}$. Thus the number of solutions is $N(x^2+y^2=1)=p-1$ if $p\equiv 1(4)$ and $p+1$ if $p\equiv 3(4)$.

In the case of $N(x^3 + y^3 = 1)$, applying Theorem 1.3.1 leads to the result

$$N(x^3 + y^3 = 1) = q - \chi(-1) - \chi^2(-1) + J(\chi,\chi) + J(\chi^2,\chi^2).$$

Since $-1 = (-1)^3$, we have $\chi(-1) = \chi^3(-1) = 1$. Notice that $\chi^2 = \chi^{-1} = \overline{\chi}$. Then

$$N(x^3 + y^3 = 1) = q - 2 + J(\chi,\chi) + J(\overline{\chi},\overline{\chi}) = q - 2 + J(\chi,\chi) + \overline{J(\chi,\chi)}) = q - 2 + \mathrm{Re}J(\chi,\chi).$$

This result is not as nice as the result for $N(x^2 + y^2 = 1)$, however, we can bound the number of solutions:

$$|N(x^3 + y^3 = 1) - q + 2| = |\mathrm{Re}J(\chi,\chi)| = |J(\chi,\chi) + \overline{J(\chi,\chi)}| \leq |J(\chi,\chi)| + |J(\overline{\chi},\overline{\chi})| \leq 2q^{1/2}.$$

The estimate says that $N(x^3+y^3 = 1)$ is approximately equal to $q-2$ with an "error term" $2q^{1/2}$.

Now we will provide some interesting results where the Jacobi sum are involved. They will be usefull when we compute the zeta function for some curves.

**Theorem 1.3.2.** Let q be a power of a prime. If $q \equiv 1(4)$, then there exist integers $a$ and $b$ such that $a^2 + b^2 = q$. If $q \equiv 1(3)$, then there exist integers $a$ and $b$ such that $a^2 - ab + b^2 = q$.

*Proof.* If $q \equiv 1(4)$, there is a character $\chi$ of order 4. If $\lambda$ has order $q-1$, let $\chi = \lambda^{(q-1)/4}$. The values of $\chi$ are in the set $\{1,-1,i,-1\}$. Thus $J(\lambda,\lambda) = \sum_{s+t=1} \chi(s)\chi(t) \in \mathbb{Z}[i]$. It follows that $J(\chi,\chi) = a + bi$, where $a, b \in \mathbb{Z}$; thus $q = |J(\chi,\chi)|^2 = a^2 + b^2$ due to theorem 1.3.1.

If $q \equiv 1(3)$, there is a character $\chi$ of order 3. The values of $\chi$ are in the set $\{1,\omega,\omega^2\}$, where $\omega = e^{2\pi i/3}$. Thus $J(\chi,\chi) \in \mathbb{Z}[\omega]$. As above, we have $J(\chi,\chi) = a + b\omega$ where $a, b \in \mathbb{Z}$, and $q = |J(\chi,\chi)|^2 = |a + b\omega|^2 = a^2 - ab + b^2$. □

**Remark 1.3.3.** For $q = p$, the fact that primes $p \equiv 1(4)$ can be written as the sum of two squares was discovered by Fermat. If $a, b > 0$, $a$ is odd and $b$ is even, then the representation $p = a^2 + b^2$ is unique.

**Theorem 1.3.4.** If $q \equiv 1(3)$, then there are integers $A$ and $B$ such that $4q = A^2 + 27B^2$. In this representation of $4q$, $A$ and $B$ are uniquely determined up to sign.

*Proof.* There exist integers $a, b$ such that $q = a^2-ab+b^2$. Notice $4q = (2a-b)^2+3b^2 = (2b-a)^2+3a^2 = (a + b)^2 + 3(a - b)^2$. We claim that 3 divides either $a, b$, or $a - b$. Suppose that $3 \nmid a$ and $3 \nmid |b$. Assume that $a \equiv 1(3)$ and $b \equiv 2(3)$, then

$$q = a^2 - ab + b^2 = (3m + 1)^2 - (3m + 1)(3l + 2) + (3l + 2)^2 = 3B \text{ for some } B \in \mathbb{Z}$$

which its a contradiction, so the claim is true and $4q = A^2 + 27B^2$. The proof of uniqueness is omitted. □

**Theorem 1.3.5.** Suppose that $q \equiv 1(n)$ and that $\chi$ is a character of order $n$. Then

$$g(\chi)^n = \chi(-1)qJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2}).$$

*Proof.* Using part 4. of theorem 1.3.1 we have $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$. Multiply both sides by $g(\chi)$ we get $g(\chi)^3 = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$. In this way, we arrive at

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\chi^{n-1}).$$

Multiplying both side by $g(\chi)$, it gives us

$$g^n(\chi) = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\chi^{n-1})g(\chi)$$

$$= J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\chi^{-1})g(\chi) = \chi(-1)qJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2}),$$

since $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = -\chi(-1)q$. □

**Corolary 1.3.1.** If $\chi$ is a cubic character, then

$$g(\chi)^3 = qJ(\chi\chi).$$

*Proof.* Take $n = 3$ in the latter theorem. □

**Theorem 1.3.6.** Suppose that $q \equiv 1\,(3)$ and that $\chi$ is a cubic character. Set $J(\chi,\chi) = a + b\omega$. Then

1. $b \equiv 0\,(3)$.
2. $a \equiv -1\,(3)$.

*Proof.* We shall work with congruences in the ring of integers.

$$g(\chi)^3 = (\sum_t \chi(t)\psi(t))^3 \equiv \sum_t \chi(t)^3\psi(3t)\ (3),$$

and

$$\overline{g(\chi)}^3 = g(\overline{\chi})^3 = (\sum_t \overline{\chi}(t)\psi(t))^3 \equiv \sum_t \overline{\chi}(t)^3\psi(3t)\ (3).$$

Since $\chi(0) = \overline{\chi}(0) = 0$ and $\chi(t)^3 = \overline{\chi}(t)^3 = 1$ for $t \neq 0$ we have

$$\sum_t \chi(t)^3\psi(3t) = \sum_{t\neq 0} \psi(3t) = -1$$

and

$$\sum_t \overline{\chi(t)}^3\psi(3t) = \sum_{t\neq 0} \psi(3t) = \sum_{s\neq 0} \psi(s) = -1$$

by theorem 1.2.2.

Set $q = 3k + 1$ for some $k \in \mathbb{Z}$. Thus

$$g(\chi)^3 = qJ(\chi,\chi) = q(a + b\omega) = (3k + 1)(a + b\omega) \equiv a + b\omega \equiv -1\ (3),$$

and

$$\overline{g(\chi)}^3 = g(\overline{\chi})^3 = q\overline{J(\chi,\chi)} = q(a + b\overline{\omega}) = (3k + 1)(a + b\overline{\omega}) \equiv a + b\overline{\omega} \equiv -1\ (3),$$

Subtracting yields

$$b(\omega - \overline{\omega}) \equiv 0\,(3) \ \Rightarrow\ b\sqrt{-3} \equiv 0\,(3).$$

Thus $-3b2 \equiv 0\,(9)$ and it follows that

$$-3b^2 = 9k \ \Rightarrow\ -b^2 = 3k \ \Rightarrow\ 3|b^2 \ \Rightarrow\ 3|b \text{ since 3 is prime.}$$

Now the congruence $a + b\omega \equiv -1\,(3)$ is equivalent to $a \equiv -1\,(3)$. □

The theorem 1.3.2 guarantees us the existence of the $A$ and $B$, but the next two statements show us a method for computing the values $A$ and $B$.

**Corolary 1.3.2.** Assume all the hypothesis of Theorem 1.3.6. Let $A = 2a - b$ and $B = b/3$. Then $A \equiv 1\,(3)$ and

$$4q = A^2 + 27B^2.$$

*Proof.* Since $J(\chi,\chi) = a + b\omega$ and $|J(\chi,\chi)|^2 = q$ we have $q = a^2 - ab + b^2$. Thus $4q = (2a)^2 - 2(2a)b + 4b^2 = (2a)^2 - 2(2a)b + b^2 + 3b^2 = (2a - b)^2 + 3b^2$ and $4q = A^2 + 27B^2$. By theorem 1.3.6, $3|b$ and $a \equiv -1\,(3)$. Therefore $b \equiv 0\,(3)$ and $2a \equiv -2 \equiv 1\,(3)$, so $A = 2a - b \equiv 1\,(3)$ as we required. □

**Theorem 1.3.7.** Suppose that $q \equiv 1(3)$. Then there are integers $A$ and $B$ such that $4q = A^2 + 27B^2$. If we require that $A \equiv 1(3)$, $A$ is uniquely determined, and

$$N(x^3 + y^3 = 1) = q - 2 + A.$$

*Proof.* We have already shown that $N(x^3 + y^3 = 1) = q - 2 + 2\mathrm{Re}J(\chi,\chi)$. Since $J(\chi,\chi) = a + b\omega$ as above, we have $2\mathrm{Re}J(\chi,\chi) = (2a - b) = A \equiv 1(3)$. We omit the proof of uniqueness. □

**Remark 1.3.8.** From the proof we can obtain that $J(\chi,\chi) + J(\overline{\chi},\overline{\chi}) = A$. The latter theorem was due Gauss.

With the definitions and theorems that we have presented so far, we will try to get the number of solutions of the polynomial $x^n + y^n = 1$ in $\mathbb{F}_q$, or, if it is not possible, try to obtain an explicit bound for $N(x^n + y^n = 1)$.

We will assume that $q \equiv 1\,(n)$. We have that

$$N(x^n + y^n = 1) = \sum_{a+b=1} N(x^n = a)N(x^n = b).$$

Let $\chi$ be a character of order $n$. By Theorem 1.1.10,

$$N(x^n = a) = \sum_{i=0}^{n-1} \chi^i(a).$$

Combining these results yields

$$N(x^n + y^n = 1) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} J(\chi^i\chi^j).$$

Set $I = \{0, 1 \ldots, n-1\}$, then

$$N(x^n + y^n = 1) = \sum_{(i,j)\in I^2} J(\chi^i\chi^j).$$

Theorem 1.3.1 can be used to estimate this sum. We find the next results:

- If $i = j = 0$ we have $J(\chi^0,\chi^0) = J(\varepsilon,\varepsilon) = q$. We just consider $(0,0)$, 1 element of $I^2$.
- If $i + j = n$, then $\chi^i = (\chi^j)^{-1}$ and $J(\chi^j,\chi^i) = -\chi^j(-1)$, j varies from 1 to $n-1$. We take $n-1$ elements of $I^2$. Hence $\sum_{j=1}^{n-1} J(\chi^j,\chi^{n-j}) = -\sum_{j=1}^{n-1} \chi^j(-1)$. Consider the sum $\sum_{j=0}^{n-1} \chi^j(-1)$, it has the value $n$ if $-1$ is an nth power, and by Corollary 1.1.1, the sum has value 0. Thus $\sum_{j=1}^{n-1} J(\chi^j,\chi^{n-j}) = 1 - \delta_n(-1)n$ where $\delta_n(-1)$ is 1 when $-1$ is an nth power and 0 otherwise.

- If $i = 0$ and $j \neq 0$ or $i \neq 0$ and $j = 0$, then $J(\chi^i, \chi^j) = 0$. In each case we consider $n-1$ elements.

Finally

$$N(x^n + y^n = 1) = p + 1 - \delta_n(-1)n + \sum_{i,j} J(\chi^i, \chi^j).$$

The sum is over indices $i$ and $j$ between 1 and $n-1$ subject to the condition that $i + j \neq n$. Subtracting the elements of the three cases analyzed before, we found that there are $(n-1)^2 - (n-1) = (n-1)(n-2)$ indices and they all have absolute value $q^{1/2}$ due to item 4. of Theorem 1.3.1. Thus

$$|N(x^2 + y^n = 1) + \delta_n(-1)n - (p+1)| \leq (n-1)(n-2)q^{1/2}.$$

Now we want to go further and try to apply the analysis we just made for the general case

$$a_2 x_1^{l_1} + a_2 x_2^{l_2} + \ldots + a_r x_r^{l_r} = b,$$

where $a_1, a_2, \ldots, a_r, b \in \mathbb{F}_q^*$. Before that, we need to generalize the notion of Jacobi Sums for more than 2 characters, and present some of its properties.

**Definition 1.3.2.** Let $\chi_1, \chi_2, \ldots, \chi_l$ be characters of $\mathbb{F}_q$. A Jacobi sum is defined by the formula

$$J(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1 + \ldots + t_l = 1} \chi_1(t_1)\chi_2(t_2)\ldots, \chi_l(t_l).$$

There is another sum that is closely related to Jacobi sums

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1 + \ldots + t_l = 0} \chi_1(t_1)\chi_2(t_2)\ldots, \chi_l(t_l).$$

The properties of the Jacobi sums of two characters shown in Theorem 1.3.1 hold for a finite number of characters.

**Theorem 1.3.9.** 1. $J_0(\varepsilon, \varepsilon, \ldots, \varepsilon) = J(\varepsilon, \varepsilon, \ldots, \varepsilon) = q^{l-1}$.

2. If some but not all of the $\chi_i$ are trivial. Then $J_0(\chi_1, \chi_2, \ldots, \chi_l) = J(\chi_1, \chi_2, \ldots, \chi_l) = 0$.

3. Assume that $\chi_l \neq \varepsilon$. Then

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \begin{cases} 0 & \text{, if } \chi_1\chi_2\ldots\chi_l \neq \varepsilon \\ \chi_l(-1)(q-1)J(\chi_1, \chi_2, \ldots, \chi_{l-1}) & \text{, otherwise} \end{cases}$$

*Proof.* The proof of the theorem can be found in [BEW98, Theorem 10.1.1 and Theorem 10.1.2]. □

The generalization of Theorem 1.3.1 is the next result:

**Theorem 1.3.10.** Assume that $\chi_1, \chi_2, \ldots, \chi_r$ are nontrivial and also that $\chi_1\chi_2\ldots\chi_r$ is nontrivial. Then

$$g(\chi_1)g(\chi_2)\ldots g(\chi_r) = J(\chi_1, \chi_2, \ldots, \chi_r)g(\chi_1\chi_2\ldots\chi_r).$$

*Proof.* The theorem is proved in [IR90, Chapter 8 Theorem 3]. □

**Corolary 1.3.3.** Suppose that $\chi_1, \chi_2, \ldots, \chi_r$ are nontrivial and that $\chi_1\chi_2\ldots\chi_r$ is trivial. Then

$$g(\chi_1)g(\chi_2)\ldots g(\chi_r) = \chi_r(-1)qJ(\chi_1, \chi_2, \ldots, \chi_{r-1}).$$

*Proof.* By theorem 1.3.10

$$g(\chi_1)g(\chi_2)\dots g(\chi_{r-1}) = J(\chi_1,\chi_2,\dots,\chi_{r-1})g(\chi_1\chi_2\dots\chi_{r-1}).$$

Now, multiplying both sides by $g(\chi_r)$

$$g(\chi_1)g(\chi_2)\dots g(\chi_{r-1})g(\chi_r) = J(\chi_1,\chi_2,\dots,\chi_{r-1})g(\chi_1\chi_2\dots\chi_{r-1})g(\chi_r),$$

since $\chi_1\dots,\chi_{r-1} = \chi_r^{-1}$

$$g(\chi_1)g(\chi_2)\dots g(\chi_r) = J(\chi_1,\chi_2,\dots,\chi_{r-1})g(\chi_r^{-1})g(\chi_r) = \chi_r(-1)qJ(\chi_1,\chi_2,\dots,\chi_{r-1}).$$

□

**Corolary 1.3.4.** Let the hypotheses be as in Corollary 1.3.3. Then

$$J(\chi_1,\dots,\chi_r) = -\chi_r(-1)J(\chi_1,\chi_2,\dots,\chi_{r-1}).$$

If $r = 2$, we set $J(\chi_1) = 1$.

*Proof.* The proof can be read in [IR90, Chapter 8 Corollary 2]. □

**Theorem 1.3.11.** Assume that $\chi_1,\chi_2,\dots,\chi_r$ are nontrivial.

1. If $\chi_1\chi_2\dots,\chi_r \neq \varepsilon$, then
$$|J(\chi_1,\chi_2,\dots,\chi_r)| = q^{(r-1)/2}.$$
2. If $\chi_1\chi_2\dots,\chi_r = \varepsilon$, then
$$|J_0(\chi_1,\chi_2,\dots,\chi_r)| = (q-1)q^{(r/2)-1}$$
and
$$|J(\chi_1,\chi_2,\dots,\chi_r)| = q^{(r/2)-1}.$$

*Proof.* 1. From theorem 1.3.10 and theorem 1.2.4

$$|g(\chi_1)g(\chi_2)\dots g(\chi_r)| = |J(\chi_1,\chi_2,\dots,\chi_r)||g(\chi_1\chi_2\dots\chi_r)|.$$

$$q^{r/2} = |g(\chi_1)|g(\chi_2)|\dots|g(\chi_r)| = |J(\chi_1,\chi_2,\dots,\chi_r)||g(\chi_1\chi_2\dots\chi_r)| = q^{1/2}|J(\chi_1,\chi_2,\dots,\chi_r)|$$

Thus $|J(\chi_1,\chi_2,\dots,\chi_r)| = q^{(r-1)/2}$.

2. From theorem 1.3.9 and corollary 1.3.4 we obtain that

$$|J(\chi_1,\chi_2,\dots,\chi_r)| = |-\chi_r(-1)J(\chi_1,\chi_2,\dots,\chi_{r-1})| = |J(\chi_1,\chi_2,\dots,\chi_{r-1})| = q^{(r-2)/2} = q^{(r/2)-1},$$

since $\chi_r^{-1} = \chi_1\dots,\chi_{r-1} \neq \varepsilon$ and we apply item 1.

$$|J_0(\chi_1,\chi_2,\dots,\chi_l)| = |\chi_l(-1)(q-1)J(\chi_1,\chi_2,\dots,\chi_{l-1})| = (q-1)|J(\chi_1,\chi_2,\dots,\chi_{l-1})| = (q-1)q^{(r/2)-1}.$$

□

It's time we consider the number of solution for the most general equation

$$a_2x_1^{l_1} + a_2x_2^{l_2} + \ldots + a_rx_r^{l_r} = b,$$

where $a_1, a_2, \ldots, a_r, b \in \mathbb{F}_q^*$. Let $N$ be the number of solutions. Again, we use the methods that provided us $N(x^n + y^n = 1)$.

To begin with, we have

$$N = \sum N(x_1^{l_1} = u_1)(x_2^{l_2} = u_2)\ldots(x_r^{l_r} = u_r) \tag{1.1}$$

where the sum is over all $r$-tuples $(u_1, u_2, \ldots, u_r)$ such that $\sum_{i=1}^{r} a_iu_i = b$.

We shall assume that $l_1, l_2, \ldots, l_r$ are divisors of $q-1$, although this condition is not necessary. We explain this reason later. Then $l_i = (l_i, q-1)$ for all $i \in \{1, \ldots, r\}$. Let $\chi_i$ vary over the characters of order $l_i$. Then

$$N(x_i^{l_i} = u_i) = \sum_{\chi_i} \chi_i(u_i).$$

Now, substituting into equation 1.1 we obtain

$$N = \sum_{\chi_1,\chi_2,\ldots,\chi_r} \sum_{\sum a_iu_i=b} \chi_1(u_1)\chi_2(u_2)\ldots\chi_r(u_r).$$

The inner sum is closely related to the Jacobi sums we have presented so far. In order to obtain the explicit formula of the Jacobi sum and the sum $J_0$, we need to perform a change of variable depending if $b = 0$ or not.

If $b = 0$, let $t_i = a_iu_i$. Then the inner sum becomes

$$\sum_{\sum a_iu_i=b} \chi_1(u_1)\chi_2(u_2)\ldots\chi_r(u_r) = \sum_{\sum t_i=0} \chi_1(a_1^{-1}t_1)\chi_2(a_2^{-1}t_2)\ldots\chi_r(a_r^{-1}t_r)$$

$$= \chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1}) \sum_{\sum t_i=0} \chi_1(t_1)\chi_2(t_2)\ldots\chi_r(t_r) = \chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1})J_0(\chi_1,\chi_2,\ldots,\chi_r).$$

If $b \neq 0$, let $t_i = b^{-1}a_iu_i$ and by a similar computation to the case $b = 0$ the inner sum becomes

$$\sum_{\sum a_iu_i=b} \chi_1(u_1)\chi_2(u_2)\ldots\chi_r(u_r) = \chi_1\chi_2\ldots\chi_r(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1})J(\chi_1,\chi_2,\ldots,\chi_r).$$

Using Theorem 1.3.9 we obtain that in both cases, if $\chi_1 = \chi_2 = \ldots = \chi_r = \varepsilon$ the term has the value $q^{r-1}$. If some but not all the $\chi_i$ are equal to $\varepsilon$, then the term has the value zero. In the first case, the value is zero unless $\chi_1\chi_2\ldots\chi_r = \varepsilon$.

In summary, we conclude the following

**Theorem 1.3.12.** If $b = 0$, then

$$N = q^{r-1} + \sum \chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1})J_0(\chi_1,\chi_2,\ldots,\chi_r).$$

The sum is over all $r$-tuples of characters $\chi_1,\chi_2,\ldots,\chi_r$, where $\chi_i^{l_i} = \varepsilon$, $\chi_i \neq \varepsilon$ for $i = 1, \ldots, r$, and $\chi_1\chi_2\ldots\chi_r = \varepsilon$. If $M$ is the number of such $r$-tuples, then

$$|N - q^{r-1}| \leq M(q-1)q^{(r/2)-1}.$$

If $b \neq 0$, then

$$N = q^{r-1} + \sum \chi_1\chi_2 \dots \chi_r(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1}) \dots \chi_r(a_r^{-1})J(\chi_1, \chi_2, \dots, \chi_r).$$

The summation is over all $r$-tuples of characters $\chi_1, \chi_2, \dots, \chi_r$, where $\chi_i^{l_i} = \varepsilon$, $\chi_i \neq \varepsilon$ for $i = 1, \dots, r$. If $M_0$ is the number of such $r$- tuples with $\chi_1\chi_2 \dots \chi_r = \varepsilon$, and $M_1$ is the number of such $r$-tuples with $\chi_1\chi_2 \dots \chi_r \neq \varepsilon$, then

$$|N - q^{r-1}| \leq M_0 q^{(r/2)-1} + M_1 q^{(r-1)/2}.$$

*Proof.* To bound the number of solutions, we use theorem 1.3.11 □

**Corolary 1.3.5.** If $d_i = (l_i, q-1)$, then $\sum_{i=1}^{r} a_i x^{l_i} = b$ and $\sum_{i=1}^{r} a_i x^{d_i} = b$ have the same number of solutions.

*Proof.* The reason follows from Theorem 1.1.11. □

This corollary explains why we can assume that $l_i = (l_i, q-1)$ when we derive the theorem 1.3.12.

The next theorem is a consequence of theorem 1.3.12, and is written in terms of algebraic geometric notions, it counts the number of solutions of a hypersurface associated to a homogeneous equation.

**Theorem 1.3.13.** Let $\mathbb{F}_q$ a finite field such that $q \equiv 1(m)$. The homogeneous equation $a_0x_0^m + a_1x_1^m + \dots a_nx_n^m = 0$, $a_0, a_1, \dots, a_n \in \mathbb{F}_q^*$, defines a hypersurface in $\mathbb{P}^n(\mathbb{F}_q)$. The numbers of points on this hypersurface is given by

$$q^{n-1} + q^{n-2} + \dots + q + 1 + \frac{1}{q-1} \sum_{\chi_0, \chi_1, \dots, \chi_n} \chi_0(a_0^{-1}) \dots \chi_n(a_n^{-1})J_0(\chi_0, \chi_1, \dots, \chi_n),$$

where $\chi_i^m = \varepsilon$, $\chi_i \neq \varepsilon$, and $\chi_0\chi_1 \dots \chi_n = \varepsilon$. Moreover, under these conditions

$$\frac{1}{q-1} J_0(\chi_0, \chi_1, \dots, \chi_n) = \frac{1}{q} g(\chi_0)g(\chi_1) \dots g(\chi_n).$$

*Proof.* By theorem 1.3.12 we have

$$N_{\mathbb{A}} = q^n + \sum \chi_0(a_0^{-1}) \dots \chi_n(a_n^{-1})J_0(\chi_0, \chi_1, \dots, \chi_n)$$

solution in $\mathbb{A}^{n+1}(\mathbb{F}_q)$. Hence, the number of points in $\mathbb{P}^n(\mathbb{F}_q)$ is given by

$$N = \frac{N_{\mathbb{A}} - 1}{q-1} = q^{n-1} + q^{n-2} + \dots + q + 1 + \frac{1}{q-1} \sum_{\chi_0, \chi_1, \dots, \chi_n} \chi_0(a_0^{-1}) \dots \chi_n(a_n^{-1})J_0(\chi_0, \chi_1, \dots, \chi_n)$$

By theorem 1.3.10 and corollary 1.3.3 we obtain

$$J(\chi_1, \chi_2, \dots, \chi_n) = \frac{g(\chi_0)g(\chi_1)g(\chi_2) \dots g(\chi_n)}{g(\chi_0)g(\chi_1\chi_2 \dots \chi_n)} = \frac{\chi_0(-1)qJ(\chi_1, \dots, \chi_n)}{g(\chi_0)g(\chi_1\chi_2 \dots \chi_n)}$$
$$\Rightarrow \; g(\chi_0)g(\chi_1\chi_2 \dots \chi_n) = \chi_0(-1)q.$$

Substituting in the result of theorem 1.3.9 gives us

$$\frac{1}{q-1} J_0(\chi_0, \chi_1, \chi_2, \dots, \chi_n) = \chi_0(-1) \frac{g(\chi_0)g(\chi_1)g(\chi_2) \dots g(\chi_n)}{g(\chi_0)g(\chi_1\chi_2 \dots \chi_n)}$$
$$\Rightarrow \; \frac{1}{q-1} J_0(\chi_0, \chi_1, \chi_2, \dots, \chi_n) = \frac{1}{q} g(\chi_0)g(\chi_1)g(\chi_2) \dots g(\chi_n).$$

□

## 1.4 Restrictions and Lifts of Characters

Let $F$ be a finite field with $q$ elements and $E$ a field containing $F$ with $q^s$ elements.

Now we define the generalization of the trace for arbitrary finite fields and introduce the notion of norm that will lead to lifted characters . In fact it is possible to generalize both ideas for arbitrary finite fields extension.

**Definition 1.4.1.** If $\alpha \in E$, the trace of $\alpha$ from $E$ to $F$ is given by

$$\mathrm{tr}_{E/F}(\alpha) = \sum_{j=0}^{s-1} \alpha^{q^j}.$$

If q = p, then the definition of the trace reduces to definition 1.2.1.

Some properties of the trace are the following:

**Theorem 1.4.1.** If $\alpha, \beta \in E$ and $a \in F$, then

1. $\mathrm{tr}_{E/F}(\alpha) \in F$.
2. $\mathrm{tr}_{E/F}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$.
3. $\mathrm{tr}(a\alpha) = a\mathrm{tr}(\alpha)$.
4. $\mathrm{tr}_{E/F}$ maps $E$ onto $F$.
5. $\mathrm{tr}_{E/F}(\alpha) = \mathrm{tr}_{K/F}(\mathrm{tr}_{E/K}(\alpha))$, where $K$ is an intermediate field between $F$ and $E$.

*Proof.* The proof of 1. to 4. is exactly analogous to that of Theorem 1.2.1. The proof of item 5. can be consulted in [IR90, Theorem 11.2.3]. More properties related to the trace are stated in [BEW98, Theorem 11.4.6]. □

**Definition 1.4.2.** The norm of $\alpha$ from $E$ to $F$ is given by

$$\mathrm{N}_{E/F}(\alpha) = \prod_{j=0}^{s-1} \alpha^{q^j}.$$

The most useful properties of the norm are:

**Theorem 1.4.2.** If $\alpha, \beta \in E$ and $a \in F$, then

1. $\mathrm{N}_{E/F}(\alpha) \in F$.
2. $\mathrm{N}_{E/F}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.
3. $\mathrm{N}(a\alpha) = a^s\mathrm{N}(\alpha)$.
4. $\mathrm{N}_{E/F}$ maps $E$ onto $F$.
5. $\mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{K/F}(\mathrm{N}_{E/K}(\alpha))$, where $K$ is an intermediate field between $F$ and $E$.

*Proof.* The proof of the properties can be read in [IR90, Theorem 11.2.2]. Additional properties of the norm can be obtained in [BEW98, Theorem 11.4.3]. □

**Definition 1.4.3.** If a character $\chi$ on a finite field $E$ is restricted to a subfield $F$, it defines a character on that subfield which we denote by $\chi\big|_F$ or $\chi^*$ if it is known the field where it is defined.

**Definition 1.4.4.** Let $\chi$ be a character $F$. The lift $\chi'$ of the character $\chi$ from F to the extension $E$ is given by

$$\chi'(\alpha) = \chi(N_{E/F}(\alpha)) \qquad \alpha \in E.$$

The lifted characters provide us a powerful tool that allow us to compute the number of solution of equations of any extension $E$ of the field $F$ using the characters of the small one. The next theorem provides some properties of lifted characters that will help us later.

**Theorem 1.4.3.** Let $\chi$ be a character on $F$ and let $\chi'$ denote the lift of $\chi$ from $F$ to $E$. For a character $\lambda$ on $E$, let $\lambda^*$ denote the restriction of $\lambda$ to $F$. Then

1. $\chi'$ is a character on $E$.
2. $(\chi')^* = \chi^s$ and $(\lambda^*)' = \lambda^d$, where $d = (q^s - 1)/(q - 1)$.
3. A character $\lambda$ on $E$ equals to the lift $\chi'$ for some character $\chi$ on $F$ if and only if the order of $\lambda$ divides $(q - 1)$
4. If $\chi_1' = \chi_2'$, then $\chi_1 = \chi_2$.
5. $\chi'$ and $\chi$ have the same order.
6. $(\chi_1\chi_2)' = \chi_1'\chi_2'$.

*Proof.* The proof of these properties are in [BEW98, Theorem 11.4.4]. □

**Definition 1.4.5.** Let $\chi$ be a charecter of $F$ and let $\chi'$ be the lift of $\chi$ from $F$ to $E$. Then the lift of the Gauss sum

$$g(\chi) = \sum_{t \in F} \chi(t)\psi(t)$$

from $F$ to $E$ is

$$g(\chi') = \sum_{t \in E} \chi'(t)\psi(t)$$

The next theorem is the most important theorem related to the lift of a character. It is a direct relation between the Gauss sum of $\chi$ with the Gauss sum of $\chi'$

**Theorem 1.4.4** (Hasse-Davenport Relation). For a nontrivial character $\chi$ on $F$, the Gauss sum of $\chi$ and the Gauss sum of $\chi'$ are related by

$$(-1)^{s-1} g(\chi)^s = g(\chi')$$

*Proof.* The proof is long enough to skip it, even though it is profoundly interesting, please refer to [IR90, Chapter 8 Section 4] and [BEW98, Theorem 11.5.2] to consult it. Even Weil proved it in [Wei49]. □

**Corolary 1.4.1.** Let $\chi_1, \chi_2, \ldots, \chi_n$ and $\chi_1\chi_2 \ldots \chi_n$ be nontrivial character on $F$. Then.

$$J(\chi_1', \chi_2', \ldots, \chi_n') = (-1)^{(s-1)(n-1)} J(\chi_1, \chi_2, \ldots, \chi_n)^s$$

*Proof.* From theorem 1.3.10 we have

$$g(\chi_1)g(\chi_2)\dots g(\chi_n) = J(\chi_1,\chi_2,\dots,\chi_n)g(\chi_1\chi_2\dots\chi_n) \Rightarrow$$

$$g(\chi_1)^s g(\chi_2)^s \dots g(\chi_n)^s = J(\chi_1,\chi_2,\dots,\chi_n)^s g(\chi_1\chi_2\dots\chi_n)^s.$$

Applying Hasse Devenport we obtain

$$(-1)^{(s-1)n} g(\chi_1')g(\chi_2')\dots g(\chi_n') = (-1)^{s-1} J(\chi_1,\chi_2,\dots,\chi_n)^s g((\chi_1\chi_2\dots\chi_n)') \Rightarrow$$

$$(-1)^{(s-1)(n-1)} J(\chi_1,\chi_2,\dots,\chi_n)^s = \frac{g(\chi_1')g(\chi_2')\dots g(\chi_n')}{\chi_1'\chi_2'\dots\chi_n'} = J(\chi_1',\chi_2',\dots,\chi_n').$$

□

# Chapter 2

# First steps to understand the Zeta Function

The second purpose of this work is to introduce the Zeta Function for a finite field, this function led to the Weil conjectures. We want to understand the function and its properties. Before that, we need to introduce some notions of algebraic geometry, commutative algebra, and algebraic number theory. It is expected that the reader grasps basic notions of algebraic geometry. We omit the proof of most of the theorems.

## 2.1 Dedekind Domians & The Ideal Class Group

**Definition 2.1.1.** Let $A = \mathbb{Z}$ be the ring of integers. Let $K = \mathbb{Q}$ be the field of rational numbers. A field extension $L/\mathbb{Q}$ of finite degree is called a number field.

**Example 2.1.1.** $\mathbb{Q}(\sqrt{d})$ is a number field of degree 2 over $\mathbb{Q}$ if $d$ is not a square in $\mathbb{Q}$.

**Definition 2.1.2.** Let $A$ be a subring of a ring $L$. An element $\alpha \in L$ is said to be integral over $A$ if it is the root of a monic polynomial $f(x)$ in $A[x]$. If $A = \mathbb{Z}$, $\alpha$ is called algebraic integer in $L$. Let $C$ be a ring that contains $A$. The ring $C$ is said to be integral over $A$, or to be a integral extension of $A$, if every element of $C$ is integral over $A$.

**Theorem 2.1.2.** Let $A$ be a subring of the field $L$. The set $B$ consisting of all the elements of $L$ that are integral over $A$ is a ring.

*Proof.* The theorem is proved in [Lor96][Chapter I, Corollary 2.11]. □

**Definition 2.1.3.** The ring of Theorem 2.1.2 is called the integral closure $B$ of $A$ in $L$. It is denoted by $O_L$. When $L$ is a number field, the integral closure $B$ of $\mathbb{Z}$ in $L$ is called the ring of integers of $L$.

A domain $A$ is said to be integrally closed if it is equal to its integral closure in its field of fractions.

**Example 2.1.3.** The rings $\mathbb{Z}$ and $k[x]$ are integrally closed. More generally, any factorial domain is integrally closed. [Lor96] provide some reason that justify this example.

Now, we define what a Dedekind domain is and give a characterization.

**Definition 2.1.4.** Let $R$ be an integral domain. The ring $R$ is called a Dedekind domain if it has the following three properties

1. $R$ is noetherian.
2. $R$ has dimension 1.
3. $R$ is integrally closed (in its field of fractions).

**Theorem 2.1.4.** Let $A$ be a Dedekind domain. Let $L/K$ be a finite separable extension of the field of fractions $K$ of $A$. Then the integral closure $B$ of $A$ in $L$ is a Dedekind domain.

*Proof.* [Lor96] proves that $B$ is a Dedekind domain. □

To state a characterization for Dedekind domains, we need to introduce the notion of factorization of ideal into prime ideals that resembles the idea of factorization of integers into prime numbers.

**Definition 2.1.5.** An integral domain $R$ is said to have the property of unique factorization of ideals if every nontrivial ideal $I \subseteq R$ can be written as $I = \mathfrak{P}_1 \dots \mathfrak{P}_s$, where $\mathfrak{P}_i$ is a prime ideal of $R$ for $i = 1, \dots, s$ , and its factorization is essentially unique, i.e., whenever $I = \mathfrak{Q}_1 \dots \mathfrak{Q}_n$, then $n = s$ and $\mathfrak{P}_i = \mathfrak{Q}_j$ for some permutation.

**Theorem 2.1.5.** Let $R$ be a noetherian domain of dimension 1. The ring is a Dedekind domian if and only if $R$ has the property of unique factorization of ideals.

*Proof.* This characterization is proved in [Lor96][Chapter III, Theorem 2.8] □

**Remark 2.1.6.** Every prime ideal in a Dedekind domain $R$ is a maximal ideal. The reason is (0) is a prime ideal and for any prime $\mathfrak{p}$ we have $(0) \subset \mathfrak{p}$. Since $R$ has dimension 1, then $\mathfrak{p}$ must be maximal.

The idea behind the ideal class group is to measure how far the ring $A$ is to be a principal ideal domain. [Lor96] gives us a historic review of how this theory developed. This theory was invented by Krummer in the case of cyclotomic ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ in the mid-nineteenth century, while he worked on Fermat's Last Theorem. Krummer's fundamental theorem states that Fermat's Last Theorem is true for the exponent $p$ provided that the order of the ideal class group of the ring $\mathbb{Z}[\exp 2\pi i/p]$ is not divisible by $p$.

**Definition 2.1.6.** Let $A$ be any commutative domain. The set $\mathcal{M}(A)$ consisting of all the nonzero ideals of $A$ is commutative monoid when endowed with the composition law of multiplication of

1. Given $I, J \in \mathcal{M}(A)$, $IJ \in \mathcal{M}(A)$.
2. The unit ideal $(1) = A$ is an identity element for the multiplication of ideals

**Theorem 2.1.7.** Let $A$ be any commutative domain. Consider the following relation on the monoid $\mathcal{M}(A)$:

$$I \sim J \text{ if and only if there exist } \alpha, \beta \in A - \{0\} \text{ such that } (\alpha)I = (\beta)J.$$

This relation is an equivalence relation. Set $\mathrm{Cl}(A) = \mathcal{M}(A)/\sim$. If $A$ is a Dedekind domain, then $\mathrm{Cl}(A)$ is an abelian group under the product of ideals

$$\mathcal{M}(A) \times \mathcal{M}(A) \to \mathcal{M}(A)$$

$$(\text{class of } I, \text{class of } J) \mapsto \text{class of } IJ$$

The group $\mathrm{Cl}(A)$ is called the ideal class group of $A$.

*Proof.* Let's prove that $\sim$ is an equivalence relation.

1. Take $I \in \mathcal{M}(A)$, notice $(1)I = (1)I$ and $I \sim I$.
2. Suppose $I \sim J$, there exist $\alpha, \beta \in A - \{0\}$ s.t $(\alpha)I = (\beta)J$, that is, $J \sim I$.
3. Suppose $I \sim J$, and $J \sim K$, there exist $\alpha, \beta, \gamma, \lambda \in A - \{0\}$ s.t $(\alpha)I = (\beta)J$, and $(\gamma)J = (\lambda)K$. Then $(\alpha\gamma)I = (\beta\lambda)K$, that is, $I \sim K$.

Hence $\sim$ is an equivalence relation.

Suppose $I \sim I^*$ and $J \sim J^*$, that is, $(\alpha)I = (\alpha^*)I^*$, and $(\beta)J = (\beta^*)J^*$, where $\alpha, \alpha^*, \beta, \beta^* \in A - \{0\}$. Since $A$ is commutative, we have

$$(\alpha\beta)IJ = (\alpha)(\beta)IJ = (\alpha)I(\beta)J = (\alpha^*)I^*(\beta^*)J^* = (\alpha^*)(\beta^*)I^*J^* = (\alpha^*\beta^*)I^*J^*.$$

$\alpha\beta, \alpha^*\beta^* \in A - \{0\}$ since $A$ is an integral domain, so $IJ \sim I^*J^*$. Hence, the product is well defined. Let $I, J, K \in Cl(A)$, we need to see that $I(JK) = (IJ)K$. Since the product of ideals is associative we have $I(JK) =$ class of $I(JK) =$ class of $(IJ)K$, so the product in $Cl(A)$ is associative.
The identity is $(1) = A$, so $Cl(A)$ is a monoid, it doesn't matter if $A$ is a Dedekind domain or not. Let $\alpha \in I$, $\alpha \neq 0$. Since the nontrivial ideals of $A$ have a unique factorization into a product of maximal ideals, we can write that $(\alpha) = IJ$ for some ideal $J$ in $\mathcal{M}(A)$, i.e. $(\alpha)A = (1)IJ$, so $IJ \sim (1)$ and $J$ is the inverse of $I$. We conclude $Cl(A)$ is a group.

□

**Lemma 2.1.1.** Let $A$ be a commutative domain. Then $\mathrm{Cl}(A) = \{(1)\}$ if and only if $A$ is a principal ideal domain.

*Proof.* Suppose that $\mathrm{Cl}(A) = \{(1)\}$. Let $I \in \mathcal{M}(A)$. Then there exist $a, b \in A$ such that $(a)I = (b)$. In particular, $b = ac$, for some $c \in I$. We want to see that $(c) = I$. We have already known that $(c) \subseteq I$. Let $x \in I$, then $ax = bd$ for some $d \in A$. Hence, $a(x - cd) = 0$. Since $A$ is a domain, we obtain that $x = cd \in (c)$.

Suppose that $A$ is a principal ideal domain, consider $I = (a)$ and $J = (b)$ with $a, b \in A$. Then $(a)(b) = (b)(a)$, so $I \sim J$ and $\mathrm{Cl}(A) = \{(1)\}$. □

[Lor96] proves that $\mathrm{Cl}(A)$ is a finite group when $A = \mathbb{Z}$, and $A$ is the integral closure of $k[x]$ in a finite extension of $k(x)$, with $k$ a finite field. However, we omit the reasons.

We start with the definition of finite quotients and its norm that will help us letter to obtain the Zeta function.

**Definition 2.1.7.** We say that a Dedekind domain $A$ has finite quotients if, for any $P \in \mathrm{Max}(A) :=$ {the set of maximal ideals of $A$}, the residue field $A/P$ is a finite field.

**Definition 2.1.8.** Let $A$ be a Dedekind domain with finite quotients. We define the norm of a non-zero ideal $I$ to be

$$\|I\|_A := \text{cardinality of } A/I.$$

**Remark 2.1.8.** $\|I\|_A = 1$ if and only if $I = A$.

**Example 2.1.9.** The ring $A = \mathbb{Z}$ has finite quotients since the maximal ideals are the ideals generated by a prime number, and $\mathbb{Z}/p\mathbb{Z}$ is a finite field. Because $\mathbb{Z}$ is a principal ideal domain, let $I = (a)$ be any non-zero ideal. Then

$$\|I\|_A := |\mathbb{Z}/a\mathbb{Z}| = |a|$$

Moreover, for any real number $\lambda$, there exist only finitely many ideals $I$ in $\mathbb{Z}$ with $\|I\|_{\mathbb{Z}} \leq \lambda$.

In this example, the norm is an integer. This behavior holds for any Dedekind domain.

**Lemma 2.1.2.** Let $A$ be a Dedekind domain. Let $P \in \mathrm{Max}(A)$. Then, for all $n \in \mathbb{N}$, the $A-$module $P^{n-1}/P^n$ is isomorphic to the $A-$module $A/P$. In particular, if the set $A/P$ is finite, then the set $A/P^r$ is also finite, and $|A/P^r| = |A/P|^r$.

*Proof.* We need this lemma to prove that $\|I\|_A$ is an integer. The proof is in [Lor96][Chapter V, Lemma 3.4.] □

**Theorem 2.1.10.** Let $A$ be a Dedekind domain with finite quotients. The norm of any nonzero ideal of $A$ is an integer, and the map $|\cdot|_A : \mathcal{M}(A) \to \mathbb{N}$ is multiplicative.

*Proof.* Let $P \in \mathrm{Max}(A)$. By Lemma 2.1.2 we have that $|A/P^r| = |A/P|^r$. If $I := P_1^{a_1} \dots P_r^{a_r}$ is any non-zero ideal of $A$, then the isomorphism

$$A/I \cong A/P_1^{a_1} \times \ldots \times A/P_r^{a_r}$$

shows that $\|I\|_A := \prod_{i=1}^r \|P_i\|_A^{a_i}$. □

The next theorem establish that the integrally closure of a Dedekind domain with finite quotient inherits these properties.

**Theorem 2.1.11.** Let $A$ be a Dedekind domain with finite quotients. Let $K$ be its field of fraction. Let $L/K$ be a finite extension. Assume that the integral closure $B$ of $A$ in $L$ is a finitely generated $A$-module. Then $B$ is a Dedekind domain with finite quotients.

*Proof.* [Lor96][Chapter V, Proposition 3.6] □

Assume that $A$ denotes either the ring $\mathbb{Z}$ or the ring $k[x]$, with $k$ a finite field. $L$ denotes a finite extension of degree $n$ of the field of fraction $K$ of $A$, and we let $B$ be the integral closure of $A$ in $L$.

**Theorem 2.1.12.** Assume $B$ is a finitely generated $A$-module. Fix a number $\lambda \in \mathbb{R}$. There exist only finitely many ideals $I$ of $B$ with $\|I\|_B \leq \lambda$.

*Proof.* The theorem is proved in [Lor96][Chapter V, Lemma 3.7] □

## 2.2 Valuations, Nonsingular Complete Curves & Divisors.

Before introducing the concepts of nonsingular complete curve which is a generalization of a nonsingular curve, we need to define what a valuation is.

**Definition 2.2.1.** Let $L$ be any field. A valuation of $L$ is a map $v : L^* \to \mathbb{Z}$ such that the following properties are satisfied:

1. $v(xy) = v(x) + v(y)$ for all $x, y \in L^*$, i.e., $v$ is a group homomorphism.

2. $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in L^*$.

We extend $v$ to $L$ by setting $v(0) = +\infty$.

**Remark 2.2.1.** Let $\Gamma$ be any totally ordered abelian group (e.g. $\Gamma = (\mathbb{R}, +, \geq)$). A map $v : L^* \to \Gamma$ satisfying the axioms of valuation is also called a valuation of $L$. When the study of valuation with target groups $\Gamma$ different from $(\mathbb{Z}, +)$ is required, the valuation defined on definition 2.2.1 is called discrete valuation of $L^*$.

It is possible to associate an absolute value throughout $e^{-v(x)}$. For more detail, look at [Lor96][Chapter V, Lemma 6.6]

**Example 2.2.2.** Let $v : L^* \to \mathbb{Z}$ be a valuation. Let $n \in \mathbb{N}$. The map $nv : L^* \to \mathbb{Z}$, which sends $x$ to $nv(x)$, is also a valuation of $L$. Similarly, for each $s \in \mathbb{R}_{>0}$, the map $sv : L^* \to \mathbb{R}$ is a valuation of $L$.

**Example 2.2.3.** Let $v : L^* \to 0 \subset \mathbb{Z}$. Clearly, $v$ is a valuation. It is called the trivial valuation.

**Example 2.2.4** ($p$-adic valuation of $\mathbb{Q}$.). Let $p$ be a prime number. We define a valuation $v_p : \mathbb{Q}^* \to \mathbb{Z}$ as follows. Let $x \in \mathbb{Q}^*$. We can factor $x$ as $\prod_{p \text{ prime}} p^{\text{ord}_p(x)}$, where $\text{ord}_p(x)$ is defined as follows: Let $z \in \mathbb{Z}$, $\text{ord}_p(z)$ is the highest power of $p$ which divides $z$. If $p \nmid |z$, then $\text{ord}_p(z) = 0$ For a rational number $x = \frac{a}{b} \in \mathbb{Q}^*$, $\text{ord}_p(x)$ is defined by

$$\text{ord}_p(\frac{a}{b}) = \text{ord}_p(a) - \text{ord}_p(b).$$

Set $v_p(x) := \text{ord}_p(x)$. The map $v_p$ is a valuation.
To see it, consider $x, y \in \mathbb{Q}^*$, where $x = \prod_{p \text{ prime}} p^{\text{ord}_p(x)}$ and $y = \prod_{p \text{ prime}} p^{\text{ord}_p(y)}$. The product $xy$ can be represented as $\prod_{p \text{ prime}} p^{\text{ord}_p(xy)}$, however $xy = \left(\prod_{p \text{ prime}} p^{\text{ord}_p(x)}\right)\left(\prod_{p \text{ prime}} p^{\text{ord}_p(y)}\right) = \prod_{p \text{ prime}} p^{\text{ord}_p(x)+\text{ord}_p(y)}$.
Hence $v_p(xy) = \text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y) = v_p(x) + v_p(y)$.
Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$, where $\gcd(a, b) = 1$ and $\gcd(c, d) = 1$. Let $p$ be any fixed prime number. We will prove that $v_p(x + y) \geq \min(v_p(x), v_p(y))$ in three cases.

1. Suppose $p^{\text{ord}_p(a)}|a$ and $p^{\text{ord}_p(c)}|c$, then $a = p^{\text{ord}_p(a)}m$ and $c = p^{\text{ord}_p(c)}n$. Assume $\text{ord}_p(a) \geq \text{ord}_p(c)$.

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{p^{\text{ord}_p(a)}md + p^{\text{ord}_p(c)}nb}{bd} = \frac{p^{\text{ord}_p(c)}(p^{\text{ord}_p(a)-\text{ord}_p(c)}md + nb)}{bd}.$$

   Let $z = p^{\text{ord}_p(a)-\text{ord}_p(c)}md + nb$, notice $\text{ord}_p(z) \geq 0$, so $x + y = \frac{p^{\text{ord}_p(c)+\text{ord}_p(z)}k}{bd}$, for some $k \in \mathbb{Z}$, and $v_p(x + y) = \text{ord}_p(x + y) = \text{ord}_p(c) + \text{ord}_p(z) \geq \text{ord}_p(c) = \min\{\text{ord}_p(a), \text{ord}_p(c)\} = \min\{\text{ord}_p(x), \text{ord}_p(y)\}$.

2. Suppose $p^{\text{ord}_p(a)}|a$ and $p^{\text{ord}_p(d)}|d$, then $a = p^{\text{ord}_p(a)}m$ and $d = p^{\text{ord}_p(d)}n$. Evidently $\text{ord}_p(a) \geq -\text{ord}_p(d)$.

$$x+y = \frac{a}{b}+\frac{c}{d} = \frac{p^{ord_p(a)}m}{b}+\frac{c}{p^{ord_p(d)}n} = p^{-ord_p(d)}(\frac{p^{ord_p(a)+ord_p(d)}m}{b}+\frac{c}{n}) = p^{-ord_p(d)}(\frac{p^{ord_p(a)+ord_p(d)}mn + cb}{bn}).$$

Let $z = p^{\mathrm{ord}_p(a)+\mathrm{ord}_p(d)}mn + cb$, notice $\mathrm{ord}_p(z) \geq 0$, so $x + y = \frac{p^{-\mathrm{ord}_p(d)+\mathrm{ord}_p(z)}k}{bn}$, for some $k \in \mathbb{Z}$, and $v_p(x + y) = \mathrm{ord}_p(x + y) = -\mathrm{ord}_p(d) + \mathrm{ord}_p(z) \geq -\mathrm{ord}_p(d) = \min\{\mathrm{ord}_p(a), -\mathrm{ord}_p(d)\} = \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$

3. Suppose $p^{\mathrm{ord}_p(b)}|b$ and $p^{\mathrm{ord}_p(d)}|d$, then $b = p^{\mathrm{ord}_p(b)}m$ and $d = p^{\mathrm{ord}_p(d)}n$. Notice $\mathrm{ord}_p(x) = -\mathrm{ord}_p(b)$ and $\mathrm{ord}_p(y) = -\mathrm{ord}_p(d)$ . Assume $-\mathrm{ord}_p(b) \geq -\mathrm{ord}_p(d)$, that is, $\mathrm{ord}_p(d) \geq \mathrm{ord}_p(b)$.

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{ap^{ord_p(d)}n + cp^{ord_p(b)}m}{p^{ord_p(b)+ord_p(d)}nm} = \frac{p^{ord_p(b)}(p^{ord_p(d)-ord_p(b)}an + cm)}{p^{ord_p(b)+ord_p(d)}nm} =$$

$$p^{-ord_p(d)}(\frac{p^{ord_p(d)-ord_p(b)}an + cm}{nm}).$$

Let $z = p^{\mathrm{ord}_p(d)-\mathrm{ord}_p(b)}an + cm$, notice $\mathrm{ord}_p(z) \geq 0$, so $x + y = \frac{p^{-\mathrm{ord}_p(d)+\mathrm{ord}_p(z)}k}{bn}$, for some $k \in \mathbb{Z}$, and $v_p(x + y) = \mathrm{ord}_p(x + y) = -\mathrm{ord}_p(d) + \mathrm{ord}_p(z) \geq -\mathrm{ord}_p(d) = \min\{-\mathrm{ord}_p(b), -\mathrm{ord}_p(d)\} = \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$.

In conclusion $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in \mathbb{Q}^*$.

This valuation is called the $p$-adic valuation of $\mathbb{Q}$. The $p$-adic absolute value $|\cdot|_p$ of $\mathbb{Q}$ attached to $v_p$ is defined as

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$$
$$x \mapsto |x|_p := p^{-v_p(x)}, \text{ if } x \neq 0$$

and $|0|_p = 0$. Note that in order for an integer $x$ to have a small absolute value $|x|_p$, it must be divisible by a large power of $p$.

**Example 2.2.5** ($P$-adic valuations). Let $A$ be a Dedekind domain, and let $K$ denote its field of fractions. Let $P \subset A$ be a maximal ideal. We associate to $P$ a surjective valuation $v_P : K^* \to \mathbb{Z}$ as follows. If $x \in A$, then write the factorization of the ideal $(x)$ in $A$ as

$$(x) := \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(x)},$$

where $\mathrm{ord}_P(x)$ is defined in analogy with $\mathbb{Z}$. Define $v_P(x) := \mathrm{ord}(x)$. If $x = a/b \in K$, with $a, b \in A$, the set

$$v_P(x) := v_P(a) - v_P(b).$$

$v_p$ is a valuation of $K$. Unlike the p-adic valuation of $\mathbb{Q}$, we omit the proof that $v_P$ is a valuation. When $A$ has finite quotients, we define the standardized absolute value $|\cdot|_P$ associated to $v_P$ as follows:

$$|\cdot|_P : K \to \mathbb{R}_{\geq 0}$$
$$x \mapsto |x|_P := |A/P|^{-v_P(x)}, \text{ if} x \neq 0,$$

and $|0|_P = 0$.

From a valuation, we can obtain a local ring as follows:

**Theorem 2.2.6.** Let $K$ be any field. Consider the valuation $v : K^* \to \mathbb{Z}$. Define

$$\mathcal{O}_v := \{\alpha \in K^* : v(\alpha) \geq 0\} \sqcup \{0\}, \qquad \text{and} \qquad \mathcal{M}_v := \{\alpha \in K^* : v(\alpha) > 0\} \sqcup \{0\}.$$

The set $\mathcal{O}_v$ is a ring, and the set $\mathcal{M}_v$ is a proper ideal. An element of $\mathcal{O}_v$ is invertible in $\mathcal{O}_v$ if and only if $v(\alpha) = 0$. Moreover $\mathcal{O}_v$ is a local ring with maximal ideal $\mathcal{M}_v$.

*Proof.* The proof follows from the definition of a valuation. To prove $\mathcal{O}_v$ is a ring, let $\alpha, \beta \in \mathcal{O}_v$, that is, $v(\alpha) \geq 0$, and $v(\beta) \geq 0$. If one of them is zero, say $\alpha$, then $v(\alpha + \beta) \geq 0$ and $\alpha + \beta \in \mathcal{O}_v$. Assume neither is zero, so $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\} \geq 0$, then $\alpha + \beta \in \mathcal{O}_v$. Observe that $v(\beta^2) = v((-\beta)(-\beta)) = 2v(-\beta) \geq 0$, then $v(-\beta) \geq 0$ and $-\beta \in \mathcal{O}_v$. The product is closed in $\mathcal{O}_v$ since $v(\alpha\beta) = v(\alpha) + v(\beta) \geq 0$. $\mathcal{O}_v$ has unit because $v(1) = v(1 \cdot 1) = 2v(1) \Rightarrow v(1) = 0$ and $1 \in \mathcal{O}_v$. Hence $\mathcal{O}_v$ is a ring with unit. For $\alpha, \beta \in \mathcal{M}_v$ by the same arguments we have $\alpha - \beta \in \mathcal{M}_v$. Take $\gamma \in \mathcal{O}_v$, and $\alpha \in \mathcal{M}_v$, then $v(\gamma\alpha) = v(\gamma) + v(\alpha) > 0$. We conclude $\mathcal{M}_v$ is an ideal of $\mathcal{O}_v$. Notice $1 \notin \mathcal{M}_v$ due $v(1) = 0$, so $\mathcal{M}_v$ is a proper ideal.
Let $\alpha \in \mathcal{O}_v$ a unit, there exists $\beta \in \mathcal{O}_v$ s.t $0 = v(1) = v(\alpha\beta) = v(\alpha) + v(\beta)$, therefore $v(\alpha) = 0$, and $\alpha \notin \mathcal{M}_v$, i.e. $M_v$ is the set of non-units, and $\mathcal{O}_v$ is a local ring with maximal ideal $\mathcal{M}_v$. If $v(\alpha) = 0$, then $\alpha$ is a unit. □

**Remark 2.2.7.** Let $k_v := \mathcal{O}_v/\mathcal{M}_v$ denote the residue field.

**Theorem 2.2.8.** Let $K$ be any field. Let $v : K^* \to \mathbb{Z}$ be a non-trivial valuation. Then $\mathcal{O}_v$ is a local principal ideal domain. The map $v$ is uniquely determined by the value $v(t)$, where $t$ is a generator of $\mathcal{M}_v$. The map $v \mapsto \mathcal{O}_v$, from the set of surjective valuations of $K$ to the set of local principal ideal domains contained in $K$ and with field of fractions $K$, is a bijection.

*Proof.* This theorem is proved in [Lor96][Chapter V, Proposition 9.1]. □

**Definition 2.2.2.** For A non-trivial discrete valuation $v : K^* \to \mathbb{Z}$, the ring $\mathcal{O}_v$ is called a discrete valuation ring.

**Definition 2.2.3.** Let $k$ be any field. Let $L/k$ be any field extension. We say that a valuation $v : L^* \to \mathbb{Z}$ is trivial on $k$ if $v(k^*) = \{0\}$. Let $\mathcal{V}(L/k)$ denote the set of surjective valuations $v : L^* \to \mathbb{Z}$ trivial on $k$.

**Definition 2.2.4.** Let $k$ be any field. A field $L$ containing $k$ is called a field of transcendece degree $n$ over $k$ if there exist $x_1, \ldots, x_n$ in $L$ such that $L$ is a finite extension of $k(x_1, \ldots, x_n)$, and such that $k(x_1, \ldots, x_n)$ is isomorphic, as $k-$algebra, to the field of rational fractions in $n$ variables over $k$.

We have the necessary concepts to introduce the nonsingular complete curves.

**Definition 2.2.5.** Let $k$ be any field. A nonsingular complete curve $X/k$ over $k$ is a pair $(X, k(X)/k)$ consisting in a field $k(X)/k$ of transcendence degree 1 over $k$, and a set $X$ identified with the set $\mathcal{V}(k(X)/k)$ through a given bijection between $X$ and $\mathcal{V}(k(X)/k)$. An element $P$ of $X$ is called a point. The field $k(X)$ is called the field of rational functions on $X$. To each point corresponds a valuation $v_p$ of $\mathcal{V}(k(X)/k)$, and a local principal ideal domain $\mathcal{O}_P := \mathcal{O}_{v_P}$, with maximal ideal $\mathcal{M}_P$. The ring $\mathcal{O}_P$ is called the ring of rational function defined at $P$. An element of $\mathcal{O}_P$ is called a function on $X$ defined at $P$. A function $\alpha \in \mathcal{O}_P$ is said to vanish at $P$, or to have a zero at $P$, if $\alpha \in \mathcal{M}_P$. The integer $v_P(\alpha)$ is called the order of vanishing of $\alpha$ at $P$, sometimes, we denote it by $\mathrm{ord}_P(\alpha)$. A function $\alpha \in k(X) \backslash \mathcal{O}_P$ is said to have a pole of $\alpha$ at $P$. The domain of $\alpha \in k(X)$ is the set of points in $X$ where $\alpha$ is defined. If $U \subseteq X$, then we let $\mathcal{O}_X(U) := \cap_{P \in U} \mathcal{O}_P$, and we call this the ring of functions on $X$ defined everywhere on $U$. We assume $\mathcal{O}_X(X) = k$. We endow $X$ with the Zariski topology, where a set $C$ is closed if and only if $C$ is either empty, $X$, or a finite set of points.

**Definition 2.2.6.** An open set $U$ of $X$ is called affine if the ring $\mathcal{O}_X(U)$ is a finitely generated $k$-algebra and a Dedekind domain, and if the map $U \to \mathrm{Max}(\mathcal{O}_X(U))$, with $P \mapsto \mathcal{M}_P \cap \mathcal{O}_X(U)$, is well defined and bijective.

In other words, the open set $U$ is an affine open set if it is in bijection, as above, with the nonsingular affine curve $(\mathrm{Max}(\mathcal{O}_X(U)), \mathcal{O}_X(U))$.

**Remark 2.2.9.** Any field $L/k$ of transcendence degree 1 over $k$ defines a nonsingular complete curve $X/k$, namely, $(\mathcal{V}(L/k), L/k)$.

**Definition 2.2.7.** Let $X/k$ and $Y/k$ be two nonsingular complete curves over $k$. A (nonconstant) morphism $\varphi : X \to Y$ of nonsingular complete curves over $k$ is a map given by a homomorphism of $k$-algebras $\varphi^* : k(Y) \to k(X)$ in the following way: if $P \in X$ corresponds to the valuation $v_P$, then $\varphi(P)$ correspond in $Y$ to the unique surjective valuation attached to the valuation $v_P \circ \varphi$.

**Theorem 2.2.10.** Let $X_F(\bar{k})$ be a nonsingular curve in $\mathbb{P}^2(\bar{k})$. Let $P \in X_F(\bar{k})$. The ring $\mathcal{O}_P \subseteq \bar{k}(X_F)$ is a local principal ideal domain. Let $\pi \in \mathcal{O}_P$ be a generator of the maximal ideal $\mathcal{M}_P$ of $\mathcal{O}_P$. The map $v_P : \bar{k}(X_F)^* \to \mathbb{Z}$, with $z \mapsto v_P(z) = \mathrm{ord}_\pi(z)$, is a surjective valuation such that $\mathcal{O}_{v_P} = \mathcal{O}_P$.

Let $F \in k[x_0, x_1, x_2]$ be a homogeneous polynomial. Assume that the plane projective curve $X_F(\bar{k})$ is nonsingular. Then the map

$$X_F(\bar{k}) \to \mathcal{V}(\bar{k}(X_F)/\bar{k})$$

$$P \mapsto v_P$$

is bijective.

**Remark 2.2.11.** As consequence, $X_F(\bar{k})$ is a nonsingular complete curve.

**Definition 2.2.8.** Let $k$ be any field. A field $L$ containing $k$ is called a function field over $k$ if the field $L$ is a field of transcendence degree 1 over $k$, and $k$ is algebraically closed in $L$.

**Definition 2.2.9.** Let $\mathbb{F}_q$ be a finite field with $q$ elements. Let $X/\mathbb{F}_q$ be a nonsingular complete curve. Let $\mathbb{F}_q(X)$ denote the function field of $X$, and fix an algebraic closure $\overline{\mathbb{F}_q(X)}$ of $\mathbb{F}_q(X)$. Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be any algebraic extension of $\mathbb{F}_q$ contained in $\overline{\mathbb{F}_q(X)}$. Let $\mathbb{F}_{q^n}(X) := \mathbb{F}_{q^n} \cdot \mathbb{F}_q(X) =$ subfield of $\overline{\mathbb{F}_q(X)}$ generated by $\mathbb{F}_{q^n}$ and $\mathbb{F}_q(X)$. Let $X_{\mathbb{F}_{q^n}}/\mathbb{F}_{q^n}$ denote the nonsingular complete curve associated to the function field $\mathbb{F}_{q^n}(X)/\mathbb{F}_{q^n}$. The curve $X_{\mathbb{F}_{q^n}}/\mathbb{F}_{q^n}$ is said to be obtained from $X/\mathbb{F}_q$ by a constant field extension or by extension of the scalars, or by base change. The extension $\mathbb{F}_{q^n}(X)/\mathbb{F}_q(X)$ is called a constant field extension.

**Remark 2.2.12.** This definition works for any perfect field.

When we are dealing with affine or projective curves in a finite field $\mathbb{F}_q$, where $q$ is a power of a prime $p$, these sets have finite elements. For any affine variety, notice $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$, so every algebraic set has at least $q^n$ elements. For the projective case observe that $\mathbb{A}^{n+1}(\mathbb{F}_q) - \{(0, 0, \ldots, 0)\}$ has $q^{n+1} - 1$ elements. Since $\mathbb{F}_q^*$ has $q - 1$ elements each equivalence class has $q - 1$ elements. Thus $\mathbb{P}^n(\mathbb{F}_q)$ has $(q^{n+1} - 1)/(q - 1) = q^n + q^{n-1} + q^{n-2} + \ldots + q + 1$ elements, and every algebraic set has at most this number of elements. The same occurs if we work over nonsingular complete curves curves.

**Theorem 2.2.13.** Let $X/\mathbb{F}_q$ be a nonsingular complete curve. Then for all $n \in \mathbb{N}$, the set $X(\mathbb{F}_q)$ is finite.

*Proof.* The statement is verified in [Lor96][Chapter 7, Lemma 6.18]. □

In the previous chapter, we obtain a formula to compute the number of points in an affine, and projective hypersurface defined over $\mathbb{F}_q$ using characters, Gauss, and Jacobi sums, and by the Hasse-Davenport relation, we extend it to $\mathbb{F}_{q^n}$. Now, we derive other method to determine the number of points in any affine, projective, and complete curves using algebraic tools. Firstly, we state the affine case.

**Theorem 2.2.14.** Fix an algebraic closure $\overline{\mathbb{F}}_q$ of the field $\mathbb{F}_q$. Denote by $\mathbb{F}_{q^n}$ the unique subfield of degree $n$ over $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[x,y]$ be an absolutely irreducible polynomial. Let $C_f := \mathbb{F}_q[x,y]/(f)$. Then the set $\{M \in \mathrm{Max}(C_f) : [C_f/M : \mathbb{F}_q] = d\}$ and the set $Z_f(\mathbb{F}_{q^n})$ are finite. Let $N_n := |Z_f(\mathbb{F}_{q^n})|$, and let $b_d := |\{M \in \mathrm{Max}(C_f) : [C_f/M : \mathbb{F}_q] = d\}|$. Then $N_n = \sum_{d|n} db_d$.

*Proof.* We have already proof that $N_n$ is finite. The rest of the prove can be consulted in [Lor96][Chapter 7, Proposition 3.5]. □

**Theorem 2.2.15.** The group $\mathrm{Gal}(\overline{k}/k)$ acts on $\mathbb{P}^2(\overline{k})$ as follows:

$$\mathrm{Gal}(\overline{k}/k) \times \mathbb{P}^2(\overline{k}) \to \mathbb{P}^2(\overline{k})$$

$$(\sigma, [x_0, x_1, x_2]) \mapsto \sigma \cdot [x_0, x_1, x_2] := [\sigma(x_0), \sigma(x_1), \sigma(x_2)].$$

*Proof.* First, we need to check that the map is well-defined. Let $\sigma \in \mathrm{Gal}(\overline{k}/k)$, and $[x_0, x_1, x_2] = [\lambda x, \lambda y, \lambda z] \in \mathbb{P}^2(\overline{k})$, where $\lambda \in k^*$. Then

$$\sigma \cdot [\lambda x_0, \lambda x_1, \lambda x_2] = [\sigma(\lambda x_0), \sigma(\lambda x_1), \sigma(\lambda x_2)]$$

$$= [\sigma(\lambda)\sigma(x_0), \sigma(\lambda)\sigma(x_1), \sigma(\lambda)\sigma(x_2)] = [\sigma(x_0), \sigma(x_1), \sigma(x_2)] = \sigma \cdot [x_0, x_1, x_2].$$

Let $id \in \mathrm{Gal}(\overline{k}/k)$, then

$$id \cdot [x_0, x_1, x_2] = [id(x_0), id(x_1), id(x_2)] = [x_0, x_1, x_2].$$

Take $\sigma, \tau \in \mathrm{Gal}(\overline{k}/k)$, then

$$\sigma \cdot (\tau \cdot [x_0, x_1, x_2]) = \sigma \cdot [\tau(x_0), \tau(x_1), \tau(x_2)] = [\sigma\tau(x_0), \sigma\tau(x_1), \sigma\tau(x_2)] = \sigma\tau \cdot [x_0, x_1, x_2].$$

In conclusion, the map defines an action.

□

**Remark 2.2.16.** Let $F \in k[x_0, x_1, x_2]$ be a homogeneous polynomial. Since $F$ has coefficients in $k$, the action of the group $\mathrm{Gal}(\overline{k}/k)$ induces, by restriction, an action on $X_F(\overline{k})$.

**Theorem 2.2.17.** Assume the hypothesis of theorem 2.2.14. Let $F \in \mathbb{F}_q[x_0, x_1, x_2]$ be a homogeneous polynomial such that $X_F(\overline{\mathbb{F}}_q)$ is a nonsingular projective curve. Let $b_d$ denote the number of orbits of length $d$ of $X_F(\overline{F}_q)$ under $\mathrm{Gal}(\overline{F}_q/\mathbb{F}_q)$. Then $N_n = \sum_{d|n} db_d$.

*Proof.* We omit the proof, if the reader want to consult it, refer to [Lor96][Chapter 7, Proposition 3.11]. □

**Definition 2.2.10.** Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. Let $Q \in X$, corresponding to a principal ideal domain $\mathcal{O}_Q$ in $k(X)$. The degree of $Q$, denoted by $\deg(Q)$, is the integer $[\mathcal{O}_Q/\mathcal{M}_Q : k]$.

**Theorem 2.2.18.** Let $X/\mathbb{F}_q$ be a nonsingular curve. Fix an algebraic closure $\overline{\mathbb{F}_q(X)}$ of $\mathbb{F}_q(X)$. Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$ in $\overline{\mathbb{F}_q(X)}$. Let $\mathbb{F}_{q^n}$ denote the unique subfield of $\overline{\mathbb{F}}_q$ of degree $n$ over $\mathbb{F}_q$. Let $N_n := |X(\mathbb{F}_{q^n})|$, and $b_d := \{Q \in X : \deg(Q) = d\}$. Then $N_n := \sum_{d|n} d b_d$.

*Proof.* This theorem is shown in [Lor96]. □

We want to associate to each nonsingular complete curve $X/k$ an abelian group called the Picard group. In [Lor96], they consider a more general case for a field $L$ containing the Dedekind domain $B$ whose field of fractions is $L$. This abelian group gives rise to a new description of the group $\mathrm{Cl}(B)$, however, we omit this case.

**Definition 2.2.11.** Let $L/k$ be any extension and $\mathcal{V}(L/k)$ defined in definition 2.2.3. When $\mathcal{V}(L/k) \neq \emptyset$, the free abelian group $\mathrm{Div}(L/k)$ generated by the set $\{x_v : v \in \mathcal{V}(L/k)\}$,

$$\mathrm{Div}(L/k) := \oplus_{v \in \mathcal{V}(L/k)} \mathbb{Z} x_v$$

is called the group divisors of $L/k$. An element $D$ in $\mathrm{Div}(L/k)$ is written as a sum $D = \sum a_v x_v$, with $a_v \in \mathbb{Z}$, and $a_v$ for all but finitely many $v \in \mathcal{V}(L/k)$. The element $D$ is called a divisor of $L$. If $a_v \geq 0$, for all $v \in \mathcal{V}(L/k)$, then $D$ is called an effective, or positive divisor. The set of effective divisor is denoted by $\mathrm{Eff}(L/k)$.

Consider the map

$$\begin{aligned} \mathrm{div}_L : L^* &\to \mathrm{Div}(L/k) \\ f &\mapsto \mathrm{div}_L(f) := \sum_{v \in \mathcal{V}(L/k)} v(f) x_v. \end{aligned}$$

The next proposition provide a reason why $\mathrm{div}_L$ is well defined.

**Theorem 2.2.19.** Let $k$ be any field. Let $L/k$ be a field of transcendence degree one over $k$. Let $\alpha \in L^*$. Then the set $\{v \in \mathcal{V}(L/k) : v(\alpha) \neq 0\}$ is a finite set.

*Proof.* The theorem is shown in [Lor96][Chapter VI, Proposition 4.11]. □

**Definition 2.2.12.** Let $L/k(x)$ be a finite extension. The Picard group $\mathrm{Pic}(L/k)$ is the quotient of the group $\mathrm{Div}(L/k)$ by the image of the map div.

**Theorem 2.2.20.** The following sequence of abelian groups is exact

$$(1) \to \bigcap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v^* \xrightarrow{i} L^* \xrightarrow{\mathrm{div}} \mathrm{Div}(L/k) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(L/k) \longrightarrow (0).$$

$i$ denotes the inclusion and cl the canonical projection.

*Proof.* The sequence is exact by the definition of the groups and the homomorphism. □

The previous definition holds for any function field $K(x)/k$, so we can extend these definitions to nonsingular complete curves as follows:

**Definition 2.2.13.** Let $k$ be any field. Let $k(X)/k$ be a function field, and let $X/k$ denote the associated nonsingular complete curve. To each point $P \in X$ is associated a local principal ideal domain $\mathcal{O}_P$ with valuation $v_P$. Let $\mathrm{Div}(X/k) := \oplus_{P\in X}\mathbb{Z}P$, and $\mathrm{div} : k(X)^* \to \mathrm{Div}(X/k)$, with $f \mapsto \sum_{P\in X} v_P(f)P$. Since we identify $X$ with $\mathcal{V}(k(X)/k)$, the group $\mathrm{Div}(X/k)$ can be identified with the group $\mathrm{Div}(k(X)/k)$ is such a way that the map div becomes identified with $\mathrm{div}_{k(X)}$. Let $\mathrm{Pic}(X/k)$ denote the quotient of $\mathrm{Div}(X/k)$ by the image of div.

**Theorem 2.2.21.** The following sequence of abelian groups is exact

$$(1) \longrightarrow k^* \longrightarrow k(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(X/k) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(X/k) \longrightarrow (0).$$

*Proof.* From the definition of nonsingular complete curve we have that $\bigcap_{v\in\mathcal{V}(L/k)} \mathcal{O}_v^* = k^*$, and by theorem 2.2.20 we have that the sequence is exact. □

**Example 2.2.22.** Let $F \in \bar{k}[x_0, x_1, x_2]$ be a homogeneous polynomial defining a nonsingular plane projective curve $X_F(\bar{k})$. Let $\bar{k}(X_F)/k$ denote the function field of $X_F(\bar{k})$. Let $X/\bar{k}$ denote the nonsingular complete curve associated to $\bar{k}(X_F)/k$. Upon identifying $X$ with the set $X_F(\bar{k})$, a divisor $D \in \mathrm{Div}(X/\bar{k})$ can be thought of as a finite set of points of $X_F(\bar{k})$ with multiplicities. A standard way to produce geometrically meaningful effective divisors on $X_F(\bar{k})$ is to intersect the curve $X_F(\bar{k})$ with other plane curves. Let $X_H(\bar{k})$ be any other plane curve that intersects $X_F(\bar{k})$ in finitely many points. For each point $P$ in $X_F(\bar{k}) \cap X_H(\bar{k})$, consider the intersection number $I_P(X_F, X_H)$. The positive integer $I_P(X_F, X_H)$ equals 1 if the given curves have distinct tangent lines at $P$, and is bigger than 1 otherwise. If $P \notin X_F(\bar{k}) \cap X_H(\bar{k})$, then set $I_P(X_F, X_H) = 0$. The divisor $\sum_{P\in X} I_P(X_F, X_H)P$ is called the intersection divisor of $X_F(\bar{k})$ and $X_H(\bar{k})$. If the reader is interested in the definititon of intersection number, consult [Ful89].

**Definition 2.2.14.** Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. The map

$$\deg : \mathrm{Div}(X/k) \to \mathbb{Z}$$

$$\deg(\sum_{P\in X} a_P P) = \sum_{P\in X} a_P \deg(P).$$

is called the degree map.

**Theorem 2.2.23.** Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. Then, for all $\alpha \in k(X)^*$, $\deg(\mathrm{div}(\alpha)) = 0$.

*Proof.* Refer to [Lor96][Chapter VII, Theorem 7.9] to consult the proof. □

**Theorem 2.2.24.** Let $X/k$ be a nonsingular complete curve. The map $\deg : \mathrm{Div}(X/k) \to \mathbb{Z}$ induces a nontrivial group homomorphism $\deg : \mathrm{Pic}(X/k) \to \mathbb{Z}$, with $\mathrm{cl}(D) \mapsto \deg(D)$.

*Proof.* The proof is included in [Lor96][Chapter VII, Corollary 7.10.] □

**Definition 2.2.15.** Let $\mathrm{Div}^0(X/k)$ denote the kernel of the map $\deg : \mathrm{Div}(X/k) \to \mathbb{Z}$. Let $\mathrm{Pic}^0(X/k)$ denote the kernel of the map $\deg : \mathrm{Pic}(X/k) \to \mathbb{Z}$.

**Theorem 2.2.25.**

$$\mathrm{Pic}^0(X/k) = \mathrm{Div}^0(X/k)/\mathrm{div}(k(X)^*).$$

*Proof.* Let $\mathcal{L} \in \mathrm{Pic}^0(X/k)$, there exists $D \in \mathrm{Div}(X/k)$ s.t. $\mathrm{cl}(D) = \mathcal{L}$, however, $\deg(D) = \deg(\mathcal{L}) = 0$ so $D \in \mathrm{Div}^0(X/k)$, and $\mathrm{cl}(D) \in \mathrm{Div}^0(X/k)/\mathrm{div}(K(X)^*)$. Let $\mathcal{L} \in \mathrm{Div}^0(X/k)/\mathrm{div}(K(X)^*) \subseteq \mathrm{Div}(X/k)/\mathrm{div}(K(X)^*) = \mathrm{Pic}^0(X/k)$. □

**Theorem 2.2.26.** The following sequence of abelian groups is exact

$$(1) \longrightarrow k^* \longrightarrow k(X)^* \longrightarrow \mathrm{Div}^0(X/k) \xrightarrow{\mathrm{cl}} \mathrm{Pic}^0(X/k) \longrightarrow (0).$$

*Proof.* This results follows by theorem 2.2.20 and theorem 2.2.27. □

**Theorem 2.2.27.** Let $k$ be a finite field. Let $X/k$ be a nonsingular complete curve. Then the group $\mathrm{Pic}^0(X/k)$ is finite.

*Proof.* The proof can be consulted in [Lor96][Chapter VII, Theorem 7.13]. It uses the Riemann-Roch theorem which we introduce in the next section. □

**Remark 2.2.28.** When $k$ is a finite field, the order of the group $\mathrm{Pic}^0(X/k)$ is called the class number of $X/k$, and is denoted by the letter $h$.

**Definition 2.2.16.** Let $d \in \mathbb{N}$. Set $\mathrm{Pic}^d(X/k) := \{\mathcal{L} \in \mathrm{Pic}(X/k) : \deg(\mathcal{L})) = d\}$. Set $\mathrm{Eff}^d(X/k) := \{D \in \mathrm{Eff}(X/k) : \deg(D) = d\}$.

The map deg is a group homomorphism, so $\deg(\mathrm{Pic}(X/k)) = e\mathbb{Z}$, where $e \in \mathbb{N}$. Later we see that $e = 1$. The proof of theorem 2.2.27 uses the following result:

**Theorem 2.2.29.** Let $d \in \mathbb{N} \cap \deg(\mathrm{Pic}(X/k))$. The set $\mathrm{Pic}^d(X/k)$ and $\mathrm{Pic}^0(X/k)$ are in bijection.

*Proof.* Every left coset of $\mathrm{Pic}^0(X/k)$ has the same cardinality. Let $\mathcal{L}$ be any element of $\mathrm{Pic}^d(X/k)$, then $\mathcal{L} + \mathrm{Pic}^0(X/k) \subseteq \mathrm{Pic}^d(X/k)$ since deg is a group homomorphism. On the other hand, pick $\mathcal{L}^* \in \mathrm{Pic}^d(X/k)$, then $\deg(\mathcal{L} - \mathcal{L}^*) = \deg(\mathcal{L}) - \deg(\mathcal{L}^*) = 0$, and $\mathcal{L}^* \in \mathcal{L} + \mathrm{Pic}^0(X/k)$. Hence $\mathrm{Pic}^d(X/k)$ is a left coset of $\mathrm{Pic}^0(X/k)$ in $\mathrm{Pic}(X/k)$. □

## 2.3 Riemann-Roch Theorem

The proof of the Weil conjectures uses an important result in Algebraic Geometry, Riemann-Roch theorem. In this section we provide the basic elements to state the theorem and some of its consequence that will be helpful later.

**Definition 2.3.1.** Let $X/k$ be any nonsingular complete curve. We denote by $O$ the identity element of $\mathrm{Div}(X)$. Consider the following partial ordering $\geq$ on the group $\mathrm{Div}(X)$:

$$D' \geq D \text{ if and only if } D' - D \text{ is a positive divisor.}$$

In particular, $D$ is a positive divisor if and only if $D \geq 0$.

By definition 2.2.13, to each function $\alpha \in k(X)^*$ is associated a divisor $\mathrm{div}(\alpha) \in \mathrm{Div}(X)$. We add another element, called $\mathrm{div}(0)$, to the set $\mathrm{Div}(X) \sqcup \{\mathrm{div}(0)\}$. This element satisfies that $\mathrm{div}(0) \geq D$ for all $D \in \mathrm{Div}(X)$. Let $D \in \mathrm{Div}(X)$, define $H^0(D) := \{\alpha \in k(X) : \mathrm{div}(\alpha) + D \geq 0\}$.

**Example 2.3.1.** Let $k$ be an algebraically closed field. Let $D = \sum_{i=1}^{s} a_i P_i \geq 0$ be an effective divisor. Then $H^0(D)$ is the set of all functions in $k(X)$ with poles of order at most $a_i$ at $P_i$ and no poles anywhere else. In particular, $H^0(D) \supset k$.

**Example 2.3.2.** Let $D \in \mathrm{Div}(X)$ be such that $\deg(D) < 0$. Then $H^0(D) = \{0\}$. If $\alpha \in k(X)^*$, then $\deg(\mathrm{div}(\alpha) + D) = 0 + \deg(D) < 0$. Therefore, $\mathrm{div}(\alpha) + D$ cannot be a positive divisor.

**Example 2.3.3.** Let $D = 0$. Then $H^0(D) = k$. By definition, the only functions in $k(X)$ with no poles are the constant functions. Similarly, if $\alpha \in k(X)^*$, then $H^0(\mathrm{div}(\alpha)) = k\alpha^{-1}$. Let $\alpha^{-1} \in H^0(\mathrm{div}(\alpha))$, and if $\beta \in H^0(\mathrm{div}(\alpha))$, $\beta \neq 0$, then $\mathrm{div}(\beta) + \mathrm{div}(\alpha) = \mathrm{div}(\beta\alpha) \geq 0$, that is, $\beta\alpha \in k$ and $\beta = \beta\alpha \cdot \alpha^{-1} \in k\alpha^{-1}$.

We are interested in $H^0(D)$ because it has a vector space structure. Moreover, it is a finite-dimensional vector space, but we see it later.

**Theorem 2.3.4.** $H^0(D)$ is a $k$-vector space.

*Proof.* By definition $\mathrm{div}(0) \geq -D$, then $0 \in H^0(D)$. Let $\alpha, \beta \in H^0(D)$ and $c \in k$. Then

$$\mathrm{div}(\alpha + \beta) = \sum_{P_v \in X} v(\alpha + \beta) P_v = \sum_{P_v \in X} \min(v(\alpha), v(\beta)) P_v.$$

Set $\sum_{P_v \in X} a_v P_v$. Notice $\min(v(\alpha), v(\beta)) + a_v \geq 0$, hence $\mathrm{div}(\alpha + \beta) + D \geq 0$, and $\alpha + \beta \in H^0(D)$.
Now,

$$\mathrm{div}(c\alpha) = \sum_{P \in X} v(c\alpha) P = \sum_{P \in X} (v(c) + v(\alpha)) P = \sum_{P \in X} v(\alpha) P,$$

since $v$ is trivial on $k$, we have $c\alpha \in H^0(D)$. In conclusion $H^0(D)$ is a vector space. □

To prove that $H^0(D)$ is finite-dimensional we try to find a bound.

**Definition 2.3.2.** Let $k$ be any field and $X/k$ be a nonsingular complete curve. Let $D \in \mathrm{Div}(X)$. For each $P \in X$, define

$$\mathcal{L}(D)_P := \{\alpha \in k(X) : \mathrm{ord}_P(\alpha) \geq -\mathrm{ord}_P(D)\}.$$

Consider the following map of $k$-vector spaces

$$\varphi_D : k(X) \to \oplus_{P \in X} (k(X)/\mathcal{L}(D)_P)$$

$$f \mapsto \oplus_{P \in X} (f \bmod \mathcal{L}(D)_P).$$

By definition, $\mathrm{Ker}(\varphi_D) = H^0(D)$. Let $H^1(D) := \mathrm{Coker}(\varphi_D)$.

**Remark 2.3.5.** Like $H^0(D)$, $H^1(D)$ is finite dimensional vector spaces, let $h^0(D)$ and $h^1(D)$ be their dimension, respectively. The reasons are provided in the remainder of the section.

**Definition 2.3.3.** Let $X/k$ be a nonsingular complete curve. The integer $h^1(0)$ is called the genus of $X$, and is denoted by $g = g(X)$.

**Theorem 2.3.6.** Let $D \in \mathrm{Div}(X)$ with $\deg(D) \geq 0$. Then $h^0(D) \leq \deg(D) + 1$. For all $D \in \mathrm{Div}(X)$, $H^0(D)$ is a finite-dimensional vector space.

*Proof.* The theorem is proved in [Lor96][Chapter VIII, Lemma 3.7] □

The last theorem proves that $H^0(D)$ is a finite finite-dimensional vector space, the next does the same for $H^1(D)$.

**Theorem 2.3.7.** Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. Then, given $D \in \mathrm{Div}(X)$, the $k$-vector space $H^1(D)$ has finite dimension, denoted by $h^1(D)$. Moreover, $h^0(D) = \deg(D) + 1 - g + h^1(D)$.

*Proof.* The reader can consult the proof in [Lor96][Chapter VIII, Theorem 3.8] □

**Remark 2.3.8.** Notice that $\deg(D) + 1 - h^0(D) + h^1(D)$ is constant.

**Theorem 2.3.9** (Riemann's Theorem). For all $D \in \mathrm{Div}(X)$,

$$h^0(D) \geq \deg(D) + 1 - g$$

*Proof.* It follows from the previous theorem. Since $h^1(D)$ is a finite nonnegative integer we obtain the inequality □

**Theorem 2.3.10** (Riemann-Roch). Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. Then there exists a divisor $K$ in $\mathrm{Div}(X)$ such that, for all $D \in \mathrm{Div}(X)$, the $k$-vector space $\mathrm{Hom}_k(H^1(D), k)$ is isomorphic to the space $H^0(K - D)$. In particular, $h^1(D) = h^0(K - D)$ and

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D).$$

**Corolary 2.3.1.** 1. $h^1(O) = h^0(K - O) = g$,

2. $h^1(K) = h^0(K - K) = 1$, and

3. $\deg(K) = h^0(K) - 1 + g - h^1(K) = 2g - 2$.

*Proof.* 1. By example 2.3.1 we have $h^0(0) = \deg(0)+1-g+h^1(0) \Leftrightarrow 1 = +1-g+h^1(0) \Leftrightarrow h^1(0) = g$.

2. $h^1(K) = h^0(K - K) = k^0(0) = 1$.

3. $\deg(K) = h^0(K) - 1 + g - h^1(K) \Leftrightarrow \deg(K) = 2g - 2$.

□

**Remark 2.3.11.** The class of $K$ in $\mathrm{Pic}(X/k)$ is called the canonical class. A divisor in the canonical class is called a canonical divisor.

**Corolary 2.3.2.** Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. Let $\mathcal{L} \in \mathrm{Pic}(X/k)$. If $\deg(\mathcal{L}) \geq 2g - 1$, then $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g$.

*Proof.* Let $D$ be a divisor whose class in $\mathrm{Pic}(X/k)$ is $\mathcal{L}$. Since $\deg(D) > \deg(K)$, we find that $\deg(K - D) < 0$, and hence, $h^0(K - D) = 0$ by example 2.3.1. □

**Definition 2.3.4.** Fix an element $\mathcal{L} \in \mathrm{Pic}(X)$. Let $E_{\mathcal{L}} := \{D \in \mathrm{Div}(X) : D \geq 0 \text{ and } \mathrm{cl}(D) = \mathcal{L}\}$.

**Remark 2.3.12.** $E_L = \emptyset$ if $\deg(\mathcal{L}) < 0$, since the degree of an effective divisor is always nonnegative.

**Theorem 2.3.13.** Let $k$ be any field. Let $X/k$ be a nonsingular complete curve. Let $L \in \mathrm{Pic}(X)$. Assume that $E_{\mathcal{L}} \neq \emptyset$ and let $D \in E_{\mathcal{L}}$. Let $\psi_D : H^0(D)\backslash\{0\} \to E_{\mathcal{L}}$, with $\alpha \mapsto \mathrm{div}(\alpha) + D$. Then the map $\psi_D$ is surjective. Moreover, the group $k^*$ acts on $H^0(D)\backslash\{0\}$ by

$$k^* \times H^*\backslash\{0\} \mapsto H^0(D)\backslash\{0\}$$

$$(c, \alpha) \mapsto c\alpha,$$

and $E_{\mathcal{L}}$ can be identified with the quotient of $H^0(D)\backslash\{0\}$ by the action of $k^*$. In particular, $E_{\mathcal{L}}$ is in bijection with $\mathbb{P}^{h^0(D)-1}(k)$.

*Proof.* Consult [Lor96][Chapter VIII, Lemma 1.7] to find details about the proof. □

**Corolary 2.3.3.**

$$|E_{\mathcal{L}}| = \frac{q^{h^0(D)} - 1}{q - 1}.$$

# Chapter 3

# The Zeta Function & Weil Conjetures.

## 3.1 A Litlle Bit of History

This historical review is taken from [Lor96][Chapter VIII, Introduction]. Let $p$ be a prime and let $q = p^r$ for some $r \geq 1$, and consider $\mathbb{F}_q$. Let $F \in \mathbb{F}_q[x_0, x_1, x_2]$ be a homogeneous polynomial, and define $N_n := |X_F(\mathbb{F}_q)|$, where $\mathbb{F}_{q^n}$ denotes the unique Galois extension of $\mathbb{F}_q$ of degree $n$.

To study the behavior of the sequence $\{N_n\}_{n\in\mathbb{N}}$ attached to a given nonsingular curve $X_F(\overline{\mathbb{F}}_q)$, we will consider the power series

$$\mathbf{Z}(X_F/\mathbb{F}_q, T) := \exp \sum_{n=1}^{\infty} N_n \frac{T^n}{n}.$$

The definition of the zeta function of a curve is made in analogy with the definition of the historical Riemann $\zeta-$function and Dedekind $\zeta-$functions. It was Artin, in the 1920s, who first developed the theory of the zeta-function in the case of hyperelliptic curves. Once arithmetic geometers realized how to translate the definition of these fuctions from the context of number fields to the context of function fields, it became clear to them that they should also try to prove that the analogues of these properties hold in the context of function fields. In 1931, Schmidt proved the functional equation of the zeta function of a curve and conjectured that the analogue of the Riemann hypothesis holds. Hasse soon thereafter proved this conjecture in the case of elliptic curves. The general case was proved in 1940s by Weil. The Riemann hypothesis for number fields is still an open question today. Weil, in [Wei49] proposed a series of conjectures that, if true, would extend his result for curves to higher dimensions. These conjectures became known as the Weil Conjectures..

## 3.2 The Zeta Function

In the first part of this section, we introduce the Riemann $\zeta$-function and the Dedekind $\zeta$-function. The idea is to compere the proposition and conjectures stated for these $\zeta$-functions that are valid for the Zeta function of nonsingular curves. From now on, we just call it the Zeta function.

**Definition 3.2.1.** Let $\{a_n\}_{n\in\mathbb{N}}$ be an infinite sequence with $a_n \in \mathbb{C}$, for all $n \in \mathbb{N}$. The infinite series $\sum_{n=0}^{\infty} a_n n^{-s}$, with $s \in \mathbb{C}$, is called a Dirichlet series.

Let $r \in \mathbb{R}$. Let

$$\mathcal{H}_r := \{s \in \mathbb{C} | \mathrm{Re}(s) > r\}.$$

If there exists $s_0 \in \mathbb{C}$ such that the infinite series $\sum_{n=0}^{\infty} a_n n^{-s_0}$ converges, then the series $\sum_{n=0}^{\infty} a_n n^{-s}$ converges for all $s \in \mathcal{H}_{\mathrm{Re}(s_0)}$. Moreover, the Dirichlet series converges uniformly on any compact subspace of $\mathcal{H}_{\mathrm{Re}(s_0)}$, and the function $s \mapsto \sum_{n=0}^{\infty} a_n n^{-s}$ is holomorphic on $\mathcal{H}_{\mathrm{Re}(s_0)}$.

**Definition 3.2.2.** The Dirichlet series $\zeta(s) := \sum_{n=0}^{\infty}$ is called the Riemann $\zeta$-function.

**Theorem 3.2.1.** The $\zeta$-function defines a holomorphic function $\zeta : \mathcal{H}_1 \to \mathbb{C}$. It can be extended to a meromorphic function on $\mathbb{C}$, with a simple pole at $s = 1$. Moreover, $\lim_{s \to 1} \zeta(s)(s-1) = 1$.

*Proof.* The proof is omitted. □

**Conjecture 3.2.1** (Riemann Hypothesis.). Let $s \in \mathbb{C}$ be such that $\zeta(s) = 0$. If $0 \leq \mathrm{Re}(s) \leq 1$, then $\mathrm{Re}(s) = \frac{1}{2}$.

The strip $\{s : 0 \leq \mathrm{Re}(s) \leq 1\}$ is called the critical strip. The line $\{s : \mathrm{Re}(s) = \frac{1}{2}\}$ is called the critical line. We can restate the Riemann Hypothesis, that is, the zeros of $\zeta(s)$ in the critical strip lie in the critical line.

**Theorem 3.2.2** (Functional equations of the Riemann $\zeta$-function.). Let $\Gamma(s)$ denote the Gamma function. Let $\overline{\zeta}(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Then $\overline{\zeta}(s) = \overline{\zeta}(1-s)$.

Now let $K/\mathbb{Q}$ be any number field. For $n \in \mathbb{N}$, let $j_n$ denote the number of ideals of $\mathcal{O}_k$ with $\|I\|_{\mathcal{O}_k} := |\mathcal{O}_k/I| = n$. By remark, 2.1.8, $j_1 = 1$. By Theorem 2.1.12, $j_n$ is a finite number for all $n \in \mathbb{N}$.

**Definition 3.2.3.** Let $K/\mathbb{Q}$ be a number field. The Dirichlet series $\zeta(K, s) := \sum_{n=0}^{\infty} \frac{j_n}{n^s}$ is called the Dedekind $\zeta$-function of the number field $K$.

**Example 3.2.3.** $\zeta(\mathbb{Q}, s)$ is equal to the Riemann $\zeta$-function. This result is derived from example 2.1.9 and the fact that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

There is a result that generalizes theorem 3.2.2 for Dedekind $\zeta$-fuction, but it is necessary to define several concepts, so we omit it.

Conjectures which predict that the non-trivial zeros of a given Dirichlet series lie on a specific vertical lines are referred to in the literature as Generalized Riemann Hypothesis (GRH), or Extended Riemann Hypothesis (ERH). A Dedekind $\zeta$-function is also conjecture to satisfy an ERH describing the location of its zeros in the critical strip.

In analogy with the case of number fields, we now associate a $\zeta$-function to any Dedekind domain with finite quotients.

**Definition 3.2.4.** Let $A$ be any Dedekind domain with finite quotients. The formal expression

$$\zeta(A, s) := \sum_{I \in \mathcal{M}(A)} \frac{1}{\|I\|^s}$$

is called the $\zeta$-function of $A$.

Let $j_n := |\{I \in \mathcal{M}(A) : \|I\| = n\}|$. If $j_n < \infty$ for all $n \in \mathbb{N}$, then

$$\zeta(A, s) := \sum_{I \in \mathcal{M}(A)} \frac{1}{\|I\|^s} = \sum_{n=1}^{\infty} \frac{j_n}{n^s}$$

Again, this $\zeta$-function is a generalization of the other two $\zeta$-functions we have presented so far.

**Example 3.2.4.** If $A = \mathbb{Z}$, then $\zeta(\mathbb{Z}, s)$ is the Riemann $\zeta$-function.

**Example 3.2.5.** If $A = K$, where $K$ is a number field and $O_K$ its ring of integers. Then $\zeta(O_k, s)$ is equal to the Dedekind $\zeta$-function associated to $K$.

Let $A$ be any Dedekind domain with finite quotients. Every ideal $I \in \mathcal{M}(A)$ factors into a product $I = P_1^{a_1} \dots P_r^{a_r}$, where $P_1 \dots, P_r$ are maximal ideals of $A$. This factorization is unique up to permutation of the indices. By definition 2.1.10, the norm of ideals is multiplicative, so we can make the following computations.

$$\frac{1}{1 - \frac{1}{\|P\|^s}} = 1 + \frac{1}{\|P\|^s} + \frac{1}{\|P\|^{2s}} + \dots = \sum_{n=0}^{\infty} \frac{1}{\|P\|^{ns}}.$$

Then

$$\sum_{I \in \mathcal{M}(A)} = \prod_{P \in \mathrm{Max}(A)} (\sum_{n=0}^{\infty} \frac{1}{\|P\|^{ns}}) = \prod_{P \in \mathrm{Max}(A)} (1 - \frac{1}{\|P\|^s})^{-1}.$$

The right hand side of this equality is sometimes called the factorization of $\zeta(A, s)$ into a Euler product.

**Remark 3.2.6.** Let $A = \mathbb{Z}$. Then

$$\zeta(\mathbb{Z}, s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_{\text{p prime}} (1 - \frac{1}{p^s})^{-1}.$$

To continue with the derivation of the Zeta function we need the next result taken from [Lor96][Chapter VII, Corollary 2.7]

**Theorem 3.2.7.** Let $k$ be any field. Let $f \in k[x, y]$ be an absolutely irreducible polynomial. If $Z_f(\overline{k})$ is nonsingular or, equivalently, if $\overline{C}_f := \overline{k}[x, y]/(f)$ is a Dedekind domain, then $C_f := k[x, y]/(f)$ is a Dedekind domain. Moreover, if $k$ is a finite field, then $C_f$ is a domain with finite quotients.

Let us now define the main objective of study of this work, the Zeta function.
Let $f \in \mathbb{F}_q[x, y]$ be an absolutely irreducible polynomial. Assume that $Z_f(\overline{\mathbb{F}}_q)$ is a nonsingular curve, then the ring $C_f := \mathbb{F}_q[x, y]/(f)$ is a Dedekind domain with finite qoutients.
Let

$$\zeta(Z_f/\mathbb{F}_q, s) := \zeta(C_f, s) = \sum_{I \in \mathcal{M}(C_f)} \frac{1}{\|I\|^s} = \prod_{M \in \mathrm{Max}(C_f)} (1 - \frac{1}{\|M\|^s})^{-1}.$$

Consider

$$b_d := \#\{M \in \mathrm{Max}(C_f) : |C_f/M : \mathbb{F}_q| = d\}.$$

From theorem 2.2.14, we know that $b_d$ is an integer. If $|C_f/M : \mathbb{F}_q| = d$, then $\|M\| = |C_f/M| = q^d$. Therefore,

$$\zeta(Z_f/\mathbb{F}_q, s) = \prod_{d\in\mathbb{N}}(1 - \frac{1}{q^{sd}})^{-b_d}.$$

Let $T := q^{-s}$. Define

$$\mathbf{Z}(Z_f/\mathbb{F}_q, T) := \prod_{d\in\mathbb{N}}(1 - T^d)^{-b_d},$$

so that $\mathbf{Z}(Z_f/\mathbb{F}_q, T) = \zeta(Z_f/\mathbb{F}_q, s)$. When no confusion may result, we will denote the function $\mathbf{Z}(Z_f/\mathbb{F}_q, T)$ simply by $\mathbf{Z}(T)$.

Taking the logarithm, we find that

$$\log(\mathbf{Z}(T)) = -\sum_{d\in\mathbb{N}} b_d \log(1 - T^d) \;\Rightarrow\; \log(\mathbf{Z}(T)) = \sum_{d\in\mathbb{N}} b_d(\sum_{i=1}^{\infty} \frac{T^{di}}{i}).$$

Reordering the terms in the above series, and using the theorem 2.2.14, we obtain that

$$\log(\mathbf{Z}(T)) = \sum_{n=1}^{\infty}(\sum_{d|n} db_d)\frac{T^n}{n} = \sum_{n=1}^{\infty} \frac{N_n T^n}{n}.$$

Therefore

$$\mathbf{Z}(Z_f/\mathbb{F}_q, T) = \exp(\sum_{n=1}^{\infty} \frac{N_n T^n}{n}).$$

**Definition 3.2.5.** The power series $\mathbf{Z}(T)) \in \mathbb{Q}[[T]]$ is called the zeta-function of the affine curve $Z_f(\overline{\mathbb{F}}_q)$ over $\mathbb{F}_q$.

From theorems 2.2.17 & 2.2.18 we can derive the zeta function for projective curves and for nonsigular complete curves. We just state the definitions.

**Definition 3.2.6.** Let $F \in \mathbb{F}_q[x_0, x_1, x_2]$ be a homogeneous polynomial. Let $N_n := |X_F(\mathbb{F}_{q^n})|$. The zeta-function of $X_F(\overline{\mathbb{F}}_q)$ over $\mathbb{F}_q$ is the power series

$$\mathbf{Z}(X_F/\mathbb{F}_q, T)) = \exp(\sum_{n=1}^{\infty} \frac{N_n T^n}{n}).$$

**Definition 3.2.7.** The zeta function of a nonsingular complete curve $X/\mathbb{F}_q$ is the power series

$$\mathbf{Z}(X_F/\mathbb{F}_q, T)) = \prod_{P\in X}(1 - T^{\deg(P)})^{-1} = \exp(\sum_{n=1}^{\infty} \frac{N_n T^n}{n}),$$

where $N_n = |X(\mathbb{F}_{q^n})|$.

**Theorem 3.2.8.** Let $X/\mathbb{F}_{q^n}$. Consider $X_{\mathbb{F}^{q^n}}/\mathbb{F}_{q^n}$ the nonsingular complete curve associated to $\mathbb{F}_{q^n}(X)/\mathbb{F}_{q^n}$. See definition 2.2.9. Then

$$\mathbf{Z}(X_{\mathbb{F}^{q^n}}/\mathbb{F}^{q^n}, T^n) = \prod_{i=1}^{n} \mathbf{Z}(X/\mathbb{F}_q, \xi_n^i T),$$

where $\xi_n$ is a $n$-th root of unity.

*Proof.* [Lor96][Chapter VIII, Lemma 5.12] □

## 3.3 Examples of the Zeta Function

Now we want to give some interesting examples of the computation of the zeta function where the Jacobi sums are involved. Most of the cases we examined are not curves but hypersurfaces, but the definition of the Zeta function for this set of solutions is the same.

**Example 3.3.1.** Let $f = 0 \in \mathbb{F}_q[x, y]$. Hence $Z_f(\mathbb{F}_{q^n}) = \mathbb{A}^1(\mathbb{F}_{q^n})$, and $N_n = q^n$.

The zeta function is

$$\mathbf{Z}(T) = \exp\Big(\sum_{n=1}^{\infty} \frac{q^n T^n}{n}\Big) = \exp(-\log(1 - qT)) = \frac{1}{1 - qT}.$$

**Example 3.3.2.** Consider the polynomial $F = x_m \in \mathbb{F}_q(x_0, x_1, \ldots, x_m)$, the zeta function of $X_F(\overline{\mathbb{F}}_q)$ is

$$\mathbf{Z}(X_F/\mathbb{F}_q, T) = (1 - q^{n-1}T)^{-1}(1 - q^{n-2}T)^{-1} \ldots (1 - qT)^{-1}(1 - T)^{-1}$$

To see it, notice that the zeros of $F$ are the points $(a_0, \ldots, a_m) \in \mathbb{P}^m(\mathbb{F}_{q^n})$ with $a_m = 0$, i.e., the points at infinite. Then

$$N_n = |\mathbb{P}^{m-1}(\mathbb{F}_{q^n})| = q^{n(m-1)} + q^{n(m-2)} + \ldots + q^n + 1,$$

so

$$\sum_{n=1}^{\infty} \frac{N_n T^n}{n} = \sum_{i=0}^{m-1}\Big(\sum_{n=1}^{\infty} \frac{(q^i T)^n}{n}\Big) = -\sum_{i=0}^{m-1} \log(1 - q^i u).$$

Finally, the zeta function of $X_F(\overline{\mathbb{F}}_q)$ is is given by

$$\mathbf{Z}(T) = \exp\Big(-\sum_{i=0}^{m-1} \log(1 - q^n T)\Big) = (1 - q^{m-1}T)^{-1}(1 - q^{m-2}T)^{-1} \ldots (1 - qT)^{-1}(1 - T)^{-1}.$$

**Example 3.3.3.** Consider the hypersurface defined by $-x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ over $\mathbb{F}_q$. Using theorem 1.3.13 (assuming $2 \nmid q$) we obtain

$$N_1 = q^2 + q + 1 + \chi(-1)\frac{1}{q} g(\chi)^2,$$

where $\chi$ is the character of order 2 on $\mathbb{F}_q$. We know that $g(\chi)^2 = \chi(-1)q$. Thus

$$N_1 = q^2 + q + 1 + \chi(-1)q.$$

To compute $N_n$, notice the latter computation holds for the character of order 2 of $\mathbb{F}_{q^n}$. Then we must just replace $q$ by $q^n$ and $\chi$ by $\chi_n$, where $\chi_n$ is the character of order 2 on $\mathbb{F}_{q^n}$. Then

$$N_n = q^{2n} + q^n + 1 + \chi_n(-1)q^n.$$

If $-1$ is a square in $\mathbb{F}_q$, ie., $-1 = a^2$ for some $a \in \mathbb{F}_q^*$, then for all $n$ we have $\chi_n(-1) = \chi_n(a^2) = \chi_n^2(a)$, but the values of $\chi_n$ are 1 and $-1$. Thus $\chi_s(-1) = 1$.

If $-1$ is not a square in $\mathbb{F}_q$, notice

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}}(-1) = (-1)(-1)^q \ldots (-1)^{q^{n-1}} = (-1)^n = \begin{cases} -1 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even} \end{cases}$$

and

$$\chi_n(-1) = \chi(\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(-1)) = \begin{cases} -1 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even} \end{cases}$$

Since $\chi_n$ and $\chi$ have the same order, the latter equality is true.
In the first case

$$\sum_{n=1}^{\infty} \frac{N_n T^n}{n} = \sum_{n=1}^{\infty} \frac{(q^2T)^n}{n} + 2\sum_{n=1}^{\infty} \frac{(qT)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n},$$

and so

$$\mathbf{Z}(T) = (1-q^2T)^{-1}(1-qT)^{-2}(1-T)^{-1}.$$

In the second case the last term gives rise to the sum

$$\sum_{n=1}^{\infty} \frac{(-qT)^n}{n} = -\log(1+qT).$$

Thus in this case

$$\mathbf{Z}(T) = (1-q^2T)^{-1}(1-qT)^{-1}(1+qT)^{-1}(1-T)^{-1}.$$

In conclusion

$$\mathbf{Z}(T) = \begin{cases} (1-q^2T)^{-1}(1-qT)^{-2}(1-T)^{-1} & \text{if } -1 \text{ is square in } \mathbb{F}_q \\ (1-q^2T)^{-1}(1-qT)^{-1}(1+qT)^{-1}(1-T)^{-1} & \text{if } -1 \text{ is not square in } \mathbb{F}_q \end{cases}$$

**Example 3.3.4.** Consider the curve $x_0^3 + x_1^3 + x_2^3 = 0$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p is a prime congruent to 1 module 3.

Again. taking into account the theorem 1.3.13 we find that

$$N_1 = p + 1 + \frac{1}{p} \sum_{\chi_0,\chi_1,\chi_2} \chi_0(1)\chi_1(1)\chi_2(1) g(\chi_0)g(\chi_1)g(\chi_2),$$

where $\chi_i^3 = \varepsilon$, $\chi_i \neq \varepsilon$, and $\chi_0\chi_1\chi_2 = \varepsilon$.

$$N_1 = p + 1 + \frac{1}{p} \sum_{\chi_0,\chi_1,\chi_2} g(\chi_0)g(\chi_1)g(\chi_2)$$

Let $\chi$ the character of order 3 of $\mathbb{Z}/p\mathbb{Z}$. Then

$$N_1 = p + 1 + \frac{1}{p}[g(\chi)^3 + g(\chi^2)^3] = p + 1 + \frac{1}{p}[g(\chi)^3 + g(\chi^{-1})^3] =$$

$$p + 1 + \frac{1}{p}[p\pi + p\overline{\pi}] = p + 1 + \pi + \overline{\pi}$$

The latter is true since $g(\chi)^3 = p\pi$, where $\pi = J(\chi,\chi)$, and $\pi\overline{\pi} = p$. Thus

$$N_1 = p + 1 + \pi + \overline{\pi}.$$

By the corollary to Hasse-Davenport Relation we obtain that

$$N_n = p^n + 1 - (-\pi)^n - (-\overline{\pi})^n.$$

Then

$$\mathbf{Z}(T) = \exp(\sum_{n=1}^{\infty} \frac{[p^n + 1 - (-\pi)^s - (-\overline{\pi})^n]T^n}{n}) = \exp(\sum_{n=1}^{\infty} \frac{(pT)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n} - \sum_{n=1}^{\infty} \frac{(-\pi T)^n}{n} - \sum_{n=1}^{\infty} \frac{(-\overline{\pi}T)^n}{n})$$

$$= \exp[-\log(1-pT) - \log(1-T) + \log(1+\pi T) + \log(1+\overline{\pi}T)] = (1-pT)^{-1}(1-T)^{-1}(1+\pi T)(1+\overline{\pi}T)$$

$$= \frac{1 + (\pi + \overline{\pi})T + |\pi|^2 T^2}{(1-pT)(1-T)} = \frac{1 + AT + pT^2}{(1-pT)(1-T)}$$

where $A = \pi + \overline{p}$ derived from theorem 1.3.7.

The next example is an adaptation of the previous one. It provides a description about how the zeta function changes when we replace the smallest field for another one.

**Example 3.3.5.** The Zeta function of $X_F(\overline{\mathbb{F}}_4)$ where $F = x_0^3 + x_1^3 + x_2^3$ is

$$\mathbf{Z}(X_F/\overline{\mathbb{F}}_4, T) = \frac{(1+2u)^2}{(1-u)(1-4u)}.$$

To obtain this result we reasoning in the same way to example 3.3.4, in fact, the computations are the same, we just need to change $p$ for $q = 4$ since we used theorem 1.3.13 there. Then

$$N_1 = q + 1 + \frac{1}{q}g(\chi)^3 + \frac{1}{q}g(\chi^2)^3 = q + 1 + \pi + \overline{\pi}.$$

For $N_n$ we obtain

$$N_n = q^n + 1 - (-\pi)^n - (-\overline{\pi})^n$$

Then

$$\mathbf{Z}(T) = \frac{1 + (\pi + \overline{\pi})T + |\pi|^2 T^2}{(1-qT)(1-T)}$$

From theorem 1.3.7, we obtain that $A = 4$, so

$$\mathbf{Z}(T) = \frac{(1 + 4T + 4T^2)}{(1-4T)(1-T)} = \frac{(1+2T)^2}{(1-4T)(1-T)}.$$

The next theorem described the zeta function of $X_F(\mathbb{F}_q)$ where $F$ is the polynomial considered in theorem 1.3.13. Due this theorem and Hasse-Davenport Relation, the proof follows directly from computing the zeta function of the number of solutions.

**Theorem 3.3.6.** Let $F = a_0 x_0^m + a_1 x_1^m + \ldots + a_n x_n^m$, where $a_0, a_1, \ldots, a_n \in \mathbb{F}_q^*$, and $q \equiv 1(m)$. Then the zeta function $\mathbf{Z}(X_F/\mathbb{F}_q, T)$ is a rational function of the form

$$\frac{P(T)^{(-1)^n}}{(1-T)(1-qT)\ldots(1-q^{n-1}T)},$$

where $P(T)$ is the polynomial

$$\prod_{\chi_0, \chi_1, \ldots, \chi_n} (1 - (-1)^{n+1} \frac{1}{q} \chi_0(a_0^{-1}) \ldots \chi_n(a_n^{-1}) g(\chi_0) g(\chi_1) \ldots g(\chi_n) T),$$

where the $(n+1)$-tuples $\chi_0, \chi_1, \ldots, \chi_n$ being subject to the condition $\chi_i^m = \varepsilon$, $\chi_i \neq \varepsilon$, and $\chi_0 \chi_1 \ldots \chi_n = \varepsilon$.

The next theorem is a generalization of the example 3.3.3, it exhibits how the zeta function changes when the number of variables is altered.

**Example 3.3.7.** Consider the polynomial $F = a_0x_0^2 + a_1x_1^2 + \dots a_nx_n^2$ over $\mathbb{F}_p$.

If $n$ is even, by theorem 3.3.6 we obtain that

$$Z(X_F/\mathbb{F}_p, T) = \frac{1}{(1-T)(1-pT)\dots(1-p^{n-1}T)}$$

since there is only one character of order 2, say $\chi$, and $\chi^{n+1} = \chi \neq \varepsilon$ so $P(u) = 1$.
If $n$ is odd, again by theorem 3.3.6

$$Z(X_F/\mathbb{F}_p, T) = \frac{P(T)^{(-1)^n}}{(1-T)(1-pT)\dots(1-p^{n-1}T)},$$

and

$$P(T) = 1 - \frac{1}{p}\chi(a_0^{-1})\dots\chi(a_n^{-1})g(\chi)^{n+1}T = 1 - \frac{1}{p}\chi(a_0^{-1}\dots a_n^{-1})g(\chi)^{n+1}u,$$

where $\chi$ is the character of order 2, in fact, it is the Legendre symbol. Using the fact that $g(\chi)^2 = \chi(-1)p$ we obtain

$$P(T) = 1 - p^{(n-1)/2}(\chi(-1))^{(n+1)/2}\chi(a_0^{-1}\dots a_n^{-1})T,$$

If $p \equiv 1\,(4)$, the Legendre symbol gives us that $\chi(-1) = 1$, and

$$P_1(T) = 1 - p^{(n-1)/2}\chi(a_0^{-1}\dots a_n^{-1})T,$$

If $p \equiv 3\,(4)$, the Jacobi symbol gives us that $\chi(-1) = -1$, and

$$P_3(T) = 1 - (-1)^{(n+1)/2}p^{(n-1)/2}\chi(a_0^{-1}\dots a_n^{-1})T.$$

In conclusion, the zeta function is

$$Z(X_F/\mathbb{F}_q, T) = \begin{cases} (1-T)^{-1}(1-pT)^{-1}\dots(1-p^{n-1}T)^{-1} & \text{if } n \text{ is even} \\ (1-T)^{-1}(1-pT)^{-1}\dots(1-p^{n-1}T)^{-1}P_1(T)^{-1} & \text{if } n \text{ is odd and } p \equiv 1\,(4) \\ (1-T)^{-1}(1-pT)^{-1}\dots(1-p^{n-1}T)^{-1}P_3(T)^{-1} & \text{if } n \text{ is odd and } p \equiv 3\,(4) \end{cases}$$

**Example 3.3.8.** In this example we compare the zeta function of the curve $y^2 = x^3 + x^2$ over $\mathbb{F}_p$ considering it as a affine curve and a projective curve.

We need to find $N_n$. For any $n$ (0,0) belongs to $Z_f(\overline{\mathbb{F}}_p)$. For $n = 1$, suppose $x \neq 0$ and let $t = \frac{y}{x}$. Consider $f(x,t) = x^3 + x^2 - x^2t^2$, so

$$f(x,t) = 0 \;\Leftrightarrow\; x + 1 - t^2 = 0 \;\Leftrightarrow\; x = t^2 - 1 \;\Leftrightarrow\; f(t^2-1, t) = 0.$$

Notice that the zeros depends on $t$ which varies over all $\mathbb{F}_p$ omitting 1 and $-1$ since for $t = \pm 1$ we have $x = 0$, so there are $p-2$ zeros, hence $N_1 = p - 1$. This computation didn't depend on $n$, so $N_n = p^n - 1$.

For the affine case, the zeta function is

$$\mathbf{Z}(Z_f/(\mathbb{F}_p, T) = \exp(\sum_n^\infty (p^n - 1)\frac{T^n}{n}) = \exp(\sum_n^\infty \frac{(pT)^n}{n} - \sum_{n=1}^\infty \frac{T^n}{n}) = \exp(-\log(1-pT) - \log(1-T)) =$$

$$(1-pT)^{-1}(1-T)^{-1}$$

To obtain the projective case, we just need to add the point at infinity of $f$. Let $F = x^3+x^2z-y^2z$, the unique infinity point is $[0,1,0]$ for all $n$, so $N_n = q$ and the zeta function is equal to

$$\mathbf{Z}(X_F/\mathbb{F}_p, T) = (1-p)^{-1}.$$

## 3.4 Weil Conjectures for Nonsingular Curves.

First of all, we recall the tools we need to use to prove two of the Weil Conjectures, these are consequences of the Riemann-Roch theorem, and we have talked about them in the previous chapter.
There exists an integer $g$ and, for each $\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)$, there is a non-negative integer $h^0(\mathcal{L})$, such that

1. $|E_{\mathcal{L}}| = \frac{q^{h^0(\mathcal{L})}-1}{q-1}$ (I).
2. If $\deg(\mathcal{L}) \geq 2g-1$, then $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g$ (II).
3. There exists an element $\mathcal{K} \in \mathrm{Pic}^{2g-2}(X/\mathbb{F}_q)$, such that, for all $\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)$ we have $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g + h^0(\mathcal{K}-\mathcal{L})$ (III).

All the examples above exhibit an important property of the zeta function that every nonsingular curve satisfies: it is a rational function. This is the first Weil conjecture.

**Theorem 3.4.1** (Rationality of the Zeta Function). Let $X/\mathbb{F}_q$ be a nonsingular curve of genus $g$. Then

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \frac{f(T)}{(1-T)(1-qT)},$$

with $f(T) \in \mathbb{Z}[T]$ a polynomial of degree at most $2g$.

*Proof.*

$$\mathbf{Z}(X/\mathbb{F}_q, T) := \prod_{P\in X}(1-T^{\deg(P)})^{-1} = \prod_{P\in X}(\sum_{n_P=0}^{\infty} T^{a_{n_P}\deg(P)}) = \sum_{D\in \mathrm{Eff}(X/\mathbb{F}_q)} T^{\deg(P)} =$$

$$\sum_{\substack{\mathcal{L}\in\mathrm{Pic}(X/\mathbb{F}_q)\\ \deg(\mathcal{L})\geq 0}} \Big(\sum_{\substack{D\in\mathrm{Eff}(X/\mathbb{F}_q)\\ \mathrm{cl}(D)=\mathcal{L}}} T^{\deg(D)}\Big) = \sum_{\substack{\mathcal{L}\in\mathrm{Pic}(X/\mathbb{F}_q)\\ \deg(\mathcal{L})\geq 0}} |E_{\mathcal{L}}|T^{\deg(\mathcal{L})}$$

Assume that $g = 0$. Using the fact that $|E_{\mathcal{L}}| = \frac{q^{\deg(\mathcal{L})+1}-1}{q-1}$ if $\deg(\mathcal{L}) \geq 0$, we find that

$$\frac{h}{(1-T)(1-qT)} = \left(\sum_{i=0}^{\infty} T^i\right)\left(\sum_{j=0}^{\infty}(qT)^j\right) = h\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} q^jT^{i+j}.$$

Let $n = i + j$ and $n - i = j$, then

$$h\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} q^jT^{i+j} = h\sum_{n=0}^{\infty}\sum_{j=0}^{n} q^jT^n = h\sum_{n=0}^{\infty}\frac{q^{n+1}-1}{q-1}T^n = \sum_{\substack{\mathcal{L}\in\mathrm{Pic}(X/\mathbb{F}_q)\\ \deg(\mathcal{L})\geq 0}}\frac{q^{\deg(\mathcal{L})+1}-1}{q-1}T^{\deg(\mathcal{L})} = \mathbf{Z}(X/\mathbb{F}_q, T).$$

Let $g \geq 1$, then

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \sum_{\substack{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0\leq \deg(\mathcal{L})\leq 2g-2}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} + \sum_{\substack{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L})\geq 2g-1}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})}.$$

Set

$$\alpha(T) = \sum_{\substack{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q) \\ 0\leq \deg(\mathcal{L})\leq 2g-2}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})}$$

and

$$\beta(T) = \sum_{\substack{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L})\geq 2g-1}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})}.$$

By theorem 2.2.27, we know $\mathrm{Pic}^0(X/\mathbb{F}_q)$ has order $h$. Therefore, for all $d \in \mathbb{N}$, the set $\mathrm{Pic}^d(X/\mathbb{F}_q)$ is either empty, or has order $h$. Let $e \in \mathbb{N}$ be the unique integer such that $\deg(\mathrm{Pic}(X/\mathbb{F}_q)) = e\mathbb{Z}$. It follows that

$$\nu(T) = \sum_{\substack{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L})\leq 2g-2}} |E_{\mathcal{L}}| T^{\frac{\deg(\mathcal{L})}{e}}$$

is a polynomial in $T$ with integer coefficients, of degree at most $2g-2$. Then $\nu(T^e) = \alpha(T)$.
From the formula of $|E_{\mathcal{L}}|$, and the fact that $|\mathrm{Pic}^0(X/\mathbb{F}_q)| = h$ we imply that

$$\sum_{\substack{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L})\geq 2g-1}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} = h \sum_{\substack{d \\ de\geq 2g-1}} \frac{q^{de+1}-1}{q-1} T^{de}.$$

Let $d_0$ denote the smallest integer such that $d_0 e \geq 2g-1$. Then

$$\frac{h}{q-1}\Big(\sum_{de\geq 2g-1} (q^{de+1-g}-1)T^{de}\Big) = \frac{h}{q-1}\Big(q^{d_0e+1-g}T^{d_0e}\Big(\sum_{d=0}^{\infty}(qT)^{de}\Big) - T^{d_0e}\Big(\sum_{d=0}^{\infty} T^{de}\Big)\Big) =$$

$$\frac{h}{q-1}\left(\frac{q^{d_0e+1-g}T^{d_0e}}{1-q^eT^e} - \frac{T^{d_0e}}{1-T^e}\right) = \frac{h}{q-1}\frac{(q^{d_0e+1-g}-1)(T^e)^{d_0} + (q^e - q^{d_0e+1-g})(T^e)^{d_0+1}}{(1-q^eT^e)(1-T^e)}$$

$$= h\frac{u(T^e)}{(1-q^eT^e)(1-T^e)},$$

where

$$u(T) = \frac{(q^{d_0e+1-g}-1)T^{d_0} + (q^e - q^{d_0e+1-g})T^{d_0+1}}{q-1}.$$

Notice $u(T) \in \mathbb{Z}[T]$ is a polynomial of degree at most $2g$. Otherwise $d_0$ is not the smallest integer such that $d_0 e \geq 2g-1$. Then $\beta(T) = h\frac{u(T^e)}{(1-q^eT^e)(1-T^e)}$.
It follows that

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \nu(T^e) + h\frac{u(T^e)}{(1-q^eT^e)(1-T^e)} = \frac{\nu(T^e)(1-q^eT^e)(1-T^e) + hu(T^e)}{(1-q^eT^e)(1-T^e)}$$

$$= \frac{f(T^e)}{(1-q^eT^e)(1-T^e)}, \tag{3.1}$$

where

$$f(T) = v(T)(1 - q^e T)(1 - T) + hu(T) \in \mathbb{Z}[T]$$

is a polynomial of degree at most $2g$. Moreover, the zeta function has a simple pole at $T = 1$, and

$$\lim_{T\to 1}(T-1)\mathbf{Z}(X/\mathbb{F}_q, T) = \lim_{T\to 1}(T-1)v(T^e) + (T-1)h\frac{u(T^e)}{(1-q^eT^e)(1-T^e)} = \frac{h}{(q-1)e}. \tag{3.2}$$

Now we need to show that $e = 1$, that is, $\deg : \mathrm{Pic}(X/\mathbb{F}_q) \to \mathbb{Z}$ is surjective. Consider the curve $X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}$ obtained from $X/\mathbb{F}_q$ by base change. Let $\xi_e$ be a primitive $e$-th root of unity. Theorem 3.2.8 shows that

$$\mathbf{Z}(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e) = \prod_{i=1}^{e}\mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T) \tag{3.3}$$

Formula 3.2 applied to the zeta function $\mathbf{Z}(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e)$ shows that this function has a simple pole at $T = 1$. The description of $\mathbf{Z}(X/\mathbb{F}_q, T)$ given in the equation 3.1 shows that

$$\prod_{i=1}^{e}\mathbf{Z}(X/\mathbb{F}_q, \xi_e^i T) = \left(\frac{f(T^e)}{(1-q^eT^e)(1-T^e)}\right)^e.$$

This product has a pole of order $e$ at $T = 1$. By comparison of the order of the pole at $T = 1$ on each side of the equation 3.3, we find that $e = 1$. In conclusion

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \frac{f(T)}{(1-qT)(1-T)},$$

and the first conjecture is proved. □

**Remark 3.4.2.** By definition of the zeta function, $\mathbf{Z}(X/\mathbb{F}_q, 0) = 1$ and $f(0) = 1$, so we can factorize $f$ as

$$f(T) = \prod_{i=1}^{2g}(1 - \omega_i T) \in \overline{\mathbb{Q}}[T].$$

**Example 3.4.3.** If $X/\mathbb{F}_q$ is an elliptic curve. Then

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)},$$

where $a = \omega_1 + \omega_2$.

At the beginning of this chapter, we stated that the Riemann $\zeta$-function and the Dedekind $\zeta$-function of number fields all satisfy a functional equation relating $\zeta(s)$ and $\zeta(1-s)$. The zeta function $\mathbf{Z}(X/\mathbb{F}_q, T)$ also satisfies a functional equation. That is the second conjecture.

**Theorem 3.4.4** (Functional equation of the zeta-function). Let $X/\mathbb{F}_q$ be a nonsingular complete curve of genus $g$. Let $\mathbf{Z}(T) := \mathbf{Z}(X/\mathbb{F}_q, T) = \frac{f(T)}{(1-qT)(1-T)}$. Then

$$\mathbf{Z}(\frac{1}{qT}) = (qT^2)^{1-g}\mathbf{Z}(T).$$

*Proof.* Let $\mathbf{Z}'(T) := (q-1)\mathbf{Z}(T)$. Then

$$\mathbf{Z}'(T) = (q-1) \sum_{\substack{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q) \\ \deg(\mathcal{L}) \geq 0}} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})}.$$

Using (I), we can rewrite $\mathbf{Z}'(T)$ as a sum of two terms $\alpha(T) + \beta(T)$, where

$$\alpha(T) := \sum_{0 \leq \deg(\mathcal{L}) \leq 2g-2} q^{h^0(\mathcal{L})} T^{\deg(\mathcal{L})},$$

and

$$\beta(T) := \sum_{\deg(\mathcal{L}) \geq 2g-1} q^{h^0(\mathcal{L})} T^{\deg(\mathcal{L})} - \sum_{\deg(\mathcal{L}) \geq 0} T^{\deg(\mathcal{L})}.$$

Using statement (II) above, we find that

$$\beta(T) = h \sum_{d \geq 2g-1} q^{d+1-g} T^d - h \sum_{d \geq 0} T^d = hq^{1-g}(qT)^{2g-1} \left( \sum_{f \geq 0} (qT)^f \right) - \frac{h}{1-T} = h\left( \frac{q^g T^{2g-1}}{1-qT} \right) - h\left( \frac{1}{1-T} \right).$$

$\beta(1/qT) = q^{1-g} T^{2-2g} \beta(T)$ since

$$q^{1-g} T^{2-2g} \beta(T) = q^{1-g} T^{2-2g} h\left( \frac{q^g T^{2g-1}}{1-qT} - \frac{1}{1-T} \right) = h\left( \frac{qT}{1-qT} - \frac{q^{1-g} T^{2-2g}}{1-T} \right),$$

and

$$\beta\left(\frac{1}{qT}\right) = h\left( \frac{q^g \left(\frac{1}{qT}\right)^{2g-1}}{1 - q\left(\frac{1}{qT}\right)} - \frac{1}{1 - \frac{1}{qT}} \right) = h\left( \frac{q^g q^{1-2g} T^{2-2g}}{T-1} - \frac{qT}{qT-1} \right) = h\left( \frac{qT}{1-qT} - \frac{q^{1-g} T^{2-2g}}{1-T} \right).$$

Then $\beta(\frac{1}{qT}) = q^{1-g} T^{2-2g} \beta(T)$. Now, let's proceed similarly for $\alpha(T)$. Let $\mathcal{K} \in \mathrm{Pic}^{d_0}(X/\mathbb{F}_q)$ be any divisor class of degree $d_0$. The map

$$\bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathbb{F}_q) \to \bigcup_{0 \leq d \leq d_0} \mathrm{Pic}^d(X/\mathbb{F}_q)$$

$$\mathcal{L} \mapsto \mathcal{K} - \mathcal{L}$$

is a bijection. Indeed, if $0 \leq \deg(\mathcal{L}) \leq d_0$, then

$$0 \leq \deg(\mathcal{K} - \mathcal{L}) = \deg(\mathcal{K}) - \deg(\mathcal{L}) \leq d_0,$$

the inverse is the same application.
Choosing $\mathcal{K}$ to be the canonical class of degree $2g-2$ allows us to write

$$\alpha(T) = \sum_{0 \leq \deg(\mathcal{L}) \leq 2g-2} q^{h^0(\mathcal{K}-\mathcal{L})} T^{\deg(\mathcal{K}-\mathcal{L})}.$$

By statement (III), we obtain

$$\alpha(T) = \sum_{0 \leq \deg(\mathcal{L}) \leq 2g-2} q^{h^0(\mathcal{L}) - \deg(\mathcal{L}) - 1 + g} T^{\deg(\mathcal{K}) - \deg(\mathcal{L})} =$$

$$q^{g-1}T^{\deg(\mathcal{K})}\sum_{0\leq\deg(\mathcal{L})\leq 2g-2}q^{h^0(\mathcal{L})}\frac{1}{(qT)^{\deg(\mathcal{L})}}=q^{g-1}T^{2g-2}\alpha(\frac{1}{qT}).$$

In conclusion

$$\mathbf{Z}'(T)=\alpha(T)+\beta(T)=q^{g-1}T^{2g-2}\alpha(\frac{1}{qT})+q^{g-1}T^{2g-2}\beta(\frac{1}{qT})=q^{g-1}T^{2g-2}\mathbf{Z}'(\frac{1}{qT})$$

$$\mathbf{Z}(T)=q^{g-1}T^{2g-2}\mathbf{Z}(\frac{1}{qT})$$

□

**Corolary 3.4.1.** The degree of $f(T)$ is equal $2g$.

*Proof.* Replacing $\mathbf{Z}(T)=\frac{f(T)}{(1-T)(1-qT)}$ in the previous result gives us $f(T)=q^gT^{2g}f(\frac{1}{qT})$. This implies that

$$f(T)=\prod_{i=1}^{2g}(1-\omega_iT)=q^gT^{2g}\prod_{i=1}^{2g}(1-\omega_i\frac{1}{qT})=q^gT^{2g}\prod_{i=1}^{2g}\frac{qT-\omega_i}{qT}=q^{-g}\prod_{i=1}^{2g}(qT-\omega_i).$$

Hence $f(T)$ is a polynomial of degree $2g$. □

**Remark 3.4.5.** $\omega_i$ are algebraic integers. To prove this, let $h(s):=s^{2g}f(1/s)=s^{2g}\prod_{i=1}^{2g}(1-\frac{\omega_i}{s})=\prod_{i=1}^{2g}(s-\omega_i)\in\mathbb{Z}[s]$. Then $h(\omega_i)=0$.

**Corolary 3.4.2.** $\prod_{i=1}^{2g}\omega_i=q^g$, and the map $\omega_i\mapsto q/\omega_i$, from the set $\{\omega_1,\ldots,\omega_{2g}\}$ to itself, is well-defined and bijective.

*Proof.* From the proof of the previous theorem we have

$$f(T)=q^{-g}\prod_{i=1}^{2g}(qT-\omega_i).$$

Take $T=0$, then

$$1=f(0)=q^{-g}\prod_{i=1}^{2g}\omega_i\ \Rightarrow\ \prod_{i=1}^{2g}\omega_i=q^g.$$

Notice $\{\omega_i\}_{i=1}^{2g}$ are the inverses of the zeros of $\mathbf{Z}(T)$. An element of this set may appear multiple times depending on the multiplicity of each root. Apply $T=\omega_i/q$ in the functional equation $\mathbf{Z}(\frac{1}{qT})=(qT^2)^{1-g}\mathbf{Z}(T)$. The result is

$$0=\mathbf{Z}(\frac{1}{\omega_i})=(q(\frac{\omega_i}{q})^2)^{1-g}\mathbf{Z}(\omega_i/q)\ \Rightarrow\ \mathbf{Z}(\omega_i/q)=0,$$

and $q/\omega_i\in\{\omega_i\}_{i=1}^{2g}$.

Let $\omega_i,\omega_j$ such that $\omega_i=\omega_j$, i.e, they are the same root, then $\omega_i/q=\omega_j/q$, and the map is well-defined. Now assume that $\omega_i\neq\omega_j$, then $\omega_i/q\neq\omega_j/q$, so the map is injective. Hence it is also bijective. □

**Remark 3.4.6.** Corollary 3.4.2 allows us, upon a possible renumbering of the indices, to write the set $\{\omega_1,\ldots,\omega_{2g}\}$ as $\{\omega_1,\ldots,\omega_g,q/\omega_1,\ldots,q/\omega_q\}$

There is a formula that expresses the value of $N_n$ in terms of $\omega_i$. To obtain it, observe that

$$\log(\mathbf{Z}(T)) = \log(f(T)) - \log((1-T)(1-qT)) = \sum_{i=1}^{2g} \log((1-\omega_i T)) - \log((1-T)) - \log((1-qT))$$

$$= \sum_{n=0}^{\infty} \left( q^n + 1 - \sum_{i=1}^{2g} \omega_i^n \right) \frac{T^n}{n}.$$

Then $N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n$.

The main goal of our study of curves over finite fields is to obtain explicit bounds for the integers $N_n$. The third conjecture, called the Riemann hypothesis for curves provides this bounds. Recall that the Riemann hypothesis of the Riemann $\zeta$-function says that

$$\text{If } 0 \leq \mathrm{Re}(s) \leq 1, \text{ and } \zeta(s) = 0, \text{ then } \mathrm{Re}(s) = 1/2.$$

By analogy, the statement for the zeta function says

$$\text{If } 0 \leq \mathrm{Re}(s) \leq 1, \text{ and } \mathbf{Z}(q^{-s}) = 0, \text{ then } \mathrm{Re}(s) = 1/2. \tag{3.4}$$

Since $\mathbf{Z}(T)$ is a rational function, the algebraic integers $1/\omega_i$ are the only zeros of $\mathbf{Z}(T)$. If $1/\omega_i = q^{-s}$, then $|\omega_i| = q^{\mathrm{Re}(s)}$. The statement 3.4, if true, would imply that $|\omega_i| = q^{1/2}$.

**Theorem 3.4.7** (Riemann Hypothesis for curves over finite fields).

$$|\omega_i| = q^{1/2}, \quad \forall i = 1, \ldots 2g.$$

From the Riemann Hypothesis for curves and the formula for $N_n$ we obtain that

$$|N_n - (q^n + 1)| \leq 2gq^{n/2}. \tag{3.5}$$

Unfortunately, we do not prove this theorem, although we prove that the Riemann hypothesis follows from a statement seemingly weaker than 3.5.

**Theorem 3.4.8.** Assume that there exist two constants, $C_0$ and $C_1$, and an integer $d \geq 1$ such that for all $n \in \mathbb{N}$,

$$|N_{dn} - (q^{dn} + 1)| = |\sum_{i=1}^{2g} \omega_i^n| \leq C_0 + C_1 q^{dn/2}.$$

Then the Riemann hypothesis holds.

*Proof.* Assume that $|\omega_1| \leq |\omega_2| \leq \ldots \leq |\omega_{2g}|$.

$$|N_{dn} - (q^{dn} + 1)| \leq |C_0 + C_1 q^{dn/2}| \leq |C_0| + |C_1 q^{dn/2}| \leq q^{dn/2}|C_0| + |C_1| q^{dn/2} = (|C_0| + |C_1|) q^{dn/2} = C q^{dn/2},$$

where $C := (|C_0| + |C_1|)$.

*Claim:* Let $\lambda_1, \ldots, \omega_s \in \mathbb{C}$ be such that $|\lambda_1| = \ldots = |\lambda_s| = 1$. Then, $\forall \epsilon > 0$, there exist arbitrarily large integers $n$ such that $|\lambda_1^n + \ldots + \lambda_s^n| \geq s - \epsilon$.

*Proof.* The proof is omitted. □

*Claim:* Let $\omega_1, \ldots, \omega_s \in \mathbb{C}$ with $|\omega_1| \leq \ldots \leq |\omega_s|$. Then, for all $\epsilon > 0$, there exist arbitrarily large integers $n$ such that $|\omega_1^n + \ldots + \omega_s^n| \geq (1 - 2\epsilon)|\omega_s|^n$.

*Proof.* Let $l < s$ be such that $|\omega_s| = \ldots = |\omega_{l+1}| > |\omega_l|$. Then there exist arbitrarily large integers $n$ such that

$$|\frac{\omega_s^n}{|\omega_s|^n} + \ldots \frac{\omega_{l+1}^n}{|\omega_{l+1}|^n}| \geq (s - l - \epsilon) \Rightarrow |\omega_s^n + \ldots \omega_{l+1}^n| \geq |\omega_s|^n(s - l - \epsilon),$$

and

$$|\omega_s^n + \ldots \omega_1^n| \geq |\omega_s^n + \ldots \omega_{l+1}^n| - |\omega_l^n + \ldots \omega_1^n|$$

$$\geq |\omega_s|^n(s - l - \epsilon) - l \cdot |\omega_l|^n \geq |\omega_s|^n(1 - \epsilon) - |\omega_l|^n(s - 1).$$

If $n$ is large enough, then $|\omega_l|^n(s - 1) < \epsilon|\omega_s|^n$. Therefore

$$|\omega_s^n + \ldots \omega_1^n| \geq |\omega_s|^n(1 - \epsilon) - |\omega_l|^n(s - 1) \geq |\omega_s|^n(1 - \epsilon) - \epsilon|\omega_s|^n = (1 - 2\epsilon)|\omega_s|^n.$$

□

The inequality of the previous claim imply that, for arbitrarily large $n$,

$$Cq^{dn/2} \geq |\omega_{2g}^{dn} + \ldots + \omega_1^{dn}| \geq (1 - 2\epsilon)|\omega_{2g}^d|^n.$$

Hence $|\omega_{2g}^d|/(q)^{d/2} \leq |C/(1 - 2\epsilon)|^{1/n}$. Since $|C/(1 - 2\epsilon)|^{1/n}$ tends to 1 as $n$ tends to $\infty$, then $|\omega_{2g}| \leq q^{1/2}$. Since $\omega_1 = q/\omega_{2g}$ and $|\omega_1| \leq |\omega_{2g}|$, we conclude that $|\omega_i| = q^{1/2}$ for all $i = 1, \ldots, 2g$. □

The hypothesis of theorem 3.4.8 is always true, however, we omit it. The proof is in [Lor96] which is based on the proof given in [Bom74].

To conclude, we want to summarize the conjectures stated above but for a variety, including the fourth conjecture. Also, a historical overview of the work will be given.

**Conjecture 3.4.1** (Weil Conjectures). Let $X$ be a smooth projective variety of dimension $n$ over $\mathbb{F}_q$. We define its zeta function by

$$\mathbf{Z}(X, T) := \exp(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}),$$

where $N_n$ is the number of closed points of $X$ where considered over $\mathbb{F}_{q^n}$.

The Weil conjectures are:

1. (Rationality) $\mathbf{Z}(X, T)$ is a rational function of $T$.

2. (Functional equation) Let $E$ be the Euler characteristic of $X$ considered over $\mathbb{C}$. Then

$$\mathbf{Z}(\frac{1}{q^n T}) = \pm q^{nE/2} T^E \mathbf{Z}(T).$$

3. (Riemann hypothesis) We can write

$$\mathbf{Z}(T) = \frac{P_1(T)\dots P_{2n-1}(T)}{P_0(T)\dots P_{2n}(T)},$$

where $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^n T$ and all the $P_i(T)$ are integer polynomials that can be written as

$$P_i(T) = \prod_j (1 - \alpha_{ij} T).$$

Finally, $|\alpha_{ij}| = q^{i/2}$.

4. (Betti numbers) The degree of the polynomials $P_i$ are the Betti numbers of $X$ considered over $\mathbb{C}$.

In [Har77][Appendix C], there is a short historical review about the effort to prove these conjectures. We just mention the most remarkable discoveries, so we invite the reader to consul the reference for more information. One of Weil's major pieces of work is in his book [Wei48a], the proof that Weil conjectures hold for curves. The rationality and the functional equation follow from the Riemann-Roch theorem on the curve. He deduces the analogue of Riemann hypothesis from an inequality of Castelnuovo and Severy about correspondences on a curve. In [Wei48b], Weil gave another proof using $l$-adic representation of Frobenius on abelian varieties, which inspired the later cohomological approaches.

For higher-dimensional varieties, the rationality of the zeta function and the functional equation were first proved by Dwork in [Dwo60]. He used methods of $p$-adic analysis. Most other work on the Weil conjectures has centered aroung the search for a good cohomology theory for varieties defined over fields of characteristic $p$, which would give the right Betti numbers. Furthermore, the cohomology theory should have its coefficients in a field of characteristic zero, so that one can count the fixed points of a morphism as a sum of traces on cohomology groups.
The first cohomology introduced into abstract algebraic geometry was that of Serre using coherent sheaves. Although it could not satisfy the present need, because of its coefficients being in the field over which the varieties is defined, it served as a basis for the development of later cohomology theories. Grothendieck inspired by some of Serre's ideas, saw that one could obtain a good theory by considering the variety together with all its unramified covers. This was the beginning of his theory of étale topology, developed jointly with M. Artin, which he used to define the $l$-adic cohomology, and thus to obtain another proof of the rationality and functionality equation of the Zeta function which can be found in [Gro95].
The analogue of the Riemann hypothesis has proved more difficult to handle. Lang and Weil established an inequality for $n$-dimensional varieties, which is equivalent to the analogue of the Riemann hypothesis if $n = 1$, but falls short of it if $n \geq 2$. It was until seventies that Deligne in [Del74] proved the general analogue of the Riemann hypothesis.

To conclude, we invite the reader to consult the following references: [FK88] and [KW01] to read about étale cohomology and the proof of the Weil conjectures. [Gro73] to consult the foundations of étale chomology by Grothendieck et. al.

# Bibliography


[Apo76] Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[Bom74] Enrico Bombieri. Counting points on curves over finite fields (d'après S. A. Stepanov). In *Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430*, Lecture Notes in Math., Vol. 383, pages 234–241. Springer, Berlin, 1974.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[Dwo60] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960.

[FK88] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné.

[Ful89] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[Gro73] *Théorie des topos et cohomologie étale des schémas. Tome 3*. Lecture Notes in Mathematics, Vol. 305. Springer-Verlag, Berlin-New York, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat.

[Gro95] Alexander Grothendieck. Formule de Lefschetz et rationalité des fonctions *L*. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55. Soc. Math. France, Paris, 1995.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Kob82] Neal Koblitz. Why study equations over finite fields? *Math. Mag.*, 55(3):144–149, 1982.

[KW01] Reinhardt Kiehl and Rainer Weissauer. *Weil conjectures, perverse sheaves and l'adic Fourier transform*, volume 42 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2001.

[Lor96] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[Wei48a] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann & Cie, Paris, 1948.

[Wei48b] André Weil. *Variétés abéliennes et courbes algébriques*, volume 8 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann & Cie, Paris, 1948.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.