Master Thesis

L-functions of Algebraic Curves over Finite Fields

Author:
Ha Van Hieu

Supervisor:
Prof. Boas Erez

Università degli Studi di Padova

UNIVERSITÀ DEGLI STUDI DI PADOVA

UNIVERSITÉ BORDEAUX 1

July 2013

Abstract

Counting the number of solutions of a homogeneous polynomial is one of the fundamental unity of mathematics. Studying them will lead to the studying of zeta functions (a special case of L-functions). Indeed, let's begin by a simple example. Consider the curve C of genus 3 with equation $X^3Y+Y^3Z+Z^3X=0$ defined over $k=\mathbb{F}_2$. Let N_d be the number of points with coordinates in $\mathbb{F}_{2^d}$. By direct computing, we have that $N_d = 2^d+1$ if $3 \nmid d$, and $N_d = 2^d+1-a_d$ if $3 \mid d$, where the a_i are found from $a_3=-15, a_6=27$ and $a_{3k+6}+5a_{3k+3}+8a_{3k}=0 (k \geq 1)$.
Put

$$Z(C,t) = exp\big(\sum_{i\geq 1}\frac{1}{i}N_i t^i\big).$$

Then in this example, it is easy to see that

$$Z(C,t) = \frac{1+5t^3+8t^6}{(1-t)(1-2t)},$$

a simple rational function that encodes the values of all N_i. Conversely, if we know that

$$Z(C,t) = \frac{1+5t^3+8t^6}{(1-t)(1-2t)},$$

we can easily implies the values of N_i. In other words, the given expression of $Z(C,t)$ is equivalent to the given values of N_i.
We can easily see that the zeta functions defined in the example is a rational function and all of roots of $1+5t^3+8t^6$ have the norm $2^{-1/2}$. In general, let X be a complete smooth curve over $\mathbb{F}_q$ with N_i points over $\mathbb{F}_{q^i}$ and the zeta function of X be

$$Z(X,t) = exp\big(\sum_{i\geq 1}\frac{1}{i}N_i t^i\big).$$

Then Hasse (for genus $g=1$) and Weil (for the general case) showed that this function is a rational function of the form

$$\frac{P(t)}{(1-t)(1-qt)}$$

where $P(t)$ is a polynomial in t of degree $2g$. Moreover, by studying Weil cohomology, he is also available to prove the *the functional equation* and the *Riemann hypothesis* (see detail in the chapter 3). Besides, he gave the conjecture that they also hold for any variety. The story of the Weil conjectures is really a marvelous example of mathematical imagination, and one of the most striking instances exhibiting the fundamental unity of mathematics. The essential ideas which led to their proof are due to six men: E. Artin,

F.K.Schmidt, H. Hasse, A. Weil, A. Grothendieck, and P. Deligne, over a period of fifty years (1923 - 1973). Firstly, Weil used the Weil cohomology to prove for the curves, and Deligne used the étale cohomology defined the Grothendick to prove for the general case.

The aim of this master thesis is to study the *rationality* of the *Weil conjectures* of Zeta and L-functions of Algebraic Curves over finite fields by using the étale cohomology. The development of étale cohomology was motivated by work of Weil. Grothendieck had built the general theory of schemes that, following a remark of Serre, he was able to generalize in a very original way both of concept "topology" and the concept of "sheaf". He also attached to every variety (or scheme) X a cohomology algebra $H^{\bullet}(X_{\text{ét}}, \mathbb{Q}_l)$, where l is a prime different from the characteristic of X. More precisely, he defined

$$H^{\bullet}(X_{\text{ét}}, \mathbb{Q}_l) = \varprojlim H^{\bullet}(X_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

This cohomology satisfies:

- (Dimension) If X has dimension d, then $H^i(X_{\text{ét}}, \mathbb{Q}_l) = 0$ for every $i > d$.
- (Finiteness) $H^{\bullet}(X_{\text{ét}}, \mathbb{Q}_l)$ is a finite dimensional vector space over $\mathbb{Q}_l$.
- (Duality) There exists a perfect pairing $H^i \times H^{2d-i} \to \mathbb{Q}_l$.

By using the étale cohomology, one can prove the Lefschetz trace formula which states that if X is a complete nonsingular variety over an algebraically closed field k, and $f : X \to X$ is a morphism of schemes which induces the linear morphism $f^{\bullet} : H^{\bullet}(X_{\text{ét}}, \mathbb{Q}_l) \to H^{\bullet}(X_{\text{ét}}, \mathbb{Q}_l)$ of $\mathbb{Q}_l$-vector spaces, then

$$(\Gamma_f \centerdot \Delta) = \sum_r (-1)^r Tr(f | H^r(X, \mathbb{Q}_l))$$

where Γ_f is the graph of f, and Δ is the diagonal in $X \times X$. Thus $(\Gamma_f \centerdot \Delta)$ is the number of fixed points of f counted with multiplicities. And finally, since the definition of zeta and L-functions, one can prove the Weil conjectures by rewriting the formulas of zeta functions and L-functions in the terms of étale cohomology.

Acknowledgements

I would like to thank my supervisor, Prof. Boas Erez, for having introduced me to this fascinating and beautiful subject. His enthusiasm, his wonderful explanations and guidance have given me a new view on what mathematics means. My deepest thanks to him. I gratefully thank Jilong Tong for his great help on this thesis. Also I would like to offer my gratitude to the whole ALGANT Program for providing me the great opportunity of studying in a wonderful program.

Contents

Chapter 1

Algebraic Curves over finite fields

In this chapter, we will recall some basic knowledge of finite fields, schemes theory and Algebraic curves.

1.1 Finite fields

For a prime number p, the residue class ring $\mathbb{Z}/p\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers forms a field. We also denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. It is a prime field in the sense that there are no proper subfields of $\mathbb{F}_p$. There are exactly p elements in this field. In general, a field is called a *finite field* if it contains only a finite number of elements.

Proposition 1.1. *Let k be a finite field with q elements. Then:*

a. There exists a prime p such that $\mathbb{F}_p \subset k$;

b. $q = p^n$ for some integer $n \geq 1$;

c. $\alpha^q = \alpha$ for all $\alpha \in k$.

Theorem 1.2. *For every prime number p and every integer $n \geq 1$, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$.*

The above theorem shows that for given $q = p^n$, the finite field with q elements is unique in a fixed algebraic closure $\overline{\mathbb{F}_p}$. We denote this field by $\mathbb{F}_q$ and call it the finite field of order q. It follows from the the above theorem that $[\mathbb{F}_q : \mathbb{F}_p]$ is a Galois extension of degree n. The following theorem yields the structure of the Galois group $Gal(\mathbb{F}_q/\mathbb{F}_p)$.

Theorem 1.3. *Let q be a prime power. Then:*

a. $\mathbb{F}_q$ *is a subfield of* $\mathbb{F}_{q^n}$ *for every integer* $n \geq 1$.

b. $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *is a cyclic group of order* n *with generator* $\sigma : a \mapsto a^q$.

c. $\mathbb{F}_{q^m}$ *is a subfield of* $\mathbb{F}_{q^n}$ *if and only if* m *divides* n.

d. The algebraic closure of $\mathbb{F}_q$ *is the union* $\bigcup\limits_{n=1}^{\infty} \mathbb{F}_{q^n}$. *Moreover,* $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim Gal(\mathbb{F}_{q^i}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$.

1.2 Scheme theory

1.2.1 First properties of schemes

Definition 1.4. A scheme X is *locally noetherian* if it can be covered by open affine subsets $SpecA_i$, where each A_i is a noetherian ring. X is *noetherian* if it is locally noetherian and quasi-compact. Equivalently, X is noetherian if it can be covered by a finite number of open affine subsets $SpecA_i$, with each A_i a noetherian ring.

Proposition 1.5. *1. An affine scheme* $Spec(A)$ *is noetherian if and only if* A *is noetherian. In particular, if* X *is a noetherian scheme then the local ring* $\mathcal{O}_{X,x}$ *is noetherian for any point* $x \in X$.

2. Let X *be a locally noetherian scheme (resp. noetherian scheme), then so is any open subscheme of* X.

3. For X *a noetherian scheme, its underlying topological space is a noetherian topological space. In particular, any closed subset of* X *can be decomposed as a finite union of its irreducible components.*

Proof. 1. The latter condition is clearly sufficient. We show that it's also necessary. Let $X = Spec(A)$ be an affine scheme which is noetherian. Since a localization of a noetherian ring is again noetherian, X contains a topological basis $\mathcal{B}$ which consists of open principal $D(f) = Spec(A_f)$ with A_f noetherian. In particular, X can be covered by finitely many principal open in $\mathcal{B}$: $X = \bigcup\limits_i X_i$ with $X_i = Spec(A_{f_i})$. Now, as A_{f_i} is noetherian, $\mathfrak{a}_{f_i} \subset A_{f_i}$ is an ideal of finite type. Let $\{a_{ij}\}_j$ be a family of generators of I_{f_i}, we may assume that $a_{ij} \in I$. We claim that $\{a_{ij} : i, j\}$ gives then a family of generators of $\mathfrak{a}$. Indeed, for each $a \in I$, and for each i, there exists $\lambda_{ij} \in A$ and $e_{ij} \in \mathbb{Z}_{\geq 1}$ such that

$$a = \sum_j \frac{\lambda_{ij}.a_{ij}}{f_i^{e_{ij}}} \in A_{f_i}.$$

Up to replacement e_{ij} by some bigger integer, we may assume that $e_{ij} = e$ is independent of i, j. Moreover there exists $m_i \in \mathbb{Z}_{\geq 0}$ such that

$$f_i^{m_i+e} a = \sum_j f_i^{m_i} \lambda_{ij} a_{ij}.$$

On the other hand, since $X = \bigcup_i D(f_i) = \bigcup_i D(f_i^{m_i+e})$, one can find $\mu_i \in A$ such that $1 = \sum_i \mu_i f_i^{m_i+e}$. So finally, we get

$$a = \sum_i a\mu_i f_i^{m_i+e} = \sum_i \sum_j \mu_i f_i^{m_i} \lambda_{ij} a_{ij}.$$

This gives (1)

2. As the localization of a noetherian ring is again noetherian, X contains then an open basis consisting of noetherian affine schemes. This shows that any open subscheme of a locally noetherian scheme is locally noetherian. If moreover, X is noetherian, any open subset of X is quasi-compact, in particular, any open subscheme is noetherian.

3. The proof of (3) is similar.

□

Definition 1.6. (a) Let X be a scheme. X is called *connected* (resp. *irreducible*, resp. *quasi-compact*) if its underlying topological space is connected (resp. irreducible, resp. quasi-compact).

(b) A scheme X is *reduced* if for every open subset U of X, the ring $\mathcal{O}_X(U)$ has no nilpotent elements. Equivalently, X is reduced if and only if the local rings $\mathcal{O}_P(\mathcal{O}_{X,P})$ have no nilpotent elements for all $P \in X$.

(c) A scheme X is *integral* if X is irreducible and the local rings $\mathcal{O}_P$ is integral for all $P \in X$. Equivalently, X is integral if and only if the ring $\mathcal{O}_X(U)$ is an integral domain, for every open subset U of X.

Proposition 1.7. *[Liu02] A scheme is integral if and only if it is both reduced and irreducible.*

Definition 1.8. Let X be a topological space. Let $x, y \in X$ be points of X. We say that y is a *specialization* of x, or that x *specializes* y if $y \in \overline{\{x\}}$. We say that $x \in X$ is a *generic point* if x is the unique point of X that specializes to x.

Proposition 1.9. *Let X be a scheme.*

1. *Any irreducible closed subset of X contains a unique generic point.*

2. *For any generic point $\xi \in X$, $\overline{\{\xi\}}$ is an irreducible component of X, In particular, if X is irreducible then there exists unique generic point ξ such that $\overline{\{\xi\}} = X$.*

Proof. When $X = Spec(A)$ is affine, a closed subset $V(I) \subset X$ is irreducible if and only if $\sqrt{I} = P$ with $P \subset A$ a prime ideal. In this case, the point P is a generic point of $V(I) \subset X$. Now, for X an arbitrary scheme, let $Z \subset X$ be an irreducible subset. Let $x \in X$ be a point contained in X, then x has a affine neighborhood $U \subset X$. Since Z is irreducible, $U \cap Z \subset Z$ is dense and irreducible. Moreover, $U \cap Z \subset U$ is closed and irreducible with U an affine scheme, so it contains a generic point, which gives also a generic point of Z. The uniqueness follows from the fact that the underlying topological space of a scheme if a T_0-space. This gives (1).
For (2), let $Z \subset X$ be an irreducible component of X, and $\xi \in Z$ be its generic point. Then we claim that ξ is a generic point of X, that is, no point being different from ξ can specialize to ξ: indeed, if η specializes to ξ, then $\xi \in \overline{\{\eta\}}$, hence $Z = \overline{\{\xi\}} \subset \overline{\{\eta\}}$. As Z is a maximal irreducible closed subset of X, we must have $\overline{\{\xi\}} = \overline{\{\eta\}}$, hence $\xi = \eta$. This shows that $\xi \in X$ is a generic point. The proposition is proved completely. □

Proposition 1.10. *Let X be an integral scheme with generic point ξ. The followings are hold*

1. *Let V be an affine open subset of X, then $\mathcal{O}_X(V) \to \mathcal{O}_{X,\xi}$ induces an isomorphism $Frac(\mathcal{O}_X(V)) \cong \mathcal{O}_{X,\xi}$.*

2. *For any open subset U of X, and any point $x \in U$. The canonical morphism $\mathcal{O}_X(U) \to \mathcal{O}_{X,\xi}$ and $\mathcal{O}_{X,x} \to \mathcal{O}_{X,\xi}$ are injective.*

3. *By identifying $\mathcal{O}_X(U)$ and $\mathcal{O}_{X,x}$ to subrings of $\mathcal{O}_{X,\xi}$, we have $\mathcal{O}_X(U) = \bigcap_{x \in U} \mathcal{O}_{X,x}$.*

Proof. The first assertion (1) is clear. Indeed, if $V = Spec(A)$, then $\mathcal{O}_{X,\xi}$ is exactly the fraction field $Frac(A)$, and the canonical map $\mathcal{O}_X(V) \to \mathcal{O}_{X,\xi}$ is then the natural map $A \hookrightarrow Frac(A)$. Hence, the conclusion follows.
For (2), let $f \in \mathcal{O}_X(U)$ be any element such that its image $f_x \in \mathcal{O}_{X,x}$ is zero. Then there exists an affine open neighborhood V of x such that $f|_V = 0$. In particular, the image $f_\xi \mathcal{O}_{X,\xi}$ is zero. Now by applying the first assertion, we see that for any affine open V' of X, we have $f|_{V'} = 0$. Hence, $f = 0$. This gives the injectivity of the first morphism. For the second injectivity, we take any affine open neighborhood $V = Spec(A)$ of x, and suppose that x corresponds to the prime ideal $\mathfrak{p} \subset A$, then the canonical map $\mathcal{O}_{X,x} \to \mathcal{O}_{X,\xi}$ is just the canonical inclusion $A_\mathfrak{p} \hookrightarrow Frac(A)$, where comes the desired injectivity.

For (3), we have clearly $\mathcal{O}_X(U) \subset \bigcap_{x \in U} \mathcal{O}_{X,x}$. Conversely, by the sheaf condition and the injectivity proved in (2), we may assume that $U = Spec(A)$ is affine. Then we are reduced to show that $A = \bigcap\limits_{\mathfrak{p} \in Spec(A)} A_{\mathfrak{p}}$, seen as subring of $Frac(A)$. Indeed, for a fraction $f \in Frac(A)$ which is contained in $\bigcap_{\mathfrak{p} \in Spec(A)} A_{\mathfrak{p}}$, then for each $\mathfrak{p} \in Spec(A)$, there exists $s_{\mathfrak{p}} \in A - \mathfrak{p}$, and $a_{\mathfrak{p}} \in A$ such that $f = a_{\mathfrak{p}}/s_{\mathfrak{p}}$. As A is integral, we deduce then $f.s_{\mathfrak{p}} \in A$. Now, if we take the family $\{s_{\mathfrak{p}} : \mathfrak{p} \in Spec(A)\}$, which generates the unit ideals. Hence, one can find $b_{\mathfrak{p}} \in A$, almost all zero, such that $1 = \sum\limits_{\mathfrak{p}} b_{\mathfrak{p}} s_{\mathfrak{p}}$. From where, we find $f = \sum\limits_{\mathfrak{p}} b_{\mathfrak{p}} s_{\mathfrak{p}} f = \sum\limits_{\mathfrak{p}} b_{\mathfrak{p}} a_{\mathfrak{p}} \in A$. This gives the result. □

Definition 1.11. Let X be an integral scheme, with generic point ξ. We denote the field $\mathcal{O}_{X,\xi}$ by $K(X)$. Sometimes, when X is an algebraic over a field k, we also denote $K(X)$ by $k(X)$. An element of $K(X)$ is called a *rational function* on X. We call $K(X)$ the *field of rational functions* or *function field* of X. We say that $f \in K(X)$ is *regular* at $x \in X$, if $f \in \mathcal{O}_{X,x}$. A rational f is regular at any point of $x \in U$ is contained in $\mathcal{O}_X(U)$.

Definition 1.12. Let X be a topological space, we define the *(Krull) dimension* of X, which we denote by $dim(X)$, to be the supremum of the lengths of the chains of irreducible closed subsets of X. Dimension of a scheme X is the dimension of the underlying topological space.

From the definition of dimension of a topological space. It is easy to deduce the following

Proposition 1.13. *[Liu02] Let X be a topological space.*

1. *For any subset Y of X endowed with the induced topology, then $dimY \leq dimX$.*
2. *Suppose X is irreducible of finite dimension, and let $Y \subset X$ be a closed subset. Then $Y = X$ if and only if $dimY = dimX$.*
3. *The dimension of X is the supremum of the dimensions of its irreducible components.*
4. *Let's denote $dim_x X = inf\{dimU : U$ an open neighborhood of $x\}$ then $dimX = sup\{dim_x X : x \in X\}$*

Theorem 1.14. *(Noether normalization lemma) Let A be a finitely generated algebra over a field k. Then there exists an integer $d \geq 0$, and a finite injective homomorphism $k[T_1, T_2, \cdots, T_d] \hookrightarrow A$.*

Corollary 1.15. *Let X be an integral scheme of finite type over a field k. Then for any non-empty open subset $U \subset X$, we have $dim(U) = dim(X) = tr.deg(K(X)/k)$.*

Proposition 1.16. *[Liu02] Let A be a finitely generated integral domain over a field k. Let $\mathfrak{p} \subset A$ be a prime ideal.*

1. *$ht(\mathfrak{p}) + dim(A/\mathfrak{p}) = dim(A)$.*
2. *If $\mathfrak{p}$ is maximal then $dim(A) = dim(A_{\mathfrak{p}})$.*

Corollary 1.17. *Let X be an irreducible finite type scheme over a field k. Let $x \in X$ be a closed point. Then $dim(X) = dim(\mathcal{O}_{X,x})$.*

1.2.2 Some global properties of schemes

Definition 1.18. Let S be a scheme, and let X, Y be two schemes over S. We define the *fibred product* of X, Y over S to be an S-scheme $X \times_S Y$, together with two morphisms of S-schemes $p : X \times_S Y \to X, q : X \times_S Y \to Y$ (called the *projections*), verifying the following universally property:
Let $f : Z \to X, g : Z \to Y$ be two morphisms of S-schemes then there exists a unique morphism of S-schemes $\gamma = (f, g) : Z \to X \times_S Y$ making the following diagram commutative:

$$\begin{tikzcd}
Z \arrow[dr, "\exists!\gamma"] \arrow[drr, bend left, "g"] \arrow[ddr, bend right, "f"'] & & \\
& X \times_S Y \arrow[r, "p"'] \arrow[d, "q"] & X \arrow[d, "\alpha"'] \\
& Y \arrow[r, "\beta"] & S
\end{tikzcd}$$

Proposition 1.19. *Let S be a scheme, and let X, Y be two S-schemes. Then the fibred product $(X \times_S Y, p, q)$ exists, and is unique up to isomorphism. If X, Y, S are affine, then $X \times_S Y = Spec\big(Spec(\mathcal{O}_X(X) \otimes_{\mathcal{O}_S(S)} \mathcal{O}_Y(Y))\big)$, and the projection morphisms are induced by the canonical homomorphisms $\mathcal{O}_X(X), \mathcal{O}_Y(Y) \to \mathcal{O}_X(X) \otimes_{\mathcal{O}_S(s)} \mathcal{O}_Y(Y)$*

Definition 1.20. Let S be a scheme, and X be an S-scheme. For any S-scheme S', the second projection $q : X \times_S S' \to S'$ endows $X \times_S S'$ with a structure of an S'-scheme. Such a process is called the *base change* of X by $S' \to S$. We sometimes denote the S'-scheme $X \times_S S'$ by $X_{S'}$. For a morphism of S-schemes $f : X \to Y$, its base change by $S' \to S$ is the morphism $f \times_S 1_{S'} : X \times_S S' \to Y \times_S S'$, sometimes it is denoted by $f_{S'}$.

Definition 1.21. Let $f : X \to Y$ be a morphism of schemes. For any point $y \in Y$, we set $X_y = X \times_Y Spec(k(y))$, where $Spec(k(y)) \to Y$ is the canonical map associated to the point $y \in Y$. We call X_y be the *fiber of f over y*. Remark that the second projection $X_y = X \times_Y Spec(k(y)) \to Spec(k(y))$ makes X_y into a scheme over $k(y)$. If Y is irreducible with the generic point $\xi \in Y$, we call the fiber product X_ξ over ξ the *generic fibre* of f.

Definition 1.22. Let P be a property of a morphism of schemes $f : X \to Y$

1. The property P is said to be *local on the base* Y if the following assertions are equivalent:

   (a) f verifies P;

   (b) for any $y \in Y$, there exists an affine neighborhood V of y such that $f|_{f^{-1}(V)}$ verifies P.

2. The property P is said to be *stable under the base change* if for any morphism $f : X \to Y$ verifying P, and for any morphism $Y' \to Y$, the base change $f_{Y'} : X_{Y'} \to Y'$ verifies again the property P.

Definition 1.23. An *open subscheme* of a scheme X is a scheme U, whose topological space is an open subset of X, and whose structure sheaf $\mathcal{O}_U$ is isomorphic to the restriction $\mathcal{O}_X|_U$ of the structure of X. An *open immersion* is a morphism $f : X \to Y$ which induces an isomorphism of X with an open subscheme of Y.

Definition 1.24. A morphism of schemes $f : X \to Y$ is called a *closed immersion* if for any affine open U of Y, the inverse image $f^{-1}(U) \subset X$ is again affine, and the induced map $\mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}(U))$ is surjective.

Definition 1.25. A morphism of schemes $f : X \to Y$ is called *separated* if the diagonal morphism $\delta : X \to X \times_Y X$ is a closed immersion. We say that X is a *separated Y-scheme* or X is *separated over Y*. A scheme X is said to be *separated* if X is separated over $Spec(\mathbb{Z})$.

Proposition 1.26. *[Liu02] Let $f : Y \to X$ be a morphism of schemes with $X = Spec(A)$ affine. The following conditions are equivalent:*

1. *f is separated.*

2. *For any two affine opens $U, V \subset Y$, their intersection $U \cap V \subset Y$ is again affine, moreover, the canonical map $\mathcal{O}_Y(U) \otimes_A \mathcal{O}_Y(V) \to \mathcal{O}_Y(U \cap V)$ is surjective.*

3. *There exists an open affine covering $Y = \bigcup_{i \in I} U_i$ such that $U_i \cap U_j$ is affine, and that the canonical map $\mathcal{O}_Y(U_i) \otimes \mathcal{O}_Y(U_j) \to \mathcal{O}_Y(U_i \cap U_j)$ is surjective for any $i, j \in I$.*

Proposition 1.27. *[Liu02]*

1. *Open and closed immersions are separated.*

2. *The composition of two separated morphisms is again separated. In particular, immersions are separated.*

3. *Let $f : X \to Y$, and $g : Y \to Z$ be two morphisms such that $g \circ f$ and f are both separated, then f is separated.*

4. *Separated morphisms are stable under base change. i.e. any base change of a separated morphism is again a separated morphism.*

Definition 1.28. Let $f : X \to Y$ be a morphism of locally noetherian schemes.

1. f is said to be *universally closed* if for any morphism $Y' \to Y$, the base change

$$f_{Y'} : X' = X \times_Y Y' \to Y'$$

is a closed map between the underlying topological spaces.

2. f is said to be *finite type* if f is *quasi-compact* (that is, for any quasi-compact open subset $V \subset Y$, the inverse image $f^{-1}(U)$ is quasi-compact) and *locally of finite-type* (that is, for any affine opens $U = Spec(A) \subset X$ and $V = Spec(B) \subset Y$ such that $f(U) \subset V$, then the induced map $B = \mathcal{O}_Y(V) \to \mathcal{O}_X(U) = A$ makes A into a B-algebra of finite type).

3. f is said to be *proper* if f is separated, of finite type, and universally closed.

Proposition 1.29. *[Liu02] We have the following properties:*

1. *Closed immersions are proper.*

2. *The composition of two proper morphisms is proper.*

3. *The base change of a proper morphism is still proper.*

4. *If the composition of $X \to Y$ and $Y \to Z$ is proper, and if the second morphism $Y \to Z$ is separated. Then the first morphism $X \to Y$ is also proper.*

5. *Let $f : X \to Y$ be a surjective morphism of S-schemes. Let us suppose that Y is separated and of finite type over S, and that X is proper over S, then Y is proper over S.*

1.2.3 Some local properties of schemes

Definition 1.30. Let $(A, \mathfrak{m})$ be a noetherian local ring with residue field k. Recall that $dim(A) \leq dim_k \mathfrak{m}/\mathfrak{m}^2$. We call a noetherian local ring $(A, \mathfrak{m})$ *regular* if $dim(A) = dim_k \mathfrak{m}/\mathfrak{m}^2$.

Theorem 1.31. *Let $(A, \mathfrak{m})$ be a noetherian local ring of dimension d. The following three statements are equivalent:*

1. *A is regular.*
2. *$\mathfrak{m} \subset A$ can be generated by d elements.*
3. *$gr_{\mathfrak{m}}(A) := \bigoplus_{n=0}^{\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is isomorphic, as k-algebra, to the ring of polynomials in d variables.*

Proposition 1.32. *Let $(A, \mathfrak{m})$ be a regular noetherian local ring. Then A is an integral domain.*

Definition 1.33. Let X be a locally noetherian scheme, and let $x \in X$ be a point. We say that X is *regular* at $x \in X$, or x is regular point of X if $\mathcal{O}_{X,x}$ is regular. We say that X is regular if X is regular at all its points. A point x in X which is not regular is called a *singular point* of X. A scheme that is not regular is said to be singular.

1.3 Algebraic Curves over finite fields

Definition 1.34. Let k be a field. An affine *variety over k* is the affine scheme associated to a finitely generated algebra over k. An *algebraic variety over k* is a k-scheme X such that there exists a covering by a finite number of affine open subschemes X_i which are affine varieties over k. A *projective variety over k* is a projective scheme over k. Projective varieties are algebraic varieties. By definition, a *morphism of algebraic varieties over k* is a morphism of k-schemes.

Definition 1.35. Let k be a field. An algebraic variety over k whose irreducible components are of dimension 1 is called an *algebraic curve over k (or curve over k).*

Definition 1.36. A curve Y is said to be *smooth* if and only if $\overline{Y} = Y_{\overline{k}}$ is regular.

Definition 1.37. A curve Y over a finite field $k = \mathbb{F}_q$ is called complete smooth curve if Y is a k -scheme of finite type, $dimY = 1$, and $\overline{Y}$ is regular, proper, integral over $\overline{k}$.

From now on, we assume all curves to be complete smooth curve (hence, projective).

Proposition 1.38. *[Liu02] Let Y be an algebraic variety over finite field $\mathbb{F}_q$ then:*

1. *If Y is smooth then Y is regular.*
2. *$dimY = dim\overline{Y}$, for every U open in Y then $dimU = dimY$. If V is a closed subset of Y then $V = Y$ if and only if $dimV = dimY$.*
3. *Closed subsets of an algebraic curve are $\emptyset, Y$ or finite union of closed points.*

Next, we will state the Jacobian criterion for a projective curve. Let $C = V(I) \subset \mathbb{P}^n$ be a curve with generators $f_1, f_2, \cdots, f_m \in I$. Then C is smooth at $P \in C$ if and only if

$$rank \begin{pmatrix} \frac{\delta f_1}{\delta x_0}(P) & \cdots & \frac{\delta f_1}{\delta x_n}(P) \\ \vdots & \ddots & \vdots \\ \frac{\delta f_m}{\delta x_0}(P) & \cdots & \frac{\delta f_m}{\delta x_n}(P) \end{pmatrix} = n-1$$

Example 1.1. *The curves in $\mathbb{P}^2$*

$$\begin{aligned} C_1: &\quad X_0^r + X_1^r + X_2^r = 0 \\ C_2: &\quad X_0^3X_1 + X_1^3X_2 + X_2^3X_0 = 0 \\ C_3: &\quad X_1^qX_2 + X_1X_2^q = X_0^{q+1} \end{aligned}$$

are all smooth.

Proposition 1.39. *Let X be a scheme of finite-type over $\mathbb{F}_q$ and let $x \in X$. The following properties are equivalent:*

a. *$\{x\}$ is closed in X.*

b. *The residue field $k(x)$is finite.*

Proof. Use the Noether normalization lemma or Zariski's theorem. □

Chapter 2

Étale morphisms and Cohomology

This chapter covers some basic notions about étale cohomology so that we can use in the next chapter. We will prove that the category of sheaves of abelian groups on $X_{\text{ét}}$ is abelian and has enough injectives. Therefore, we can define the étale cohomology as the right derived functor of global section. After considering a family of cohomology of constant sheaf, we can give the definition of *l-adic cohomology*. The aim of this notion is to state (without proof) of the Lefschetz fixed point formula which is the main tool to study chapter 3.

2.1 Étale morphisms

2.1.1 Étale morphisms

Flat morphisms: A morphism $\varphi : Y \to X$ of schemes (or varieties) is said to be *flat* if the local homomorphisms $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ are flat for all $y \in Y$.
We recall that a homomorphism of rings $A \to B$ is flat if one of the following equivalent conditions holds:

- The functor $M \mapsto B \otimes_A M$ from the A-modules category to the B-modules category is exact.
- $J \otimes_A B \to B$ is injective for every $J \subset A$ ideal.
- The local homomorphism $A_{f^{-1}(\mathfrak{m})} \to B_{\mathfrak{m}}$ is flat for every maximal ideal $\mathfrak{m}$ in B.

Remark 2.1. If A is an integral domain, then any flat morphism $A \to B$ is injective. Conversely, if A is a Dedekind domain then any injective morphism is flat.

Theorem 2.2. *[Mil80] Any flat morphism that is locally of finite-type is open. Moreover, let $f : Y \to X$ be locally of finite type then the set of points $y \in Y$ such that $\mathcal{O}_y$ is flat over $\mathcal{O}_{f(y)}$ is open in Y and it is non-empty if X is integral.*

Unramified morphisms: A morphism $\varphi : Y \to X$ of schemes (or varieties) is said to be *unramified* if it is of finite type and if the local homomorphisms $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ are unramified for all $y \in Y$.
We recall that a local homomorphism $A \to B$ of local rings is unramified if one of the following equivalent conditions holds:

- $B/f(\mathfrak{m}_A)B$ is a finite separable field extension of $A/\mathfrak{m}_A$.
- $f(\mathfrak{m}_A)B = \mathfrak{m}_B$ and the field $B/\mathfrak{m}_B$ is finite and separable over $A/\mathfrak{m}_A$.

Remark 2.3. It suffices to check the condition of unramified morphism of schemes for the closed points y in Y only.

Proposition 2.4. *[Mil80] Let $f : Y \to X$ be a locally of finite-type. Then the following are equivalent:*

i. *f is unramified*

ii. *$\forall x \in X, Y_x \to Spec(k(x))$ is unramified.*

iii. *All geometric fibres of f are unramified, that is, for every $Spec(k) \to X$ with k separably closed, then $Y \times_X Spec(k) \to Spec(k)$ is unramified.*

iv. *For all $x \in X$, Y_x has an open covering by spectra of finite separable $k(x)$-algebras.*

v. *For all $x \in X$, Y_x is a disjoint sum of $Spec(k_i)$ where $[k_i : k(x)]$ is finite separable extension.*

Étale morphism: A morphism $\varphi : Y \to X$ of schemes is *étale* if it is flat and unramified (hence, it is of finite type).
In particular, a homomorphism of rings $f : A \to B$ is étale if the corresponding morphism $Spec(B) \to Spec(A)$ is étale. Equivalently, it is étale if

(a) B is a finitely generated A-algebra,

(b) B is a flat A-algebra,

(c) $B_{\mathfrak{n}}/f(\mathfrak{p}B_{\mathfrak{n}})$ is a finite separable field extension of $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ for all maximal ideals $\mathfrak{n} \subset B$ and $\mathfrak{p} = f^{-1}(\mathfrak{n})$.

2.1.2 Properties of étale morphisms

In this section, we will study some basic properties of étale morphisms.

Proposition 2.5. *1. Any open immersion is étale.*

2. Composition of two étale morphisms is an étale morphism.

3. Any base change of an étale morphism is an étale morphism.

4. If $\varphi \circ \psi$ and φ are étale, then so also is ψ.

Statement (1) says that if U is an open subscheme of X, then the inclusion $U \hookrightarrow X$ is étale. The statements (2) and (3) also hold for flat morphisms and unramified morphisms, hence, they do for étale morphisms.

Proposition 2.6. *Let $p : X \to S$ and $q : Y \to S$ be morphisms of varieties over an algebraically closed field. Assume that p is étale and that Y is connected. Let φ, φ' be morphisms $Y \to X$ such that $p \circ \varphi = q$ and $p \circ \varphi' = q$. If φ and φ' agree at a single point of Y, then they are equal on the whole of Y.*

One of the important properties of étale morphisms is that if $Y \to X$ is étale, then Y inherits many of the good properties of X. They comes from a "nice" local property of étale morphism which is called standard étale morphisms as follows

Theorem 2.7. *[Mil80] A morphism $f : Y \to X$ is étale if and only if for every $y \in Y$, there exist open affine neighborhoods $V = Spec(C)$ of y and $U = Spec(A)$ of $x = f(y)$ such that*

$$C = A[T_1, T_2, \cdots, T_n]/(P_1, \cdots, P_n)$$

where $det(\delta P_i/\delta T_j)$ is a unit in C.

An immediate property implied from the previous theorem is that $Y \to X$ étale and X locally noetherian implies Y locally noetherian. Moreover, we can prove that

Proposition 2.8. *If $\phi : Y \to X$ is an étale morphism, then:*

1. For all $y \in Y$, $\mathcal{O}_{Y,y}$ and $\mathcal{O}_{X,x}$ have the same Krull dimension.

2. The morphism ϕ is quasi-finite.

3. The morphism ϕ is open on the underlying topological spaces (however, it is not necessarily an open immersion).

4. *If X is reduced (respectively, normal, or regular), then so also is Y.*

Remark 2.9. In general, if X is integral, it is not necessary that Y is also integral. More precisely, if X is irreducible, Y is not necessarily irreducible.

2.2 Sheaf theory

2.2.1 Presheaves and sheaves

We shall be concerned with classes E of morphisms of schemes satisfying the following conditions:

(e_1) All isomorphism are in E.

(e_2) The composite of two morphisms in E is in E.

(e_3) Any base change of a morphism in E is in E.

A morphism in such a class E will be referred to as an $E-morphism$. The full subcategory of the category of $X-schemes$ Sch/X whose structure morphism is an $E-morphism$ will be written E/X.

Example 2.1. *The following examples of such classes will be particularly important:*

1. *the class $E = (Zar)$ of all open immersions;*

2. *the class $E =$ (ét) of all étale morphisms of finite-type;*

3. *the class $E = (fl)$ of all flat morphisms that are locally of finite-type;*

Definition 2.10. Fix a base scheme X and a class E as above. Let C/X be a full subcategory of Sch/X such that C/X is closed under fiber products and for any morphism $Y \to X$ in C/X and any $E-morphism$ $U \to Y$, then the composite $U \to X$ is in C/X.

1. An $E-covering$ of an object Y of C/X is a family $(g_i : U_i \to Y)_{i\in I}$ of $E-morphisms$ such that $Y = \bigcup_{i\in I} g_i(U_i)$. The class of all such objects is called an $E-topology$ on C/X.

2. The category C/X together with the $E-topology$ is called an $E-site$ over X and we denote it by $(C/X)_E$ or simply as X_E

3. The *étale site* (respectively, *Zariski site*, or *flat site*) on X is the full subcategory $(\text{ét})/X$ (respectively, $(\text{Zar})/X$, or $(\text{fl})/X$) of Sch/X together with the étale (respectively, Zariski, or flat) topology, that is for every $Y \to X$ étale (respectively, open immersion, or flat morphism that are locally of finite-type) then the étale (respectively, Zariski, or flat) covering of Y is a family $(U_i \to Y)_{i \in Y}$ of the class *(ét)* (respectively, *(Zar)* or *(fl)*).

Remark 2.11. The étale site, (Zar)-site and (fl)-site sastify the following conditions:

1. if $\phi : U \to U$ is an isomorphism in the corresponding site then it is a covering;
2. if $(U_i \to U)_i$ is a covering, and $(V_{ij} \to U)_j$ is a covering for every i, then $(V_{ij} \to U)_{i,j}$ is also a covering;
3. if $(U_i \to U)_i$ is a covering then the family of base changes $(U_i \otimes_U V \to V)$ is also a covering.

Definition 2.12. A *presheaf* P of abelian groups on a site $(C/X)_E$ is a contravariant functor $C/X \to Ab$.
Thus P associates with each U in C/X an abelian group $P(U)$, which we shall sometimes write as $\Gamma(U, P)$ and whose elements we shall sometimes refer to as *sections* of P over U. A morphism of presheaves $\phi : P \to P'$ is simply a morphism of functors $P \to P'$.

Since the category of abelian groups is abelian, so is the category of presheaves of abelian groups on X_E. We denote this category by $PrS(X_E)$ or $P(X_E)$.

Example 2.2. *Let X_E be an E-site.*

1. *Constant presheaf: for any abelian group M, the constant presheaf P_M on X_E is defined to have $P_M(U) = M$ for every $U \neq \emptyset$, and $P_M(f) = 1_M$ for all f.*
2. *The presheaf $\mathbb{G}_a$ satisfies $\mathbb{G}_a(U) = \Gamma(U, \mathcal{O}_U)$ regarded as an additive group for all U, and for any morphism $U \to U'$, $\mathbb{G}_a(f)$ is the map $\Gamma(U', \mathcal{O}_{U'}) \to \Gamma(U, \mathcal{O}_U)$ induced by f.*
3. *The presheaf $\mathbb{G}_m$ has $\mathbb{G}_m(U) = \Gamma(U, \mathcal{O}_U)^*$ for all U and for any morphism $U \to U'$, $\mathbb{G}_m(f)$ is the map $\Gamma(U', \mathcal{O}_{U'})^* \to \Gamma(U, \mathcal{O}_U)^*$ induced by f.*

Definition 2.13. A presheaf P on X_E is a *sheaf* if it satisfies:

(S_1) For every $s \in P(U)$, if there is a covering $(U_i \to U)_{i \in I}$ of U such that $\forall i$: $res_{U_i,U}(s) = 0$ then $s = 0$.

(S_2) For every covering $(U_i \to U)_{i\in I}$ and every family $(s_i)_{i\in I} \in (P(U_i))_{i\in I}$ with

$$res_{U_i\otimes_U U_j,U_i}(s_i) = res_{U_i\otimes_U U_j,U_j}(s_j) \text{ for all } i,j$$

then there exists an $s \in P(U)$ such that $res_{U_i,U}(s) = s_i$ for all i.

In other words, a presheaf P is a sheaf if a section is determined (uniquely) by its restriction to a covering, and a compatible family of sections on a covering always arises from a global section. This means that the sequence

$$(S) : P(U) \to \prod_i P(U_i) \rightrightarrows \prod_{i,j} P(U_i \otimes_U U_j)$$

is exact for all coverings $(U_i \to U)$.

Remark 2.14. If P is a sheaf then $P(\emptyset) = O$.

In general, a sheaf of X_{Zar} is not a sheaf of $X_{\text{ét}}$. In the next theorem, we will give a criterion for a sheaf of $X_{\text{ét}}$

Theorem 2.15. *Let P be a presheaf for the étale (or flat site) on X. Then P is a sheaf if and only if it satisfies the following two conditions:*

(a) for any U in the category then the restriction of P to the usual Zariski topology on U is a sheaf;

(b) for any covering $(U' \to U)$ with U and U' both affine, then

$$(S) : P(U) \to P(U') \rightrightarrows P(U' \otimes_U U')$$

is exact.

Corollary 2.16. *On the flat and étale topologies, both presheaves $\mathbb{G}_a$ and $\mathbb{G}_m$ are sheaves.*

Remark 2.17. The constant presheaf defined as above is not a sheaf in general. We define the *constant sheaf* as follows: let X be a variety or a quasi-compact scheme, and for any abelian group M, define $\mathcal{F}_M(U) = M^{\pi_0(U)}$ - the product of copies of M indexed by the set $\pi_0(U)$ of connected components of U. with the restriction map, it is a sheaf, called the *constant sheaf* (associated to the constant presheaf) on $X_{\text{ét}}$ defined by M.

2.2.2 The category of (étale) sheaves of abelian groups

In this section, we study the category of sheaves of abelian groups on $X_{\text{ét}}$. In particular, we will show that this category is an abelian category with enough injective. We start with the notion of **stalks**. Let x be a point in a scheme X and k be a separably closed field of residue field $k(x)$. The embedding $k(x) \hookrightarrow k$ induces a morphism of schemes $\overline{x} : Spec(k) \to X$. An *étale neighborhood of* $\overline{x}$ is a commutative diagram:

$$\begin{tikzcd} Spec(k) \arrow[rr] \arrow[dr] & & U \arrow[dl, "\text{étale}"] \\ & X & \end{tikzcd}$$

Then étale neighborhoods of a *geometric point* $\overline{x}$ form a filtered category. Recall that a category J is filtered if the following holds:

- it is not empty,
- for every two objects j and j' in J then there exist an object k and two arrows $j \to k, j' \to k$ in J,
- for every two arrows $u, v : i \to j$ in J then there exists k and an arrow $w : j \to k$ such that $wu = wv$.

A filtered colimit is a limit of a functor $F : J \to \mathcal{C}$.

Definition 2.18. *Definition of stalks:* Let $\mathcal{F}$ be a presheaf on $X_{\text{ét}}$. We define its stalk at the geometric point $\overline{x}$ to be the direct limit

$$\mathcal{F}_{\overline{x}} = \varinjlim \mathcal{F}(U).$$

where U runs through all étale neighborhoods of x.

Remark 2.19. With the above notions, we have:

1. The functor $P \mapsto \mathcal{F}_{\overline{x}}$ from the category of presheaves of abelian group on $X_{\text{ét}}$ to the category of abelian groups is an exact functor.
2. Let $U \to X$ be an étale morphism such that the image of U contains the point x. Then there are many different ways to make U become an étale neighborhood of x. So, in general, there is no (unique) canonical map $P(U) \to \mathcal{F}_{\overline{x}}$. Of course, once U has been given a structure of étale neighborhood of x, we will have the canonical map $P(U) \to p_{\overline{x}}$ which we often write as $s \mapsto s_{\overline{x}}$.
3. Since all separably closure of $k(x)$ are isomorphic, $\mathcal{F}_{\overline{x}}$ only depends on x. Hence, $\mathcal{F}_{\overline{x}}$ is also denoted by $\mathcal{F}_x$.

Proposition 2.20. *Let $\mathcal{F}$ be a sheaf on $X_{ét}$. If $s \in \mathcal{F}(U)$ is non-zero, then there is an $x \in X$ and an étale neighborhood U of x such that $s_{\overline{x}}$ is non-zero.*

Proof. key property: Let (A_i, ϕ_{ij}) be a direct system of abelian groups over a direct category I. Let $\phi_i : A = \varinjlim A_i \to A_i$ be the canonical morphism. If $a \in A_i$ such that $\phi_i(a) = 0$ then there exists $i \to k$ arrow in I such that $\phi_{ik}(x) = 0$.
Proof of the proposition By contradiction, assume that for all $x \in X$ and for all étale neighborhood U of x, we always have that $s_{\overline{x}} = 0$. For every $u \in U$ mapping to $x \in X$, then $k(x) \to k(u)$ is finite separable extension (since $U \to X$ is étale). So $k(u)$ must be contained in the separably closed field k of $k(x)$. So the étale neighborhood U of x induces from the embeddings: $k(x) \hookrightarrow k(u) \hookrightarrow k$. By the key property, we have that $\exists V_u \to U$ étale such that $s|_{V_u} = 0$ for every $u \in U$. The family $(V_u \to U)_{u \in U}$ is a étale covering. By the definition of sheaf, we have that $s = 0$. $\square$

Since the category of sheaves of abelian groups on $X_{\text{ét}}$ is an additive category, we require that a morphism of two sheaves is always an additive morphism of sheaves. A morphism of sheaves (or presheaves) $\alpha : \mathcal{F} \to \mathcal{F}'$ is said to be *locally surjective* if, for every U and $s \in \mathcal{F}'(U)$, there exists a covering $(U_i \to U)$ such that $s|_{U_i}$ is in the image of $\mathcal{F}(U_i) \to \mathcal{F}'(U_i)$ for each i.

Lemma 2.21. *Let $\alpha : \mathcal{F} \to \mathcal{F}'$ be a morphism of sheaves on $X_{ét}$. The following are equivalent:*

1. *the sequence of sheaves $\mathcal{F} \to \mathcal{F}' \to 0$ is exact,*
2. *the map α is locally surjective,*
3. *for each geometric point $\overline{x} \to X$, the map $\alpha_{\overline{x}} : \mathcal{F}_{\overline{x}} \to \mathcal{F}'_{\overline{x}}$ is surjective.*

Proof. We will prove that (2) $\Rightarrow$ (1) $\Rightarrow$ (3)

(2) $\Rightarrow$ (1) Let $\beta : \mathcal{F}' \to \mathcal{H}$ be a morphism of sheaves such that $\beta_o \alpha = 0$. We need to prove that $\beta = 0$.
Let $U \to X$ be étale morphism and $s \in \mathcal{F}'(U)$. Since α is locally surjective, there exists a covering $(U_i \to U)_i$ such that $s|_{U_i}$ is in the image of $\mathcal{F}(U_i) \to \mathcal{F}'(U_i)$. This implies $\beta(U_i)(s|_{U_i}) = 0$.
Moreover, the diagram:

$$\begin{tikzcd}
\mathcal{F}(U_i) \arrow[r] \arrow[d] & \mathcal{F}'(U_i) \arrow[r] \arrow[d] & \mathcal{H}(U_i) \arrow[d] \\
\mathcal{F}(U) \arrow[r] & \mathcal{F}'(U) \arrow[r] & \mathcal{H}(U)
\end{tikzcd}$$

is commutative. So $\beta(U)(s)|_{U_i} = 0$ for very i, hence $\beta(U)(s) = 0$.

(1) $\Rightarrow$ (3) By contradiction, assume that $\alpha_{\overline{x}}$ is not surjective for some $x \in X$. Let $\Lambda = coker(\mathcal{F}_{\overline{x}} \to \mathcal{F}'_{\overline{x}})$. For $U \to X$ étale, we define a presheaf $\Lambda^{\overline{x}}(U) = \bigoplus_{Hom_X(\overline{x},U)} \Lambda$. Then $\Lambda^{\overline{x}}$ is a sheaf and

$$Hom(\mathcal{G}, \Lambda^{\overline{x}}) \cong Hom(\mathcal{G}_{\overline{x}}, \Lambda) \textit{ for every sheaf } \mathcal{G}.$$

In particular, $Hom(\mathcal{F}', \Lambda^{\overline{x}}) \cong Hom(\mathcal{F}'_{\overline{x}}, \Lambda)$, so the coker morphism $\mathcal{F}'_{\overline{x}} \to \Lambda$ corresponds to a non-zero morphism $\beta : \mathcal{F}' \to \Lambda^{\overline{x}}$. In the equivalence $Hom(\mathcal{F}, \Lambda^{\overline{x}}) \cong Hom(\mathcal{F}^{\overline{x}}, \Lambda)$, $\beta \circ \alpha$ correspond to the morphism 0, so $\beta_o \alpha = 0$, but $\beta \neq 0$. Hence, α is not surjective. (!!!)

(3) $\Rightarrow$ (2) Let $U \to X$ be étale, and let $\overline{u} \to U$ be a geometric point of U, then $\overline{u} \to U \to X$ is a geometric point of X. Let's denote it by $\overline{x}$. A étale neighborhood of $\overline{u}$ gives a étale neighborhood of $\overline{x}$.

$$\begin{tikzcd}
V \arrow[r] & U \arrow[r] & X \\
\overline{u} \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Moreover, the étale neighborhood of $\overline{x}$ arising in this fashion are cofinal. Indeed, let W be a neighborhood of $\overline{x}$, then $W \otimes_X U$ is an étale neighborhood of $\overline{u}$:

$$\begin{tikzcd}
W \times_X U \arrow[r] & U \arrow[r] & X \\
\overline{u} \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Therefore, $\mathcal{F}_{\overline{u}} \cong \mathcal{F}_{\overline{x}}$ for every sheaf $\mathcal{F}$ on $X_{\text{ét}}$. Thus, the hypothesis implies that $\mathcal{F}_{\overline{u}} \to \mathcal{F}'_{\overline{u}}$ is surjective for every geometric point $\overline{u} \to U$ of U.

Let $s \in \mathcal{F}'(U)$, for each $u \in U$, we have $\overline{u} \to U$ is a geometric point of U with image u. Since $\mathcal{F}_{\overline{u}} \to \mathcal{F}'_{\overline{u}}$ is surjective, then there exists $V \to U$ étale whose image contains u and which is such that $s|_V$ is in the image of $\mathcal{F}(V) \to \mathcal{F}'(V)$ (We know that $\mathcal{F}_{\overline{u}} = \bigsqcup \mathcal{F}(V) / \backsim$ where $\backsim$ is a certain relation, so if $\mathcal{F}_{\overline{u}} \to \mathcal{F}'_{\overline{u}}$ then there exist $t_{\overline{u}} \mapsto s_{\overline{x}}, s \in \mathcal{F}(W), t \in \mathcal{F}(E)$, let $V = W \times_U E$). Apply this for all $u \in U$, we have that affine is locally surjective.

$\square$

Proposition 2.22. *Let*

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}''$$

be a sequence of sheaves on $X_{ét}$. The following are equivalent:

1. *the sequence is exact in the category of sheaves;*

2. *the sequence:*
$$0 \to \mathcal{F}'(U) \to \mathcal{F}(U) \to \mathcal{F}''(U)$$
is exact for all étale $U \to X$;

3. *the sequence*
$$0 \to \mathcal{F}'_{\overline{x}} \to \mathcal{F}_{\overline{x}} \to \mathcal{F}''_{\overline{x}}$$
is exact for every geometric point $\overline{x} \to X$ of X.

Proof. We know that direct limit is an exact functor in the category of abelian groups. So we have that (2) $\Rightarrow$ (3). (3) $\Rightarrow$ (2) comes from the proposition 2.20. For the equivalence between (1), and (2), we will prove (later) that the functor $i : Sh(X_{\text{ét}}\ ) \to PreSh(X_{\text{ét}})$ has a left adjoint a, - the associated sheaf functor, hence i is left exact. □

From two previous propositions, we easily deduce the following

Proposition 2.23. *Let*
$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$
be a sequence of sheaves on $X_{ét}$. The following are equivalent:

1. *the sequence is exact in the category of sheaves;*

2. *the map $\mathcal{F} \to \mathcal{F}''$ is locally surjective and the sequence:*
$$0 \to \mathcal{F}'(U) \to \mathcal{F}(U) \to \mathcal{F}''(U)$$
is exact for all étale $U \to X$;

3. *the sequence*
$$0 \to \mathcal{F}'_{\overline{x}} \to \mathcal{F}_{\overline{x}} \to \mathcal{F}''_{\overline{x}} \to 0$$
is exact for every geometric point $\overline{x} \to X$ of X.

To finish the proof of *proposition 2.22*, we need to construct a functor associating a presheaf to a sheaf which is exact. If so, we can define the *kernel, cokernel, image, coimage...* of a morphism by taking the corresponding associated sheaf.

The sheaf associated with a presheaf

Definition 2.24. Let $\mathcal{P} \to a\mathcal{P}$ be a morphism from a presheaf $\mathcal{P}$ to a sheaf; then $a\mathcal{P}$ is said to be the sheaf associated with $\mathcal{P}$ (or to be the sheafification of $\mathcal{P}$) if all other morphism from $\mathcal{P}$ to a sheaf factor uniquely through $\mathcal{P} \to a\mathcal{P}$, i.e. $Hom(\mathcal{P}, \mathcal{F}) \cong Hom(a\mathcal{P}, \mathcal{F})$ for all sheaves $\mathcal{F}$, i.e. the functor $a : PreSh(X_{\text{ét}}\ ) \to Sh(X_{\text{ét}})$ is the left adjoint of the functor $i : Sh(X_{\text{ét}}\ ) \to PreSh(X_{\text{ét}})$.

Clearly, $a\mathcal{P}$ endowed with the map $\mathcal{P} \to a\mathcal{P}$, is unique up to isomorphism if it exists. In the following, we will construct explicitly $a\mathcal{P}$ for a given presheaf $\mathcal{P}$.

Lemma 2.25. ***(key lemma)*** *Let $\mathcal{P}$ be a presheaf of abelian groups on $X_{ét}$. If $i : Sh(X_{ét}\ ) \to PreSh(X_{ét})$ exists then the sections of $\mathcal{P}$ to have the same image in $\mathcal{F}(U)$ are those that are locally equal, i.e. for all $U \to X$ étale and for all $s_1, s_2 \in \mathcal{P}(U)$ such that $i(s_1) = i(s_2)$ then s_1 and s_2 are locally equal, i.e. such s_1, s_2 satisfies $s_1|_{U_i} = s_2|_{U_i}$ for some covering $(U_i \to U)_{i\in I}$.*

Proof. For each $x \in X$, let $i : \overline{x} \to X$ be a geometric point of X. For any étale map $\phi : U \to X$, we define

$$\Lambda^{\overline{x}}(U) = \bigoplus_{Hom_X(\overline{x}, U)} \Lambda$$

where Λ is the constant sheaf of the abelian group Λ. Then it is easy to prove that $\Lambda^{\overline{x}}$ is a sheaf and satisfies $Hom(\mathcal{F}, \Lambda^{\overline{x}}) \cong Hom(\mathcal{F}_{\overline{x}}, \Lambda)$. For $\mathcal{P}$ a presheaf on $X_{\text{ét}}$, define $\mathcal{P}^* = \prod_{x\in X} (\mathcal{P}_{\overline{x}})^{\overline{x}}$. Then $\mathcal{P}^*$ is a sheaf and the natural map $\mathcal{P} \to \mathcal{P}^*$ satisfies the condition of lemma. Since $\mathcal{P} \to \mathcal{P}^*$ can be factored through $\mathcal{P} \to a\mathcal{P}$, we are done. □

Lemma 2.26. *Let $i : \mathcal{P} \to \mathcal{F}$ be a morphism from presheaf $\mathcal{P}$ to a sheaf $\mathcal{F}$. Assume that:*

1. *the only sections of $\mathcal{P}$ to have the same image in $\mathcal{F}(U)$ are those that are locally equal,*
2. *i is locally surjective.*

Then $(\mathcal{F}, i)$ is the sheaf associated with $\mathcal{P}$.

Proof. Let $i' : \mathcal{P} \to \mathcal{F}'$ be any morphism from $\mathcal{P}$ into a sheaf $\mathcal{F}'$. Let $s \in \mathcal{F}(\mathcal{U})$ with $U \to X$ étale. We must construct an image of s in $i'(\mathcal{P}(U))$.
Since i is locally surjective, $\exists s_i \in \mathcal{P}(U_i)$ such that $i(s_i) = s|_{U_i}$ for some covering $(U_i \to U)_{i\in I}$ of U. Because of (1), and property of sheaf $\mathcal{F}'$ then $i'(s_i) \in \mathcal{F}'(U_i)$ is independent of the choice of s_i, and moreover that the restrictions of $i'(s_i)$ and $i'(s_j)$ to $\mathcal{F}'(U_i \otimes_U U_j)$

agree. We define $\alpha(s)$ to be the unique element of $\mathcal{F}'(U)$ that restricts to $i'(s_i)$ for all i. Then we have the commutative diagram:

$$\begin{tikzcd} \mathcal{P} \arrow[rr, "i"] \arrow[dr, "i'"'] & & \mathcal{F} \arrow[dl, "\exists!\alpha"] \\ & \mathcal{F}' & \end{tikzcd}$$

□

Lemma 2.27. *Let $\mathcal{P}$ be a subpresheaf of a sheaf $\mathcal{F}$. For each U, let $\mathcal{P}'(U)$ be the set of $s \in \mathcal{F}(U)$ that are locally in $\mathcal{P}$ in the sense that there exists a covering $(U_i \to U)_{i\in I}$ such that $s|_{U_i} \in \mathcal{P}(U_i)$ for each i, i.e.*

$$\mathcal{P}'(U) = \{s \in \mathcal{F}(U) | \exists a \text{ covering } (U_i \to U)_{i\in I} \text{ s.t. } s|_{U_i} \in \mathcal{P}(U_i) \forall i \in I\}.$$

Then $\mathcal{P}'$ is a subsheaf of $\mathcal{F}$, and $\mathcal{P} \to \mathcal{P}'$ is locally surjective. We call $\mathcal{P}'$ the subsheaf of $\mathcal{F}$ generated by $\mathcal{P}$.

Proof. The locally surjective property of $\mathcal{P} \to \mathcal{P}'$ is clear from the definition of $\mathcal{P}'(U)$. It suffices to prove that $\mathcal{P}'$ is a sheaf. Let $(U_i \to U)_{i\in I}$ be a covering of $U \to X$ étale, we need to prove that the sequence

$$\mathcal{P}'(U) \hookrightarrow \prod_i \mathcal{P}'(U_i) \rightrightarrows \prod_{i,j} \mathcal{P}'(U_i \otimes_U U_j)$$

is exact. Since $\mathcal{P}'$ is a subpresheaf of $\mathcal{F}$, it suffices to prove that

$$\forall (s_i) \in \prod \mathcal{P}'(U_i) \text{ s.t } s_i|_{U_i\otimes_U U_j} = s_j|_{U_i \otimes_U U_j} \text{ then } \exists s \in \mathcal{P}'(U) \text{ such that } s|_{u_i} = s_i.$$

Because $\mathcal{F}$ is a sheaf then

$$\exists s \in \mathcal{F}(U) \text{ such that } s|_{u_i} = s_i.$$

We need to prove that $s \in \mathcal{P}'(U)$ Indeed, by definition of $\mathcal{P}'$, we know that there exists a covering $(V_{ij} \to U_i)_j$ such that $s_i|_{V_{ij}} \in \mathcal{P}(V_{ij})$ for each i. So $s|_{V_{ij}} = s_i|_{V_ij} \in \mathcal{P}(V_{ij})$ and $(V_{ij} \to U)$ is an étale covering of U. Hence, $s \in \mathcal{P}'(U)$. □

Lemma 2.28. *If $i : \mathcal{P} \to \mathcal{F}$ satisfies conditions (1) and (2) of lemma 3, then*

$$i_{\overline{x}} : \mathcal{P}_{\overline{x}} \to \mathcal{F}_{\overline{x}}$$

is an isomorphism for all geometric points $\overline{x}$ of X.

Proof. It suffices to prove that $i_{\overline{x}}$ is injective and surjective for all geometric points $\overline{x}$ of X.

- Fix a geometric point $\overline{x}$ of X, we will prove that

$$i_{\overline{x}} : \mathcal{P}_{\overline{x}} \to \mathcal{F}_{\overline{x}}$$

is injective.

Indeed, let $s_{\overline{x}}$ in $\mathcal{P}_{\overline{x}}$ be such that $i_{\overline{x}}(s_{\overline{x}}) = 0$ where $s \in \mathcal{P}(U)$ for some étale neighborhood U of $\overline{x}$. Consider the diagram

$$\begin{tikzcd} \mathcal{P}(U) \arrow[r, "i"] \arrow[d] & \mathcal{F}(U) \arrow[d] \\ \mathcal{P}_{\overline{x}} \arrow[r, "i_{\overline{x}}"] & \mathcal{F}_{\overline{x}} \end{tikzcd}$$

This implies that $i(s)_{\overline{x}} = 0$, so there is V such that

$$\begin{tikzcd} V \arrow[r, "\text{étale}"] & U \arrow[r] & X \\ \overline{x} \arrow[u] \arrow[ur] \arrow[urr] & & \end{tikzcd}$$

commutes and $i(s)|_V = 0$

Since i is locally equal (in the sense of *lemma 2.25*), there exists W such that

$$\begin{tikzcd} \exists W \arrow[r, "\text{étale}"] & V \\ \overline{x} \arrow[u] \arrow[ur] & \end{tikzcd}$$

commutes and $s|_W = 0$. Hence $s_{\overline{x}} = 0$ or $i_{\overline{x}}$ is injective.

- Similarly, we will prove that $i_{\overline{x}} : \mathcal{P}_{\overline{x}} \to \mathcal{F}_{\overline{x}}$ is surjective.

Indeed, let $t_{\overline{x}} \in \mathcal{F}_{\overline{x}}$ where $t \in \mathcal{P}(U)$ for some étale neighborhood U of $\overline{x}$. Consider the diagram

$$\begin{tikzcd} \mathcal{P}(U) \arrow[r, "i"] \arrow[d] & \mathcal{F}(U) \arrow[d] \\ \mathcal{P}_{\overline{x}} \arrow[r, "i_{\overline{x}}"] & \mathcal{F}_{\overline{x}} \end{tikzcd}$$

Since i is locally surjective, there exists a covering $(U_i \to U)_i$ such that t_{U_i} is in the image of $\mathcal{P}_{U_i} \to \mathcal{F}_{U_i}$. Consider the diagram

$$\begin{tikzcd}
\mathcal{P}(U) \arrow[r, "i"] \arrow[d] & \mathcal{F}(U) \arrow[d] \\
\mathcal{P}(U_i) \arrow[r] & \mathcal{F}(U_i)
\end{tikzcd}$$

$$\Rightarrow \exists s \in \mathcal{P}(U) : s|_{U_i} = s_i$$

$$\Rightarrow t|_{U_i} = i(s|_{U_i}) = i(s)|_{U_i}$$

$$\Rightarrow t|_{\overline{x}} = i(s)_{\overline{x}} = i_{\overline{x}}(s_{\overline{x}}).$$

This means that $i_{\overline{x}}$ is surjective.

$\square$

Theorem 2.29. *For any presheaf $\mathcal{P}$ on $X_{ét}$, there exists an associated sheaf $i : \mathcal{P} \to a\mathcal{P}$. Moreover, the map i induces isomorphisms $\mathcal{P}_{\overline{x}} \to (a\mathcal{P}_{\overline{x}})$ on the stalks. The functor $a : PreSh(X_{ét}\ ) \to Sh(X_{ét})$ is exact.*

Proof. Define the sheaf $\mathcal{P}^*$ as in *lemma 2.2.19* (key lemma). Then $\mathcal{P}^*$ is a sheaf and the natural map $\mathcal{P} \to \mathcal{P}^*$ satisfies conditions (1) and (2) of lemma 3. Take $a\mathcal{P}$ to be the subsheaf of $\mathcal{P}^*$ generated by $i(\mathcal{P})$. Then $i : \mathcal{P} \to a\mathcal{P}$ satisfies the conditions (1) and (2) of Lemma 3. So $i : \mathcal{P} \to a\mathcal{P}$ is the sheafification of $\mathcal{P}$.
For the second statement, let

$$\mathcal{P}' \to \mathcal{P} \to \mathcal{P}''$$

is an exact sequence of abelian groups, then

$$\mathcal{P}'_{\overline{x}} \to \mathcal{P}_{\overline{x}} \to \mathcal{P}''_{\overline{x}}$$

is exact for all $x \in X$ (because direct limit is an exact functor).

$$\Longrightarrow (a\mathcal{P}')_{\overline{x}} \to (a\mathcal{P})_{\overline{x}} \to (a\mathcal{P})''_{\overline{x}}$$

is also an exact sequence. Which shows that

$$a\mathcal{P}' \to a\mathcal{P} \to a\mathcal{P}''$$

is exact. $\square$

Finally, by considering the sheafification of a presheaf we have that the category of sheaves of abelian groups on $X_{\text{ét}}$ is abelian.

Theorem 2.30. *Since the functor $i : PreSh(X_{ét}\ ) \to Sh(X_{ét})$ is left exact, and its left adjoint functor $a : PreSh(X_{ét}\ ) \to Sh(X_{ét})$ is exact, the kernel (resp., cokernel, image and co-image) of a morphism in the category of sheaf $Sh(X_{ét})$ is the associated sheaves of the kernel (resp., cokernel, image and co-image) of the morphism in the category of presheaf $PreSh(X_{ét})$. In particular, the map from the co-image of a morphism to its image is an isomorphism because it is on stalks. Hence, the category of sheaves of abelian groups $Sh(X_{ét})$ is abelian.*

Example 2.3. *A group Λ defines a constant presheaf $\mathcal{P}_\Lambda$ such that $\mathcal{P}_\Lambda(U) = \Lambda$ for all $U \neq \emptyset$. Then the sheaf associated with $\mathcal{P}_\Lambda$ is $\mathcal{F}_\Lambda$ defined by $\mathcal{F}_\Lambda(U) = \Lambda^{\pi_0(U)}$ where $\pi_0(U)$ is the number of connected components of U.*

In the proof of the above theorems, we see that if $(\mathcal{F}_i)_{i\in I}$ is a family of sheaves of abelian groups on $X_{\text{ét}}$. Then the presheaf defined by $\mathcal{P}(U) = \prod_{i\in I} \mathcal{F}_i(U)$ for all $U \to X$ étale and the obvious restriction maps is a sheaf. Moreover, it is the product of $(\mathcal{F}_i)_{i\in I}$ in the category. But, in general, the presheaf defined by $\mathcal{P}(U) = \bigoplus_{i\in I} \mathcal{F}_i(U)$ is not a sheaf.

Direct and inverse images of sheaves

Direct images: Let $\pi : Y \to X$ be a morphism of schemes, and let $\mathcal{P}$ be a presheaf on $Y_{\text{ét}}$. For $U \to X$ étale, define

$$\pi_*\mathcal{P}(U) = \mathcal{P}(U \otimes_X Y).$$

With the obvious restriction maps, $\pi_*\mathcal{P}$ becomes a presheaf on $X_{\text{ét}}$. Moreover, we can easily obtain that if we have the diagram of morphisms $Z \xrightarrow{\pi} Y \xrightarrow{\pi'} X$ then $(\pi' \circ \pi)_* = \pi'_* \circ \pi_*$.

Lemma 2.31. *If $\mathcal{F}$ is a sheaf then so also is $\pi_*\mathcal{F}$. Moreover, since the functor $\pi_* : PreSh(Y_{ét}\ ) \to PreSh(X_{ét}\ )$ defined as above is exact, the functor $\pi_* : Sh(Y_{ét}\ ) \to Sh(X_{ét}\ )$ is left exact.*

Proof. For a morphism $V \to X$, we denote V_Y the fibre product $V \otimes_X Y$ over Y. Then $V \to V_Y$ is a functor taking the étale maps to étale maps, sujective families of maps to sujective families, and the fibre products over Y.
Let $(U_i \to U)_i$ be a surjective family of étale maps in $X_{\text{ét}}$. Then $U_{iY} \to U_Y$ is a surjective family of étale maps in $Y_{\text{ét}}$, and so

$$\mathcal{F}(U_Y) \to \prod_i \mathcal{F}(U_{iY}) \to \prod_{i,j} \mathcal{F}(U_{iY} \otimes_Y U_{jY})$$

is exact. Hence,

$$(\pi_*\mathcal{F})(U) \to \prod_i (\pi_*\mathcal{F})(U_i) \to \prod_{i,j} (\pi_*\mathcal{F})(U_i \otimes_X U_j)$$

is exact. This means that $\pi_*\mathcal{F}$ is a sheaf.
The functor the functor $\pi_* : PreSh(Y_{\text{ét}}) \to PreSh(X_{\text{ét}})$ is exact by definition.
Let $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ be an exact sequence of sheaf. Then

$$0 \to \mathcal{F}'(U_Y) \to \mathcal{F}(U_Y) \to \mathcal{F}''(U_Y)$$

is exact for every $U \to X$ étale. Hence

$$0 \to (\pi_*\mathcal{F}')(U) \to (\pi_*\mathcal{F})(U) \to (\pi_*\mathcal{F}'')(U)$$

is exact for every U. Hence,

$$0 \to \pi_*\mathcal{F}' \to \pi_*\mathcal{F} \to \pi_*\mathcal{F}''$$

is exact.

□

Proposition 2.32. *[Mil80]*

1. *Let $\pi : V \hookrightarrow X$ be an open immersion,i.e. the inclusion of an open subscheme into X. Then*
$$(\pi_*\mathcal{F})_{\overline{x}} = \mathcal{F}_{\overline{x}} \quad \text{if } x \in V$$

2. *Let $\pi : V \hookrightarrow X$ be an open immersion,i.e. the inclusion of a closed subscheme into X. Then*
$$(\pi_*\mathcal{F})_{\overline{x}} = \begin{cases} \mathcal{F}_{\overline{x}} & x \in V \\ 0 & x \notin V \end{cases}$$

3. *Let $\pi : Y \to X$ be a finite map. Then*
$$(\pi_*\mathcal{F})_{\overline{x}} = \bigoplus_{y \mapsto x} \mathcal{F}_{\overline{x}}^{d(y)}$$
where $d(y)$ is the separable degree of $k(y)$ over $k(x)$. For example, if π is a finite étale map of degree d of varieties over an algebraically closed field, then
$$(\pi_*\mathcal{F})_{\overline{x}} = \mathcal{F}_{\overline{x}}^{d(y)}$$

Corollary 2.33. *The functor π_* is exact if π is finite or closed immersion.*

Next, we will prove that there exists a left adjoint functor to the functor direct image, and we call it *inverse image functor*

Inverse images: Again, let $\pi : Y \to X$ be a morphism of schemes on $X_{\text{ét}}$. For $V \to Y$ étale, define

$$\mathcal{P}'(V) = \varinjlim \mathcal{P}(U)$$

where the direct limit is over the commutative diagrams

$$\begin{tikzcd} V \arrow[r] \arrow[d] & U \arrow[d, "\text{étale}"] \\ Y \arrow[r] & X \end{tikzcd}$$

It's easy to prove that the category of such objects U and the morphism defined by the étale morphism is a filtered category, and so, we can take the direct limit.
Moreover, since the universal property of the fibre product, one can see easily that, for any presheaf $\mathcal{Q}$ on $Y_{\text{ét}}$, there are natural one-to-one correspondences between

- morphisms $\mathcal{P}' \to \mathcal{Q}$,
- families of maps $\{\mathcal{P}'(V) \to \mathcal{Q}(V)\}_{V\to Y \text{étale}}$ indexed by $V \to Y$ étale,
- families of maps $\{\varinjlim \mathcal{P}(U) \to \mathcal{Q}(V)\}_{V\to Y \text{ étale}}$ where the limit is taken over the above commutative diagrams,
- families of maps $\{\{\mathcal{P}(U) \to \mathcal{Q}(V)\}_{U\to X \text{ étale, commutative, compatible,}}\}_{V\to Y \text{ étale}}$, where the families $\mathcal{P}'(U) \to \mathcal{Q}(V)$ is indexed by commutative diagrams as above such that they are compatible with restriction maps,
- families of maps $\{\{\mathcal{P}(U) \to \mathcal{Q}(V)\}_{V\to Y \text{ étale, commutative, compatible}}\}_{U\to X \text{ étale}}$, where the families $\{\mathcal{P}'(U) \to \mathcal{Q}(V)\}_{V\to Y}$ is indexed by commutative diagrams as above such that they are compatible with restriction maps,
- $\{\mathcal{P}(U) \to \mathcal{Q}(U \otimes_X Y)\}_{U\to X \text{ étale}}$.

This means that there is natural one-to-one correspondences between

- morphisms $\mathcal{P}' \to \mathcal{Q}$,
- morphisms $\mathcal{P} \to \pi_*\mathcal{Q}$.

Thus,

$$Hom_{Y_{\text{ét}}}(\mathcal{P}', \mathcal{Q}) \cong Hom_{X_{\text{ét}}}(\mathcal{P}, \pi_*\mathcal{Q}),$$

functorially in $\mathcal{P}$ and $\mathcal{Q}$.
Unfortunately, $\mathcal{P}'$ need not be a sheaf even when $\mathcal{P}$ is. Therefore, for $\mathcal{F}$ a sheaf on $X_{\text{ét}}$, we define

$$\pi^*\mathcal{F} = a(\mathcal{F}') \text{ the associated sheaf of } \mathcal{F}'.$$

Then, for any sheaf $\mathcal{G}$ on $Y_{\text{ét}}$, we have that

$$Hom_{Y_{\text{ét}}}(\pi_*\mathcal{F}, \mathcal{G}) \cong Hom_{Y_{\text{ét}}}(\mathcal{F}', \pi_*\mathcal{G}) \cong Hom_{X_{\text{ét}}}(\mathcal{F}, \pi_*\mathcal{G}).$$

This means that π^* is a left adjoint to $\pi_* : Sh(Y_{\text{ét}}) \to Sh(X_{\text{ét}})$.
We know that for a diagram of morphisms $Z \xrightarrow{\pi} Y \xrightarrow{\pi'} X$ then $(\pi' \circ \pi)_* = \pi'_* \circ \pi_*$. Since π^* is a left adjoint to π_*, it is easy to prove that $(\pi' \circ \pi)^* = \pi^* \circ \pi'^*$.

Example 2.4. *Inverse images of étale constant sheaves are étale constant sheaves. That means $f^*(\Lambda) = \Lambda$ for every abelian group Λ.*

We have proved some properties of exactness of some special functors. In the next proposition, we will state again the exactness of some special functors. Moreover, in category theory, we know that if a functor R admits an exact left adjoint then it preserves injectives (if they exist).

Proposition 2.34. *Let X be a scheme, and $\pi : Y \to X$ a morphism of schemes. Then*

1. *The functor $i : Sh(X_{ét}) \to PreSh(X_{ét})$ has a left adjoint functor $a : PreSh(X_{ét}) \to Sh(X_{ét})$, hence i is left exact and a is right exact. Moreover, the functor $a : PreSh(X_{ét}) \to Sh(X_{ét})$ is exact. So, the functor i preserves injectives.*

2. *The functor $\pi_* : Sh(Y_{ét}) \to Sh(X_{ét})$ has left adjoint functor $\pi^* : Sh(X_{ét}) \to Sh(Y_{ét})$, hence, π_* is left exact, and π^* is right exact. Moreover, the functor $\pi^* : Sh(X_{ét}) \to Sh(Y_{ét})$ is exact. So, the functor π_* preserves injectives.*

3. *Let $j : U \to X$ be an étale morphism, and $\mathcal{F}$ be a sheaf on $U_{ét}$. For any $\phi : V \to X$ étale, define*
$$\mathcal{F}_!(V) = \bigoplus_{\alpha} \mathcal{F}(V)$$
where the sum is over the morphism $\alpha : V \to U$ such that $j \circ \alpha = \phi$. Denote $j_!\mathcal{F}$ the sheaf associated with the presheaf $\mathcal{F}_!$.
Then the functor $j_!$ is a left adjoint to $j^* : Sh(X_{ét}) \to Sh(U_{ét})$. Moreover the functor $j_!$ is exact; hence, j^* is exact and preserves injectives.

Proof. The assertion (1) is proved in the previous propositions.
For (2), let $i : \overline{x} \to X$ be a geometric point of X and $\mathcal{F}$ be any sheaf on $X_{\text{ét}}$, then

by definition $(i^*\mathcal{F})(\overline{x}) = a\mathcal{F}'(\overline{x}) = \mathcal{F}'(\overline{x}) = \varinjlim \mathcal{F}(U)$ where the direct limit is over the commutative diagrams:

$$\begin{tikzcd} \overline{x} \arrow[r] \arrow[d] & U \arrow[d, "\text{étale}"] \\ \overline{x} \arrow[r] & X \end{tikzcd}$$

This means that the direct limit is over the étale neighborhood of $\overline{x}$. So $(i^*\mathcal{F})(\overline{x}) = \mathcal{F}_{\overline{x}}$. Therefore, for any geometric point $i : \overline{y} \to Y$ of Y, we have that

$$(\pi^*\mathcal{F})_{\overline{y}} = i^*(\pi^*\mathcal{F})(\overline{y}) = \mathcal{F}_{\overline{x}}$$

where $\overline{x}$ is the geometric point $\overline{y} \to Y \to X$ of X.
Since this is true for all geometric point of Y, we see that π^* is exact and therefore that π_* preserves injectives.
For (3), we need to prove that $Hom_{X_{\text{ét}}}(j_!\mathcal{F}, \mathcal{G}) \cong Hom_{U_{\text{ét}}}(\mathcal{F}, j^*\mathcal{G})$. Indeed, by the definition of sheafification, we have $Hom_{X_{\text{ét}}}(j_!\mathcal{F}, \mathcal{G}) \cong Hom_{X_{\text{ét}}}(\mathcal{F}_!, \mathcal{G})$ and $Hom_{U_{\text{ét}}}(\mathcal{F}, j^*\mathcal{G}) \cong Hom_{U_{\text{ét}}}(\mathcal{F}, \mathcal{G}|_U)$. By the universal property of direct sum, there are one to one correspondence between:

- morphisms $\varphi : \mathcal{F}_! \to \mathcal{G}$,
- families of maps $\{\varphi(V) : \mathcal{F}_!(V) \to \mathcal{G}(V)\}_{V \to X \text{ étale}}$,
- families of maps $\{\varphi(V) : \bigoplus\limits_{\alpha} \mathcal{F}(V) \to \mathcal{G}(V)\}_{V \to X \text{ étale}}$, where the sum is taken over all of $\alpha : V \to U$ such that $j \circ \alpha = V \to X$,
- families of maps $\{\varphi(V) : \mathcal{F}(V) \to \mathcal{G}(V)\}_{V \to U \to X \text{ étale}}$,
- families of maps $\{\varphi(V) : \mathcal{F}(V) \to \mathcal{G}(V)\}_{V \to U \text{ étale}}$,
- $\varphi : \mathcal{F} \to \mathcal{G}|_U$.

To prove the second statement, it suffices to prove that

$$(j_!\mathcal{F})_{\overline{x}} = \begin{cases} \mathcal{F}_{\overline{x}} & \text{if } x \in j(U) \\ 0 & \text{otherwise.} \end{cases}$$

Indeed,

$$(j_!\mathcal{F})_{\overline{x}} = \varinjlim (j_!\mathcal{F}(V)) = \varinjlim \bigoplus_{\alpha} \mathcal{F}(V) = \bigoplus_{\alpha} \varinjlim \mathcal{F}(V) = \bigoplus_{x \in j(U)} \mathcal{F}_{\overline{x}} = \begin{cases} \mathcal{F}_{\overline{x}} & \text{if } x \in j(U) \\ 0 & \text{otherwise.} \end{cases}$$

$\square$

Remark 2.35. In particular, if $\varphi : U \hookrightarrow X$ is an open immersion, then $j_!\mathcal{F}$ is the associated sheaf of the presheaf

$$\mathcal{F}_!(V) = \begin{cases} \mathcal{F}(V) & \text{if } \varphi(V) \subset U \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.36. *Let X be a scheme, then every sheaf $\mathcal{F}$ on $Sh(X_{\acute{e}t})$ can be embedded into an injective sheaf.*

Proof. For each point $x \in X$, choose a geometric point $i_x : \overline{x} \to X$ with image x . Since the category of abelian groups has enough injective, we can choose an injective group $I(x)$ such that $\mathcal{F}_{\overline{x}} \hookrightarrow I(x)$. Since i_{x*} preserves injectives, $\mathcal{I}^x := i_{x*}(I(x))$ is injective. On the other hand, a product of injective objects is injective, so $\mathcal{I} := \prod \mathcal{I}^x$ will be an injective sheaf. Let $\mathcal{F}^* = \prod_{x\in X} (\mathcal{F}_{\overline{x}})^{\overline{x}}$ be the sheaf defined as before, then we have the canonical embedding

$$\mathcal{F} \hookrightarrow \mathcal{F}^* \hookrightarrow \mathcal{I}.$$

(the second canonical embedding comes from the fact that π_{x*} is left exact). This proves the theorem. □

Theorem 2.37. *Some important exact sequences of sheaves:*

1. *Let $j : U \hookrightarrow X$ be an open immersion, Z be the complement of U in X and denote the inclusion $Z \hookrightarrow X$ by i. Let $\mathcal{F}$ be any sheaf on $X_{\acute{e}t}$, there is a canonical morphism $j_!j^*\mathcal{F} \to \mathcal{F}$, corresponding by adjointness to the identity map on $j^*\mathcal{F}$ and a canonical morphism $\mathcal{F} \to i_*i^*\mathcal{F}$, corresponding by adjointness to the identity map on $i^*\mathcal{F}$. Then the sequence*

$$0 \to j_!j^*\mathcal{F} \to \mathcal{F} \to i_*i^*\mathcal{F} \to 0$$

is exact.

2. ***(Kummer sequence)** Let n be an integer that is not divisible by the characteristic of any residue field of X (if so, we say that n is invertible in X.) For example, if X is a variety over a field k of characteristic $p \neq 0$, then we require that p not divide n. Then the sequence of sheaves:*

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{t \mapsto t^n} \mathbb{G}_m \longrightarrow 0$$

is exact.

Proof. 1. It suffices to prove the exact sequences on stalks. For $x \in U$, the sequence of stalks is

$$0 \longrightarrow \mathcal{F}_{\overline{x}} \xrightarrow{id} \mathcal{F}_{\overline{x}} \longrightarrow 0 \longrightarrow 0 \ ,$$

and for $x \notin U$, the sequence of stalks is

$$0 \longrightarrow 0 \longrightarrow \mathcal{F}_{\overline{x}} \xrightarrow{id} \mathcal{F}_{\overline{x}} \longrightarrow 0 \ .$$

Both are exact.

2. Firstly, I remark that n is invertible in X if and only if n is invertible in $\mathcal{O}_X(X)$. Indeed, by the property of sheaf, it suffices to prove the statement for $X = Spec(A)$ affine. From the assumption, we have $n \notin pA_p$ for all$p \subset A$ prime $\Rightarrow n \not| np \forall p \Rightarrow$ n is invertible in A. The converse is clear.
For the proof of exactness of the Kummer sequence, it is easy to see that

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{t \mapsto t^n} \mathbb{G}_m$$

is exact. So, it suffices to prove that $\mathbb{G}_m \xrightarrow{t \mapsto t^n} \mathbb{G}_m \longrightarrow O$ is exact. We will prove that the morphism $t \mapsto t^n$ is locally surjective.
Let $U \to X$ étale, $a \in G_m(U) = \mathcal{O}_U(U)^\times$. Assume that $U = \bigcup_{i \in I} Spec(A_i)$. Let

$$U_i = Spec\big(A_i[T]/(T^n - a|_{Spec(A_i)})\big),$$

Since n is invertible in X, n is also invertible in U (hence, in A_i), then $T^n - a$ is separable. Therefore, $(U_i \to U)_{i \in I}$ is an étale covering of U. The map $\mathbb{G}_m \xrightarrow{t \mapsto t^n} \mathbb{G}_m$ becomes

$$Spec\big(A_i[T]/(T^n - a|_{Spec(A_i)})\big) \xrightarrow{t \mapsto t^n} Spec\big(A_i[T]/(T^n - a|_{Spec(A_i)})\big)$$

And so $a|_{Spec(A_i)}$ is in the image of the map $t \mapsto t^n$ above.

□

Remark 2.38. 1. If $\varphi : j_! j^* \mathcal{F} \to \mathcal{F}$ is the canonical morphism corresponding by adjointness to the identity map on $j^*\mathcal{F}$ then, for every $x \in U$, for every étale neighborhood V of x, we can choose V small such that $V \to X$ factors through U. And so, the mapping $\varphi_{\overline{x}} = id_{\overline{x}}$. And similarly, let $f : X \to Y$ be a morphism of scheme and $\alpha : f^* f_* \mathcal{F} \to \mathcal{F} \in Hom_{X_{\text{ét}}}(f^* f_* \mathcal{F}, \mathcal{F})$ corresponding by adjointness to the identity map $f_* \mathcal{F} \to f_* \mathcal{F}$ then for every $x \in X$ such that $\mathcal{O}_{Y,f(x)}/\mathfrak{m}_{f(x)} \to \mathcal{O}_{X,x}/\mathfrak{m}_x$ is a separable extension (hence, the geometric point $\overline{x} \to X$ is also a geometric point of Y), we have $\alpha_{\overline{x}} = id_{\overline{x}}$. Similarly, if $\beta : \mathcal{F} \to f_* f^* \mathcal{F}$ is the canonical morphism corresponding to the identity $f^*\mathcal{F} \to f^*\mathcal{F}$ then for every $y \in Y$ such that $\overline{y} \to Y$ factors through X then $\beta_y = id_{\overline{y}}$.

2. In fact, to define $j_!$ and have the exact sequence, we don't need $U \hookrightarrow X$ open immersion, we just need $U \to X$ étale, and so we can take $Z = X \setminus j(U)$. Moreover, in the situation of the exact sequence, we only need that j satisfies the following condition: if $\varphi = j \circ \alpha$ is étale then α is étale. Hence, we only need to assume j is unramified, and the stalk doesn't change (note that an unramified morphism is not an open map, in general, so we must change the situation of Z in the exact sequence).

2.3 Étale Cohomology

In the last section, we showed that the category of sheaves of abelian groups $Sh(X_{\text{ét}})$ is an abelian category with enough injectives.
The functor of global section

$$\Gamma(X, -) : Sh(X_{\text{ét}}) \to Ab$$

is left exact, and so we can define $H^r(X_{\text{ét}}, -)$ to be its r-th right derived functor. Explicitly, for a sheaf $\mathcal{F}$, choose an injective resolution

$$0 \to \mathcal{F} \to \mathcal{I}^0 \to \mathcal{I}^1 \to \mathcal{I}^2 \to \cdots,$$

and apply the functor $\Gamma(X, -)$ to obtain a complex

$$0 \to \Gamma(X, \mathcal{I}^0) \to \Gamma(X, \mathcal{I}^1) \to \Gamma(X, \mathcal{I}^2) \to \cdots$$

This is no longer exact in general, and $H^r(X_{\text{ét}}, -)$ is defined to be its r-th cohomology group.
The theory of derived functors shows that:

- for any sheaf $\mathcal{F}$, then $H^0(X_{\text{ét}}, \mathcal{F}) \cong \Gamma(X, \mathcal{F})$,
- if $\mathcal{I}$ is injective, then $H^r(X_{\text{ét}}, \mathcal{I}) = 0$ for every $r > 0$,
- a short exact sequence of sheaves

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

gives rise to long exact sequence

$$0 \to H^0(X_{\text{ét}}, \mathcal{F}') \to H^0(X_{\text{ét}}, \mathcal{F}) \to H^0(X_{\text{ét}}, \mathcal{F}'') \to H^1(X_{\text{ét}}, \mathcal{F}') \to \cdots,$$

and the association of the long exact sequence with the short exact sequence is functorial.

Remark 2.39. The functors $H^r(X_{\text{ét}}, -)$ are uniquely determined (up to a unique isomorphism) by above properties (universal property of derived functors).

Example 2.5. *Some basic examples of étale cohomology.*

1. *Let $\varphi : U \to X$ be an étale morphism. Then $\varphi^* : Sh(X_{ét}) \to Sh(U_{ét})$ is exact and preserves injectives (propsition 2.2.22). Moreover φ^* is just the restriction, we see that the composite*

$$Sh(X_{ét}) \xrightarrow{\varphi^*} Sh(U_{ét}) \xrightarrow{\Gamma(U,-)} Ab$$

is $\Gamma(U,-)$. So the right derived functors of $\mathcal{F} \to \mathcal{F}(U) : Sh(X_{ét}) \to Ab$ are $\mathcal{F} \to H^r(U_{ét}, \mathcal{F}|_U)$. We often denote $H^r(U_{ét}, \mathcal{F}|_U)$ by $H^r(U_{ét}, \mathcal{F})$.

2. *Let $\varphi : Y \to X$ be a morphism. We know that φ^* is exact, and therefore a short exact sequence*

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

of sheaves on X gives rise to a long exact sequence

$$0 \to H^0(Y_{ét}, \varphi^*\mathcal{F}') \to \cdots \to\to H^r(Y_{ét}, \varphi^*\mathcal{F}') \to H^0(Y_{ét}, \varphi^*\mathcal{F}) \to H^0(Y_{ét}, \varphi^*\mathcal{F}'') \to \cdots$$

of cohomology groups.
By the universal property of derived functors, the natural map $H^0(X_{ét}, \mathcal{F}) \to H^0(Y_{ét}, \varphi^*\mathcal{F})$ extends uniquely to a family of natural maps $H^r(X_{ét}, \mathcal{F}) \to H^r(Y_{ét}, \varphi^*\mathcal{F})$ compatible with the boundary maps.

3. *(Cohomology of a geometric point) Let x be a geometric point of X then $H^r(x, \mathcal{F}) = 0$ for $r > 0$*

4. *For a fixed sheaf $\mathcal{F}_0$, the functor $\mathcal{F} \mapsto Hom_X(\mathcal{F}_0, \mathcal{F})$ is left exact, and we denote its $r-th$ right derived functor by $Ext^r(\mathcal{F}_0, -)$. Because $Hom_X(\mathcal{F}_0, -)$ is functorial in $\mathcal{F}_0$, so also is $Ext^r_X(\mathcal{F}_0, -)$. In particular, if $\mathbb{Z}$ is denoted the constant sheaf on X. Then for any sheaf $\mathcal{F}$ on X, the map $\alpha \mapsto \alpha(1)$ is an isomorphism $Hom_X(\mathbb{Z}, \mathcal{F}) \to \mathcal{F}(X)$. Thus $Hom_X(\mathbb{Z}, -) \cong \Gamma(X, -)$, and so $Ext^r_X(\mathbb{Z}, -) \cong H^r(X_{ét}, -)$. Beside*

the normal long exact sequence of cohomology, we also have that: a short exact sequence

$$0 \to \mathcal{F}_0' \to \mathcal{F}_0 \to \mathcal{F}_0'' \to 0$$

of sheaves on $X_{ét}$*gives rise to a long exact sequence*

$$\cdots \to Ext^r_X(\mathcal{F}_0'', \mathcal{F}) \to Ext^r_X(\mathcal{F}_0, \mathcal{F}) \to Ext^r_X(\mathcal{F}_0', \mathcal{F}) \to \cdots$$

for any sheaf $\mathcal{F}$.

5. *Let* Z *be a closed subscheme of* X, *and let* $U = X \setminus Z$. *For any sheaf* $\mathcal{F}$ *on* $X_{ét}$, *define*

$$\Gamma_Z(X, \mathcal{F}) = Ker\big(\Gamma(X, \mathcal{F}) \to \Gamma(U, \mathcal{F})\big).$$

Then the functor $\mathcal{F} \mapsto \Gamma_Z(X, \mathcal{F})$ *is obviously left exact, and we denote its* $r-th$ *right derived functor by* $H^r_Z(X, -)$ *(cohomology of* $\mathcal{F}$ *with support on* Z*). Then for any sheaf* $\mathcal{F}$ *on* $X_{ét}$*and closed* $Z \hookrightarrow X$, *there is a long exact sequence*

$$\cdots \to H^r_Z(X, \mathcal{F}) \to H^r(X, \mathcal{F}) \to H^r(U, \mathcal{F}) \to H^{r+1}_Z(X, \mathcal{F}) \to \cdots$$

And the sequence is functorial in the pair $(X, X \setminus Z)$ *and* $\mathcal{F}$.

Next, we would like to compute the cohomology $H^r(X_{\text{ét}}, \mu_n)$. For this, by Kummer sequence, it suffices to compute the cohomology $H^r(X_{\text{ét}}, G_m)$. Let X be an integral and quasi-compact scheme (hence, $U \to X$ étale implies U integral and quasi-compact), $g : Spec(K) \hookrightarrow x$ be the inclusion of the generic point. Denote $G_{m,K}$ the sheaf G_m on $Spec(K)_{\text{étale}}$, i.e. $G_{m,K}(U) = \Gamma(\mathcal{O}_U, U)^\times$ for every $U \to Spec(K)$ étale.
Claim: For $U \to X$ étale, then $g_* G_{m,K}(U) = \Gamma(U \otimes_X Spec(K), G_m) = k(U)^\times$ where $k(U)$ is the rational field of U.
For every $U \to X$ étale, we define morphism

$$\varphi(U) : G_m(U) \to g_* G_{m,K}(U)$$

as the injective morphism $\mathcal{O}_U(U) \hookrightarrow k(U)^\times$. Then we obtain an injective morphism of sheaves: $\varphi : G_m \to g_* G_{m,K}$.
Assume in addition, X is regular. We can define the Weil divisor sheaf as follows: let X_1 be the set of points x in X of codimension 1 (i.e. codimension of $\overline{\{x\}}$ is 1, equivalently, $\mathcal{O}_{X,x}$ has dimension 1, hence $\mathcal{O}_{X,x}$ is a discrete valuation ring). The sheaf Div_X of Weil divisors on $X_{\text{ét}}$is defined as the sum of direct image of constant sheaves on $\overline{\{x\}}$:

$$Div_X = \bigoplus_{x \in X_1} i_{x*}\mathbb{Z},$$

where $i_x : \overline{\{x\}} \hookrightarrow X$ the closed immersion. Remark that this sheaf is the associated sheaf of the presheaf defined by $\bigoplus_{x \in X_1} (i_{x,*}\mathbb{Z}(U))$, more precisely, $Div_X(U)$ is the free abelian group generated by *prime divisors* of U (a *prime divisors* of U is a closed integral subscheme Z of codimension 1).
Moreover, we have the following 1-1 correspondence:

$$\{X_1 = \text{set of points } x \in X \text{ of codimension } 1\} \longrightarrow \{\text{prime divisors of X}\} \ .$$

This correspondence comes from the correspondence between a closed integral subscheme and its generic point.
Similarly, for every non-empty $\varphi : U \to X$ étale, a prime divisor Z of X is said to meet U if intersection of Z and image of U is non-empty. Then the map $Z \to \varphi^{-1}(Z)$ define a bijection:

$$\{\text{set of prime divisors of X meeting U}\} \longrightarrow \{\text{set of prime divisors of U}\}$$

where the inverse map sends a prime divisor of U to closure of $\varphi(U)$.
If U is an open affine subscheme of X, with $\Gamma(U, \mathcal{O}_X) = A$ say, then the map $\mathfrak{p} \to V(\mathfrak{p})$ is a bijection:

$$\{\text{set of prime ideals of A of height one}\} \longrightarrow \{\text{set of prime divisors of U}\}$$

where the inverse map sends a prime divisor Z of U to the ideal $I(Z)$.
In particular, every prime divisor Z on X defines a discrete valuation ord_Z on K, namely, that corresponding the ideal $I(Z) \subset \Gamma(U, \mathcal{O}_U)$ where U is an open affine meeting Z.
So, for if $f \in k(U)^\times$ we can associate a map $f \to \sum ord_Z(f)$ where the sum is taken over all prime divisors of U. From a well-know result, we know that there are only finite prime divisors Z of U such that $ord_Z(f) \neq 0$, hence $\sum ord_Z(f) \in Div_X(U)$.

Theorem 2.40. *Then the sequence of sheaves*

$$0 \to G_m \to g_* G_{m,K} \to Div_X \to 0$$

is exact.

Proof. It suffices to prove that for every $x \in X$, the corresponding sequence of stalks at the geometric point $\overline{x}$ is exact. Since X is regular (hence, $U \to X$ étale implies U regular), we have that the sequence

$$0 \to \mathcal{O}_{X,\overline{x}} \to Frac(\mathcal{O}_{X,\overline{x}}) \to \bigoplus_{ht(p)=1} \mathbb{Z} \to 0$$

where the sum is taken over all prime ideal of $\mathcal{O}_{X,\overline{x}}$ of height 1. So, it suffices to calculus the stalks of all sheaves in the sequence at any geometric point $\overline{y} \in X$.

- The stalk of G_m at $\overline{y}$ is $\mathcal{O}_{X,\overline{y}} := \varinjlim \mathcal{O}_U(U)$ where the direct limit is taken over all étale neighborhood of $\overline{y}$.
- The stalk of $g_* G_{m,K}$ at $\overline{y}$ is $\big(Frac\mathcal{O}_{X,\overline{y}}\big)^\times$. Indeed,

$$(g_* G_{m,K})_{\overline{y}} = \varinjlim G_m(U \otimes_X \overline{\{y\}}) = \varinjlim k(U)^\times = \varinjlim \big(Frac\mathcal{O}_U(U)\big)^\times$$

$$= \big(Frac\big(\varinjlim \mathcal{O}_U(U)\big)\big)^\times = \big(Frac\mathcal{O}_{X,\overline{y}}\big)^\times.$$

- The stalk of Div_X at $\overline{y}$: Since $i_x : \overline{\{x\}} \hookrightarrow X$ is a closed immersion,

$$Div_{X,\overline{y}} = \sum_{x \in X_1} \big(i_{x,*}\mathbb{Z}\big)_{\overline{y}} = \sum_{x \in X_1 : y \in \overline{\{x\}}} \mathbb{Z}.$$

  Let $Spec(A) \subset X$ be an open neighborhood of y, then from the third correspondence, we have that

$$\{x \in X_1 : y \in \overline{\{x\}}\} \longrightarrow \{\mathfrak{p} \subset \mathcal{O}_{X,y} : ht(\mathfrak{p}) = 1\} \ .$$

  Hence, $Div_{X,\overline{y}} = \bigoplus_{ht(p)=1} \mathbb{Z}$.

□

2.3.1 Cohomology of curves

In this subsection, we will compute explicitly some cohomology groups of curves. More precisely, we will compute $H^r(X_{\text{ét}}, G_n)$ and $H^r(X_{\text{ét}}, \mu_n)$.

Theorem 2.41. *For a connected nonsingular curve X over an algebraically closed field,*

$$H^r(X_{\acute{e}t}, G_m) = \begin{cases} \Gamma(X, \mathcal{O}_X^\times) & \text{if } r = 0 \\ Pic(X) & \text{if } r = 1 \\ 0 & \text{if } r \geq 2. \end{cases}$$

Theorem 2.42. *Let X be a complete connected nonsingular curve over an algebraically closed field k. For any n prime to the characteristic of k, we have*

$$H^r(X_{ét}, \mu_n) = \begin{cases} \mu_n(k) & \text{if } r = 0 \\ (\mathbb{Z}/n\mathbb{Z})^{2g} & \text{if } r = 1 \\ \mathbb{Z}/n\mathbb{Z} & \text{if } r = 2 \\ 0 & \text{if } r > 2. \end{cases}$$

where g is the genus of X.

By considering the long exact sequence of Kummer sequence, and use the first theorem, we can easily prove the second theorem from the following lemma

Lemma 2.43. *Let X be a complete connected nonsingular curve over an algebraically closed field k. Then the sequence*

$$0 \to Pic^0(X) \to Pic(X) \to \mathbb{Z} \to 0$$

is exact where the morphism $Pic(X) \to \mathbb{Z}$ is the degree morphism and $Pic^0(X)$ is the quotient of the group of divisors of degree 0 $Div^0(X)$ by the subgroup of principal divisors. Moreover, for any integer n relatively prime to the characteristic of k, then the morphism

$$Pic^0(X) \to Pic^0(X)$$

defined by $z \mapsto nz$ is surjective such that its kernel equals to a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$ with g genus of X.

Proof. The first point of the lemma is easy. The proof of the second statement is more difficult. And so, we just consider an easy case $g = 1$ (i.e. elliptic curve over $\mathbb{C}$). For this, let E be an elliptic curve over $\mathbb{C}$ then $Pic^0(X) \cong E \cong \mathbb{C}/L$ where L is the lattice corresponding to E. So, the kernel is isomorphic to

$$\frac{1}{n}L/L \cong \mathbb{Z}/n\mathbb{Z}.$$

For an arbitrary algebraic closed field, the proof is similar (see [Mil80]). □

For curve, we only need the second theorem, but for general variety of dimension d, we also have that $H^r(X_{ét}, \Delta) = 0$ for every $r \geq 2d$ and Δ the constant sheaf. (see [Mil80]).

2.3.2 l-adic Cohomology

In the previous section, we have computed the cohomology of $\mathbb{Z}/l^n\mathbb{Z}$. However, it will be important for us to consider

$$H^1(X_{\text{ét}}, \mathbb{Z}_l) := \varprojlim H^1(X_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}).$$

Definition 2.44. *A sheaf of* $\mathbb{Z}_l$ *- modules* on X (or an l-adic sheaf) is a family $(\mathcal{M}_n, f_{n+1} : \mathcal{M}_{n+1} \to \mathcal{M}_n)$ such that

(a) for each n, $\mathcal{M}_n$ is a constructible sheaf of $\mathbb{Z}/l^n\mathbb{Z}$ - modules,

(b) for each n, the map $f_{n+1} : \mathcal{M}_{n+1} \to \mathcal{M}_n$ induces an isomorphism $\mathcal{M}_{n+1}/l^n\mathcal{M}_{n+1} \to \mathcal{M}_n$ where $\mathcal{M}_{n+1}/l^n\mathcal{M}_{n+1}$ is the sheafification of the presheaf defined by $\mathcal{M}_{n+1}/l^n\mathcal{M}_{n+1}(U) = \mathcal{M}_{n+1}(U)/l^n\mathcal{M}_{n+1}(U)$. Remark that $\mathcal{M}_{n+1}/l^n\mathcal{M}_{n+1} = \mathcal{M}_{n+1} \otimes \mathbb{Z}/l^n\mathbb{Z}$.

Let $(\mathcal{M}_n, f_n)_{n\in N}$ be a sheaf of $\mathbb{Z}_l$- modules on X. By induction, we obtain a canonical isomorphism $\mathcal{M}_{n+s}/l^n\mathcal{M}_{n+s} \cong \mathcal{M}_n$.
On the other hand, we have a sequence of constant sheaves:

$$0 \longrightarrow \mathbb{Z}/l^s\mathbb{Z} \xrightarrow{l^n} \mathbb{Z}/l^{n+s}\mathbb{Z} \longrightarrow \mathbb{Z}/l^n\mathbb{Z} \longrightarrow 0$$

(it is exact since the correspondent sequence of stalks is exact). On tensoring this sequence with $\mathcal{M}_{n+s}$, we obtain a sequence:

$$0 \longrightarrow \mathcal{M}_s \xrightarrow{l^n} \mathcal{M}_{n+s} \longrightarrow \mathcal{M}_n \longrightarrow 0$$

We say that $\mathcal{M}$ is *flat* if this sequence is exact for all n and s. Remark that by definition of associated sheaf, we imply that the morphism l^n is the scalar multiplication with l^n for every $U \to X$ étale.

For a sheaf $\mathcal{M} = (\mathcal{M}_n)$ of $\mathbb{Z}_l$-modules, we have a canonical morphism $H^r(X_{\text{ét}}, \mathcal{M}_{n+1}) \to H^r(X_{\text{ét}}, \mathcal{M}_n)$ induced by the morphismm f_{n+1}. So, we can define the *l-adic cohomology* by

$$H^r(X_{\text{ét}}, \mathcal{M}) = \varprojlim H^r(X_{\text{ét}}, \mathcal{M}_n).$$

For example, if we let $\mathbb{Z}_l$denote the sheaf of $\mathbb{Z}_l$-modules with $\mathcal{M}_n$ the constant sheaf $\mathbb{Z}/l^n\mathbb{Z}$ and the obvious f_n, then

$$H^r(X_{\text{ét}}, \mathbb{Z}_l) = \varprojlim H^r(X_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}).$$

In module theory, we know that to give a finitely generated $\mathbb{Z}_l$-module M is the same as to give a family $(M_n, f_{n+1} : M_{n+1} \to M_n)_{n\in\mathbb{N}}$ such that

(a) for all n, M_n is a finite $\mathbb{Z}/l^n\mathbb{Z}$- module,

(b) for all n, the map $f_{n+1} : M_{n+1} \to M_n$ induces an isomorphism $M_{n+1}/l^n M_{n+1} \to M_n$

We recall the finiteness theorem

Theorem 2.45. *Let X be a variety over a separably closed field k, and let $\mathcal{F}$ be a constructible sheaf on $X_{ét}$. The groups $H^r(X_{ét}, \mathcal{F})$ are finite in each of the following two cases:*

(a) X is complete, or

(b) $\mathcal{F}$ has no p-torsion, where p is the characteristic of k.

Hence, we can prove that the $l - adic$ cohomology is a finitely generated $\mathbb{Z}_l$-module.

Theorem 2.46. *Let $\mathcal{M} = (\mathcal{M}_n)$ be a flat sheaf of $\mathbb{Z}_l$-modules on a variety X over a field k. Assume k is separably closed, and that either X is complete of that $l \neq char(k)$. Then each $H^r(X_{ét}, \mathcal{M})$ is finitely generated, and there is an exact sequence of cohomology groups*

$$\cdots \to H^r(X_{ét}, \mathcal{M}) \to H^r(X_{ét}, \mathcal{M}) \to H^r(X_{ét}, \mathcal{M}_n) \to H^{r+1}(X_{ét}, \mathcal{M}) \to \cdots$$

Proof. For each $s \geq 0$, we ge an exact sequence

$$0 \to \mathcal{M}_n \to \mathcal{M}_{n+s} \to \mathcal{M}_n \to 0.$$

These are compatible in the sense that

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M}_{s+1} \arrow[r, "l^n"] \arrow[d] & \mathcal{M}_{n+s+1} \arrow[r] \arrow[d] & \mathcal{M}_n \arrow[r] \arrow[d, "id"'] & 0 \\
0 \arrow[r] & \mathcal{M}_s \arrow[r, "l^n"] & \mathcal{M}_{n+s} \arrow[r] & \mathcal{M}_n \arrow[r] & 0
\end{tikzcd}$$

commutes. On forming the cohomology sequence for each n and passing to the inverse limit over all n, we obtain an exact sequence

$$\cdots \to H^r(\mathcal{M}) \to H^r(\mathcal{M}) \to H^r(\mathcal{M}_n) \to H^{r+1}(\mathcal{M}) \to \cdots$$

where the first morphism is the l^n morphism.
This gives an exact sequence

$$0 \to H^r(\mathcal{M})/l^n H^r(\mathcal{M}) \to H^r(\mathcal{M}_n) \to H^{r+1}(\mathcal{M})_{l^n} \to 0.$$

Since $H^r(\mathcal{M})$ is an inverse limit of finite groups killed by some l^n, $\varprojlim H^{r+1}(\mathcal{M})_{l^n} = 0$, hence

$$\varprojlim H^r(\mathcal{M})/l^n H^r(\mathcal{M}) \cong H^r(\mathcal{M}).$$

Therefore, $H^r(\mathcal{M})$ is finitely generated as $\mathbb{Z}_l$ - module. $\square$

Sheaves of $\mathbb{Q}_l$-modules

A sheaf of $\mathbb{Q}_l$-vector spaces is just a $\mathbb{Z}_l$-sheaf $\mathcal{M} = (\mathcal{M}_n)$, except that we define

$$H^r(X_{\text{ét}}, \mathcal{M}) = \left(\varprojlim H^r(X_{\text{ét}}, \mathcal{M}_n)\right) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

For example,

$$H^r(X_{\text{ét}}, \mathbb{Q}_l) = \left(\varprojlim H^r(X_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z})\right) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = H^r(X_{\text{ét}}, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

By the previous theorem, we have that $H^r(X_{\text{ét}}, \mathcal{M})$ is a $\mathbb{Q}_l$-vector spaces of finite dimension.

2.3.3 Action of a morphism on cohomology

Let $f : X \to Y$ be a morphism of schemes. Then it induces the direct image $f_* : Sh(X_{\text{ét}}) \longrightarrow Sh(Y_{\text{ét}})$ and inverse image $f^* : Sh(Y_{\text{ét}}) \longrightarrow Sh(X_{\text{ét}})$ where $f_*(\mathcal{F})(U) = \mathcal{F}(U \times_Y X)$ for every $U \to X$ étale, $\mathcal{F}$ sheaf on $X_{\text{ét}}$, and $f^*(\mathcal{F})$ is the associated sheaf of presheaf $U \mapsto \underset{\rightarrow}{\ } F(V)$ defined in the previous chapter.

Proposition 2.47. *Let $f : X \to Y$ be a morphism of schemes. Then for any sheaf $\mathcal{F}$ on Y, we get a natural map*

$$f^\bullet : H^\bullet(Y, \mathcal{F}) \to H^\bullet(X, f^*\mathcal{F}).$$

Proof. Choose an injective resolution $0 \to \mathcal{F} \to \mathcal{I}^\bullet$ of $\mathcal{F}$. Applying the functor f^*, which is exact, we obtain a resolution (not necessary injective) of $f^*\mathcal{F}$. Let $0 \to f^*\mathcal{F} \to j^\bullet$ be an injective resolution of $f^*\mathcal{F}$, then we have the diagram

$$\begin{tikzcd}
0 \arrow[r] & f^*\mathcal{F} \arrow[r] \arrow[d, "id"'] & f^*\mathcal{I}^\bullet \arrow[d] \\
0 \arrow[r] & f^*\mathcal{F} \arrow[r] & \mathcal{J}^\bullet
\end{tikzcd}$$

By the definition of f^*, we induce morphisms

$$\Gamma(Y, \mathcal{I}^\bullet) \to \Gamma(X, f^*\mathcal{I}^\bullet) \to \Gamma(X, \mathcal{J}^\bullet)$$

which give rise to the desired map in cohomology. □

Remark 2.48. 1. Similarly, if $\mathcal{F}$ is a sheaf of X there is a map

$$H^{\bullet}(Y, f_*\mathcal{F}) \to H^{\bullet}(X, \mathcal{F})$$

obtained as the composition

$$H^{\bullet}(Y, f_*\mathcal{F}) \to H^{\bullet}(X, f^*f_*\mathcal{F}) \to H^{\bullet}(X, \mathcal{F})$$

where the second map comes from the adjunction map $f^*f_*\mathcal{F} \to \mathcal{F}$.

2. If $f : X \to Y$ is a morphism of schemes and Λ is a constant sheaf, since $f^*\Lambda = \Lambda$, we get a map

$$f^{\bullet} : H^{\bullet}(Y_{\text{ét}}, \Lambda) \to H^{\bullet}(X_{\text{ét}}, \Lambda)$$

in cohomology. In particular, if $\Lambda = \mathbb{Z}/l^n\mathbb{Z}$, we obtain a compatible families of maps

$$f^{\bullet} : H^{\bullet}(Y_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}) \to H^{\bullet}(X_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}).$$

They induce a map of $l-adic$ cohomology

$$f^{\bullet} : H^{\bullet}(Y_{\text{ét}}, \mathbb{Q}_l) \to H^{\bullet}(X_{\text{ét}}, \mathbb{Q}_l)$$

2.4 Frobenius morphism and Lefschetz formula in étale cohomology

In this section, I will discuss some more or less related issues revolving around the main idea relating (étale) cohomology via the Lefschetz trace formula, studying the zeta and L-function amounts to studying the representation of the Frobenius on morphism cohomology. Let's start by studying the Frobenius morphism in some generality.

2.4.1 The Frobeniuses on $\overline{X}$

Definition 2.49. A scheme X is said to be of *characteristic* p if $p\mathcal{O}_X = O$.

Of course, a non-trivial scheme cannot have two distinct prime characteristics. Remark that saying that X is of characteristic p is the same thing as saying that it may be viewed as a scheme over $\mathbb{F}_p$.

Definition 2.50. Let X be a scheme of characteristic p. We define the *(absolute) Frobenius endomorphism* of X

$$F_{X/\mathbb{F}_p} : X \longrightarrow X$$

as the morphism which is the identity on the underlying topological space $|X|$ and the p^{th}-power map on $\mathcal{O}_X$. (we also can drop the $\mathbb{F}_p$ from the notation of Frobenius morphism when this causes no ambiguity)

Remark 2.51. Let's keep the notations as the above definition.

1. The morphism defined in the definition is really a morphism of sheaves of rings since $p\mathcal{O}_X = 0$.
2. If X is a scheme over $\mathbb{F}_q$, where $q = p^n$, then it may also be viewed as a scheme over $\mathbb{F}_p$, so it has a Frobenius morphism $F_{X/\mathbb{F}_p}$ and $F_{X/\mathbb{F}_q}$ (or F_X^n) (which raises functions to the q^{th}-power) is a morphism of X as a scheme over $\mathbb{F}_q$.
3. The Frobenius morphism behaves functionally, in the sense that for each morphism $Y \to X$ (which automatically makes Y into a scheme over $\mathbb{F}_p$ provided X is one), the following diagram commutes:

$$\begin{tikzcd} Y \arrow[r, "F_Y"] \arrow[d] & X \arrow[d] \\ X \arrow[r, "F_X"'] & X \end{tikzcd}$$

In order to simplify the notation, let k denote the field $\mathbb{F}_q$ of q elements and fix an algebraic closure $k \hookrightarrow \overline{k}$ of k. If X is a scheme over k, we can extend the scalars to get a scheme $\overline{X}$ over $\overline{k}$,

$$\overline{X} := X \times_k \overline{k}.$$

It appears that on $\overline{X}$, there coexists four different Frobenius morphisms:

1. The *absolute Frobenius morphism*

$$F = F_{\overline{X}} : \overline{X} \longrightarrow \overline{X}$$

   which we discussed in the previous section.

2. The *relative Frobenius morphism*

$$F_r := F_X \times_k 1_{\overline{k}}$$

   obtained by base change of the Frobenius morphism of X (it is also sometimes called the $\overline{k}$*-linear Frobenius morphism* of X).

3. The *arithmetic Frobenius morphism*

$$F_a := 1_X \times_k F_{Spec\overline{k}}$$

obtained by base change the Frobenius morphism of $Spec\overline{k}$.

4. The *geometrical Frobenius morphism*

$$F_g := 1_X \times_k F^{-1}_{Spec\overline{k}}$$

which is the inverse of the arithmetical Frobenius morphism.

Example 2.6. *In the case $X = Spec(A)$ where $A = k[t_1, t_2, \cdots, t_n]$ is a finitely generated k -algebra, then*

$$\overline{X} = Spec(\overline{k} \otimes_k A) = Spec(\overline{k}[t_1, \cdots, t_n]).$$

Then on an element of $\overline{k}[t_1, \cdots, t_n]$, which is a polynomial in the t_i's with coefficient in $\overline{k}$:

1. *The relative Frobenius morphism F_r corresponds to raising the t_i's to the power of p.*

2. *The arithmetical Frobenius morphism F_a corresponds to raising the coefficients to the power of p.*

3. *The geometrical Frobenius morphism F_g corresponds to taking p^{th} roots of the coefficients.*

4. *The absolute Frobenius morphism F corresponds to raising both the t_i's and the coefficients to the power of p, which is the same thing as raising the element to the power of p.*

Remark 2.52.

1. By universal property of base change, we have $F = F_r \circ F_a = F_a \circ F_r$.

2. Since F is the identity on $|X|$, the continuous maps F_r, F_a induce on the étale site of $\overline{X}$ are inverse one to the other. This means that F_r is an homeomorphism of $\overline{X}_{\text{ét}}$ with inverse F_a, i.e. the relative Frobenius F_r and the geometrical Frobenius $F_g = F_a^{-1}$ induce the same continuous function

$$F : \overline{X}_{\text{ét}} \longrightarrow \overline{X}_{\text{ét}}$$

which we may call the *geometrical Frobenius correspondence* on $\overline{X}_{\text{ét}}$.

3. Since the continuous map $F : X_{\text{ét}} \to X_{\text{ét}}$ induced by the absolute Frobenius morphism $F : X \to X$ is identity, the relative Frobenius morphism and arithmetic Frobenius morphism induce the same map in cohomology.

2.4.2 The Lefschetz trace formula

One of the most important results in étale cohomology is the so called Lefschetz trace formula (or Lefschetz fixed point formula). With this formula applying to Frobenius morphism we can give a formula for the number of rational points of a variety. So, it is very important tool to prove the Weil conjectures.

Theorem 2.53. *Let X be a complete nonsingular variety over an algebraically closed field k, and let $f : X \to X$ be a morphism of schemes which a linear morphism $f^\bullet$: $H^\bullet(X_{ét}, \mathbb{Q}_l) \to H^\bullet(X_{ét}, \mathbb{Q}_l)$ of $\mathbb{Q}_l$-vector spaces, then*

$$(\Gamma_f \centerdot \Delta) = \sum_r (-1)^r Tr(f|H^r(X, \mathbb{Q}_l))$$

where Γ_f is the graph of f, and Δ is the diagonal in $X \times X$. Thus $(\Gamma_f \centerdot \Delta)$ is the number of fixed points of f counted with multiplicities.

Let consider a very basic example.

Example 2.7. *(Lefschetz trace formula for 0-dimensional scheme)*
Let X be a scheme of dimension 0. We know that $H^r(X_{ét}, \Lambda) = 0$ for every $r > 0$ and $H^0(X_{ét}, \Lambda) = \Lambda^{\pi_0(X)}$ where $\pi_0(X)$ is the set of its connected components. The morphism f induces the linear morphism $f^0 : H^0(X_{ét}, \Lambda) \to H^0(X_{ét}, \Lambda)$ where $\pi_0(f)$: $\pi_0(X) \to \pi_0(X)$ sends the connected component of a point x to the connected component of $f(x)$. So its trace is the number of connected components stabilized by f, i.e. the number of fixed points of $\pi_0(f) : \pi_0(X) \to \pi_0(X)$. In particular, the trace of f^0 : $H^0(X, \mathbb{Q}_l) \to H^0(X, \mathbb{Q}_l)$ is the number of connected components of X stabilized by f (since $trace(f \otimes g) = trace(f) \cdot trace(g)$). On the other hand, because X is of dimension 0, we have the connected components of X are just its points, so that Number of fixed points of f $L(f, X)$ is the number of fixed points of $\pi_0(f)$ and so

$$L(f, X) = Tr(f^0|H^0(X, \mathbb{Q}_l)).$$

We obtain the Lefschetz fixed point formula for 0-dimensional scheme (remark that in this case every fixed point of f has multiplicity 1).

Chapter 3

Zeta functions and L-functions according to Grothendieck

In this chapter, I would like to define the *zeta functions* and *L - functions* of any varieties, for instance, curves over finite fields. By using the Lefschetz fixed point formula, we are able to prove the rationality of the functions. In some examples, we will also discuss a little bit about the Riemann hypothesis.

3.1 Zeta functions and Weil conjectures

Suppose that X is a variety over a finite field $k = \mathbb{F}_q$. For every $m \geq 1$, let $N_m = |X(\mathbb{F}_{q^m})|$ be the number of points on X with coordinates in $\mathbb{F}_{q^m}$, i.e. the cardinality of

$$X(\mathbb{F}_{q^m}) := Hom_{Spec\,k}(Spec\,\mathbb{F}_{q^m}, X)$$

$$= \bigsqcup_{x \in X} Hom_{k-alg}(k(x), \mathbb{F}_{q^m}) = \bigsqcup_{deg(x)|m} Hom_{k-alg}(k(x), \mathbb{F}_{q^m}).$$

It is also equal to the number of points of $X \times_k \mathbb{F}_{q^m}$ of degree 1. We define the *(Hasse-Weil) zeta function* of X to be

$$Z(X,t) = exp(\sum_{m \geq 1} N_m \frac{t^m}{m}) := 1 + \sum_{m \geq 1} N_m \frac{t^m}{m} + \frac{1}{2!}(\sum_{m \geq 1} N_m \frac{t^m}{m})^2 + \cdots \in \mathbb{Q}[[t]].$$

Note that

$$\frac{d}{dt} log Z(X,t) = \sum_{m \geq 1} N_m t^{m-1}$$

Remark 3.1. If X is a scheme over $Spec\,\mathbb{Z}$, then for any prime number p, we are able to compute the zeta function $Z(X_p, t)$ of $X_p := X \times_{\mathbb{Z}} Spec\,\mathbb{F}_p$ as a scheme over $\mathbb{F}_p$ and then multiply them all together to obtain

$$\zeta(X,s) = \prod_p Z(X_p, p^{-s})$$

- the *global zeta function* of X.

3.1.1 The statements of the Weil conjectures

Suppose that X is a smooth, geometrically connected, projective variety of dimension n over a finite field $k = \mathbb{F}_q$.

Conjecture 3.2. (Rationality). $Z(X,t)$ is a rational function, i.e. it lies in $\mathbb{Q}(t)$.

Conjecture 3.3. (Functional equation). If $E = (\Delta \bullet \Delta)$ is the self-intersection of the diagonal $\Delta \hookrightarrow X \times X$, then

$$Z(X, \frac{1}{q^n t}) = \pm q^{nE/2} t^E Z(X,t).$$

Especially, if X is a curve of genus g then

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

Conjecture 3.4. (Analogue of the Riemann hypothesis). One can write

$$Z(X,t) = \frac{P_1(t) \cdot P_3(t) \cdots P_{2n-1}(t)}{P_0(t) \cdot P_2(t) \cdots P_{2n}(t)}$$

with $P_0(t) = 1-t$, $P_{2n}(t) = 1 - q^n t$ and for $1 \leq i \leq 2n-1$, we have $P_i(t) \in \mathbb{Z}[t] : P_i(t) = \prod_j (1 - \alpha_{ij} t)$ with α_{ij} algebraic integers satisfying $|\alpha_{ij}| = q^{i/2}$. Especially, if X is a curve of genus g then

$$Z(X,t) = \frac{P(t)}{(1-t)(1-qt)}$$

where $P(t)$ is a polynomial satisfying that

$$P(t) = \prod_{i=0}^{2g} (1 - \alpha_i t)$$

with $|\alpha_i| = q^{\frac{1}{2}}$.

Example 3.1. *Since,* $\mathbb{P}^n(\mathbb{F}_{q^r}) = q^{rn} + q^{r(n-1)} + \cdots + q^r + 1$, *the zeta function of the projective space is*

$$Z(\mathbb{P}^n_k, t) = exp(\sum_{r \geq 1} \frac{T^r}{r} \sum_{j=0}^{n} q^{rj}) = \frac{1}{(1-t)(1-qt)\cdots(1-q^n t)}.$$

3.1.2 Some properties of the *zeta* functions

Theorem 3.5. *The zeta function*

$$Z(X,t) = exp\big(\sum_{m\geq 1} N_m \frac{t^m}{m}\big) := 1 + \sum_{m\geq 1} N_m \frac{t^m}{m} + \frac{1}{2!}\big(\sum_{m\geq 1} N_m \frac{t^m}{m}\big)^2 + \cdots$$

converges for $|t| < q^{-dimX}$.

Proof. First, assume that $X = Spec\,\mathbb{F}_q[T_1, T_2, \cdots, T_r]$ to be the spectrum of a polynomial ring. By the definition of the zeta function, we have

$$logZ(X,t) = \sum_{m=1}^{\infty} \frac{N_m t^m}{m}.$$

Since $N_m = |X(\mathbb{F}_{q^m})|$ is the number of points in X with coordinates in $\mathbb{F}_{q^m}$, $N_m \leq q^{dimX}$. If $|t| < q^{-dimX}$, there exists $\epsilon > 0$ such that $|t| \leq q^{-dimX} q^{\epsilon}$

$$\Rightarrow |\frac{N_m t^m}{m}| \leq \frac{q^{\epsilon m}}{m} \leq \frac{1}{mq^{\epsilon m}}$$

$\Rightarrow Z(X,t)$ converges since $\sum\limits_{m=1}^{\infty}$. For the general case, we will reduce to the first case by the following lemma. □

Lemma 3.6. *Let X be the finite union of subschemes X_i. If the theorem holds for all X_i then so it does for X. Moreover, if $f : X \to Y$ is finite and the theorem is valid for Y then it is valid for X.*

Proof. Indeed, by the definition of $X(K)$ we have that $|X(K)| \leq \sum\limits_{finite} X_i(K)$. Since

$$logZ(X,t) = \sum_{m=1}^{\infty} \frac{N_m t^m}{m}$$

and $dim(X) \geq dim(X_i)$ for every i, we obtain the first statement. For the second, we remark that a finite morphism is a closed map of underlying topological spaces. □

Proposition 3.7. *For every variety X over $\mathbb{F}_q$, we have*

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

Proof. By definition,

$$log(1+t) = \sum_{m\geq 1} \frac{(-1)^{m+1} t^m}{m},$$

so

$$log(1 - t^{deg(x)}) = -\sum_{m\geq 1} \frac{t^{m\,deg(x)}}{m}.$$

Hence,

$$log\Big(\prod_{x\in X_{cl}} \big(1 - t^{deg(x)}\big)^{-1}\Big) = \sum_{x\in x_{cl}} \sum_{m\geq 1} \frac{t^{m\,deg(x)}}{m} = \sum_{m\geq 1} \sum_{deg(x)|m} \frac{deg(x)t^m}{m}.$$

To prove the above proposition, it suffices to prove the following lemma. □

Lemma 3.8. *If X is a variety over the finite field $\mathbb{F}_q$, then*

$$X(\mathbb{F}_{q^m}) = \sum_{e|r} e \cdot |\{x \in X_{cl} : deg(x) = e\}|.$$

Proof.

$$X(\mathbb{F}_{q^m}) = \bigsqcup_{deg(x)|m} Hom_{\mathbb{F}_q-alg}(\mathbb{F}_q(x), \mathbb{F}_{q^m}).$$

If $deg(x) = e|m$, then $G(\mathbb{F}_q(x), \mathbb{F}_q) \cong \mathbb{Z}/e\mathbb{Z}$ and $G(\mathbb{F}_{q^m}, \mathbb{F}_q)$ are Galois. So $\mathbb{F}_q(x) = \mathbb{F}_q(\alpha)$ where α is a root of an minimal irreducible polynomial in $\mathbb{F}_q[T]$ of degree e. Since the extensions are separable,

$$X(\mathbb{F}_{q^m}) = \sum_{deg(x)|m} deg(x) = \sum_{e|r} e \cdot |\{x \in X_{cl} : deg(x) = e\}|.$$

□

Corollary 3.9. *If X is a disjoint union (which may be infinite) of subschemes X_i, then*

$$Z(X,t) = \prod_i Z(X_i, t).$$

3.1.3 Rationality

Theorem 3.10. *For any complete nonsingular variety X of dimension d over $\mathbb{F}_q$, we have*

$$Z(X,t) = \frac{P_1(X,t)\cdots P_{2d-1}(X,t)}{P_0(X,t)\cdots P_{2d}(X,t)}$$

where $P_r(X,t) = det(1 - Ft|_{H^r(X_{ét},\mathbb{Q}_l)})$.
In particular, if X is an algebraic curve of genus g then

$$Z(X,t) = \frac{P_1(X,t)}{P_0(X,t)\cdot P_2(X,t)} = \frac{P_1(X,t)}{(1-t)(1-qt)}$$

where $P_1(t)$ is a polynomial of degree $2g$.

Proof. Firstly, we will prove that N_m is the number of fixed points of F^m on $\overline{X} = X_{\overline{k}}$. Indeed, for $m = 1$, $X(\mathbb{F}_q) = \{x \in X : deg(x) = 1\}$. Then for each $x \in X(\mathbb{F}_q)$, we can consider an affine neighbourhood of the form $Spec\,\mathbb{F}_q[X_1, \cdots, X_n]$. Assume $x = (X_1 - a_1, X_2 - a_2, \cdots, X_n - a_n)$ where $a_i \in \overline{\mathbb{F}_q}$. On the other hand, the Frobenius morphism at locally is $(X_1, \cdots, X_n) \mapsto (X_1^q, \cdots, X_n^q)$. So,

$$deg(x) = 1 \text{ iff } a_1^q = a_1, \cdots, a_n^q = a_n^q \text{ iff } x \in X^F.$$

Similarly for arbitrary m.

Hence, by the Lefschetz trace formula, we have

$$N_m = \sum_{r=0}^{2d} (-1)^r Tr(F^m|_{H^r(X,\mathbb{Q}_l)}).$$

Therefore,

$$Z(X,t) = exp\big(\sum_m N_m \frac{t^m}{m}\big) = exp\big(\sum_m \sum_{r=0}^{2d} (-1)^r Tr(F^m|_{H^r(X,\mathbb{Q}_l)}) \frac{t^m}{m}\big)$$

$$= \prod_{r=0}^{2d} \big(exp(\sum_m Tr(F^m|_{H^r(X,\mathbb{Q}_l)})) \frac{t^m}{m}\big)^{(-1)^r} = \prod_{r=0}^{2d} P_r(t)^{(-1)^{r+1}}$$

□

Corollary 3.11. *The power series $Z(X,t)$ is a rational function with coefficients in $\mathbb{Q}$, i.e. it lies in $\mathbb{Q}(t)$.*

This corollary is proved easily from the fact that if $k \subset K$ are fields, and $f(t) \in k[[t]]$ such that $f(t) \in K(t)$ then $f(t) \in k(t)$.

Remark 3.12. The corollary doesn't imply that the polynomial $P_r(X,t)$ must have rational coefficients. It says that, once any common factors have been removed, the numerator and denominator of the expression will be polynomials with coefficients in $\mathbb{Q}$, and will be independent of l.

Theorem 3.13. *Let*

$$Z(X,t) = \frac{P(t)}{Q(t)}$$

where $P(t), Q(t) \in \mathbb{Q}[t]$ are relatively prime. When P and Q are chosen to have constant terms 1, they have coefficients in $\mathbb{Z}$.

Proof. By proposition 3.1.7, we have

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

hence $Z(X,t) \in 1 + t\mathbb{Z}[[t]]$. So, to prove the theorem, it suffices to prove that if

$$f(t) = \frac{g(t)}{h(t)} \in 1 + t\mathbb{Z}[[t]] \text{ where } g(t), h(t) \in 1 + t\mathbb{Q}_l[t] \text{ relative prime,}$$

then g, h both have coefficients in $\mathbb{Z}_l$. For this, after possibly replacing $\mathbb{Q}_l$ with a finite extension field, we may assume $h(t)$ splits, say $h(t) = \prod(1 - c_i t)$. If $|c_i|_l > 1$ then $|c_i|_l < 1$, and the power series $f(c_i^{-1})$ converges. But then

$$f(t) \cdot h(t) = g(t) \Rightarrow f(c_i^{-1}) \cdot h(c_i^{-1}) = g(c_i^{-1}).$$

Since $h(c_i^{-1}) = 0$, $g(c_i^{-1}) = 0, \Rightarrow f$ and g are not relative prime (contradiction). Therefore, for all i: $|c_i|_l < 1$ i.e. $h(t) \in \mathbb{Z}_l[t]$. Similarly, since $f(t)^{-1} \in 1 + t \cdot \mathbb{Z}[[t]]$, we have $g(t) \in \mathbb{Z}_l[t]$. □

3.2 L-functions and Weil conjectures

3.2.1 Quotients by finite group actions

Definition 3.14. Let X be a scheme, G a finite group acting (on the right) on X by algebraic automorphism corresponding to $g \in G$ (i.e. G is endowed with a group homomorphism $G \to Aut(X)$). A *quotient of X by G* consists of a scheme $(Y, \mathcal{O}_Y)$ and a morphism (of schemes) $\pi : X \to Y$ (called *quotient morphism*), verifying the following universal property:

i. π is G -invariant, that is $\pi \circ \sigma_g = \pi$ for every $\sigma_g \in G$. (sometimes, we can denote σ_g by g).

ii. π is universal with this property: for every scheme Z , and every G -invariant morphism $f : X \to Z$, there exists a unique morphism $h : Y \to Z$ such that $h \circ \pi = f$.

The quotient scheme of X by the action of G is denoted by X/G.

Remark 3.15. 1. We can define the quotient space of a ringed topological space $(X, \mathcal{O}_X)$ by the same universal property.

2. In the case of category of ringed spaces, the quotient space always exists. If $(X, \mathcal{O}_X)$ is a ringed space, then the quotient space of X over a finite group G is the ringed space $(Y, \mathcal{O}_Y)$ consisting of $Y = X/G$ as the quotient set with the quotient topology, π the canonical projection and $\mathcal{O}_Y(V) = \mathcal{O}_X(\pi^{-1}(V))^G$ for every open subset V of Y.

3. In the category of schemes, the quotient scheme does not, in general, exist. Even if the quotient scheme exists, it does not always coincide with the quotient as a ringed topological space.

Proposition 3.16. *Let A be a ring, G be a finite group of automorphisms of A , and A^G the subring of elements of A which are invariant under G . Then $\pi : Spec\, A \to Spec\, A^G$ is the quotient scheme of $Spec\, A$ over G and this is also the quotient as a ringed topological space. Moreover, if U is an open subscheme of $Spec\, A$ that is stable under G then G acts on U and the quotient scheme U/G is isomorphic to $\pi(U)$.*

Proof. 1. Firstly, it is easy to see that the ring extension $A^G \hookrightarrow A$ is a integral extension. Indeed, for every $a \in A$, put $P(T) = \prod\limits_{\sigma \in G} (T - g(a))$ then $T(a) = 0$.
Moreover, the group G acts transitively on the set of prime ideals of A above a given prime ideal $\mathfrak{p} \in Spec\, A^G$. i.e. for every $\mathfrak{q}_1, \mathfrak{q}_2 \subset A$ primes such that $\mathfrak{q}_1 \cap A^G = \mathfrak{q}_2 \cap A^G$ then $\exists \sigma \in G$ such that $\mathfrak{q}_1 = \sigma \mathfrak{q}_2$. Indeed, let $x \in \mathfrak{q}_1$ then $\prod\limits_{\sigma \in G} \sigma x \in \mathfrak{q}_1 \cap A^G \Longrightarrow \prod \sigma \in G \sigma x \in \mathfrak{q}_2 \Longrightarrow \exists \sigma \in G : \sigma x \in \mathfrak{q}_2$, hence $\mathfrak{q}_1 \subseteq \bigcup\limits_{\sigma \in G} \sigma \mathfrak{q}_2$.
By the prime avoidance lemma, we have $\exists \sigma \in G : \mathfrak{q}_1 \subseteq \sigma \mathfrak{q}_2$; similarly, we have $\exists \sigma' \in G : \mathfrak{q}_2 \subseteq \sigma' \mathfrak{q}_2$, so $\mathfrak{q}_1 = \sigma \mathfrak{q}_2$.

2. Consider the following diagram:

$$\begin{tikzcd} Spec\, A \arrow[rr, "\pi"] \arrow[dr, "p"'] & & Spec\, A^G \arrow[dl, "f"] \\ & Y & \end{tikzcd}$$

where p is any G-invariant morphism of schemes. And $f = (f, f^\sharp)$ is defined as follows

$$f : Spec\, A \longrightarrow Y$$

such that $\mathfrak{p} \mapsto f(\mathfrak{p}) := p(\mathfrak{q})$ where $\mathfrak{q}$ is above $\mathfrak{p}$.
This map is well-defined and continuous. Let $U \subseteq Y$ closed then $p^{-1}(U) = V(I)$ for some ideal $I \subseteq A$. It suffices to show that $f^{-1}(U) = V(I \cap A^G)$. $f^{-1}(U) \subseteq V(I \cap A^G)$ is clear, and the converse $V(I \cap A^G) \subseteq f^{-1}(U)$ comes from the fact that the extension $A^G/I \cap A^G \hookrightarrow A/I$ is also integral.
Let any $U \subseteq Y$ open, then the map $f^\sharp(U) : \mathcal{O}_Y(U) \longrightarrow \mathcal{O}_{SpecA^G}(f^{-1}(U))$ where $p^{-1}(U) = SpecA - V(I)$ and $f^{-1}(U) = SepcA^G - V(I \cap A^G)$ is canonical induced

from the diagram:

$$\begin{tikzcd}
\mathcal{O}_Y(U) \arrow[rr, "\pi"] \arrow[dr, "p"'] & & \mathcal{O}_{SpecA}(SpecA - V(I)) \arrow[dl, "f"] \\
& \mathcal{O}_{SpecA^G}(SpecA^G - V(I \cap A^G)) &
\end{tikzcd}$$

(remark that $\pi^{-1}(SpecA^G - V(I \cap A^G) = SpecA - V(I))$.

Similarly for subscheme $U \subseteq SpecA$ which is stable under G, we have that U/G exists and is isomorphic to $\pi(U)$.

□

Remark 3.17. $\pi : Spec\,A \longrightarrow Spec\,A^G$ defined as above is an open map of underlying topological spaces.

Proof. It suffices to prove that $\forall a \in A$ then $\pi(D(a)) = \bigcup\limits_i^n D(b_i)$ where b_i are the coefficients of

$$\prod_{\sigma \in G}(T - \sigma a) = T^n + b_1 T^{n-1} + \cdots + b_n.$$

Firstly, we will prove that $\pi(D(a)) \subseteq \bigcup\limits_i^n D(b_i)$. Indeed, let $x \in \pi(D(a))$ then there exists $y \in D(a)$ such that $x = \pi(y)$. i.e. there exists $a \notin y$ such that $x = \pi(y) = y \cap A^G$. Assume that $x \notin \bigcup\limits_{i=1}^n D(b_i)$,then

$$x \notin D(b_i) \quad \forall i \Rightarrow b_i \in x \quad \forall i \Rightarrow b_i \in Y \quad \forall i.$$

On the other hand, $a^n + b_1 a^{n-1} + \cdots + b_n = 0$, so $a^n \in y$ or $a \in Y$ (!!!)

Secondly, let $x \in D(b_i)$ for some i, then $b_i \notin x$. By contradiction, assume that $x \notin \pi(D(a))$ then $\forall y$ s.t. $y \cap A^G = x$ i.e. $x = \pi(y)$ we have $y \notin D(a)$ or $a \in Y$. So, $a \in y \forall y$ above x, from the proof of the theorem, we know that G acts transitively on $\{y : y|x\}$; hence, $\sigma(a) \in Y\, \forall \sigma \in G$. This implies that $b_1 = \sum\limits_{\sigma \in G} \sigma a \in Y, \cdots, b_n = \prod\limits_{\sigma \in G} \sigma a \in Y$ (!!!).

This contradiction implies that π is an open map. □

By gluing schemes, we can easily see that:

Proposition 3.18. *Let G be a finite group acting on a scheme X. We suppose that every point $x \in X$ has an affine open neighborhood that is stable under G then the quotient scheme X/G exists.*

For example, if Y is quasi-projective scheme, then for each point $y \in Y$, the finite point $\{\sigma(y) : \sigma \in G\}$ lie in a finite number of affine open subschemes of Y. Hence, $\{\sigma(y) : \sigma \in G\}$ is contained in the intersection of a finite number of affine schemes, which is also affine, since Y is separable.

Corollary 3.19. *Let X be a quasi-projective scheme over a scheme S, and let G be a finite group acting on the S-scheme X. Then the quotient scheme X/G exits and G acts transitively on the fibres of $X \to X/G$. Moreover, the canonical morphism $X \to X/G$ is a finite morphism if S is locally noetherian.*

Proposition 3.20. *Let X be a quasi-projective scheme over a locally noetherian scheme S. Let G be a finite group acting on X. Then the quotient morphism $\pi : X \to Y$ commutes with flat base change.*

Proof. We can deduce to the affine case. Let A be a ring, B an A -algebra and C be a flat A -algebra. Suppose that G is a finite group acting on B (i.e. G is endowed with a homomorphism $G \to Aut_A(B)$) then each element in G induces an automorphisms $B \otimes_A C \to B \otimes_A C$:

$$\begin{tikzcd} B \arrow[r, "g"] \arrow[d] & B \arrow[d] \\ B \otimes_A C \arrow[r, "g\otimes Id_C"] & B \otimes_A C \end{tikzcd}$$

It suffices to prove that if $Spec\, B \to Spec\, A$ is quotient of scheme then $(B \otimes_A C)^G = C$. In general, we will prove that $(B \otimes_A C)^G = B^G \otimes_A C$. For every $\sigma \in G$, consider

$$\alpha_\sigma : B \longrightarrow B$$

defined by $\alpha_\sigma(b) = \sigma b - b$ for every $b \in B$. Since C is flat and the sequence

$$O \longrightarrow ker\alpha_g \longrightarrow B \longrightarrow Im\alpha_g \longrightarrow O$$

is exact,

$$O \longrightarrow ker\alpha_g \otimes_A C \longrightarrow B \otimes_A C \longrightarrow Im\alpha_g \otimes_A C \longrightarrow O$$

is also exact. This implies that $ker\, \alpha_\sigma \otimes_A C = ker(\alpha_\sigma \otimes Id_C)$. Since G is finite, we only need to prove that $\forall \sigma, \sigma' \in G$ then $ker(\alpha_\sigma \otimes Id_C) \bigcap ker(\alpha_{\sigma'} \otimes Id_C) = (ker\, \alpha_\sigma \cap ker\, \alpha_{\sigma'}) \otimes C$. Once again, it comes from the fact that if C is flat then the sequence

$$O \longrightarrow (ker\, \alpha_\sigma \cap ker\, \alpha_{\sigma'}) \otimes_A C \longrightarrow B \otimes_A C \longrightarrow Im(\alpha_\sigma, \alpha_{\sigma'}) \otimes_A C \longrightarrow O$$

is exact and $(\alpha_\sigma, \alpha_{\sigma'}) \otimes_A Id_C = (\alpha_\sigma \otimes Id_C, \alpha_{\sigma'} \otimes Id_C)$. $\square$

By [Har92], we will give a more precise description of the quotient scheme of a projective scheme over finite group. To begin with, observe that any action of a finite group on a projective variety $X \subset \mathbb{P}^n$ can be made projective, i.e. after embedding X into a suitable projective scheme $\mathbb{P}^N$, we may assume that G acts on $\mathbb{P}^N$ carrying X into itself. Now let $S(X)$ be the homogeneous coordinate ring of X in $\mathbb{P}^n$ and consider the subring $B = S(X)^G \subset S(X)$ invariant under the action of G. B is again a graded ring, though it may not be generated by its first graded piece B_1 (since B_1 may be zero or not homogeneous). Put

$$B^{(i)} = \bigoplus_{n=0}^{\infty} B_{ni}$$

where B_{ni} are the homogeneous ring. Since B is finitely generated, for some i, $S(Y) = B^{(i)}$ will be generated by its first graded piece. Thus we can write

$$S(Y) = K[Z_0, Z_1, \cdots, Z_m]/(F_1(Z), \cdots, F_l(Z))$$

where the F_j are homogeneous polynomials. Finally, we claim that $Y = V(F_1, \cdots, F_l) \subset \mathbb{P}^m$ is the quotient of X by G. Remark that m, l may be different from n, but $dim\, X = dim\,(X/G)$. For detail examples, see the examples of L - functions.

Definition 3.21. Let X be a quasi-projective scheme over a the finite field $\mathbb{F}_q$ and G a finite group acting on X. We know that the quotient scheme $Y = X/G$ exists.

1. Fix a point $x \in X$ then the subgroup $G_x = \{g\sigma \in G | \sigma x = x\}$ is called the *decomposition group of x*.

2. By definition, the decomposition group G_x acts canonically on $\mathcal{O}_{X,x}$. Hence, this induces a group homomorphism $G_x \to Gal(k(y)/k(x))$ where $y = f(x)$. The *inertia group* I_x of x is the kernel of this homomorphism. (remark that $[k(y) : k(x)]$ is finite since $A^G \hookrightarrow A$ is integral and finitely generated.)

Proposition 3.22. *[Liu02] Let X be a complete smooth variety over the finite field $\mathbb{F}_q$ and G a finite subgroup of automorphism of $\mathbb{F}_q$ -scheme X. Put $Y = X/G$ the quotient scheme of X over G, then for every $x \in X$ the sequence of groups*

$$1 \to I_x \to G_x \to Gal(k(x)/k(y)) \to 1$$

is exact where $y = \pi(x)$.

Proof. Since X is complete smooth variety, there exists an affine neighborhood of x which is fixed by G_x. So, we may choose $x \in SpecA \hookrightarrow Y$ affine open neighborhood of x. Assume first that $G = G_x, Y := X/G = Spec\, A^G = Spec\, A^{G_x}$. Since $k(x), k(y)$

are finite extension of $\mathbb{F}_q$, $k(x) = k(y)(\overline{\theta})$ with $\theta \in A$ (remark that for x closed point, $\mathcal{O}_{X,x}/m_x = A/x$).
Since $G_x = G$, we can consider $f(T) := \prod_{\sigma\in G} (T - \sigma(\overline{\theta})) \in k(y)[T]$. Let $g(T) \in k(y)[T]$ be the minimal polynomial of $\overline{\theta}$ then $g(T)|f(T)$.
Hence, for every $\delta \in Gal(k(x)/k(y))$, we have $f(\delta\,\overline{\theta}) = 0$. This means that there exists $\sigma \in G$ such that $\sigma(\overline{\theta}) = \delta(\overline{\theta})$, i.e. $\sigma = \delta$.
For the general case, we need to prove that the residue field of each closed point $u \in Spec\, A^{G_y} \mapsto x \in Spec\, A^G$ then their residue fields are equal, i.e. $A^{G_y}/u = A^G/x$. And so, we deduce to the first case. $\square$

3.2.2 L-functions

Definition 3.23. Let Y be a complete smooth curve (or more general, variety) over the finite field $k = \mathbb{F}_q$; let G be a finite group of k-automorphisms of Y, and $X = Y/G$. For any $y \in Y^0$ (i.e. y is a closed point of Y), Denote G_y, I_y to be the decomposition and inertia groups at y respectively, so there is an exact sequence:

$$1 \longrightarrow I_y \longrightarrow G_y \longrightarrow Gal(k(y)/k(x)) \longrightarrow 1.$$

Write $\overline{Y} := Y \otimes_k \overline{k}$ where $\overline{k}$ is the algebraic closure of k, Then G acts on $\overline{Y}$ and $\overline{Y}/G = \overline{X} = X\otimes_k\overline{k}$. Let Ω be a field containing $\mathbb{Q}_l$ where $(l, q) = 1$, and $\rho : G \to Aut_\Omega(V)$ be a finite-dimensional representation of G. Write f_y for the canonical generator of $Gal(k(y)/k(x))$, that is, $f_y(a) = a^{q^{deg(x)}}$; we may identify f_y with an element of G_y/I_y. Then the *Artin L-series* of ρ is the formal power series

$$L(Y, \rho, t) = \prod_{x\in X^0} \frac{1}{det(1 - t^{deg(x)}\rho(f_y)|V^{I_y})}$$

where, for each $x \in X^0$, a choice is made of a $y \in Y^0$ mapping to x.

Remark 3.24. The term corresponding to x in $L(Y, \rho, t)$ is independent of the choice of y. Indeed, let another y' above x then there exists σ in G such that $y' = \sigma y$, so $G_{y'} = \sigma G_y \sigma^{-1}$ and $I_{y'} = \sigma I_y \sigma^{-1}$. This implies that $G_{y'}/I_{y'} = \sigma(G_y/I_y)\sigma^{-1}$; moreover f_y is the canonical generator of $Gal(k(y)/k(x)) \cong G_y/I_y$ and $f_{y'}$ is the canonical generator of $Gal(k(y')/k(x)) \cong G_{y'}/I_{y'}$. Hence $f_{y'} = \sigma f_y \sigma^{-1}$, so $det(1 - t^{deg(x)}\rho(f_y)|V^{I_y}) = det(1 - t^{deg(x)}\rho(f_{y'})|V^{I_{y'}})$.

In the next proposition, we will give some basic properties of L-functions

Proposition 3.25. *Let $\rho : G \to Aut_\Omega(V), \rho_1 : G \to Aut_\Omega(V)$ and $\rho_2 : G \to Aut_\Omega(V)$ be finite-dimensional representations of G then:*

1. $L(Y, \rho_1 \oplus \rho_2, t) = L(Y, \rho_1, t)L(Y, \rho_2, t)$;
2. $L(Y, \rho, t) = Z(X, t)$ *the zeta-function of* X *if* ρ *is trivial representation;*
3. $L(Y, \rho, t) = Z(Y, t)$ *the zeta-function of* Y *if* ρ *is regular representation;*
4. $Z(Y, t) = Z(X, t)\big(\prod L(Y, \rho, t)^{dim\rho}\big)$ *where the product is over the non-trivial, irreducible representations* ρ *of* G.

Proof. (1), (2) are clear from the definition of $L(Y, \rho, t)$. For (3), let

$$\rho : G \to GL_{\Omega}(V)$$

be the regular representation where $V = \Omega\, G$. Then ρ induces $\rho : G_y/I_y \to GL_{\Omega}(V^{I_y})$. Firstly, we will prove that

$$(dim\, V^{I_y}).|I_y| = dim\, V = |G| = |\pi^{-1}(x)| \cdot |G_y|.$$

Indeed, by the transitivity of the actions of G on the set $\pi^{-1}(x)$, we have the canonical bijective morphism of sets $G/G_y \to \pi^{-1}(x)$ defined by $g \cdot G_y \mapsto g \cdot y \Rightarrow |G| = |\pi^{-1}(x)| \cdot |G_y|$. To prove $(dim\, V^{I_y}).|I_y| = dim\, V = |G|$, we can prove that V^{I_y} is a Ω - vector space generated by $|G|/|I_y|$ vectors. For example, if $G = \mathbb{Z}/8\mathbb{Z}$ and $I_y = 0, 2, 4, 6$ then V^{I_y} is generated by $\{1 \cdot 0 + 1 \cdot 2 + 1 \cdot 4 + 1 \cdot 6, 1 \cdot 1 + 1 \cdot 3 + 1 \cdot 5 + 1 \cdot 7\}$.
Put m to be the order of $Gal(k(y)/k(x))$, since $G_y/I_y \cong Gal(k(y)/k(x)) = \langle f_y \rangle$ then we can choose a suitable base of V^{I_y} as follows: $\{g_1, f_y \cdot g_1, \cdots, f_y^{m-1} \cdot g_1, g_2, \cdots\}$ so that $g_i \notin \{g_j, f_y \cdot g_j, \cdots, f_y^{m-1} \cdot g_j\} \quad \forall\, i \neq j$ and the matrix of ρ has the form

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}.$$

where A is the following matrix of order m

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

On the other hand, for each $x \in X^0, det(1 - t^{deg\, x} \cdot A) = (1 - t^{deg\, y})$. Hence, we have $L(Y, \rho, t) = Z(Y, t)$.

(4) comes from the decomposition of the regular representation to irreducible representations. $\square$

Theorem 3.26. *If Y is a curve and ρ is irreducible, non-trivial; then*

$$L(Y,\rho,t) = det(1 - Ft|H^1(\overline{Y}, V^*)^G) := det(1 - Ft|(H^1(\overline{Y}, \mathbb{Q}_l) \otimes V^*)^G)$$

where $F : \overline{Y} \to \overline{Y}$ is the relative Frobenius morphism obtained by base change of the Frobenius morphism of X , $F : X \to X$. and (V^*, ρ^*) is the contragredient representation, that is, $\rho^*(g) = \rho(g^{-1})^t$ as matrices. In particular, $L(Y,\rho,t)$ is a polynomial in t that divides the numerator of $Z(Y,t)$.

In order to prove this theorem, we need some lemmas:

Lemma 3.27. *We keep the notations and hypotheses of the previous definition, let*

$$\rho^{av}(f_y) = \frac{1}{|f_y|} \sum_{g \in G_y \mapsto f_y} \rho(g),$$

then

$$L(Y,\rho,t) = \prod_{x \in X^0} \frac{1}{det(1 - t^{deg(x)} \rho^{av}(f_y)|V)}.$$

Proof. It suffices to show that

$$det(1 - t^{deg(x)} \rho^{av}(f_y)|V) = det(1 - t^{deg(x)} \rho(f_y)|V^{I_y})$$

Indeed, we have

$$\rho^{av}(f_y) = \frac{1}{|I_y|} \sum_{g \in G_y \mapsto f_y} \rho(g) = \frac{1}{|I_y|} \sum_{g \in I_y} \rho(g)\rho(f_y) = \frac{1}{|I_y|} \rho(f_y) \sum_{g \in I_y} \rho(g)$$

Let

$$P = \frac{1}{|I_y|} \sum_{g \in I_y} \rho(g)$$

then P is the projection $V \to V^{I_y}$ and

$$\rho(g)P = P\rho(g) = \rho^{av}(f_y).$$

So the matrix of $\rho^{av}(f_y)$ is

$$\begin{pmatrix} A & B \\ O & O \end{pmatrix}$$

where A is the matrix of $\rho(f_y)|V^{I_y}$. Hence

$$det(1 - t^{deg(x)}\rho^{av}(f_y)|V) = det(1 - t^{deg(x)}\rho(f_y)|V^{I_y}).$$

$\square$

Let α be an endomorphism of a finite-dimensional vector space V, then

$$log(det(1 - \alpha t|V)^{-1}) = \sum_{n\geq} Tr(\alpha^n|V)\frac{t^n}{n}.$$

Indeed, if V is vector space of dimension 1 and α acts as multiplication by a, then the formula is simply the identity

$$log(1 - at) = -\sum \frac{a^n t^n}{n}.$$

In the general case, we choose a suitable basis of V such that the matrix of α is triangular, then the general formula is a sum of $dim(V)$ such above identities.
Therefore, we have that

$$logL(Y, \rho, t) = \sum_{x\in X^0}\sum_{n\geq 1} Tr(\rho(f_y^n)|V)\frac{t^{ndeg(x)}}{n} = \sum_{m\geq 1}\sum_{deg(x)|m} Tr(\rho^{av}(f_y^{\frac{m}{deg(x)}})|V)deg(x).$$

Let χ be the character of ρ, and for any $x \in X(\mathbb{F}_{q^n})$ (that is, point of $X \otimes \mathbb{F}_{q^n}$ of degree 1), write

$$\chi(x) = \frac{1}{|I_y|}\sum_{g\in G_y \mapsto f_y} \chi(g)$$

where $y \in Y \otimes \mathbb{F}_{q^n}$ maps to x. Then it is easy to see that $\chi(x) = Tr(\rho^{av}(f_y)|V)$. We will show that

$$L(Y, \rho, t) = exp(\sum_{n\geq 1} \frac{\nu_n(Y, \chi)t^n}{n})$$

where $\nu_n(Y, \chi) = \sum_{x\in X(\mathbb{F}_{q^n})} \chi(x)$.

We also know that $\forall x' \in X(\mathbb{F}_{q^n})$ mapping to x then $f_y^{m/deg(x)} = f_{y'}$ and $I_y = I_{y'}, G_y = G_{y'}$. So, it suffices to prove the corresponding between $X(\mathbb{F}_{q^n})$ and $\{x \in X^0 : degx|n\}$.

Lemma 3.28. *Let $X \otimes \mathbb{F}_{q^n}$ be the fibre product of X and $Spec\,\mathbb{F}_{q^n}$ over $Spec\,\mathbb{F}_q$*

$$\begin{tikzcd}
X \otimes \mathbb{F}_{q^n} \arrow[r] \arrow[d, "\alpha"'] & Spec\mathbb{F}_{q^n} \arrow[d, "\beta"] \\
X \arrow[r] & Spec\mathbb{F}_q
\end{tikzcd}$$

Then

1. *For all $x \in X^0$ such that $deg(x)|n$ then $\alpha^{-1}(x) \subset X(\mathbb{F}_{q^n})$,*

2. *For all $x' \in X(\mathbb{F}_{q^n})$ then $\alpha(x') \in X^0$ and $deg\,\alpha(x')|n$,*

3. *For all $x \in X^0$ such that $deg(x)|n$ then $|\alpha^{-1}(x)| = deg(x)$*

Proof. Before proving this lemma, I remark that α is closed map since β is universally closed and we can reduce to the affine case $X = SpecA$

1. Let x be in X^0, and x' be an inverse image of x in $X \otimes \mathbb{F}_{q^n}$ then x' is a closed point. So

$$k(x') = \big((A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})_{x'} \diagup x'(A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})_{x'}\big) \cong A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \diagup x' \cong [A/x \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}] \diagup x'.$$

   Moreover $A/x = \mathbb{F}_{q^m}$ with m a divisor of n. Since every finite extension of a finite field is Galois extension. Therefore, $A/x = \mathbb{F}_q/(f(T))$ where $deg(f) = m$

$$\Rightarrow k(x') \cong \big(\mathbb{F}_{q^n}[T]/(f(T))\big) \diagup g$$

   where g is a irreducible factor of f in $\mathbb{F}_{q^n}[T]$. On the other hand, $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$, hence g is a linear factor of $f \Rightarrow k(x') \cong \big(\mathbb{F}_{q^n}[T]/(f(T))\big) \diagup g \cong \mathbb{F}_{q^n}$, this means that $deg(x') = 1$ or $x' \in X(\mathbb{F}_{q^n})$.

2. Let $x' \in X(\mathbb{F}_{q^n})$ be such that $deg(x') = 1$, i.e.

$$A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}/x' \cong \mathbb{F}_{q^n}.$$

   Assume that $A/x = \mathbb{F}_{q^m}$ then

$$A/x = \mathbb{F}_q[T]/(f(T)) \text{ with } deg(f) = m$$

$$\Rightarrow (A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}) \diagup x' \cong (A/x \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}) \diagup x' \cong \mathbb{F}_{q^n}.$$

$$\Rightarrow \big[\mathbb{F}_{q^n}[T]/(f(T))\big] \diagup (g(T)) \cong \mathbb{F}_{q^n}$$

$$\Rightarrow \big[\mathbb{F}_{q^n}[T]/(g(T)) \cong \mathbb{F}_{q^n}$$

   where $g(T)$ is the irreducible factor of f corresponding to the maximal ideal x'. This implies that g is a linear factor of f in $\mathbb{F}_{q^n}[T]$ for every x' above x. So, every irreducible factor of f is linear in $\mathbb{F}_{q^n}[T]$. In the other words, $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n} \Longrightarrow m|n$.

3. We have $\alpha^{-1}(x)$ is finite set of closed points. Moreover,

$$A/x \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \cong \mathbb{F}_{q^n}[T]/(f(T)) \cong \mathbb{F}_{q^n} \oplus \mathbb{F}_{q^n} \oplus \cdots \oplus \mathbb{F}_{q^n} (deg(x) \text{ times}).$$

So, $|\{\text{close points of } A/x \otimes \mathbb{F}_{q^n}\}| = deg(x)$.
Therefore, it suffices to prove that the cardinality of $\alpha^{-1}(x)$ = the cardinality of $\{$close points of $A/x \otimes \mathbb{F}_{q^n}\}$. We will prove a general result as following: Let A and B be two k - algebras (k is any field), denote $P_1 \subset A, P_2 \subset B$ prime ideals, $T = A \otimes B$, $\Gamma = \{Q \in SpecT : Q \cap A = P_1, Q \cap B = P_2\}, k(P_1) = A_{P_1}/P_1A_{P_1}, k(P_2) = B_{P_2}/P_2B_{P_2}, T' = k(P_1) \otimes_k k(P_2)$. Then $\sharp\Gamma = \sharp Spec(T')$.
Indeed, denote

$$\overline{A} = A/P_1\overline{B} = B/P_2, \overline{T} = \overline{A} \otimes_k \overline{B}$$

and

$$\overline{\Gamma} = \{J \in Spec(\overline{T}) : J \cap \overline{A} = (O), J \cap \overline{B} = (O)\}.$$

Since $A \twoheadrightarrow A/P_1$ and $B \twoheadrightarrow B/P_2$ then we have the surjective map $T \twoheadrightarrow \overline{T}$ with kernel $P_1 \otimes B + A \otimes P_2 = P_1T + P_2T$. Hence, we have the canonical injective map:

$$f^\sharp Spec(\overline{T}) \hookrightarrow SpecT \text{ and } f^\sharp(\overline{\Gamma}) = \Gamma.$$

Moreover, we also have that

$$A/P_1 \longrightarrow A_{P_1}/P_1A_{P_1} \text{ and } B/P_2 \longrightarrow B/P_2/P_2B_{P_2}$$

induces the canonical map $\overline{T} \longrightarrow T'$. Since $T' \cong \overline{T}_S$ where

$$S = \{\overline{r_1} \otimes \overline{r}_2 | r_1 \in \overline{A} - \{0\}, r_2 \in \overline{B} - \{0\}\}.$$

$$\Longrightarrow g^\sharp : Spec(T') \longrightarrow Spec\overline{T} \text{ is injective and } \Im(g^\sharp) = \overline{\Gamma}.$$

$$\Longrightarrow f^\sharp_o g^\sharp \text{ is injective and } Im(f^\sharp_o g^\sharp) = \overline{\Gamma}.$$

Return to the our case, I remark that we only need the morphism $f^\sharp$ and moreover the mapping $A \otimes \mathbb{F}_{q^n} \longrightarrow (A/x) \otimes \mathbb{F}_{q^n}$ is surjective (hence integral). Hence, $|\alpha^{-1}(x)| = |\{\text{close points of } A/x \otimes \mathbb{F}_{q^n}\}|$.

□

From these lemmas, we are able to express the L - functions in the terms of the fixed points formula. Let's study the following lemma

Lemma 3.29.
$$\nu_n(Y,\chi) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})L(\sigma F^n)$$
where $L(\sigma F^n)$ is the number of fixed points of σF^n on $\overline{Y}$.

Proof. Let
$$L_x(\sigma F) := |\{\overline{y}\in\overline{Y} : \overline{y}\mapsto x \text{ and } \sigma F(\overline{y}) = \overline{y}\}|.$$

Since every points $y\mapsto x$ have the same degree, we have

$$\begin{aligned} L_x(\sigma F) &= |\{\overline{y}\in\overline{Y} : \overline{y}\mapsto \pi^{-1}(x) \text{ and } \sigma F(\overline{y}) = \overline{y}\}| \\ &= |\pi^{-1}(x)|\cdot|\{\overline{y}\in\overline{Y} : \overline{y}\mapsto y\mapsto x \text{ and } \sigma F(\overline{y}) = \overline{y}\}| \quad (\text{for some } y\mapsto x)\ . \\ &= |\pi^{-1}(x)|\cdot deg(y) \end{aligned}$$

Indeed, since k is separable, there are $deg(y)$ distinct points $\overline{y}$ mapping to y for each $y\mapsto x$. So, we only need to prove that, for each point $y\mapsto x$, if $|\{\overline{y}\in\overline{Y} : \overline{y}\mapsto y \text{ and } \sigma F(\overline{y}) = \overline{y}\}|\neq 0$, i.e. $\exists\overline{y}\mapsto y : \sigma F(\overline{y})\mapsto\overline{y}$ then all of points $\overline{y}\mapsto y$ are in $\{\overline{y}\in\overline{Y} : \overline{y}\mapsto y \text{ and } \sigma F(\overline{y}) = \overline{y}\}$. On the other hand, we may assume that $F(\overline{y})\neq\overline{y}$ (if not, then $\overline{y} = y$, and there is nothing to prove). Put $u = \sigma^{-1}(\overline{y})$ then $u\mapsto y$. Since σ and F commutes, $\sigma F(u) = u$. Similarly, for $v = \sigma^{-1}(u)$, then $\sigma F(v) = v\cdots$ Remark that $\sigma y = y$, hence all of points $\overline{y}\mapsto$ are $\{\overline{y},\sigma^{-1}(\overline{y}),\cdots\}$. Therefore,

$$|\{\overline{y}\in\overline{Y} : \overline{y}\mapsto y\mapsto x \text{ and } \sigma F(\overline{y}) = \overline{y}\}| = deg(y).$$

Moreover, to have $|\{\overline{y}\in\overline{Y} : \overline{y}\mapsto y\mapsto x \text{ and } \sigma F(\overline{y}) = \overline{y}\}|$ different from 0 is equivalent to have $\sigma\cdot f_y\in I_y$. So,

$$L_x(\sigma F) = \begin{cases} |\pi^{-1}(x)|\cdot|deg(y)| & \text{if } \sigma\cdot f_y\in I_y \\ 0 & \text{otherwise} \end{cases}$$

From the proof of above proposition, we have

$$|G| = |\pi^{-1}(x)|\cdot|G_y| = |\pi^{-1}(x)|\cdot|I_y|\cdot deg(y)/deg(x).$$

This implies that
$$\chi(x) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})L_x(\sigma F).$$

Hence,
$$\nu_n(Y,\chi) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})L(\sigma F^n).$$

□

Proof of the theorem By the Lefschetz fixed point formula for σF^n, we have

$$\begin{aligned} \nu_n(Y,\chi) &= \frac{1}{|G|}\sum_{\sigma\in G} Tr(\rho(\sigma^{-1})|_V)\sum_r(-1)^r Tr(\sigma F^n|_{H^r(\mathbb{Q}_l)}) \\ &= \sum_r(-1)^r Tr\big[\big(\frac{1}{|G|}\sum_{\sigma\in G}\rho^*(\sigma)\otimes\sigma\big)\circ(1\otimes F^n)|_{V^*\otimes_{\mathbb{Q}_l}H^r(\mathbb{Q}_l)}\big] \end{aligned}.$$

Moreover $\frac{1}{|G|}\sum_\sigma \rho^*(\sigma)\otimes\sigma$ is a projection $V^*\otimes H^r \to (V^*\otimes H^r)^G$. But ρ is irreducible and $H^0(X,\mathbb{Q}_l)\cong H^2(X,\mathbb{Q}_l)\cong\mathbb{Q}_l$ then $(V^*)^G = 0$. Hence

$$L(Y,\rho,t) = det(1-Ft|H^1(\overline{Y},V^*)^G) = det(1-Ft|(H^1(\overline{Y},\mathbb{Q}_l)\otimes V^*)^G).$$

Remark 3.30. Similarly to the properties of zeta functions, we can prove some properties of L-functions easily. For example, the L-function $L(X,\rho,t)$ converges absolutely when $|t| < q^{-dimX}$.

3.3 Some examples

3.3.1 Zeta functions of Grassmannians

Definition 3.31. The Grassmannian $G(d,n)$: Let V be a vector space of dimension $n \geq 2$ over the field $k = \mathbb{F}_q$. Let $1 \leq d \leq n$ be any integer. Then the Grassmannian $G(d,n)$ is defined to be the set of all d-dimensional subspaces of V, i.e.

$$G(d,n) = \{W : W \subset V \text{ as subspace of dimension d}\}.$$

Theorem 3.32. *The Grassmannian $G(d,n)$ is a smooth projective variety of $\dim G(d,n) = d(n-d)$ which can be considered as a variety over any finite field $\mathbb{F}_q$.*

In order to compute the zeta function of the Grassmannian $G(d,n)$, we need to compute the number of points of $G(d,n)$ over any finite extension of $\mathbb{F}_q$. For this, we consider the action of $Gal(\overline{k}/k)$ on $G(d,n)(\overline{k}) \subset \mathbb{P}^N(\overline{k})$. For each $\sigma\in\Gamma = Gal(\overline{k}/k)$ and $(a_0 : a_1 : \cdots : a_N)\in\mathbb{P}^N(\overline{k})$, we define

$$\sigma(a_0 : a_1 : \cdots : a_N) = (\sigma(a_0) : \sigma(a_1) : \cdots : \sigma(a_N)).$$

It is easy to see that this action is well defined and $\sigma_1\sigma_2(a_0 : \cdots : a_N) = \sigma_1(\sigma_2(a_0 : \cdots : a_N))$.
Moreover one can prove the following lemma:

Lemma 3.33. *The Galois group* $\Gamma = Gal(\overline{k}/k)$ *acts on* $\mathbb{P}^N(\overline{k})$ *and the fixed points are precisely the points in* $\mathbb{P}^N(k)$*, i.e.*

$$\{u = (a_0 : \cdots : a_N) \in \mathbb{P}^N(\overline{k}) | \sigma(u) = u \quad \forall \sigma \in \Gamma\} = \mathbb{P}^N(k).$$

Hence, we can consider the action of Galois group $\Gamma = Gal(\overline{k}/k)$ on $G(d,n)$ and we have

$$|G(d,n)(k)| = |[G(d,n)(\overline{k})]^{\Gamma}|$$

which is the number of d - dimensional subspaces of $\overline{k}^n$ which are Γ invariant.
Without loss of generality, suppose that the n-dimensional vector space V is $\overline{k}^n$ and $G(d,n)$ is the collection of all d dimensional subspaces of $\overline{k}^n$ and Γ acts on it as follows: for $U \in G(d,n)$ and $\sigma \in \Gamma$, the action of σ induces

$$\sigma(U) = \{\sigma(x_1, x_2, \cdots, x_n) = (\sigma(x_1), \cdots, \sigma(x)n)) : (x_1, \cdots, x_n) \in U\}.$$

It is easy to see that if U has a basis $\{w_1, w_2, \cdots, w_d\}$ such that $w_i \in k^n$ then U is Γ invariant, i.e. $\sigma(U) = U \quad \forall \sigma \in \Gamma$. In fact the converse is also hold. And this gives a way to calculate $|[G(d,n)(\overline{k})]^{\Gamma}|$.

Lemma 3.34. $U \in G(d,n)$ *is* Γ *invariant if and only if* U *has a basis* $\{w_1, w_2, \cdots, w_d\}$ *with each* $w_i \in k^n$*.*

By the lemma, we have that $G(d,n)(\mathbb{F}_q)$ is the number of vector spaces with bases $\{v_1, v_2, \cdots, v_d\}$ such that $v_i \in k^n$. Let J denote the collection of all bases $\{v_1, v_2, \cdots, v_d\}$ such that $v_i \in k^n$, then

$$G(d,n)(\mathbb{F}_q) = \frac{|J|}{|GL(d)(\mathbb{F}_q)|}.$$

For calculating J, we choose the base as follows: $v_1 \in \mathbb{F}_q^n \setminus \{0\}$, then $v_2 \in \mathbb{F}_q^n \setminus \mathbb{F}_q v_1$ and $v_3 \in \mathbb{F}_q^n \setminus \mathbb{F}_q v_1 + \mathbb{F}_q v_2 \cdots$ So there are

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{d-1})$$

such vector bases $\{v_1, v_2, \cdots, v_d\}$. Similarly, the number of invertible matrices of $GL(d)$ is also the number of linearly independent vector spaces in $\mathbb{F}_q^d$. Hence

$$G(d,n)(\mathbb{F}_l) = \frac{|J|}{|GL(d)(\mathbb{F}_l)|} = \frac{(l^n - 1)(l^{n-1} - 1) \cdots (l^{n-d+1} - 1)}{(l^d - 1)(l^{d-1} - 1) \cdots (l - 1)}$$

where $l = q^r$.
This is the usual Gaussian Binomial coefficient

$$\begin{pmatrix} n \\ d \end{pmatrix}_l := \frac{(l^n-1)(l^{n-1}-1)\cdots(l^{n-d+1}-1)}{(l^d-1)(l^{d-1}-1)\cdots(l-1)}.$$

By [And98], we know that it can be interpreted as a polynomial in l. More precisely,

$$\begin{pmatrix} n \\ d \end{pmatrix}_l = \sum_{i=0}^{d(n-d)} b_i \cdot l^i.$$

For example

$$\begin{pmatrix} 4 \\ 2 \end{pmatrix}_l = 1 + l + 2l^2 + l^3 + l^4.$$

Hence

$$Z(G(d,n),t) = \frac{1}{(1-t)^{b_0}(1-qt)^{b_1}\cdots(1-q^{d(n-d)})^{b_{d(n-d)}}}.$$

3.3.2 L - functions with group of order 2

Weighted Projective Spaces: Probably the most basic examples of quotients of projective varieties by finite groups are quotients of projective space by the action of abelian groups acting diagonally, *weighted projective spaces*. To have a finite abelian subgroup of the group of automorphisms of schemes, we can find the group of order 2. For example, consider the group $G = \{1, \sigma\}$ where $\sigma : \mathbb{P}^1 \to \mathbb{P}^1$ is the morphism defined by

$$\sigma(z_0 : z_1) = (z_0 : -z_1).$$

Remark that if $f(z_0, z_1)$ is a homogeneous polynomial then $f(z_0, z_1)$ is a product of linear factors in $\overline{k}$ then $\sigma(u)$ is the product of σ of the linear factors. It is easy to see that σ is really a morphism of schemes $\mathbb{P}^1(k)$ over any field k. The subring of the homogeneous coordinate ring of $\mathbb{P}^1$ invariant under the action of G, say X is thus generated by the monomials z_0, z_1^2. Put $w_0 = z_0^2, w_1 = z_1^2$ with no relation among them. So, we have that $X = Projk[w_0, w_1] \cong \mathbb{P}^1(k)$.
Consider the L-function of the regular action of G:

$$\rho : G \to GL(\mathbb{Q}_l\, G).$$

It is easy to see that ρ is decomposed to $\rho_1 = id$ and ρ_2 such that ρ_1, ρ_2 are representation of dimension 1 and $\rho_2(\sigma) = -1$. We have:

$$Z(\mathbb{P}^1, t) = L(\mathbb{P}^1, \rho, t) = Z(X, t)L(\mathbb{P}^1, \rho_2, t).$$

Since

$$Z(\mathbb{P}^1, t) = \frac{1}{(1-t)(1-qt)}, Z(X, t) = \frac{1}{(1-t)(1-qt)}$$

and $L(\mathbb{P}^1, \rho_2, t)$ is a polynomial, hence we should have $L(\mathbb{P}^1, \rho_2, t) = 1$. Since $|G_y| \leq 2$ then $[k(y) : k(x)] \leq 2$. If $[k(y) : k(x)] = 1$ and $|G_2| = 2$ then $\chi(\mathbb{P}^1, x) = 0$. If $[k(y) : k(x)] = 1$ and $|G_2| = 1$ then $\chi(\mathbb{P}^1, x) = 1$ and if $[k(y) : k(x)] = 2$ and $|G_2| = 2$ then $\chi(\mathbb{P}^1, x) = -1$. So, we should have the number of points x in X such that $deg(y) = deg(x)$ is equal to the number of points x in X such that $deg(y) = 2deg(x)$.

Klein Quartic: Consider the curve $C := X^3Y + Y^3Z + Z^3X$ of genus 3 over $k = \mathbb{F}_2$. We know that

$$Z(C) = \frac{1 + 5t^3 + 8t^6}{(1-t)(1-2t)}.$$

Consider group $G = \{1, \sigma\}$ where $\sigma(X, Y, Z) = (-X, -Y, -Z)$ then G acts on C. Moreover the coordinate ring of C is

$$S(C) = k[X, Y, Z]/(X^3Y + Y^3Z + Z^3X).$$

Hence $S(X)^G$ is generated by $\{X^2, Y^2, Z^2, XY, XZ, YZ\}$.
Therefore, C/G is generated by

$$\begin{aligned}&(T_1T_4 + T_2T_5 + T_3T_6, T_1T_2 - T_4^2, T_1T_3 - T_6^2, T_2T_3 - T_5^2, T_1T_5 - T_4T_6, T_2T_6 - T4T_5,\\ &T_3T_4 - T_5T_6, T_1T_5 - T_4T_6, T_2T_6 - T_4T_5, T_3T_4 - T_5T_6)\end{aligned}$$

- a projective curve in $\mathbb{P}^5$.
Hence its zeta functions is of the form

$$Z(C/G, t) = \frac{f(t)}{(1-t)(1-2t)}.$$

Consider the regular representation $\rho : G \to GL(\mathbb{Q}_l\, G)$ then

$$Z(C, t) = Z(C/G, t)\, L(C, \rho_2, t).$$

Since $1 + 5t^3 + 8t^6$ is irreducible. Then C/G is a curve of genus 3, $L(C, \rho_2, t) = 1$, $Z(C/G, t) = Z(C, t)$. By taking the derivative of the same zeta function, we have that $N_i(C) = N_i(C/G)$.

3.4 Application of zeta and L-functions

For an application of Weil conjectures, we want to use the Weil conjectures to describe more explicit about the zeta functions of an elliptic curve. Precisely, we would like to under stand $P(t)$ in

$$Z(C,t) = \frac{P(t)}{(1-t)(1-qt)}$$

where $C \subset \mathbb{P}^2(k)$ is an elliptic curve over $k = \mathbb{F}_q$, finite field.
Recall that elliptic curve is curve of genus 1, hence, by the Riemann hypothesis, we have that

$$P(t) = 1 + at + bt^2.$$

By the functional equation, we have that

$$(qt^2) \cdot P(\frac{1}{qt}) = P(t).$$

Hence, $b = q$, $P(t) = 1 + at + qt^2$. Since

$$N_1 = \frac{d}{dt} Z(C,t)|_{t=0}$$

then

$$a_1 + q + 1 = N_1,$$

so $a_1 = N_1 - q - 1$.

Theorem 3.35. *If $C \subset \mathbb{P}^2(\mathbb{F}_q)$ is an elliptic curve then*

$$Z(C,t) = \frac{1 + (N_1 - q - 1)t + qt}{(1-t)(1-qt)} = 1 + \frac{N_1 t}{(1-t)(1-qt)}$$

where $N_1 = C(\mathbb{F}_q)$ the number of points of X with coordinates in $\mathbb{F}_q$.

Let us consider a special case when $q = p$ a prime number. By using the Riemann hypothesis we have that

Theorem 3.36. *If $C \subset \mathbb{P}^2(\mathbb{F}_p)$ is an elliptic curve then*

$$N_1 = 2a + p + 1$$

with $|a| \leq 2\sqrt{p}$.

Proof. Put $\lambda = N_1 - p - 1$, we know that $P(t) = 1 + \lambda\, t + pt^2 = (1 - \alpha t)(1 - \beta t)$ where $|\alpha|^2 = |\beta|^2 = p$. This implies that

$$\begin{cases} \alpha \cdot \beta = p \\ \alpha + \beta = \lambda \\ |\alpha|^2 = |\beta|^2 = p \end{cases}$$

Let $\alpha = a + bi$, $\beta = c + di$ then

$$\begin{cases} a + c = \lambda \\ b + d = 0 \\ ac - bd = p \\ ad + bc = 0 \\ a^2 + b^2 = c^2 + d^2 = p \end{cases}$$

Since p is prime then:

$$\Rightarrow \begin{cases} a = c = \lambda/2 \\ b = -d \neq 0 \\ a^2 + b^2 = p \end{cases}$$

The theorem is proved completely. □

Remark 3.37. In the small case of this theorem - elliptic curve, then it is easy to see that $P(t) = 1 + aT + pt^2$ has two roots of absolute values $p^{1/2}$, i.e. for every root α, β of $P(t)$ then $|\alpha|^2 = |\beta|^2 = p$, if and only if $|a| = |N_1 - p - 1| \leq 2\sqrt{p}$. This is one way to prove the Riemann hypothesis on curve. In fact, one can prove that if $p \neq 2, 3$, then there is an elliptic curve over $\mathbb{F}_p$ with $N_1 = p + 1 + 2a$ if and only if $a = 0$ (see [Xin07])

References

[AM69] Michael Francis Atiyah and Ian Grant Macdonald, *Introduction to commutative algebra*, vol. 2, Addison-Wesley Reading, 1969.

[And98] George E Andrews, *The theory of partitions*, vol. 2, Cambridge University Press, 1998.

[FK88] Eberhard Freitag and Reinhardt Kiehl, *Étale cohomology and the weil conjecture*, Springer-Verlag Berlin-Heidelberg-New York, 1988.

[GD60] Alexander Grothendieck and Jean Dieudonné, *Eléments de géométrie algébrique*, Publications Mathématiques de l'IHÉS **4** (1960), no. 1, 5–214.

[Har92] Joe Harris, *Algebraic geometry: a first course*, vol. 133, Springer Verlag, 1992.

[Har97] Robin Hartshorne, *Algebraic geometry*, Springer, 1997.

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford university press, 2002.

[Mac68] Ian Grant Macdonald, *Algebraic geometry: Introduction to schemes*, WA Benjamin New York, 1968.

[Mil80] James S Milne, *Étale cohomology*, Princeton University Press, 1980.

[Mor93] Carlos Moreno, *Algebraic curves over finite fields*, vol. 97, Cambridge University Press, 1993.

[NS99] Jürgen Neukirch and Norbert Schappacher, *Algebraic number theory*, vol. 9, Springer Berlin, 1999.

[Ser63] Jean-Pierre Serre, *Zeta and l-functions*, Proc. Conf. Purdue Univ, 1963, pp. 82–92.

[Ste94] Serguei A Stepanov, *Arithmetic of algebraic curves*, Consultants Bureau, 1994.

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc **55** (1949), no. 5, 497–508.

[Xin07] Chaoping Xing, *Zeta-functions of curves of genus 2 over finite fields*, Journal of Algebra **308** (2007), no. 2, 734–741.