LECTURE 2. THE HASSE-WEIL ZETA FUNCTION: DEFINITION AND ELEMENTARY PROPERTIES

In this lecture we introduce the Hasse-Weil zeta function, and prove some elementary properties. Before doing this, we review some basic facts about finite fields and varieties over finite fields.

1. Review of finite fields

Recall that if k is a finite field, then $|k| = p^e$ for some $e \geq 1$, where $p = \mathrm{char}(k)$. Furthermore, two finite fields with the same cardinality are isomorphic. We denote a finite field with $q = p^e$ elements (where p is a prime positive integer) by $\mathbf{F}_q$.

Let us fix $k = \mathbf{F}_q$. Given a finite field extension K/k, if $r = [K : k]$, then $|K| = q^r$. Conversely, given any $r \geq 1$, there is a field extension $k \hookrightarrow K$ of degree r. Furthermore, if $k \hookrightarrow K'$ is another such extension, then the two extensions differ by an isomorphism $K \simeq K'$. More generally, if $[K' : k] = s$, then there is a morphism of k-algebras $K \to K'$ if and only if $r|s$.

If $\overline{k}$ is an algebraic closure of k, then we have an element $\sigma \in G(\overline{k}/k)$ given by $\sigma(x) = x^q$. This is called the *arithmetic Frobenius element*, and its inverse in $G(\overline{k}/k)$ is the *geometric Frobenius element*. There is a unique subextension of k of degree r that is contained in $\overline{k}$: this is given by $K = \{x \in \overline{\mathbf{F}_q} \mid \sigma^r(x) = x\}$.

In fact, the Galois group $G(K/k)$ is cyclic or order r, with generator $\sigma|_K$. Furthermore, we have canonical isomorphisms

$$G(\overline{k}/k) \simeq \mathrm{projlim}_{K/k\,\mathrm{finite}} G(K/k) \simeq \mathrm{projlim}_{r \in \mathbf{Z}_{>0}} \mathbf{Z}/r\mathbf{Z} =: \widehat{\mathbf{Z}},$$

with σ being a topological generator of $G(\overline{k}/k)$.

2. Preliminaries: varieties over finite fields

By a variety over a field k we mean a reduced scheme of finite type over k (possibly reducible). From now on we assume that $k = \mathbf{F}_q$ is a finite field. Recall that there are two notions of points of X in this context, as follows.

Note that X is a topological space. We denote by X_{cl} the set of closed points of X (in fact, these are the only ones that we will consider). Given such $x \in X_{\mathrm{cl}}$, we have the local ring $\mathcal{O}_{X,x}$ and its residue field $k(x)$. By definition, $k(x)$ is isomorphic to the quotient of a finitely generated k-algebra by a maximal ideal, hence $k(x)$ is a finite extension of k by Hilbert's Nullstellensatz. We put $\deg(x) := [k(x) : k]$.

On the other hand, we have the notion of K-valued points of X. Recall that if $k \to K$ is a field homomorphism, the the set of K-valued points of X is

$$X(K) := \mathrm{Hom}_{\mathrm{Spec}\,k}(\mathrm{Spec}\,K, X) = \bigsqcup_{x \in X} \mathrm{Hom}_{k-\mathrm{alg}}(k(x), K).$$

We will always consider the case when the extension K/k is algebraic. In this case, if $\varphi\colon \mathrm{Spec}\,K \to X$ is in $X(K)$, the point $x \in X$ that is the image of the unique point in $\mathrm{Spec}\,K$ is closed: indeed, we have $\dim \overline{\{x\}} = \mathrm{trdeg}(k(x)/k) = 0$. In particular, we see that if K/k is a finite extension of degree r, then

$$X(K) = \bigsqcup_{\deg(x)|r} \mathrm{Hom}_{k-\mathrm{alg}}(k(x), K). \tag{1}$$

Note that if $\deg(x) = e|r$, then $\mathrm{Hom}_{k-\mathrm{alg}}(k(x), K)$ carries a transitive action of $G(\mathbf{F}_{q^r}/\mathbf{F}_q) \simeq \mathbf{Z}/r\mathbf{Z}$. The stabilizer of any element is isomorphic to $G(\mathbf{F}_{q^r}/\mathbf{F}_{q^e})$, hence

$$|\mathrm{Hom}_{k-\mathrm{alg}}(k(x), K)| = e.$$

In particular, this proves the following

Proposition 2.1. *If X is a variety over the finite field k, and K/k is a field extension of degree r, then*

$$|X(K)| = \sum_{e|r} e \cdot |\{x \in X_{\mathrm{cl}} \mid \deg(x) = e\}.$$

Remark 2.2. It is clear that if $X = Y_1 \cup \ldots \cup Y_m$, where each Y_i is a locally closed subset of X, then $X(K) = Y_1(K) \cup \ldots \cup Y_m(K)$. Furthermore, if the former union is disjoint, then so is the latter one.

Remark 2.3. Suppose that X is affine, and consider a closed embedding $X \hookrightarrow \mathbf{A}^n_k$ defined by the ideal $(F_1, \ldots, F_d) \subseteq k[x_1, \ldots, x_n]$. If K/k is a field extension, then we have an identification

$$X(K) = \{(u_1, \ldots, u_n) \in K^n \mid f_i(u_1, \ldots, u_n) = 0 \,\text{for}\, 1 \leq i \leq d\}.$$

In particular, we see that if K/k is finite, then $X(K)$ is finite. The formula in Proposition 2.1 now implies that for every $e \geq 1$, there are only finitely many $x \in X$ with $\deg(x) = e$. Of course, by taking an affine open cover of X, we deduce that these assertions hold for arbitrary varieties over k.

It is often convenient to think of K-valued points in terms of an algebraic closure of the ground field. Suppose that $\overline{k}$ is a fixed algebraic closure of k, and let us write $\mathbf{F}_{q^r}$ for the subfield of $\overline{k}$ of degree r over k. Let $\overline{X} = X \times_{\mathrm{Spec}\,k} \mathrm{Spec}\,\overline{k}$. This is a variety over $\overline{k}$ (the fact that $\overline{X}$ is reduced follows from the fact that X is reduced and k is perfect; however, we will not need this). Note that by definition we have $\overline{X}(\overline{k}) = X(\overline{k})$.

Consider the Frobenius morphism $\mathrm{Frob}_{X,q}\colon X \to X$ on X. This is the identity on X, and the morphism of sheaves of rings $\mathcal{O}_X \to \mathcal{O}_X$ is given by $u \to u^q$ (since $u^q = u$ for every $u \in k$, we see that $\mathrm{Frob}_{X,q}$ is a morphism of schemes over k. In particular, it induces a morphism of schemes over $\overline{k}$:

$$\mathrm{Frob}_{\overline{X},q} = \mathrm{Frob}_{X,q} \times \mathrm{id}\colon \overline{X} \to \overline{X}.$$

Note that this is a functorial construction. In particular, if X is affine and if we consider a closed immersion $X \hookrightarrow \mathbf{A}_k^N$, then $\mathrm{Frob}_{\overline{X},q}$ is induced by $\mathrm{Frob}_{\mathbf{A}_{\overline{k}}^N,q}$. This is turn corresponds to the morphism of $\overline{k}$-algebras

$$\overline{k}[x_1,\ldots,x_N] \to \overline{k}[x_1,\ldots,x_N],\ x_i \to x_i^q,$$

hence on $\overline{k}$-points it is given by $(u_1,\ldots,u_N) \to (u_1^q,\ldots,u_N^q)$. We conclude that the natural embedding

$$X(\mathbf{F}_{q^r}) \hookrightarrow X(\overline{k}) = \overline{X}(\overline{k})$$

identifies $X(\mathbf{F}_{q^r})$ with the elements of $\overline{X}(\overline{k})$ fixed by $\mathrm{Frob}_{\overline{X},q}^r$. Indeed, this is clear when $X = \mathbf{A}_k^N$ by the previous discussion, and the general case follows by considering an affine open cover, and by embedding each affine piece in a suitable affine space.

In other words, if $\Delta, \Gamma_r \subset \overline{X} \times \overline{X}$ are the diagonal, and respectively, the graph of $\mathrm{Frob}_{\overline{X},q}^r$, then $X(\mathbf{F}_{q^r})$ is in natural bijection with the closed points of $\Gamma_r \cap \Delta$. The following proposition shows that when X smooth, this is a transverse intersection.

Proposition 2.4. *If X is smooth over $k = \mathbf{F}_q$, then the intersection $\Gamma_r \cap \Delta$ consists of a reduced set of points.*

Note that since k is perfect, X is smooth over k if and only if it is nonsingular.

Proof. We have already seen that the set $\Gamma_r \cap \Delta$ is finite, since it is in bijection with $X(\mathbf{F}_{q^r})$. In order to show that it is a reduced set, let us consider first the case when $X = \mathbf{A}_{\mathbf{F}_q}^n$. In this case, if $R = \overline{k}[x_1,\ldots,x_n,y_1,\ldots,y_n]$, then $\Delta \subset \operatorname{Spec} R$ is defined by $(y_1 - x_1,\ldots,y_n - x_n)$ and Γ_r is defined by $(y_1 - x_1^q,\ldots,y_r - x_r^q)$. Therefore $\Gamma_r \cap \Delta$ is isomorphic to $\prod_{i=1}^n \operatorname{Spec} k[x_i]/(x_i - x_i^q)$, hence it is reduced (note that the polynomial $x_i^q - x_i$ has no multiple roots).

For an arbitrary smooth variety X, let us consider $u \in X(\mathbf{F}_{q^e})$, and let $x \in X$ be the corresponding closed point. If $t_1,\ldots,t_n$ form a regular system of parameters of $\mathcal{O}_{X,x}$, it follows that $(t_1,\ldots,t_n)$ define an étale map $U \to \mathbf{A}^n$, where U is an open neighborhood of x. Note that the restriction to $\overline{U} \times \overline{U}$ of Δ and Γ_r are the inverse images via $\overline{U} \times \overline{U} \to \mathbf{A}_{\overline{k}}^n \times \mathbf{A}_{\overline{k}}^n$ of the corresponding subsets for $\mathbf{A}_{\overline{k}}^n$. Since the inverse image of a smooth subscheme by an étale morphism is smooth, we deduce the assertion in the proposition for X from the assertion for $\mathbf{A}_k^n$. □

Exercise 2.5. Let X and $\overline{X}$ be as above. The group $G = G(\overline{k}/k)$ acts on the right on $\operatorname{Spec} \overline{k}$, by algebraic automorphisms.

i) Show that G has an induced right action on $\overline{X}$, by acting on the second component of $X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. Of course, these automorphisms are not of schemes over $\overline{k}$.
ii) Let $\tau \colon \overline{X} \to \overline{X}$ be the action of the arithmetic Frobenius element. Describe τ when $X = \mathbf{A}_k^n$. Show that $\tau \circ \mathrm{Frob}_{\overline{X},q} = \mathrm{Frob}_{\overline{X},q} \circ \tau$, and they are equal to the absolute q-Frobenius morphism of $\overline{X}$ (recall: this is the identity on $\overline{X}$, and the morphism of sheaves of rings $\mathcal{O}_{\overline{X}} \to \mathcal{O}_{\overline{X}}$ is given by $u \to u^q$).

iii) We also have a natural left action of G on $X(\overline{k})$ that takes (g,φ) to $\varphi\circ g$ (where we identify g with the corresponding automorphism of $\operatorname{Spec}\overline{k}$). Show that the arithmetic Frobenius acts on $X(\overline{k})=\overline{X}(\overline{k})$ by the map induced by $\mathrm{Frob}_{\overline{X},q}$.

iv) The canonical projection $\overline{X}\to X$ induces a map $\overline{X}_{\rm cl}\to X_{\rm cl}$. Show that this is identified via $X(\overline{k})=\overline{X}(\overline{k})=\overline{X}_{\rm cl}$ with the map described at the beginning of this section, that takes a $\overline{k}$-valued point of X to the corresponding closed point of X.

v) We similarly have a left action of $G(\mathbf{F}_{q^r}/\mathbf{F}_q)$ on $X(\mathbf{F}_{q^r})$. Show that the fibers of the map $X(\mathbf{F}_{q^r})\to X_{\rm cl}$ that takes an $\mathbf{F}_{q^r}$-valued point to the corresponding closed point of X are precisely the orbits of the $G(\mathbf{F}_{q^r}/\mathbf{F}_q)$-action.

3. The Hasse-Weil zeta function

3.1. **The exponential and the logarithm power series.** Recall that the exponential formal power series is given by

$$\exp(t)=\sum_{m\geq 0}\frac{t^n}{n!}\in\mathbf{Q}[\![t]\!].$$

We will also make use of the logarithm formal power series, defined by

$$\log(1+t)=\sum_{m\geq 1}\frac{(-1)^{m+1}t^m}{m}\in\mathbf{Q}[\![t]\!].$$

In particular, we may consider $\exp(u(t))$ and $\log(1+u(t))$ whenever $u\in t\mathbf{Q}[\![t]\!]$.

We collect in the following proposition some well-known properties of the exponential and logarithm formal power series. We will freely use these properties in what folows.

Proposition 3.1. *The following properties hold:*

i) *We have* $\exp(t)'=\exp(t)$ *and* $\log(1+t)'=(1+t)^{-1}$.
ii) $\exp(s+t)=\exp(s)\cdot\exp(t)$ *in* $\mathbf{Q}[\![s,t]\!]$. *In particular, we have* $\exp(u+v)=\exp(u)\cdot\exp(v)$ *for every* $u,v\in t\mathbf{Q}[\![t]\!]$.
iii) $\exp(mt)=\exp(t)^m$ *for every* $m\in\mathbf{Z}$. *In particular,* $\exp(mu)=\exp(u)^m$ *for every* $u\in t\mathbf{Q}[\![t]\!]$.
iv) $\log(\exp(u))=u$ *and* $\exp(\log(1+u))=1+u$ *for every* $u\in t\mathbf{Q}[\![t]\!]$.
v) $\log((1+u)(1+v))=\log(1+u)+\log(1+v)$ *for every* $u,v\in t\mathbf{Q}[\![t]\!]$.
vi) $\log((1+u)^m)=m\cdot\log(1+u)$ *for every* $m\in\mathbf{Z}$ *and every* $u\in t\mathbf{Q}[\![t]\!]$.

Proof. The proofs are straightforward. i) and ii) follow by direct computation, while iii) is a direct consequence of i). It is enough to prove the assertions in iv) for $u=t$. The first assertion now follows by taking formal derivatives of the both sides. Note that we have two ring homomorphisms $f,g\colon\mathbf{Q}[\![t]\!]\to\mathbf{Q}[\![t]\!]$, $f(u)=\log(1+u)$ and $g(v)=\exp(v)-1$. They are both isomorphisms by the formal Inverse Function theorem, and $f\circ g=\mathrm{Id}$ by the first equality in iv). Therefore $g\circ f=\mathrm{Id}$, which is the second equality in iv). The assertions in v) and vi) now follow from ii) and iii) via iv). $\square$

3.2. **The definition of the Hasse-Weil zeta function.** Suppose that X is a variety over a finite field $k = \mathbf{F}_q$. For every $m \geq 1$, let $N_m = |X(\mathbf{F}_{q^m})|$[1]. The Hasse-Weil zeta function of X is

$$Z(X,t) = \exp\left(\sum_{m\geq 1} \frac{N_m}{m} t^m\right) \in \mathbf{Q}[\![t]\!]. \tag{2}$$

The following proposition gives a product formula for $Z(X,t)$ that is very useful in practice.

Proposition 3.2. *For every variety X over $\mathbf{F}_q$, we have*

$$Z(X,t) = \prod_{x\in X_{\mathrm{cl}}} (1 - t^{\deg(x)})^{-1}. \tag{3}$$

In particular, $Z(X,t) \in \mathbf{Z}[\![t]\!]$.

By making $t = p^{-s}$, we see that the above formula is analogous to the product formula for the Riemann zeta function.

Proof. Let us put $a_r := |\{x \in X_{\mathrm{cl}} \mid [k(x) : \mathbf{F}_q] = r\}|$ for every $r \geq 1$. Therefore the right-hand side of (3) is equal to $\prod_{r\geq 1}(1-t^r)^{-a_r}$. It is clear that this product is well-defined in $\mathbf{Z}[\![t]\!]$.

Recall that by Proposition 2.1, we have $N_m = \sum_{r|m} r\cdot a_r$. It follows from definition that

$$\log(Z(X,t)) = \sum_{m\geq 1} \frac{N_m}{m} t^m = \sum_{m\geq 1}\sum_{r|m} \frac{r\cdot a_r}{m} t^m = \sum_{r\geq 1} a_r \cdot \sum_{\ell\geq 1} \frac{t^{\ell r}}{\ell} = \sum_{r\geq 1} (-a_r)\cdot \log(1-t^r)$$
$$= \sum_{r\geq 1} \log(1-t^r)^{-a_r} = \log\left(\prod_{r\geq 1}(1-t^r)^{-a_r}\right).$$

The formula (3) now follows applying exp on both sides. □

Remark 3.3. Suppose that $q = (q')^m$. If X is a variety over $\mathbf{F}_q$, we may consider X as a variety over $\mathbf{F}_{q'}$, in the natural way. For every closed point $x \in X$, we have $\deg(k(x)/\mathbf{F}_{q'}) = m\cdot \deg(k(x)/\mathbf{F}_q)$. It follows from Proposition 3.2 that $Z(X/\mathbf{F}_{q'}, t) = Z(X, \mathbf{F}_q, t^m)$.

Remark 3.4. One can interpret the formula in Proposition 3.2 by saying that $Z(X,t)$ is a generating function for the effective 0-cycles on X. Recall that the group of 0-cycles $Z_0(X)$ is the free abelian group generated by the (closed) points of X. Given a 0-cycle $\alpha = \sum_{i=1}^r m_i x_i$, its degree is $\deg(\alpha) = \sum_{i=1}^r m_i \deg(x_i)$. A 0-cycle $\sum_i m_i x_i$ is *effective* if all m_i are nonnegative. With this terminology, we see that the formula in Proposition 3.2 can be rewritten as

$$Z(X,t) = \prod_{x\in X_{\mathrm{cl}}} (1 + t^{\deg(x)} + t^{2\deg(x)} + \ldots),$$

[1]If k' is a finite extension of k of degree m, then the set $X(k')$ depends on this extension. However, any two extension of k of the same degree differ by a k-automorphism, hence $|X(k')|$ only depends on $|k'|$.

and multiplying we obtain

$$Z(X,t)=\sum_{\alpha}t^{\deg(\alpha)}, \tag{4}$$

where the sum is over all effective 0-cycles on X.

3.3. **Examples and elementary properties.** We start with the example of the affine space.

Example 3.5. Let $k=\mathbf{F}_q$, and $X=\mathbf{A}^n_k$. It is clear that for every finite extension k'/k we have $X(k')=(k')^n$, hence $|X(k')|=|k'|^n$. We conclude that

$$Z(\mathbf{A}^n,t)=\exp\left(\sum_{m\geq 1}\frac{q^{mn}}{m}t^m\right)=\exp\left(-\log(1-q^nt)\right)=\frac{1}{(1-q^nt)}.$$

Example 3.6. More generally, note that for every two varieties X and Y, we have $X\times Y(k')=X(k')\times Y(k')$. In particular, if $X=\mathbf{A}^n$, we have $|\mathbf{A}^n\times Y(\mathbf{F}_{q^m})|=|Y(\mathbf{F}_{q^m})|q^{mn}$, hence

$$Z(\mathbf{A}^n\times Y,t)=\exp\left(\sum_{m\geq 1}\frac{|Y(\mathbf{F}_{q^m})|q^{mn}}{m}t^m\right)=Z(Y,q^nt).$$

Proposition 3.7. *If X is a variety over $\mathbf{F}_q$, and Y is a closed subvariety of X, then $Z(X,t)=Z(Y,t)\cdot Z(U,t)$, where $U=X\smallsetminus Y$.*

Proof. It is clear that for every $m\geq 1$ we have $|X(\mathbf{F}_{q^m})|=|Y(\mathbf{F}_{q^m})|+|U(\mathbf{F}_{q^m})|$. The assertion in the proposition is an immediate consequence of this and of the fact that $\exp(u+v)=\exp(u)\cdot\exp(v)$ for every $u,v\in t\mathbf{Q}[\![t]\!]$. □

Corollary 3.8. *The zeta function of the projective space is given by*

$$Z(\mathbf{P}^n_{\mathbf{F}_q},t)=\frac{1}{(1-t)(1-qt)\cdots(1-q^nt)}.$$

Proof. The assertion follows from Example 3.5 by induction on n, using Proposition 3.7, and the fact that we have a closed embedding $\mathbf{P}^{n-1}_{\mathbf{F}_q}\hookrightarrow\mathbf{P}^n_{\mathbf{F}_q}$, whose complement is isomorphic to $\mathbf{A}^n_{\mathbf{F}_q}$. □

Proposition 3.9. *Let X be a variety over $k=\mathbf{F}_q$, and let k'/k be a field extension of degree r. If $X'=X\times_{\operatorname{Spec}k}\operatorname{Spec}k'$, then*

$$Z(X',t^r)=\prod_{i=1}^{r}Z(X,\xi^it),$$

where ξ is a primitive root of order r of 1.

Proof. Let us put $N'_m:=|X'(\mathbf{F}_{q^{rm}})|$ and $N_m=|X(\mathbf{F}_{q^m})|$, hence $N'_m=N_{mr}$. By definition, it is enough to show that

$$\sum_{m\geq 1}\frac{N_{mr}}{m}t^{mr}=\sum_{i=1}^{r}\sum_{\ell\geq 1}\frac{N_\ell}{\ell}\xi^{i\ell}t^\ell.$$

This is a consequence of the fact that $\sum_{i=1}^{r} \xi^{i\ell} = 0$ if r does not divide ℓ, and it is equal to r, otherwise. $\square$