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*

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

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:

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

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? □

3.3.2. Rationality of ζ. — 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

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

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 3.19. — *The exists a divisor of degree* 1 *on* C. *In other words,* $\delta_C = 1$.

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

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

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

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

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

$$(q-1) \cdot Z(C/\mathbb{F}_q, T) = F_2(T^{\delta_C}) + \frac{h(C) \cdot q^{1-g}}{1 - q^{\delta_C} T^{\delta_C}} - \frac{h(C)}{1 - T^{\delta_C}}, \tag{3}$$

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, 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 "δ" 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:

$$Z(C/\mathbb{F}_{q'}, T^{\delta_C}) = \prod_{\zeta^{\delta_C} = 1} Z(C/\mathbb{F}_q, \zeta \cdot T),$$

where the product is over the complex δ_C-th roots of unity. For each such ζ, since $Z(C/\mathbb{F}_q, T)$ is actually a rational function in T^{δ_C} (see (3)), we have $Z(C/\mathbb{F}_q, \zeta \cdot T) = Z(C/\mathbb{F}_q, T)$. In particular,

$$Z(C/\mathbb{F}_{q'}, T^{\delta_C}) = \prod_{\zeta^{\delta_C} = 1} Z(C/\mathbb{F}_q, T) = Z(C/\mathbb{F}_q, T)^{\delta_C}.$$

Both $Z(C/\mathbb{F}_{q'}, T^{\delta_C})$ and $Z(C/\mathbb{F}_q, T)$ have a simple pole at $T = q^{-1}$, so that this last relation implies that $\delta_C = 1$. $\square$

Remark 3.20. — 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 $C/\mathbb{F}_3$ defined by

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

The curve C has genus 2, and one checks that C has no $\mathbb{F}_3$-rational points (sample check: if $x = 0$, then $-(x^3 - x)^2 - 1 = -1 = 2$ is not a square in $\mathbb{F}_3$, ...). Denote by α_1, α_2 the roots of $z^2 = -1$ in $\overline{\mathbb{F}_3}$: α_1 and α_2 are conjugate under the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_3}/\mathbb{F}_3)$ (actually, under $\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z}$) and the two points $(0, \alpha_1)$, $(0, \alpha_2)$ on C are also conjugate. In particular, they define the same $\mathbb{F}_3$-place v_2 of degree 2 on C. Similarly, denote by $\beta_1, \beta_2, \beta_3$ the roots of $z^3 - z = -1$ in $\overline{\mathbb{F}_3}$: the β_i's are of degree 3 over $\mathbb{F}_3$ 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 $\mathbb{F}_3$-place v_3 of degree 3 on C. Let $D = 1 \cdot v_3 - 1 \cdot v_2 \in \mathrm{Div}(C)$: the divisor D on C has degree $3 - 2 = 1$.

The theorem above allows us to prove an important rationality result on $Z(C/\mathbb{F}_q, T)$: 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 Riemman-Roch" theorem to give a more precise version.

***Theorem 3.21* (Rationality I).** — *Let $C/\mathbb{F}_q$ ba a smooth projective curve of genus g over a finite field $\mathbb{F}_q$. The zeta function $Z(C/\mathbb{F}_q, T)$ is a rational function of T. Moreover, it is of the form*

$$Z(C/\mathbb{F}_q, T) = \frac{L(C/\mathbb{F}_q, T)}{(1 - T)(1 - qT)}, \tag{4}$$

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

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

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

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

$$\begin{aligned}
Z(C/\mathbb{F}_q, T) &= \sum_{n<2g-1} A_n(C) \cdot T^n + \sum_{n \geq 2g-1} A_n(C) \cdot T^n \\
&= F_1(T) + \frac{h(C)}{q-1} \cdot \sum_{n \geq 2g-1} \left(q^{n+1-g} - 1\right) \cdot T^n \\
&= F_2(T) + \frac{h(C)}{q-1} \cdot \sum_{n \geq 0} \left(q^{n+1-g} - 1\right) \cdot T^n \\
&= F_2(T) + \frac{h(C) \cdot q^{1-g}}{q-1} \cdot \frac{1}{1-qT} - \frac{h(C)}{q-1} \cdot \frac{1}{1-T},
\end{aligned}$$

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

$$(q - 1) \cdot Z(C/\mathbb{F}_q, T) = F_3(T) + \frac{h(C) \cdot q^{1-g}}{1 - qT} - \frac{h(C)}{1 - T}, \tag{5}$$

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.

3.3.3. 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 3.22 **(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:*

$$Z(C/\mathbb{F}_q, T) = q^{g-1}T^{2g-2} \cdot Z\left(C/\mathbb{F}_q, \frac{1}{qT}\right). \tag{6}$$

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 (which explains why (6) is called a "functional equation").

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 ≤ 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 $T \mapsto 1/qT$. Lemmas 3.17 above implies that, for all $n \geq 0$,

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

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

$$(q-1)\cdot X(T) = (q-1)\cdot T^{1-g}\cdot Z(C/\mathbb{F}_q, T) = T^{1-g}\cdot \sum_{n=0}^{\infty}\left(\sum_{\substack{[D]\in \mathrm{Pic}(C)\\ \deg[D]=n}} q^{\ell(D)} - 1\right)\cdot T^n.$$

Denote by $\mathcal{D}$ the set of divisor classes $[D] \in \mathrm{Pic}(C)$ 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:

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

The middle sum is easy to compute:

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

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 $\deg D \geq 2g-1$):

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

So we have proved that

$$(q-1)\cdot X(T) = \underbrace{\sum_{[D]\in\mathcal{D}} q^{\ell(D)}T^{1-g+\deg D}}_{:=X_1(T)} + \underbrace{h(C)\cdot\left(\frac{q^gT^g}{1-qT} - \frac{T^{1-g}}{1-T}\right)}_{:=X_2(T)}.$$

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 $[K_C]\in\mathrm{Pic}(C)$ (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! $\square$

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

Corollary 3.23 **(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*

$$L(C/\mathbb{F}_q, T) = q^gT^{2g}\cdot L\left(C/\mathbb{F}_q, \frac{1}{qT}\right). \tag{7}$$

3.3.4. Consequences of the functional equation. — Last time, we proved the functional equation for the zeta function of a curve. Let us review what we know so far about the numerator L.

Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g over a finite field $\mathbb{F}_q$. Write its zeta function as

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

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

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

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

As a consequence, one deduces:

Proposition 3.24. — *Write $L(C/\mathbb{F}_q, T) = \sum_{i=0}^{2g} a_i T^i$, with $a_i \in \mathbb{Z}$. Then*

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

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

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

$$\begin{aligned}(qT^2)^g \cdot L(C/\mathbb{F}_q, (qT)^{-1}) &= \sum_{i=0}^{2g} q^g T^{2g} \cdot a_i \cdot q^{-i} T^{-i} = \sum_{i=0}^{2g} q^{g-i} a_i \cdot T^{2g-i} \\ &= \sum_{j=0}^{2g} q^{j-g} a_{2g-j} \cdot T^j = \sum_{i=0}^{2g} a_i \cdot T^i = L(C/\mathbb{F}_q, T).\end{aligned}$$

It remains to identify coefficients of T. □

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

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

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

Proposition 3.25. — *For all integers $n \geq 1$,*

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{2g} \alpha_j^n. \tag{8}$$

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

Proof. — We start with the relation:

$$(1-T)(1-qT) \cdot Z(C/\mathbb{F}_q, T) = \prod_{j=1}^{2g} (1 - \alpha_j \cdot T).$$

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

$$\sum_{n\geq 1}(1+q^n+\#C(\mathbb{F}_{q^n}))\,\frac{T^n}{n}=\sum_{n\geq 1}\left(\sum_{j=1}^{2g}\alpha_j^n\right)\cdot\frac{T^n}{n}.$$

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

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

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

Now, for all $n\geq 1$, put

$$\sigma_n(C)=\#C(\mathbb{F}_{q^n})-q^n-1=-\sum_{j=1}^{2g}\alpha_j^n.$$

It is clear that $\sigma_n(C)$ can be expressed in terms of the symmetric polynomials in the α_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 α_j. The detailed computation (left as an exercise) leads to the recursive relation:

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

It is now clear that the computation of the zeta function of $C/\mathbb{F}_q$ requires only the knowledge of $\#C(\mathbb{F}_{q^n})$ for $n=1,\cdots,g$.

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

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

Example 3.26. — Let $k=\mathbb{F}_3$ and consider the curve C_0 defined over $\mathbb{F}_3$ with affine equation

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

We denote by $C\subset\mathbb{P}^2$ 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 $C/\mathbb{F}_3$, we need only compute $\#C(\mathbb{F}_3)$. The affine curve C_0 has 3 points over $\mathbb{F}_3$: $(0,0)$, $(1,0)$ 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 $\mathbb{F}_3$-rational, we have $\#C(\mathbb{F}_3)=4$.

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

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

Example 3.27. — Now set $k=\mathbb{F}_2$ and consider the two curves

$$C_1/\mathbb{F}_2:\quad y^2+xy=x^3+x,\qquad C_2/\mathbb{F}_2:\quad y^2+y=x^3.$$

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

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

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

Example 3.28. — 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 can not 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 3.29. — 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:

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