

# Title

*D. Zack Garza*

# Contents

1	Lecture 15: The $L$ -Polynomial	3
---	---------------------------------	---

# 1 | Lecture 15: The $L$ -Polynomial

Recall that we had  $Z(t) + F(t) + G(t)$ :

$$(q-1)F(t) = \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} t^{\deg(C)}$$

$$(q-1)G(t) = h \left( \frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \right).$$

Note that  $F(t)$  is a polynomial of degree at most  $2g-2$ , and clearing denominators in  $G(t)$  yields a polynomial of degree at most  $2g$

**Definition 1.0.1** (The  $L$ -polynomial)

The  $L$ -polynomial is defined as

$$L(t) := (1-t)(1-qt)Z(t) = (1-t)(1-qt) \sum_{n=0}^{\infty} A_n t^n \in \mathbb{Z}[t].$$

It turns out that the degree bound of  $2g$  is sharp, and the coefficients closer to the middle are most interesting:

**Theorem 1.0.2** (?).

Let  $K/\mathbb{F}_q$  be a function field of genus  $g \geq 1$ , then

- $\deg L = 2g$ .
- $L(1) = h$
- $L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right)$ .
- Writing  $L(t) = \sum_{j=1}^{2g} a_j t^j$ ,
  - $a_0 = 1$  and  $a_{2g} = q^g$ .
  - For all  $0 \leq j \leq g$ , we have  $a_{2g-j} = q^{g-j} a_j$ .
  - $a_1 = |\Sigma_1(K/\mathbb{F}_q)| - (q+1)$ , which notably does not depend on  $g$ .
  - Write  $L(t) = \prod_{j=1}^{2g} (1 - \alpha_j t) \in \mathbb{C}[t]$  <sup>a</sup>
- The  $\alpha_j \in \bar{\mathbb{Z}}^b$  (which were *a priori* in  $\mathbb{C}$ ) and can be ordered such that for all  $1 \leq j \leq g$ , we have  $a_j a_{g+j} = q$ . <sup>c</sup>

f. If  $L_r(t) = (1-t)(1-q^r t)Z_r(t)$  then  $L_r(t) = \prod_{j=1}^{2g} (1 - \alpha_j^r t)$ , where  $K_r$  is the constant extension  $K\mathbb{F}_{q^r}/\mathbb{F}_{q^r}$

<sup>a</sup>The polynomial isn't monic, but rather has a constant coefficient, so this expansion is somewhat more natural than (say)  $\prod (t - \alpha)$ .

<sup>b</sup> $\bar{\mathbb{Z}}$  denotes the algebraic integers.

<sup>c</sup>This is the first hint at the Riemann hypothesis: if for example they all had the same complex modulus, this would force  $|a_j| = \sqrt{q}$ . Thus proving that they all have the same absolute value is 99% of the content!

Note that the  $\alpha_j$  are reciprocal roots.

*Proof (of a).*

We saw from  $Z(t) = F(t) + G(t)$  that  $\deg L \leq 2g$ . Equality will follow from the proof of (d) part 1, since this would imply that  $a_{2g} = q^g \neq 0$ . ■

*Proof (of b).*

Our formula  $Z(t) = F(t) + G(t)$  and Schmidt's theorem (showing  $\delta = 1$ ) gives

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1} \left( q^g t^{2g-2} (1-t) - (1-qt) \right),$$

where we've expanded  $G$  but not  $F$  because it involves various  $\ell(D)$  which are difficult to compute. It is some polynomial though, and we can evaluate  $L$  at 1 to get  $L(1) = h$ . Thus the class number is the sum of the coefficients! ■

*Proof (of c).*

This follows easily from the functional equation for  $Z(t)$ , which we already established using the Riemann-Roch theorem:

$$Z(t) = q^{g-1} t^{2g-2} Z\left(\frac{1}{qt}\right).$$

We can compute

$$\begin{aligned} q^g t^{2g} L\left(\frac{1}{qt}\right) &= q^g t^{2g} \left(1 - \frac{1}{qt}\right) \left(1 - \frac{1}{t}\right) Z\left(\frac{1}{qt}\right) \\ &= q^{g-1} t^{2g-2} (1-t)(1-qt) Z\left(\frac{1}{qt}\right) \\ &= (1-t)(1-qt) Z(t) \\ &:= L(t), \end{aligned}$$

where we've distributed one  $q$  and two  $t$ s in the first steps. ■

*Proof (of d).*

Using the functional equation from (c), we can write

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \left(\frac{a_{2g}}{q^g}\right) + \left(\frac{a_{2g-1}}{q^{g-1}}\right)t + \cdots + (a_0 q^g) t^{2g},$$

where we're correcting by enough in  $t$  but not enough in  $q$  and seeing what we get. Equating coefficients, for  $0 \leq j \leq g$  we have

$$a_{2g-j} = q^{g-j} a_j. \quad (1)$$

Using the fact that  $A_0$  is the number of effective degree zero divisors, which is only zero, we have  $A_0 = 1$  and we can multiply formal power series to obtain

$$\begin{aligned} L(t) &= a_0 + a_1 t + \cdots + a_{2g} t^{2g} = (1-t)(1-qt) \sum_{n=0}^{\infty} A_n t^n \\ &= \left(1 - (q+1)t + qt^2\right) (1 + A_1 t + A_2 t^2 + \cdots) \\ &= 1 + (A_1 - (q+1))t + \cdots \end{aligned}$$

From this, we can read off

- $L(0) = a_0 = 1$
- $a_1 = A_1 - (q+1) = \Sigma_1(K/k) - (q+1)$
- $a_{2g} = a_{2g-0} = q^{g-0} a_0 = a^g$  by taking  $j = 0$  in eq. 1, and thus  $\deg L = 2g$ .

■

*Proof (of e (the most interesting!)).*

Consider the **reciprocal polynomial**

$$L^\perp(t) := t^{2g} L\left(\frac{1}{t}\right) = t^{2g} + a_1 t^{2g-1} + \cdots + q^g.$$

The original polynomial had  $\mathbb{Z}$  coefficients and constant term 1, so this polynomial is monic and has a nonzero constant term. Thus its roots are patently nonzero algebraic integers in  $\overline{\mathbb{Z}}^\bullet$ .

If  $L^\perp(t) = \prod_{j=1}^{2g} (t - \alpha_j)$ , then

$$L(t) = t^{2g} L^\perp\left(\frac{1}{t}\right) = \prod_{j=1}^{2g} (1 - \alpha_j t)$$

and if the roots of  $L(t)$  are  $r_j$ , then the roots of  $L^\perp(t)$  are the reciprocal roots  $1/r_j$  and vice-versa. This shows the first assertion that  $r_j \in \overline{\mathbb{Z}}$  as well.

The most interesting part is what follows. Making the substitution  $t = qu$  and using (c) we

get

$$\begin{aligned}
 L^\perp(t) &= \prod_{j=1}^{2g} (t - \alpha_j) \\
 &:= t^{2g} L\left(\frac{1}{t}\right) \\
 &= q^{2g} u^{2g} L\left(\frac{1}{qu}\right) \quad \text{by (c).}
 \end{aligned}$$

Using  $u = t/q$ , we can write

$$\begin{aligned}
 q^g L(u) &= q^g \prod_{j=1}^{2g} (1 - \alpha_j u) \\
 &= q^g \prod_{j=1}^{2g} \left(1 - \frac{\alpha_j}{q} t\right) \\
 &= q^g \prod_{j=1}^{2g} \frac{\alpha_j}{q} \prod_{j=1}^{2g} \left(t - \frac{1}{\alpha_j}\right) \\
 &= \prod_{j=1}^{2g} \left(t - \frac{q}{\alpha_j}\right),
 \end{aligned}$$

where we've pulled out a factor of  $-\alpha_j/q$  and in the last step we've used that  $\prod_{j=1}^{2g} \alpha_j = q^g$ .

This follows because the  $\alpha_j$  are the roots of  $L^\perp$ , which has even degree, so the product of all of the roots is equal to the constant term of  $L^\perp$ , which is the leading term of  $L$ , which we showed was  $q^g$ .

This says that if we take these roots  $\alpha_j$  as a multiset and replace each  $\alpha_j$  with  $q/\alpha_j$ , we get the same multiset back. I.e., this multiset is stable under the involution

$$\begin{aligned}
 \mathbb{C}^\times &\rightarrow \mathbb{C}^\times \\
 z &\mapsto \frac{q}{z}.
 \end{aligned}$$

This almost pairs up the elements of this finite set of roots, except it may have fixed points. The complex numbers  $\alpha$  such that  $\alpha = q/\alpha$  are precisely  $\pm\sqrt{q}$ . So group the  $\alpha_i^{-1}$  into

- $k$  **pairs** of nonfixed points, where  $\alpha_i \neq q/\alpha_i$ ,
- $m$  points such that  $\alpha_i = \sqrt{q}$ ,
- $n$  points such that  $\alpha_i = -\sqrt{q}$ .

So we'd like to show that  $m$  and  $n$  are both even, so when we're pairing roots with reciprocals these get paired with themselves. We know  $2k + m + n = 2g$ , so  $m + n$  is even. We also know

that

$$\begin{aligned}
 q^g &= \prod_{j=1}^{2g} \alpha_j \\
 &= q^k (\sqrt{q})^m (-\sqrt{q})^n \\
 &= (-1)^n q^{k + \frac{m}{2} + \frac{n}{2}} \\
 &= (-1)^n q^g.
 \end{aligned}$$

This forces  $n$  to be even, and since  $m = 2g - 2k - n$ ,  $m$  must be even as well. ■

*Proof (of f).*

We used Dirichlet's character-style decomposition of  $Z(t)$  in Schmidt's theorem, and we'll use it again here. Write

$$\begin{aligned}
 L_r(t^r) &= (1 - t^r)(1 - q^r t^r) Z_r(t^r) \\
 &= (1 - t^r)(1 - q^r t^r) \prod_{\xi \in \mu_r} Z(\xi t) \\
 &= (1 - t^r)(1 - q^r t^r) \prod_{\xi \in \mu_r} \frac{L(\xi t)}{(1 - \xi t)(1 - q\xi t)} \\
 &= \prod_{\xi \in \mu_r} L(\xi t),
 \end{aligned}$$

where we've used that

$$\begin{aligned}
 \prod_{\xi \in \mu_r} \frac{1}{1 - \xi t} &= 1 - t^r \\
 \prod_{\xi \in \mu_r} \frac{1}{1 - q\xi t} &= 1 - q^r t^r
 \end{aligned}$$

which leads to all of the denominators canceling. We can then expand  $L_r(t^r)$  as a product to compute

$$\begin{aligned}
 L_r(t^r) &= \prod_{\xi \in \mu_r} L(\xi t) \\
 &= \prod_{\xi \in \mu_r} \prod_{j=1}^{2g} (1 - \alpha_j q t) \\
 &= \prod_{j=1}^{2g} \prod_{\xi \in \mu_r} (1 - \alpha_j q t) && \text{since these are finite products} \\
 &= \prod_{j=1}^{2g} (1 - \alpha_j^r t^r).
 \end{aligned}$$

From this we can conclude that  $L_r(t) = \prod_{j=1}^{2g} (1 - \alpha_j^r t)$ , since  $t^r$  is just an indeterminate and these are all identities of polynomials. ■

**Corollary 1.0.3(?)**.

Suppose  $K/\mathbb{F}_q$  is genus  $g \geq 1$  and  $L(t) = \prod_{j=1}^{2g} (1 - \alpha_j t)$ . Then for all  $r \in \mathbb{Z}^{\geq 0}$ , we have a nice expression for  $N_r$ :

$$N_r := |\Sigma_1(K_r/\mathbb{F}_{q^r})| = q^r + 1 - \sum_{j=1}^{2g} \alpha_j^r.$$

*Proof (?)*.

Let  $L_r(t) = \sum_{j=1}^{2g} a_{j,r} t^j = \prod_{j=1}^{2g} (1 - \alpha_j^r t)$ , so  $a_{1,r} = -\sum_{j=1}^{2g} \alpha_j^r$ . Then using (d) part 3, we can write

$$|\Sigma_1(K_r/\mathbb{F}_{q^r})| = q^r + 1 + a_{1,r} = q^r + 1 - \sum_{j=1}^{2g} \alpha_j^r.$$

This follows from consider  $\prod (1 - \alpha_j^r t)$ , where extracting the  $t^1$  coefficient involves choosing  $-\alpha_j^r$  once and 1 from all of the remaining terms, and then you sum over the disjoint possibilities. ■

**Remark 1.0.4:** We'd really like to compute the coefficients of the  $L$  polynomials, since we can solve a polynomial equation to get the roots. But the Galois groups of these polynomials may not be solvable, so the term  $\sum \alpha_j^r$  will in general be some symmetric function in the complex roots. Note that any symmetric polynomial in the roots is also a symmetric polynomial in the coefficients. ✍

**Corollary 1.0.5(?)**.

For  $K/\mathbb{F}_q$  a function field, define

$$S_r := N_r - (q^r + 1) = -\sum_{j=1}^{2g} \alpha_j^r.$$

Note that  $N_r = |\Sigma(K_r/\mathbb{F}_{q^r})|$  is the number of  $\mathbb{F}_{q^r}$ -rational point. Then

- a.  $L'(t)/L(t) = \sum_{r=1}^{\infty} S_r t^{r-1}$ .
- b.  $a_0 = 1$ , and for all  $1 \leq i \leq g$ ,

$$ia_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}.$$



**Remark 1.0.6:** What's the usefulness here? If you only have the coefficients of the  $L$  polynomials, taking the logarithmic derivative gives access to these quantities  $S_r$ . The second formula is a recursive expression for the  $a_i$  in terms of the  $S_i$ . So you can compute the coefficients of the  $L$  polynomial by counting  $\mathbb{F}_{q^r}$ -rational points on your curve (or places on your function field) for  $r = 1, 2, \dots, g$ . Similarly, if you have all of the coefficients for a  $Z$  polynomial, you can solve for the  $S_i$ .

*Proof (of a).*

Essentially just a computation. Logarithmically differentiating both sides of  $L(t) = \prod_{j=1}^{2g} (1 - \alpha_j t)$  and expanding in a geometric series yields

$$\begin{aligned} \frac{L'(t)}{L(t)} &= \sum_{j=1}^{2g} \frac{-\alpha_j}{1 - \alpha_j t} \\ &= \sum_{j=1}^{2g} (-\alpha_j) \sum_{r=0}^{\infty} (\alpha_j t)^r \\ &= \sum_{r=1}^{\infty} \left( \sum_{j=1}^{2g} (-\alpha_j^r) \right) t^{r-1} \\ &= \sum_{r=1}^{\infty} S_r t^{r-1}. \end{aligned}$$

■

*Proof (of b).*

Clearing denominators and equating coefficients in  $L'(t) = L(t) \sum_{r=1}^{\infty} S_r t^{r-1}$  yields the result immediately, since the  $ia_i$  are what appear as coefficients in the derivative of a formal power series, whereas the RHS is a Cauchy product.

■

**Remark 1.0.7:** The moral: to compute zeta functions, you don't have to enumerate divisors and compute dimensions of Riemann-Roch spaces. Note that the Riemann-Roch theorem tells us something interesting about these dimensions, but doesn't compute the dimension outright! Instead, it suffices to compute  $\mathbb{F}_{q^r}$ -rational points for  $r \leq g$ .

A few lectures ago we discussed the places on a hyperelliptic function field, including a place at infinity. Computing the zeta function of a hyperelliptic curve involves plugging in  $x$ -values and determining if it is

- A nonzero non-square: no  $y$ -values,
- Zero: exactly one  $y$ -value,
- A nonzero square: two  $y$ -values.

This is what happens at the finite places. To handle the place at  $\infty$ , there is a recipe for the degree of the polynomial in terms of the coefficients. So for any hyperelliptic function field (and in particular, for any elliptic function field) we have a concrete algorithm for computing their zeta functions. Note that this is not necessarily a *good* algorithm: it still involves plugging in many values and checking if things are squares in finite values. It seems that most people who compute a lot of zeta functions mostly focus on hyperelliptic function fields.

How are you going to compute zeta functions or even places for more complicated function fields? The Riemann-Hurwitz formula says that since any function field is a finite degree extension of a rational function field, the curve is given as a degree 2 branched cover of  $\mathbb{P}^1$ . 