CHAPTER 3

RIEMANN-ROCH AND THE RATIONALITY OF ZETA FUNCTIONS

3.1. 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:

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

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

$$\deg : \mathrm{Div}(C) \to \mathbb{Z}, \quad \sum n_c \cdot v \mapsto \sum n_v \cdot \deg v,$$

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

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

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

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.

3.1.1. 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

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

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 ord_P to the whole of $\overline{\mathbb{F}_q}(C)$ by setting

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

We then restrict the obtained map to $\mathbb{F}_q(C) \subset \overline{\mathbb{F}_q}(C)$: we still denote by $\mathrm{ord}_P : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}$ the resulting valuation. We use the usual terminology: for $f \in \mathbb{F}_q(C)^\times$, if $\mathrm{ord}_P f \geq 0$ (resp. $\mathrm{ord}_P f > 0$, resp. $\mathrm{ord}_P f < 0$), 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:

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

The rational function $f \in \mathbb{F}_q(C)$ and the map above are usually identified without comments.

Lemma 3.1. — *Let P and Q be two $\overline{\mathbb{F}_q}$-rational points on C. Then*

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

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

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

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

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

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

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

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

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

This proves that two conjugates points on C give rise to the same function $\mathrm{ord} : \mathbb{F}_q(C) \to \mathbb{Z} \cup \{\infty\}$. 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 $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, that is $P \in v$ and $Q \in w$ belong to two distinct places of C. We need to prove that $\mathrm{ord}_P \neq \mathrm{ord}_Q$ 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 $t_R \in \overline{\mathbb{F}_q}(C)$ such that $\mathrm{ord}_R\, t_R = 1$ (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 $g \in \overline{\mathbb{F}_q}(C)^\times$ by the (finite) product:

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

One can check that $\mathrm{ord}_{P'}\, g = -1$ at all points $P' \in v$, while $\mathrm{ord}_{Q'}\, g = 1$ 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

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

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 ord_R, one has that

$$\mathrm{ord}_P\, h = -m \qquad \text{and } \mathrm{ord}_Q\, h = m.$$

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

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

Proposition 3.2. — *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 $f \in \mathbb{F}_q(C) \smallsetminus \mathbb{F}_q$ (one says that f is nonconstant), then f has a 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 3.3. — 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 $\mathrm{ord}_v f$ and $\mathrm{ord}_v g$.

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

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

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 $\mathrm{ord}_v(f) = 0$ and this happens for all but finitely many places v. We thus obtain a map

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

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

Proposition 3.4. — *The following statements hold:*

(i) For $f \in \mathbb{F}_q(C)^\times$, $\mathrm{div}(f) = 0$ 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 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

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

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

Example 3.5. — 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 $\mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$. We don't prove item (iii), which is a bit more difficult: for details, see [**NX09**, Thm. 3.4.2, Coro. 3.4.3]. □

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

Definition 3.6. — The Picard group of C is the quotient

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

and the class-group of C is the "part of degree 0 of $\mathrm{Pic}(C)$":

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

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

Two divisors $D, D' \in \mathrm{Div}(C)$ are called (linearly) equivalent if they have the same image in $\mathrm{Pic}(C)$, that is, if there exists a rational function $f \in \mathbb{F}_q(C)^\times$ such that $D = D' + \mathrm{div}(f)$. 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 3.7. — On $C = \mathbb{P}^1$, every divisor of degree 0 is principal. This implies that $\mathrm{Pic}^0(\mathbb{P}^1)$ is the trivial group. To prove this, assume that $D = \sum_v n_v \cdot v$ has degree 0, fix a point P_v 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

$$f_D := \prod_{\substack{v \in |\mathbb{P}^1| \\ n_V \neq 0}} \left(\prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(v)/\mathbb{F}_q)} (\sigma(y_P)X - \sigma(x_P)Y) \right)^{n_v}.$$

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

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

Example 3.8. — Assume that $\mathrm{char}(\mathbb{F}_q) \neq 2$ 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_∞. For $i = 1, 2, 3$, let $P_i = (e_i, 0) \in C$. Then

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

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.

3.2. Riemann-Roch theorem

Recall that a divisor $D = \sum n_v \cdot v \in \mathrm{Div}(C)$ 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 $\mathrm{Div}(C)$. Similarly, for two divisors $D_1, D_2 \in \mathrm{Div}(C)$, one writes $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

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

3.2.1. Riemann-Roch spaces. — Writing down inequalities between divisors (of functions) is a convenient way to describe their poles and zeroes:

Example 3.9. — 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:

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

As another example, the inequality

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

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 ≥ 2 at $w \in |C|$.

Definition 3.10. — Let $D \in \mathrm{Div}(C)$ be a divisor on C. We associate to D the set:

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

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 3.11. — *Let $D, D' \in \mathrm{Div}(C)$.*

(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* $\mathrm{Pic}(C)$ *(i.e. they differ by a principal divisor:* $D' = D + \mathrm{div}(g)$ *for some* $g \in \overline{k}(C)^\times$*), then* $\mathcal{L}(D) \simeq \mathcal{L}(D')$.

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

$$0 = \deg(\mathrm{div}(f)) \geq \deg(-D) = -\deg(D).$$

So, the existence of $f \in \mathcal{L}(D) \smallsetminus \{0\}$ 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 $\mathrm{div}(f)$ and the properties of ord_v :

$$\forall f_1, f_2 \in \mathbb{F}_q(C)^\times,\ \forall \lambda \in \mathbb{F}_q^\times, \qquad \mathrm{ord}_v(f_1 + f_2) \geq \min\{\mathrm{ord}_v f_1, \mathrm{ord}_v f_2\}, \quad \mathrm{ord}_v(\lambda \cdot f_1) = \mathrm{ord}_v f_1.$$

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 $\mathcal{L}(0) = \mathbb{F}_q$ (0 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 $D' = D + \mathrm{div}(g)$ 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. □

Given a divisor $D \in \mathrm{Div}(C)$, 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 $\mathrm{Pic}(C)$. And we have mentioned that $\ell(D) \leq \deg D + 1$.

3.2.2. Riemman-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 quantifty $\ell(D)$ in terms of $\deg D$ and of an invariant of C (which does not depend on D) called the genus of C:

Theorem 3.12 **("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) for all $D \in \mathrm{Div}(C)$*,*

$$\ell(D) \geq \deg D - g + 1;$$

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

$$\forall D \in \mathrm{Div}(C), \quad \ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

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 3.14. — *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".

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

Theorem 3.15. — *Let C be a smooth projective curve over a finite field $\mathbb{F}_q$. Then its class-group $\mathrm{Pic}^0(C)$ is a finite abelian group.*

Proof. — The fact that $\mathrm{Pic}^0(C)$ is abelian is obvious: $\mathrm{Pic}^0(C)$ 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:

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

Choose a big enough integer $d \geq 0$ (say, $d \geq g$): for any divisor $D \in \mathrm{Div}(C)$ 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 $f \in \mathcal{L}(D)$. By definition, this means that the divisor $E := D + \mathrm{div}(f)$ is effective and $\deg E = \deg D = d$.

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

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

The order of $\mathrm{Pic}^0(C)$ 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.

Example 3.16. — For $C = \mathbb{P}^1$, we have $g(\mathbb{P}^1) = 0$, and we have seen above that all divisors of degree 0 on $\mathbb{P}^1$ are principal: this means that $\mathrm{Pic}^0(\mathbb{P}^1) = 0$, *i.e.* $h(\mathbb{P}^1) = 1$.

For a less trivial example, consider a curve E over $\mathbb{F}_q$ of genus $g = 1$ and assume that $E(\mathbb{F}_q)$ is nonempty: fix a point $P_0 \in E(\mathbb{F}_q)$. As usual, we identify $\mathbb{F}_q$-rational points P on E with the associated $\mathbb{F}_q$-place $v_P = \{P\}$ of degree 1 of E. As an exercise, using the Riemann-Roch theorem, you can show that the map $P \in E(\mathbb{F}_q) \mapsto P - P_0 \in \mathrm{Div}^0(E)$ induces an isomorphism

$$E(\mathbb{F}_q) \simeq \mathrm{Pic}^0(E).$$

In particular, $h(E) = \#E(\mathbb{F}_q)$.

3.3. Rationality and functional equation of the zeta function

3.3.1. Preliminary results. — Let us first prove two more lemmas about divisors on curves.

Lemma 3.17. — *Let $D \in \mathrm{Div}(C)$ be a divisor, then*

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

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

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

There are exactly $q^{\ell(D)} - 1$ nonzero functions in $\mathcal{L}(D)$ (because $\mathcal{L}(D) \simeq (\mathbb{F}_q)^{\ell(D)}$ 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 $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ is a subgroup of $\mathbb{Z}$: by the structure theorem of such subgroups, there exists an integer $\delta_C \geq 1$ such that

$$\deg(\mathrm{Div}(C)) = \mathbb{Z} \cdot \delta_C.$$

For any integer $n \geq 0$, let

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

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 3.18. — *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*

$$A_n(C) = \frac{h(C)}{q - 1} \cdot \left(q^{n+g-1} - 1\right),$$

where $h(C) = \#\,\mathrm{Pic}^0(C)$ is the class-number of C.

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

$$\#\{D \geq 0 : deg D = n\} = \sum_{i=1}^{h} \{D \geq 0 : \ [D] = [D_i] \in \mathrm{Pic}(C)\} = \sum_{i=1}^{h} \frac{q^{\ell(D_i)} - 1}{q - 1}.$$

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:

$$A_n(C) = \sum_{i=1}^{h} \frac{q^{\ell(D_i)} - 1}{q - 1} = \sum_{i=1}^{h} \frac{q^{n+2-g} - 1}{q - 1} = \frac{h}{q - 1} \cdot (q^{n+1-g} - 1).$$

The use of the hypothesis that δ_C divides n is implicit, where have we made use of it? □