4.1. More on divisors

In this section, $C$ will be a smooth projective curve over a finite field $\mathbb{F}_q$.
In the last chapter, we defined divisors on $C$ as $\mathbb{Z}$-linear combinations of $\mathbb{F}_q$-places of $C$:

$$\text{Div}(C) := \left\{ \sum_{v \in |C|} n_v \cdot v : n_v \in \mathbb{Z} \text{ almost all 0} \right\}.$$ 

The set $\text{Div}(C)$ is naturally endowed with the structure of an abelian group (“component-wise” addition). We have also defined a degree map:

$$\text{deg} : \text{Div}(C) \to \mathbb{Z}$$

which is a group homomorphism (i.e. $\text{deg}(D + D') = \text{deg} D + \text{deg} D'$). This map is well-defined because the sum is actually finite. We can thus consider its kernel

$$\text{Div}^0(C) = \ker(\text{deg} : \text{Div}(C) \to \mathbb{Z}),$$

a subgroup of $\text{Div}(C)$.

Our next goal is to explain how to associate a divisor to each rational function $f \in \mathbb{F}_q(C)^\times$, and to give some of the properties of such divisors.

4.1.1. Places and valuations. — Let $P \in C$. Since $C$ is smooth, $P$ is a smooth point of $C$ and the local ring $\mathcal{O}_{C,P} \subset \overline{\mathbb{F}}_q(C)$ is a discrete valuation ring. More concretely, it means that there is a valuation

$$\text{ord}_P : \mathcal{O}_{C,P} \to \mathbb{Z} \cup \{\infty\}, \quad f \mapsto \text{ord}_P(f) = \max \{ \nu \in \mathbb{Z}_{>0} : f \in \mathbb{M}_P^\nu \},$$

giving, for each $f \in \mathcal{O}_{C,P}$, the order of vanishing of $f$ at $P$ as a function $C \to \mathbb{P}^1$. One can extend $\text{ord}_P$ to the whole of $\overline{\mathbb{F}}_q(C)$ by setting

$$\forall f, g \in \overline{\mathbb{F}}_q(C) \times \overline{\mathbb{F}}_q(C)^\times, \quad \text{ord}_P(f/g) := \text{ord}_P(f) - \text{ord}_P(g).$$

We then restrict the obtained map to $\mathbb{F}_q(C) \subset \overline{\mathbb{F}}_q(C)$: we still denote by $\text{ord}_P : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}$ the resulting valuation. We use the usual terminology: for $f \in \mathbb{F}_q(C)^\times$, if $\text{ord}_P f \geq 0$ (resp. $\text{ord}_P f > 0$, resp. $\text{ord}_P f < 0$), one says that $f$ is regular (resp. has a zero, resp. has a pole) at $P \in C$. These terms refer implicitly to the map $f : C \to \mathbb{P}^1$ that can be canonically associated to $f \in \mathbb{F}_q(C)$ by:

$$f : C \to \mathbb{P}^1, \quad P \in C \mapsto \begin{cases} [f(P) : 1] & \text{if } f \text{ is regular at } P \\ [1 : 0] = \infty & \text{otherwise}. \end{cases}$$

The rational function $f \in \mathbb{F}_q(C)$ and the map above are usually identified without comments.
Lemma 4.1. — Let $P$ and $Q$ be two $\overline{\mathbb{F}}_q$-rational points on $C$. Then

$$\text{ord}_P = \text{ord}_Q \text{ on } \mathbb{F}_q(C) \iff P \text{ and } Q \text{ are Gal}(\mathbb{F}_q/\mathbb{F}_q)$-conjugate points,$$

i.e. $P$ and $Q$ give rise to the “same” ord function if and only if they belong to the same $\mathbb{F}_q$-place of $C$.

As a consequence, to each place $v$ of $C$, we can define a map

$$\text{ord}_v : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}, \quad f \mapsto \text{ord}_P f \quad \text{(any choice of } P \in v).$$

Proof. — Recall that there are Gal$(\mathbb{F}_q/\mathbb{F}_q)$-actions on $C(\mathbb{F}_q)$ and on $\overline{\mathbb{F}}_q(C)$, and that those actions are compatible in the sense that

$$\forall \sigma \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_q), \forall f \in \mathbb{F}_q(C), \forall P \in C(\mathbb{F}_q), \quad \sigma(f(P)) = \sigma(f)(\sigma(P)).$$

As a consequence, one can check that, for all $f \in \mathbb{F}_q(C)$,

$$\text{ord}_P \sigma(f) = \text{ord}_{\sigma(P)} f.$$

Here the functions we consider are elements of $\mathbb{F}_q(C)$ and thus, are Gal$(\mathbb{F}_q/\mathbb{F}_q)$-invariants. Hence, for all $P \in C(\mathbb{F}_q)$, and all $f \in \mathbb{F}_q(C)$, we have

$$\text{ord}_P f = \text{ord}_{\sigma(P)} f.$$

This proves that two conjugates points on $C$ give rise to the same function $\text{ord} : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}$.

We only sketch the proof of the converse statement. Let $P$, $Q$ be two points on $C$ and assume that they are not conjugate under Gal$(\mathbb{F}_q/\mathbb{F}_q)$, that is $P \in v$ and $Q \in w$ belong to two distinct places of $C$. We need to prove that $\text{ord}_P \neq \text{ord}_Q$ on $\mathbb{F}_q(C)$.

Recall that for each point $R \in C$, the fact that $\mathcal{O}_{C,R}$ is a discrete valuation ring implies the existence of uniformizers at $R$: these are functions $t_R \in \mathbb{F}_q(C)$ which “vanish at order 1 at $R$” i.e. such that $\text{ord}_RT_R = 1$ (the existence is a consequence of: $\mathcal{O}_{C,R}$ is discrete valuation ring if and only if the maximal ideal $\mathfrak{m}_R$ is principal). Then we can define a rational function $g \in \mathbb{F}_q(C)^\times$ by the (finite) product:

$$g := \prod_{Q' \in w} t_{Q'} \cdot \prod_{P' \in v} t_{P'}^{-1} \in \mathbb{F}_q(C)^\times.$$

One can check that $\text{ord}_{P'} g = -1$ at all points $P' \in v$, while $\text{ord}_{Q'} g = 1$ at all $Q' \in w$. Now fix a big enough finite extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ such that $P, Q$ are $\mathbb{F}_{q^m}$-rational, and $g$ is defined over $\mathbb{F}_{q^m}$. Let

$$h = \prod_{\sigma \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(g) \in \mathbb{F}_q(C).$$

Now, by construction of $h$ as a product of Galois conjugate, one checks that $h \in \mathbb{F}_q(C)^\times$. By the properties of $\text{ord}_R$, one has

$$\text{ord}_P h = -m \quad \text{and} \quad \text{ord}_Q h = m.$$

So, two non conjugate points ($P$ and $Q$) define distinct valuations $\text{ord}_P$ and $\text{ord}_Q$ on $\mathbb{F}_q(C)$. □

4.1.2. Zeroes and poles. — We now gather some more properties on the valuation maps $\text{ord}_v : \mathbb{F}_q(C)^\times \to \mathbb{Z}$ that we have just defined.

Proposition 4.2. — Let $f \in \mathbb{F}_q(C)$. Then:

(i) If $f$ has no poles, then $f$ is constant (i.e. $f \in \mathbb{F}_q \subset \mathbb{F}_q(C)$).
(ii) If the map $f : C \to \mathbb{P}^1$ is not constant, then it is surjective.
(iii) Hence, if $f \in \mathbb{F}_q(C) \setminus \mathbb{F}_q$ (one says that $f$ is nonconstant), then $f$ has at least a zero and at least a pole.
(iv) In general, $f$ has finitely many zeroes and poles.

We don’t prove this here, but see [NX09, Prop 3.3.1, Coro 3.3.2], Fulton’s book [Ful89], or [Har77].
Example 4.3. — As examples, consider the following two elements of $\mathbb{F}_q(x) = \mathbb{F}_q(\mathbb{P}^1)$, seen as rational functions on $C = \mathbb{P}^1$:

$$f(x) = \frac{x^2(x^3 + 1)}{(x + 1)^3(x^2 + 1)}, \quad g(x) = x^3.$$

For any place $v$ of $\mathbb{P}^1$, you can write down the values of $\text{ord}_v f$ and $\text{ord}_v g$.

4.1.3. Divisors of functions. — For all $f \in \mathbb{F}_q(C)^\times$, we put

$$\text{div}(f) := \sum_{v \in |C|} \text{ord}_v(f) \cdot v.$$

The last item in the previous proposition implies that this sum is actually finite: indeed, if $v$ is neither a pole or a zero of $f$, then $\text{ord}_v(f) = 0$ and this happens for all but finitely many places $v$. We thus obtain a map

$$\text{div} : \mathbb{F}_q(C)^\times \to \text{Div}(C), \quad f \mapsto \text{div}(f),$$

which is a group homomorphism: $\text{div}(fg) = \text{div}(f) + \text{div}(g)$ for all $f, g \in \mathbb{F}_q(C)^\times$. We denote by $\text{Princ}(C)$ the image of $\text{div}$, divisors in the subgroup $\text{Princ}(C)$ are called principal.

Proposition 4.4. — The following statements hold:

(i) For $f \in \mathbb{F}_q(C)^\times$, $\text{div}(f) = 0$ if and only if $f$ is a constant function (i.e. $f \in \mathbb{F}_q^\times \subset \mathbb{F}_q(C)^\times$).

(ii) Two nonzero rational functions $f, g$ have the same image under $\text{div}$ if and only if there exists $c \in \mathbb{F}_q^\times$ such that $f = c \cdot g$.

(iii) Most importantly, for all $f \in \mathbb{F}_q(C)^\times$, one has

$$\deg(\text{div}(f)) = 0.$$

That is, “a rational function has as many poles as zeroes (counted with multiplicities)”.

Example 4.5. — Write down the divisors of the functions $f, g$ of the previous example and check that the last item of the Lemma is true.

Proof. — Item (i) is a direct consequence of the previous proposition (a nonconstant function has at least a pole and a zero). Item (ii) follows from item (i) because $\text{div}(f/g) = \text{div}(f) - \text{div}(g)$. We don’t prove item (iii), which is a bit more difficult: for details, see [NX09, Thm. 3.4.2, Coro. 3.4.3].

4.1.4. Class group of curves. — From the previous proposition, we deduce that $\text{Princ}(C)$ is actually a subgroup of $\text{Div}^0(C)$. We can thus define the two following groups:

Definition 4.6. — The Picard group of $C$ is the quotient

$$\text{Pic}(C) := \text{Div}(C)/\text{Princ}(C);$$

and the class-group of $C$ is the “part of degree 0 of $\text{Pic}(C)$”:

$$\text{Pic}^0(C) := \text{Div}^0(C)/\text{Princ}(C).$$

We have implicitly used the fact that $\deg : \text{Div}(C) \to \mathbb{Z}$ induces a homomorphism $\deg : \text{Pic}(C) \to \mathbb{Z}$ (this follows from the fact that we mod out $\text{Div}(C)$ by $\text{Princ}(C) \subset \ker \deg$).

Two divisors $D, D' \in \text{Div}(C)$ are called (linearly) equivalent if they have the same image in $\text{Pic}(C)$, that is, if there exists a rational function $f \in \mathbb{F}_q(C)^\times$ such that $D = D' + \text{div}(f)$. The linear equivalence of divisors is indeed an equivalence relation (exercise). Note that two equivalent divisors have the same degree.

The class-group is an important invariant of a curve, it has several interpretations: it is the analogue of the class-group of a number field, it is also the set of $\mathbb{F}_q$-rational points on a variety canonically associated to $C$ (the Jacobian variety).
**Example 4.7.** — On $C = \mathbb{P}^1$, every divisor of degree 0 is principal. This implies that $\text{Pic}^0(\mathbb{P}^1)$ is the trivial group. To prove this, assume that $D = \sum v n_v \cdot v$ has degree 0, fix a point $P_0$ in each place $v$ with $n_v \neq 0$, and write each $P_v$ in homogeneous coordinates $P_v = [x_P : y_P] \in \mathbb{P}^1$. Now let $f_D$ be the rational function

$$f_D := \prod_{v \in [\mathbb{P}^1]} \left( \prod_{\sigma \in \text{Gal}(\mathbb{F}_q(v)/\mathbb{F}_q)} (\sigma(y_P)X - \sigma(x_P)Y) \right)^{n_v}.$$  

It is easy to check that $f_D$ is indeed a rational function, that $f_D \in \mathbb{F}_q(C)^\times$ and that $\text{div}(f_D) = D$. Note that $\sum n_v \deg v = 0$: this ensures that $f_D \in \mathbb{F}_q(\mathbb{P}^1)$.

It follows that, in the case of $\mathbb{P}^1$, the degree map $\deg : \text{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ is an isomorphism! The converse is also true: if $C$ is a smooth projective curve with $\text{Pic}(C) \cong \mathbb{Z}$, then $C \cong \mathbb{P}^1$.

**Example 4.8.** — Assume that $\text{char}(\mathbb{F}_q) \neq 2$ and let $e_1, e_2, e_3 \in \mathbb{F}_q$ be distinct. Consider the (projective) curve $C/\mathbb{F}_q$ defined by the (affine) equation:

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

One can check that $C$ is smooth and that it has a single point at infinity, which we denote by $P_{\infty}$. For $i = 1, 2, 3$, let $P_i = (e_i, 0) \in C$. Then

$$\text{div}(x - e_i) = 2 \cdot P_i - 2 \cdot P_{\infty}, \quad \text{div}(y) = P_1 + P_2 + P_3 - 3 \cdot P_{\infty}.$$  

Note that all the points involved are $\mathbb{F}_q$-rational, so the associated places have degree 1 (i.e. contain only the point in question), so the notation makes sense.

### 4.2. Riemann-Roch theorem

Recall that a divisor $D = \sum n_v \cdot v \in \text{Div}(C)$ is called effective (some people say positive), denoted by $D \geq 0$, if $n_v \geq 0$ for all places $v \in |C|$. Warning: the set of effective divisors is not a subgroup of $\text{Div}(C)$. Similarly, for two divisors $D_1, D_2 \in \text{Div}(C)$, one writes $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$ (note that this is a set of inequalities on the “components” of $D_1, D_2$).

This defines a partial order on $\text{Div}(C)$, which is compatible with the degree: if $D_1 \geq D_2$, then $\deg D_1 \geq \deg D_2$.

#### 4.2.1. Riemann-Roch spaces.

Writing down inequalities between divisors (of functions) is a convenient way to describe their poles and zeroes:

**Example 4.9.** — Let $f \in \mathbb{F}_q(C)^\times$ be a function that is regular everywhere, except at a place $v \in |C|$, and assume that it has a pole of order at most $n$ at $v$. These conditions on $f$ can be summarized in one inequality:

$$\text{div}(f) \geq -n \cdot v.$$  

As another example, the inequality

$$\text{div}(f) \geq 2 \cdot w - n \cdot v$$

means that $f$ is regular everywhere except maybe at $v \in |C|$ where it has a pole of order $\leq n$, and $f$ has a zero of order $\geq 2$ at $w \in |C|$.

**Definition 4.10.** — Let $D \in \text{Div}(C)$ be a divisor on $C$. We associate to $D$ the set:

$$\mathcal{L}(D) := \{ f \in \mathbb{F}_q(C)^\times : \text{div}(f) \geq -D \} \cup \{0\}.$$  

In words, $\mathcal{L}(D)$ is a set of functions on $C$ having poles and zeroes “bounded” in terms of $D$. We add the 0 function for a reason that will become obvious in a minute.

Let us gather a few facts about these sets $\mathcal{L}(D)$:

**Proposition 4.11.** — Let $D, D' \in \text{Div}(C)$.  

(i) If \( \deg D < 0 \), then \( \mathcal{L}(D) = \{0\} \).
(ii) The set \( \mathcal{L}(D) \) is a \( \mathbb{F}_q \)-vector space, and \( \mathcal{L}(D) \) has finite dimension over \( \mathbb{F}_q \).
(iii) If \( D' \) and \( D \) have the same class in \( \text{Pic}(C) \) (i.e. they differ by a principal divisor: \( D' = D + \text{div}(g) \) for some \( g \in \kappa(C)^\times \)), then \( \mathcal{L}(D) \cong \mathcal{L}(D') \).

**Proof.** — Let \( f \in \mathcal{L}(D) \) be a nonzero function. Then, \( \deg \text{div}(f) = 0 \) (see above) and this implies that

\[
0 = \deg(\text{div}(f)) \geq \deg(-D) = -\deg(D).
\]

So, the existence of \( f \in \mathcal{L}(D) \setminus \{0\} \) forces \( \deg(D) \geq 0 \). The fact that \( \mathcal{L}(D) \) is a \( \mathbb{F}_q \)-vector space is not difficult to prove: use the definition of \( \text{div}(f) \) and the properties of \( \text{ord}_v : \forall f_1, f_2 \in \mathbb{F}_q(C)^\times, \forall \lambda \in \mathbb{F}_q^\times, \text{ord}_v(f_1 + f_2) \geq \min\{\text{ord}_v f_1, \text{ord}_v f_2\}, \text{ord}_v(\lambda \cdot f_1) = \text{ord}_v f_1. \)

The hardest part of (ii) is showing that the dimension of \( \mathcal{L}(D) \) is finite: the proof of this is not that difficult, but it would take us a bit too far (for details, see [Har77, II.5.19], [Ful89] or [NX09, §3.4] or [?]). The idea is simple enough: \( D \) is a finite formal sum of places, so one can do an induction argument on the number of places that “appear” in \( D \) (more precisely on \( \sum |n_v| \)). If one can understand what happens to \( D \mapsto \mathcal{L}(D) \) on “removing a point”, i.e. replacing \( D \) by \( D - v \), we would be done. Indeed, one has \( \mathcal{L}(0) = \mathbb{F}_q \) (the zero divisor = the empty sum) because a function that has no poles is constant. One can prove that, if \( D_1 \leq D_2 \), then \( \mathcal{L}(D_1) \subset \mathcal{L}(D_2) \) (easy) and \( \dim_{\mathbb{F}_q}(\mathcal{L}(D_2)/\mathcal{L}(D_1)) \leq \deg D_2 - \deg D_1 \) (more difficult). The proof even gives a trivial upper bound on the dimension:

\[
\dim_{\mathbb{F}_q} \mathcal{L}(D) \leq \deg D + 1.
\]

Finally, if \( D' = D + \text{div}(g) \) for some \( g \in \mathbb{F}_q(C)^\times \), one can check that the map

\[
\mathcal{L}(D') \to \mathcal{L}(D), \quad f \mapsto fg
\]

gives the desired isomorphism. \( \square \)

Given a divisor \( D \in \text{Div}(C) \), we can define

\[
\ell(D) := \dim_{\mathbb{F}_q} \mathcal{L}(D).
\]

So far, we have proved that \( \ell(D) \) is finite for all \( D \), that \( \ell(D) = 0 \) if \( \deg D < 0 \), that \( \ell(0) = 1 \), and that \( \ell(D) = \ell(D') \) if \( D \) and \( D' \) have the same class in \( \text{Pic}(C) \). And we have mentioned that \( \ell(D) \leq \deg D + 1 \).

### 4.2.2. Riemann-Roch.

We can now state a fundamental result in the algebraic geometry of curves. Its importance lies in its ability to tell us whether there are functions on a curve having prescribed zeroes and poles and if so, how many. More precisely, it computes the quantity \( \ell(D) \) in terms of \( \deg D \) and of an invariant of \( C \) (which does not depend on \( D \)) called the genus of \( C \):

**Theorem 4.12 (“Weak Riemann-Roch”).** — Let \( C \) be a smooth projective curve. There exists an integer \( g \geq 0 \), called the genus of \( C \) such that:

1. \( \ell(D) \geq \deg D - g + 1 \);
2. moreover, if \( \deg D \geq 2g - 1 \), there is equality:

\[
\ell(D) = \deg D - g + 1.
\]

We shall also need the stronger version:

**Theorem 4.13 (Riemann-Roch).** — Let \( C \) be a smooth projective curve over \( \mathbb{F}_q \). There exists a divisor class \( K_C \in \text{Pic}(C) \) (the canonical class of \( C \)), and an integer \( g \geq 0 \) called the genus of \( C \), such that:

\[
\forall D \in \text{Div}(C), \quad \ell(D) - \ell(K_C - D) = \deg D - g + 1.
\]
We won’t prove this theorem, but you can have a look at [NX09, §3.5-§3.6], or [Har77], [Ful89]. Let us show that the stronger version implies the weaker one. Here is a corollary of the strong version:

**Corollary 4.14.** — Let $C$ be a smooth projective curve.

(i) $\ell(K_C) = g$, 

(ii) $\deg K_C = 2g - 2$, 

(iii) if $\deg D > 2g - 2$, then $\ell(D) = \deg D - g + 1$.

**Proof.** — For part (i), take $D = 0$ in the Theorem: we obtain the claimed equality. For part (ii), apply Riemann-Roch to $D = K_C$ and use part (i). Finally, for part (iii), use Riemann-Roch and the fact that $\ell(D) = 0$ whenever $\deg D < 0$.

The identities in the Corollary directly imply that the “strong Riemann-Roch theorem” implies “weak Riemann-Roch”.

**Example 4.15.** — Note that $\mathbb{P}^1$ has genus 0. Moreover, there are two main situations where we will need to know how to compute the genus of a curve.

1. Plane smooth curves. Let $C \subset \mathbb{P}^2$ be a smooth projective curve given by a single homogenous equation $F(x, y, z) \in \mathbb{F}_q[x, y, z]$ (we implicitly assume that $F$ is irreducible in $\mathbb{F}_q[x, y, z]$). If $F$ is homogeneous of degree $d$, then the genus of $C$ is given by:

$$g(C) = \frac{(d-1)(d-2)}{2}.$$ 

Warning: this formula is only valid for a smooth curve $C$!

2. Hyperelliptic curves. Let $\mathbb{F}_q$ be a finite field of odd characteristic, and $f(x) \in \mathbb{F}_q[x]$ be a squarefree polynomial of degree $\geq 3$. Let $C$ be the smooth projective curve over $\mathbb{F}_q$ associated to the affine plane curve $C_0$ of equation $y^2 = f(x)$ as in Homework #1 (so we have $C_0 \subset \mathbb{A}^2$ and $C \subset \mathbb{P}^N$ for some $N$ depending only on $\deg f$). Then the genus of $C$ is given by

$$g(C) = \left\lfloor \frac{\deg f - 1}{2} \right\rfloor.$$ 

### 4.2.3. Finiteness of $\text{Pic}^0(C)$. — As a first application of the Riemann-Roch theorem, we prove the following important finiteness result:

**Theorem 4.16.** — Let $C$ be a smooth projective curve over a finite field $\mathbb{F}_q$. Then its class-group $\text{Pic}^0(C)$ is a finite abelian group.

**Proof.** — The fact that $\text{Pic}^0(C)$ is abelian is obvious: $\text{Pic}^0(C)$ is defined as the quotient of an abelian group. So we now turn to the proof of the finiteness statement. Given an integer $d \geq 0$, we have proved at the beginning of this chapter that the following set is finite:

$$\{ E \in \text{Div}(C) : E \geq 0 \text{ and } \deg E = d \}.$$ 

Choose a big enough integer $d \geq 0$ (say, $d \geq g$): for any divisor $D \in \text{Div}(C)$ of degree $d$, the (weak) Riemann-Roch theorem tells us that $\ell(D) \geq d + 1 - g$, i.e. that $\ell(D) > 0$. This implies that there exists a nonzero function $f \in L(D)$. By definition, this means that the divisor $E := D + \text{div}(f)$ is effective and $\deg E = \deg D = d$.

We have just proved that, for any $D \in \text{Div}(C)$ of degree $d \geq g$, there exists an effective divisor $E \in \text{Div}(C)$ which lies in the same class in $\text{Pic}(C)$. This shows that there is a surjection from the set of effective divisors of degree $d$ to the set of divisor classes of degree $d$. Since the set of effective divisors of degree $d$ is finite (see above), we conclude that the set of divisor classes in $\text{Pic}(C)$ of degree $d$ is finite.

To finish the proof, it remains to note that there is a bijection between $\text{Pic}^0(C)$ (the set of divisor classes of degree 0) and the set $\text{Pic}^d(C)$ of divisor classes of degree $d$: indeed, the map
\[ [D] \in \Pic^d \mapsto [D - D_0] \in \Pic^0, \] where \( D_0 \in \Div(C) \) is a fixed divisor of degree \( d \), gives such a bijection.

The order of \( \Pic^0(C) \) is called the class-number of \( C \), denoted by \( h(C) \). This is another important invariant of \( C \): it serves as a more geometric analogue of the class-number of number fields. Later on (spoiler alert), we will see how to recover \( h(C) \) from the zeta function of \( C \).

### 4.3. Rationality and functional equation of the zeta function

#### 4.3.1. Preliminary results

Let us first prove two more lemmas about divisors on curves.

**Lemma 4.17.** Let \( D \in \Div(C) \) be a divisor, then

\[
\# \{ E \in \Div(C) : E \geq 0 \text{ and } [E] = [D] \text{ in } \Pic(C) \} = \frac{q^{\deg(D)} - 1}{q - 1}.
\]

In words: the class \([D] \in \Pic(C)\) of \( D \) contains \((q^{\deg(D)} - 1)/(q - 1)\) effective divisors.

**Proof.** For a divisor \( G \in \Div(C) \) in the class \([D] \) of \( D \), there is a function \( f \in \mathbb{F}_q(C)^\times \) such that \( G = D + \Div(f) \). Then \( G \) is effective if and only if \( f \in \mathcal{L}(D) \setminus \{0\} \) (see above).

There are exactly \( q^{\deg(D)} - 1 \) nonzero functions in \( \mathcal{L}(D) \) (because \( \mathcal{L}(D) \simeq (\mathbb{F}_q)^{\deg(D)} \) as \( \mathbb{F}_q \)-vector spaces), and two of them give rise to the same divisor if and only if they differ by a (multiplicative) constant \( c \in \mathbb{F}_q^\times \). Hence the result.

Given our curve \( C \), the image of the degree map \( \deg : \Div(C) \to \mathbb{Z} \) is a subgroup of \( \mathbb{Z} \): by the structure theorem of such subgroups, there exists an integer \( \delta_C \geq 1 \) such that

\[
\deg(\Div(C)) = \mathbb{Z} \cdot \delta_C.
\]

For any integer \( n \geq 0 \), let

\[
A_n(C) := \{ D \in \Div(C) : D \geq 0 \text{ and } \deg D = n \}.
\]

Recall that the zeta function of \( C/\mathbb{F}_q \) can be written under the form

\[
Z(C/\mathbb{F}_q, T) = \sum_{D \geq 0} T^{\deg D} = \sum_{n=0}^{\infty} A_n(C) \cdot T^n = 1 + \sum_{n=1}^{\infty} A_n(C) \cdot T^n.
\]

Thus, it will be of interest to be able to “compute” \( A_n(C) \) for many values of \( n \). We now give a formula for this number \( A_n(C) \) of effective divisors on \( C \) of a given degree \( n \in \mathbb{Z}_{>0} \), at least for some \( n \):

**Lemma 4.18.** Let \( C \) be a smooth projective curve over \( \mathbb{F}_q \) of genus \( g \). For all integers \( n \geq 1 \) such that \( \delta_C \mid n \) and \( n \geq \max\{0, 2g - 1\} \), one has

\[
A_n(C) = \frac{h(C)}{q - 1} \cdot (q^{n+g-1} - 1),
\]

where \( h(C) = \# \Pic^0(C) \) is the class-number of \( C \).

**Proof.** Let \( h = h(C) \), and fix representatives \( D_1, \ldots, D_h \) in \( \Div(C) \) of all divisor classes of degree \( n \) (remember that there is a bijection between the finite set \( \Pic^0(C) \) and the set of all divisors classes of degree \( n \) on \( C \)). Then, by the previous Lemma, we obtain:

\[
\# \{ D \geq 0 : \deg D = n \} = \sum_{i=1}^{h} \{ D \geq 0 : [D] = [D_i] \in \Pic(C) \} = \sum_{i=1}^{h} \frac{q^{\deg(D_i)} - 1}{q - 1}.
\]
Now by the weak Riemann-Roch theorem, for \( n \geq \max\{0, 2g - 1\} \), we have \( \ell(D_i) = \deg D_i + 1 - g = n + 1 - g \) (for all \( i \in [1, h] \)). This leads to the result:

\[
A_n(C) = \sum_{i=1}^{h} \frac{q^{\ell(D_i)} - 1}{q - 1} = \sum_{i=1}^{h} \frac{q^{n+1-g} - 1}{q - 1} = \frac{h}{q - 1} \cdot (q^{n+1-g} - 1).
\]

The use of the hypothesis that \( \delta_C \) divides \( n \) is implicit, where have we made use of it?

**4.3.2. Rationality of \( \zeta \).** — Let \( C/\mathbb{F}_q \) be a smooth projective curve over a finite field \( \mathbb{F}_q \). For any integer \( n \geq 0 \), let \( A_n(C) \) be the number of effective divisors on \( C \) of degree \( n \) (we have seen earlier that this number is finite). Recall that

\[
Z(C/\mathbb{F}_q, T) = \sum_{D \in \text{Div}(C)} A_n(C)T^n \in \mathbb{Z}[T].
\]

To know more about the zeta function, we “compute” as many coefficients \( A_n(C) \) as possible. We start by proving the following result.

**Theorem 4.19.** — There exists a divisor of degree 1 on \( C \). In other words, \( \delta_C = 1 \).

**Proof.** — We make use of the previous Lemma: denoting by \( h(C) = \# \text{Pic}^0(C) \) the class-number of \( C \), we have proved that, for all \( n \geq 1 \) such that \( \delta_C \mid n \) and \( n \geq \max\{0, 2g - 1\} \),

\[
A_n(C) = \frac{h(C)}{q - 1} \cdot (q^{n+1-g} - 1).
\]

Note that \( A_n(C) = 0 \) for all \( n \geq 1 \) that are not divisible by \( \delta_C \) (by construction of \( \delta_C \), which generates the image of the degree map). This shows that

\[
Z(C/\mathbb{F}_q, T) = \sum_{n=0}^{\infty} A_n(C) \cdot T^n = \sum_{k=0}^{\infty} A_{k\delta_C}(C) \cdot T^{k\delta_C}
= \sum_{k\delta_C < 2g-1} A_{k\delta_C}(C)T^{k\delta_C} + \sum_{k\delta_C \geq 2g-1} A_{k\delta_C}(C)T^{k\delta_C}
= F_1(T^{\delta_C}) + \frac{h(C)}{q - 1} \sum_{k\delta_C \geq 2g-1} (q^{k\delta_C+1-g} - 1) \cdot T^{k\delta_C},
\]

where \( F_1 \) is a polynomial with integral coefficients. Computing the last sum (which is the sum of two geometric series), we obtain that

\[
(q - 1) \cdot Z(C/\mathbb{F}_q, T) = F_2(T^{\delta_C}) + \frac{h(C) \cdot q^{1-g}}{1 - q^{\delta_C}T^{\delta_C}} - \frac{h(C)}{1 - T^{\delta_C}},
\]

where \( F_2 \) is a polynomial with integral coefficients. This already shows that \( Z(C/\mathbb{F}_q, T) \) is a rational function of \( T^{\delta_C} \), and moreover that \( Z(C/\mathbb{F}_q, T) \) has a simple pole at \( T = 1 \) (because \( 1 - T^{\delta} = (1 - T) \cdot (T^{\delta-1} + \cdots + 1) \) vanishes at order 1 at \( T = 1 \)).

Let us now consider the “base changed” situation: \( C \) being defined over \( \mathbb{F}_q \), it makes sense to consider it as a curve over \( \mathbb{F}_{q'} \) where \( q' = q^{\delta_C} \). Doing the same computation as above with \( C/\mathbb{F}_{q'} \) instead of \( C/\mathbb{F}_q \), we would get that \( Z(C/\mathbb{F}_{q'}, T) \) has a simple pole at \( T = 1 \) (even if the “\( \delta \)” of \( C/\mathbb{F}_{q'} \) is different from that of \( C/\mathbb{F}_q \)). Thus, the rational function \( Z(C/\mathbb{F}_q, T^{\delta_C}) \) also has a simple pole at \( T = 1 \). Now recall from the last lecture the “base change relation” for zeta functions:

\[
Z(C/\mathbb{F}_q, T^{\delta_C}) = \prod_{\zeta^{\delta_C} = 1} Z(C/\mathbb{F}_q, \zeta \cdot T),
\]
Thus, by a similar computation to that we did in the proof of 3.19, we have

$$Z(C/F_q, T^{\delta c}) = \prod_{\zeta^c \equiv 1} Z(C/F_q, T) = Z(C/F_q, T)^{\delta c}.$$  

Both $Z(C/F_q, T^{\delta c})$ and $Z(C/F_q, T)$ have a simple pole at $T = q^{-1}$, so that this last relation implies that $\delta c = 1$. 

**Remark 4.20.**— Note that the existence of a divisor of degree 1 on a curve $C$ does not imply the existence of a rational point.

For example, consider the curve $C/F_3$ defined by

$$C: \quad y^2 = -(x^3 - x)^2 - 1.$$  

The curve $C$ has genus 2, and one checks that $C$ has no $F_3$-rational points (sample check: if $x = 0$, then $-(x^3 - x)^2 - 1 = -1 = 2$ is not a square in $F_3, ...$). Denote by $\alpha_1, \alpha_2$ the roots of $z^2 = -1$ in $F_3$: $\alpha_1$ and $\alpha_2$ are conjugate under the Galois group $\text{Gal}(F_3/F_3)$ (actually, under $\text{Gal}(F_9/F_3) \simeq \mathbb{Z}/2\mathbb{Z}$) and the two points $(0, \alpha_1), (0, \alpha_2)$ on $C$ are also conjugate. In particular, they define the same $F_3$-place $v_0$ of degree 2 on $C$. Similarly, denote by $\beta_1, \beta_2, \beta_3$ the roots of $z^3 - z = -1$ in $F_3$: the $\beta_i$’s are of degree 3 over $F_3$ and they are Galois conjugates, so that the three points $(\beta_1, 1), (\beta_2, 1)$ and $(\beta_3, 1)$ on $C$ generate the same $F_3$-place $v_0$ of degree 3 on $C$. Let $D = 1 \cdot v_3 - 1 \cdot v_2 \in \text{Div}(C)$: the divisor $D$ on $C$ has degree $3 - 2 = 1$.

The theorem above allows us to prove an important rationality result on $Z(C/F_q, T)$: the following is based on Lemma 3.18, which is a consequence of the “weak Riemann-Roch” theorem. Later on, we make use of the “strong Riemann-Roch” theorem to give a more precise version.

**Theorem 4.21 (Rationality I).**— Let $C/F_q$ be a smooth projective curve of genus $g$ over a finite field $F_q$. The zeta function $Z(C/F_q, T)$ is a rational function of $T$. Moreover, it is of the form

$$Z(C/F_q, T) = \frac{L(C/F_q, T)}{(1 - T)(1 - qT)},$$

where $L(C/F_q, T) \in \mathbb{Z}[T]$ is a polynomial with integral coefficients, of degree $\leq 2g$ and which satisfies $L(C/F_q, 0) = 1$ and $L(C/F_q, 1) = h(C)$.

**Proof.**— If the genus of $C$ is $g = 0$, there is nothing to prove. So we now assume that $g \geq 1$. In this situation, Lemma 3.18 and Theorem 3.19 imply that

$$\forall n \geq 2g - 1, \quad A_n(C) = \frac{h(C)}{q - 1} \cdot (q^{n+1-g} - 1).$$

Thus, by a similar computation to that we did in the proof of 3.19, we have

$$Z(C/F_q, T) = \sum_{n \leq 2g - 1} A_n(C) \cdot T^n + \sum_{n \geq 2g - 1} A_n(C) \cdot T^n = F_1(T) + \frac{h(C)}{q - 1} \cdot \sum_{n \geq 2g - 1} (q^{n+1-g} - 1) \cdot T^n = F_2(T) + \frac{h(C)}{q - 1} \cdot \sum_{n \geq 0} (q^{n+1-g} - 1) \cdot T^n = F_2(T) + \frac{h(C) \cdot q^{1-g}}{q - 1} \cdot \frac{1}{1 - qT} - \frac{h(C)}{q - 1} \cdot \frac{1}{1 - T},$$

where $F_1$ and $F_2$ are certain polynomials with integral coefficients, of degree $\leq 2g - 2$. Thus

$$(q - 1) \cdot Z(C/F_q, T) = F_3(T) + \frac{h(C) \cdot q^{1-g}}{1 - qT} - \frac{h(C)}{1 - T},$$
where $F_3$ is a polynomial with integral coefficients (all divisible by $q - 1$), of degree $\leq 2g - 2$. Summing the three contributions and simplifying the denominators, we obtain the first assertion of the Theorem. The fact that the degree of $L(C/\mathbb{F}_q, T)$ is $\leq 2g$ follows from the fact that $\deg F_3 \leq 2g - 2$. Finally, we compute the values of $L(C/\mathbb{F}_q, T)$ at $T = 0$ and $T = 1$ as follows. First, by definition of $Z(C/\mathbb{F}_q, T)$, we have $Z(C/\mathbb{F}_q, 0) = A_0(C) \cdot T^0 + 0 = 1$; on the other hand, (4) gives $Z(C/\mathbb{F}_q, 0) = L(C/\mathbb{F}_q, 0)$. To evaluate $L(C/\mathbb{F}_q, T)$ at $T = 1$, first multiply (4) by $1 - T$ and then put $T = 1$: we get $L(C/\mathbb{F}_q, 1)/(1 - q) = ((1 - T) \cdot Z(C/\mathbb{F}_q, T)) (T = 1)$. On the other hand, multiplying (5) by $1 - T$ and evaluating at $T = 1$ gives the desired value. 

The numerator $L(C/\mathbb{F}_q, T)$ of $Z(C/\mathbb{F}_q, T)$ is called the $L$-polynomial or the $L$-function of $C/\mathbb{F}_q$. We see from (4) that $L(C/\mathbb{F}_q, T)$ is the “interesting part” of the zeta function, since the denominator does not really depend on $C/\mathbb{F}_q$. This $L$-function has several important properties, among which is the following.

4.3.3. Functional equation. — Let us now make use of the strong Riemann-Roch theorem and prove the theorem below, which is a very nice complement to Theorem 3.21:

**Theorem 4.22 (Functional Equation).** — Let $C/\mathbb{F}_q$ be a smooth projective curve of genus $g$ over a finite field $\mathbb{F}_q$. The zeta function $Z(C/\mathbb{F}_q, T)$ satisfies the functional equation:

$$Z(C/\mathbb{F}_q, T) = q^{g-1}T^{2g-2} \cdot Z \left( C/\mathbb{F}_q, \frac{1}{qT} \right).$$

As an exercise, translate this relation (given in terms of the variable $T$) into a relation in terms of the “$s$-variable” (with $T = q^{-s}$). You should obtain a relation between $\zeta(C/\mathbb{F}_q, s)$ and $\zeta(C/\mathbb{F}_q, 1 - s)$, that you should compare to the functional equation satisfied by the usual Riemann zeta function.

**Proof.** — Again, in the case where $g = 0$, there is nothing to prove: we already know that $L(C/\mathbb{F}_q, T)$ is a polynomial with degree $\leq 0$ whose value at $T = 0$ is 1, so that $L(C/\mathbb{F}_q, T) = 1$ and a direct substitution $T \leftrightarrow 1/qT$ in $Z(C/\mathbb{F}_q, T) = (1 - T)^{-1}(1 - qT)^{-1}$ gives (6). We now assume that $g \geq 1$.

To prove (6), it suffices to prove that the rational function

$$X : T \mapsto T^{1-g} \cdot Z(C/\mathbb{F}_q, T)$$

is invariant under the transformation $T \mapsto 1/qT$. Lemma 3.17 above implies that, for all $n \geq 0$,

$$A_n(C) = \sum_{\substack{[D] \in \text{Pic}(C) \\ \deg[D] = n}} \frac{q^{\ell(D)} - 1}{q - 1},$$

the sum ranging over all divisor classes of degree $n$ in Pic($C$) (note that $\ell(D)$ depends only on the class of $D$ in Pic($C$)). Since there are exactly $h(C)$ divisor classes of degree $n$ in Pic($C$) (recall the bijection between Pic$^0(C)$ and that set), we obtain that

$$(q - 1) \cdot X(T) = (q - 1) \cdot T^{1-g} \cdot Z(C/\mathbb{F}_q, T) = T^{1-g} \left( \sum_{n=0}^{\infty} \sum_{\substack{[D] \in \text{Pic}(C) \\ \deg[D] = n}} q^{\ell(D)} - 1 \right) \cdot T^n.$$
Denote by $\mathcal{D}$ the set of divisor classes $[D] \in \text{Pic}(C)$ with $0 \leq \deg[D] \leq 2g - 2$. Separating terms with $0 \leq n \leq 2g - 2$ from those with $n \geq 2g - 1$ in the last displayed equation, we get:

$$(q - 1) \cdot X(T) = \sum_{[D] \in \mathcal{D}} \left( q^{\ell(D)} - 1 \right) T^{1-g+\deg D} + \sum_{n \geq 2g-1} \left( \sum_{[D] \in \text{Pic}(C)} \sum_{\deg[D] = n} q^{\ell(D)} - 1 \right) \cdot T^n.$$

The middle sum is easy to compute:

$$\sum_{[D] \in \mathcal{D}} T^{1-g+\deg D} = \sum_{n=0}^{2g-2} h(C) \cdot T^{1-g+n} = h(C) \cdot T^{1-g} \cdot \frac{T^{2g-1} - 1}{T - 1} = h(C) \cdot \frac{Tg - T^{1-g}}{T - 1}.$$

The last sum has (essentially) already been computed in the proof of the rationality of the zeta function (based on the fact that $\ell(D) = \deg D + 1 - g$ when $\deg D \geq 2g - 1$):

$$\sum_{n \geq 2g-1} \left( \sum_{[D] \in \text{Pic}(C)} \sum_{\deg[D] = n} q^{\ell(D)} - 1 \right) \cdot T^n = h(C) \cdot \left( \frac{(qT)^{1-g}}{1 - qT} - \frac{T^{1-g}}{1 - T} \right).$$

So we have proved that

$$(q - 1) \cdot X(T) = \sum_{[D] \in \mathcal{D}} q^{\ell(D)} T^{1-g+\deg D} + h(C) \cdot \left( \frac{q^g T^g}{1 - qT} - \frac{T^{1-g}}{1 - T} \right).$$

The fact that the second part $X_2(T)$ is invariant under the substitution $T \mapsto 1/qT$ can be checked by a direct computation. It remains to see why $X_1(T) = X_1(1/qT)$ and we will be done.

We have

$$X_1(1/qT) = \sum_{[D] \in \mathcal{D}} q^{\ell(D)} \cdot (qT)^{-\deg D - 1 + g} = \sum_{[D] \in \mathcal{D}} q^{\ell(D) - \deg D - 1 + g} \cdot T^{-\deg D - 1 + g}.$$

Now, choose a divisor $K_C$ in the canonical class $[K_C] \in \text{Pic}(C)$ (whose existence is asserted by the Riemann-Roch theorem). Recall that $\deg K_C = 2g - 2$. Further, the map $D \mapsto D' = K_C - D$ is a permutation of $\mathcal{D}$. Now, by the Riemann-Roch theorem, we have

$$\ell(D) - \deg D - 1 + g = \ell(K_C - D),$$

and thus

$$X(1/qT) = \sum_{[D] \in \mathcal{D}} q^{\ell(K_C - D)} \cdot T^{\deg(K_C - D) + 1 - g} = \sum_{[D'] \in \mathcal{D}} q^{\ell(D')} \cdot T^{\deg D' + 1 - g} = X_1(T).$$

Finally, we have $X(1/qT) = X(T)$ because both $X_1$ and $X_2$ satisfy such a relation. Which proves the functional equation (6) for the zeta function!

From (6), one deduces immediately the following result.

**Corollary 4.23 (Rationality II).** — Let $L(C/\mathbb{F}_q, T)$ be the numerator of the zeta function of $C/\mathbb{F}_q$. The $L$-polynomial $L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ has degree $2g$ and satisfies

$$(7) \quad L(C/\mathbb{F}_q, T) = q^g T^{2g} \cdot L \left( C/\mathbb{F}_q, \frac{1}{qT} \right).$$
4.3.4. Consequences of the functional equation. — Let us review what we know so far about the numerator $L$.

Let $C/F_q$ be a smooth projective curve of genus $g$ over a finite field $F_q$. Write its zeta function as

$$Z(C/F_q, T) = \frac{L(C/F_q, T)}{(1 - T)(1 - qT)}.$$

The denominator of $Z(C/F_q, T)$ does not really depend on $C$, but only on the base field $F_q$. So, to compute $Z(C/F_q, T)$ for a given curve $C$, we need only compute the numerator $L(C/F_q, T)$.

We already know that $L(C/F_q, T)$ has integral coefficients and degree $2g$, and that $L(C/F_q, 0) = 1$. Moreover this polynomial satisfies a functional equation

$$L(C/F_q, T) = (qT^2)^g \cdot L \left( C/F_q, \frac{1}{qT} \right).$$

As a consequence, one deduces:

**Proposition 4.24.** — Write $L(C/F_q, T) = \sum_{i=0}^{2g} a_i T^i$, with $a_i \in \mathbb{Z}$. Then

$$\forall i \in \{0, \ldots, g\}, \quad a_{2g-i} = q^{g-i} \cdot a_i.$$

In particular, since $a_0 = 1$, we have $a_{2g} = q^g$.

**Proof.** — The relation follows from the functional equation (7):

$$(qT^2)^g \cdot L(C/F_q, (qT)^{-1}) = \sum_{i=0}^{2g} q^g T^{2g} \cdot a_i \cdot q^{-i} T^{-i} = \sum_{i=0}^{2g} q^{g-i} a_i \cdot T^{2g-i} = \sum_{j=0}^{2g} q^{j-g} a_{2g-j} \cdot T^j = \sum_{i=0}^{2g} a_i \cdot T^i = L(C/F_q, T).$$

It remains to identify coefficients of $T$.

Since we know that $a_0 = 1$, that $a_{2g} = q^g$ and that we can deduce $a_{g+1}, \ldots, a_{2g-1}$ from $a_1, \ldots, a_g$, it remains to find a way to compute these $g$ coefficients. These can be computed recursively if we know $\#C(F_{q^n})$ for sufficiently many small values of $n$ ($n = 1, \ldots, g$ will do). More precisely, factor $L(C/F_q, T)$ as a product

$$L(C/F_q, T) = \prod_{j=1}^{2g} (1 - \alpha_j \cdot T),$$

for some complex numbers $\alpha_j \in \mathbb{C}^*$ (this factorization certainly exists because $L(C/F_q, 0) = 1$, the $\alpha_j$ are then the inverses of the roots of $L$ in $\mathbb{C}$). With this notation:

**Proposition 4.25.** — For all integers $n \geq 1$,

$$(8) \quad \#C(F_{q^n}) = q^n + 1 - \sum_{j=1}^{2g} \alpha_j^n.$$

The set $\{\alpha_j\}_{j=1,\ldots,2g}$ is stable under the map $\alpha \mapsto q/\alpha$.

**Proof.** — We start with the relation:

$$(1 - T)(1 - qT) \cdot Z(C/F_q, T) = \prod_{j=1}^{2g} (1 - \alpha_j \cdot T).$$
4.3. RATIONALITY AND FUNCTIONAL EQUATION OF THE ZETA FUNCTION

We take a (formal) logarithm of this expression and expand the resulting power series, using that 
\(- \log(1 - z \cdot T) = \sum_{n \geq 1} \frac{(1 + q^n + \#C(F_q^n)) T^n}{n}\), we obtain that:

\[
\sum_{n \geq 1} \left(1 + q^n + \#C(F_q^n)\right) \frac{T^n}{n} = \sum_{n \geq 1} \left(\sum_{j=1}^{2g} \alpha_j^n\right) \frac{T^n}{n}.
\]

Which leads to the desired relation, by identification of coefficients of \(T\). The second statement follows from the functional equation because

\[
(qT^2) \cdot L(C/F_q, (qT)^{-1}) = \prod_{j=1}^{2g} \left(1 - \frac{q}{\alpha_i} \cdot T\right) = \prod_{j=1}^{2g} (1 - \alpha_j \cdot T) = L(C/F_q, T).
\]

Note also that \(\prod_{j=1}^{2g} \alpha_j = q^g\) because the leading coefficient \(a_{2g}\) of \(L\) is \(q^g\).

Now, for all \(n \geq 1\), put

\[
\sigma_n(C) = \#C(F_{q^n}) = q^n - 1 = - \sum_{j=1}^{2g} \alpha_j^n.
\]

It is clear that \(\sigma_n(C)\) can be expressed in terms of the symmetric polynomials in the \(\alpha_j\) (by the so-called Newton’s formulae). Moreover, by the relations between the coefficients and the roots of a polynomial, there is a link between the \(a_i\) and the inverse roots \(\alpha_j\). The detailed computation (left as an exercise) leads to the recursive relation:

\[
\forall i = 1, \ldots, g, \quad i \cdot a_i = \sum_{j=0}^{i-1} \sigma_{i-j}(C) \cdot a_j.
\]

It is now clear that the computation of the zeta function of \(C/F_q\) requires only the knowledge of \(\#C(F_{q^n})\) for \(n = 1, \ldots, g\).

Again, computing \(Z(C/F_q, T)\) (a power series defined in terms of \(\#C(F_{q^n})\) for all \(n\)) is equivalent to knowing only \(\#C(F_{q^n})\) for a very small number of small \(n\)! This is more or less standard nowadays, but it is still surprising.

4.3.5. Examples. — Before moving on to the next chapter, let us give a few examples of how to actually compute zeta functions.

**Example 4.26.** — Let \(k = F_3\) and consider the curve \(C_0\) defined over \(F_3\) with affine equation

\[
C_0 \subset \mathbb{A}^2 : \quad y^2 = x^3 - x.
\]

We denote by \(C \subseteq \mathbb{P}^2\) the projective closure of \(C_0\) (i.e. the curve in \(\mathbb{P}^2\) defined by homogenizing the equation for \(C_0\)). It is readily checked that \(C\) is indeed a curve, and that it is smooth. Since \(C\) is a smooth plane curve defined by a cubic equation (that is, by homogeneous polynomial of degree 3), it has genus \(g = 1\).

By the above, to compute the zeta function of \(C/F_3\), we need only compute \(\#C(F_3)\). The affine curve \(C_0\) has 3 points over \(F_3\): \((0, 0)\), \((1, 0)\) and \((2, 0)\) (as can be seen by a direct check), and \(C\) has only one point at infinity, with projective coordinates \([0 : 1 : 0] \in C\). Since this last point is clearly \(F_3\)-rational, we have \(\#C(F_3) = 4\).

After a quick computation using facts in the previous subsection, we find that

\[
Z(C/F_3, T) = \frac{3T^2 + 1}{(1 - T)(1 - 3T)} = \frac{(1 + i\sqrt{3} \cdot T)(1 - i\sqrt{3} \cdot T)}{(1 - T)(1 - 3T)}.
\]

**Example 4.27.** — Now set \(k = F_2\) and consider the two curves

\[
C_1/F_2 : \quad y^2 + xy = x^3 + x, \quad C_2/F_2 : \quad y^2 + y = x^3.
\]
As in the previous example, we only give their affine equations, but we are really dealing with the underlying projective curves. Both $C_1$ and $C_2$ are smooth projective curves over $\mathbb{F}_2$, and they both have genus 1, and one point at infinity $\infty = [0 : 1 : 0]$ which is $\mathbb{F}_2$-rational (i.e. when counting rational points, we count the affine points, which are basically solutions to the affine equations above, and we add 1 to the result). Again, computing only $\#C_1(\mathbb{F}_2)$ and $\#C_2(\mathbb{F}_2)$ will yield their zeta functions. And again, by a direct case-by-case computation, we find that

$$C_1(\mathbb{F}_2) = \{(0, 0), (1, 0), (1, 1), \infty\}, \text{ and } C_2(\mathbb{F}_2) = \{(0, 0), (0, 1), \infty\}.$$  

The arguments above lead to expressions for the zeta functions:

$$Z(C_1/\mathbb{F}_2, T) = \frac{2T^2 + T + 1}{(1 - T)(1 - 2T)}, \text{ and } Z(C_2/\mathbb{F}_2, T) = \frac{2T^2 + 1}{(1 - T)(1 - 2T)}.$$  

Note that the numerator of the first zeta function can be factored as 

$$2T^2 + T + 1 = \left(1 - \frac{-1 + i\sqrt{7}}{2}. T\right) \left(1 - \frac{-1 - i\sqrt{7}}{2}. T\right),$$  

where $-\frac{-1 \pm i\sqrt{7}}{2}$ has magnitude $\sqrt{2}$.

**Example 4.28.** — Let $p$ be a prime number such that $p \equiv 2 \bmod 3$, and consider the projective curve $C/\mathbb{F}_p$ defined by the homogeneous equation

$$C \subset \mathbb{P}^2: \quad X^3 + Y^3 + Z^3 = 0.$$  

One checks that this curve is irreducible and smooth (remember that $p$ has to be $\neq 3$), and that it has genus 1.

Since $p \equiv 2 \bmod 3$, the map $x \mapsto x^3$ is a bijection $\mathbb{F}_p \to \mathbb{F}_p$ (this map always sends 0 to 0, and its restriction to $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is a group isomorphism because 3 is coprime to the order of $\mathbb{F}_p^\times$). In particular, we deduce that there is a bijection between $C(\mathbb{F}_p) \subset \mathbb{P}^2(\mathbb{F}_p)$ and $H(\mathbb{F}_p) \subset \mathbb{P}^2(\mathbb{F}_p)$, where $H \subset \mathbb{P}^2$ is the line $H : x + y + z = 0$. Thus, $\#C(\mathbb{F}_p)$ is the same as the number of $\mathbb{F}_p$-rational points on a projective line, that is to say $\#C(\mathbb{F}_p) = \#\mathbb{P}^1(\mathbb{F}_p) = p + 1$.

From this, one easily deduces that

$$Z(C/\mathbb{F}_p, T) = \frac{pT^2 + 1}{(1 - T)(1 - pT)}.$$  

Note that, if $p \equiv 1 \bmod 3$, the curve $C/\mathbb{F}_p$ still makes sense, and is still smooth of genus 1. But we cannot use the simple argument above to compute $\#C(\mathbb{F}_p)$. Nonetheless, we know that the zeta function of $C/\mathbb{F}_p$ has the form

$$Z(C/\mathbb{F}_p, T) = \frac{pT^2 + a \cdot T + 1}{(1 - T)(1 - pT)},$$  

for some integer $a$. A more intricate computation of $\#C(\mathbb{F}_p)$ involving character sums gives a closed formula for $a$ in terms of $p$.

**Example 4.29.** — As a final example for this type of computation, let us consider the smooth projective curve $M/\mathbb{F}_3$ defined as the projective closure of the curve given by the affine equation

$$M/\mathbb{F}_3: \quad y^3 + y = x^4.$$  

One checks that $M$ is irreducible and smooth. It has genus $g = 3$. To compute its zeta function, we need only find $\#M(\mathbb{F}_3)$, $\#M(\mathbb{F}_9)$ and $\#M(\mathbb{F}_{27})$. Either by a direct case by case computation, or with a more clever point count (see Homework #1), one finds:

$$Z(M/\mathbb{F}_3, T) = \frac{27T^6 + 27T^4 + 9T^2 + 1}{(1 - T)(1 - 3T)}.$$