THE GENESIS OF THE WEIL CONJECTURES IN THE WORKS OF EMIL ARTIN AND FRIEDRICH SCHMIDT.

Adrian Barquero-Sanchez and Jimmy Calvo-Monge

In the present notes we provide an exposition of the work of Emil Artin and Friedrich Scmidt in the 1920's and 1930's concerning the zeta function of algebraic function fields, as a motivation to the further developments in Algebraic Geometry known as the *Weil Conjectures.* We draw inspiration from Peter Roquette's article *The Riemann hypothesis in characteristic p, its origin and development* (2002) ([7]), where the subject is also discussed with greater historical and mathematical detail. We provide a translation of some of the most important parts of the works of Artin and Schmidt, therefore we try to maintain their original notations when possible.

1. WHAT ARE THE WEIL CONJECTURES?

The Weil conjectures have something to do with counting solutions to polynomial equations in finite fields. But, what do we mean by counting solutions in finite fields? There are different ways in which this can be done, and we explain a few instances in the next examples.

Example. Consider the polynomial $f(x, y) := x^2 + y^2 - 1$. As is well known, the set of solutions (x, y) in $\mathbb{R}^2$ to the equation $f(x, y) = 0$ describes the usual unit circle as in Figure 1.

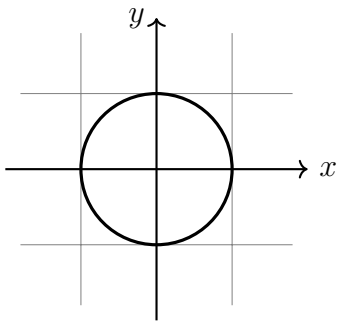


FIGURE 1. The unit circle $x^2 + y^2 - 1 = 0$ on $\mathbb{R}^2$.

On the other hand, if we want to work instead over finite fields, we loose this geometric picture, but we can count the solutions and list them explicitly if we choose a particular finite field. For example, over $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ the solutions are just the two points $(0, 1)$ and $(1, 0)$. Similarly, over the field $\mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ there are four solutions, namely $(1, 0), (2, 0), (0, 1)$ and $(0, 2)$.

Now, in general it is not possible to give an explicit formula (say in the form of a parametrized family) for the solution set of $f(x, y) = 0$ in a finite field $\mathbb{F}_p$. Nevertheless, a related question that

has been treated instead is the question of how many solutions $N_p(f)$ there are to the equation $f(x,y)=0$ in $\mathbb{F}_p$. For example, in the case of the "circle" $f(x,y)=x^2+y^2-1=0$ we have the following counts for varying values of the prime p.

p	$N_p(f)$
2	2
3	4
5	4
7	8
11	12
13	12
17	16
19	20

TABLE 1. The numbers of solutions $N_p(f)$ of the equation $f(x,y)=x^2+y^2-1=0$ over the finite field $\mathbb{F}_p$ for varying values of p.

The reader might notice an interesting pattern in these counts. For odd $p \leqslant 19$, the results in the above table can be summarized as

$$N_p(f)=\begin{cases} p-1 & \text{if } p\equiv 1 \pmod 4,\\ p+1 & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

It turns out that this is not a mere coincidence and it holds true for every odd prime p. In the next example we will prove this in a more general setting.

Another way in which solutions can be counted is given in the following example.

Example. Consider again the polynomial $f(x,y)=x^2+y^2-1$. We will now fix a prime number p and investigate the number of solutions to the equation $f(x,y)=0$ in the finite extensions $\mathbb{F}_{p^n}$ of $\mathbb{F}_p[x]$ for $n=1,2,3,\ldots$.

First, recall that one can construct explicitly the extension $\mathbb{F}_{p^n}$ by taking the quotient of the polynomial ring $\mathbb{F}_p[x]$ by a principal ideal $\langle Q(x)\rangle$, where $Q(x)\in\mathbb{F}_p$ is an irreducible polynomial of degree n. Let us now write $N_{p^n}(f)$ for the number of solutions of $f(x,y)=0$ the finite field $\mathbb{F}_{p^n}$.

We start with $p=2$. We already saw in the previous example that $N_2(f)=2$. Now, it is easy to see that x^2+x+1 is the only irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$. Hence

$$\mathbb{F}_4 := \frac{\mathbb{F}_2[x]}{\langle x^2+x+1\rangle} = \{\bar{0},\bar{1},\bar{x},\bar{x}+\bar{1}\},$$

where the bar denotes the corresponding equivalence class in the quotient. Now, with this explicit description is it a simple matter to check that the solutions to the equation $x^2 + y^2 - 1 = 0$ in $\mathbb{F}_4$ are $(\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{x}, \bar{x} + \bar{1})$ and $(\bar{x} + \bar{1}, \bar{x})$. Thus $N_4(f) = 4$. Similarly, the polynomial $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, so we can construct

$$\mathbb{F}_8 := \frac{\mathbb{F}_2[x]}{\langle x^3 + x + 1 \rangle} = \{\bar{0}, \bar{1}, \bar{x}, \bar{x} + \bar{1}, \bar{x}^2, \bar{x}^2 + 1, \bar{x}^2 + x, \bar{x}^2 + \bar{x} + \bar{1}\}.$$

Again, a calculation shows that the solutions to the equation $x^2 + y^2 - 1 = 0$ in $\mathbb{F}_8$ are the ordered pairs

$$(0, 1), (\bar{1}, \bar{0}), (\bar{x}, \bar{x} + 1), \left(\bar{x}^2, \bar{x}^2 + 1\right), (\bar{x} + 1, \bar{x}), \left(\bar{x}^2 + \bar{x}, \bar{x}^2 + \bar{x} + 1\right),$$
$$\left(\bar{x}^2 + \bar{x} + 1, \bar{x}^2 + \bar{x}\right), \left(\bar{x}^2 + 1, \bar{x}^2\right).$$

Thus, we see that $N_8(f) = 8$. In fact, we can easily see that $N_{2^n}(f) = 2^n$ as follows. Note that since $\mathbb{F}_{2^n}$ has characteristic 2, we have

$$f(x, y) = x^2 + y^2 - 1 = (x + y + 1)^2$$

in $\mathbb{F}_{2^n}[x, y]$. Hence this shows that $f(x, y) = 0 \iff y = x + 1$. Thus the set of solutions of $f(x, y) = 0$ in $\mathbb{F}_{2^n}$ is

$$\mathcal{S}_{f,n} = \{(P(\bar{x}), P(\bar{x}) + \bar{1}) : P(x) \in \mathbb{F}_2[x],\ \deg P(x) < n\}.$$

The reader can see that the solutions given above for $\mathbb{F}_4$ and $\mathbb{F}_8$ have this form and that $\#\mathcal{S}_{f,n} = 2^n$ since there are exactly 2^n polynomials of degree less than n in $\mathbb{F}_2[x]$.

When p is an odd prime, the picture becomes more interesting. For instance, when $p = 3$ the list of solutions in $\mathbb{F}_9$ is [list solutions in there]. A simple code can be written in `COCALC` to do these computations [Write code here]. For the first few primes $p = 3, 5, 7, 11, 13$ and powers $n = 2, 3, 4, 5$ we obtain the following values

p	$N_p(f)$	$N_{p^2}(f)$	$N_{p^3}(f)$	$N_{p^4}(f)$	$N_{p^5}(f)$
3	4	8	28	80	244
5	4	24	124	624	3124
7	8	48	344	2400	16808
11	12	120	1332	14640	161052
13	12	168	2196	28560	371292

TABLE 2. The numbers of solutions $N_p^n(f)$ of the equation $f(x, y) = x^2 + y^2 - 1 = 0$ over the finite field $\mathbb{F}_p^n$ for varying values of p and n.

A careful look at this table might lead us to formulate the following conjecture on the behaviour of $N_{p^n}(f)$, which can be proven using only elementary number theory, so we state it as a theorem.

Theorem 1. *If f is the circle $f = x^2 + y^2 - 1 \in \mathbb{F}_p[x, y]$, where $p \in \mathbb{Z}$ is a prime. Then if $p = 2$ we have that for all $n \in \mathbb{Z}_{\geqslant 0}$:*

$$N_{2^n}(f) = 2^n$$

and if $p \neq 2$, then $N_{p^n}(f)$ is given by the formula

$$N_{p^n}(f) = \begin{cases} p^n - 1 & \text{if } p \equiv 1 \pmod 4, \\ p^n + (-1)^{n-1} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. We already discussed the case $p = 2$. so we asume $p > 2$. Define the function $\chi : \mathbb{F}_{p^n} \longrightarrow \mathbb{C}$ as

$$\chi(r) = \begin{cases} 0 & \text{if } r = 0, \\ 1 & \text{if } r \neq 0 \text{ and } \exists t \in \mathbb{F}_{p^n} : r = t^2. \\ -1 & \text{if } r \neq 0 \text{ and } \nexists t \in \mathbb{F}_{p^n} : r = t^2. \end{cases}$$

This function satisfies the following properties:

(i) χ is multiplicative, i.e., for $a, b \in \mathbb{F}_{p^n}$ we have $\chi(ab) = \chi(a)\chi(b)$.
(ii) The number of solutions in $\mathbb{F}_{p^n}$ to the equation $x^2 = a$, for $a \in \mathbb{F}_{p^n}$ is precisely $\chi(a) + 1$.
(iii) $\displaystyle\sum_{r \in \mathbb{F}_{p^n}} \chi(r) = 0$.

Property (ii) follows from the standard fact that the multiplicative group $\mathbb{F}_{p^n}^\times$ is cyclic, see e.g. []. From (ii) we see that

$$\begin{aligned} N_{p^n}(x^2 + y^2 - 1) = \sum_{r \in \mathbb{F}_{p^n}} [\chi(1 - r^2) + 1] &= p^n + \sum_{r \in \mathbb{F}_{p^n}} \chi(1 - r^2) \\ &= p^n + 1 + \sum_{r \in \mathbb{F}_{p^n}^\times} \chi(1 - r^2). \end{aligned} \tag{1}$$

Hence it remains to evaluate the last sum, which can be written as

$$\sum_{r \in \mathbb{F}_{p^n}^\times} \chi(1 - r^2) = \chi(-1) \sum_{r \in \mathbb{F}_{p^n}^\times \smallsetminus \{\pm 1\}} \chi(r^2 - 1) = 2\chi(-1) \sum_{\substack{\alpha \in \mathbb{F}_{p^n}^\times \smallsetminus \{1\} \\ \alpha \text{ is a square}}} \chi(\alpha - 1). \tag{2}$$

Here we used that $\chi(0) = 0$ to eliminate $r = \pm 1$ from the sum. Also, since $(-r)^2 = r^2$, each square α must be counted twice, which is the reason for the 2 appearing as a factor. Now, in the

sum

$$\sum_{\substack{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}\\ \alpha \text{ is a square}}} \chi(\alpha-1), \tag{3}$$

if $\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}$ is a square such that $\alpha - 1$ is also a square, then the contribution of α would be $\chi(\alpha-1) = 1$; if $\alpha - 1$ is not a perfect square then α would contribute $\chi(\alpha-1) = -1$ to the sum. Therefore we can write (3) as

$$\sum_{\substack{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}\\ \alpha \text{ is a square}}} \chi(\alpha-1) = \#RR - \#NR, \tag{4}$$

where $\#RR$ is the number of squares $\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}$ such that $\alpha - 1$ is also a square, and $\#NR$ is the number of squares $\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}$ such that $\alpha - 1$ is not a square. Clearly $\#RR + \#NR = \#S$, where $\#S$ is the number of squares in $\mathbb{F}_{p^n}^{\times} \setminus \{1\}$. Hence $\#RR - \#NR = \#RR - (\#S - \#RR) = 2\#RR - \#S$. Now, since $\mathbb{F}_{p^n}^{\times}$ is a cyclic group, it follows that the number of squares in $\mathbb{F}_{p^n}^{\times}$ is $(p^n-1)/2$, and since 1 is a square, then $\#S = (p^n-1)/2 - 1 = (p^n-3)/2$. Therefore, from equations (1), (2) and (4), and from the previous observations we see that

$$N_{p^n}(f) = p^n + 1 + 2\chi(-1)\left(2\#RR - \frac{p^n-3}{2}\right). \tag{5}$$

The reader familiar with elementary number theory might recognize the notation $\#RR$, which is commonly used when counting the number of pairs of consecutive squares in a finite field (see e.g. [5, Chapter]). As is usually done, in calculating $\#RR$ we use the following trick. We write $\#RR$ as

$$\#RR = \frac{1}{4}\sum_{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}} (1+\chi(\alpha))(1+\chi(\alpha-1)),$$

where, as can be checked, when both α and $\alpha - 1$ are squares, the term $(1+\chi(\alpha))(1+\chi(\alpha-1))$ is equal to 4, and in all other cases it is equal 0. Thus, we have

$$\begin{aligned}\#RR &= \frac{1}{4}\left(\sum_{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}} 1 + \sum_{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}} \chi(\alpha) + \sum_{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}} \chi(\alpha-1) + \sum_{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}} \chi(\alpha(\alpha-1))\right)\\ &= \frac{1}{4}\left((p^n-2) - \chi(1) - \chi(-1) + \sum_{\alpha\in\mathbb{F}_{p^n}^{\times}\setminus\{1\}} \chi(\alpha(\alpha-1))\right),\end{aligned}$$

where we used property (iii) to evaluate the two innermost sums above. Finally, since $\chi(\alpha^{-2}) = 1$ for every $\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}$, we have

$$\sum_{\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}} \chi(\alpha(\alpha-1)) = \sum_{\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}} \chi(\alpha(\alpha-1)\alpha^{-2}) = \sum_{\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}} \chi(1-\alpha^{-1})$$
$$= \sum_{\alpha \in \mathbb{F}_{p^n}^{\times} \setminus \{1\}} \chi(1-\alpha) = -\chi(1) - \chi(0) = -1,$$

where again we used property (iii), which shows that

$$\#RR = \frac{1}{4}\left(p^n - 4 - \chi(-1)\right). \tag{6}$$

Hence, putting this into equation (5) gives us the formula $N_{p^n}(f) = p^n - \chi(-1)$. Therefore, it remains to evaluate $\chi(-1)$. To do this, observe that since $\#RR \in \mathbb{Z}$, equation (6) implies that $\chi(-1) \equiv p^n \pmod 4$. Now, if $p \equiv 1 (\text{mod } 4)$ then for all $n \geqslant 1$ we have $p^n \equiv 1 (\text{mod } 4)$ as well, and therefore $\chi(-1) \equiv 1 (\text{ mod } 4)$, that is, $\chi(-1) = 1$. On the other hand, if $p \equiv 3 \equiv -1 (\text{mod } 4)$, the by the same argument as before, we have $\chi(-1) \equiv (-1)^n (\text{mod } 4)$, and hence $\chi(-1) = (-1)^n$. This completes the proof. □

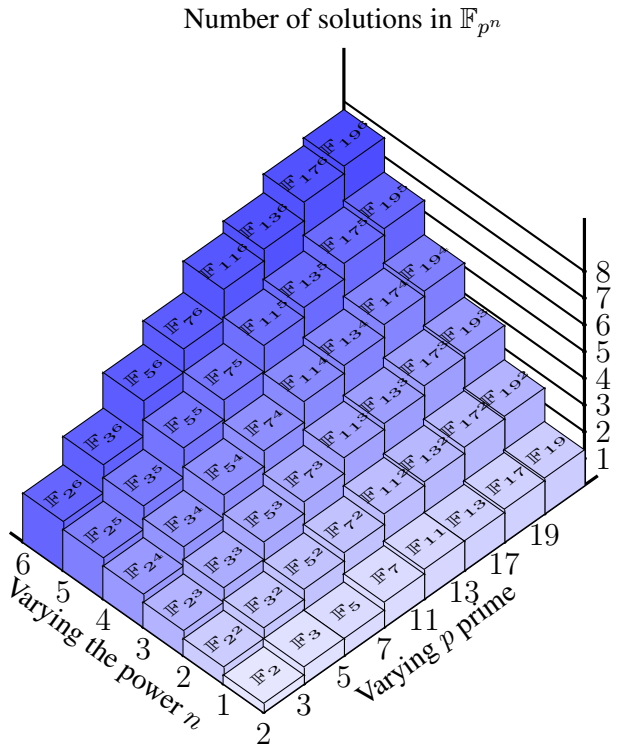


FIGURE 2. The two ways of counting: horizontally and vertically. Numbers of solutions are provided in a logarithmic (base 10) scale.

Thus, we can count those numbers of solutions in two ways, varying the prime p or varying n. In Figure 1 we can see an illustration of the counts for various p ranging over primes and n over the integers, for the curve $x^2 + y^2 - 1 = 0$. All of this can be done to any equation $f(x, y) = 0$ over $\mathbb{F}_p$.

As it happens, it is convenient to do such counting by working over projective space. Hence, let $\mathbb{F}_q$ be a finite field with q elements. Then for any $n \geqslant 1$, projective n-space over $\mathbb{F}_q$, which is denoted by $\mathbb{P}^n(\mathbb{F}_q)$, is defined to be the set of equivalence classes

$$\mathbb{P}^n(\mathbb{F}_q) := \frac{\{(a_0, \ldots, a_n) \in (\mathbb{F}_q)^{n+1}\} \setminus \{(0, 0, \ldots, 0)\}}{\sim},$$

where $\sim$ is the equivalence relation defined on tuples $(a_0, \ldots, a_n) \in (\mathbb{F}_q)^{n+1}$ and $(b_0, \ldots, b_n) \in (\mathbb{F}_q)^{n+1}$ by

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff (a_0, \ldots, a_n) = (\lambda b_0, \ldots, \lambda b_n)$$

for some $\lambda \in \mathbb{F}_q^\times$.
A member of $\mathbb{P}^n(\mathbb{F}_q)$ is denoted by $[a_0 : \cdots : a_n]$, which represents the equivalence class of the element $(a_0, \ldots, a_n) \in \mathbb{F}_q^{n+1}$. For example, in $\mathbb{P}^1(\mathbb{F}_q)$, a typical member is of the form $[a_0 : a_1]$ where $a_0, a_1 \in \mathbb{F}_q$. If we were to consider a the polynomial $x^2 + y^2 - 1$ and analyse how to define it's solutions in $\mathbb{P}^1(\mathbb{F}_q)$. For example, we would like to think that $[1 : 0]$ is a solution, because $(1, 0)$ is a root of f, however in the projective space this point is the same as $[2 : 0]$ (using $\lambda = 2$ in the definition of $\sim$) and $(2, 0)$ is not a root of $x^2 + y^2 - 1$. This means that considering the equivalence classes of solutions of the polynomial $x^2 + y^2 - 1$ in the projective space doesn't gives us a well defined set. This can be fixed by considering homogeneous polynomials. A polynomial $f \in \mathbb{F}_q[x_0, x_1, \cdots, x_n]$ is *homogeneous of degree* d if for every $(a_0, \ldots, a_n) \in \mathbb{F}_q^{n+1}$ and every $\lambda \in \mathbb{F}_q^\times$ we have

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \cdots, a_n)$$

So if f is a homogeneous polynomial of some degree in $\mathbb{F}_q[x_0, x_1, \ldots, x_n]$ the set

$$\{[a_0 : \cdots : a_n] \in \mathbb{P}^n(\mathbb{F}_q) : f(a_0, \ldots, a_n) = 0\}$$

is well defined, that is, if $(a_0, \ldots, a_n)$ is a zero of f then $(\lambda a_0, \ldots, \lambda a_n)$ is also a zero of f, so it doesn't matter which representative we select. This will be the set of projective zeros of that polynomial. Now, the polynomial $x^2 + y^2 - 1$ is not homogeneous, but there is a method of adding another variable to a non homogeneous polynomial that transforms it into a homogeneous polynomial, that process is called homogenization.

If $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ then the homogenization of f is the polynomial $\hat{f} \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$ given by

$$x_0^d f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$$

where d is the maximum of the degrees of the monomials that constitute f (Remember that the degree of a monomial is the sum of its exponents). This formula will always give us a homogeneous polynomial of degree d. For example, one can check that the homogenization of $x^2 + y^2 - 1$ is $x^2 + y^2 - z^2$ (z being the new variable added).
So, if $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, let $\hat{f} \in \mathbb{F}_q[x_0, \cdots, x_n]$ it's homogenization, we will denote by $N_{q^m}(f)$ the number of projective zeros of $\hat{f}$ in the space $\mathbb{P}^n(\mathbb{F}_{q^m})$. You might ask how is this related to the classical count that we discussed earlier, for that note that a zero $(a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ of f gives us a zero $[1 : a_1 : \cdots : a_n] \in \mathbb{P}^n(\mathbb{F}_{q^m})$ of $\hat{f}$, so the zeros of f are included in the count. The points left, which are those with the first coordinate equal to zero, are called the *zeros (or points) at infinity* of f, these will be of importance later.
If we have a collection $\mathcal{S}$ of homogeneous polynomials in $\mathbb{F}_q[x_0, \ldots, x_n]$ the set of common projective zeros of the elements in $\mathcal{S}$, in $\mathcal{P}^n(\mathcal{F}_{q^m})$, that is

$$\{[a_0 : \cdots : a_n] \in \mathbb{P}^n(\mathbb{F}_{q^m}) : f(a_0, \cdots, a_n) = 0 \text{ for all } f \in \mathcal{S}\}$$

is called a *projective variety*. [1]

1.1. **Statement of the Weil conjectures.** Let $X/\mathbb{F}_q$ be a smooth projective variety, where $q = p^m$ for some prime p, in other words, X is the set of solutions in $\mathbb{P}^N(\mathbb{F}_q)$ to a system of homogeneous polynomial equations

$$\begin{cases} f_1(x_0, \ldots, x_N) = 0 \\ \qquad \vdots \\ f_k(x_0, \ldots, x_N) = 0 \end{cases}$$

with $f_j(x_0, \ldots, x_N) \in \mathbb{F}_q[x_0, \ldots, x_N]$. Thus, for $n \in \mathbb{Z}_{\geqslant 1}$ we define the sequence $N_n(X) := \#X(\mathbb{F}_{q^n})$ and consider the the exponential of the previously discussed generating funtion, that is, let

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

This function $Z(X/\mathbb{F}_q, T)$ is known as the *Zeta function* of the variety X. Then, the Weil conjectures state the following.

Theorem 2 (Weil, Dwork, Grothendieck et. al, Deligne)**.** *Let $X/\mathbb{F}_q$ be a smooth projective variety of dimension d. Then the Zeta function $Z(X/\mathbb{F}_q, T)$ satisfies the following properties:*

[1] Actually a projective variety can be defined as a more general object, but this definition will be enough for now.

(i) ***Rationality:****The Zeta function $Z(X/\mathbb{F}_q, T)$ is a rational function of T with coefficients in Q, i.e.,*

$$Z(X/\mathbb{F}_q, T) \in \mathbb{Q}(T).$$

(ii) ***Functional equation:*** *The Zeta function $Z(X/\mathbb{F}_q, T)$ satisfies a functional equation of the form*

$$Z\left(X/\mathbb{F}_q, \frac{1}{q^d T}\right) = \pm q^{de/2} T^e Z(X/\mathbb{F}_q, T),$$

where e is a certain integer called the Euler characteristic of X.

(iii) ***The Riemann hypothesis:*** *The Zeta function $Z(X/\mathbb{F}_q, T)$, which by virtue of (i), is a rational function in $\mathbb{Q}(T)$, has the factorization*

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(T) \cdots P_{2d-1}(T)}{P_0(T) \cdots P_{2d}(T)},$$

where $P_j(T) \in \mathbb{Z}[T]$ for every $0 \leqslant j \leqslant 2d$, $P_0(T) = 1 - T$ and also $P_{2d}(T) = 1 - q^d T$. Moreover, for every $0 \leqslant j \leqslant 2d$, the factorization in $\mathbb{C}$ of $P_j(T)$ is of the form

$$P_j(T) = \prod_{k=1}^{b_j} (1 - \alpha_{jk} T),$$

where $|\alpha_{jk}| = q^{j/2}$.

Remark As we can see this is quite a powerful theorem. It gives us a sufficient characterization on the zeta function for a curve. Certainly is an amazing result: this elaborated function attached to a curve actually turns out to be a rational function. The Riemann hypothesis is named that way, because if you consider the function

$$\zeta_{X/\mathbb{F}_q}(s) := Z(X/\mathbb{F}_q, q^{-s})$$

Then *(iii)* says that the zeros of $\zeta_{X/\mathbb{F}_q}$ have real part equal to $1/2$, this can be checked with an easy calculation.

Clearly, the presentation of this theorem in this way is impressive, but it has no motivation or *raison d'etre*, a lot of questions might come to mind for someone who is reading these results for the first time: Why should we count solutions in the fields $\mathbb{F}_{p^n}$ and not just in the field $\mathbb{F}_p$? Why is the zeta function constructed in such a way? Who came up with this particular way of constructing the zeta function? What is the story behind this definition? And, Why is it important to study the zeta function when trying to solve the problem of counting solutions of polynomials?

Answering these questions is the main goal of this paper. We hope that after the mathematical and historical discussion below the importance of the zeta function and the counting solutions problem becomes clear enough.

The beginning of the story doesn't have to do with curves or finite fields, rather than with field extensions, so we will start there.

2. Artin's Thesis

2.1. **Motivation.** In the decade of 1870 Richard Dedekind (1831-1916) published a series of supplements to the book *Vorlesungen über Zahlentheorie* (Lectures on Number Theory) of P.G.L. Dirichlet (1805-1859). In one of these, he developed the theory of the algebraic integers. Let us remember that an *algebraic number field* K is a subfield of $\mathbb{C}$ such that the field extension $K/\mathbb{Q}$ is finite. In particular K consists in its entirety of algebraic numbers (which are roots of polynomials with coefficients in $\mathbb{Q}$). Clearing denominators in the polynomials, we can see that every element of K is root of a polynomial with coefficients in $\mathbb{Z}$. The subset $\mathcal{O}_K$ formed by those elements of K which are roots of monic polynomials with coefficients in $\mathbb{Z}$ is a ring, it is called the *ring of integers* of K.

Many interesting properties about this ring were discovered in the 19th century. For instance, if I is any ideal of $\mathcal{O}_K$ then there are unique distinct prime ideals of $\mathcal{O}_K$, $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ for some $e_1, \cdots, e_r \in \mathbb{Z}_{\geqslant 1}$. This serves as a unique factorization theorem, like in $\mathbb{Z}$.

Another feature of this ring is that if I is a non-zero ideal of $\mathcal{O}_K$, then I is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, that is there exists $\mathbb{Z}$-linearly independent elements of I given by $\alpha_1, \cdots, \alpha_n$ such that every $\alpha \in I$ can be expressed as a sum $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ for some $a_i \in \mathbb{Z}$. If $\mathcal{B}_1 = \{\alpha_1, \cdots, \alpha_n\}$ is a $\mathbb{Z}$-basis for I (i.e. a basis for I as a free $\mathbb{Z}$-module) it is easy to see that it is also a basis for K as a $\mathbb{Q}$-vector space (we only would have to check that is linearly independent over $\mathbb{Q}$, because it has length n, equal to the dimension of K over $\mathbb{Q}$). If we have any $\mathbb{Q}$-basis of K, $\mathcal{B}_2 = \{\omega_1, \cdots, \omega_n\}$, we can consider the transition matrix $\mathbf{A}$ from basis $\mathcal{B}_2$ to basis $\mathcal{B}_1$, which is a matrix with coefficients in $\mathbb{Q}$. The absolute value of the determinant of this matrix is actually a non-negative integer. It is easy to see that this determinant is independent of the selections of the two basis, so we define the norm of the ideal as the number

$$N_{K/\mathbb{Q}}(I) := |\det(\mathbf{A})|$$

Another basic property of this ring is that if I is a non-zero ideal of $\mathcal{O}_K$, then the quotient ring $\mathcal{O}_K/I$ is finite, and also an impressive relationship occurs, we have the equality

$$N_{K/\mathbb{Q}}(I) = \#\mathcal{O}_K/I.$$

The norm function is a multiplicative function, that is, if $\mathfrak{a}, \mathfrak{b} \in I_K$ then $N_{K/\mathbb{Q}}(\mathfrak{ab}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{b})$, where $\mathfrak{ab}$ is the usual product of ideals.

Thus, if K is a number field we can define the Zeta function for the extension K as the function

$$\zeta_K(s) := \sum_{\mathfrak{a} \in I_K} \frac{1}{[N_{K/\mathbb{Q}}(\mathfrak{a})]^s}$$

defined (to avoid complications) for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$.

2.2. **Algebraic function fields.** The context presented in the previous sections can be varied by considering extensions of the field of rational functions $\mathbb{F}_q(z)$. In this section we aim to develop a new case of field extensions in which the former discussion about algebraic number fields can find a natural analogue. Consider the ring of polynomials $\mathbb{F}_q[z]$ and it's fraction field $\mathbb{F}_q(z)$, the field of rational functions with coefficients in $\mathbb{F}_q$. Now we consider a finite field extension of $\mathbb{F}_q(z)$, which we will call F. As in the number field case, we can construct the ring of integers $\mathcal{O}_F$, that consists of all the elements of F which are roots of monic polynomials with coefficients in $\mathbb{F}_q[z]$. Perhaps the following figure can clear up this setting.

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathcal{O}_K \end{array} \qquad\qquad \begin{array}{ccc} \mathbb{F}_q(z) & \hookrightarrow & F \\ \uparrow & & \uparrow \\ \mathbb{F}_q[z] & \hookrightarrow & \mathcal{O}_F \end{array}$$

FIGURE 3. The analogy between algebraic number fields and algebraic function fields in one variable.

As we can see, we have is a similar situation as in the case of algebraic number fields. The field F is called an *algebraic function field*. Actually, function fields need not to be constructed with the field $\mathbb{F}_q$ as the field of coefficients, but this is the case that we will study here.

The ring $\mathcal{O}_F$ also has the prime factorization property: if I is a non-zero ideal of $\mathcal{O}_F$ then there exists unique prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ and positive integers $a_1, \cdots, a_r$ such that $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$.

In the algebraic function field case, we can define the norm of ideals just as in the previous part. Denote I_F the set of non-zero ideals of $\mathcal{O}_F$ (in analogy with I_K defined earlier). We have that every ideal $I \in I_F$ is a free $\mathbb{F}_q[z]$-module of rank $n = [F : \mathbb{F}_q(z)]$. If we select a basis $\mathcal{B}_1 = \{\alpha_1, \cdots, \alpha_n\}$ of F as a $\mathbb{F}_q(z)$ vector space, and a basis $\mathcal{B}_2 = \{\beta_1, \cdots, \beta_n\}$ of I as a $\mathbb{F}_q[z]$-module. We can easily see that $\mathcal{B}_2$ is also a basis for F as a $\mathbb{F}_q[z]$-vector space. Indeed, if we have a linear combination $h_1\beta_1 + \cdots + h_n\beta_n = 0$, where $h_i \in \mathbb{F}_q(z)$ are not all equal to zero, writing every h_i as $h_i = f_i/g_i$ where $f_i, g_i \in \mathbb{F}_q[z]$, we can clear denominators and arrive to an expression of the form $q_1\beta_1 + \cdots q_n\beta_n = 0$, where the $q_i \in \mathbb{F}_q[z]$ are not all equal to zero, which is impossible, because $\mathcal{B}_1$ is a $\mathbb{F}_q[z]$-basis for I. So, both $\mathcal{B}_1$ and $\mathcal{B}_2$ are linearly independent over $\mathbb{F}_q(z)$, and given that they have the same number of elements, they are both basis for F as a $\mathbb{F}_q(z)$-vector space.
Denote $\mathbf{A}$ the transition matrix from the basis $\mathcal{B}_1$ to the basis $\mathcal{B}_2$, then $\mathbf{A}$ has entries in $\mathbb{F}_q(z)$, but actually it just so happens that det($\mathbf{A}$) is in $\mathbb{F}_q[z]$. We define the norm of the ideal I as the principal ideal of $\mathbb{F}_q[z]$ generated by det($\mathbf{A}$), that is

$$N_{F/\mathbb{F}_q(z)}(I) := \det(\mathbf{A}) \cdot \mathbb{F}_q[z]$$

Note that in the number field case, the norm was an element of $\mathbb{Z}$, so we would expect the norm in the algebraic function field case to be an element of $\mathbb{F}_q[z]$. We ought to check that this definition does not depend on the selection of the basis $\mathcal{B}_1$ and $\mathcal{B}_2$. The degree of any polynomial that is a generator of the principal ideal $N_{F/\mathbb{F}_q(z)}(I)$ is uniquely determined (because is p_1 and p_2 are two generators of this ideal then $p_1 = kp_2$ where k is an unit of $\mathbb{F}_q[z]$, that is $k \in \mathbb{F}_q[z]$). So we can define de degree of the norm $\deg(N_{K/\mathbb{F}_q(z)}(I))$ as the degree of any generator of the principal ideal $N_{F/\mathbb{F}_q(z)}(I)$ of $\mathbb{F}_q[z]$, and with this we can define the absolute norm of the ideal I as

$$|N_{K/\mathbb{F}_q(z)}(I)| := q^{\deg(N_{K/\mathbb{F}_q(z)}(I))}$$

It can be proved that

$$|N_{K/\mathbb{F}_q(z)}(I)| = \#\mathcal{O}_F/I$$

Being this equality an analogue for the relationship between the norm and the quotient $\mathcal{O}_K/I$ in the number field case. From now on, we will work with the absolute value function $|\cdot|$ defined for a polynomial $f(z) \in \mathbb{F}_q[z]$ as $|f(z)| := q^{\deg f(z)}$. In particular, the absolute norm is just the absolute value of the regular norm.

2.3. **Quadratic function fields.** In algebraic number theory, one finds that there is a particularly common case of number fields to be studied. If $d \in \mathbb{Z}$ is a square-free integer (not divisible by any square), then we can form the extension field $K = \mathbb{Q}(\sqrt{d})$. This is an algebraic number field because it is a finite extension of $\mathbb{Q}$. Number fields of this kind are called *quadratic number fields*, they have been thoroughly studied in this area. Although they seem simple extensions to work with, the results they can provide are quite important and helpful in some applications.

If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic number field, then every element in K can be written as $a+b\sqrt{d}$ where $a, b \in \mathbb{Q}$. The ring $\mathcal{O}_K$ in this case can be explicitly calculated as

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \bmod 4. \\ \{a + b\frac{1+\sqrt{d}}{2} : a, b \in \mathbb{Z}\} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

As we stated in the last section, now we want to study the case of algebraic function fields, as an analogue of algebraic number fields. This was the idea behind Artin's thesis. In the context of algebraic function fields he wanted to study the quadratic case. So, naturally, want he did was to investigate the algebraic function field $F = \mathbb{F}_q(z)(\sqrt{D})$ where $D \in \mathbb{F}_q[z]$ is not divisible by the square of any polynomial in $\mathbb{F}_q[z]$. Such an extension is called a *quadratic function field*, just as the reader might expect it to be named.
The first question to be considered is to study the ring of integers $\mathcal{O}_F$ of F. In this case we have that

$$\mathcal{O}_F = \{a + b\sqrt{D} : a, b \in \mathbb{F}_q[z]\}, \tag{7}$$

thanks to [1, Satz pág. 162].

2.4. **Ideals in quadratic function fields.** The first part of Artin's thesis concerns the arithmetic details of quadratic function fields, and it has precisely the name *Arithmetic Part* (Arithmetischer Teil). It deals mainly with the relations between elements of the ring $\mathcal{O}_F$, as given by (7); in particular when it comes to the treatment of ideals. His purpose was to emulate the theoretic body of the number fields and their integer rings, therefore the reader with knowledge from algebraic number theory will see the similarities right away.

If F is an element of the ring of polynomials $\mathbb{F}_q[t]$, let's say

$$F = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0,$$

where $a_n \neq 0$, the sign of F is it's main coefficient: $\text{sign}(F) := a_n$, and the 'size' (Betrag in german, have not found a better translation) of F is the number $|F| := q^n$, where $n = \deg(F)$. We can provide some properties, for example, $|FG| = |F||G|$ for every pair of polynomials F and G, and if $|F| < |G$, then $|F + G| = |G|$ and $\text{sign}(F) + \text{sign}(G) = \text{sign}(G)$.

The former concepts can be similarly defined for expressions of the form

$$F = \sum_{v=-\infty}^{n} a_v t^v = a_n t^n + a_{n-1} t^{n-1} + \cdots$$

for some $n \in \mathbb{Z}$. For a sequence $\{F_n\}$ and an element F, which are expressions of that form, we say that

$$F = \lim_{n \to \infty} F_n$$

if for every $\epsilon \geqslant 0$ exists an N such that for every $n \geqslant N$ we have $|F - F_n| = q^{\deg(F - F_n)} < \epsilon$. In an natural way then we can define the meaning of an expression of the form

$$\sum_{n=0}^{\infty} F_n.$$

Real and Imaginary quadratic function fields (following Artin): Let us consider the equation $X^2 = \Delta$, where

$$\Delta = a^2 t^{2n} + a_{2n-1} t^{2n-1} + \cdots,$$

for some $a \in \mathbb{F}_q$ and $n \in \mathbb{Z}$. This Δ can be written in the form

$$\Delta = a^2 t^{2n}(1 + \Phi), \text{ where } \Phi := \frac{a_{2n-1}}{a^2} t^{-1} + \frac{a_{2n-2}}{a^2} t^{-2} + \cdots,$$

In this case $|\Phi| \leqslant q^{-1}$, and applying a criterion by absolute convergence we can conclude that the power series

$$\sum_{v=0}^{\infty} \binom{\frac{1}{2}}{v} \Phi^v$$

converges to the value $(1+\Phi)^{1/2}$. Therefore a solution to the equation $X^2 = \Delta$ is given by

$$X = \sqrt{\Delta} = at^n \sum_{v=0}^{\infty} \binom{\frac{1}{2}}{v} \Phi^v.$$

In this case we say that $\sqrt{\Delta}$ is **real**. Clearly this emulates the (analytic) construction of roots of real numbers. In other cases of Δ ($\deg(\Delta)$ is odd or the main coefficient of Δ is not a square or both) we say that $\sqrt{\Delta}$ is **imaginary**. Note that given Δ, if g is a generator of the cyclic group $\mathbb{F}_q^{\times}$ then there are four possibilities:

(1) $\sqrt{\Delta}$ is real.
(2) $\sqrt{g\Delta}$ is real. ($\operatorname{sgn}(\Delta)$ is not a square).
(3) $\sqrt{t\Delta}$ is real. ($\deg(\Delta)$ is odd).
(4) $\sqrt{gt\Delta}$ is real. ($\operatorname{sgn}(\Delta)$ is not a square and $\deg(\Delta)$ is odd).

A quadratic function field $\mathbb{F}_q(t)(\sqrt{D})$ is called **real** (resp. **imaginary**) if $\sqrt{D}$ is real (resp. **imaginary**). Throughout Artin's thesis many important results vary in form depending if the field is real or imaginary.

Integral elements and norms

Every element α of F can be expressed as $\alpha = A + B\sqrt{D}$, where $A, B \in \mathbb{F}_q[t]$. The (Galois) **conjugate** of α is the element $\alpha' = A - B\sqrt{D}$. The product $\alpha\alpha' = A^2 - B^2 D$ is called the **norm** of α, and it is denoted by $N(\alpha)$.

An element α of $\mathbb{F}_q(t)(\sqrt{D}) = F$ is said to be **integral** if there are $A_1, A_2 \in \mathbb{F}_q[t]$ such that

$$\alpha^2 + A_1\alpha + A_2 = 0.$$

A classic result that is true in this case is the following: if $\alpha \in \mathbb{F}_q(t)$ and is integral, then $\alpha \in \mathbb{F}_q[t]$, that is a rational integral function is a polynomial. A characterization of integral elements is given by Artin in the following result.

Proposition 1. [1, Satz p. 162] If $\alpha = A + B\sqrt{D} \in F$ is integral if and only if $A, B \in \mathbb{F}_q[t]$.

Observe that the norm of an integral element $\alpha = A + B\sqrt{D}$, is the polynomial $A^2 - B^2 D \in \mathbb{F}_q[t]$.

Units: Dirichlet obtained some important results on the units of rings of integers. Artin proposed a suitable analogy of these results to the case of quadratic function fields. We give the basic definition here.

An integer function $\alpha \in F$ is called a multiple of an integer function β (or β is a divisor of α) if one can find an integer function γ such that $\alpha = \beta\gamma$. A unit of $\mathcal{O}_F$ is a divisor of 1. A classic result is that an integer function ϵ is an unit if and only if $N(\epsilon)$ is a unit in the ring $\mathbb{F}_q[t]$.

Ideals following Artin: A system of integral functions in $F = \mathbb{F}_q(t)(\sqrt{D})$ is called an **ideal** if, whenever α_1, α_2 belong to the ideal, then $\gamma_1\alpha_1 + \gamma_2\alpha_2$ also belongs to the ideal, if γ_1, γ_2 are any elements of the field K. Equivalently, Artin showed the following.

Proposition 2. [1, Satz, p.164] Every ideal $\mathfrak{a}$ has a basis. That is, there are two elements ω_1, ω_2 of the field F such that

$$\mathfrak{a} = \{X\omega_1 + Y\omega_2 | X, Y \in \mathbb{F}_q[t]\}.$$

Artin's proof of this statement considers what he calls an *adapted* basis. Note that if α, an integral function, is an element of $\mathfrak{a}$, then $\alpha\alpha' = N\alpha$ also belongs to the ideal $\mathfrak{a}$, and therefore $\mathfrak{a}$ contains elements of $\mathbb{F}_q[t]$. For that we set T to be the greatest common divisor of the elements of $\mathbb{F}_q[t]$ that belong to $\mathfrak{a}$ [in modern words T is a generator of the ideal $\mathfrak{a} \cap \mathbb{F}_q[t]$]. Also we consider the term $R + S\sqrt{D} \in \mathfrak{a}$, where S is the greatest common divisor of all the coefficients with $\sqrt{D}$ of elements of $\mathfrak{a}$. Then we have that

$$\omega_1 = T \quad \omega_2 = R + S\sqrt{D},$$

is a basis of the ideal. Indeed, if $\alpha = A + B\sqrt{D}$ belongs to $\mathfrak{a}$ then B is a multiple of S, lets say $B = YS$, so $\alpha - Y\omega_2 = A - YR$ belongs to $\mathbb{F}_q[t] \cap \mathfrak{a}$, and therefore there is an polynomial X such that $\alpha - Y\omega_2 = XT$, and therefore we have $\alpha = X\omega_1 + Y\omega_2$. A condition for elements of this form to be a basis is given by the following result.

Proposition 3. [1, Satz p.165] The necessary and sufficient condition for $\omega_1 = T$ and $\omega_2 = R + S\sqrt{D}$ to be a basis of the ideal, is this: there exists polynomials A, B, C such that

$$T = 2CS, \quad R = BS, \quad \frac{B^2 - D}{2C} = 2A.$$

Then the basis has the form

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}) \quad \text{where } D = B^2 - 4AC.$$

In this case it can be proven that A, B, C have greatest common divisor equal to 1. The next result shows the relation between two bases of an ideal of $\mathcal{O}_F$.

Proposition 4. [1, Satz, p. 166] Let ω_1, ω_2 and ω_1^*, ω_2^* be two bases of an ideal $\mathfrak{a}$ in $\mathcal{O}_F$, then we have that

$$\begin{cases} \omega_1^* = A_1\omega_1 + A_2\omega_2 \\ \omega_2^* = B_1\omega_1 + B_2\omega_2, \end{cases}$$

where

$$a = \begin{vmatrix} A_1 & A_2 \\ B_1 & B_2 \end{vmatrix}$$

is an unit.

If ω_1, ω_2 is a basis of the ideal $\mathfrak{a}$, then we can prove the existence of the following expression:

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix} = a^2 \cdot (N\mathfrak{a})^2 \cdot D,$$

where a is a quadratic residue in $\mathbb{F}_q$ and $N\mathfrak{a}$ is a monic polynomial in $\mathbb{F}_q[t]$. Such element $N\mathfrak{a}$ is called by Artin the **norm** of the ideal $\mathfrak{a}$ and it coincides with the general definition that we gave above. Using the adapted basis given above, $\omega_1 = T = 2CS$, $\omega_2 = S(B + \sqrt{D})$, then a calculation shows that

$$N\mathfrak{a} = \frac{CS^2}{\operatorname{sgn}(CS^2)}.$$

If $\mathfrak{a}, \mathfrak{b}$ are ideals, then the product ideal $\mathfrak{ab}$ consists of functions of the form

$$\sum_{i=1}^{r} \gamma_i \alpha_i \beta_i,$$

where r is some positive integer, $\alpha_i \in \mathfrak{a}$, $\beta_i \in \mathfrak{b}$ and $\gamma_i \in F$, for all $i = 1, \cdots, r$. [check this!]. The conjugate ideal of $\mathfrak{a}'$ is the ideal that consists of the conjugates of elements of $\mathfrak{a}$. If ω_1, ω_2 is a basis of $\mathfrak{a}$ then ω_1', ω_2' is a basis of $\mathfrak{a}'$. If $\mathfrak{a} = \mathfrak{a}'$ then $\mathfrak{a}$ is called an **ambig** ideal (following Hilbert's Zahlbericht).

Proposition 5. [1, Satz 1,2 and 3. p. 168] If $\mathfrak{a}$ is an ideal then $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$, and therefore it is a principal ideal. Also, the norm of product of ideals is the product of the norms of the ideals, that is

$$N(\mathfrak{ab}) = N\mathfrak{a} \cdot N\mathfrak{b}.$$

Besides the norm of a principal ideal equals the norm of it's generator, that is

$$N((\alpha)) = N(\alpha).$$

Now we present several results concluded by Artin on the nature of the product of ideals.

If α, β are two integral functions, and $\mathfrak{a}$ is an ideal, we say $\alpha \equiv \beta (\text{mod } \mathfrak{a})$ if $\alpha - \beta$ belongs to $\mathfrak{a}$. If $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ we say that $\mathfrak{a}$ is a multiple of $\mathfrak{b}$, or that $\mathfrak{b}$ is a divisor of $\mathfrak{a}$. A prime ideal is an ideal with no divisors (other than the ideal (1).

Proposition 6. [1, Satz I-VII, p. 168-169]

I. If $(\gamma) \cdot \mathfrak{a} = (\gamma) \cdot \mathfrak{b}$, where $\gamma \in \mathcal{O}_F$, then $\mathfrak{a} = \mathfrak{b}$.
II. If $\mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b} \cdot \mathfrak{c}$, then $\mathfrak{a} = \mathfrak{b}$.
III. If $\mathfrak{b}$ is a divisor of $\mathfrak{a}$ and $\alpha \equiv 0 (\text{mod } \mathfrak{a})$, then $\alpha \equiv 0 (\text{mod } \mathfrak{b})$.
IV. An ideal $\mathfrak{a}$ has only a finite number of divisors.
V. When for every function β of the ideal $\mathfrak{b}$ we have that $\beta \equiv 0 \text{mod } \mathfrak{a}$, then $\mathfrak{b}$ is a multiple of the ideal $\mathfrak{a}$, and vice versa.
VI. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals, then we define the ideal $\mathfrak{d}$ to be formed by the union of all the functions that belong both to $\mathfrak{a}$ and $\mathfrak{b}$, clearly it determines all the properties of the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, so we write it as $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$. When $(\mathfrak{a}, \mathfrak{b}) = (1)$ we say that the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Then we can find functions $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha + \beta = 1$.
VII. When a product of ideals $\mathfrak{a}\mathfrak{b}$ is a multiple of a prime ideal $\mathfrak{b}$ then one of the factors must be a multiple of $\mathfrak{p}$.

With all of this, we can conclude the theorem on prime ideal factorization.

Proposition 7. [1, Satz, p. 169] Each ideal $\mathfrak{a}$ can be divided into one, and apart from the arrangement, only way into primary ideals.

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n.$$

Prime ideals and Legendre symbols:

The prime ideals of $\mathcal{O}_F$ are a somewhat strange object, however, the prime ideals of $\mathbb{F}_q[z]$ are not, because we know that the latter are principal ideals generated by an irreducible (or prime) monic polynomial of $\mathbb{F}_q[z]$. The ideals of $\mathcal{O}_F$ can be related to the ideals of $\mathbb{F}_q[z]$ (which is a subring of $\mathcal{O}_F$). To study that relationship we must define the Legendre and Jacobi symbols. The usual definition for those symbols is given in number theory, but we will remember it here.

Definition. (1) (**Usual Legendre and Jacobi Symbols**) If p is a prime number and $m \in \mathbb{Z}$ then the *Legendre symbol* is defined as

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{if } p|m \\ 1 & \text{if } p \not| m \text{ and } \exists n \in \mathbb{Z} \text{ such that } p \text{ divides } m - n^2. \\ -1 & \text{if } p \not| m \text{ and } \not\exists n \in \mathbb{Z} \text{ such that } p \text{ divides } m - n^2. \end{cases}$$

Now if $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geqslant 0}$ has a factorization in primes $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then we define the *Jacobi symbol as*

$$\left(\frac{m}{n}\right) := \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)^{\alpha_i}$$

Where we use the Legendre symbol in the product. Both symbols have the same notation.

(2) (**Legendre and Jacobi symbols for polynomials**) If P is a prime polynomial in $\mathbb{F}_q[x]$, and $M \in \mathbb{F}_q[x]$ then the *Legendre symbol* is defined as

$$[M/P] = \begin{cases} 0 & \text{if } P|M \\ 1 & \text{if } P \not| M \text{ and } \exists N \in \mathbb{F}_q[x] \text{ such that } P \text{ divides } M - N^2. \\ -1 & \text{if } P \not| M \text{ and } \nexists N \in \mathbb{F}_q[x] \text{ such that } P \text{ divides } M - N^2. \end{cases}$$

Now if $M, N \in \mathbb{F}_q[x]$ and N has a factorization in primes $N = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ then we define the *Jacobi symbol as*

$$[M/N] := \prod_{i=1}^{r} [M/P_i]^{\alpha_i}$$

Where we use the Legendre symbol in the product.

With this definition, we can state the following result, which will prove very helpful later.

Theorem 3. ***Relationship between prime ideals in*** $\mathcal{O}_F$ ***and prime ideals in*** $\mathbb{F}_q[z]$**.** *Let P be a prime monic polynomial in $\mathbb{F}_q[z]$ and D a polynomial in $\mathbb{F}_q[z]$ that is squarefree. Denote $P \cdot \mathcal{O}_F$ the principal ideal of $\mathcal{O}_F$ generated by P.*

(1) *If P divides D then there exists a unique prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ such that $P \cdot \mathcal{O}_F = \mathfrak{p}^2$. In this case $N\mathfrak{p} = P$ and $\mathfrak{p} = \langle P, \sqrt{D} \rangle$.*
(2) *If P and D are relatively prime and $\left[D/P\right] = 1$ then there are two different unique prime ideals of $\mathcal{O}_F$, $\mathfrak{p}, \mathfrak{p}'$ such that $P \cdot \mathcal{O}_F = \mathfrak{p}\mathfrak{p}'$, in this case $N\mathfrak{p} = N\mathfrak{p}' = P$, and also $\mathfrak{p} = \langle P, B + \sqrt{D} \rangle, \mathfrak{p}' = \langle P, B - \sqrt{D} \rangle$, where B is a solution of $X^2 \equiv D \ mod(P)$.*
(3) *If P and D are relatively prime and $\left[D/P\right] = -1$ then $P \cdot \mathcal{O}_F$ is a prime ideal in $\mathcal{O}_F$ and $P \cdot \mathcal{O}_F = \langle P, \sqrt{P} \rangle = \mathfrak{p}$, and $N\mathfrak{p} = P^2$.*

Furthermore, when P goes through all prime monic polynomials of $\mathbb{F}_q[z]$ the list of $\mathfrak{p}$ and $\mathfrak{p}'$ goes through all prime ideals of $\mathcal{O}_F$, that means that every prime ideal of $\mathcal{O}_F$ is present at the factorization of some prime ideal of $\mathbb{F}_q[z]$.

Ideal classes and the ideal class number: Now we turn to the concept of ideal classes, which proves to be very useful in handling the zeta function that we will define later.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called equivalent, if there are two integral functions α, β of the field F such that

$$(\beta) \cdot \mathfrak{a} = (\alpha) \cdot \mathfrak{b}.$$

We write it as

$$\mathfrak{a} \simeq \mathfrak{b}.$$

Also we write it with the symbolic relation

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta} = \varrho.$$

This is indeed an equivalence relation, and also some basic results follow:

(1) From $\mathfrak{a} \simeq \mathfrak{b}$ and $\mathfrak{b} \simeq \mathfrak{c}$ follows $\mathfrak{a} \simeq \mathfrak{b}$.
(2) From $\mathfrak{a} \simeq \mathfrak{b}$ and $\mathfrak{c} \simeq \mathfrak{d}$ follows $\mathfrak{ac} \simeq \mathfrak{bd}$.
(3) From $\mathfrak{ac} \simeq \mathfrak{bd}$ and $\mathfrak{a} \simeq \mathfrak{b}$ follows $\mathfrak{c} \simeq \mathfrak{d}$.
(4) From $\mathfrak{a} \simeq \mathfrak{b}$ it follows $\mathfrak{a}' \simeq \mathfrak{b}'$.
(5) The principal ideals (and only those) are all equivalent to the ideal (1).
(6) When $\frac{\mathfrak{a}}{\mathfrak{b}} = \varrho$ and ω_1, ω_2 is a basis of $\mathfrak{b}$, then $\varrho\omega_1, \varrho\omega_2$ is a basis of $\mathfrak{a}$.

With this (particularly property 2.) we can define the product of ideal classes. If $\mathfrak{K}_1, \mathfrak{K}_2$ are two ideal classes, the product $\mathfrak{K}_1\mathfrak{K}_2$ is the class formed by the products of ideals in $\mathfrak{K}_1$ with ideals of $\mathfrak{K}_2$. For the principal class $\mathfrak{K}_0$ (this is the class of the ideal (1)) we have that $\mathfrak{K}_0\mathfrak{K} = \mathfrak{K}$, and from 4. we can consider the conjugate class $\mathfrak{K}'$ of a class $\mathfrak{K}$. From the formula $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$ it follows $\mathfrak{K}\mathfrak{K}' = \mathfrak{K}_0$. All af this tells us that the ideal classes form an Abelian group (with inverse $\mathfrak{K}^{-1} = \mathfrak{K}'$). A class $\mathfrak{K}$ is called an ambige class if $\mathfrak{K} = \mathfrak{K}^{-1} = \mathfrak{K}'$.

An important result obtained by Artin in his thesis is the following.

Proposition 8. [1] In an imaginary field $\mathbb{F}_q(t)(\sqrt{D})$, the number h of ideal classes is finite. The number of ambige classes is also finite and when $D = aP_1P_2\cdots P_s$ is a factorization of D in to primes, it equals

$$2^{s-1} \quad \text{or} \quad 2^s,$$

depending on whether D divisible by an odd degree prime function or not. This is, for the group of ideal classes, the number of the **genus**. For the ideal class number h in both cases we have the expression

$$h = 2^{s-1} \cdot f \quad \text{or} \quad h = 2^s \cdot f,$$

where f is an integer. Therefore the ideal class number h can only be odd if D has odd degree.

Proposition 9. When D is square free and quadratic we have that $h = 2$.

Reciprocity laws and the numbers σ_v:

The Jacobi Symbol for polynomials satisfies the quadratic reciprocity law

$$[Q/P] = [P/Q] \cdot \left(\frac{-1}{p}\right)^{\deg Q \deg P}$$

where p is the characteristic of the field $\mathbb{F}_q$.

Actually, we can prove easily that if $v \geqslant \deg D = n$, then $\sigma_v = 0$. If $\deg Q \geqslant \deg D$ we can write $Q = kD + W$ where $W \in \mathbb{F}_q[z]$ with $\deg W = \deg Q$, and $k \in \mathbb{F}_q^\times$. Using the Reciprocity law that we mentioned above we have that

$$\begin{aligned}
\sigma_v = \sum_{\substack{Q \text{ monic} \\ \deg Q = v}} [D/Q] &= \left(\frac{-1}{p}\right)^{vn} \sum_{\substack{Q \text{ monic} \\ \deg Q = v}} [Q/D] \\
&= \left(\frac{-1}{p}\right)^{vn} \sum_{\substack{W \text{ monic} \\ \deg W = v \\ k \in \mathbb{F}_q^\times}} [(kD + W)/D] \\
&= \left(\frac{-1}{p}\right)^{vn} \sum_{\substack{W \text{ monic} \\ \deg W = v \\ k \in \mathbb{F}_q^\times}} [W/D] \\
&= \left(\frac{-1}{p}\right)^{vn} \#\mathbb{F}_q^\times \sum_{\substack{W \text{ monic} \\ \deg W = v}} [W/D] \\
&= \left(\frac{-1}{p}\right)^{vn} \#\mathbb{F}_q^\times \sigma_v
\end{aligned}$$

This implies that $\sigma_v = 0$. We used the periodicity equality: $[(kD + W)/D] = [W/D]$, which is easy to prove from the definition of the Jacobi symbol.

2.5. **Artin's zeta function for quadratic function fields.** With the definitions of the last part, it's very natural to define the zeta function for the quadratic function field $F = \mathbb{F}_q(z)(\sqrt{D})$, this is simply

$$Z_F(s) := \sum_{I \in I_F} \frac{1}{|N_{F/\mathbb{F}_q(z)}(I)|^s}$$

Where I_F is the set of non-zero ideals of the ring $\mathcal{O}_F$ of algebraic integers of F, and in the sums we have the absolute norms of those ideals. It is with the definition of this function that our journey begins, and that is because of the many interesting features that this function has to offer. To start we will present in here a method for an explicit calculation of this function, devised by

Artin. With this procedure he proved, in a fairly comprehensible way, that this infinite series is actually a rational function (in a certain variable).

First, because of the factorization in prime ideals that occurs in I_K we can write the zeta function as

$$\prod_{\mathfrak{p}} \frac{1}{1-|N_{K/\mathbb{F}_q(z)}(\mathfrak{p})|^{-s}}$$

where the product is taken over all prime ideals of $\mathcal{O}_F$. Now we will proceed to make some calculations. Select a prime polynomial $P \in \mathbb{F}_q[z]$. Using the last theorem we have three cases to consider.

(1) If P, which we identify with the principal ideal $P \cdot \mathcal{O}_F$ in $\mathcal{O}_F$, is such that $[D/P] = 1$ then it has a factorization $P \cdot \mathcal{O}_F = \mathfrak{p}\mathfrak{p}'$ with $\mathfrak{p}, \mathfrak{p}'$ are different prime ideals in R, then we have $N\mathfrak{p} = N\mathfrak{p}' = P$, therefore

$$\frac{1}{1-|N\mathfrak{p}|^{-s}} \cdot \frac{1}{1-|N\mathfrak{p}'|^{-s}} = \frac{1}{1-|P|^{-s}} \cdot \frac{1}{1-|P|^{-s}} = \frac{1}{1-|P|^{-s}} \cdot \frac{1}{1-[D/P]\cdot|P|^{-s}}$$

(2) If we have the situation $[D/P] = -1$ then $P \cdot \mathcal{O}_F = \mathfrak{p}$

$$\frac{1}{1-|N\mathfrak{p}|^{-s}} = \frac{1}{1-|P|^{-2s}} = \frac{1}{1-|P|^{-s}} \cdot \frac{1}{1+|P|^{-s}} = \frac{1}{1-|P|^{-s}} \frac{1}{1-[D/P]\cdot|P|^{-s}}$$

(3) Finally if P divides D, that is $[D/P] = 0$, then $P \cdot \mathcal{O}_F = \mathfrak{p}^2$, $N\mathfrak{p} = P$ and therefore

$$\frac{1}{1-|N\mathfrak{p}|^{-s}} = \frac{1}{1-|P|^{-s}} = \frac{1}{1-|P|^{-s}} \cdot \frac{1}{1-[D/P]\cdot|P|^{-s}}$$

We note that we used that $N(P \cdot \mathcal{O}_F) = P$. When we go through all prime monic polynomials of $\mathbb{F}_q[z]$, all of these cases exhaust the possibilities for $\mathfrak{p}$, because of the previous theorem, so we can decompose the Euler product for the Zeta function as

$$\zeta_F(s) = \prod_P \frac{1}{1-|P|^{-s}} \cdot \prod_P \frac{1}{1-[D/P]\cdot|P|^{-s}}$$

Using that the absolute value function $|\cdot|$ and the Jacobi Symbol $[D/\cdot]$ are both multiplicative functions and also that every monic polynomial $Q \in \mathbb{F}_q[z]$ can be factored as a product of prime monic polynomials, we have that these two products can be written as

$$Z_F(s) = \sum_Q \frac{1}{|Q|^s} \cdot \sum_Q \frac{[D/Q]}{|Q|^s}$$

where the sums go through all monic polynomials in $\mathbb{F}_q[z]$. Given that we are working over a finite field, it's easy to see that there are q^v polynomials of degree v in $\mathbb{F}_q[z]$, so the first sum is equal to

$$\sum_{v=0}^{\infty} \frac{q^v}{q^{vs}} = \frac{1}{1-q^{-(s-1)}}$$

The second sum can be rewritten as

$$\sum_{Q} \frac{[D/Q]}{|Q|^s} = \sum_{v=0}^{\infty} \frac{\sigma_v}{q^{vs}}$$

where

$$\sigma_v := \sum_{\substack{Q \text{ monic} \\ \deg Q = v}} [D/Q].$$

So putting all of this together we have that

$$Z_F(s) = \frac{1}{1-q^{-(s-1)}} \cdot \sum_{v=0}^{\infty} \frac{\sigma_v}{q^{vs}}.$$

In the last subsection we proved that if $v \geqslant \deg D = n$, then $\sigma_v = 0$, thus finally we have that

$$Z_F(s) = \frac{1}{1-q^{-(s-1)}} \cdot \sum_{v=0}^{n-1} \frac{\sigma_v}{q^{sv}}. \tag{8}$$

The term σ_0 is equal to 1, and the other terms can be calculated (although not very easily). Naturally this is quite an easier version to work with than our original version of the zeta function, which involved an infinite series. Note that this function is a rational function on the variable q^{-s}, so if $u = q^{-s}$ we can make a change of variable to obtain the function

$$Z_F(u) := \frac{\sigma_0 + \sigma_1 u + \cdots + \sigma_{n-1} u^{n-1}}{1 - qu}$$

This expression will become very common in the treatment ahead. For now, let us be content with this simple form and proceed to investigate what can be done with it.

2.6. **First properties of the Zeta function.** Now we present some initial features of the zeta function introduced by Artin.

Formulas for the ideal class number

Proposition 10. [2, p. 216-217] Let h be the ideal class number of an imaginary quadratic function field $F = \mathbb{F}_q(t)(\sqrt{D})$. Then,

(1) If $D = g$, then

$$h = \sum_{v=0}^{n-1} \sigma_v.$$

[Check this in page 216 at the start].

(2) If the degree of D is odd, then

$$h = \sqrt{\frac{|D|}{q}} \cdot \sum_{v=0}^{n-1} \frac{\sigma_v}{q^v}.$$

(3) If the degree of D is even, then

$$h = \frac{2\sqrt{|D|}}{q+1} \cdot \sum_{v=0}^{n-1} \frac{\sigma_v}{q^v}.$$

A way to prove it is to consider the auxiliary functions

$$Z_F(s, \mathfrak{K}) := \sum_{\mathfrak{a} \in \mathfrak{K}} \frac{1}{|N\mathfrak{a}|^s},$$

where $\mathfrak{K}$ is an ideal class. Then we have

$$Z_F(s) = \sum_{\mathfrak{K}} Z_F(s, \mathfrak{K}).$$

Functional equation for the Zeta function and relations between the numbers σ_v.

Theorem 4 (Functional Equation)**.** *Consider the quadratic function field $F = \mathbb{F}_q(t)(\sqrt{D})$.*

Case I. *If F is an imaginary field.*

I.I *If the degree of D is odd, then*

$$Z_F(1-s) = \frac{1 - q^{-(s-1)}}{1 - q^s} \left(\sqrt{\frac{|D|}{q}}\right)^{2s-1} Z(s).$$

I.II *If the degree of D is even, then*

$$Z_F(1-s) = \frac{1 - q^{-2(s-1)}}{1 - q^{2s}} \left(\sqrt{|D|}\right)^{2s-1} Z(s).$$

Case II. *If F is a real field, then*

$$Z_F(1-s) = \left(\frac{1 - q^{-(s-1)}}{1 - q^s}\right)^2 \left(\sqrt{|D|}\right)^{2s-1} Z(s).$$

Theorem 5 (Relations between the numbers σ_v)**.** *Consider the quadratic function field $F = \mathbb{F}_q(t)(\sqrt{D})$.*

I. *If $|D| = q^{2m+1}$ (F real or imaginary), then for every $0 \leqslant v \leqslant 2m$, we have that*

$$\sigma_{2m-v} = q^{m-v}\sigma_v,$$

in particular, given that $\sigma_0 = 1$, we have that $\sigma_{2m} = q^m$.

II. *If* $|D| = q^{2m}$ *(*F *imaginary), then*

$$\sigma_{2m-v} + q\sigma_{2m-v-1} = q^{m-v}(\sigma_v + q\sigma_{v-1}) \quad \textit{for } 1 \leqslant v \leqslant 2m-1, \textit{ and}$$
$$\sigma_{2m-1} = q^{m-1}.$$

This can be written as the formula

$$\sigma_{2m-v} = q^{m-v}[\sigma_{v-1} + (q-1)(\sigma_{v-2} - \sigma_{v-3} + \sigma_{v-4} - \cdots + (-1)^{v-2}\sigma_0)],$$
$$\textit{for } 2 \leqslant v \leqslant 2m.$$

III. *If* $|D| = q^{2m}$ *(*F *real), then*

$$\sigma_{2m-v} - q\sigma_{2m-v-1} = q^{m-v}(\sigma_v - q\sigma_{v-1}) \quad \textit{for } 1 \leqslant v \leqslant 2m-1, \textit{ and}$$
$$\sigma_{2m-1} = -q^{m-1}.$$

This can be written as the formula

$$\sigma_{2m-v} = q^{m-v}[-\sigma_{v-1} + (q-1)(\sigma_{v-2} + \sigma_{v-3} + \sigma_{v-4} + \cdots + \sigma_1 + \sigma_0)],$$
$$\textit{for } 2 \leqslant v \leqslant 2m.$$

This last theorem is important because it allows us to calculate the numbers σ_v (and subsequently the zeta function) in a more efficient way than doing it by definition (which can be rather long).

The number of ideals with a given absolute norm Lets set the number $H(x)$ to be the number of ideals with $|N\mathfrak{a}| = x$. Clearly this implies that

$$Z_F(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s} = \sum_{v=0}^{\infty} \frac{H(p^v)}{p^{vs}},$$

and from the rational expression of the zeta function, it follows that for $v \geqslant n-1$

$$H(q^v) = q^v\sigma_0 + q^{v-1}\sigma_1 + \cdots + q^{v-(n-1)}\sigma_{n-1} = q^v \sum_{\mu=0}^{n-1} \frac{\sigma_\mu}{q^\mu} = \frac{h}{\chi} q^v,$$

where (using the formulas for the ideal class number) the number χ is given by [2]

$$\chi = \begin{cases} \frac{2\sqrt{|D|}}{q+1} & F \text{ imaginary and the degree of } D \text{ is even.} \\ \sqrt{\frac{|D|}{q}} & F \text{ imaginary and the degree of } D \text{ is odd.} \end{cases}$$

Given that the absolute norm is always a power of q we have proven that

$$H(x) = \frac{h}{\chi} x \quad \text{for} \quad x \geqslant \frac{|D|}{q}.$$

[2]There is also the real case but it uses the theorem of units in $\mathcal{O}_F$ which we will not discuss here.

As we said before, when handling the rational form of the zeta function we can consider the polynomial

$$z^{n-1} + \sigma_1 z^{n-2} + \sigma_2 z^{n-3} + \cdots + \sigma_{n-1}.$$

If $\beta_1, \beta_2 \cdots, \beta_{n-1}$ are the roots of this polynomial, then each $\beta_v = q^{\varrho}$, where ϱ is a root of Z_F. Then we can consider the trivial zeros, those with $\mathrm{Re}(s) = 0$. When D is linear, quadratic or cubic, there are no such zeros. Also, when D has odd degree there are no trivial zeros, but if the degree is even (in the real or imaginary case) there are trivial zeros. Let θ be the supremum of the real parts of the zeros of $Z_F(s)$. Apart from the exceptional cases when there are trivial roots, we have that

$$\frac{1}{2} \leqslant \theta \leqslant 1,$$

and also

$$|\beta_v| \leqslant q^{\theta}.$$

Observe that we can express $Z_F(s)$ with the product representation

$$Z_F(s) = \frac{1}{1 - q^{-(s-1)}} \prod_{v=1}^{n-1} (1 - \beta_v q^{-s}).$$

From this it follows that

$$\begin{aligned} \log Z_F(s) &= -\log(1 - q^{-(s-1)}) + \sum_{\nu=1}^{n-1} \log(1 - \beta_\nu q^{-s}) \\ &= \sum_{v=1}^{\infty} \frac{q^v - \beta_1^v - \beta_2^v - \cdots \beta_{n-1}^v}{v q^{vs}} \quad \text{for } Re(s) > 1. \end{aligned}$$

Now, let's define $\pi(x)$ to be the number of prime ideals of $\mathcal{O}_F$ with absolute norm equal to x. Using the Euler product factorization for $Z_F(s)$ we have that

$$\begin{aligned} \log Z_F(s) = -\sum_{\mathfrak{p}} \log(1 - |N\mathfrak{p}|^{-s}) = \sum_{\mathfrak{p}, v \geqslant 1} \frac{1}{|N\mathfrak{p}|^{vs}} \\ &= \sum_{v=1}^{\infty} \frac{\sum_{d|v} \frac{\pi(q^d)}{\frac{v}{d}}}{q^{vs}} \\ &= \sum_{v=1}^{\infty} \frac{\sum_{d|v} d\pi(q^d)}{v q^{vs}} \quad \text{for } Re(s) > 1. \end{aligned}$$

And finally, using both expressions for $\log Z_F(s)$ we have the formula

$$\sum_{d|v} d\pi(q^d) = q^v - \beta_1^v - \beta_2^v - \cdots \beta_{n-1}^v, \tag{9}$$

which, according to Artin, is an analogue of the Riemann-von Mangoldt formula for the Riemann zeta function $\zeta(s)$. Finally we present an asymptotic result related to the function $\pi(x)$, that is analogous to the prime number theorem.

Theorem 6. *If x is a power of q and $\pi(x)$ denotes the number of prime ideals of $\mathcal{O}_F$ with absolute norm equal to x, then the function π fulfils the asymptotic formula*

$$\pi(x) = \frac{x}{\log x}\log q + O\left(\frac{x^\theta}{\log x}\right),$$

where $\frac{1}{2} \leqslant \theta \leqslant 1$.

Proof. According to our results on the norm of prime ideals, $\pi(q^d)$ is now at most double the number of prime polynomials of degree d plus the number of prime polynomials of degree $d/2$. And therefore we can find an absolute constant C such that

$$\pi(q^d) \leqslant C\frac{q^d}{d}.$$

Considering divisors of v different than 1 and the former bound we see that

$$\begin{aligned}
&\frac{v}{2}\pi(q^{\frac{v}{2}}) + \frac{v}{3}\pi(q^{\frac{v}{3}}) + \cdots + \frac{v}{v}\pi(q^{\frac{v}{v}}) \\
&\leqslant C(q^{\frac{v}{2}} + q^{\frac{v}{3}} + \cdots + q^{\frac{v}{v}}) \\
&\leqslant C(q^{\frac{v}{2}} + vq^{\frac{v}{3}}) = O(q^{v/2}).
\end{aligned}$$

And therefore, using equation (9) it follows that

$$v\pi(q^v) + O(p^{\frac{v}{2}}) = p^v - \beta_1^v - \beta_2^v - \cdots - \beta_{n-1}^v,$$

however we know that

$$|\beta_\mu^v| \leqslant q^{\theta v},$$

where θ is the supremum of the real parts of the zeros of $Z_F(s)$, and therefore we have

$$v\pi(q^v) = q^v + O(q^{\frac{v}{2}}) + O(q^{\theta v}) = p^v + O(p^{\theta v})$$

or

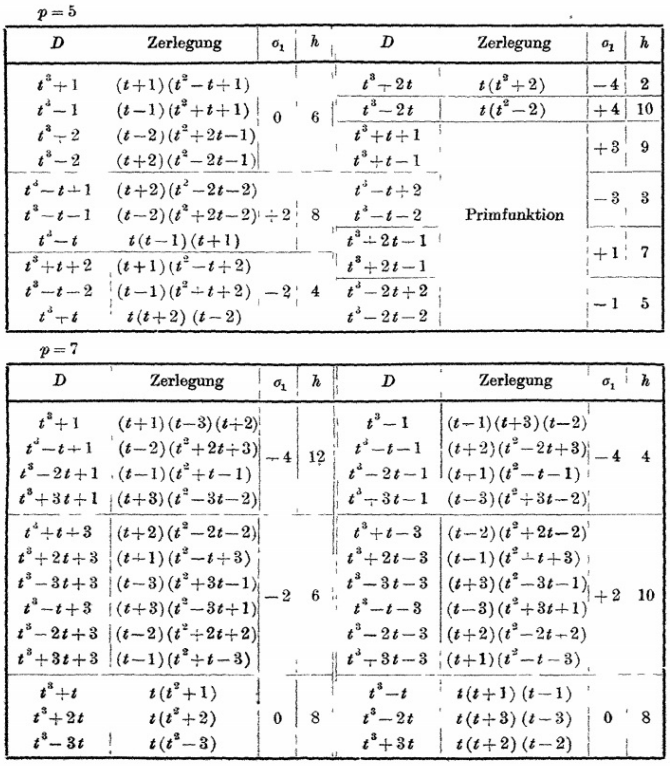
$$\pi(q^v) = \frac{q^v}{v} + O\left(\frac{q^{\theta v}}{v}\right),$$

This gives us the desired formula if $x = q^v$. □

2.7. **The Riemann Hypothesis.** To make things a bit more concrete, now let us compute some zeta functions for various algebraic function fields of the form $\mathbb{F}_q(x)(\sqrt{D})$, that is quadratic function fields. Hopefully a pattern on the behaviour of these functions will be discovered.

As we see, all of these zeta functions fulfil the Riemann Hypothesis, and actually this is no surprise, this is part of the Weil conjectures we mentioned earlier. How was this fact discovered? It was discovered by Artin in his thesis. He performed concrete calculations for 36 polynomials and noticed this impressive condition. We show some of his calculations in the next figure. Above we

provided those calculations for more complicated examples, thanks to the advantage of computer calculation.



$p = 5$

D	Zerlegung	σ_1	h	D	Zerlegung	σ_1	h
t^2+1	$(t+1)(t^2-t+1)$			t^3+2t	$t(t^2+2)$	-4	2
t^4-1	$(t-1)(t^2+t+1)$	0	6	t^3-2t	$t(t^2-2)$	$+4$	10
t^3+2	$(t-2)(t^2+2t-1)$			t^3+t+1		$+3$	9
t^3-2	$(t+2)(t^2-2t-1)$			t^3+t-1			
t^4-t+1	$(t+2)(t^2-2t-2)$			t^3-t+2		-3	3
t^3-t-1	$(t-2)(t^2+2t-2)$	$+2$	8	t^3-t-2	Primfunktion		
t^4-t	$t(t-1)(t+1)$			t^3+2t-1		$+1$	7
t^3+t+2	$(t+1)(t^2-t+2)$			t^3+2t-1			
t^3-t-2	$(t-1)(t^2+t+2)$	-2	4	t^3-2t+2		-1	5
t^3+t	$t(t+2)(t-2)$			t^3-2t-2			

$p = 7$

D	Zerlegung	σ_1	h	D	Zerlegung	σ_1	h
t^2+1	$(t+1)(t-3)(t+2)$			t^3-1	$(t-1)(t+3)(t-2)$		
t^4-t+1	$(t-2)(t^2+2t+3)$	-4	12	t^4-t-1	$(t+2)(t^2-2t+3)$	-4	4
t^3-2t+1	$(t-1)(t^2+t-1)$			t^3-2t-1	$(t+1)(t^2-t-1)$		
t^3+3t+1	$(t+3)(t^2-3t-2)$			t^3+3t-1	$(t-3)(t^2+3t-2)$		
t^4+t+3	$(t+2)(t^2-2t-2)$			t^3+t-3	$(t-2)(t^2+2t-2)$		
t^3+2t+3	$(t+1)(t^2-t+3)$			t^3+2t-3	$(t-1)(t^2+t+3)$		
t^3-3t+3	$(t-3)(t^2+3t-1)$			t^3-3t-3	$(t+3)(t^2-3t-1)$		
t^3-t+3	$(t+3)(t^2-3t+1)$	-2	6	t^3-t-3	$(t-3)(t^2+3t+1)$	$+2$	10
t^3-2t+3	$(t-2)(t^2+2t+2)$			t^3-2t-3	$(t+2)(t^2-2t+2)$		
t^3+3t+3	$(t-1)(t^2+t-3)$			t^3+3t-3	$(t+1)(t^2-t-3)$		
t^3+t	$t(t^2+1)$			t^3-t	$t(t+1)(t-1)$		
t^3+2t	$t(t^2+2)$	0	8	t^3-2t	$t(t+3)(t-3)$	0	8
t^3-3t	$t(t^2-3)$			t^3+3t	$t(t+2)(t-2)$		

FIGURE 4. Some of Artin's Original Calculations

However Artin did not provide a proof for this result an it seems that after working on his doctoral thesis he devoted to other subjects. Other mathematicians would continue with the task of proving this assertion and other features of the zeta function. We can discuss the case where the degree of D is small, like 2 or 3.

From the last section we know that $\sigma_{2m} = p^m$ if the degree of D equals $2m + 1$. If, for example, $\deg D = 3$, then we have $\sigma_2 = p$, hence in this case we can express the zeta function as

$$Z_F(s) = \frac{1}{1-p^{1-s}} \cdot \left(1 + \frac{\sigma_1}{p^s} + \frac{p}{p^{2s}}\right) = \frac{1}{p^{2s}(1-p^{1-s})} \cdot (z^2 + \sigma_1 z + p)$$

where $z = p^s$. We see that the roots of the polynomial $Q(z) = z^2 + \sigma_1 z + p$ are

$$\beta = \frac{-\sigma_1}{2} \pm \frac{1}{2}\sqrt{\sigma_1^2 - 4p}$$

If the following inequality were true

$$|\sigma_1| < 2\sqrt{p} \tag{10}$$

That is, if the discriminant of the polynomial Q is negative, then a root s of Z must have $\mathrm{Re}(s) = 1/2$, because if $s = a + bi$ then $p^s = \beta$ implies

$$(a+bi)\log p = \log(|\beta|) + i\arg\beta = \frac{1}{2}\log p + i\arg\beta$$

and therefore $a = 1/2$. So, in order to prove the Riemann hypothesis in the case where $\deg D = 3$, we would need to prove inequality 10. This was recognized by Artin, but the proof for this inequality came some years later, thanks to the work of the German mathematician Helmut Hasse.

Actually, the number σ_1 counts the number of solutions of certain polynomial in $\mathbb{F}_q[x,y]$. If $D = x^3 + ax^2 + bx + c$ then to compute σ_1 we note that

$$\sigma_1 = \sum_{d=0}^{p-1}\Big[\frac{x^3+ax^2+bx+c}{x-d}\Big] = \sum_{d=0}^{p-1}\Big[\frac{d^3+ad^2+bd+c}{x-d}\Big] = \sum_{d=1}^{p-1}\Big(\frac{d^3+ad^2+bd+c}{p}\Big)$$

Indeed, the first equality comes from the fact that this Jacobi symbol is periodic in the polynomial in the denominator, specifically this means that

$$\Big[\frac{M+SN}{N}\Big] = \Big[\frac{M}{N}\Big]$$

for all $M, N, S \in K[x]$. The second equality because if $\alpha \in \mathbb{F}_p$ is a quadratic residue mod $(t-c)$ then there are polynomials q, r such that $\alpha = r(t)^2 + (t-c)q(t)$, evaluating in $t = c$ gives α a quadratic residue mod p. And conversely if $\alpha = m^2, m \in \mathbb{F}_p$ then we can take $r(t) = m$ and $q(t) = 0$ so that $\alpha = r(t)^2 + (t-c)q(t)$ and therefore α is a quadratic residue mod $(t-c)$. If $f(x,y)$ is the polynomial $f(x,y) = y^2 - D(x) = y^2 - x^3 - ax^2 - bx - c$, then, the number of solutions of f in $\mathbb{F}_p^2$ can be counted using the Legendre symbol and is equal to

$$N_q(f) = \sum_{d=0}^{p-1}\Big[1 + \Big(\frac{d^3+ad^2+bd+c}{p}\Big)\Big] = p + \sigma_1$$

So we can write inequality (10) as

$$|N_p(f) - p| < 2p^{1/2}.$$

Hasse proved the more general inequality,

$$|N_{p^n}(f) - p^n| < 2p^{n/2}$$

for all $n \in \mathbb{Z}_{>0}$.

2.8. **The zeta function and the counting problem.** The reader might ask what does the theory of algebraic function fields contributes to the problem of counting solutions to curves over finite fields, which was the problem we set out to study initially. We expect that the relationship becomes clearer in the following sections, but for now we can give a small hint. Remember our base example: the circle x^2+y^2-1, this is a polynomial in $\mathbb{F}_q[x,y]$. This polynomial can be seen also as a polynomial in the variable y with coefficients in $\mathbb{F}_p[x]$, so let's look at it in that way. Then a 'solution' to this

polynomial will be a member of a finite extension of the field $\mathbb{F}_q(x)$, namely it will be $\sqrt{1-x^2}$, therefore we can assign the algebraic function field $\mathbb{F}_q(x)(\sqrt{1-x^2})$ to the circle. Any curve $f(x,y)$ can be seen as a polynomial in the variable y with coefficients in $\mathbb{F}_q[x]$, so, by considering solutions to this polynomial, we can create a particular algebraic function field related to this initial curve.

This algebraic function field is what is known as the *field of functions* of V. It can be constructed more generally. If V is an algebraic irreducible variety, let's say affine for the moment, and is given by the zeros of the ideal $\mathfrak{a}$ of $\mathbb{F}_q[x_1, \cdots, x_n]$ then the *Coordinate ring of* V is the ring

$$\Gamma(V) = \frac{\mathbb{F}_q[x_1, \cdots, x_n]}{\mathfrak{a}}$$

which is an integral domain. Then the field of functions of V, denoted $\mathbb{F}_q(V)$ is the field of fractions of $\Gamma(V)$. In the case of the circle it can easily seen to be isomorphic to the field $\mathbb{F}_q(x)(\sqrt{1-x^2})$. It turns out that there is an important connection between counting the number of solutions of a polynomial (points in projective space satisfied by the homogenization of the curve) and observing the nature of the algebraic function field attached to this polynomial. This is our primary motivation to use the theory we have presented previously.

Artin Zeta function can be writen as

$$Z_F(s) = \prod_{\mathfrak{p}} \frac{1}{1-|N\mathfrak{p}|^{-s}} = \prod_{\mathfrak{p}} \frac{1}{1-(\#\mathcal{O}_F/\mathfrak{p})^{-s}}$$

If $b_n = \#\{\mathfrak{p} : \#(\mathcal{O}_K/\mathfrak{p}) = q^n\} = \{\mathfrak{p} : [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_q] = n\}$ (which is a finite number) then we can express the zeta function as

$$Z_F(s) = \prod_{n=1}^{\infty} \left(\frac{1}{1-q^{-sn}}\right)^{b_n}.$$

If $u = q^{-s}$ then

$$Z_F(u) = \prod_{n=1}^{\infty} \left(\frac{1}{1-u^n}\right)^{b_n},$$

taking logarithms and rearranging we would have that

$$\log Z_F(u) = \sum_{m=1}^{\infty} \frac{\left(\sum_{n|m} n b_n\right) u^m}{m}.$$

Finally, our initial expression

$$Z_F(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m u^m}{m}\right)$$

becomes a consequence of the following result.

Proposition 11. If V is an affine algebraic variety over $\mathbb{F}_q$, N_m is the number of affine points of V over the field $\mathbb{F}_{q^m}$ and F is the field of functions of V over $\mathbb{F}_q$ (an algebraic function field) then

$$N_m = \sum_{n|m} nb_n$$

where

$$b_n = \#\{\mathfrak{p} \in \text{Spec}(\mathcal{O}_F) : [\mathcal{O}_F/\mathfrak{p} : \mathbb{F}_q] = n\}$$

For the proof we use an argument given in [5, p.157] together with an application of Hilbert's Nullstellensatz. Let us consider the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. Generally it is written as

$$\overline{\mathbb{F}_q} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{q^n}.$$

We will consider the algebraic variety $\overline{V}$ over $\overline{\mathbb{F}_q}$, that is the set of $\mathbb{A}^n(\overline{\mathbb{F}_q})$ defined by the same equations that define V. If $\alpha = (a_1, \cdots, a_n) \in \overline{V}$, we say that $\deg(\alpha) = d$ if $\mathbb{F}_{q^d}$ is the smallest field that contains all of the a_i. In this case $\alpha^{q^j} = (a_1^{q^j}, \cdots, a_n^{q^j})$ is still an element of $\overline{V}$ of degree $\deg(\alpha^{q^j}) = d$, for $j = 0, 1, \cdots, d-1$. A set of the form $\mathfrak{P} = \{\alpha^{q^j} | j = 0, 1, \cdots, d-1\}$ for some α of degree d is called a *prime zero cycle of degree* d over $\mathbb{F}_q$. Observe that all of these elements are different, so each $\mathfrak{P}$ of degree d has d elements. Actually this set non other than the orbit $\mathfrak{P} = [\alpha]$ of the element α under the action of the Galois group $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ over $\overline{V}$.

Lemma 1. Let $\Gamma(V)$ be the coordinate ring of an affine variety V defined over $\mathbb{F}_q[x_1, \cdots, x_n]$. Consider the algebraic closure $\overline{\mathbb{F}_q}$ and let $\overline{V}$ the affine variety defined over $\overline{\mathbb{F}_q}$ by the same equations as in V.

(1) Every maximal ideal of $\Gamma(V)$ is of the form

$$\mathfrak{m} = \frac{ker(ev_\alpha)}{\mathfrak{a}},$$

for some $\alpha \in \overline{V}$. Where ev_α is the evaluation map

$$ev_\alpha : \mathbb{F}_q[x_1, \cdots, x_n] \to \overline{\mathbb{F}_q}$$
$$f(x_1, x_2, \cdots, x_n) \mapsto f(\alpha) = f(a_1, a_2, \cdots, a_n).$$

(2) There is a correspondence

$$\mathfrak{m} = \frac{ker(ev_\alpha)}{\mathfrak{a}} \to \mathfrak{P} = [\alpha] = \{\alpha^{q^j} | j = 0, 1, \cdots, d-1\},$$

between maximal ideals of $\Gamma(V)$ and orbits of elements of $\overline{V}$ under the Galois action of $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. This correspondence is such that

$$[\Gamma(V)/\mathfrak{m} : \mathbb{F}_q] = \deg(\mathfrak{P}).$$

Proof. See [11]. □

This lemma gives us the proof of our proposition. Indeed a point α in N_m, lies in its orbit $[\alpha] = \mathfrak{P}$, where $\mathfrak{P}$ is of degree d, for some divisor d of m (the smallest field $\mathbb{F}_d$ such that $\alpha \in \mathbb{A}^n(\mathbb{F}_{q^d})$ is contained in $\mathbb{F}_{q^m}$ so $d|m$. By the correspondence it is linked to an unique prime (therefore maximal) ideal $\mathfrak{p}$ such that $[\Gamma(V)/\mathfrak{p} : \mathbb{F}_q] = d$. Noticing that $\Gamma(V) = \mathcal{O}_F$ of course. Now in each orbit $\mathfrak{P}$ of degree d there are exactly d points which are all in $V(\mathbb{F}_{q^d}) = \mathbb{A}^n(\mathbb{F}_{q^d}) \cap \overline{V}$, so each such prime ideal is associated to d points in $V(\mathbb{F}_{q^m})$, clearly this gives us the desired formula.

The results of this proposition can be visualized in the following figure.

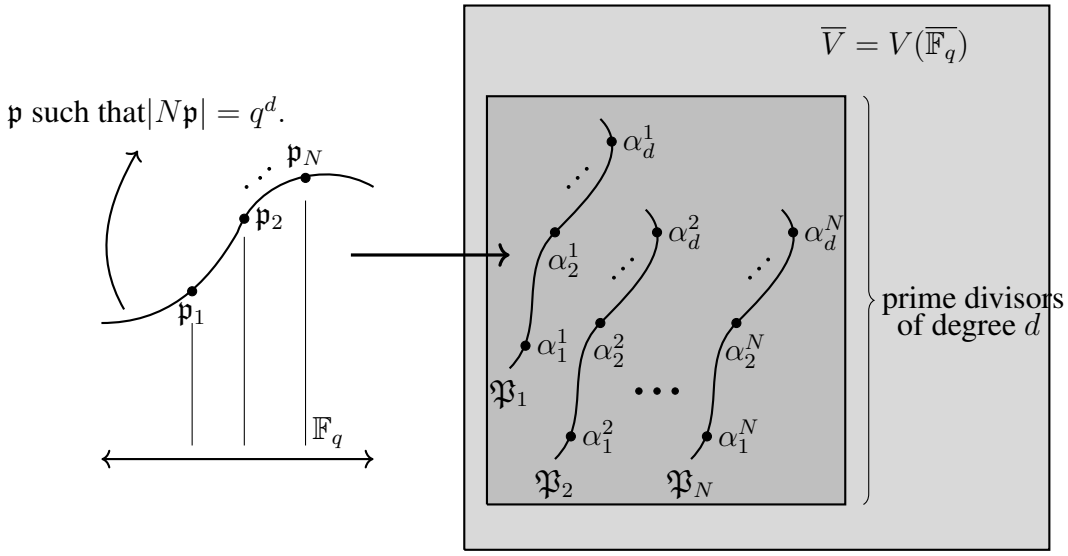


FIGURE 5. Galois orbits of points defined over $\overline{\mathbb{F}_p}$ and their correspondence with maximal ideals. Here $N = \pi(q^d)$.

Note that if $[\mathcal{O}_F/\mathfrak{p} : \mathbb{F}_q] = n$, then $\#\mathcal{O}_F/\mathfrak{p} = q^n$, and that is $|N\mathfrak{p}| = q^n$, therefore $b_n = \pi(q^n)$. In the case V given by the curve $y^2 - D(x)$, so $F = \mathbb{F}_q(t)(\sqrt{D(t)}$, from the rationality of the zeta function and the formula (9) we see that

$$N_m = q^m - \beta_1^m - \beta_2^m - \cdots - \beta_{n-1}^m.$$

This gives us then a nice formula to find the numbers N_m! Actually this can be done in general (not just for a curve $y^2 - D(x)$. The rationality part of the conjectures is of great importance when it comes to calculating the number of solutions of a curve. This observation can be found in [5]. If the zeta function

$$Z(u) = \exp\Big(\sum_{n=1}^{\infty} \frac{N_n u^n}{n}\Big)$$

were a rational function

$$Z(u) = \frac{\prod_{i=1}^{m}(1 - \alpha_i u)}{\prod_{j=1}^{r}(1 - \beta_j u)}$$

Then by a simple process of logarithmic derivatives, one can conclude that for every n we would have

$$N_n = \sum_{j=1}^{r} \beta_j^n - \sum_{i=1}^{m} \alpha_i^n.$$

See this argument in [5, Proposition 11.1.1, p.155]. Therefore, if we have the explicit form of the Zeta function of a curve, we can calculate it's zeros N_n by just looking at the complex roots of the polynomials in the rational expression for Z, and so calculating those zeros becomes an easy task, provided we have such a rational expression!

3. Schmidt's Generalization

3.1. **Historical motivation.** In 1931, a german mathematician named Friedrich Karl Schmidt, published the article *Analytische Zahlentheorie in Körpern del Charakteristik p* [8], which translates to Analytic Number Theory in Fields of Characteristic p. The goal of his work was to extend the examinations made by Artin to the general case of a finite field extension F of the field $\mathbb{F}_q(t)$. In this section we will take a careful look at his work.
Let us consider F a finite field extension of $\mathbb{F}_q(t)$, as we defined earlier, and $\mathcal{O}_F$ the integral closure of $\mathbb{F}_q[t]$ in F. As before we could define the zeta function of this field as

$$Z_F(s) = \sum_{I \in I_F} \frac{1}{|N_{F/\mathbb{F}_q(t)}(I)|^s}$$

where I_F is the set of non-zero ideals of $\mathcal{O}_F$. This is what we will call the Artin zeta function for the field F. As we saw above, this Zeta function gives us a tool to count the affine points of a curve in a finite field, however it becomes insufficient when trying to include in the count the projective points. Schmidt solved this problem by means of the theory of *divisors*, which we will explain shortly. To understand why this new theory came to play we have to place ourselves in some context.

In the 1850's Berhard Riemann was the first person to consider curves as objects with a topological nature. He envisioned algebraic curves as sheeted surfaces, creating the first intuitive idea of a manifold. His revolutionary approach was the beginning of the modern treatment of curves. His ideas were very powerful, and allowed him to prove many results and solve ongoing problems in algebraic geometry at the time. This point of view then became an useful tool to obtain a more general and complete perspective on mathematical objects such as curves and surfaces. The ultimate formalization of these ideas arrived only until the twentieth century with the works of Hermann Weyl and others, with the notion of topology and differential geometry. Indeed Riemann's contribution was groundbreaking. However his methods were not very rigorous and some of his arguments raised doubts among the mathematical community. Given that those ideas seemed

worthy of consideration, it became the effort of some mathematicians to endow Riemann's methods with rigour. Richard Dedekind and Heinrich Weber made quite an original attempt. In 1882 they published *Theorie der algebraischen functionen einer veränderlichen* (Theory of algebraic functions in one variable), in which their purpose was to justify some of Riemann's claims with purely algebraic tools. By then, Dedekind had already established his theory of algebraic numbers (1870's) so the influence of that theory in this paper is palpable. We are mainly concerned on how Dedekind and Weber defined a 'Riemann surface' using an algebraic function field. For this account we take inspiration from Stillwell's excellent explanation and translation of Dedekind and Weber's work, given in [10].

The treatment made by Dedekind and Weber was focused on algebraic function fields over $\mathbb{C}$, that is, finite field extensions of $\mathbb{C}(z)$, so for the moment we consider that scenario and later we will return to our finite field based exposition. If $f(x,y) \in \mathbb{C}[x,y]$ is an irreducible polynomial, then the ideal $\langle f(x,y)\rangle$ is a prime ideal and thus the quotient $\mathbb{C}[x,y]/\langle f(x,y)\rangle$ is a domain. If V is the affine variety given by f, that is V is the set of zeros of f in $\mathbb{C}^2$, then the later domain is denoted $\Gamma(V)$ and is called the coordinate ring of V, and the fraction field of $\Gamma(V)$ is called the function field of V, and is written as $\mathbb{C}(V)$. V is an example of a 'Riemann surface' (we will actually not devote too much time to define precisely what a Riemann surface is, for that we recommend [6]) and $\mathbb{C}(V)$, the function field of this surface, is a finite field extension of $\mathbb{C}(x)$, so it is an algebraic function field. The elements of $\mathbb{C}(V)$ can be viewed as functions on the Riemann surface V. Now suppose we have K an arbitrary algebraic function field over $\mathbb{C}$, we can then ask the reverse question: ¿Is there a Riemann surface (some set of points) whose function field is isomorphic to K?

The idea Dedekind and Weber had to solve this question is to consider a dual construction. A point in the Riemann surface corresponds to an evaluation of the functions, so if we have the field K, we define a point $\mathfrak{P}$ as an assignment $f \to f_0$ of numbers to each $f \in K$ such that $(f \pm g)_0 = f_0 \pm g_0, (fg)_0 = f_0 g_0, (f/g)_0 = f_0/g_0$ and $f_0 = f$ if f is a constant. This assignment includes the possibility $f_0 = \infty$, and we use the laws $1/0 = \infty, 1/\infty = 0$. We say that $f = f_0$ en $\mathfrak{P}$ and we say that f vanishes at $\mathfrak{P}$ if $f_0 = 0$. And we say that two points are different iff there is a function on which they assign different values.

Actually there is a way to obtain all the points $\mathfrak{P}$ associated to the function field F. If a point $\mathfrak{P}$ is given, we can suppose that our base variable z fulfils $z_0 < \infty$ (if not replace z by $1/z$, and the field keeps being the same). Note that if $w \in \mathcal{O}_K$, that is, w is integral over $\mathbb{C}[z]$ then $w_0 < \infty$ as well. The set $\mathfrak{p}$ of elements of $\mathcal{O}_K$ that vanish at $\mathfrak{P}$ is actually a prime ideal in $\mathcal{O}_K$, we say that $\mathfrak{p}$ is the prime ideal generated by $\mathfrak{P}$. In fact this ideal cannot be generated by a different point than $\mathfrak{P}$. Conversely, if z is any variable in K and $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ (the integral closure of $\mathbb{C}[z]$ in K, then there is a (unique) point $\mathfrak{P}$ such that $\mathfrak{p}$ is the ideal generated by $\mathfrak{P}$. This correspondence tells us how to obtain all the points $\mathfrak{P}$ of K: first fix a variable z such that K is a finite extension of $\mathbb{C}[z]$, then from all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ we obtain all the points $\mathfrak{P}$ at which z is finite. If $\mathfrak{P}'$ is a point different from these, then $1/z$ is of finite value at $\mathfrak{P}'$, then the prime ideal generated by $\mathfrak{P}'$ is a prime ideal in the integral closure of $\mathbb{C}[1/z]$ and contains $1/z$, reversely any such ideal defines

a point $\mathfrak{P}'$ that has value 0 at $1/z$ and therefore has value ∞ at z. Furthermore, of this last kind or points there are finitely many, because the ring $\mathcal{O}_F(1/z)$ is Noetherian. The set of all points over K will be denoted $\mathcal{S}$ and is what Dedekind and Weber called the Riemann Surface of the function field K.

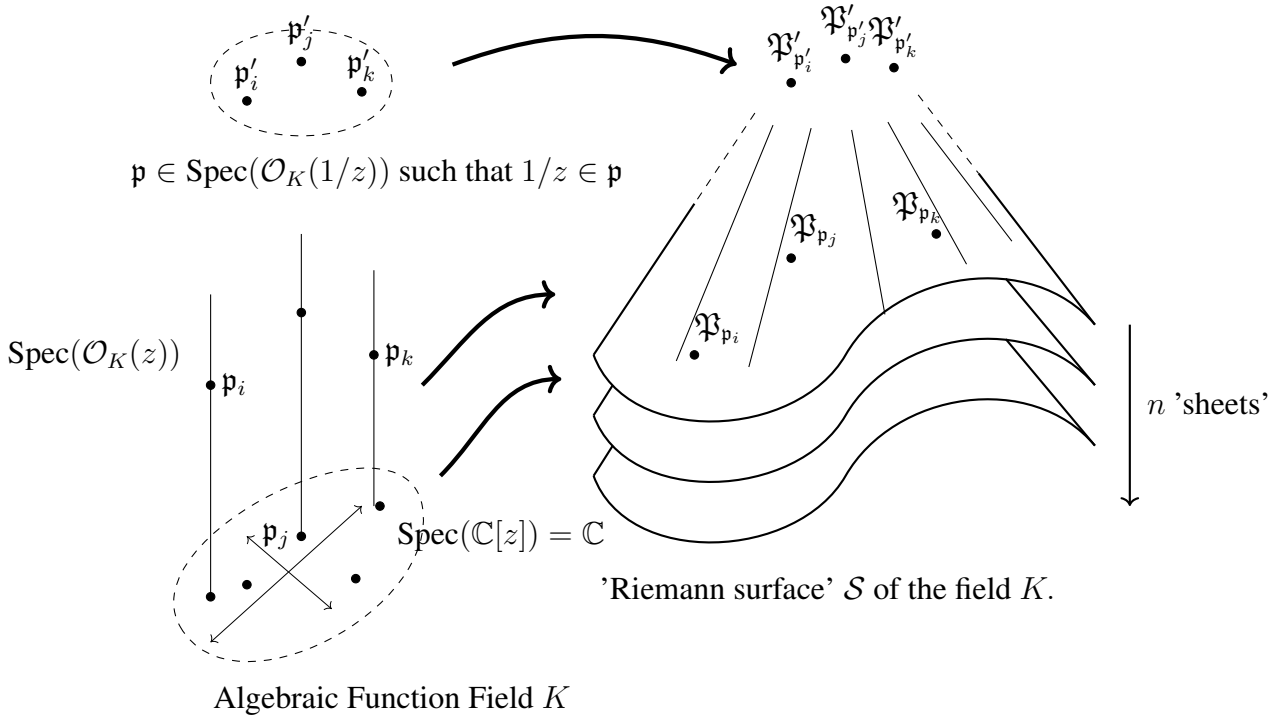


FIGURE 6. Illustration of Dedekind and Weber's construction of a 'Riemann surface' from an algebraic function field over $\mathbb{C}$. We write $\mathcal{O}_K(z)$ the integral closure of $\mathbb{C}[z]$ in K, and $\mathcal{O}_K(1/z)$ the integral closure of $\mathbb{C}[1/z]$ in K.

This 'Riemann surface' is for the moment being just a set of points, with no particular structure. After this construction, Dedekind and Weber prove that if n is the degree of K over $\mathbb{C}(z)$, being z any element in K and not in $\mathbb{C}$, then for every $c \in \mathbb{C} \cup \{\infty\}$, z takes the value c at exactly n points, thus this gives the set $\mathcal{S}$ a n-sheeted structure (it covers $\mathbb{C} \cup \{\infty\}$ n times). Knowing this basic introduction to the work of Dedekind and Weber, we can now formulate the ideas of Schmidt, and they will be understandable from this historical context. The next step taken by Dedekind and Weber was to define the notion of a divisor and with this prove the Riemann-Roch theorem. In Schmidt's work this theory is developed in the particular case of an algebraic function field over $\mathbb{F}_q$, so we will discuss it in the next section.

3.2. **Algebraic function fields and the theory of divisors.** In Schmidt's generalization we consider a ground field, or field of coefficients, k with prime characteristic p. The field F is obtained

first by adjoining k with a transcendental element t and then considering a finite algebraic extension of $k(t)$. Nothing will be initially assumed on the number of elements in k, however if it is finite it will be written as q, where q is a power of p, so in this case $k = \mathbb{F}_q$. We sometimes will use Schmidt's notation and sometimes we will change it to our convenience.

Preliminaries The first section of Schmidt's article is titled *Zusammenstellung bekannter Tatsachen aus der Körper und Idealtheorie* which translates to *Compilation of known facts about the theory of fields and ideals*. In this section Schmidt's presents a series of preliminary facts to be used later in his article. Now we endeavour to give a small presentation of some of those facts.

Some facts

(1) If the field $\mathfrak{L}$ is a finite extension of the field $\mathfrak{K}$, $m = (\mathfrak{L} : \mathfrak{K})$ is the degree of $\mathfrak{L}$ with respect to $\mathfrak{K}$, $\beta_1, \cdots, \beta_m$ is a basis of $\mathfrak{L}$ with respect to $\mathfrak{K}$, then an element α of $\mathfrak{L}$ we have the expressions

$$\alpha\beta_i = c_{i1}\beta_1 + \cdots + c_{im}\beta_m.$$

The Matrix

$$C = \begin{bmatrix} c_{11} & \cdots & c_{1m} \\ \cdots & \cdots & \cdots \\ c_{m1} & \cdots & c_{mm} \end{bmatrix}$$

is formed by the elements c_{ij} that belong to $\mathfrak{R}$. The characteristic function

$$F(x) = x^m + b_1 x^{m-1} + \cdots + b_m = |xI - C|$$

does not depend on the selected basis $\beta_1, \cdots, \beta_m$, and has α as a root. The characteristic function $F(x)$ has in it's factorization an irreducible polynomial with coefficients in $\mathfrak{K}$

$$P(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

with α as a root. With the help of the characteristic function we define the known Norm $N(\alpha)$ and trace $S(\alpha)$ [we denote it by S following the german word for trace: Spur] of the element α of $\mathfrak{L}$ with respect to $\mathfrak{K}$ as given by the equations

$$N(\alpha) = (-1)^m b_m = \begin{vmatrix} c_{11} & \cdots & c_{1m} \\ \cdots & \cdots & \cdots \\ c_{m1} & \cdots & c_{mm} \end{vmatrix}, \quad S(\alpha) = -b_1 = c_{11} + \cdots + c_{mm}.$$

For a system $\gamma_1, \cdots, \gamma_m$ of m elements of $\mathfrak{L}$ we define the discriminant $\Delta(\gamma_1, \cdots, \gamma_m)$ as given by the expression

$$\Delta(\gamma_1, \cdots, \gamma_m) = \begin{vmatrix} S(\gamma_1\gamma_1) & \cdots & S(\gamma_1\gamma_m) \\ \cdots & \cdots & \cdots \\ S(\gamma_m\gamma_1) & \cdots & S(\gamma_m\gamma_m) \end{vmatrix}.$$

When $\mathfrak{L}$ is of the second kind with respect to $\mathfrak{K}$ then the discriminant of any system of m elements of $\mathfrak{L}$ with respect to $\mathfrak{K}$ equals 0. When, on the contrary, $\mathfrak{L}$ is of the first kind with respect to $\mathfrak{K}$ then the discriminant $\Delta(\gamma_1, \cdots, \gamma_m)$ is different of 0 if and only if $\gamma_1, \cdots, \gamma_m$ is a basis of $\mathfrak{L}$ with respect to $\mathfrak{K}$.

(2) A multiplication ring $\mathfrak{R}$ (Multiplikationsring) is a ring that is integrally closed in it's field of fractions. If $\mathfrak{a}$ is an ideal of $\mathfrak{R}$, we consider the ring $\mathfrak{R}_\mathfrak{a}$ of all quotients of two elements of $\mathfrak{R}$ such that the denominator does not belong to $\mathfrak{a}$ (This is the localization of $\mathfrak{R}$ at the ideal $\mathfrak{a}$). The ring $\mathfrak{R}_\mathfrak{a}$ is a principal ideal ring (Hauptidealring, or what we know today as a principal ideal domain), and the ideals of $\mathfrak{R}_\mathfrak{a}$ are of the form $\mathfrak{R}_\mathfrak{a} \cdot \mathfrak{c}$, where $\mathfrak{c}$ is an ideal that does not contain $\mathfrak{a}$, in this case we have that $\mathfrak{R}_\mathfrak{a} \cdot \mathfrak{c} \cap \mathfrak{R} = \mathfrak{c}$.

(3) Consider an extension of (multiplication) rings $\mathfrak{R} \subset \mathfrak{S}$, such that $\mathfrak{S}$ is a finite $\mathfrak{R}$-module, therefore every ideal $\mathfrak{c}$ of $\mathfrak{S}$ is a finite $\mathfrak{R}$-module as well, and besides the field of fractions $\mathfrak{L} = Q(\mathfrak{S})$ (Q for quotientenkörper in german) is a finite extension of the field of fractions $\mathfrak{K} = Q(\mathfrak{R})$, and the characteristic function of an element $\alpha \in \mathfrak{L}$ with respect to $\mathfrak{K}$ has coefficients in $\mathfrak{R}$ if and only if $\alpha \in \mathfrak{S}$. Therefore $\mathfrak{S}$ consists of elements that are integral over $\mathfrak{R}$. The degree f of a prime ideal $\mathfrak{P}$ of $\mathfrak{S}$ is the degree of the field of equivalence clases $\mathfrak{S}/\mathfrak{P}$ over the subfield $\mathfrak{R}/\mathfrak{R} \cap \mathfrak{P}$. For a prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ we have the factorization in $\mathfrak{S}$ given by

$$\mathfrak{S} \cdot \mathfrak{p} = \mathfrak{P}_1 e_1 \cdot \cdots \cdot \mathfrak{P}_s^{e_s},$$

and if $\mathfrak{P}_i$ has degree f_i with respect to $\mathfrak{R}$ and $m = (\mathfrak{L} : \mathfrak{K})$, then

$$m = e_1 f_1 + \cdots + e_s f_s.$$

(4) To define the Norm of an ideal $\mathfrak{U}$ of $\mathfrak{S}$ first we do it in the case where $\mathfrak{R}$ is a principal ideal ring. The every ideal of $\mathfrak{S}$, including $\mathfrak{S}$ it self, has a basis of $m = (\mathfrak{L} : \mathfrak{K})$ elements that are linearly independent over $\mathfrak{R}$. So, is $\alpha_1, \cdots, \alpha_m$ is a basis of $\mathfrak{U}$ over $\mathfrak{R}$ and $\sigma_1, \cdots, \sigma_m$ is a basis of $\mathfrak{S}$ over $\mathfrak{R}$, then we consider the m equations

$$\alpha_i = c_{i1}\sigma_1 + \cdots + c_{im}\sigma_m,$$

that the elements $\sigma_1, \cdots, \sigma_m$ generate for the elements $\alpha_1, \cdots, \alpha_m$. The determinant of the c_{ik} is what will be called the Norm of the ideal $\mathfrak{U}$ with respect to $\mathfrak{R}$. Note that this is exactly the definition that we gave before in our special case. For the general case of $\mathfrak{R}$, we consider the ideal $\mathfrak{b} = \mathfrak{U} \cap \mathfrak{R}$, and the Norm of $\mathfrak{U}$ is defined to be intersection with $\mathfrak{R}$ of the norm of the ideal $\mathfrak{S}_{\mathfrak{S}\cdot\mathfrak{b}} \cdot \mathfrak{U}$ with respect to the principal ideal ring $\mathfrak{R}_\mathfrak{a}$. The Norm of a prime ideal $\mathfrak{P}$ of $\mathfrak{S}$ equals the f-power of the prime ideal $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{R}$ of $\mathfrak{R}$, where f is the degree of $\mathfrak{P}$ with respect to $\mathfrak{R}$.

(5) Let $\mathfrak{S}$ be a ring. A fractional ideal is a subset of the field of fractions $\mathfrak{L} = Q(\mathfrak{S})$ that is a finite $\mathfrak{S}$-module. The ideals that contain only elements of $\mathfrak{S}$ are called integral ideals. If $\mathfrak{R} \subset \mathfrak{S}$ is an inclusion of rings, and $\mathfrak{U}$ is any ideal of $\mathfrak{S}$ let $\mathfrak{U}^*$ be the subset of elements α^* in $\mathfrak{L}(\mathfrak{S})$ such that the trace $S_{\mathfrak{L}/\mathfrak{K}}(\alpha^*\alpha)$ belongs to $\mathfrak{R}$ for every $\alpha \in \mathfrak{U}$, where $\mathfrak{K} = Q(\mathfrak{R})$

is the field of fractions of $\mathfrak{R}$. (Note that in this case we have a field extension $\mathfrak{L}/\mathfrak{K}$, so we can consider the trace $S_{\mathfrak{L}/\mathfrak{K}}$, denoted by S for it's word in german: Spur). We have that $\mathfrak{U}^*$ is a fractional ideal complementary to $\mathfrak{U}$ with respect to $\mathfrak{R}$, and also $\mathfrak{U}^* = \frac{1}{\mathfrak{U}\cdot\mathfrak{D}}$ where $\mathfrak{D}$ is an integral ideal of $\mathfrak{S}$ independent from $\mathfrak{U}$. The ideal $\mathfrak{D}$ is called the different ideal of $\mathfrak{S}$ with respect to $\mathfrak{R}$, and the norm of $\mathfrak{D}$ with respect to $\mathfrak{R}$ equals the discriminant of $\mathfrak{S}$ with respect to $\mathfrak{R}$. If $\mathfrak{a}$ is an ideal of $\mathfrak{R}$, the different ideal of $\mathfrak{S}_{\mathfrak{S}\cdot\mathfrak{a}}$ with respect to $\mathfrak{R}_{\mathfrak{a}}$ equals $\mathfrak{S}_{\mathfrak{S}\cdot\mathfrak{a}}\cdot\mathfrak{D}$. This definition follows the treatment given by E. Hecke in his *Vorlesungen über die Theorie der algebraischen Zahlen* (Lectures on the theory of algebraic numbers) in 1923.

(6) Following notations as above, if $(\mathfrak{L} : \mathfrak{K}) = m$ and $\sigma_1, \cdots, \sigma_m$ is a system of m elements of $\mathfrak{S}$ that are linearly independent over $\mathfrak{R}$ then the ideal generated by $\Delta(\sigma_1, \cdots, \sigma_m)$ (the discriminant from $\mathfrak{L}$ with respect to $\mathfrak{K}$) is called the discriminant of $\mathfrak{S}$ with respect to $\mathfrak{R}$. (it is different than zero if the extension $\mathfrak{L}/\mathfrak{K}$ is of the first kind).

Divisor theory The first notion to work with is that of a *place* of an algebraic function field. Using the motivation from Dedekind and Weber's construction we could define a place of F, a finite extension of $k(t)$, to be an prime ideal in $\mathcal{O}_F(t)$, the integral closure of $k[t]$ in F, or a prime ideal of $\mathcal{O}_F(1/t)$, the integral closure of $k[1/t]$ in F. The last kind of places are called the places at infinity of F. If one reads Schmidt's original article this is not exactly the definition he gives, but it is almost the same. Schmidt defines a place $\mathfrak{P}$ of F, as an integrally closed ring $\mathfrak{P} \subset F$ in which the non invertible elements form an ideal (that is a local ring). To see why this is related to the former definition of place we note the following theorem, presented in Schmidt.

Theorem 7. *Let z be a variable in the algebraic function field F (that is an element $z \in F$ such that F is a finite extension of $k(z)$). If $\tilde{\mathfrak{p}}$ is a prime ideal of $\mathfrak{F} = \mathcal{O}_F(z)$, then the localization $\mathfrak{F}_{\mathfrak{p}}$ is a place of F. Conversely, if $z \in \mathfrak{P}$ is an element not in k, where $\mathfrak{P}$ is a place of F, and if $\tilde{\mathfrak{p}} = \mathfrak{p} \cap \mathfrak{F}$ then $\tilde{\mathfrak{p}}$ is a prime ideal of $\mathfrak{F}$, and $\mathfrak{F}_{\tilde{\mathfrak{p}}} = \mathfrak{P}$.*

So we have that all places (in the sense of Schmidt) are localizations at prime ideals of integral closures in F. Another result presented by Schmidt is the following.

Theorem 8. *If $\mathfrak{P}$ is a place of F then every $\alpha \in \mathfrak{P}$ has a representation of the form $\alpha = \epsilon\pi^e$ where ϵ is a unit of $\mathfrak{P}$, π is a generator of the ideal $\mathfrak{p}$ of non-units of $\mathfrak{P}$ and e is a non-negative integer.*

A reader experienced in commutative algebra would recognize this as a discrete valuation ring. Later we will return to the reason of naming such rings that way. Theorem 8 implies that $\mathfrak{p}$ is the only prime ideal of the place $\mathfrak{F}_{\mathfrak{p}}$. A feature of places is that if $\alpha \in F$ and $\mathfrak{P}$ is a place of F then $\alpha \in \mathfrak{F}$ or $1/\alpha \in \mathfrak{P}$, this is a key observation that allows for the next result.

Theorem 9. *Let $\mathfrak{F}$ and $\mathfrak{F}'$ be the rings of elements integral over z and $1/z$ respectively, for an element $z \in F$ but not in k. Then the set of all places of F consists of the places of the form $\mathfrak{F}_\mathfrak{p}$ and those of the form $\mathfrak{F}'_{\mathfrak{p}'}$, where $\mathfrak{p}$ is a prime ideal of $\mathfrak{F}$ and $\mathfrak{p}'$ is a prime ideal of $\mathfrak{F}'$ that contains $1/z$.*

This tells us that basically considering these places (as defined by Schmidt) is the same as considering the places in the former sense. Following the path of Dedekind and Weber, Schmidt proceeds to define the concept of a divisor. In fact, one could say that Schmidt's exposition is generally inspired in Dedekind and Weber's work. We follow Schmidt's article in a somewhat close way but not completely literal.

Definition. A *divisor*, $\mathfrak{c}$, is a formal expression of the form $\mathfrak{c} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\mathfrak{r}{}^{e_r}$, where the $\mathfrak{p}_i$ are prime ideals of a place of F. A divisor consisting of just one such prime ideal $\mathfrak{p}$ is called a *prime divisor*. An *integral divisor* is a divisor where all the coefficients e_i are non-negative.

The definition of divisors emulates the fact that in $\mathcal{O}_F$ there is factorization in prime ideals. Dedekind and Weber gave the name *polygon* to what we refer to as a divisor, a polygon is a formal expression $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where $\mathfrak{P}_i$ are points of their Riemann surface. Given the equivalence between points and the prime ideals described these concepts are basically the same.

Definition (Order of a Divisor)**.** If $\mathfrak{p}$ is a prime divisor, where $\mathfrak{p}$ is a prime ideal of the place $\mathfrak{P}$, we define the degree of $\mathfrak{p}$ as the integer $f = [\mathfrak{P}/\mathfrak{p} : \mathbb{F}_q]$. Note that this implies that $\#(\mathfrak{P}/\mathfrak{p}) = q^f$, which is related to the absolute norm in Artin's discussion. For a general divisor $\mathfrak{c} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the degree of $\mathfrak{p}_i$ is f_i we define the order of $\mathfrak{c}$ as the integer $f = e_1 f_1 + \cdots + e_r f_r$.

Note that, when $\mathfrak{F}_\mathfrak{p}$ is a place (where $\mathfrak{F} = \mathcal{O}_F(z)$) and then the order of the divisor $\mathfrak{p}$ is equal to $[\mathcal{O}_F(z)/\mathfrak{p} : k]$.

If z is any element in F, but not in k, then there are a finite amount of prime ideals of $\mathcal{O}_F(z)$ that contain z, and prime ideals of $\mathcal{O}_F(1/z)$ that contain $1/z$. If $\mathfrak{P}_i$ $i = 1, \cdots, r$ are the places associated to those ideals, then, because of Theorem 8 for every i there are $e_i \in \mathbb{Z}$ such that $\mathfrak{P}_i \cdot z = \mathfrak{p}_i^{e_i}$. The divisor $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ is called the divisor of the element z. In modern divisor theory this is what is known as a principal divisor. The divisor $\mathfrak{c}$ of an element z can be written formally as

$$\mathfrak{c} = \frac{\mathfrak{c}_1}{\mathfrak{c}_2},$$

where $\mathfrak{c}_1, \mathfrak{c}_2$ are both integral divisors: $\mathfrak{c}_1$ is the product of all the $\mathfrak{p}_i^{e_i}$ in the factorization $\mathfrak{c} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ such that $e_i > 0$, and $\mathfrak{c}_2$ is the product of all $\mathfrak{p}_i^{-e_i}$ such that $e_i < 0$. The divisor $\mathfrak{c}_2$ is called the denominator divisor (Nennerdivisor in german) of z. The order of the divisor of an element of F is equal to zero.

Definition (Divisor Class Group)**.** The set of divisors of F can be endowed with a multiplicative structure, in an obvious way , by concatenating divisors. If we add the null divisor (the divisor with no prime divisors), called $\mathfrak{e}$ which is is the divisor of any element in k, we have a group, denoted $\mathfrak{D}$. The set of divisors of elements of F is a subgroup (because if $\mathfrak{c}, \mathfrak{c}'$ are the divisors of the elements α, β respectively, then $\mathfrak{c}\mathfrak{c}'$ is the divisor of the element $\alpha\beta$). Call this set $\mathfrak{H}$. The *Divisor class group* is the quotient $\mathfrak{D}/\mathfrak{H}$.

As the order of the product of two divisors is the sum of the orders, and the order of the divisor of an element of F is zero, then in every equivalence class (called a divisor class) the order is constant, so we van define the order of a divisor class.

Diferential quotients and genus (Differentialquotienten und Geschlecht): Now we study the definition of the genus of an algebraic function field, as presented by Schmidt. The genus is an important algebraic invariant used to describe such fields.

Definition. Let F^* be a subfield of F and $\mathfrak{P}^*$ a place of F^*, the different divisor of F with respect to $\mathfrak{P}^*$ is the different ideal of $\mathfrak{O}$ with respect to $\mathfrak{P}^*$, where $\mathfrak{O}$ is the ring of all elements of F that are integral over $\mathfrak{P}^*$. The different divisor of F with respect to $\mathfrak{P}^*$ is denoted by $\mathfrak{d}_{F\mathfrak{P}^*}$. It's norm is $\mathfrak{d}^*_{F\mathfrak{P}^*} := N(\mathfrak{d}_{F\mathfrak{P}^*})$ and it equals the discriminant of $\mathfrak{O}$ with respect to $\mathfrak{P}^*$. The order of the divisor $\mathfrak{d}_{FF^*}$ (being F^* trivially a place of F^*) is called the ramification number (verzweignungszahl in german) of F with respect to F^*.

According to Schmidt, the ramification number w_z of F with respect to $k(z)$ can be calculated as follows. If $\mathfrak{F}$ (resp. $\mathfrak{F}'$) denotes the ring of all elements of F integral over z (resp. $1/z$), then w_z equals the degree of the discriminant of $\mathfrak{F}$ with respect to $k(z)$ multiplied by the exponent of the higher power of $1/z$ in the discriminant of $\mathfrak{F}'$ with respect to $k[1/z]$. Now we present the definition of differential quotients given by Schmidt.

Definition. Let α and β be two elements of F that are not in k, such that α is algebraic over $k(\beta)$. Then there is an irreducible polynomial $P(x, \beta)$ with coefficients in k such that $P(\alpha, \beta) = 0$ and $P'_1(x, \beta) \neq 0$. We define the differential quotient $\frac{d\alpha}{d\beta}$ by the equation

$$\frac{d\alpha}{d\beta} = -\frac{P'_2(\alpha, \beta)}{P'_1(\alpha, \beta)}.$$

Some (expected at least from the notation) properties can be proven for the differential quotients, for example:

$$\frac{d(\alpha+\beta)}{d\gamma} = \frac{d\alpha}{d\gamma} + \frac{d\beta}{d\gamma}, \quad \frac{d(\alpha\beta)}{d\gamma} = \frac{d\alpha}{d\gamma}\beta + \frac{d\beta}{d\gamma}\alpha, \quad \frac{d\left(\frac{\alpha}{\beta}\right)}{d\gamma} = \frac{\frac{d\alpha}{d\gamma}\beta - \frac{d\beta}{d\gamma}\alpha}{\beta^2},$$

and also the chain rule:

$$\frac{d\alpha}{d\gamma} = \frac{d\alpha}{d\gamma}\frac{d\beta}{d\gamma}.$$

An important theorem that establishes a relationship between differential quotients and different divisors is the following.

Theorem 10. [8, Satz 4, p.15] *Let α and β be two elements of F but not of k, such that F is of the first kind over $k(\alpha)$ and $k(\beta)$, $\mathfrak{a}$ and $\mathfrak{b}$ the denominator divisors of α and β respectively, and $\mathfrak{d}_\alpha$ and $\mathfrak{d}_\beta$ the different divisors of F with respect to $k(\alpha)$ and $k(\beta)$ respectively. Then the divisor of $\frac{d\alpha}{d\beta}$ equals $\frac{\mathfrak{d}_\alpha \mathfrak{b}^2}{\mathfrak{d}_\beta \mathfrak{a}^2}$.*

From this theorem, the definition of genus can be constructed. As we know the order of the divisor of an element equals zero, this implies that

$$\text{order}\left(\frac{\mathfrak{d}_\alpha \mathfrak{b}^2}{\mathfrak{d}_\beta \mathfrak{a}^2}\right) = 0,$$

and we also know that the order of a product of divisors equals the sum of the orders, so last equation implies that

$$\text{order}(\mathfrak{d}_\alpha \mathfrak{b}^2) = \text{order}(\mathfrak{d}_\beta \mathfrak{a}^2),$$

which gives us that

$$\text{order}(\mathfrak{d}_\alpha) + 2\text{order}(\mathfrak{b}) = \text{order}(\mathfrak{d}_\beta) + 2\text{order}(\mathfrak{a}),$$

or in other words

$$\frac{w_\alpha}{2} - \text{order}(\mathfrak{a}) = \frac{w_\beta}{2} - \text{order}(\mathfrak{b}),$$

where we used the definition $w_z = \text{order}(\mathfrak{d}_z)$. This means that the number

$$\frac{w_z}{2} - \text{order}(n_z) + 1$$

is constant for every z not in k, where n_z is the denominator divisor of z. We add a $+1$ for convenience reasons to be explained later. This number is called the genus of the algebraic function field F, and it is written g. Actually the genus equals

$$\frac{w_z}{2} - m_z + 1,$$

for any $z \in F$ and not in $\mathbb{F}_q$, where $m_z = (F : \mathbb{F}_q(z))$, and this is because of the equality $\text{order}(n_z) = m_z$. We can verify this equality using fact 3 that we gave above. From the definition of divisor of an element we can conclude that the numerator divisor of an element z equals $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$, where we have the prime ideal factorization

$$\mathfrak{F} \cdot z = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

in $\mathfrak{F} = \mathcal{O}_F(z)$, the ring of elements of F that are integral over z. The denominator divisor and the numerator divisor of z both have the same order, because the order of the divisor of z equals zero but it also equals the difference between the order of the numerator divisor and the denominator divisor, so we have that

$$\text{order}(n_z) = e_1 f_1 + \cdots e_s f_s,$$

by definition. However thanks to fact 3 this equals $(Q(\mathfrak{F}) : Q(k[z])) = (K : k(z))$.

Riemann-Roch theorem: In this section Schmidt endeavours to prove a version of this important theorem for his case of algebraic function fields. Riemann Roch provides a simple formula to compute the dimension of a divisor class, that uses the genus of the field K. The proof of this formula is not at all trivial, and it uses a somewhat elaborated theory on normal bases. For the sake of completeness let us mention some results on normal bases and modules of multiples of divisors that allow to understand the statement of the Riemann-Roch theorem. First of all we say that an element z is a multiple of a divisor $\mathfrak{c}$ if the divisor of z equals $\mathfrak{c}\mathfrak{d}$ where $\mathfrak{d}$ is an integral divisor, in other words, the divisor of z is a multiple (as a divisor) of $\mathfrak{c}$. The set of all elements that are multiples of a divisor $\mathfrak{c}$ is denoted by $\mathfrak{m}(\mathfrak{c})$ and actually it is a k-module (if z, w are divisible by the divisor $\mathfrak{c}$ then for every $\alpha \in k$ we have that $\alpha z w$ is also divisible by $\mathfrak{c}$, because the divisor of $\alpha z w$ equals the product of the divisors of z and w). In this section Schmidt proves that the k-module $\mathfrak{m}(\mathfrak{c})$ is actually of finite dimension over k.
If z is an element of F that is not in k such that F is algebraic (and of the first kind) over $k(z)$, let $\mathfrak{F}$ the ring of all elements of F that are integral over z, $\widetilde{\mathfrak{c}}$ an ideal of $\mathfrak{F}$ and $\mathfrak{O}$ the intersection of all the places that occur in the denominator divisor of z, we also set $\mathfrak{P}^* = \mathfrak{O} \cap k(z)$, which gives us a place $\mathfrak{P}^*$ of the field $k(z)$, and actually $\mathfrak{P}^*$ is formed by all quotients of two elements of $k[1/z]$ such that the denominator is divisible by $1/z$. It is possible to prove that for every element $\alpha \in F$ there is at least one integer e (that can be negative) such that $z^e \alpha$ belongs to $\mathfrak{O}$. The largest such integer (positive or negative) is called the exponent of α in $1/z$, and it is written e_α.
The exponent is an example of what is known today as a valuation, because it satisfies the following properties: if $e_\alpha \leqslant e_\beta$ are the exponents of two elements α and β, then the exponent of $\alpha\beta$ equals $e_\alpha + e_\beta$, and the exponent of $\alpha + \beta$ is at least the same as e_α and it equals exactly e_α when $e_\alpha < e_\beta$. If we set $m = (F : k(z))$ then $\widetilde{\mathfrak{c}}$ is a $k[z]$-module of rank m. An abbreviation of several theorems given by Schmidt concerning the basis of $\widetilde{\mathfrak{c}}$ is given by the next result.

Theorem 11. *Let $\gamma_1, \cdots, \gamma_m$ be a system of m elements in $\widetilde{\mathfrak{c}}$, and let e_i be the exponent of γ_i, for $i = 1, \cdots, m$. The following conditions are then equivalent.*

(1) *The system $\gamma_1, \cdots, \gamma_m$ is a basis of the $k[z]$-module $\widetilde{\mathfrak{c}}$ and for every other basis $\gamma'_1, \cdots, \gamma'_m$ with respective exponents $e'_1, \cdots, e'_m$, then $e'_i \leqslant e_i$ for each $i = 1, \cdots, m$.*
(2) *The system $\gamma_1, \cdots, \gamma_m$ satisfies that (after a possible rearrangement) γ_1 has the largest possible exponent amongst all the elements of $\widetilde{\mathfrak{c}}$ and for $i = 1, \cdots, m-1$, γ_{i+1} has the*

largest possible exponent amongst all elements of $\widetilde{\mathfrak{c}}$ that are linearly independent over $k(z)$ with the elements $\gamma_1, \cdots, \gamma_i$.

And, in the case where $1/z$ is not divisible by the square of any prime divisor these conditions are equivalent to the condition that the degree in z of the discriminant $\Delta(\gamma_1, \cdots, \gamma_m)$ -taken with respect to $k[z]$- equals $-2(e_1 + \cdots + e_m)$.

Definition. A basis $\gamma_1, \cdots, \gamma_m$ of $\widetilde{\mathfrak{c}}$ over $k[z]$ that satisfies the conditions of this last theorem is called a normal basis of $\widetilde{\mathfrak{c}}$ with respect to k.

Every ideal $\widetilde{\mathfrak{c}}$ admits a normal basis [8, Satz 6, p. 19] and it follows from the definition that the exponents of two normal basis, after perhaps a suitable rearrangement, are the same. A normal basis allows us to compute the exponents of elements in $\widetilde{\mathfrak{c}}$, Schmidt proved that is $\gamma_1, \cdots, \gamma_m$ is a normal basis of $\widetilde{\mathfrak{c}}$ with respect to $k[z]$, then the exponent of an element $\gamma = c_1\gamma_1 + \cdots + c_m\gamma_m \in \widetilde{\mathfrak{c}}$, with $c_i \in k[z]$ equals the minimum of the exponents of the $c_i\gamma_i$ [8, Satz 7, p. 19]. From this result it follows that the module $\mathfrak{m}(\mathfrak{c})$ has a finite basis over $k[z]$. This is according to the following result.

Theorem 12. [8, Satz 11, p. 22] *Let the elements of a normal basis $\gamma_1, \cdots, \gamma_m$ of $\widetilde{\mathfrak{c}}$ have exponents $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_m$, and let e_r be the last non-negative of these exponents, then the k-module of all multiples of a divisor $\mathfrak{c}$ that belongs to $\widetilde{\mathfrak{c}}$ has a basis over k with $(e_1 + 1) + \cdots + (e_r + 1)$ elements.*

The argument made by Schmidt to conclude this is as follows: all, and only these, the elements of the form

$$\gamma = c_1\gamma_1 + \cdots + c_m\gamma_m \quad (c_i \in k[z])$$

whose exponent is not negative are multiples of $\mathfrak{c}$. According to what we have mentioned, the exponent of γ equals the minimum of the exponents of each $c_i\gamma_i$, therefore γ has non-negative exponent when $c_{r+1} = \cdots = c_r = 0$, and for $i = 1, \cdots r$ c_i has at most degree e_i in z (because the exponent of $c_i\gamma_i$ equals $e_i - d_i$, where d_i is the degree of c_i in z). This means that the $(e_1 + 1) + \cdots + (e_r + 1)$ elements

$$\gamma_i, z\gamma_i, \cdots, z^{e_i}\gamma_i \quad (i = 1, \cdots, r)$$

form a basis of $\mathfrak{m}(\mathfrak{c})$ over k.

Theorem 13. [8, Satz 12, p. 22] *If the divisors $\mathfrak{c}_1, \mathfrak{c}_2$ belong to the same divisor class, then the modules $\mathfrak{m}(\mathfrak{c}_1)$ and $\mathfrak{m}(\mathfrak{c}_2)$ have the same rank over k.*

It is easy to see why this is true. If r_1 and r_2 are the ranks of $\mathfrak{m}(\mathfrak{c}_1)$ and $\mathfrak{m}(\mathfrak{c}_2)$ respectively and z is an element whose divisor is $\frac{\mathfrak{c}_2}{\mathfrak{c}_1}$ then if $\eta_1, \cdots, \eta_{r_1}$ is a system of elements linearly independent over k in $\mathfrak{m}(\mathfrak{c}_1)$, then $\eta\eta_1, \cdots, \eta\eta_{r_1}$ is a system of elements linearly independents over k in $\mathfrak{m}(\mathfrak{c}_2)$

and therefore $r_2 \geqslant r_1$, using that the divisor of $1/\eta$ is $\frac{\mathfrak{c}_1}{\mathfrak{c}_2}$ we can similarly prove that $r_1 \geqslant r_2$.
Now let $\mathfrak{C}$ be a divisor class, we know that if $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are two divisors in the class $\mathfrak{C}$ then $\frac{e}{\mathfrak{c}_1}$ and $\frac{e}{\mathfrak{c}_2}$ are also in the class $\mathfrak{C}$ (where $\mathfrak{e}$ is the null divisor), so the modules $\mathfrak{m}\left(\frac{e}{\mathfrak{c}_1}\right)$ and $\mathfrak{m}\left(\frac{e}{\mathfrak{c}_2}\right)$ have the same rank. We say that the dimension of the class $\mathfrak{C}$ is the rank over k of the module $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$, where $\mathfrak{c}$ is any divisor that belongs to $\mathfrak{C}$.

Now, let $\mathfrak{c}$ be a fixed divisor in $\mathfrak{C}$, note that if α is an element in $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$, then the divisor of the element α equals $\frac{\mathfrak{c}'}{\mathfrak{c}}$ for some $\mathfrak{c}'$ that is an integral divisor (this because of the definition of multiples of divisors), and necessarily $\mathfrak{c}'$ is an integral divisor that belongs to $\mathfrak{C}$ (because it is equivalent to $\mathfrak{c}$). Conversely, for every integral divisor $\mathfrak{c}'$ in $\mathfrak{C}$, there is an element in $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$ whose divisor is $\frac{\mathfrak{c}'}{\mathfrak{c}}$. This argument then gives us a relation between

$$\{ \text{ Integral divisors that belong to } \mathfrak{C}\}$$

and

$$\left\{ \text{ Elements of the module } \mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)\right\},$$

where $\mathfrak{c}$ is a fixed divisor in $\mathfrak{C}$. This relation is not a bijection, because α and $a\alpha$ have the same divisor if α belongs to $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$ and $a \neq 0$ belongs to k. If the field k is finite, so $k = \mathbb{F}_q$, then the module $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$ contains $q^r - 1$ elements different than zero, where r is the rank of $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$ over k. As we said, multiplying by elements in k does not alter the divisor of two elements of $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$, so this tells us that there are in total

$$\frac{q^r - 1}{q - 1}$$

different divisors derived from the elements of $\mathfrak{m}\left(\frac{e}{\mathfrak{c}}\right)$, and thus the above relation becomes a correspondence modulo the multiples of k. All of this gives us the next result.

Theorem 14. *If $\mathfrak{C}$ is a divisor class and $\{\mathfrak{C}\}$ denotes it's dimension, then there are*

$$\frac{q^{\{\mathfrak{C}\}} - 1}{q - 1}$$

integral divisors in $\mathfrak{C}$.

Finally we can state the version of the Riemann-Roch theorem as given by Schmidt. Let z any element of F that is not in k, and set n_z the denominator divisor of z and $\mathfrak{d}_z$ the different divisor of F with respect to $k(z)$, the class determined by the divisor $\frac{\mathfrak{d}_z}{n_z}$ is called the differential class $\mathfrak{M}$ of F. For any divisor class the class $\mathfrak{C}' := \frac{\mathfrak{M}}{\mathfrak{C}}$ is called the supplementary class of $\mathfrak{C}$, the reader can verify that theorem 10 implies that this is well defined, in other words, it does not depend on the choice of z. According to Schmidt the proof of the following theorem can be done using the same methods employed by Kurt Hensel and Georg Landsberg in their 1902 article *Theorie der algebraischen funcktionen einer variabeln und ihre anwendung auf algebraische kurven und Abelsche integrale*

(Theory of algebraic functions in one variable and their applications to algebraic curves and Abel integrals).

Theorem 15 (Riemann-Roch Theorem)**.** *If $\mathfrak{C}$ is a divisor class of order q, and $\{\mathfrak{C}\}$ denotes the dimension of the class, then*

$$\{\mathfrak{C}\} = \left\{\frac{\mathfrak{M}}{\mathfrak{C}}\right\} + q - g + 1$$

where $\mathfrak{M}$ is the differential class.

From this easily follows the equality

$$\{\mathfrak{C}\} - \frac{q}{2} = \{\mathfrak{C}'\} - \frac{q'}{2}$$

where q' is the order of the supplementary class $\mathfrak{C}'$. Indeed, it is only a matter of noticing that $(\mathfrak{C}')'$ equals clearly $\mathfrak{C}$, so we can clearly apply Riemann-Roch's theorem twice:

$$\begin{aligned} 2\{\mathfrak{C}\} - q &= \underbrace{\{\mathfrak{C}\} - q}+\{\mathfrak{C}\} \\ \text{(Riemann-Roch)} &= \underbrace{\{\mathfrak{C}'\} - g + 1}+\{\mathfrak{C}\} \\ &= \underbrace{\{\mathfrak{C}\} - g + 1}+\{\mathfrak{C}'\} \\ \text{(Riemann-Roch)} &= \underbrace{\{\mathfrak{C}'\} - q'}+\{\mathfrak{C}'\} \\ &= 2\{\mathfrak{C}'\} - q'. \end{aligned}$$

Another important consequence of this theorem is the following result.

Corollary 1. If $\mathfrak{C}$ is a divisor class of order d, where $d \geqslant 2g - 2$ then

$$\{\mathfrak{C}\} = d - g + 1.$$

Arithmetic properties of the divisor class group: Now we describe the arithmetic behaviour of divisors.

Theorem 16. *Every divisor $\mathfrak{c}$ of F has a representation $\mathfrak{c} = \mathfrak{c}_0\mathfrak{c}_1^m$ where $\mathfrak{c}_0$ is a divisor of order 0 and $\mathfrak{c}_1$ is a divisor with the least positive order (called d) among all integral divisors of F,and $m \in \mathbb{Z}_{\geqslant 0}$. In particular the order of $\mathfrak{c}$ is a multiple of d, or it is equal to 0. In other words: The quotient group $\mathfrak{D}/\mathfrak{D}_0$, where $\mathfrak{D}$ is the group of all divisors, and $\mathfrak{D}_0$ is the subgroup of divisors of order 0.*

This follows easily by applying the division algorithm. If $\mathfrak{c}_1$ is such that divisor, then for any divisor of order n we necessarily have $n = ds$, for some integer s, using the minimality of d, and then the divisor $\frac{\mathfrak{c}}{\mathfrak{c}_1^s}$ has order 0.

Theorem 17. *If k is a finite field, the subgroup $\mathfrak{D}_0$ of all divisors with order zero has a finite number of equivalence classes in the divisor class group. We call that number h.*

Theorem 18. *If n is a multiple of d, the least positive order of an integral divisor of F, then there are exactly h divisor classes of order n, where h is the number of divisor classes of order 0.*

3.3. **Zeta function of an algebraic function field.** With all of this theory we can see how Schmidt constructed his zeta function.
Definition and Rational expression: We set the following notation: if $\mathfrak{c}$ is a divisor of F with degree f, we write $|\mathfrak{c}| := q^f$.

Definition (Zeta function for an algebraic function field)**.** If F is an algebraic function field with field of constants $\mathbb{F}_q$ then the zeta function for F is defined to be

$$\zeta_F(s) = \sum_{\mathfrak{c}} \frac{1}{|c|^s} \tag{11}$$

where the sum is extended over all integral divisors of F.

Clearly in this zeta function we have an Euler factorization as well,

$$\zeta_F(s) = \prod_{\mathfrak{p}} \frac{1}{1 - |p|^{-s}} \tag{12}$$

where the product is extended over all prime divisors $\mathfrak{p}$ of F. With the previous results, Schmidt proves directly that his zeta function is a rational function. Let's see the argument made there. Let $k \in \mathbb{Z}_{>0}$ and let $\mathfrak{C}_k^1, \cdots, \mathfrak{C}_k^h$ the h classes of order dk, where k is a positive integer, d is the least possible order of an integral divisor in F and h is the number of divisor classes of order 0. In every $\mathfrak{C}_k^i$ there are exactly

$$\frac{q^{\{\mathfrak{C}_k^i\}} - 1}{q - 1}$$

integral divisors, because of 14. Using (11) we have that

$$\begin{aligned}
\zeta_F(s) &= \frac{1}{q-1} \sum_{k=1}^{\infty} \sum_{i=1}^{h} \frac{q^{\{\mathfrak{C}_k^i\}} - 1}{q^{dks}} \\
&= \frac{1}{q-1} \sum_{k=1}^{\infty} \sum_{i=1}^{h} \frac{q^{\{C_k^i\}}}{q^{dks}} - \frac{h}{p-1} \sum_{k=1}^{\infty} \frac{1}{q^{dks}} \\
&= \frac{1}{q-1} \sum_{k=1}^{\infty} \sum_{i=1}^{h} \frac{q^{\{C_k^i\}}}{q^{dks}} + \frac{h}{q-1} \cdot \frac{1}{1 - q^{ds}}
\end{aligned}$$

If k_0 is the least integer such that $k_0 d \geqslant 2g-2$, then for $k \geqslant k_0$, we have that $\{\mathfrak{C}_k^i\} = dk - g + 1$, because of Corollary (1). Therefore

$$\begin{aligned}\zeta_F(s) &= \frac{1}{q-1}\sum_{k=1}^{k_0-1}\sum_{i=1}^{h}\frac{q^{\{\mathfrak{C}_k^i\}}}{q^{dks}} + \frac{hq^{1-g}}{q-1}\sum_{k=k_0}^{\infty}\frac{q^{dk}}{q^{dks}} + \frac{h}{q-1}\cdot\frac{1}{1-q^{ds}} \\ &= \frac{1}{q-1}\sum_{k=1}^{k_0-1}\sum_{i=1}^{h}\frac{q^{\{\mathfrak{C}_k^i\}}}{q^{dks}} + \frac{hq^{1-g}}{q-1}\cdot\frac{q^{dk_0(1-s)}}{1-q^{d(1-s)}} + \frac{h}{q-1}\cdot\frac{1}{1-q^{ds}}\end{aligned}$$

Which is a rational function in the variable $u = q^{-s}$.

Zeros and period: It can be seen that the Zeta function $\zeta_F(s)$ is periodic of period $\frac{2\pi i}{\log q}$, which was similarly observed by Artin. Also it is a regular function on the entire complex plane except on the points $0 + \frac{2l\pi i}{\log q}$ and $1 + \frac{2l\pi i}{\log q}$ where it has poles of first orders with residuum $-\frac{h}{(q-1)\log q}$ and $\frac{hq^{1-g}}{(q-1)\log q}$ respectively. From the equation 11, it can be concluded that if d is the least possible positive order of a (integral) divisor then the zeta function also has the period $\frac{2\pi i}{\log q_1}$, where $q_1 = q^d$. Being this period also equal to $\frac{2\pi i}{\log q}$, it follows right away that d must be equal to 1.

Functional Equation: Given that $d = 1$ we have then that $k_0 = 2g-2$, and therefore we obtain the representation

$$\zeta_F(s) = \frac{1}{q-1}\sum_{k=1}^{2g-3}\sum_{i=1}^{h}\frac{q^{\{\mathfrak{C}_k^i\}}}{q^{ks}} + \frac{hq^{-(g-1)}}{q-1}\frac{q^{(2g-2)(1-s)}}{1-q^{1-s}} + \frac{h}{q-1}\frac{1}{1-q^{s}}. \tag{13}$$

Theorem 19 (Functional Equation for the Zeta Function)**.** *The function $\zeta_F(s)$ fulfils the functional equation*

$$\zeta_F(1-s) = q^{(g-1)(2s-1)}\zeta_F(s) \tag{14}$$

Proof. To help us with the proof we will consider the function

$$\Xi(s) = q^{s(g-1)}\zeta_F\Big(\frac{1}{2}+s\Big)$$

then we have to prove $\Xi(-s) = \Xi(s)$. With formula (13) we have that

$$\begin{aligned}\Xi(s) &= \frac{1}{q-1}\left(q^{s(g-1)}\sum_{k=1}^{2g-3}\sum_{i=1}^{h}\frac{q^{\{\mathfrak{C}_q^i\}}}{q^{\frac{k}{2}+ks}}\right) + \frac{h}{q-1}\left(\frac{q^{-s(g-1)}}{1-q^{\frac{1}{2}-s}} + \frac{q^{s(g-1)}}{1-q^{\frac{1}{2}+s}}\right) \\ &= S_1(s) + S_2(s)\end{aligned}$$

where

$$\begin{aligned}S_1(s) &= \frac{1}{q-1}q^{s(g-1)}\sum_{k=1}^{2g-3}\sum_{i=1}^{h}\frac{q^{\{\mathfrak{C}_q^i\}}}{q^{\frac{k}{2}+ks}} \\ S_2(s) &= \frac{h}{q-1}\left(\frac{q^{-s(g-1)}}{1-q^{\frac{1}{2}-s}} + \frac{q^{s(g-1)}}{1-q^{\frac{1}{2}+s}}\right)\end{aligned}$$

So it is enough to prove that $S_i(s) = S_i(-s)$ for $i = 1, 2$. For $S_2(s)$ this relation is clear. For $S_1(s)$ we can use the Riemann-Roch theorem. We note that

$$(q-1)S_1(s) = q^{s(g-1)} \sum_{k=1}^{2g-3} \sum_{i=1}^{h} \frac{q^{\{\mathfrak{C}_q^i\}}}{q^{\frac{k}{2}+ks}} = \sum_{k=1}^{2g-3} \sum_{i=1}^{h} \frac{q^{\{\mathfrak{C}_q^i\}-\frac{k}{2}}}{q^{s(k-g+1)}}.$$

If $\mathfrak{C}_k$ is a class of order k, then it's supplementary class $\mathfrak{C}'_k$ has order $k' = 2g-2-k$, so we have that both $\mathfrak{C}_k$ and $\mathfrak{C}'_k$ go through all classes of order less that $2g-2$ and therefore we have

$$(q-1)S_1(s) = \sum_{k=1}^{2g-3} \sum_{i=1}^{h} \frac{q^{\{(\mathfrak{C}_q^i)'\}-\frac{k'}{2}}}{q^{s(k'-g+1)}} = \sum_{i=1}^{h} \frac{q^{\{(\mathfrak{C}_q^i)'\}-\frac{k'}{2}}}{q^{-s(k-g+1)}},$$

and thus it follows that

$$(q-1)S_1(s) = \frac{1}{2} \sum_{k=1}^{2g-3} \sum_{i=1}^{h} \left(\frac{q^{\{\mathfrak{C}_q^i\}-\frac{k}{2}}}{q^{s(k-g+1)}} + \frac{q^{\{(\mathfrak{C}_q^i)'\}-\frac{k'}{2}}}{q^{-s(k-g+1)}} \right),$$

and the equality

$$\{\mathfrak{C}_q^i\} - \frac{k}{2} = \{(\mathfrak{C}_q^i)'\} - \frac{k'}{2},$$

that we presented as a consequence of Riemann-Roch's theorem, gives us clearly that $S_1(-s) = S_1(s)$. □

3.4. **Including the points at infinity.** Finally, let's see why Schmidt's function adds points at infinity to the count of solutions made with the zeta function. A analogue of proposition 11 is needed here.

Proposition 12. Let V be a projective variety over $\mathbb{F}_q$, N_m the number of projective points of V over $\mathbb{F}_{q^m}$ and F the field of functions of V over $\mathbb{F}_q$ (an algebraic function field), then

$$N_m = \sum_{n|m} n b_n$$

where

$$b_n := \#\{\mathfrak{p} \text{ prime divisors of } F : \deg \mathfrak{p} = n\}$$

If $\tilde{N}_m$ is the number of points at infinity (after a de-homogenization) using the result from proposition 11 and the characterization of divisors we have to prove that

$$\tilde{N}_m = \sum_{n|m} n c_n$$

where

$$c_n := \#\{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K(1/z)) : 1/z \in \mathfrak{p} \text{ and } \deg \mathfrak{p} = n\}$$

Then using the same argument as before we have that

$$\zeta_F(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m u^m}{m}\right)$$

where the N_m include the points at infinity of a curve over $\mathbb{F}_q$.

3.5. **Relationship between both zeta functions.** As we saw, we can construct the zeta function using ideals, or the zeta function using divisors. The fundamental difference is that the divisor approach adds the notion of points at infinity, whereas the ideal approach corresponds to counting only the affine points of a curve. Both zeta functions, the one we called Artin zeta function, and the Schmidt zeta function, are related by the equation

$$\zeta_F(s) = \prod_{\mathfrak{u}} \frac{1}{1 - |\mathfrak{u}|^{-s}} Z_F(s)$$

where the product extends over all divisors $\mathfrak{u}$ over $1/z$, an equation mentioned in the last section of Schmidt's paper: *Anwendungen* (Applications). This is because of Theorems 5 and 6, and the observation that we made after the definition of the order of a Divisor, that the degree of a prime divisor of the form $\mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of $\mathfrak{F} = \mathcal{O}_F$, fulfils the relationship $f = [\mathcal{O}_F/\mathfrak{p} : \mathbb{F}_q]$, so $q^f = \#(\mathcal{O}_F/\mathfrak{p})$, which is equal to the absolute norm. As a special case of this relation, in the quadratic (or hyperelliptic) case we have that

Proposition 13. If $Z_F(s)$ is the Zeta function as defined by Artin, for the quadratic function field $F = \mathbb{F}_p(z, \sqrt{D(z)})$, where $D(z)$ is a square-free monic polynomial, then

$$\zeta_F(s) = Z_F(s) \cdot \frac{1}{(1 - p^{-s})^n} \tag{15}$$

where n is the number of points at infinity of the curve $y^2 - D(x)$, which is $n = 1$ if deg $D \neq 2$ and $n = 2$ if deg $D = 2$.

Therefore the general zeta function for a hyperelliptic curve $y^2 - D(x)$ can be calculated explicitly using Artin's method.

4. Appendix: Computations with Artin Zeta Function

Now we provide some minor examples, so that the reader can see visually some of the properties of the zeta function that we have just discussed. The code to compute the coefficients σ_v of Artin zeta function is really simple. Here we present a sage sheet containing those calculations. Notice that we used the relations between the coefficients proved by Artin. This method is just a calculation and might not be very fast for large values of p. After the given code the reader can see some computational examples with illustrations that show us the behaviour of the zeta function.

At the beginning we put $q = 3$ because of the computations at the end, but of course this can be changed to any power of a prime. **This is presented as an attachment after the references.**

REFERENCES

[1] Emil Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. I. (German)* Math. Z. **19** (1924), no. 1, 153–206.

[2] Emil Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. II. (German)* Math. Z. **19** (1924), no. 1, 207–246.

[3] Jean A. Dieudonne *History of Algebraic Geometry* Wadsworth Mathematics Series. Belmont, CA: Wadsworth International Group, 1985. Translated from the French by Judith D. Sally.

[4] Robin Hartshorne, *Algebraic geometry.* Graduate Texts in Mathematics, No. **52**. Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp.

[5] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics, **84**. Springer-Verlag, New York, 1990. xiv+389 pp.

[6] Frances Kirwan, *Complex Algebraic Curves /.* London Mathematical Society, Cambridge University Press, New York, 1992.

[7] Peter Roquette *The Riemann hypothesis in characteristic p, its origin and development. Part 1. The formation of the zeta functions of Artin and F. K. Schmidt. /* Mitteilungen der Mathematischen Gesellschaft in Hamburg, Band XXI/2 (2002) 79– 157 2, 6, 28

[8] Friedrich Karl Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p. (German)* Math. Z. **33** (1931), no. 1, 1–32.

[9] Joseph H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, **106**. Springer, Dordrecht, 2009. xx+513 pp.

[10] John Stillwell, *Theory of algebraic functions in one variable* American Mathematical Society, 2012.

[11] Matteo Tamiozzo, *Zeta and L-functions of elliptic curves /.* Tesi di Laurea in Teoria dei Numeri. Universita di Bologna, 2014.

[12] André Weil, Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* **55**, (1949). 497–508.

Artin Zeta Function.sagews

Author	**Jimmy Calvo Monge**
Date	**2020-09-06T20:23:12**
Project	**b3001d5e-d496-4d7b-9871-85d35ff84fa4**
Location	Artin Zeta Function.sagews
Original file	Artin Zeta Function.sagews

```
q=3
F = GF(q)
R.<x> = F[]

def legendre_poly(D, P): ###Returns the Legendre symbol [D/P] when P is a prime polynomial
        if P.divides(D):
            return 0
        else:
            OP = R.quotient_by_principal_ideal(P, 'X')
            squares = Set([M^2 for M in OP])
            if OP(D) in squares:
                return 1
            else:
                return -1

def jacobi_poly(D,Q): ###Returns the Jacobi symbol [D/Q] for general Q
    z=list(Q.factor())
    r=[]
    #r.append(len(z))
    for i in range(0,len(z)):
        r.append(legendre_poly(D,z[i][0])^(z[i][1]))
    return prod(r)

def sigma(D,v): ###Returns the value of the coefficient sigma_v
    sig=[]
    for p in R.monics( of_degree = v ):
        sig.append(jacobi_poly(D,p))
    return sum(sig)


def zeta_artin(D): ###Returns an array [sigma_0,sigma_1,...,sigma_(n-1)]
                   ###for the Artin zeta function of the curve y^2=D(z)
    n=D.degree()
    f=D.coefficients()[0]
    m=(n-1)/2
    t=n/2
    sigm=[]
    if is_odd(n):
        for i in range(0,m+1):
            sigm.append(sigma(D,i))
        for j in range(1,m+1):
            sigm.append((q^j)*sigm[m-j])
        return(sigm)
    else:
        if f in squares: ##Real case
            for i in range(0,t):
                sigm.append(sigma(D,i))
            for j in range(0,t-1):
                sigm.append((q^j)*(-sigm[t-j-1] +(q-1)*(sum([sigm[k] for k in range(0,t-j-1)]))))
            sigm.append(-q^(t-1))
            return(sigm)
        else: ##Imaginary case
            for i in range(0,t):
                sigm.append(sigma(D,i))
            for j in range(0,t-1):
                sigm.append((q^j)*(sigm[t-j-1] +(q-1)*(sum([sigm[k]*(-1)^(t-j-k) for k in range(0,t-j-1)]))))
            sigm.append(q^(t-1))
            return(sigm)

## In the following level curve plots we can see the Riemann Hypothesis in action.
D3= x^3+2*x^2+x+1
D3.is_irreducible()
show(D3)
zeta_artin(D3)
show("$Z_F(s)=\\frac{1}{1-3^{1-s}} (1+3^{-s}+3\cdot 3^{-2s} ).$")
```

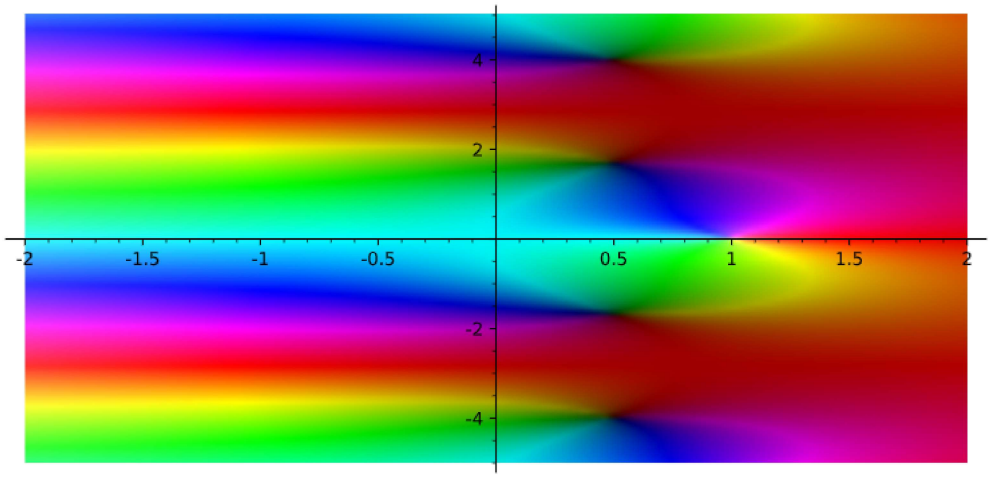
```
True
```

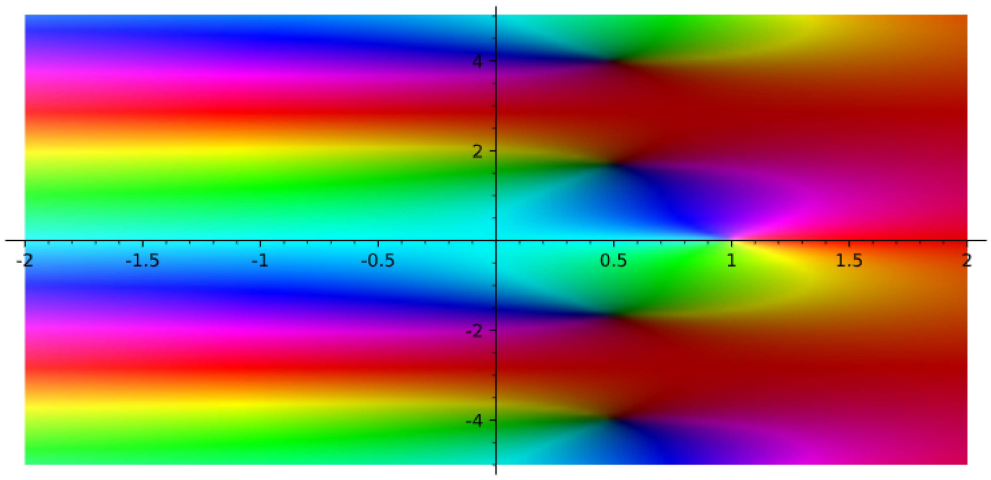
$$x^3+2x^2+x+1$$

```
[1, 1, 3]
```

$$Z_{F'}(s) = \frac{1}{1-3^{1-s}}(1+3^{-s}+3\cdot 3^{-2s}).$$

```
61 complex_plot(lambda z: (1 +(3^(-z))+ 3*(3^(-2*z)))/(1-3^(1-z)), (-2, 2), (-5, 5))
```






```
62 D5= x^5+2*x^4+2*x^2+2*x+1
63 D5.is_irreducible()
64 show(D5)
65 zeta_artin(D5)
66 show("$Z_F(s)=\\frac{1}{1-3^{1-s}} (1-3^{-s}+5\cdot 3^{-2s} -3 \cdot 3^{-3s} +9 \cdot 3^{-4s} ).$")
```

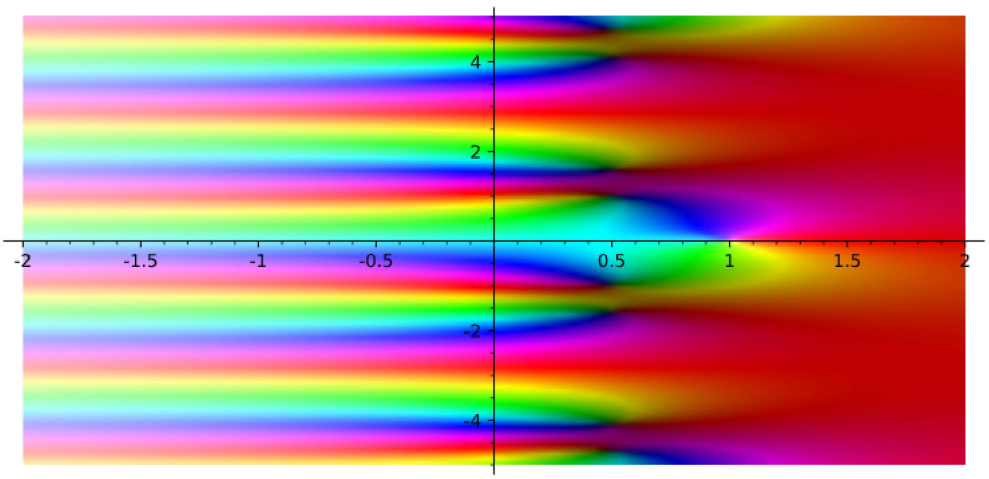
```
True
```

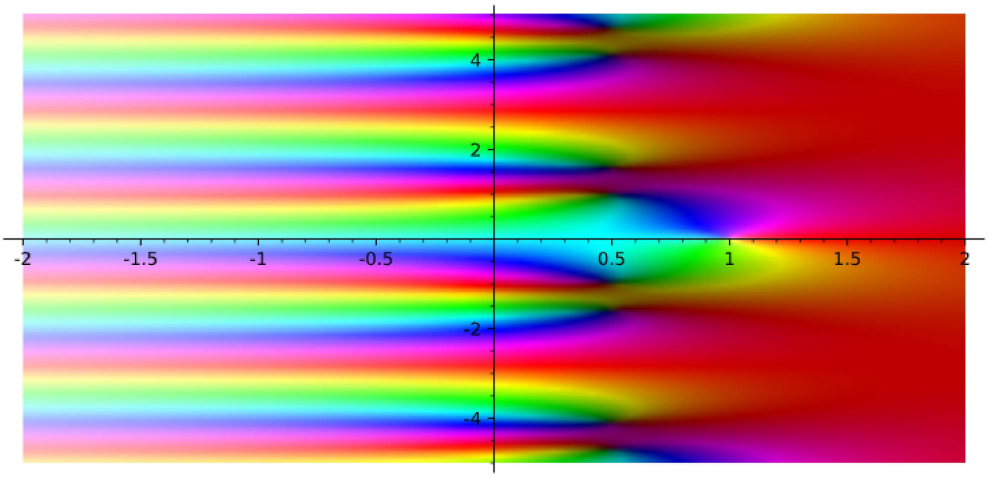
$$x^5+2x^4+2x^2+2x+1$$

```
[1, -1, 5, -3, 9]
```

$$Z_F(s) = \frac{1}{1-3^{1-s}}(1-3^{-s}+5\cdot 3^{-2s}-3\cdot 3^{-3s}+9\cdot 3^{-4s}).$$

```
67 complex_plot(lambda z: (1 -(3^(-z))+ 5*(3^(-2*z)) -3*(3^(-3*z)) +9*(3^(-4*z)) )/(1-3^(1-z)), (-2, 2), (-5, 5))
```






```
68 D7= x^7+x^6++2*x^5+x^4+2*x+1
69 D7.is_irreducible()
70 show(D7)
71 zeta_artin(D7)
72 show("$Z_F(s)=\\frac{1}{1-3^{1-s}} (1+3^{-s}+3\cdot 3^{-2s} -3^{-3s} +9 \cdot 3^{-4s} +9 \cdot 3^{-5s} +27\cdot 3^{-6s}).$")
```

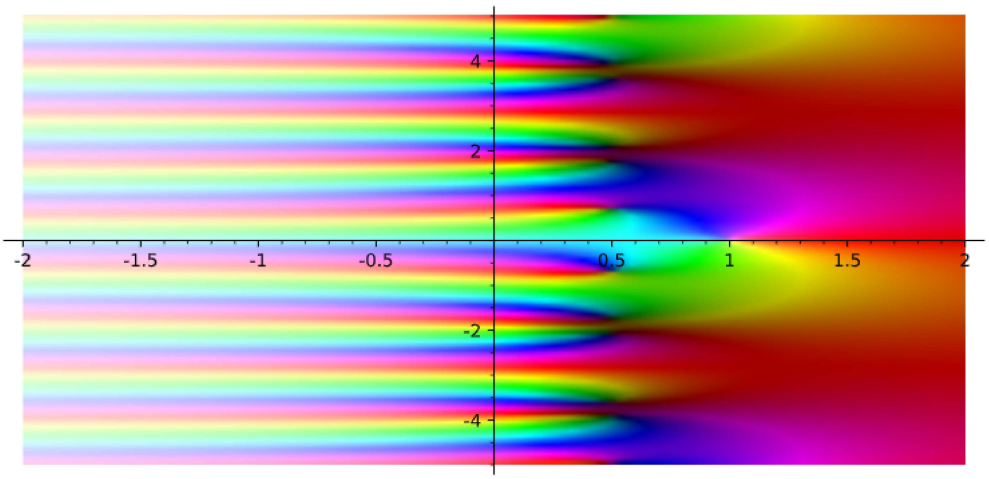
```
True
```

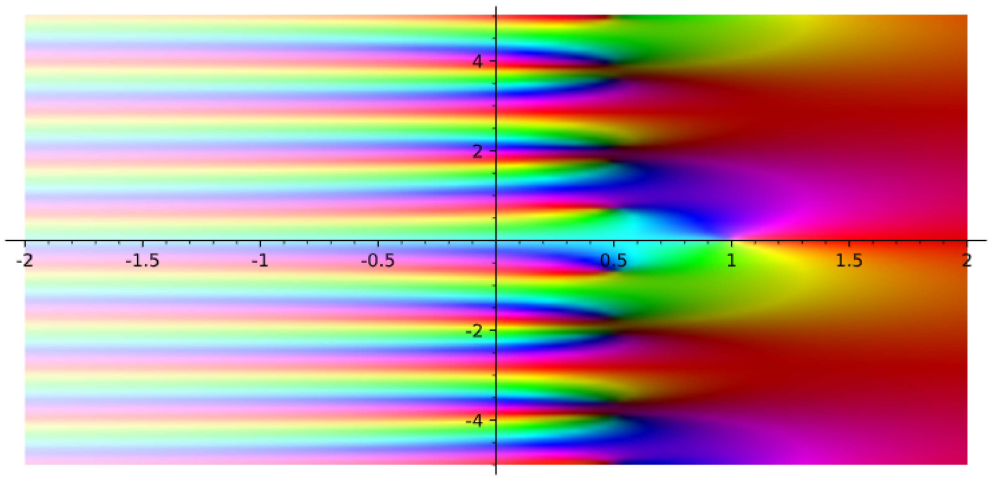
$$x^7+x^6+2x^5+x^4+2x+1$$

```
[1, 1, 3, -1, 9, 9, 27]
```

$$Z_F(s)=\frac{1}{1-3^{1-s}}(1+3^{-s}+3\cdot 3^{-2s}-3^{-3s}+9\cdot 3^{-4s}+9\cdot 3^{-5s}+27\cdot 3^{-6s}).$$

```
73 complex_plot(lambda z: (1 +(3^(-z))+ 3*(3^(-2*z)) -(3^(-3*z)) +9*(3^(-4*z)) +9*(3^(-5*z)) +27*(3^(-6*z)) )/(1-3^(1-z)), (-2, 2), (-5, 5))
```






```
74 D10=x^10+x^3+x^2+1
75 D10.is_irreducible()
76 show(D10)
77 zeta_artin(D10)
78 show("$Z_F(s)=\\frac{1}{1-3^{1-s}} (1+3^{-s} +3\cdot 3^{-2s} + 5 \cdot 3^{-3s} + 5 \cdot 3^{-4s} + 9 \cdot 3^{-5s} + 33 \cdot 3^{-6s} + 27 \cdot 3
```

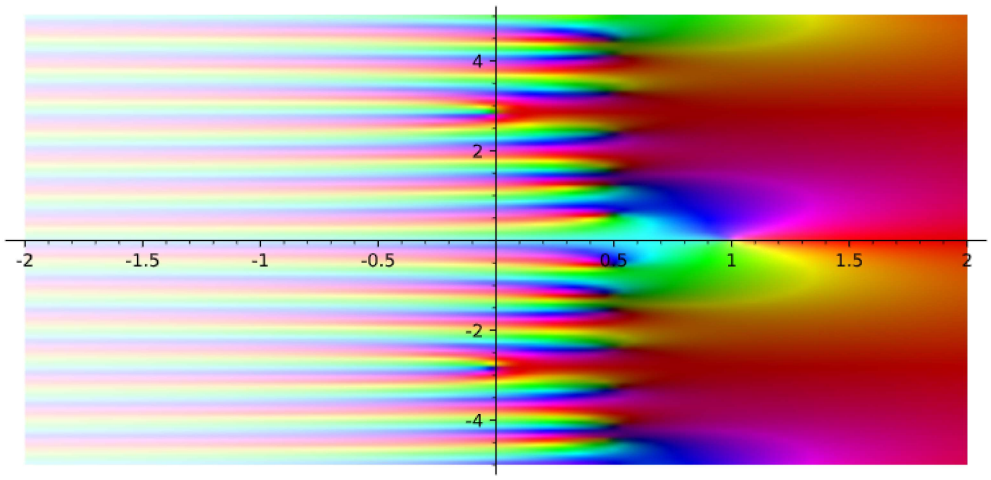
```
True
```

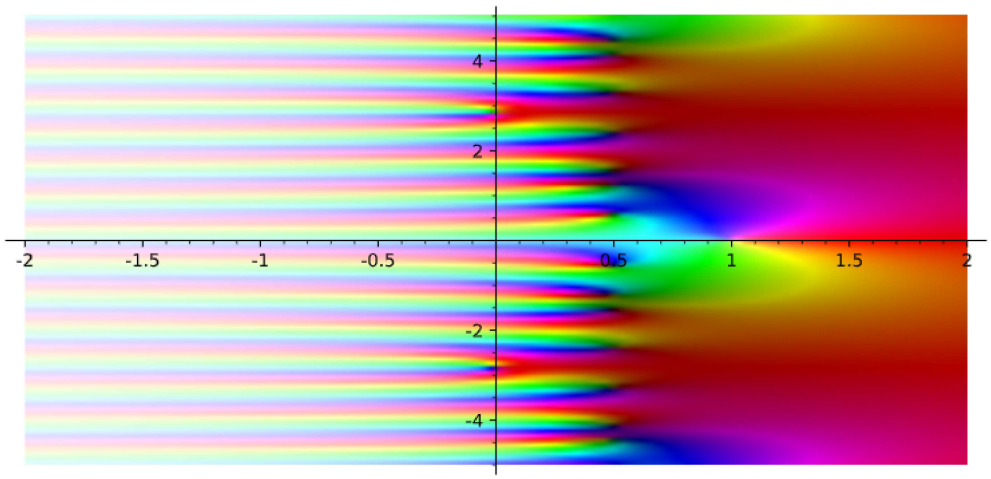
$$x^{10}+x^3+x^2+1$$

```
[1, 1, 3, 5, 5, 9, 33, 27, 81, 81]
```

$$Z_F(s)=\frac{1}{1-3^{1-s}}(1+3^{-s}+3\cdot 3^{-2s}+5\cdot 3^{-3s}+5\cdot 3^{-4s}+9\cdot 3^{-5s}+33\cdot 3^{-6s}+27\cdot 3^{-7s}+81\cdot 3^{-8s}+81\cdot 3^{-9s}).$$

```
79 complex_plot(lambda z: (1 +(3^(-z))+ 3*(3^(-2*z)) +5*(3^(-3*z)) +5*(3^(-4*z)) +9*(3^(-5*z)) +33*(3^(-6*z)) + 27*(3^(-7*z)) +81*(3^(-8*z)) + 81*(3^
```

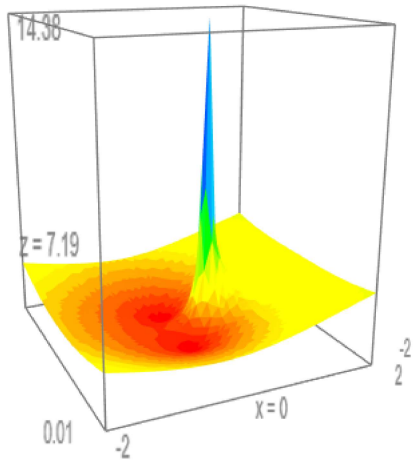





```
##To plot in 3d we take the absolute value of the function Z_F(u), with the change of coordinates u=q^{-s}.
##Please note that these ARE NOT the plots of the absolute values of the functions above, because of the change of variables.
##However we can note the presence of a pole in u=1/3 (which is s=1).
var('x y');
p3=plot3d(lambda x,y:abs((1+(x+I*y)+3*(x+I*y)^2)/(1-3*(x+I*y))),(x,-2,2),(y,-2,2),adaptive=True, color=rainbow(60, 'rgbtuple'), max_bend=.1, max_d
show("$Z_F(u)= \\frac{1}{1-3u}\cdot(1+u+3u^2).$ Zeta function for the curve $y^2=x^3+2x^2+x+1$")
p3.show(aspect_ratio=(3,3,1))
```

```
(x, y)
```

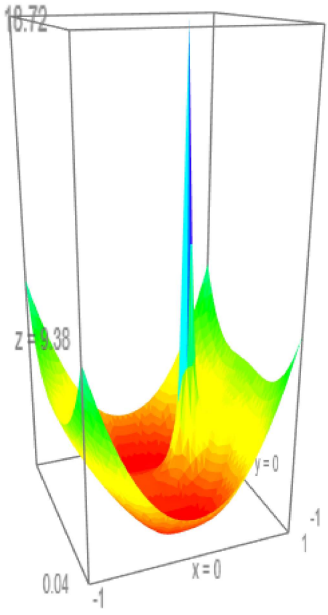
$Z_F(u) = \frac{1}{1-3u} \cdot (1 + u + 3u^2)$. Zeta function for the curve $y^2 = x^3 + 2x^2 + x + 1$




```
var('x y');
p5=plot3d(lambda x,y:abs((1-(x+I*y)+5*(x+I*y)^2 -3*(x+I*y)^3 +9*(x+I*y)^4)/(1-3*(x+I*y))),(x,-1,1),(y,-1,1),adaptive=True, color=rainbow(60, 'rgbt
show("$Z_F(u)= \\frac{1}{1-3u}\cdot(1-u+5u^2-3u^3+9u^4).$ Zeta function for the curve $y^2=x^5+2x^4+2x^2+2x+1$")
p5.show(aspect_ratio=(4,4,1))
```

```
(x, y)
```

$Z_F(u) = \frac{1}{1-3u} \cdot (1 - u + 5u^2 - 3u^3 + 9u^4)$. Zeta function for the curve $y^2 = x^5 + 2x^4 + 2x^2 + 2x + 1$




```
var('x y');
p7=plot3d(lambda x,y:abs((1+(x+I*y)+3*(x+I*y)^2 -1*(x+I*y)^3 +9*(x+I*y)^4  +9*(x+I*y)^5 +27*(x+I*y)^6)/(1-3*(x+I*y))),(x,-0.7,0.7),(y,-0.7,0.7),ad
show("$Z_F(u)= \\frac{1}{1-3u}\cdot(1+u+3u^2-u^3+9u^4+9u^5+27u^6).$ Zeta function for the curve $y^2=x^7+x^6+2x^5+x^4+2x+1$")
p7.show(aspect_ratio=(7,7,1))
```

```
(x, y)
```

$Z_F(u) = \frac{1}{1-3u} \cdot (1 + u + 3u^2 - u^3 + 9u^4 + 9u^5 + 27u^6)$. Zeta function for the curve $y^2 = x^7 + x^6 + 2x^5 + x^4 + 2x + 1$