

### 2.3. Zeta functions

In this section, we consider a smooth projective curve  $C$  defined over a finite field  $k = \mathbb{F}_q$ . Assume that  $C$  is given as a projective algebraic subset of  $\mathbb{P}^n$  (i.e.  $C \subset \mathbb{P}^n$ ).

**2.3.1. Places/closed points.** — Recall that there is an action of  $G_k = \text{Gal}(\bar{k}/k)$  on  $C(\bar{k})$ , and that a point  $P \in C(\bar{k})$  is called  $k$ -rational if  $\sigma(P) = P$  for all  $\sigma \in G_k$ . In particular, given an integer  $m \geq 1$ , we can define

$$C(\mathbb{F}_{q^m}) = \text{the set of } \mathbb{F}_{q^m}\text{-rational points on } C = \{P \in C(\overline{\mathbb{F}}_q) : \sigma(P) = P, \forall \sigma \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^m})\}.$$

**Lemma 2.21.** — *For any integer  $m \geq 1$ , the set of  $\mathbb{F}_{q^m}$ -rational points on  $C$  is finite. In other words,  $C$  has only finitely many  $\mathbb{F}_{q^m}$ -rational points.*

*Proof.* — By construction,  $C$  is embedded in  $\mathbb{P}^n$  for some  $n$ . Thus  $C(\mathbb{F}_{q^m}) \subset \mathbb{P}^n(\mathbb{F}_{q^m})$  and it suffices to prove that  $\mathbb{P}^n$  has only finitely many  $\mathbb{F}_{q^m}$ -rational points. Which can be done “by hand”: more precisely, we note that

$$\#C(\mathbb{F}_{q^m}) \leq \#\mathbb{P}^n(\mathbb{F}_{q^m}) = \frac{(q^m)^{n+1} - 1}{(q^m) - 1} = (q^m)^n + (q^m)^{n-1} + \cdots + (q^m) + 1.$$

A more precise bound can be obtained by noticing that there exists a surjective algebraic map  $C \rightarrow \mathbb{P}^1$ : grouping  $\mathbb{F}_{q^m}$ -rational points according to their image by this map, one can show the existence of a  $\gamma_C > 0$  (depending only on  $C$ ) such that

$$\forall m \geq 1; \quad \#C(\mathbb{F}_{q^m}) \leq \gamma_C \cdot \#\mathbb{P}^1(\mathbb{F}_{q^m}) \leq \gamma_C \cdot (q^m + 1).$$

This latter bound can be used to prove that  $\zeta(C/\mathbb{F}_q, s)$  converges for  $\text{Re}(s) > 1$  (see below).  $\square$

Since the Galois group  $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$  is generated (topologically) by the Frobenius  $\text{Fr}_q : x \mapsto x^q$ , it can be proved that

$$C(\mathbb{F}_{q^m}) = \{P \in C(\overline{\mathbb{F}}_q) : \text{Fr}_q^m(P) = P\}.$$

It will be sometimes easier to count rational points by grouping them as follows:

**Definition 2.22.** — For a point  $P \in C(\bar{k})$ , the set of its conjugate under the action of  $G_k$ , that is  $\{\sigma(P), \sigma \in G_k\}$ , is called a place of  $C$  (over  $k$ ), or a closed point over  $k$  (or a  $k$ -closed point). The place of  $C$  associated to a point  $P$  will be denoted by  $v_P$ .

Two points in a place of  $C$  over  $k$  are called conjugate over  $k$ , they give rise to the same place. The set of places of  $C$  over  $k$  is denoted by  $|C|$ .

By construction, a place of  $C$  over  $k$  is a subset of  $C(\bar{k})$  (which is why we avoid calling a place a closed point: a closed point is not a point, it is a Galois orbits of points). Notice that a point  $P \in C(\bar{k})$  is  $k$ -rational (i.e.  $P$  has  $k$ -rational coordinates) if and only if the corresponding place has only one element.

**Lemma 2.23.** — *Let  $v$  be a place of  $C$ . Then  $v$  is a finite subset of  $C$ . We can thus define the degree of a place  $v$  of  $C$  over  $k$  to be its cardinality, denoted by  $\deg v$ .*

*Proof.* — Let  $P = [a_0 : \dots : a_n] \in C(\overline{\mathbb{F}}_q)$  be a point, and  $v = v_P$  be the corresponding place. For all  $i = 1, \dots, n$ , there exists  $m_i \in \mathbb{Z}_{\geq 1}$  such that  $a_i \in \mathbb{F}_{q^{m_i}}$ . Now put  $m = \prod m_i$ . Then  $P$  is a  $\mathbb{F}_{q^m}$ -rational point (since all its coordinates are elements of  $\mathbb{F}_{q^m}$ ). This implies that

$$\#v_P = \#\{\sigma(P), \sigma \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\} \leq \#\{\sigma(P), \sigma \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)\} \leq \#\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = m.$$

Since any place of  $C$  is of the form  $v_P$  for some  $P \in C(\overline{\mathbb{F}}_q)$ , we are done.  $\square$

A place  $v$  of  $C$  over  $\mathbb{F}_q$  has degree 1 if and only if it contains only one point  $P$ , which has to be  $\mathbb{F}_q$ -rational. Such a place is called a rational place:

$$\#\{v \in |C| : \deg v = 1\} = \#C(\mathbb{F}_q).$$

**Remark 2.24.** — For a point  $P \in C(\overline{\mathbb{F}_q})$ , say  $P = [a_0 : \dots : a_n]$  with  $a_0 \neq 0$ , the definition field of  $P$  over  $\mathbb{F}_q$ , denoted by  $k(P)$ , is defined by

$$k(P) := \mathbb{F}_q \left( \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0} \right).$$

It is a finite extension of  $\mathbb{F}_q$  and one can check that this extension is well-defined (independent of the choice of homogeneous coordinates for  $P$ , and of the index  $i$  such that  $a_i \neq 0$  (here we had  $i = 0$ )). If  $P$  and  $Q$  are two conjugate points in  $C(\overline{\mathbb{F}_q})$ , say  $Q = \sigma(P)$  for some  $\sigma \in G_k$ , then  $a_i(P) \neq 0$  if and only if  $a_i(Q) \neq 0$ , and one can show that  $k(P) = k(Q)$ . We can thus define the definition field of a place  $v$  to be  $k(P)$  for any  $P \in v$ .

The degree of  $v$  is then the degree of the extension  $k(P)/\mathbb{F}_q$ . Exercise: check the assertions in this remark.

Note also that the set  $|C|$  of all  $\mathbb{F}_q$ -places of  $C$  is the set of Galois conjugacy classes of points in  $C(\overline{\mathbb{F}_q})$ . In a sense,  $|C|$  is  $C(\overline{\mathbb{F}_q})$  modulo the Galois action. We prove two things:

**Lemma 2.25.** — For any integer  $d \geq 1$ , there are only finitely many places of  $C$  of degree  $d$ .

*Proof.* — Left as an (easy) exercise. □

**Lemma 2.26.** — For any integer  $m \geq 1$ , one has

$$C(\mathbb{F}_{q^m}) = \bigsqcup_{\substack{v \in |C| \text{ s.t.} \\ \deg v | m}} v.$$

This leads to

$$(2) \quad \#C(\mathbb{F}_{q^m}) = \sum_{d|m} d \cdot \#\{v \in |C| : \deg v = d\}.$$

*Proof.* — The second formula is a direct consequence of the first one (just take cardinality on both sides and group places according to their degrees). Now let  $P \in C(\mathbb{F}_{q^m})$  be a point and  $v_P$  be the associated place (i.e.  $v_P$  is the orbit of  $P$  under the action of  $G_{\mathbb{F}_q}$ ). Then  $v_P$  has degree (i.e. cardinality) the degree of the extension  $\mathbb{F}_q(P)/\mathbb{F}_q$ , which is a subextension of  $\mathbb{F}_{q^m}/\mathbb{F}_q$ . So that, by transitivity of degrees in finite extensions,  $\deg v_P$  divides  $m$ . To any point in  $C(\mathbb{F}_{q^m})$ , we've just associated a place  $v$  of degree  $\deg v$  dividing  $m$  with  $P \in v$ . That proves the “ $\subset$ ” inclusion, the reverse inclusion is obvious. □

You have already seen the relation (2) under a slightly different form: where?

**2.3.2. Divisors.** — One last thing we need before introducing the zeta function of a curve is the notion of divisors. The divisor group of  $C$ , denoted by  $\text{Div}(C)$ , is the free abelian group generated by the places of  $C$ . More explicitly, a divisor  $D \in \text{Div}(C)$  is a formal sum

$$D = \sum_{v \in |C|} n_v \cdot v, \quad \text{where } n_v \in \mathbb{Z} \text{ and all but finitely many } n_v \text{ are } 0.$$

And divisors are added “component-wise”. The degree of a divisor  $D$  is then defined to be  $\deg D = \sum_v n_v \cdot \deg v$ . Clearly,  $\deg : \text{Div}(C) \rightarrow \mathbb{Z}$  is a homomorphism of groups. The subgroup of divisors of degree 0 on  $C$ , denoted by  $\text{Div}^0(C)$ , is the kernel of  $\deg$ :

$$\text{Div}^0(C) = \left\{ D = \sum_v n_v \cdot v \in \text{Div}(C) : \deg v = \sum_v n_v \deg v = 0 \right\}.$$

A divisor  $D = \sum n_v \cdot v$  is effective if all coefficients  $n_v \in \mathbb{Z}$  are nonnegative:  $n_v \geq 0$  for all  $v \in |C|$ . If  $D$  is effective, one writes that  $D \geq 0$ .

For any integer  $d \geq 1$ , let  $A_d(C)$  be the cardinality of the set of divisors  $D \in \text{Div}(C)$  such that  $D \geq 0$  and  $\deg(D) = d$ .

**Lemma 2.27.** —  $A_d(C)$  is finite for all  $d \geq 1$ .

*Proof.* — Write that  $D = \sum_v n_v \cdot v$  where  $n_v \geq 0$  are integers. By definition of  $\deg(D) = \sum n_v \deg v$ , it suffices to show that there exists only finitely many places of  $C$  of a given degree  $d$ . But we have already proved this.  $\square$

**2.3.3. Riemann zeta function.** — We briefly recall a few facts about the Riemann zeta function. The Riemann zeta function  $s \mapsto \zeta(s)$  is first defined in the complex half-plane  $\operatorname{Re}(s) > 1$  by a converging Dirichlet series (or an Euler product):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

the equality between the series on the left and the product on the right (where  $p$  ranges over the set of prime numbers) is an analytic version of the unique decomposition of an integer as a product of primes.

The Gamma function is defined for all  $s$  with  $\operatorname{Re}(s) > 0$  by

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt$$

and it is then extended to the whole complex plane by the relation  $\Gamma(s+1) = s \cdot \Gamma(s)$ .

**Theorem 2.28 (Riemann).** — *The Riemann zeta function has the following analytic properties:*

**Analytic continuation :** *The zeta function  $s \mapsto \zeta(s)$  can be extended to a meromorphic function on the whole complex plane, with a unique simple pole at  $s = 1$  (with residue 1).*

**Functional equation :** *Let  $\xi(s) := \pi^{s/2} \cdot \Gamma(s/2) \cdot \zeta(s)$  be the completed zeta function. This function satisfies the functional equation*

$$\xi(1-s) = \xi(s).$$

**Conjecture: Riemann Hypothesis :** *The zeroes of  $\xi(s)$  have real part  $\operatorname{Re}(s) = 1/2$ .*

Note that  $\zeta(s)$  can not vanish on the half-plane  $\operatorname{Re}(s) > 1$  (because of the convergence of the Euler product). Given the functional equation satisfied by  $\zeta$ , and given that the Gamma function has simple poles at all  $s = -2n$  ( $n \geq 1$  integer), the zeta function has trivial zeroes at these points (those are simple poles, they “compensate” the poles of  $\Gamma(s)$  so that  $\xi(s)$  is regular at these points). By the functional equation, the trivial zeroes are the only zeroes of  $\zeta(s)$  in the half-plane  $\operatorname{Re}(s) < 0$ .

As for the zeroes of  $\zeta(s)$  in the strip  $0 \leq \operatorname{Re}(s) \leq 1$  (the so-called critical strip), one sees that they are the same as those of  $\xi(s)$ , and that they are symmetrically distributed with respect to the critical line  $\operatorname{Re}(s) = 1/2$ .

$\zeta(s)$  is a major tool to study the repartition of the prime numbers. For example, the Prime Number Theorem is a consequence of the fact that  $\zeta(s)$  does not vanish on the line  $\operatorname{Re}(s) = 1$  (it says that the number  $\pi(x)$  of primes  $\leq x$  is  $\sim x/\log x$  when  $x \rightarrow \infty$ ). Inspired by the succes of this tool, people have tried to associate zeta functions to other objects than  $\mathbb{Z}$ . We will define a zeta function for curves over finite fields, and then describe the analogy with  $\zeta(s)$ , show that it satisfies a functional equation and that it can be extended to  $\mathbb{C}$  as a meromorphic function.

**2.3.4. Counting rational points and zeta-functions.** — Throughout this section,  $C$  is a smooth projective curve defined over a finite field  $k = \mathbb{F}_q$ , and we denote by  $K = \mathbb{F}_q(C)$  its rational function field.

**Definition 2.29.** — The zeta-function of  $C/\mathbb{F}_q$  is defined as the formal series in  $s \in \mathbb{C}$ :

$$\zeta(C/\mathbb{F}_q, s) := \sum_{D \geq 0} \frac{1}{q^{\deg D \cdot s}} \in \mathbb{Z}[[q^{-s}]],$$

where the sum runs over the set of all effective divisors  $D$  on  $C$ .

One also defines another version of the zeta function, in terms of the formal variable  $T = q^{-s}$  and denoted by  $Z(C/\mathbb{F}_q, T)$ :

$$Z(C/\mathbb{F}_q, T) = \sum_{D \geq 0} T^{\deg D} \in \mathbb{Z}[[T]].$$

In our previous notations, this can be rewritten as

$$Z(C/\mathbb{F}_q, T) = \sum_{d \geq 1} A_d(C) \cdot T^d \in \mathbb{Z}[[T]].$$

**Lemma 2.30.** — The Dirichlet series defining  $\zeta(C/\mathbb{F}_q, s)$  converges on the half-plane  $\operatorname{Re}(s) > 1$  in  $\mathbb{C}$ . In other words,  $Z(C/\mathbb{F}_q, T)$  converges on the set  $\{T \in \mathbb{C} : |T| < q^{-1}\}$ .

*Proof.* — This follows from the estimate mentioned above: there exists a constant  $\gamma_C > 0$  (depending only on  $C$ ) such that

$$\forall m \geq 1; \quad \#C(\mathbb{F}_{q^m}) \leq \gamma_C \cdot \#\mathbb{P}^1(\mathbb{F}_{q^m}) \leq \gamma_C \cdot (q^m + 1).$$

Also note that  $|T| = |q^{-s}| = q^{-\operatorname{Re}(s)}$ . □

**2.3.5. Analogy with the Riemann zeta function.** — Let us prove the following two relations

**Proposition 2.31.** — One has

$$Z(C/\mathbb{F}_q, T) = \prod_{v \in |C|} (1 - T^{\deg v})^{-1} \quad \text{or} \quad \zeta(C/\mathbb{F}_q, s) = \prod_{v \in |C|} (1 - q^{-\deg v \cdot s})^{-1},$$

where the product is over all places  $v$  of  $C$  over  $\mathbb{F}_q$ .

Note that  $q^{\deg v}$  is the cardinality of the field of definition of  $v$  (i.e. the cardinality of the residue field of the corresponding valuation on  $K = \mathbb{F}_q(C)$ ).

*Proof.* — Let us work within the ring of formal power series in  $T$ . Since every effective divisor is a (finite)  $\mathbb{Z}$ -linear combination of places (with nonnegative coefficients), one has

$$Z(C/\mathbb{F}_q, T) = \sum_{D \geq 0} T^{\deg D} = \sum_{(n_v)_{v \in |C|}} T^{\sum n_v \deg v} = \prod_{v \in |C|} \left( \sum_{n_v \geq 0} T^{n_v \deg v} \right)$$

Now use the known formula for the sum of the geometric series

$$\sum_{n_v \geq 0} (T^{\deg v})^{n_v} = \frac{1}{1 - T^{\deg v}} = (1 - T^{\deg v})^{-1}.$$

□

**Proposition 2.32.** — One has

$$Z(C/\mathbb{F}_q, T) = \exp \left( \sum_{m \geq 1} \#C(\mathbb{F}_{q^m}) \cdot \frac{T^m}{m} \right).$$

*Proof.* — Expand  $\log Z(C/\mathbb{F}_q, T)$  as a power series:

$$\log Z(C/\mathbb{F}_q, T) = \sum_v -\log(1 - T^{\deg v}) = \sum_v \sum_{m=1}^{\infty} \frac{(T^{\deg v})^m}{m} = \sum_v \sum_{m=1}^{\infty} \frac{T^{m \cdot \deg v}}{m}.$$

This double sum can be rearranged into

$$\sum_v \sum_{m=1}^{\infty} \frac{T^{m \cdot \deg v}}{m} = \sum_{n=1}^{\infty} \left( \sum_{\substack{v, m \text{ s.t.} \\ m \deg v = n}} \frac{1}{m} \right) \cdot T^n,$$

where, for all  $n \geq 1$ , one has

$$\sum_{\substack{v, m \text{ s.t.} \\ m \deg v = n}} \frac{1}{m} = \frac{1}{n} \sum_{\substack{v \in |C| \text{ s.t.} \\ \deg v | n}} \deg v = \frac{\#C(\mathbb{F}_{q^n})}{n}.$$

The last equality follows from a proposition above (relation between places and rational points).  $\square$

**2.3.6. Examples “by hand”.** — Let us start by computing the zeta function of  $\mathbb{P}^1$ .

*Example 2.33.* — Let  $a_d$  be the number of places of  $\mathbb{P}^1$  of degree  $d$  (for all  $d \geq 1$ ). So  $a_1 = \#\mathbb{A}^1(\mathbb{F}_q) + 1 = q + 1$  and for  $d > 1$ ,  $a_d$  is the number of monic irreducible polynomials in  $\mathbb{F}_q[X]$  of degree  $d$ . We have seen that

$$\#\mathbb{P}^1(\mathbb{F}_{q^m}) = \sum_{d|m} d \cdot a_d = q^m + 1.$$

Therefore, a straightforward computation leads to

$$\log \left( \prod_{d \geq 1} (1 - T^d)^{-a_d} \right) = \sum_{m \geq 1} \frac{1}{m} \sum_{d|m} d a_d \frac{T^m}{m} = \sum_{m \geq 1} \frac{q^m + 1}{m} T^m.$$

And this easily implies that

$$Z(\mathbb{P}^1/\mathbb{F}_q, T) = \frac{1}{(1 - T)(1 - qT)}.$$

Or, in terms of the variable  $s$ :

$$\zeta(\mathbb{P}^1/\mathbb{F}_q, s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}.$$

We see that the function  $s \mapsto \zeta(\mathbb{P}^1/\mathbb{F}_q, s)$  is  $2\pi i / \log q$ -periodic, that it has only poles at  $s = 0$  and  $s = 1$  (modulo the period), and that it satisfies a functional equation

$$\zeta(1 - s) = q^{1-s} \zeta(s).$$

Note also that the different expressions obtained for  $Z(\mathbb{P}^1/\mathbb{F}_q, T)$  lead to

$$\begin{aligned} \forall d > 1, \# \{v \in |\mathbb{P}^1| : \deg v = d\} &= \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e} \\ &= \# \{P \in \mathbb{F}_q[X] : P \text{ monic irreducible of degree } d\}, \end{aligned}$$

and  $\#\mathbb{P}^1(\mathbb{F}_q) = q + 1$  is the number of places of degree 1.

**Example 2.34.** — Suppose that  $k = \mathbb{F}_3$  and consider the projective smooth curve  $C$ , defined over  $\mathbb{F}_3$ , whose affine equation is

$$C : y^2 = x^3 - x.$$

Then it follows from a special case of a computation of Koblitz (see [Kob75, pp. 204 – 208], article on the website of the course) that one has

$$Z(C/\mathbb{F}_3, T) = \frac{1 + 3T^2}{(1 - T)(1 - 3T)}.$$

The article [Kob75] uses elementary techniques to arrive at this result (but the proof is not the simplest...).

**Example 2.35.** — For  $p \neq 3$ , consider the projective curve  $C/\mathbb{F}_p$  defined by

$$C : x^3 + y^3 + z^3 = 0.$$

If  $p \equiv 2 \pmod{3}$ , one obtains

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

If  $p \equiv 1 \pmod{3}$ , one can also obtain an expression, but it is more involved:

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

where  $a \in \mathbb{R}$  has an explicit description (and satisfies  $|a| \leq 2\sqrt{p}$ ). The first case is easier to deal with.

**2.3.7. Behaviour under finite extension.** — Again, let us assume that  $C$  is a smooth projective curve defined over  $\mathbb{F}_q$ . Then  $C$  is also defined over  $\mathbb{F}_{q^m}$ , for any finite extension  $\mathbb{F}_{q^m}/\mathbb{F}_q$  of  $\mathbb{F}_q$ . One can relate the zeta functions  $Z(C/\mathbb{F}_q, T)$  and  $Z(C/\mathbb{F}_{q^m}, T)$  as follows:

**Proposition 2.36.** — *Let  $C$  be as above. For any  $m \geq 1$ :*

$$Z(C/\mathbb{F}_{q^m}, T^m) = \prod_{\zeta^m=1} Z(C/\mathbb{F}_q, \zeta T),$$

where the product runs over all  $\zeta \in \mathbb{C}$  such that  $\zeta^m = 1$ .

*Proof.* — See the first homework assignment. □