Forms of Smooth Projective Varieties and Their Zeta Functions

Yu Zhao

Master of Science

Department of Mathematics and Statistics

McGill University

Montreal,Quebec

2006-08-15

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Master of Science

ACKNOWLEDGEMENTS

First, I would like to thank my wife who always has the patience to listen to my mathematical stories although her background is far away from mathematics.

I thank my supervisor Prof. Eyal Goren who gave me the opportunity to do this project. He gave me many good ideas on my thesis. I thank him for his patience, kindness and great help. I am also thankful for the financial support from Prof. Eyal Goren and the Department, otherwise it would have been impossible for me to finish my thesis.

Last but not least, I thank to all my professors not only at McGill University, who have taught me mathematics especially number theory and algebraic geometry.

ABSTRACT

In this thesis, I mainly study the forms of a smooth projective variety over a finite field k and the attached Hasse-Weil zeta functions. I also study the forms of a scheme.

The study begins with understanding the relationship between étale cohomology and the Hasse-Weil zeta function of a smooth projective variety over k. In order to classify forms of a quasi-projective variety V over a perfect field K, I study non-abelian cohomology and Galois descent to give a proof of the bijection between the equivalence classes of K'/K-forms of V and $H^1(\mathrm{Gal}(K'/K), \mathrm{Aut}_{K'}(V))$, where K'/K is some Galois extension. I also present explicitly forms of elliptic curves and their corresponding Hasse-Weil zeta functions.

The second part of my thesis is focused on forms of a scheme, especially in the affine case. This is a generalization of forms of a variety. I define an étale form of a scheme and generalize Milne's definition of the first Čech cohomology of a non-abelian sheaf to any (not necessarily abelian) presheaf. I prove there exists an injective map in the affine case from the set of equivalence classes of affine étale forms into the first Čech cohomology of a contravariant functor. I prove that the definition of an étale form of a scheme is compatible with the definition of a form of a variety over a perfect field. I also prove that the first Galois cohomology can be canonically identified with the first Čech cohomology when the base is $\mathrm{Spec}\, k$ for some perfect field k.

ABRÉGÉ

Dans cette thèse, j'étudie les formes d'une variété projective douce au-dessus d'un corps fini k et les fonctions zeta d'Hasse-Weil ci-jointes. J'étudie également les formes d'un schéma.

L'étude commence par l'arrangement le rapport entre la cohomologie étale et la fonction zeta d'Hasse-Weil d'une variété projective douce au-dessus k. Afin de classifier des formes d'une variété quasi-projective au-dessus d'un corps parfait, j'étudie la cohomologie galoisienne non abélienne et la descente galoisienne pour fournir des preuves du bijection entre K'/K-formes de V et $H^1(\mathrm{Gal}(K'/K), \mathrm{Aut}_{K'}(V))$, où K'/K est galoisien. Je présente également explicitement des formes de courbes elliptiques et de leurs fonctions zeta d'Hasse-Weil correspondantes.

La deuxième partie de ma thèse est principalement concentrée sur des formes d'un arrangement, particulièrement dans la caisse affine. C'est une généralisation des formes d'une variété. Je définis une forme étale d'un schéma et trouve une preuve dans le cas d'affinage de l'existence d'une carte injective de l'ensemble de classes d'équivalence de pour formes affines étales dans la première cohomologie de Čech d'un functor contravariant.

TABLE OF CONTENTS

CHAPTER 1
Introduction

Given a smooth projective variety X of dimension d defined over a finite field $k = \mathbb{F}_q$, one can attach to it its Hasse-Weil zeta function $Z(X/\mathbb{F}_q, T)$:

$$Z(X/\mathbb{F}_q, T) = \exp \sum_{r=1}^{\infty} \#X(\mathbb{F}_{q^r}) \frac{T^r}{r},$$

where $\#X(\mathbb{F}_{q^r})$ is the number of $\mathbb{F}_{q^r}$-points of X.

Using étale cohomology, one can prove the Weil's conjectures and the following formula:

$$Z(X, T) = \prod_{i=0}^{2d} P_i(X, T)^{(-1)^{i+1}},$$

where $P_i(X, T) = \det(1 - (\mathrm{Fr}^i)^* T \big| H^i(\overline{X}, \mathbb{Q}_\ell))(i = 0, 1, \ldots, 2d)$ and Fr is the geometric or relative Frobenius map. Chapter 1 is devoted to this purpose.

Suppose $\mathcal{X}$ is another smooth projective variety defined over k and let K/k be a Galois extension, then $\mathcal{X}$ is a K/k-form of X if $\mathcal{X}$ is isomorphic to X when both are considered defined over K, i.e. $\mathcal{X} \times_k K \cong X \times_k K$.

Since Galois descent (or coefficient extension in the language of categories) is satisfied, not only can we classify all forms of a smooth projective variety over k using non-abelian cohomology, but also there is a close relation between the Hasse-Weil zeta function of a smooth projective variety and the zeta function of a form of it.

Chapter 3 and 4 are dedicated to this purpose. Chapter 5 provides concrete examples of varieties in order to illustrate such classification and relations.

Besides giving an overview of the definition of the zeta function of a scheme over $\operatorname{Spec}\mathbb{Z}$ based on Serre's paper [22], the last chapter mainly focuses on forms of a scheme, whose definition is based on [7]. A form of a scheme is a generalization of that of a variety over a field. Let X be a scheme. I define an étale form of an X-scheme Y and prove that when both X and Y are affine, there exists an injective map from the set of equivalence classes of affine étale forms of Y into the first Čech cohomology $\check{H}^1(X_{\acute{e}t}, \operatorname{Aut}(Y \times_X -))$. Since $\operatorname{Aut}(Y \times_X -)$ is a contravariant functor from $X_{\acute{e}t}$ to the category of groups $\mathbb{G}$ but not an abelian sheaf over $X_{\acute{e}t}$ in general, I define directly the Čech cohomology $\check{H}^1(X_{\acute{e}t}, \mathscr{F})$ for any contravariant functor $\mathscr{F}$ from $X_{\acute{e}t}$ to $\mathbb{G}$. I also show that if $X = \operatorname{Spec} k$ where k is some perfect field, the definition of an étale form of an X-scheme Y coincides with that of a form of a variety over k, and moreover, $\check{H}^1((\operatorname{Spec} k)_{\acute{e}t}, \operatorname{Aut}(Y \times_k -))$ can be canonically identified with $H^1(\operatorname{Gal}(\overline{k}/k), \operatorname{Aut}(Y \times_k \overline{k}))$ as pointed sets.

CHAPTER 2
Zeta functions of varieties over finite fields

2.1 Zeta Functions

Let $k = \mathbb{F}_q$ be a finite field with q elements. Let X be a projective variety defined over k. For each positive integer r, X can also be considered as defined over the finite field $k_r = \mathbb{F}_{q^r}$ with q^r elements. Let N_r be the number of k_r-points of X. The Hasse-Weil zeta function of X is defined as a formal power series

$$Z(X,T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right). \tag{2.1}$$

When X/k is a smooth projective variety, we have the following famous Weil's conjectures proven by Dwork and Deligne:

Theorem 2.1.1 (Weil's Conjectures)**.** *Let X be a smooth projective variety of dimension d defined over $\mathbb{F}_q$. Then*

1. *$Z(X,T)$ can be written as*

$$Z(X,T) = \frac{P_1(T)P_3(T)\dots P_{2d-1}(T)}{P_0(T)P_2(T)\dots P_{2d}(T)}\ , \tag{2.2}$$

where $P_0(T) = 1 - T$, $P_{2d}(T) = 1 - q^d T$ and for $1 \le s \le 2d-1$, $P_s(T) \in \mathbb{Z}[T]$ and

$$P_s(T) = \prod_{i=1}^{\beta_s}(1 - \alpha_{s,i}T)$$

for some non-negative integer β_s, where each $\alpha_{s,i}$ is an algebraic integer with $|\alpha_{s,i}| = q^{\frac{s}{2}}$ for any choice of complex absolute value.

2. *$Z(X,T)$ satisfies the following functional equation:*

$$Z\left(X, \frac{1}{q^d T}\right) = \pm q^{\frac{\chi d}{2}} T^{\chi} Z(X,T),$$

where χ is the self-intersection number of the diagonal Δ of $X \times_{\overline{k}} X$.

The proof can be found in [8]. In the next section, we give a brief introduction to étale cohomology and the expression of zeta functions in terms of étale cohomology.

2.1.1 Étale Cohomology

For general references to étale cohomology, see for example [19] and [26]. Here we only recall some basic definitions.

Definition 2.1.2. *Let X be a scheme. Define $ét/X$ to be the category of X-schemes such that the morphism $C \to X$ is étale for any object C in $ét/X$. Such a scheme is called an étale X-scheme.*

By properties of étale morphisms ([1], p.116), any morphism between objects in $ét/X$

is also étale.

Definition 2.1.3. *The étale site $X_{ét}$ consists of the category ét/X and coverings each of which is some set $\{Y_i \xrightarrow{\phi_i} Y \mid i \in I\}$ of morphisms in ét/X, where I is some index set, such that $Y = \bigcup_{i \in I} \phi_i(Y_i)$.*

It is easy to verify that $X_{ét}$ is actually a site in the sense of Grothendieck. For the definition of Grothendieck's site, see the Appendix or [26], p.24.

The category of abelian sheaves on $X_{ét}$ is denoted by $\mathcal{S}_{X_{ét}}$; an object in $\mathcal{S}_{X_{ét}}$ is also called an abelian étale sheaf on X.

For each abelian sheaf F on X, and for each étale X-scheme Y, general theorems ([26], Chapter 1) guarantee the existence of cohomology group $H^q(Y, F)$ with values in F for any integer $q \geq 0$. $H^q(Y, F)$ is also denoted by $H^q(X_{ét}; Y, F)$. When Y is a final object in $X_{ét}$, i.e. $Y \cong X$, Y is omitted and the notation $H^q(X_{ét}, F)$ is adopted.

2.1.2 ℓ-adic Cohomology

For any abelian group G endowed with the discrete topology, we also use G to denote the constant sheaf on $X_{ét}$ with respect to G.

Let ℓ be a prime number. Using the constant sheaves $\mathbb{Z}/\ell^n\mathbb{Z}$ on $X_{ét}$, where $n \geq 1$ is

an integer, we define ([18], p.114-116)

$$H^r(X_{\acute{e}t}, \mathbb{Z}_\ell) := \varprojlim_n H^r(X_{\acute{e}t}, \mathbb{Z}/\ell^n\mathbb{Z}),$$

and

$$H^r(X_{\acute{e}t}, \mathbb{Q}_\ell) := H^r(X_{\acute{e}t}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Let X be a scheme of finite type over an algebraically closed field k, then $H^r(X_{\acute{e}t}, \mathbb{Q}_\ell)$ has the following well-known properties ([11], p.453):

- $H^r(X_{\acute{e}t}, \mathbb{Q}_\ell)$ can be considered as a vector space over $\mathbb{Q}_\ell$.
- $H^r(X_{\acute{e}t}, \mathbb{Q}_\ell) = 0$ when $r > 2 \dim X$.
- $H^r(X_{\acute{e}t}, \mathbb{Q}_\ell)$ is a finite dimensional vector space over $\mathbb{Q}_\ell$ if X is proper over k.
- $H^r(X_{\acute{e}t}, \mathbb{Q}_\ell)$ is a contravariant functor in $X_{\acute{e}t}$.
- There is the cup product structure,

  $$H^r(X_{\acute{e}t}, \mathbb{Q}_\ell) \times H^s(X_{\acute{e}t}, \mathbb{Q}_\ell) \longrightarrow H^{r+s}(X_{\acute{e}t}, \mathbb{Q}_\ell),$$

  defined for all r and s.
- (Poincaré duality) Suppose X is smooth and proper over k with dimension n, then $H^{2n}(X_{\acute{e}t}, \mathbb{Q}_\ell)$ is a 1-dimensional vector space over $\mathbb{Q}_\ell$ and the cup product,

  $$H^i(X_{\acute{e}t}, \mathbb{Q}_\ell) \times H^{2n-i}(X_{\acute{e}t}, \mathbb{Q}_\ell) \longrightarrow H^{2n}(X_{\acute{e}t}, \mathbb{Q}_\ell),$$

  is a perfect paring for each $0 \leq i \leq 2n$.
- (Lefschetz trace formula) Let k be an algebraically closed field, X be a complete smooth variety over k, and $\phi : X \to X$ be a regular map with isolated fixed

points. Denote the number of fixed points of ϕ with multiplicity by $\#\phi$, then

$$\#\phi = \sum_r (-1)^r \mathrm{Tr}(\phi | H^r(X_{\acute{e}t}, \mathbb{Q}_\ell)). \tag{2.3}$$

- (Comparison Theorem) Suppose X is a smooth scheme over the field of complex numbers $\mathbb{C}$ and A is a finite abelian group, then $H^r(X_{\acute{e}t}, A)$ can be canonically identified by the singular cohomology of $X/\mathbb{C}$, i.e. there is a natural isomorphism:

  $$H^r(X/\mathbb{C}, A) \cong H^r(X_{\acute{e}t}, A),$$

  where the X on the left hand side is regarded as a complex manifold. In particular, let $A = \mathbb{Z}/\ell^n\mathbb{Z}$, then

  $$H^r(X/\mathbb{C}, \mathbb{Z}/\ell^n\mathbb{Z}) \cong H^r(X_{\acute{e}t}, \mathbb{Z}/\ell^n\mathbb{Z}).$$

  So

  $$H^r(X/\mathbb{C}, \mathbb{Z}_\ell) = \varprojlim_n H^r(X/\mathbb{C}, \mathbb{Z}/\ell^n\mathbb{Z}) \cong \varprojlim_n H^r(X_{\acute{e}t}, \mathbb{Z}/\ell^n\mathbb{Z}) = H^r(X_{\acute{e}t}, \mathbb{Z}_\ell),$$

  and hence

  $$H^r(X/\mathbb{C}, \mathbb{Q}_\ell) \cong H^r(X_{\acute{e}t}, \mathbb{Q}_\ell).$$

2.1.3 Frobenius Maps

In this section, I mainly follow notes by Gabriel Chênevert ([4]).

Let k be the finite field $\mathbb{F}_q$, where $q = p^n$ for some prime number p and some natural number $n \geq 1$. Let X be a scheme over k. Denote by $\overline{X}$ the scheme $X \times_k \overline{k}$,

where $\overline{k}$ is the algebraic closure of k.

Definition 2.1.4. *The absolute Frobenius map* $\mathrm{Fr}_X : X \to X$ *is defined in the following way:*

- *As an endomorphism of the topological space* X, Fr_X *is the identity map.*
- *For any open set* $U \subset X$, *we have the ring homomorphism:*

$$\mathrm{Fr}_{U,X}^{\#} : \mathcal{O}_X(U) \to \mathcal{O}_X(U),\ \alpha \mapsto \alpha^q,\ \forall \alpha \in \mathcal{O}_X(U).$$

Definition 2.1.5. *The relative Frobenius morphism* Fr_r *is defined on* $\overline{X}$ *as follows:*

$$\mathrm{Fr}_r : \overline{X} \to \overline{X}, \quad \mathrm{Fr}_r := \mathrm{Fr}_X \times_k 1_{\mathrm{Spec}\,\overline{k}}\ .$$

Definition 2.1.6. *The arithmetical Frobenius morphism* Fr_a *is defined as follows:*

$$\mathrm{Fr}_a := 1_X \times_k \mathrm{Fr}_{\mathrm{Spec}\,\overline{k}}\ .$$

Definition 2.1.7. *The geometrical Frobenius morphism* Fr_g *is defined as follows:*

$$Fr_g := 1_X \times_k \mathrm{Fr}_{\mathrm{Spec}\,\overline{k}}^{-1}\ ,$$

which is the inverse of the arithmetical Frobenius morphism.

Example 2.1.8. *Let $X = \operatorname{Spec} A$ where A is the polynomial ring $\mathbb{F}_p[x]$ for some finite field $\mathbb{F}_p$, where p is a prime number. Then*

$$\overline{X} = \operatorname{Spec}(\overline{\mathbb{F}}_p \otimes_{\mathbb{F}_p} A) = \operatorname{Spec} \overline{\mathbb{F}}_p[x].$$

We have:

- Fr_r *corresponds to the map* $\overline{\mathbb{F}}_p[x] \to \overline{\mathbb{F}}_p[x]$, $x \mapsto x^p$.
- Fr_a *corresponds to the map* $\overline{\mathbb{F}}_p[x] \to \overline{\mathbb{F}}_p[x]$, $x \mapsto x$, $a \mapsto a^p, \forall a \in \overline{\mathbb{F}}_p$.
- Fr_g *corresponds to the map* $\overline{\mathbb{F}}_p[x] \to \overline{\mathbb{F}}_p[x]$, $x \mapsto x$, $a \mapsto a^{\frac{1}{p}}, \forall a \in \overline{\mathbb{F}}_p$.
- Fr_X *corresponds to the map* $\overline{\mathbb{F}}_p[x] \to \overline{\mathbb{F}}_p[x]$, $x \mapsto x^p$, $a \mapsto a^p, \forall a \in \overline{\mathbb{F}}_p$.

Proposition 2.1.9. *Let X be a scheme of characteristic p. For any étale sheaf F on $\overline{X} = X \times_k \overline{k}$, Fr_r and $\mathrm{Fr}_g = \mathrm{Fr}_a^{-1}$ induce the same map on cohomology groups:*

$$\mathrm{Fr}_g^* = \mathrm{Fr}_r^* : \ H^*(\overline{X}_{\acute{e}t}, \mathrm{Fr}_r^* F) \to H^*(\overline{X}_{\acute{e}t}, F).$$

Since $\mathrm{Fr}_r^* F = F$ if F is a constant sheaf, we see that Fr_r induces a linear transformation of the $\mathbb{Q}_\ell$-vector space $H^r(\overline{X}, \mathbb{Q}_\ell)$ for any $r \geq 0$.

2.1.4 Weil's Conjectures

Using the Lefschetz trace formula, one can prove the following result ([19], p.288):

Theorem 2.1.10. *For any smooth projective variety $X/\mathbb{F}_q$ of dimension d,*

$$Z(X,T) = \prod_{i=0}^{2d} P_i(X,T)^{(-1)^{i+1}},$$

where $P_i(X,T) = \det(1 - (\mathrm{Fr}_r^i)^* T \big| H^i(\overline{X}, \mathbb{Q}_\ell))(i = 0, 1, \ldots, 2d)$. Here $\mathrm{Fr}_r^* \big| H^i(\overline{X}, \mathbb{Q}_\ell)$ is the matrix representation of relative Frobenius morphism as a linear transformation on $H^i(\overline{X}, \mathbb{Q}_\ell)$ which is regarded as a $\mathbb{Q}_\ell$-vector space.

When X is a scheme of finite type over $\mathbb{Z}$, we have the fact that a point $x \in X$ is closed in X if and only if the residue field $k(x)$ is finite. Let $\widetilde{X}$ be the set of closed points in X and $N(x)$ the order of $k(x)$ for any $x \in \widetilde{X}$. The number of closed points whose orders of residue fields are the same is finite. One can define the zeta function of scheme X to be the formal product ([22]):

$$\zeta(X,s) = \prod_{x \in \widetilde{X}} \frac{1}{1 - N(x)^{-s}}. \tag{2.4}$$

This definition coincides with the definition of Hasse-Weil zeta function when the scheme X is of finite type and defined over $\mathbb{F}_q$. In fact in this case, for any $x \in \widetilde{X}$, the residue field $k(x)$ is a finite extension of $\mathbb{F}_q$ and we have

$$N(x) = q^{[k(x):\mathbb{F}_q]}.$$

So

$$\zeta(X,s) = \prod_{x \in \widetilde{X}} \frac{1}{1 - (q^{-s})^{[k(x):\mathbb{F}_q]}}.$$

Let $T = q^{-s}$, then

$$\zeta(X,s) = \prod_{x \in \widetilde{X}} \frac{1}{1 - T^{[k(x):\mathbb{F}_q]}}. \tag{2.5}$$

Denote the rightside of (2.5) by $\mathcal{Z}(X,T)$, then

$$\mathcal{Z}(X,T) = \prod_{n=1}^{\infty} \prod_{\substack{x \in \widetilde{X} \\ [k(x):\mathbb{F}_q]=n}} \frac{1}{1-T^n} = \prod_{n=1}^{\infty} \left(\frac{1}{1-T^n}\right)^{\alpha_n},$$

where α_n is the number of closed points whose residue fields are finite field extensions of $\mathbb{F}_q$ with degree n. So

$$\begin{aligned}
\log \mathcal{Z}(X,T) &= \sum_{n=1}^{\infty} \alpha_n \log\left(\frac{1}{1-T^n}\right) = \sum_{n=1}^{\infty} \left(\alpha_n \sum_{i=1}^{\infty} \frac{T^{ni}}{i}\right) \\
&= \sum_{n=1}^{\infty} \left(n\alpha_n \sum_{i=1}^{\infty} \frac{T^{ni}}{ni}\right) \\
&= \sum_{n,i=1}^{\infty} n\alpha_n \frac{T^{ni}}{ni} \\
&= \sum_{j=1}^{\infty} \left(\left(\sum_{d|j} d\alpha_d\right)\frac{T^j}{j}\right). \qquad (2.6)
\end{aligned}$$

On the other hand, let k_j be the finite extension of $\mathbb{F}_q$ with degree j. Denote the set of points of X in k_j by $X(k_j)$. Each point can be identified with a pair (x,f) for some $x \in \widetilde{X}$ and some injective $\mathbb{F}_q$-homomorphism of $k(x)$ into k_j which implies $k(x)$ must be a subfield of k_j and hence $[k(x):\mathbb{F}_q]|j$. Also for each $x \in \widetilde{X}$, when $k(x)$ is a subfield of k_j, $k(x)/\mathbb{F}_q$ is a finite Galois extension and hence the number of distinct injective homomorphisms of $k(x)$ into k_j is just $[k(x):\mathbb{F}_q]$. So

$$\#X(k_j) = \sum_{d|j} d\alpha_d\,. \qquad (2.7)$$

Hence we can replace $\sum_{d|j} d\alpha_d$ in (2.6) with $\#X(k_j)$ and we obtain

$$\log \mathcal{Z}(X,T) = \sum_{j=1}^{\infty} \#X(k_j)\frac{T^j}{j},$$

so

$$\mathcal{Z}(X,T) = Z(X,T).$$

Example 2.1.11. *Let X be the projective n-dimensional space $\mathbb{P}^n$ defined over a finite field $k = \mathbb{F}_q$. X is clearly a smooth projective variety and for any positive integer r,*

$$\#\mathbb{P}^n(\mathbb{F}_{q^r}) = 1 + q^r + q^{2r} + \ldots + q^{nr}.$$

Hence

$$\begin{aligned} Z(\mathbb{P}^n, T) &= \exp(\sum_{r=1}^{\infty}\sum_{j=0}^{n}(q^j)^r\frac{T^r}{r}) \\ &= \frac{1}{1-T}\cdot\frac{1}{1-qT}\cdot\cdots\cdot\frac{1}{1-q^nT}, \end{aligned}$$

which is clearly a rational function.

On the other hand, when $0 \le i \le 2n$ ([19], p.245)*,*

$$\dim_{\mathbb{Q}_\ell} H^i(\mathbb{P}^n, \mathbb{Q}_\ell) = \begin{cases} 0 & i \text{ odd,} \\ 1 & i \text{ even,} \end{cases}$$

so when i is even, Fr_r^i acts on $H^i(\mathbb{P}^n, \mathbb{Q}_\ell)$ as a multiplication by $q^{i/2}$ ([20], p.3)*. Hence when $0 \le i \le 2n$,*

$$\det(1 - (\mathrm{Fr}_r^i)^* T \big| H^i(\mathbb{P}^n, \mathbb{Q}_\ell)) = \begin{cases} 0 & i \text{ odd} \\ 1 - q^{i/2}T & i \text{ even} \end{cases},$$

and we obtain the same zeta function for $\mathbb{P}^n$, as predicted by Theorem 2.1.10*.*

Example 2.1.12. *In the case of an elliptic curve $E/\mathbb{F}_q$* ([12], p.248)*, $H^1(\overline{E}_{\acute{e}t}, \mathbb{Q}_\ell)$ can be identified with $V_\ell^*(E)$ which is the dual of $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, where $T_\ell(E)$ is*

the Tate module of $E/\mathbb{F}_q$ and ℓ is any prime number not equal to p. For any positive integer m prime to p, the m-torsion subgroup of E, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and therefore, $V_\ell(E)$ is a $\mathbb{Q}_\ell$-vector space of dimension 2, and so the dimension of $V_\ell^*(E)$ over $\mathbb{Q}_\ell$ is also 2. The zeta function of E/k has the following expression:

$$Z(E,T) = \frac{\det(1 - \mathrm{Fr}_r^* T \big| V_\ell^*(E))}{(1-T)(1-qT)} = \frac{1 - \mathrm{Tr}(\mathrm{Fr}_r^*)T + qT^2}{(1-T)(1-qT)}, \tag{2.8}$$

where $\mathrm{Tr}(\mathrm{Fr}_r^*) = \mathrm{Tr}(\mathrm{Fr}_r^* \big| V_\ell^*(E))$. Using the Lefschetz trace formula (2.3), since E has dimension 1, we have

$$\begin{aligned} \#E(\mathbb{F}_q) &= \sum_{i=0}^{2} (-1)^i \mathrm{Tr}(\mathrm{Fr}_r^* \big| H^i(\overline{E}_{\acute{e}t}, \mathbb{Q}_\ell)) \\ &= \mathrm{Tr}(\mathrm{Fr}_r^* \big| H^0(\overline{E}_{\acute{e}t}, \mathbb{Q}_\ell)) - \mathrm{Tr}(\mathrm{Fr}_r^* \big| H^1(\overline{E}_{\acute{e}t}, \mathbb{Q}_\ell)) + \mathrm{Tr}(\mathrm{Fr}_r^* \big| H^2(\overline{E}_{\acute{e}t}, \mathbb{Q}_\ell)) \\ &= 1 - \mathrm{Tr}(\mathrm{Fr}_r^*) + q. \end{aligned}$$

So

$$\mathrm{Tr}(\mathrm{Fr}_r^*) = 1 + q - \#E(\mathbb{F}_q).$$

Now let E be a supersingular elliptic curve (for the definition, see [12], p.248-251*) defined over $\mathbb{F}_p$ for some prime number p (e.g., $y^2 = x^3 + 1$ defined over $\mathbb{F}_5$, and $y^2 + y = x^3$ defined over $\mathbb{F}_2$), then $\#E(\mathbb{F}_p) = p + 1$. So in this case $\mathrm{Tr}(\mathrm{Fr}_r^*) = 0$ and the zeta function of E is*

$$Z(E,T) = \frac{1 + pT^2}{(1-T)(1-pT)}. \tag{2.9}$$

On the other hand, let us look at a specific supersingular elliptic curve E given by $y^2 = x^3 - n^2 x$ over $\mathbb{F}_p$ for some positive integer n and $p \equiv 3 (\mathrm{mod}\ 4)$ such that $p \nmid 2n$. To see E is supersingular, since $p \equiv 3 (\mathrm{mod}\ 4)$, $p > 2$ and therefore the equation $x^3 - n^2 x = 0$ has three distinct roots over $\overline{\mathbb{F}}_p$, the algebraical closure of $\mathbb{F}_p$. So from

[25], p.140, *to prove E is supersingular, it is enough to show the coefficient of x^{p-1} in $(x^3 - n^2x)^{\frac{p-1}{2}}$ is zero. On the other hand,*

$$(x^3 - n^2x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}}(x^2 - n^2)^{\frac{p-1}{2}}.$$

So it is enough to show the coefficient of $x^{\frac{p-1}{2}}$ in the binomial expansion of $(x^2-n^2)^{\frac{p-1}{2}}$ is 0. Consequently one has to show there is no positive integer b satisfying $2b = \frac{p-1}{2}$, i.e. $4 \nmid (p-1)$. But this follows from $p \equiv 3 (\mathrm{mod}\ 4)$.

Using Gauss sum and Jacobi sum, one can prove ([14], p.56-61)*:*

$$\#E(\mathbb{F}_{p^r}) = 1 + p^r - (i\sqrt{p})^r - (-i\sqrt{p})^r, \tag{2.10}$$

for any positive integer r. Hence

$$\begin{aligned}
Z(E,T) &= \exp\left(\sum_{r=1}^{\infty} \#E(\mathbb{F}_{p^r})\frac{T^r}{r}\right) \\
&= \exp\left(\sum_{r=1}^{\infty} \left(1 + p^r - (i\sqrt{p})^r - (-i\sqrt{p})^r\right)\frac{T^r}{r}\right) \\
&= \exp\left(\sum_{r=1}^{\infty} \frac{T^r}{r}\right) \exp\left(\sum_{r=1}^{\infty} \frac{(pT)^r}{r}\right) \exp\left(\sum_{r=1}^{\infty} \Big(- (i\sqrt{p})^r - (-i\sqrt{p})^r\Big)\frac{T^r}{r}\right) \\
&= \frac{1}{1-T}\frac{1}{1-pT} \exp\left(\sum_{r=1}^{\infty} \Big(- (-p)^r - (-p)^r\Big)\frac{T^{2r}}{2r}\right) \\
&= \frac{1}{(1-T)(1-pT)} \exp\left(-\sum_{r=1}^{\infty} (-1)^r (2p^r)\frac{T^{2r}}{2r}\right) \\
&= \frac{1}{(1-T)(1-pT)} \exp\left(-\sum_{r=1}^{\infty} (-1)^r \frac{(pT^2)^r}{r}\right) \\
&= \frac{1+pT^2}{(1-T)(1-pT)}.
\end{aligned}$$

So we obtain the same zeta function for E.

CHAPTER 3
Non-abelian Cohomology

3.1 Cohomology of Profinite Groups

A profinite group G can be defined as $\varprojlim G_i$, where $\{G_i \,\big|\, i \in I, I \text{ is an index set}\}$ is a projective system of finite groups each of which is endowed with the discrete topology. Equivalently, a profinite group G can also be defined as a topological group that is Hausdorff, compact, and totally disconnected. In particular, every Galois group is profinite. Conversely, every profinite group is a Galois group of some field extension ([21], p.16).

Example 3.1.1.

1. *The Prüfer group* $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ *is the Galois group of the field extension* $\overline{\mathbb{F}}_p/\mathbb{F}_p$ *for any prime number* p.
2. *For any prime* ℓ, *the ring of* ℓ*-adic integers* $\mathbb{Z}_\ell$ *can be defined as follows:*

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z},$$

which is clearly a profinite group and is also a commutative ring. For any finite field $\mathbb{F}_p$ *where* p *is a prime number, consider the following Galois extensions:*

$$\mathbb{F}_p \subset \mathbb{F}_{p^\ell} \subset \mathbb{F}_{p^{\ell^2}} \subset \cdots \subset \mathbb{F}_{p^{\ell^n}} \subset \cdots$$

Define

$$\mathbb{F}_{p^{\ell^\infty}} = \bigcup_{n=0}^{\infty} \mathbb{F}_{p^{\ell^n}}.$$

Then we have ([21], p.6)*:*

$$\mathrm{Gal}(\mathbb{F}_{p^{\ell^\infty}}/\mathbb{F}_p) \cong (\mathbb{Z}_\ell, +).$$

Definition 3.1.2. *Let G be a profinite group and let A be an abelian group endowed with the discrete topology (the operation on A is written additively). The group A is called a (discrete) G-module if we have a continuous map $G \times A \to A$, $(g, a) \mapsto g \cdot a$, such that:*

- $1 \cdot a = a$,
- $(gh) \cdot a = g \cdot (h \cdot a)$,
- $g \cdot (a + b) = g \cdot a + g \cdot b$,

for any $g, h \in G$ and any $a, b \in A$. Here 1 is the identity of G. The product $g \cdot a$ is sometimes denoted also by $g(a)$ or ${}^g a$.

In the notation above, let

$$C^q(G, A) := \{f : G^q \to A \,\big|\, f \text{ is continuous}\},$$

for any integer $q \geq 0$, and define the coboundary operator,

$$d : C^q(G, A) \to C^{q+1}(G, A),$$

by

$$\begin{aligned}(df)(g_1, g_2, \ldots, g_{q+1}) = & g_1 \cdot f(g_2, \ldots, g_{q+1}) \\ & + \sum_{i=1}^{q} (-1)^i f(g_1, g_2, \ldots, g_i g_{i+1}, \ldots, g_{q+1}) \\ & + (-1)^{q+1} f(g_1, g_2, \ldots, g_q).\end{aligned}$$

Define q-th cohomology group

$$H^q(G, A) = Z^q(G, A)/B^q(G, A),$$

where

$$Z^q(G, A) = \ker(d : C^q(G, A) \to C^{q+1}(G, A)),$$

and

$$B^q(G, A) = \mathrm{Im}(d : C^{q-1}(G, A) \to C^q(G, A)).$$

Let $\mathcal{U} = \{U \subset G \mid U \text{ is open in } G \text{ and } U \lhd G\}$, then ([21], p.114)

$$H^1(G, A) = \varinjlim_{U} H^1(G/U, A^U),$$

where U runs over $\mathcal{U}$.

Example 3.1.3. *For $H^0(G, A)$, define $B^0 = \{0\}$, the group with only the identity element, and define $G^0 = \{1\}$. Then clearly*

$$C^0(G, A) = \{f : \{1\} \to A\},$$

which can be canonically identified with A. We also have

$$df(g) = g \cdot f(1) - f(1),$$

for any $g \in G$. Hence

$$Z^0(G,A) = \{f \in C^0(G,A) \,\big|\, g \cdot f(1) = f(1) \text{ for any } g \in G\} = A^G,$$

where A^G is defined to be $\{a \in A \;\big|\; g \cdot a = a, \forall g \in G\}$.

For $H^1(G,A)$, we have

$$H^1(G,A) = Z^1(G,A)/B^1(G,A),$$

where

$$Z^1(G,A) = \{f : G \to A \;\big|\; f \text{ is continuous, } f(gh) = g \cdot f(h) + f(g), \forall g,h \in G\},$$

and

$$B^1(G,A) = \{f : G \to A \;\big|\; f \text{ is continuous and for some } a \in G,$$
$$f(g) = g \cdot a - a, \forall g \in G\}.$$

Example 3.1.4. *(The Kummer sequence) Let k be a perfect field, then its algebraic closure $\overline{k}$ is a Galois extension of k. Given a positive integer n, suppose characteristic of k is 0 or is prime to n, then we have the exact sequence:*

$$1 \to \mu_n(\overline{k}) \to \overline{k}^\times \xrightarrow{\alpha \mapsto \alpha^n} \overline{k}^\times \to 1,$$

where $\mu_n(\overline{k})$ is the group of the n-th roots of unity in $\overline{k}$. Hence we have the following exact sequence:

$$1 \to H^0(G_k, \mu_n(\overline{k})) \to H^0(G_k, \overline{k}^\times) \to H^0(G_k, \overline{k}^\times)$$
$$\to H^1(G_k, \mu_n(\overline{k})) \to H^1(G_k, \overline{k}^\times),$$

where $G_k = \mathrm{Gal}(\overline{k}/k)$. *Clearly* $H^0(G_k, \mu_n(\overline{k})) = \mu_n(k)$ *and* $H^0(G_k, \overline{k}^\times) = k^\times$. *From Hilbert's Theorem* 90, *we have* $H^1(G_k, \overline{k}^\times)$ *is trivial. Hence the following sequence is exact:*

$$1 \to \mu_n(k) \to k^\times \xrightarrow{n} k^\times \to H^1(G_k, \mu_n(\overline{k})) \to 1.$$

Therefore we have the isomorphism:

$$H^1(G_k, \mu_n(\overline{k})) \cong k^\times/(k^\times)^n. \tag{3.1}$$

In particular, let $k = \mathbb{F}_p$ *for some prime number* p ($p \nmid n$ *and not necessarily* $\mu_n(\overline{k}) \subset k^\times$). *Since* $k^\times$ *is cyclic of order* $p-1$, *we have* $k^\times/(k^\times)^2 \cong \mu_2$ *and*

$$k^\times/(k^\times)^3 \cong \begin{cases} 1, & p = 3 \text{ or } p \equiv 2(\mathrm{mod}\ 3), \\ \mu_3, & p \equiv 1(\mathrm{mod}\ 3), \end{cases} \tag{3.2}$$

and

$$k^\times/(k^\times)^4 \cong \begin{cases} \mu_4, & p > 2 \text{ and } p \equiv 1(\mathrm{mod}\ 4), \\ \mu_2, & p > 2 \text{ and } p \equiv 3(\mathrm{mod}\ 4), \\ 1, & p = 2. \end{cases} \tag{3.3}$$

3.2 Non-abelian Cohomology

This section mainly follows [24], §5.

When A is not abelian, we do not say A is a G-module any more, but a G-group if we have a continuous map $G \times A \to A$, $(g, a) \mapsto g \cdot a$ such that (the operation on A is written multiplicatively because A may be not abelian):

- $1 \cdot a = a$,
- $(gh) \cdot a = g \cdot (h \cdot a)$,
- $g \cdot (ab) = (g \cdot a)(g \cdot b)$,

for any $g, h \in G$ and any $a, b \in A$. Here A is also endowed with the discrete topology. Similarly, when A is just a set, we give A the discrete topology and call A a G-set if we have a continuous map $G \times A \to A$, $(g, a) \mapsto g \cdot a$ such that:

- $1 \cdot a = a$,
- $(gh) \cdot a = g \cdot (h \cdot a)$,

for any $g, h \in G$ and any $a \in A$.

Definition 3.2.1. *Define*

$$H^0(G, A) = A^G = \{a \in A \,|\, g \cdot a = a,\ \forall g \in G\}.$$

Let

$$Z^1(G, A) = \{f : G \longrightarrow A \ \big|\ f \text{ is continuous, } f(gh) = f(g)(g \cdot f(h)), \forall g, h \in G\}.$$

Elements in $Z^1(G, A)$ are called 1-cocycles. Two cocycles f_1 and f_2 in $Z^1(G, A)$ are called to be cohomologous if for some $b \in A$, we have

$$f_2(g) = b^{-1} f_1(g)(g \cdot b),\ \forall g \in G.$$

It is easy to check this is an equivalence relation on $Z^1(G, A)$, denoted by $\sim$.

Define $H^1(G,A) = Z^1(G,A)/\sim$. *We have the unit cocyle*

$$f : G \to A, \;\; f(g) = 1, \forall g \in G.$$

The equivalence class of the unit cocycle is called the neutral element of $H^1(G,A)$ *and is denoted by* 0 *or* 1. $H^1(G,A)$ *is a pointed set with respect to its neutral element.*

Similarly, the identity element of A *is in* $H^0(G,A)$. *Define the neutral element of* $H^0(G,A)$ *to be the identity of* A. $H^0(G,A)$ *is then a pointed set with respect to its neutral element.*

Consequently we can define exact sequences, similar to the abelian case, although now H^1 is just a pointed set, and in general we do not have H^2 cohomology sets.

Definition 3.2.2. *Let* A, B *and* C *be pointed sets whose neutral elements are* a_0, b_0 *and* c_0 *respectively. Given the following sequence,*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C, \tag{3.4}$$

where $\alpha(a_0) = b_0$ *and* $\beta(b_0) = c_0$, *we say* (3.4) *is exact if* $\alpha(A) = \ker(\beta)$, *where* $\ker(\beta) = \{b \in B \,\big|\, \beta(b) = c_0\}$. *The set* $\ker(\beta)$ *is called the kernel of* β.

Similar to cohomology groups in abelian case, let

$$\mathcal{U} = \{U \subset G \,\big|\, U \text{ is open in } G \text{ and } U \lhd G\},$$

then

$$H^1(G,A) = \varinjlim H^1(G/U, A^U), \tag{3.5}$$

where U runs over $\mathcal{U}$ ([24], p.45).

Let B be a G-group and let A be a subgroup of B closed under the action of G (i.e. $g \cdot a \in A$ for any $g \in G$ and any $a \in A$). Let the map $\gamma : A \hookrightarrow B$ be just the inclusion map. Denote by B/A the set of cosets of A in B. Clearly B/A is a well-defined G-set. It is obvious that $\overline{1}$, the coset that $1 \in B$ belongs to, is in $H^0(G, B/A)$[1] . We call $\overline{1}$ the neutral element of $H^0(G, B/A)$. Define a map $\delta : H^0(G, B/A) \longrightarrow H^1(G, A)$ as follows:

For any $\overline{c} \in (B/A)^G$, let $c \in B$ represent $\overline{c}$. Define the map $\delta(\overline{c}) : G \to A$ by $\delta(\overline{c})(g) = c^{-1}g(c), \ \forall g \in G$.

First, $\delta(\overline{c})$ is a cocycle. Indeed, for any $g_1, g_2 \in G$,

$$\begin{aligned}\delta(\overline{c})(g_1)g_1(\delta(\overline{c})(g_2)) &= c^{-1}g_1(c)g_1(c^{-1}g_2(c)) \\ &= c^{-1}g_1(c)g_1(c^{-1})g_1(g_2(c)) \\ &= c^{-1}g_1(g_2(c)) \\ &= \delta(\overline{c})(g_1g_2).\end{aligned}$$

Suppose $c_1 \in B$ also represents $\overline{c}$, then $c_1 = cb_1$ for some $b_1 \in B$. Hence

$$\begin{aligned}\delta(\overline{c}_1)(g) &= c_1^{-1}g(c_1) \\ &= (cb_1)^{-1}g(cb_1) \\ &= b_1^{-1}c^{-1}g(c)g(b_1).\end{aligned}$$

[1] Given a G-set S, define $H^0(G, S) = \{s \in S \,\big|\, g \cdot s = s \text{ for any } g \in G\}$, which is also denoted by S^G.

Hence $\delta(\overline{c}_1)$ and $\delta(\overline{c})$ are cohomologous. Finally,

$$\delta(\overline{1})(g) = 1^{-1}g(1) = 1,$$

hence δ maps the neutral element in $H^0(G, B/A)$ to the neutral element in $H^1(G, A)$. So δ is well-defined and consequently the following proposition holds.

Proposition 3.2.3. *The following sequence is exact as pointed sets:*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B).$$

If A is not only a subgroup of B but also normal in B, it is easy to see B/A is a G-group and we have a stronger result:

Proposition 3.2.4. *If A is a normal subgroup of B, the following sequence is exact as pointed sets:*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, B/A).$$

If one further assumes A is a subgroup of the center of B, we have the following result: ([24], p.55)

Proposition 3.2.5. *Suppose that as G-groups, the sequence*

$$1 \to A \to B \to C \to 1$$

is exact and A is a subgroup of the center of B, then the following sequence is exact:

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C)$$
$$\xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \to H^2(G,A).$$

Example 3.2.6. *Let k be any finite field, $G = \mathrm{Gal}(\overline{k}/k)$. Then we have* ([23], p.151) *$H^1(G, \mathrm{GL}_n(\overline{k})) = 1$. In particular, when $n = 1$, $H^1(G, \mathrm{GL}_n(\overline{k})) = H^1(G, \overline{k}^\times) = 1$, and we recover the famous Hilbert's Theorem 90. We also have the exact sequence*

$$1 \to \mathrm{SL}_n(\overline{k}) \to \mathrm{GL}_n(\overline{k}) \xrightarrow{\det} \overline{k}^\times \to 1,$$

which gives the exact sequence

$$H^0(G, \mathrm{GL}_n(\overline{k})) \to H^0(G, \overline{k}^\times) \xrightarrow{\alpha} H^1(G, \mathrm{SL}_n(\overline{k})) \xrightarrow{\beta} H^1(G, \mathrm{GL}_n(\overline{k})) = 1,$$

i.e.

$$\mathrm{GL}_n(k) \xrightarrow{\det} k^\times \xrightarrow{\alpha} H^1(G, \mathrm{SL}_n(\overline{k})) \xrightarrow{\beta} 1.$$

Since $\mathrm{GL}_n(k) \xrightarrow{\det} k^\times$ is surjective, $\ker(\alpha) = k^\times$, and therefore the image of α contains only one element 1, which is the neutral element of $H^1(G, \mathrm{SL}_n(\overline{k}))$. Hence $H^1(G, \mathrm{SL}_n(\overline{k})) = \ker(\beta) = \alpha(k^\times) = 1$.

The following lemma is used in the example bellow:

Lemma 3.2.7. *Let A and B be G-groups and let $\varphi : B \to \mathrm{Aut}(A)$ be a group homomorphism such that*

$$(\varphi(g \cdot b))(g \cdot a) = g \cdot ((\varphi(b))(a)), \tag{3.6}$$

for any $g \in G$, any $a \in A$ and any $b \in B$, then the semi-product $A \rtimes_\varphi B$ with respect to φ is a G-group, the action of G on which is defined as $g \cdot (a, b) = (g \cdot a, g \cdot b)$ for any $g \in G$ and any $(a, b) \in A \rtimes_\varphi B$.

Proof. First for the identity element 1 of G, $1 \cdot (a, b) = (1 \cdot a, 1 \cdot b) = (a, b)$ for any $(a, b) \in A \rtimes_\varphi B$.

For any $g_1, g_2 \in G$, $(g_1 g_2) \cdot (a, b) = ((g_1 g_2) \cdot a, (g_1 g_2) \cdot b)$, and $g_1 \cdot (g_2 \cdot (a, b)) = g_1 \cdot (g_2 \cdot a, g_2 \cdot b) = (g_1 \cdot (g_2 \cdot a), g_1 \cdot (g_2 \cdot b)) = ((g_1 g_2) \cdot a, (g_1 g_2) \cdot b)$. Therefore,

$$(g_1 g_2) \cdot (a, b) = g_1 \cdot (g_2 \cdot (a, b)).$$

Finally, for any $g \in G$, and any (a_1, b_1) and $(a_2, b_2) \in A \rtimes_\varphi B$,

$$\begin{aligned}
g \cdot ((a_1, b_1)(a_2, b_2)) &= g \cdot \Big(a_1 \Big(\big(\varphi(b_1)\big)\big(a_2\big) \Big), b_1 b_2 \Big) \\
&= \Big(g \cdot \Big(a_1 \Big(\big(\varphi(b_1)\big)(a_2) \Big) \Big), g \cdot (b_1 b_2) \Big) \\
&= \Big(\Big(g \cdot a_1 \Big) \Big(g \cdot \Big(\big(\varphi(b_1)\big)\big(a_2\big) \Big) \Big), (g \cdot b_1)(g \cdot b_2) \Big) \\
&\overset{(3.6)}{=} \Big(\Big(g \cdot a_1 \Big) \Big(\big(\varphi(g \cdot b_1)\big)\big(g \cdot a_2\big) \Big), (g \cdot b_1)(g \cdot b_2) \Big) \\
&= (g \cdot a_1, g \cdot b_1)(g \cdot a_2, g \cdot b_2) \\
&= \big(g \cdot (a_1, b_1)\big)\big(g \cdot (a_2, b_2)\big).
\end{aligned}$$

Hence $A \rtimes_\varphi B$ is a G-group. □

Example 3.2.8. *Let $k = \mathbb{F}_p$ for some odd prime $p > 3$. Then the absolute Galois group $G_k = \mathrm{Gal}(\overline{k}/k) \cong \hat{\mathbb{Z}}$. For any positive integer m, let μ_m be the group of m-th*

roots of the unity in $\overline{k}$. *Since* $p > 3$, μ_3 *and* μ_2 *are cyclic groups with order* 3 *and* 2 *respectively, and consequently we can let* $\mu_2 = \{\pm 1\}$ *and* $\mu_3 = \{1, \alpha, \alpha^2\}$, *where* α *is any non-trivial third root of the unity in* $\overline{k}$. *Clearly* G_k *acts trivially on* μ_2. *For any* $g \in G_k$, *any* $a \in \mu_3$ *and any* $b \in \mu_2$, *define*

$$g \cdot (a, b) = (g \cdot a, g \cdot b) = (g \cdot a, b). \tag{3.7}$$

Now we will verify that $\mu_3 \rtimes \mu_2$ *becomes a* G_k*-group under the action* (3.7) *using Lemma* 3.2.7. *Here* μ_2 *acts on* μ_3 *by the unique non-trivial way. It is enough to show*

$$(g \cdot b) \cdot (g \cdot a) = g \cdot (b \cdot a), \tag{3.8}$$

i.e.

$$b \cdot (g \cdot a) = g \cdot (b \cdot a). \tag{3.9}$$

When $b = 1$, $b \cdot (g \cdot a) = g \cdot a$ *and* $g \cdot (b \cdot a) = g \cdot b$, *so* (3.9) *holds. When* $b = -1$, $b \cdot (g \cdot a) = (g \cdot a)^2 = g \cdot (a^2) = g \cdot (b \cdot a)$, *hence* (3.9) *is also true. Therefore Lemma* 3.2.7 *shows* $\mu_3 \rtimes \mu_2$ *is a* G*-group under the action* (3.7).

So as G_k*-groups, we have the following exact sequence:*

$$1 \to \mu_3 \to \mu_3 \rtimes \mu_2 \to \mu_2 \to 1.$$

Consequently, the following sequence is exact:

$$H^0(G_k, \mu_2) \to H^1(G_k, \mu_3) \to H^1(G_k, \mu_3 \rtimes \mu_2) \to H^1(G_k, \mu_2).$$

Since $\mu_2 \subset \mathbb{F}_p$, $H^0(G_k, \mu_2) \cong \mu_2$. (3.1) *gives*

$$H^1(G_k, \mu_3) \cong k^\times / (k^\times)^3,$$

and

$$H^1(G_k, \mu_2) \cong k^\times/(k^\times)^2.$$

Hence we have the exact sequence:

$$\mu_2 \to k^\times/(k^\times)^3 \to H^1(G_k, \mu_3 \rtimes \mu_2) \to k^\times/(k^\times)^2.$$

When $p \equiv 2(mod\ 3)$, (3.2) *gives* $k^\times/(k^\times)^3 = 1$. *Hence the following sequence is exact:*

$$1 \to H^1(G_k, \mu_3 \rtimes \mu_2) \to k^\times/(k^\times)^2. \tag{3.10}$$

When $p \equiv 1(mod\ 3)$, *similarly, the following sequence is exact:*

$$\mu_2 \to \mu_3 \to H^1(G_k, \mu_3 \rtimes \mu_2) \to k^\times/(k^\times)^2.$$

Since the homomorphism $\mu_2 \to \mu_3$ *is trivial, we have the exact sequence:*

$$1 \to \mu_3 \to H^1(G_k, \mu_3 \rtimes \mu_2) \to k^\times/(k^\times)^2. \tag{3.11}$$

Now I will determine the structure of $H^1(G_k, \mu_3 \rtimes \mu_2)$ *with the help of* (3.5). *In this case, we have*

$$H^1(G_k, \mu_3 \rtimes \mu_2) = \varinjlim_n H^1(\mathbb{Z}/n\mathbb{Z}, (\mu_3 \rtimes \mu_2)^{\mathrm{Gal}(\overline{k}/k_n)}), \tag{3.12}$$

where $k_n = \mathbb{F}_{p^n}$. *If* $\mu_3 \subset \mathbb{F}_p$, *since* $x^3 - 1 = (x-1)(x^2+x+1)$, -3 *is a quadratic residue of* p, *which is equivalent to say* $p \equiv 1(\mathrm{mod}\ 3)$. *Therefore when* $p \equiv 1(\mathrm{mod}\ 3)$, $\mu_3 \subset \mathbb{F}_p$ *and consequently both* $\mathrm{Gal}(k_n/k) \cong \mathbb{Z}/n\mathbb{Z}$ *and* $\mathrm{Gal}(\overline{k}/k_n)$ *act on* $\mu_3 \rtimes \mu_2$

trivially. So when $6|n$,

$$\begin{aligned} H^1(\mathbb{Z}/n\mathbb{Z}, (\mu_3 \rtimes \mu_2)^{\mathrm{Gal}(\overline{k}/k_n)}) &= H^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2) \\ &= \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2) \\ &\cong \mu_3 \rtimes \mu_2. \end{aligned}$$

Hence (3.12) *gives*

$$H^1(G_k, \mu_3 \rtimes \mu_2) \cong \mu_3 \rtimes \mu_2. \tag{3.13}$$

If $p \not\equiv 1 (\mathrm{mod}\ 3)$, $\mu_3 \not\subset \mathbb{F}_p$. *But now* $\mu_3 \subset \mathbb{F}_p[x]/(x^2+x+1) \cong \mathbb{F}_{p^2}$, *so*

$$(\mu_3 \rtimes \mu_2)^{\mathrm{Gal}(\overline{k}/k_n)} \cong \begin{cases} \mu_3 \rtimes \mu_2 & n \equiv 0 (\mathrm{mod}\ 2), \\ \mu_2 & n \equiv 1 (\mathrm{mod}\ 2). \end{cases}$$

Hence,

$$H^1(\mathbb{Z}/n\mathbb{Z}, (\mu_3 \rtimes \mu_2)^{\mathrm{Gal}(\overline{k}/k_n)}) = H^1(\mathbb{Z}/n\mathbb{Z}, \mu_2) \cong \mu_2,\ n \equiv 1 (\mathrm{mod}\ 2). \tag{3.14}$$

When $n \equiv 0 (\mathrm{mod}\ 2)$,

$$H^1(\mathbb{Z}/n\mathbb{Z}, (\mu_3 \rtimes \mu_2)^{\mathrm{Gal}(\overline{k}/k_n)}) = H^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2).$$

Clearly an element $f \in Z^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2)$ *is fully determined by* $f(1)$. *We have the following cases:*

1. $f(1) = (\alpha, 1)$. *In this case one can easily show that*

$$f(m) = \begin{cases} (\alpha, 1), & m \equiv 1 (\mathrm{mod}\ 2), \\ (1, 1), & m \equiv 0 (\mathrm{mod}\ 2), \end{cases}$$

for $0 \leq m < n$. Hence such f is an element in $Z^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2)$. Now we calculate $(\alpha,1)^{-1} f(m)\,({}^m(\alpha,1)) = (\alpha^2,1) f(m)\,(\alpha^{p^m},1)$:

$$(\alpha^2,1) f(m)\,(\alpha^{p^m},1) = \begin{cases} (\alpha^2,1)(\alpha,1)(\alpha^2,1) = (\alpha^2,1), & \text{when } m \equiv 1 (\mathrm{mod}\ 2), \\ (\alpha^2,1)(1,1)(\alpha,1) = (1,1), & \text{when } m \equiv 0 (\mathrm{mod}\ 2). \end{cases}$$

Also

$$\begin{aligned} (\alpha^2,1)^{-1} f(m)\,({}^m(\alpha^2,1)) &= (\alpha,1) f(m)\,(\alpha^{p^m}\alpha^{p^m},1) \\ &= \begin{cases} (\alpha,1)(\alpha,1)(\alpha^2\alpha^2,1) = (\alpha^6,1) = (1,1), & \text{when } m \equiv 1 (\mathrm{mod}\ 2), \\ (\alpha,1)(1,1)(\alpha^2,1) = (\alpha^3,1) = (1,1), & \text{when } m \equiv 0 (\mathrm{mod}\ 2). \end{cases} \end{aligned}$$

Hence we have $f \sim g$ in $Z^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2)$, where $g(1) = (1,1)$ or $(\alpha^2,1)$.

2. $f(1) = (\alpha,-1)$. Similarly we have

$$\begin{aligned} f(2) &= f(1+1) = f(1)\,{}^1f(1) = (\alpha^2,1), \\ f(3) &= f(1+2) = f(1)\,{}^1f(2) = (1,-1), \\ f(4) &= f(1+3) = f(1)\,{}^1f(3) = (\alpha,-1) = f(1). \end{aligned}$$

This implies $f(m) \neq (1,1)$ for any $m > 0$. But that is impossible (because in $\mathbb{Z}/n\mathbb{Z}$, $\overline{m} = 0$ when $m = n$, and we must have $f(0) = (1,1)$).

3. $f(1) = (1,-1)$. We have $f(2) = f(1+1) = f(1)\,{}^1f(1) = (1,-1)\,{}^1(1,-1) = (1,-1)(1,-1) = (1,1)$. So $f \in Z^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2)$.

Hence there are at most two equivalence classes $[\gamma_1]$ and $[\gamma_2]$ in $H^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2)$ whose representatives γ_1 and γ_2 can be chosen to be the unit cocycle and $\gamma_2(1) = (1,-1)$ respectively. Since for any element $(a,b) \in \mu_3 \rtimes \mu_2$ and any $g \in \mathbb{Z}/n\mathbb{Z}$, the second component in $((a,b)^{-1})(1,1)\,{}^g(a,b)$ is $b^{-1}b = 1$, so γ_1 and γ_2 can not be

cohomologous in $Z^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2)$. *So we conclude that*

$$H^1(\mathbb{Z}/n\mathbb{Z}, \mu_3 \rtimes \mu_2) \cong \mu_2, \ n \equiv 0(\text{mod } 2). \tag{3.15}$$

(3.14) *and* (3.15) *give:*

$$H^1(G_k, \mu_3 \rtimes \mu_2) \cong \mu_2. \tag{3.16}$$

The proof given above shows that $H^1(G_k, \mu_3 \rtimes \mu_2)$ *can be regarded to have some intrinsic group structure, and* (3.13) *and* (3.16) *hold as groups.*

CHAPTER 4
Galois Descent and Forms

In this chapter, we will introduce Galois descent in a general setting using the language of categories. The objective is to prove Theorem 4.3.3 and obtain a relation between the action of the relative Frobenius map (or equivalently, geometric Frobenius map) on the étale cohomology of a given smooth projective variety over a finite field and the action on the forms of the variety. From such a relation, we can get a relation between the Hasse-Weil zeta function of a smooth projective variety and those of its forms. I mainly follow [3] in this chapter.

4.1 Galois Descent

The concept of Galois descent can be explained in the following example coming from classical Galois theory.

Example 4.1.1. *Let F be a field and L/F a Galois extension. Then F can be viewed as a subset of L. Galois descent here means that $x \in L$ is in F if and only if x is fixed by* $\mathrm{Gal}(L/F)$. *But this is a basic result in classical Galois theory.*

The formal definition of Galois descent is given below in terms of coefficient extension.

Definition 4.1.2. *Let $\mathfrak{C}_1$ and $\mathfrak{C}_2$ be two categories and K/k be a Galois field extension with Galois group G. A coefficient extension from k to K consists of a covariant functor F from $\mathfrak{C}_1$ to $\mathfrak{C}_2$ and for any objects X and Y in $\mathfrak{C}_1$, a (left) G-action on $\mathrm{Iso}(F(X), F(Y))$, the set of isomorphisms from $F(X)$ to $F(Y)$ in $\mathfrak{C}_2$, such that the following conditions hold:*

1. *For any objects X, Y and Z in $\mathfrak{C}_1$, any isomorphism $f:\ F(X) \to F(Y)$ and $g:\ F(Y) \to F(Z)$ and any element $s \in G$,*

$$^s(g \circ f) = (\,^s g) \circ (\,^s f).$$

2. *For any objects X and Y in $\mathfrak{C}_1$,*

$$F(\mathrm{Iso}(X, Y)) = \mathrm{Iso}(F(X), F(Y))^G,$$

where

$$\mathrm{Iso}(F(X), F(Y))^G = \{\alpha \in \mathrm{Iso}(F(X), F(Y)) \,\big|\, {}^s\alpha = \alpha,\ \forall s \in G\}.$$

Example 4.1.3. *Let k be a field and K/k be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Let $\mathfrak{C}_1$ be the category of finite dimensional vector spaces over k with linear maps of vector spaces over k. Let $\mathfrak{C}_2$ be the category of vector spaces over K with linear maps of vector spaces. Define the functor $F : \mathfrak{C}_1 \to \mathfrak{C}_2$ by $F(V) = V \otimes_k K$ for any object V in $\mathfrak{C}_1$ and $F(f) = f \otimes 1$ for any linear map $f : V_1 \to V_2$ in $\mathfrak{C}_1$. Since for any positive integer n, $\mathrm{GL}_n(K)^G = \mathrm{GL}_n(k)$, where $g \in G$ acts on any element $M \in \mathrm{GL}_n(K)$ in the usual way. Therefore for vector spaces V_1 and V_2 in $\mathfrak{C}_1$, we have*

$$F(\mathrm{Iso}(V_1, V_2)) = \mathrm{Iso}(F(V_1), F(V_2))^G,$$

after adopting the convention that $\emptyset^G = \emptyset$ ($\mathrm{Iso}(V_1, V_2) \neq \emptyset$ *if and only if* V_1 *and* V_2 *have the same dimension over* k*).*

From now on, the categories $\mathfrak{C}_1$ and $\mathfrak{C}_2$ will be denoted by $\mathfrak{C}_k$ and $\mathfrak{C}_K$ respectively. It is easy to prove the following proposition.

Proposition 4.1.4. *Let* k*,* K*,* G*,* $\mathfrak{C}_k$ *and* $\mathfrak{C}_K$ *be as above and suppose there are a covariant functor* F *from* $\mathfrak{C}_k$ *to* $\mathfrak{C}_K$ *and a left* G*-action on* $\mathrm{Hom}(F(X), F(Y))$ *for any two objects* X *and* Y *in* $\mathfrak{C}_k$*, such that*

1. *For any objects* X*,* Y *and* Z *in* $\mathfrak{C}_k$*, morphisms* $f : F(X) \to F(Y)$ *and* $g : F(Y) \to F(Z)$*, and any element* $s \in G$*,*

$$^s(g \circ f) = (\,^s g) \circ (\,^s f).$$

2. *For any objects* X *and* Y *in* $\mathfrak{C}_k$*,*

$$F(\mathrm{Hom}(X, Y)) = \mathrm{Hom}(F(X), F(Y))^G.$$

Then we have a coefficient extension after restricting the G*-action to isomorphisms.*

For any field L, denote by $\mathcal{V}ar_L$ the category of (quasi-projective) varieties over L with morphisms of varieties over L, and denote by $\mathcal{V}ar_{L,\mathrm{Iso}}$ the category of (quasi-projective) varieties over L with isomorphisms of varieties over L ($\mathcal{V}ar_{L,\mathrm{Iso}}$ is a category since for any variety V over L, the identity map $\mathrm{id}_V : V \to V$ is an isomorphism over L).

Theorem 4.1.5. ([3], p.18-24) *Let k, K and G be as in Definition* 4.1.2. *Let the functor $F: \mathcal{V}ar_k \to \mathcal{V}ar_K$ be defined as:*

$$F(X) = X_K := X \times_k K,$$

and

$$F(X \xrightarrow{f} Y) = (X_K \xrightarrow{f \times 1_{\operatorname{Spec} K}} Y_K).$$

For any $g \in G$ and $f \in \operatorname{Hom}(X_K, Y_K)$, where objects X and Y are in $\mathcal{V}ar_k$, define the action ${}^g f$ of g on f to be the morphism which makes the following diagram commutative:

$$\begin{array}{ccc} X_K & \xrightarrow{f} & Y_K \\ {\scriptstyle 1_{X_k} \times g^*}\uparrow & & \uparrow{\scriptstyle 1_{Y_k} \times g^*} \\ X_K & \xrightarrow[{}^g f]{} & Y_K \end{array}$$

where g^* is the endomorphism on $\operatorname{Spec} K$ *induced by g, so*

$${}^g f = (1_{Y_k} \times g^*)^{-1} \circ f \circ (1_{X_k} \times g^*).$$

Then we have a coefficient extension after restricting the G-action to isomorphisms, denoted by $F: \mathcal{V}ar_{k,\mathrm{Iso}} \to \mathcal{V}ar_{K,\mathrm{Iso}}$.

Example 4.1.6. *Let $X = Y = \operatorname{Spec} k[x]$ for some field k. Let K/k be a Galois extension with Galois group G. Let φ be an endomorphism of X defined over K which corresponds to a ring endomorphism*

$$\varphi^{\#}: K[x] \to K[x],\ x \mapsto f(x),$$

for some polynomial $f(x) \in K[x]$. By abuse of notation, denote $\varphi^{\#}$ by f. Any element $g \in G$ induces an isomorphism of $K[x]$, denoted by $\widetilde{g}$:

$$\widetilde{g} : K[x] \to K[x],\ x \mapsto x,\ a \mapsto g(a),\ \forall a \in K.$$

Clearly $\widetilde{g}^{-1} = \widetilde{g^{-1}}$. Consequently, ${}^{g}\varphi$ corresponds to the endomorphism f_g of $K[x]$ which makes the following diagram commutative:

$$\begin{array}{ccc} K[x] & \xrightarrow{f} & K[x] \\ {\scriptstyle \widetilde{g}}\downarrow & & \downarrow{\scriptstyle \widetilde{g}} \\ K[x] & \xrightarrow[f_g]{} & K[x] \end{array}$$

So

$$f_g = \widetilde{g} \circ f \circ \widetilde{g}^{-1}.$$

Suppose

$$f = \sum_{i=1}^{n} a_i x^i, \tag{4.1}$$

for some positive integer n and some $a_i \in K$, $i = 1, 2, \ldots, n$, then for any polynomial $h = \sum_{i=1}^{m} b_i x^i \in K[x]$,

$$\begin{aligned} f_g\left(\sum_{i=1}^{m} b_i x^i\right) &= \widetilde{g} \circ f \circ \widetilde{g}^{-1}\left(\sum_{i=1}^{m} b_i x^i\right) \\ &= \widetilde{g} \circ f\left(\sum_{i=1}^{m} g^{-1}(b_i) x^i\right) \\ &= \widetilde{g}\left(\sum_{i=1}^{m} g^{-1}(b_i)\left(\sum_{j=1}^{n} a_j x^j\right)^i\right) \\ &= \sum_{i=1}^{m} b_i \left(\sum_{j=1}^{n} g(a_j) x^j\right)^i \\ &= \sum_{i=1}^{m} b_i (\widetilde{g}(f))^i. \end{aligned}$$

Hence we have

$$f_g\left(\sum_{i=1}^{m} g(b_i)x^i\right) = \sum_{i=1}^{m} g(b_i)(\widetilde{g}(f))^i,$$

i.e.

$$f_g(\widetilde{g}(h)) = \widetilde{g}(f(h)),$$

for any $h \in K[x]$. This is equivalent to say that for any K-point $a \in \mathbb{A}^1$,

$$^{g}\varphi(\,^{g}a) = \,^{g}(\varphi(a)).$$

For any field L and any group H, denote by $\mathfrak{Rep}_L^H$ the category with objects of the form (V, ϕ) where V is a finite dimensional vector space over L and ϕ is an H-action defined on V, and morphisms being linear mappings of L-vector spaces that are H-equivariant.

Denote the absolute Galois groups of k and K by G_k and G_K respectively. Clearly we can regard G_K as a normal subgroup of G_k and $G = G_k/G_K$. Consequently, for the categories $\mathfrak{Rep}_L^{G_k}$ and $\mathfrak{Rep}_L^{G_K}$, we have a natural functor F from $\mathfrak{Rep}_L^{G_k}$ to $\mathfrak{Rep}_L^{G_K}$ given by sending (V, ϕ) to $(V, \phi\big|G_K)$ and being the identity mapping on morphisms in $\mathfrak{Rep}_L^{G_k}$. For any $\overline{s} \in G$, let s be a representative in G_k (because $G = G_k/G_K$). For any two objects (X_1, ϕ_1) and (X_2, ϕ_2) and any isomorphism

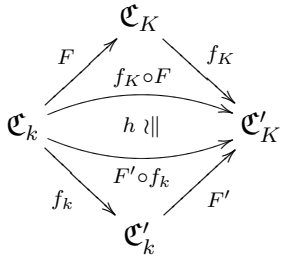
$$f:\ F((X_1, \phi_1)) = (X_1, \phi_1\big|G_K) \xrightarrow{\cong} F((X_2, \phi_2)) = (X_2, \phi_2\big|G_K),$$

define the action of $\overline{s}$ on f by

$$^{\overline{s}}f = \phi_2(s) \circ f \circ \phi_1(s)^{-1}. \tag{4.2}$$

Theorem 4.1.7. (4.2) *defines an action of G on the set of isomorphisms of any two objects in $\mathfrak{Rep}_L^{G_K}$ and $\mathfrak{Rep}_L^{G_k} \xrightarrow{F} \mathfrak{Rep}_L^{G_K}$ is a coefficient extension with respect to such action.*

Definition 4.1.8. *Suppose $\mathfrak{C}_k \xrightarrow{F} \mathfrak{C}_K$ and $\mathfrak{C}'_k \xrightarrow{F'} \mathfrak{C}'_K$ are two coefficient extensions from k to K. A morphism from F to F' is a triple (f_k, f_K, h), where $f_k : \mathfrak{C}_k \to \mathfrak{C}'_k$ and $f_K : \mathfrak{C}_K \to \mathfrak{C}'_K$ are covariant functors and $h : f_K \circ F \xrightarrow{\cong} F' \circ f_k$ is an isomorphism of functors,*



and for any two objects X and Y in $\mathfrak{C}_k$, the following diagram is G-equivariant:

$$\begin{array}{ccc} \mathrm{Iso}(F(X), F(Y)) & \xrightarrow{f_K} & \mathrm{Iso}(f_K \circ F(X), f_K \circ F(Y)) \\ & \overset{h \circ f_K}{\searrow} & \downarrow h \\ & & \mathrm{Iso}(F' \circ f_k(X), F' \circ f_k(Y)) \end{array}$$

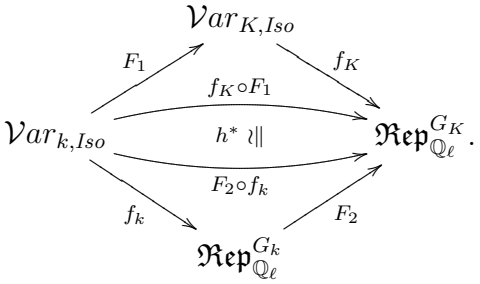
Under such definition of a morphism of coefficient extensions, we have ([3], p.91):

Theorem 4.1.9. *Let $F_1 : \mathcal{V}ar_{k,\mathrm{Iso}} \to \mathcal{V}ar_{K,\mathrm{Iso}}$ and $F_2 : \mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_k} \to \mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_K}$ be those as defined in Theorem* 4.1.5 *and Theorem* 4.1.7 *respectively, where ℓ is a prime number not equal to the characteristic of k. Fix a non-negative integer i. Define functor $f_k : \mathcal{V}ar_{k,\mathrm{Iso}} \to \mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_k}$ as follows: for any quasi-projective variety X/k, $F_k(X) = H^i(\overline{X}_{\acute{e}t}, \mathbb{Q}_\ell)$ and for any isomorphism $f : X_1 \to X_2$ in $\mathcal{V}ar_{k,\mathrm{Iso}}$, $F_k(f) = (f^*)^{-1}$, where f^* is the induced group isomorphism $H^i((\overline{X}_2)_{\acute{e}t}, \mathbb{Q}_\ell) \to H^i((\overline{X}_1)_{\acute{e}t}, \mathbb{Q}_\ell)$. The*

functor $f_K : \mathcal{V}ar_{K,\mathrm{Iso}} \to \mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_K}$ *is defined similarly. Let* $X_K = X \times_k K$. *The canonical isomorphism* $h : X \times_k \overline{k} \to X_K \times_K \overline{K}$ *induces the canonical isomorphism:*

$$h^* : f_K \circ F_1(X) = H^i((\overline{X}_K)_{\acute{e}t}, \mathbb{Q}_\ell) \to H^i(\overline{X}_{\acute{e}t}, \mathbb{Q}_\ell) = F_2 \circ f_k(X),$$

and further (f_k, f_K, h^*) *is a morphism from* F_1 *to* F_2*:*



In the above theorem, $h = 1$ if we identify $X \times_k \overline{k}$ with $X_K \times_K \overline{K}$.

4.2 Forms under Coefficient Extension

Let $\mathfrak{Cat}$ be any category, define the relation $\sim$ as follows: for any two objects A and B in $\mathfrak{Cat}$, $A \sim B$ if and only if there is an isomorphism f in $\mathfrak{Cat}$ between A and B. It is trivial to show the relation $\sim$ is an equivalence relation.

Definition 4.2.1. *Let* $F : \mathfrak{C}_k \to \mathfrak{C}_K$ *be a coefficient extension and* $\sim$ *be the equivalence relation on* $\mathfrak{C}_k$ *described above. For any object* X *in* $\mathfrak{C}_k$*, define the collection of* $\mathfrak{C}_K/\mathfrak{C}_k$*-forms of* X *to be:*

$$E(\mathfrak{C}_K/\mathfrak{C}_k, X) = \{Y \in \mathrm{Obj}(\mathfrak{C}_k) \,\big|\, F(Y) \cong F(X)\}/\sim .$$

Theorem 4.2.2. *Let Y be a $\mathfrak{C}_K/\mathfrak{C}_k$-form of X and $f : F(Y) \to F(X)$ be an isomorphism over K. Define the map $\tau = \tau_Y$ by*

$$\tau : G \to \mathrm{Aut}(F(X)), s \mapsto f \circ {}^s(f^{-1}), \forall s \in G.$$

Then $\tau \in Z^1(G, \mathrm{Aut}(F(X)))$, and the map

$$\gamma : E(\mathfrak{C}_K/\mathfrak{C}_k, X) \to H^1(G, \mathrm{Aut}(F(X))), [Y] \mapsto [\tau], \forall [Y] \in E(\mathfrak{C}_K/\mathfrak{C}_k, X)$$

is injective. If we regard $E(\mathfrak{C}_K/\mathfrak{C}_k, X)$ as a pointed set with the neutral element $[X]$, then γ maps $[X]$ to the neutral element of $H^1(G, \mathrm{Aut}(F(X)))$, i.e. γ is an injective map of pointed sets.

Proof. First, we prove γ is well-defined. For any s and t in G,

$$\begin{aligned}
\tau(st) &= f \circ {}^{st}(f^{-1}) \\
&= f \circ {}^s 1_{FY} \circ {}^{st}(f^{-1}) \\
&= f \circ {}^s(f^{-1} \circ f) \circ {}^{st}(f^{-1}) \\
&= f \circ ({}^s(f^{-1}) \circ {}^s f) \circ {}^s({}^t(f^{-1})) \\
&= (f \circ {}^s(f^{-1})) \circ ({}^s(f \circ {}^t(f^{-1}))) \\
&= \tau(s) \circ {}^s\tau(t).
\end{aligned}$$

Hence τ is a 1-cocyle.

Now we show that τ, in cohomology, does not depend on the choice of f. Suppose there is another isomorphism $f' : F(Y) \xrightarrow{\cong} F(X)$. Correspondingly, we have

the map:

$$\tau' : \ G \to \mathrm{Aut}(F(X)),\ s \mapsto f' \circ {}^s(f'^{-1}),\ \forall s \in G.$$

So

$$\begin{aligned}\tau'(s) &= f' \circ {}^s(f'^{-1}) \\ &= (f' \circ f^{-1} \circ f) \circ {}^s((f'^{-1} \circ f^{-1} \circ f)^{-1}) \\ &= (f \circ f'^{-1})^{-1} \circ (f \circ {}^s f^{-1}) \circ {}^s(f \circ f'^{-1}).\end{aligned}$$

Let $h = f \circ f'^{-1}$. The map h is clearly an element of $\mathrm{Aut}(F(X))$ and

$$\tau'(s) = h^{-1} \circ \tau(s) \circ {}^s h \sim \tau(s).$$

We also check that $\tau = \tau_Y$, in cohomology, depends only on the class of Y. Suppose there is another object Y' in $\mathfrak{C}_k$ such that $[Y] = [Y']$, then there is an isomorphism $\alpha : \ Y' \xrightarrow{\cong} Y$ over k. So $F(\alpha)$ is an isomorphism from $F(Y)$ to $F(Y')$. Hence $f \circ F(\alpha)$ is an isomorphism from $F(Y')$ to $F(X)$. Therefore with respect to Y', we have the map:

$$\tau_1 : \ G \to \mathrm{Aut}(F(X)),\ s \mapsto (f \circ F(\alpha)) \circ {}^s((f \circ F(\alpha))^{-1}),\ \forall s \in G.$$

So we have,

$$\begin{aligned}\tau_1(s) &= (f \circ F(\alpha)) \circ {}^s((f \circ F(\alpha))^{-1}) \\ &= f \circ F(\alpha) \circ {}^s(F(\alpha)^{-1}) \circ {}^s(f^{-1}).\end{aligned}$$

But F is a coefficient extension, so ${}^s(F(\alpha)^{-1}) = F(\alpha)^{-1}$. Hence

$$\begin{aligned}\tau_1(s) &= f \circ F(\alpha) \circ F(\alpha)^{-1} \circ {}^s(f^{-1}) \\ &= f \circ {}^s(f^{-1}) \\ &= \tau(s).\end{aligned}$$

This implies τ is independent of the choice of Y up to isomorphism. If we choose $Y = X$ and $f:\ F(Y) = F(X) \to F(X)$ to be the identity map, then clearly $f \circ {}^s(f^{-1})$ is the identity map on $F(X)$. So far we have established that there is a well-defined map of pointed sets $\gamma:\ E(\mathfrak{C}_K/\mathfrak{C}_k, X) \to H^1(G, \mathrm{Aut}(F(X)))$.

Suppose $\gamma([Y]) = \gamma([Y_1])$ for some object Y_1 in $\mathfrak{C}_k$ which is also a $\mathfrak{C}_K/\mathfrak{C}_k$-form of X. So $F(Y_1)$ and $F(Y)$ are isomorphic with some isomorphism q from $F(Y_1)$ to $F(Y)$. Let f be an isomorphism from $F(Y)$ to $F(X)$ and so $\gamma([Y])$ is represented by τ with $\tau(s) = f \circ {}^s f$ for any $s \in G$. Hence we have an isomorphism $f \circ q$ from $F(Y_1)$ to $F(X)$. Therefore $\gamma([Y_1])$ is represented by τ_1 with $\tau_1(s) = (f \circ q) \circ {}^s((f \circ q)^{-1})$ for any $s \in G$.

On the other hand, $\gamma([Y]) = \gamma([Y_1])$ implies $\tau(s)$ and $\tau_1(s)$ are cohomologous. So there exists $b \in \mathrm{Aut}(F(X))$, such that $\tau_1(s) = b^{-1} \circ \tau(s) \circ {}^s b$, i.e.

$$(f \circ q) \circ {}^s((f \circ q)^{-1}) = b^{-1} \circ f \circ {}^s(f^{-1}) \circ {}^s b.$$

So

$$(f \circ q) \circ {}^s(q^{-1}) \circ {}^s(f^{-1}) = b^{-1} \circ f \circ {}^s(f^{-1}) \circ {}^s b,$$

hence

$${}^s(q^{-1}) \circ {}^s(f^{-1}) \circ {}^s(b^{-1}) \circ {}^s f = q^{-1} \circ f^{-1} \circ b^{-1} \circ f,$$

i.e.

$$^s(q^{-1} \circ f^{-1} \circ b^{-1} \circ f) = q^{-1} \circ f^{-1} \circ b^{-1} \circ f.$$

Let $q' = q^{-1} \circ f^{-1} \circ b^{-1} \circ f$, then we have an isomorphism from $F(Y)$ to $F(Y_1)$ and $^sq' = q'$ for any s in G. Since F is a coefficient extension, $q' = F(w)$ for some isomorphism $w : Y \xrightarrow{\cong} Y_1$. Hence $[Y] = [Y_1]$. □

Proposition 4.2.3. *Let L be a field and $F : \mathfrak{Rep}_L^{G_k} \to \mathfrak{Rep}_L^{G_K}$ be the coefficient extension defined in Theorem* 4.1.7. *Denote the image of any element $s \in G_k$ in the canonical map $G_k \to G \cong G_k/G_K = \mathrm{Gal}(K/k)$ by $\overline{s}$. Then for any object $X = (V, \phi)$ in $\mathfrak{Rep}_L^{G_k}$ and $[\sigma] \in H^1(G, \mathrm{Aut}(F(X)))$, the map*

$$\phi^\sigma : \ G_k \to \mathrm{Aut}(V), \ s \mapsto \sigma(\overline{s}) \circ \phi(s)$$

is a group homomorphism. So (V, ϕ^σ) is an object in $\mathfrak{Rep}_L^{G_k}$, denoted by X^σ, and the equivalence class of X^σ, $[X^\sigma]$ is a $\mathfrak{Rep}_L^{G_K}/\mathfrak{Rep}_L^{G_k}$-form of X. Furthermore the map

$$\nu : \ H^1(G, \mathrm{Aut}(F(X))) \to E(\mathfrak{Rep}_L^{G_K}/\mathfrak{Rep}_L^{G_k}, X),$$

defined by

$$[\sigma] \mapsto [X^\sigma], \forall [\sigma] \in H^1(G, \mathrm{Aut}(F(X)))$$

is a bijection whose inverse is γ defined in Theorem 4.2.2.

Proof. For any s, t in G_k,

$$\begin{aligned}
\phi^\sigma(st) &= \sigma(\overline{s}\,\overline{t}) \circ \phi(st) \\
&= \sigma(\overline{s}) \circ {}^{\overline{s}}\sigma(\overline{t}) \circ \phi(s) \circ \phi(t) \\
&= \sigma(\overline{s}) \circ (\phi(s) \circ \sigma(\overline{t}) \circ \phi(s)^{-1}) \circ (\phi(s) \circ \phi(t)) \\
&= (\sigma(\overline{s}) \circ \phi(s)) \circ (\sigma(\overline{t}) \circ \phi(t)) \\
&= \phi^\sigma(s) \circ \phi^\sigma(t).
\end{aligned}$$

This proves ϕ^σ is a group homomorphism.

Suppose $s \in G_K$, then $\overline{s} = \overline{1}$, the unity in G. So when s is in G_K,

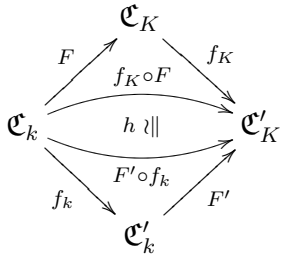
$$\phi^\sigma(s) = \sigma(\overline{1}) \circ \phi(s) = 1_{\mathrm{Aut}(F(X))} \circ \phi(s) = \phi(s).$$

Hence $(V, \phi^\sigma|G_K) = (V, \phi|G_K)$ and so $[X^\sigma]$ is a $\mathfrak{Rep}_L^{G_K}/\mathfrak{Rep}_L^{G_k}$-form of X and 1_V can be taken as an isomorphism in $\mathfrak{Rep}_L^{G_K}$ from X^σ to X. Consequently, it follows from Theorem 4.2.2 that for any $s \in G_k$,

$$\begin{aligned}
\gamma(X^\sigma)(\overline{s}) &= 1_V \circ {}^{\overline{s}}(1_V^{-1}) \\
&= 1_V \circ \phi^\sigma(s) \circ 1_V \circ \phi(s)^{-1} \\
&= \sigma(s) \circ \phi(s) \circ \phi(s)^{-1} \\
&= \sigma(s).
\end{aligned}$$

So $\gamma(X^\sigma) = [\sigma]$. □

Theorem 4.2.4. *Let $F:\ \mathfrak{C}_k \to \mathfrak{C}_K$ and $F':\ \mathfrak{C}'_k \to \mathfrak{C}'_K$ be two coefficient extensions and (f_k, f_K, h) be a morphism from F to F'.*



Then we have the following commutative diagram:

$$\begin{array}{ccc} E(\mathfrak{C}_K/\mathfrak{C}_k, X) & \xrightarrow{\varphi:\ [Y]\mapsto[f_k(Y)]} & E(\mathfrak{C}'_K/\mathfrak{C}'_k, f_k(X)) \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \gamma} \\ H^1(G, \mathrm{Aut}(F(X))) & \xrightarrow[\psi:\ [\sigma]\mapsto[h\circ f_K\circ\sigma]]{} & H^1(G, \mathrm{Aut}(F'\circ f_k(X))). \end{array}$$

Proof. φ is well-defined. Let Y be a $\mathfrak{C}_K/\mathfrak{C}_k$-form of X, so there is an isomorphism $\omega:\ F(Y) \xrightarrow{\cong} F(X)$ in $\mathfrak{C}_K$. Hence $f_K(\omega)$ is an isomorphism from $f_K(F(Y))$ to $f_K(F(x))$ in $\mathfrak{C}'_K$. Since h is an isomorphism between $f_K \circ F$ and $F' \circ f_k$, h induces an isomorphism from $f_K(F(U))$ to $F'(f_k(U))$ for any object U in $\mathfrak{C}_k$, denoted by h_U. Then the sequence

$$F'(f_k(Y)) \xrightarrow{h_Y^{-1}} f_K(F(Y)) \xrightarrow{f_K\circ\omega} f_K(F(X)) \xrightarrow{h_X} F'(f_k(X))$$

gives an isomorphism from $F'(f_k(Y))$ to $F'(f_k(X))$ in $\mathfrak{C}'_K$. So $[f_k(Y)]$ is a $\mathfrak{C}'_K/\mathfrak{C}'_k$-form of $f_k(X)$.

Suppose Y_1 is another object in $\mathfrak{C}_k$ isomorphic to Y in $\mathfrak{C}_k$ with an isomorphism $\mu:\ Y_1 \to Y$. Then $f_k(\mu):\ f_k(Y_1) \to f_k(Y)$ is an isomorphism in $\mathfrak{C}'_k$.

Take $Y = X$, then $\varphi([X]) = [f_k(X)]$, i.e. φ is a well-defined map of pointed sets.

Next we prove ψ is also well-defined. For any s and t in G,

$$\begin{aligned} h \circ f_K \circ \sigma(st) &= h \circ f_K \circ (\sigma(s) \circ {}^s\sigma(t)) \\ &= (h \circ f_K \circ \sigma(s)) \circ (h \circ f_K \circ {}^s\sigma(t)) \\ &\overset{G\text{-equivariant}}{=} (h \circ f_K \circ \sigma(s)) \circ {}^s(h \circ f_K \circ \sigma(t)). \end{aligned}$$

So $h \circ f_K \circ \sigma$ satisfies cocycle condition.

Let σ' be another cocycle with $\sigma \sim \sigma'$. This implies for any $s \in G$, $\sigma'(s) = b^{-1} \circ \sigma(s) \circ {}^s b$. Hence

$$\begin{aligned} h \circ f_K \circ \sigma'(s) &= h \circ f_K \circ (b^{-1} \circ \sigma(s) \circ {}^s b) \\ &= (h \circ f_K \circ b^{-1}) \circ (h \circ f_K \circ \sigma(s)) \circ (h \circ f_K \circ {}^s b) \\ &\overset{G\text{-equivariant}}{=} (h \circ f_K \circ b)^{-1} \circ (h \circ f_K \circ \sigma(s)) \circ {}^s(h \circ f_K \circ b). \end{aligned}$$

So $(h \circ f_K \circ \sigma')$ is cohomologous to $(h \circ f_K \circ \sigma)$. Suppose σ is the trivial cocycle in $Z^1(G, \mathrm{Aut}(F(X))$, then clearly $(h \circ f_K \circ \sigma)$ is also the trivial cocycle in $Z^1(G, \mathrm{Aut}(F'(f_k(X))))$.

Finally,

$$\begin{aligned} \gamma \circ \varphi([Y])(s) &= \gamma([f_k(Y)])(s) \\ &= (h_X \circ f_K \circ \omega \circ h_Y^{-1}) \circ {}^s((h_X \circ f_K \circ \omega \circ h_Y^{-1})^{-1}) \\ &= h_X \circ f_K \circ \omega \circ h_Y^{-1} \circ h_Y \circ {}^s(\omega^{-1}) \\ &= h_X \circ f_K \circ \omega \circ {}^s(\omega^{-1}), \end{aligned}$$

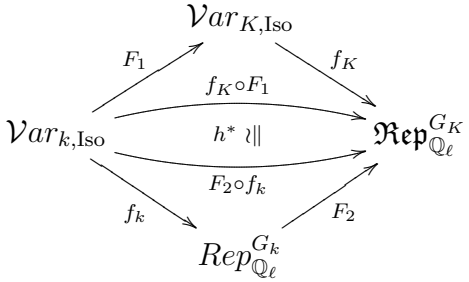
and

$$\psi \circ \gamma([Y])(s) = h_X \circ f_K \circ \omega \circ {}^s(\omega^{-1})$$

imply $\gamma \circ \varphi = \psi \circ \gamma$. □

In particular, we have:

Corollary 4.2.5. *Let* $F_1 : \mathcal{V}ar_{k,Iso} \to \mathcal{V}ar_{K,Iso}$ *and* $F_2 : \mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_k} \to \mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_K}$ *be two coefficient extensions as defined in Theorem* 4.1.5 *and Theorem* 4.1.7 *respectively and* (f_k, f_K, h^*) *be the morphism from* F_1 *to* F_2 *defined in Theorem* 4.1.9*:*



Then we have the following commutative diagram:

$$\begin{array}{ccc} E(\mathcal{V}ar_{K,\mathrm{Iso}}/\mathcal{V}ar_{k,\mathrm{Iso}}, X) & \xrightarrow{\eta:\,[Y]\mapsto[H^i(\overline{Y}_{\acute{e}t},\mathbb{Q}_\ell)]} & E(\mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_K}/\mathfrak{Rep}_{\mathbb{Q}_\ell}^{G_k}, H^i(\overline{X}_{\acute{e}t},\mathbb{Q}_\ell)) \\ \downarrow \gamma & & \downarrow \gamma=\nu^{-1} \quad \uparrow \nu \\ H^1(G, \mathrm{Aut}_K(X_K)) & \xrightarrow[\varphi:\,[\sigma]\mapsto[h^*\circ f_K\circ\sigma]]{} & H^1(G, \mathrm{Aut}_{G_K}(H^i(\overline{X}_{\acute{e}t},\mathbb{Q}_\ell))) \end{array}$$

where $X_K = X \times_k K$, $\mathrm{Aut}_{G_K}(H^i(\overline{X}_{\acute{e}t}, \mathbb{Q}_\ell))$ *is the set of all linear transformations of* $H^i(\overline{X}_{\acute{e}t}, \mathbb{Q}_\ell)$ *as* $\mathbb{Q}_\ell$*-vector space which are compatible with* G_K *action. For any* $g \in G$, $h^* \circ f_K \circ \sigma(g) = h^* \circ (\sigma(g)^*)^{-1} = h^* \circ (\sigma(g)^{-1})^* = (\sigma(g)^{-1} \circ h)^*$*, here we identify*

$$\sigma(g) : \ X_K \to X_K$$

with

$$\sigma(g) \times_K 1_K : \overline{X}_K = X_K \times_K \overline{K} \to X_K \times_K \overline{K} = \overline{X}_K.$$

For any smooth projective variety X, suppose we have a G_k-action ν_X on $H^i(\overline{X}_{\acute{e}t}, \mathbb{Q}_\ell)$:

$$\nu_X : \ G_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(H^i(\overline{X}_{\acute{e}t}, \mathbb{Q}_\ell)).$$

For any $\mathcal{V}ar_K/\mathcal{V}ar_k$-form Y of X, we have $\gamma([Y]) \in H^1(G, \mathrm{Aut}_K(X_K))$, denote $\gamma([Y])$ by $[c_Y]$ for some $c_Y \in Z^1(G, \mathrm{Aut}_K(X_K))$. Since X_K is isomorphic to Y_K over K, $H^i(\overline{X}, \mathbb{Q}_\ell) \cong H^i(\overline{Y}, \mathbb{Q}_\ell)$ as $\mathbb{Q}_\ell$-vector space. By Proposition 4.2.3, the G_k action on $H^i(\overline{Y}_{\acute{e}t}, \mathbb{Q}_\ell)$, ν_Y which is induced by Y and ν_X is:

$$\nu_Y : \ G_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(H^i(\overline{Y}_{\acute{e}t}, \mathbb{Q}_\ell)), \ \nu_Y = \nu_X^{\gamma\circ\eta(Y)}.$$

But from Corollary 4.2.5, $\varphi \circ \gamma = \gamma \circ \eta$, hence

$$\begin{aligned}\nu_Y =& \nu_X^{\varphi\circ\gamma(Y)} \\ =& \nu_X^{\varphi(c_Y)}.\end{aligned}$$

For any $g \in G_k$, let $\overline{g}$ be the image of g in G in the canonical map $G_k \to G_k/G_K = G$, then

$$\begin{aligned}\nu_Y(\overline{g}) =& \nu_X^{\varphi(c_Y)}(\overline{g}) \\ =& ((\varphi(c_Y))(\overline{g})) \circ \nu_X(\overline{g}) \\ =& h^* \circ f_K \circ c_Y(\overline{g}) \circ \nu_X(\overline{g}).\end{aligned}$$

Since $h = 1$, we have

$$\begin{aligned}\nu_Y(\overline{g}) =& f_K \circ c_Y(\overline{g}) \circ \nu_X(\overline{g}) \\ =& (c_Y(\overline{g})^{-1})^* \circ \nu_X(\overline{g})\end{aligned}$$

In particular, Suppose $k = \mathbb{F}_q$ with Frobenius map

$$f : \ \overline{k} \to \overline{k}, \ a \mapsto a^q$$

in G_k, then $\mathrm{Fr}^*_{r_Y} = (c_Y(\overline{f}^{\,-1})^{-1})^* \circ \mathrm{Fr}^*_{r_X}$. But $c_Y(\overline{f}^{\,-1}) \circ {}^{\overline{f}^{-1}}c_Y(\overline{f}) = c_Y(\overline{f}^{\,-1} \circ \overline{f}) = c_Y(1_G) = 1_{X_K}$. So we have proved the following main result:

Theorem 4.2.6. *Using notations above, we have*

$$\mathrm{Fr}^*_{r_Y} = ({}^{\overline{f}^{-1}}c_Y(\overline{f}))^* \circ \mathrm{Fr}^*_{r_X}. \tag{4.3}$$

4.3 Forms of Quasi-projective Varieties

Let X be an object in $\mathcal{V}ar_k$, where k is a field. Let K/k be a Galois field extension. Then a $\mathcal{V}ar_K/\mathcal{V}ar_k$-form of X, which is also called a K/k-form for short, is just an object Y in $\mathcal{V}ar_k$, such that $Y \times_k K \cong X \times_k K$ as K-varieties. The set of all equivalence classes of K/k-forms of X is denoted by $E(K/k, X)$. This section will build a bijection between $E(K/k, X)$ and $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(X \times_k K))$. But we will begin by giving some concrete examples.

Example 4.3.1. *Consider the projective variety* $V = \mathrm{Proj}\,\mathbb{R}[x, y, z]/(x^2 + y^2 + z^2)$, *it has no point defined over* $\mathbb{R}$ *and therefore* $V \ncong \mathbb{P}^1$ *over* $\mathbb{R}$ (*denoted by* $\mathbb{P}^1_{\mathbb{R}}$). *But when base field* $\mathbb{R}$ *is extended to* $\mathbb{C}$, *clearly we have*

$$V \otimes_{\mathbb{R}} \mathbb{C} \cong \mathrm{Proj}\,\mathbb{C}[x, y, z]/(x^2 + y^2 + z^2) \cong \mathbb{P}^1_{\mathbb{C}} = \mathbb{P}^1_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}.$$

This implies V *is a form of* $\mathbb{P}^1_{\mathbb{R}}$ *over* $\mathbb{R}$.

Similarly, it is easy to verify that the affine scheme $\operatorname{Spec}\mathbb{Q}[x]/(x^2+1)$ *over* $\mathbb{Q}$ *is a form of any affine scheme* $\operatorname{Spec}\mathbb{Q}[x]/(x^2+bx+c)$ *for some* $b, c \in \mathbb{Q}$ *such that* $b^2 - 4c \neq 0$.

Example 4.3.2. *Given the elliptic curve*

$$E: \ y^2 = x^3 + 1 \tag{4.4}$$

defined over $\mathbb{F}_5$*, the elliptic curve*

$$E': \ 2y^2 = x^3 + 1 \tag{4.5}$$

is isomorphic to E *over* $\mathbb{F}_5(\sqrt{2}) \cong \mathbb{F}_{5^2}$*. On the other hand,* E' *is equivalent to* $y^2 = \frac{1}{2}x^3 + \frac{1}{2}$*, which in turn is equivalent to* $y^2 = 3x^3 + 3$ *because* $2^{-1} = 3$ *in* $\mathbb{F}_5$*. Since* $2^3 = 3$ *in* $\mathbb{F}_5$*,* E' *is isomorphic to the elliptic curve*

$$E'': \ y^2 = x^3 + 3. \tag{4.6}$$

The j*-invariants* $j(E) = j(E') = j(E'') = 0$*, so according to the result in* [12], p.71*,* $E \cong E''$ *over* $\mathbb{F}_5$ *if and only if* $\mathbb{F}_5$ *contains a sixth root of* 3*. Since there is no element in* $\mathbb{F}_5$ *whose square is* 3*, there is no element in* $\mathbb{F}_5$ *whose sixth power is* 3*. Hence* E *and* E'' *(or* E'*) are not isomorphic over* $\mathbb{F}_5$.

The following theorem gives the classification of K/k-forms of a quasi-projective variety, where K/k is a Galois extension.

Theorem 4.3.3. *Let* K/k *be a Galois extension with Galois group* $G = \operatorname{Gal}(K/k)$*. Let* $\mathcal{V}ar_k$ *be the category of quasi-projective varieties defined over* k *with morphisms over* k *and* $\mathcal{V}ar_K$ *be the category of quasi-projective varieties defined over* K *with*

morphisms over K. Let the functor $F : \mathcal{V}ar_k \to \mathcal{V}ar_K$ be defined as follows:

$$F(X) = X_K := X \times_k K,$$

and

$$F(X \xrightarrow{f} Y) = (X_K \xrightarrow{f \times 1_{Spec\, K}} Y_K).$$

Then for any object X in $\mathcal{V}ar_k$, there is a natural bijection between the set of isomorphism equivalence classes of K/k-forms (i.e. $\mathcal{V}ar_K/\mathcal{V}ar_k$-forms) and $H^1(G, \mathrm{Aut}(X_K))$, i.e.

$$E(K/k, X) \cong H^1(G, \mathrm{Aut}(X_K)).$$

Proof. From Theorem 4.1.5, F is a coefficient extension from k to K. So from Theorem 4.2.2, one has the injective map:

$$\gamma : E(K/k, X) \to H^1(G, \mathrm{Aut}(X_K)),\ [Y] \mapsto [\tau_Y],\ \forall [Y] \in E(K/k, X),$$

where τ_Y is defined by

$$\tau_Y : G \to \mathrm{Aut}(X_K),\ s \mapsto f_Y \circ {}^s(f_Y^{-1}),\ \forall s \in G,$$

where f_Y is an isomorphism $F(Y) = Y_K \to X_K = F(X)$ in $\mathcal{V}ar_K$. Now it is enough to show γ is surjective.

Suppose $[c]$ is an element of $H^1(G, \mathrm{Aut}(X_K))$ with a representative $c \in Z^1(G, \mathrm{Aut}(X_K))$. For any $g \in G$, g induces an isomorphism on $\mathrm{Spec}\, K$, which in turn induces an isomorphism on $X_K = X \times_k K$, which is denoted by g^*. Hence we obtain an action of $G = \mathrm{Gal}(K/k)$ on $X_K = X \times_k K$ by $c(g^{-1}) \circ g^*$:

$$c(1) \circ 1^* = 1_{X_K} \circ 1_{X_K} = 1_{X_K},$$

and for any $g_1, g_2 \in G$,

$$\begin{aligned} c((g_1g_2)^{-1}) \circ (g_1g_2)^* &= c(g_2^{-1}g_1^{-1}) \circ g_2^* \circ g_1^* \\ &= c(g_2^{-1}) \circ {}^{g_2^{-1}}c(g_1^{-1}) \circ g_2^* \circ g_1^* \\ &= c(g_2^{-1}) \circ g_2^* \circ c(g_1^{-1}) \circ (g_2^*)^{-1} \circ g_2^* \circ g_1^* \\ &= (c(g_2^{-1}) \circ g_2^*) \circ (c(g_1^{-1}) \circ g_1^*). \end{aligned}$$

Based on this action of G on X_K, since X_K is a quasi-projective variety, the quotient X_K/G is also a quasi-projective variety defined over k and X_K/G is a K/k-form of X by Weil's descent theorem ([28], Proposition 1). Suppose we prove that $\gamma(X_K/G) = [c]$, then if $[c] = [c']$ for some $c' \in Z^1(G, \mathrm{Aut}(X_K))$, then under c', we have another G-action on X_K, and denote by Y the quotient variety of X_K under this G-action. Then we have $\gamma(Y) = [c'] = [c]$ and so the injectivity of γ implies $Y = X_K/G$. Hence X_K/G is independent to the choice of representative of $[c]$, which implies that X_K/G is well-defined. Now we start to prove $\gamma(X_K/G) = [c]$.

Denote X_K/G by $\mathcal{X}$. From the definition of γ, $\gamma([\mathcal{X}]) = [\tau_{\mathcal{X}}]$, where $[\tau_{\mathcal{X}}]$ is defined by

$$\tau_{\mathcal{X}} : G \to \mathrm{Aut}(X_K),\ s \mapsto f \circ {}^s(f^{-1}),\ \forall s \in G,$$

where f is an isomorphism $\mathcal{X} \times_k K \to X \times_k K$, where $\mathcal{X}_K = \mathcal{X} \times_k K$. Hence for any element $s \in G$,

$$\begin{aligned} \tau_{\mathcal{X}}(s) &= f \circ {}^s(f^{-1}) \\ &= f \circ (s^{-1} \circ f^{-1} \circ s^*). \end{aligned}$$

The left s is the action on $\mathcal{X}_K$ defined near the beginning of the proof, hence

$$\tau_{\mathcal{X}}(s) = f \circ c(s) \circ (s^*)^{-1} \circ f^{-1} \circ s^* = f \circ c(s) \circ {}^s(f^{-1}),$$

so

$$\tau_{\mathcal{X}} \sim c.$$

□

CHAPTER 5
Forms and Zeta Functions — Some General Results and Examples

In this section, $k = \mathbb{F}_q$ be a finite field with q elements, and K/k be a finite Galois extension of degree r, i.e. $K = \mathbb{F}_{q^r}$.

5.1 General Results

From the formula (4.3), we have the following theorem regarding the connection of the zeta function of a smooth projective variety and those of its forms.

Theorem 5.1.1. *Let X be a smooth projective variety of dimension d defined over a finite field k and let Y be a k-form of X, i.e. Y is isomorphic to X over some finite separable field extension K of k. Let Y correspond to $[c_Y]$ in $H^1(G, \mathrm{Aut}_K(X))$. Let the zeta function of X be*

$$Z(X/k, T) = \prod_{i=0}^{d} P_i(X, T)^{(-1)^{i+1}},$$

where $P_i(X,T) = \det(1 - (\mathrm{Fr}_r^j)^* T \big| H^i(\overline{X}, \mathbb{Q}_\ell))$, $i = 1, 2, \ldots, 2d$. Then

$$Z(Y/k, T) = \prod_{i=0}^{d} P_i'(X, T)^{(-1)^{i+1}},$$

where $P_i'(X,T) = \det(1 - ((\overline{f}^{-1} c_Y(\overline{f}))^* \circ \mathrm{Fr}_r^*)^i T \big| H^i(\overline{X}, \mathbb{Q}_\ell))$, $i = 0, 1, 2, \ldots, 2d$. Here $f \in G_k$ is the Frobenius map $a \mapsto a^q$, $\forall a \in \overline{k}$ and $\overline{f}$ is the image of f in the canonical map $G_k \to G = G_k/G_K$.

5.2 Elliptic Curves

In the case of elliptic curves, the first étale cohomology $H^1(\overline{E}_{\acute{e}t}, \mathbb{Q}_\ell)$ of E/k corresponds to $V_\ell^*(E)$, which is the dual of $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, where $T_\ell(E)$ is the Tate module of E/k and ℓ is any prime number not equal to p. Since for any positive integer m prime to p, the m-torsion subgroup of E, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $V_\ell(E)$ (and $V_\ell^*(E)$) is a $\mathbb{Q}_\ell$-vector space of dimension 2. The zeta function of E/k has the following expression:

$$\begin{aligned} Z(E,T) &= \frac{\det(1 - T\mathrm{Fr}_r^* \big| V_\ell^*(E))}{(1-T)(1-qT)} \\ &= \frac{1 - \mathrm{Tr}(\mathrm{Fr}_r^*)T + qT^2}{(1-T)(1-qT)}, \end{aligned} \tag{5.1}$$

where Fr_r is the relative Frobenius map on E. For $\mathrm{Aut}_{\overline{k}}(E)$, we have the following result:

Theorem 5.2.1. ([12], p.70-75) *Suppose E/k is an elliptic curve, then*

$$\mathrm{Aut}_{\overline{k}}(E) \cong \begin{cases} \mu_2 & j(E) \neq 0, 1728 \text{ and } char(k) \neq 2, \\ \mu_4 & j(E) = 1728 \text{ and } char(k) \neq 2, 3, \\ \mu_6 & j(E) = 0 \text{ and } char(k) \neq 2, 3, \\ \mu_2 & j(E) \neq 0 \text{ and } char(k) = 2, \\ \mathbb{Z}/3\mathbb{Z} \rtimes \mu_4 & j(E) = 0 \text{ and } char(k) = 3, \\ Q_8 \rtimes \mu_3 \cong \mathrm{SL}_2(\mathbb{F}_3) & j(E) = 0 \text{ and } char(k) = 2. \end{cases}$$

where Q_8 is the quaternion group of order 8 and μ_n is the subgroup of n-th root of unity in $\overline{k}^\times$. Further, in the case where $Aut_{\overline{k}}(E) \cong \mu_{2l}$, $(l = 1, 2 \text{ or } 3)$ and

$\mathrm{char}(k) \neq 2$, *an automorphism* $\rho \in Aut_{\overline{k}}(E)$ *is defined over* k *if and only if* $\rho \in k$ *when* ρ *is considered as an element in* μ_{2l}.

In order to determine the Galois action on $\mathrm{Aut}_{\overline{k}}(E)$ when $j(E) = 0$ and $\mathrm{char}(k) = 2$ or 3, or $j(E) \neq 0$ and $\mathrm{char}(k) = 2$, we need to explicitly write elements in $\mathrm{Aut}_{\overline{k}}(E)$. When $j(E) = 0$ and $\mathrm{char}(k) = 3$, the Weierstrass form of E can be written as:

$$y^2 = x^3 + a_4x + a_6,$$

for some a_4 and $a_6 \in k$ with $a_4 \neq 0$, then([12], p.73)

$$\mathrm{Aut}_{\overline{k}}(E) = \{(0, \pm 1), (\pm\alpha, \pm 1), (\beta, \pm i), (\beta \pm \alpha, \pm i)\},$$

where α is a solution of the equation $r^2 + a_4 = 0$ and β is a solution of the equation $r^3 + a_4r + 2a_6 = 0$ (from $\mathrm{char}k = 3$, $(\beta \pm \alpha)^3 + a_4(\beta \pm \alpha) + 2a_6 = \beta^3 \pm \alpha^3 + a_4(\beta \pm \alpha) + 2a_6 = (\beta^3 + a_4\beta + 2a_6) \pm \alpha(\alpha^2 + a_4) = 0$).

When $j(E) = 0$ and $\mathrm{char}(k) = 2$, the Weierstrass form of E can be written as:

$$y^2 + a_3y = x^3 + a_4x + a_6,$$

for some a_3, a_4 and $a_6 \in k$ with $a_3 \neq 0$, then([12], p.75),

$$\mathrm{Aut}_{\overline{k}}(E) = \{(\beta, \gamma) \,|\, \gamma^3 = 1, \beta^2 + a_3\beta + \delta^6 + \delta^2a_4 = 0 \text{ where } \delta^4 + a_3\delta + a_4 + \gamma a_4 = 0\}.$$

When $j(E) \neq 0$ and $\mathrm{char}(k) = 2$, the Weierstrass form of E can be written as:

$$y^2 + xy = x^3 + a_2x^2 + a_6,$$

for some $a_2, a_6 \in k$ with $a_6 \neq 0$. Then $\mathrm{Aut}_{\overline{k}}(E)$ is the roots of the equation $s^2+s=0$ ([12], p.75).

Theorem 5.2.2. ([25], p.329) *Suppose the elliptic curves E/k and E_1/k satisfy $j(E) = j(E_1)$, then E and E_1 are isomorphic over a Galois extension K/k of degree dividing 24 and if $j(E) \neq 0, 1728$, the extension K/k can be chosen to have degree 2.*

Now suppose $\mathrm{char}(k) \neq 2, 3$. When $j(E) \neq 0, 1728$, $\mathrm{Aut}_{\overline{k}}(E) = \mu_2$ and any $\overline{k}/k$-form E_1 is isomorphic with E over $K = \mathbb{F}_{q^2}$ and can be described by $H^1(\mu_2, \mu_2)$. But since $\mu_2 = \{1, -1\} \subset k$, which implies G acts on μ_2 trivially, $H^1(\mu_2, \mu_2) = \mathrm{Hom}(\mu_2, \mu_2) = \{1_{\mu_2}, c\}$, where 1_{μ_2} is the identity map on μ_2 and c maps every element in μ_2 to 1. Since G acts on μ_2 trivially, (4.3) becomes

$$\mathrm{Fr}^*_{r_{E_1}} = (c_{E_1}(\overline{f}))^* \circ \mathrm{Fr}^*_{r_E} \tag{5.2}$$

Clearly, $c_{E_1}(\overline{f}) = 1$ or -1, whose actions on $V^*_\ell(E)$ correspond to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ respectively for any $\mathbb{Q}_\ell$-basis of $V^*_\ell(E)$.

From Weil's conjecture, we can choose a $\mathbb{Q}_\ell$-basis of $V^*_\ell(E)$ such that the action of $\mathrm{Fr}^*_{r_E}$ on $V^*_\ell(E)$ is $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right)$, for some algebraic number α such that

$$1 - \mathrm{Tr}(\mathrm{Fr}^*_{r_E})T + qT^2 = (1 - \alpha T)(1 - \overline{\alpha}T).$$

So from(5.2), the matrix for $\mathrm{Fr}^*_{r_{E_1}}$ is $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -\alpha & 0 \\ 0 & -\overline{\alpha} \end{smallmatrix}\right)$. Consequently, the zeta function of E_1/k is

$$Z(E_1, T) = \frac{1 \pm \mathrm{Tr}(\mathrm{Fr}^*_{r_E})T + qT^2}{(1 - T)(1 - qT)}.$$

Hence when $E_1 \ncong E$,

$$Z(E_1, T) = \frac{1 + \mathrm{Tr}(\mathrm{Fr}^*_{r_E})T + qT^2}{(1-T)(1-qT)}.$$

When $j(E) = 1728$, $\mathrm{Aut}_{\overline{k}}(E) \cong \mu_4$. The Weierstrass equation of E/k can be written as ([12], p.71):

$$y^2 = x^3 + a_4 x,$$

for some $a_4 \in k^\times$. Then E/k is supersingular if and only if the coefficient of x^{p-1} in $(x^3 + a_4 x)^{\frac{p-1}{2}}$ is 0 ([25], p.140). On the other hand,

$$(x^3 + a_4 x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}}(x^2 + a_4)^{\frac{p-1}{2}},$$

so when $p \not\equiv 1 (\mathrm{mod}\ 4)$, the coefficient of x^{p-1} in $(x^3 + a_4 x)^{\frac{p-1}{2}}$ is 0, and when $p \equiv 1 (\mathrm{mod}\ 4)$, the coefficient of x^{p-1} in $(x^3 + a_4 x)^{\frac{p-1}{2}}$ is $\binom{\frac{p-1}{2}}{\frac{p-1}{4}} a_4$ which is not zero because $a_4 \neq 0$ and $p \nmid \binom{\frac{p-1}{2}}{\frac{p-1}{4}}$. Hence E/k is supersingular if and only if $p \not\equiv 1 (\mathrm{mod}\ 4)$. Suppose $p \equiv 1 (\mathrm{mod}\ 4)$, then

$$(-1)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p).$$

So from Euler's criteria for quadratic residues, there exists $x \in \mathbb{F}_p \subset k$, such that $x^2 + 1 = 0$, so $\mu_4 \subset k$. Therefore if $\mu_4 \not\subset k$, $p \not\equiv 1 (\mathrm{mod}\ 4)$ and consequently E/k is supersingular.

For any $c \in H^1(\mathrm{Gal}(\overline{k}/k), \mu_4)$, suppose $c(f) = i \in \mu_4$, where $i^2 = -1$ (the case $c(f) = \pm 1$ is trivial). When $\mu_4 \subset k$, ${}^{f^{-1}}c(f) = i$. Clearly we can choose the prime number ℓ in $\mathbb{Q}_\ell$ such that $4 | \ell - 1$, then $\mu_4 \subset \mathbb{Z}_\ell$. So when i is considered as an element in $\mathrm{Aut}_{\overline{k}}(E)$, the characteristic polynomial of i is $x^2 + 1$ over $V_\ell^*(E)$, and then there exists a basis e_1, e_2 of $V_\ell^*(E)$, such that action of i on $V_\ell^*(E)$ is the matrix $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$.

Since f^* is $\mathbb{Z}_\ell$-linear and $i \in \mathbb{Z}_\ell$, when i is defined over k, for any $v \in V_\ell^*(E)$,

$$({}^i f^*)(v) = f^*(iv) = i(f^*(v)).$$

So

$$i \circ f^* = f^* \circ i.$$

The following lemma is easy to prove:

Lemma 5.2.3. *Let V be a vector space over a field of finite dimension n. Let α and β be two linear transformations on V such that $\alpha \circ \beta = \beta \circ \alpha$. Suppose that α can be represented by a diagonal matrix in some basis, and β can be represented by a diagonal matrix in some (maybe different) basis, then there exists a basis such that in that basis, both α and β can also be represented by diagonal matrices.*

From this lemma, we have that f^* can also be represented by a diagonal matrix $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right)$ for some $\alpha \in \mathbb{C}$. Consequently

$$\mathrm{Fr}^*_{r_{E_1}} = \begin{pmatrix} \alpha i & 0 \\ 0 & -\overline{\alpha} i \end{pmatrix}.$$

Similarly we can deal with the case where $c(f) = -i$ and hence we have the following result:

Theorem 5.2.4. *Let k be a finite field $\mathbb{F}_q$ with $\mathrm{char}(k) \neq 2, 3$ and $G = \mathrm{Gal}(\overline{k}/k)$. Let E be an elliptic curve defined over k and $j(E) = 1728$ which implies $\mathrm{Aut}_{\overline{k}}(E) \cong \mu_4 = \{\pm i, \pm 1\}$ where $i^2 = -1$. When $\mu_4 \not\subset k$, E is supersingular. When $\mu_4 \subset k$, let*

a form E_1 of E correspond to $c \in H^1(G, \mu_4)$ with $c(f) = \beta \in \mu_4$, we have

$$Z(E_1, T) = \frac{1 - (\alpha\beta + \overline{\alpha\beta})T + qT^2}{(1-T)(1-qT)}.$$

We can deal with the case $j(E) = 0$ using the same technique. Now $\mathrm{Aut}_{\overline{k}}(E) \cong \mu_6 = \{1, -1, \rho, \overline{\rho}, \varrho, \overline{\varrho}\}$, where ρ and $\overline{\rho}$ are the roots of $x^2 - x + 1 = 0$ in $\overline{k}$ and ϱ and $\overline{\varrho}$ are the roots of $x^2 + x + 1 = 0$ in $\overline{k}$. The Weierstrass equation of E/k is

$$y^2 = x^3 + a_6,$$

for some $a_6 \in k^\times$. Then from ([25], p.140, Theorem 4.1), E/k is supersingular if and only if the coefficient of x^{p-1} in $(x^3 + a_6)^{\frac{p-1}{2}}$ is 0. Hence when $p \not\equiv 1 (\mathrm{mod}\ 6)$, the coefficient of x^{p-1} in $(x^3 + a_6)^{\frac{p-1}{2}}$ is 0, and when $p \equiv 1 (\mathrm{mod}\ 6)$, the coefficient of x^{p-1} in $(x^3 + a_6)^{\frac{p-1}{2}}$ is $\binom{\frac{p-1}{2}}{\frac{p-1}{3}} a_6$ which is not zero because $a_6 \neq 0$ and $p \nmid \binom{\frac{p-1}{2}}{\frac{p-1}{3}}$. So E/k is supersingular if and only if $p \not\equiv 1 (\mathrm{mod}\ 6)$. But $p \equiv 1 (\mathrm{mod}\ 6)$ means there exists $a \in \mathbb{F}_p \subset k$, such that $a^2 \equiv -3 (\mathrm{mod}\ p)$. This means each of equations $x^2 - x + 1 = 0$ and $x^2 + x - 1 = 0$ has two distinct roots in $\mathbb{F}_p$, i.e. $\mu_6 \subset k$. Hence if $\mu_6 \not\subset k$, $p \not\equiv 1 (\mathrm{mod}\ 6)$ and consequently E/k is supersingular.

Choose prime number ℓ such that $6 | \ell - 1$ and so $\mu_6 \subset \mathbb{Z}_\ell$. Since $x^2 - x + 1$ is also the characteristic polynomial of ρ and $\overline{\rho}$ over $V_\ell^*(E)$, there exists a basis e_1, e_2 such that the action of ρ on $V_\ell^*(E)$ is $\left(\begin{smallmatrix} \rho & 0 \\ 0 & \overline{\rho} \end{smallmatrix}\right)$. When ρ (so is $\overline{\rho}$) is defined over k, $\rho \circ f^* = f^* \circ \rho$, hence $f^* = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right)$ for some $\alpha \in \mathbb{C}$ and

$$\mathrm{Fr}^*_{r_{E_1}} = \begin{pmatrix} \rho\alpha & 0 \\ 0 & \overline{\rho\alpha} \end{pmatrix}.$$

Consequently we have the following theorem:

Theorem 5.2.5. *Let k be a finite field $\mathbb{F}_q$ with char$(k) \neq 2, 3$ and $G = \mathrm{Gal}(\overline{k}/k)$. Let E be an elliptic curve defined over k and $j(E) = 0$ which implies $\mathrm{Aut}_{\overline{k}}(E) \cong \mu_6 = \{\pm 1, \rho, \overline{\rho}, \varrho, \overline{\varrho}\}$. When $\mu_6 \not\subset k$, E is supersingular. When $\mu_6 \subset k$, let a form E_1 of E correspond to $c \in H^1(G, \mu_6)$ with $c(f) = \beta \in \mu_6$, we have*

$$Z(E_1, T) = \frac{1 - (\alpha\beta + \overline{\alpha\beta})T + qT^2}{(1 - T)(1 - qT)}.$$

When $\mathrm{char}(k) \neq 2, 3$, we can assume E/k has the Weierstrass equation: $y^2 = x^3 + Ax + B$ for some $A, B \in k$. Then the twisted form E_1 has one of the following expressions ([25], p.306-309):

$$E_1 : \begin{cases} dy^2 = x^3 + Ax + B & \text{for each } d(\mathrm{mod}\ k^{\times 2}) \text{ when } j(E) \neq 0, 1728\,(AB \neq 0), \\ y^2 = x^3 + dAx & \text{for each } d(\mathrm{mod}\ k^{\times 4}) \text{ when } j(E) = 1728\,(B = 0), \\ y^2 = x^3 + dB & \text{for each } d(\mathrm{mod}\ k^{\times 6}) \text{ when } j(E) = 0\,(A = 0). \end{cases} \tag{5.3}$$

For other cases, we have the following result([12], p.72-76): when $\mathrm{char}(k) = 3$ and $j(E) \neq 0$, the Weierstrass form of E can be written as

$$y^2 = x^3 + a_2x^2 + a_6,$$

for some $a_2, a_6 \in k^{\times}$, then E_1 has the form

$$y^2 = x^3 + da_2x^2 + d^3a_6,$$

for each $d(\text{mod } (k^\times)^2)$. When $\text{char}(k) = 3$ and $j(E) = 0$, the Weierstrass form of E can be written as

$$E : y^2 = x^3 + a_4x + a_6,$$

for some $a_4, a_6 \in k$ with $a_4 \neq 0$, then if $E_1 \ncong E$ over k, E_1 has the form

$$E_1 : y^2 = x^3 + da_4x + a_6',$$

for each $d \in k^\times$ and each $a_6' \in k$ such that not all the following conditions are satisfied:

- d is a forth power u^4 for some $u \in k^\times$.
- $u^6a_6' - a_6 = r^3 + a_4r$ has a solution for r in k.

$E \cong E_1$ over k if and only if both conditions above are satisfied.

When $\text{char}(k) = 2$ and $j(E) \neq 0$, the Weierstrass form of E can be written as:

$$E : y^2 + xy = x^3 + a_2x^2 + a_6,$$

for some $a_2, a_6 \in k$ with $a_6 \neq 0$, then if $E_1 \ncong E_1$ over k, E_1 has the form

$$E_1 : y^2 + xy = x^3 + (a_2 + d)x^2 + a_6,$$

for each $d \in k$ such that $d \neq r^2 + r$ for any $r \in k$ and $E \cong E_1$ over k if and only if $d = r^2 + r$ for some $r \in k$.

When $\text{char}(k) = 2$ and $j(E) = 0$, the Weierstrass form of E can be written as:

$$E_1 : y^2 + a_3y = x^3 + a_4x + a_6,$$

for some a_3, a_4 and $a_6 \in k$ with $a_3 \neq 0$, then if $E_1 \ncong E$ over k, E_1 has the form

$$E_1 : y^2 + da_3y = x^3 + a_4'x + a_6',$$

for all d and $a_4', a_6' \in k$ such that not all the following conditions are satisfied:

- d is a cube u^3 for some $u \in k$
- $s^4 + a_3 s + a_4 + u^4 a_4' = 0$ has a solution for s in k,
- $t^2 + a_3 t + (s^6 + s^2 a_4 + a_6 + u^6 a_6') = 0$ has a solution for t in k.

$E \cong E_1$ over k if and only if all conitions above are satisfied.

Let $\mathrm{char}(k) > 3$. When $j(E) = 1728$, the Weierstrass equation of E can be written as

$$y^2 = x^3 + a_4 x, \tag{5.4}$$

for some $a_4 \in k^\times$. We already know E/k is supersingular if and only if the coefficient of x^{p-1} in $(x^3 + a_4 x)^{\frac{p-1}{2}}$ is 0. From the equality $(x^3 + a_4 x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}}(x^2 - 4)^{\frac{p-1}{2}}$, we know since $a_4 \neq 0$, whether the coefficient of x^{p-1} is zero or not does not depend on the choice of a_4 but only p. Since from (5.3), any form of (5.4) can be written as $y^2 = x^3 + d a_4 x$ for some $d (\mathrm{mod}\ (k^\times)^4)$ and $d \neq 0$. So when (5.4) is supersingular, any form of it is also supersingular. Similarly, when $j(E) = 0$ and E is supersingular, any form of E is also supersingular. Hence we have the following result:

Proposition 5.2.6. *Let $k = \mathbb{F}_q$ with $\mathrm{char}(k) > 3$. Let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then when $j(E) = 0$ or 1728, any form E_1 of E is also supersingular and if $q = p$ for some prime number $p > 3$, $Z(E_1, T) = Z(E, T)$.*

5.3 Brauer-Severi Varieties

Suppose X is a variety over a field k. X is called a Brauer-Severi variety if X/K is isomorphic to $\mathbb{P}^N_K$ for some finite, separable field extension K/k and some positive integer N. K is called a splitting field for X and we say X splits over K. It is easy to prove X is projective and regular ([13], p.23).

Let K/k be a Galois extension and $B^{K/k}_{n-1}$ be the set of all non-isomorphic Brauer-Severi varieties defined over k of dimension $n-1$ that split over K. Then there is a natural bijection:

$$B^{K/k}_{n-1} \xrightarrow{\cong} H^1(\mathrm{Gal}(K/k), \mathrm{PGL}_n(K)).$$

Now let k be a finite field $\mathbb{F}_q$ and X be a Brauer-Severi variety defined over k. The following sequence is exact:

$$1 \to K^\times \to \mathrm{GL}_n(K) \to \mathrm{PGL}_n(K) \to 1.$$

Since $K^\times$ is the center of $\mathrm{GL}_n(K)$ (identify element $\alpha \in K^\times$ with αI_n where I_n is the $n \times n$ unitary matrix in $\mathrm{GL}_n(K)$), so from proposition 3.2.5, we have the exact sequence:

$$H^1(G, \mathrm{GL}_n(K)) \to H^1(G, \mathrm{PGL}_n(K)) \to H^2(G, K^\times),$$

where $G = \mathrm{Gal}(K/k)$. Since K/k is a Galois extension, we have ([23], p.162)

$$H^2(G, K^\times) = 1.$$

It is also well-known that $H^1(G, \mathrm{GL}_n(K)) = 1$ ([24], p.122). Therefore, we have the exact sequence:

$$1 \to H^1(G, \mathrm{PGL}_n(K)) \to 1.$$

So

$$H^1(G, \mathrm{PGL}_n(K)) = 1. \tag{5.5}$$

This implies any Brauer-Severi variety X defined over finite field $k = \mathbb{F}_q$ with dimension n must be isomorphic to $\mathbb{P}^n$ over k. Hence

$$Z(X/k, T) = Z(\mathbb{P}^n(k)) = \prod_{i=0}^{n} \frac{1}{1 - q^i T}.$$

For a general field L (not necessarily finite), we have the following theorem whose proof can be found in [13], p.26:

Theorem 5.3.1. *Let X be a Brauer-Severi variety of dimenstion n over a field L, then $X(L) \neq \emptyset$ if and only if $X \cong \mathbb{P}^n_L$.*

5.4 Tori

The multiplicative group $\mathbb{G}_m$ defined over a field L is $\operatorname{Spec} L[x, y]/(xy - 1)$, which is an algebraic group of dimension 1. An n-dimensional torus T over L ([9], p.11) is an algebraic group isomorphic over L to $\mathbb{G}_m^n = \underbrace{\mathbb{G}_m \times \mathbb{G}_m \times \ldots \times \mathbb{G}_m}_{n \text{ copies}}$.

Let L be a finite field $\mathbb{F}_q$, then $\mathrm{Aut}_{\overline{k}}(\mathbb{G}_m^n) \cong \mathrm{GL}_n(\mathbb{Z})$ ([9], p.14). Therefore all k-forms of $\mathbb{G}_m^n$ is classified by $H^1(G_k, \mathrm{GL}_n(\mathbb{Z}))$, where $G_k = \mathrm{Gal}(\overline{k}/k)$. Since G_k acts trivially on $\mathrm{GL}_n(\mathbb{Z})$, $H^1(G_k, \mathrm{GL}_n(\mathbb{Z}))$ is the set of conjugacy classes of homomorphisms of G_k to $\mathrm{GL}_n(\mathbb{Z})$.

One important case is when $k = \mathbb{F}_p$ for some prime number p. In this case,

$$G_k = \varprojlim_m \mathbb{Z}/m\mathbb{Z} = \widehat{\mathbb{Z}},$$

and hence

$$H^1(G_k, \mathrm{GL}_n(\mathbb{Z})) = \varinjlim_m H^1(\mathbb{Z}/m\mathbb{Z}, \mathrm{GL}_n(\mathbb{Z})).$$

Since the image of any homomorphsim from $\mathbb{Z}/m\mathbb{Z}$ to $\mathrm{GL}_n(\mathbb{Z})$ is a finite cyclic subgroup of $\mathrm{GL}_n(\mathbb{Z})$, it is enough to consider finite order elements in $\mathrm{GL}_n(\mathbb{Z})$. It follows from Jordan-Zassenhaus theorem ([5], p.110), that the number of orders of finite order elements in $\mathrm{GL}_n(\mathbb{Z})$ is finite, say, $n_1, n_2, \ldots, n_s$ and the number of conjugacy classes of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ is finite, which implies the set Θ_n of conjugacy classes of finite order elements in $\mathrm{GL}_n(\mathbb{Z})$ is finite. I use the notation $[A]$ to represent a class in Θ_n with representative A of $\mathrm{GL}_n(\mathbb{Z})$.

Since any group homomorphism γ from $\mathbb{Z}/m\mathbb{Z}$ to $\mathrm{GL}_n(\mathbb{Z})$ is determined by $\gamma(1)$, $H^1(\mathbb{Z}/m\mathbb{Z}, \mathrm{GL}_n(\mathbb{Z}))$ can be canonically identified with $\mathcal{A}_m$ which is defined to be

$$\mathcal{A}_m = \{\, [A] \in \Theta_n \,\big|\, o(A)|m\},$$

where $o(A)$ is the order of the cyclic subgroup of $\mathrm{GL}_n(\mathbb{Z})$ generated by A. So

$$H^1(G_k, \mathrm{GL}_n(\mathbb{Z})) = \varinjlim_{\substack{n_i|m \\ \text{for some} \\ i=1,2,\ldots,s}} \mathcal{A}_m.$$

It is easy to see that

$$\varinjlim_{\substack{n_i|m \\ \text{for some} \\ i=1,2,\ldots,s}} \mathcal{A}_m = \Theta_n,$$

and so

$$H^1(G_k, \mathrm{GL}_n(\mathbb{Z})) = \Theta_n.$$

When $n = 1$, $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$ whose elements are not conjugate with each other. So we have

$$H^1(\mathbb{Z}/m\mathbb{Z}, \mathrm{GL}_1(\mathbb{Z})) = \begin{cases} 1, & m \text{ is odd;} \\ \{\pm 1\}, & m \text{ is even.} \end{cases}$$

Hence one has the following proposition:

Proposition 5.4.1. *Let $K/\mathbb{F}_p$ be a finite Galois extension with $Gal(K/\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z}$ for some odd positive integer m. If there is some affine group scheme $\mathcal{G}$ over $\mathbb{F}_p$ isomorphic to $\mathbb{G}_m$ in K, then $\mathcal{G}$ is isomorphic to $\mathbb{G}_m$ in $\mathbb{F}_p$.*

If m is even, then $H^1(\mathbb{Z}/m\mathbb{Z}, \mathrm{GL}_1(\mathbb{Z})) = \{\pm 1\}$. Let $p > 2$. The element -1 corresponds to a quadratic extension $K = \mathbb{F}_p(\sqrt{d})$ for some $d \in \mathbb{F}_p^\times$ which is not a square in $\mathbb{F}_p$. We have a natural isomorphism f over K : $\mathbb{F}_p[s,t]/(st-1) \xrightarrow{\cong} \mathbb{F}_p(\sqrt{d})[x,y]/(x^2 - dy^2 - 1)$, $\overline{s} \mapsto \overline{x} + \sqrt{d}\overline{y}$, $\overline{t} \mapsto \overline{x} - \sqrt{d}\overline{y}$. Since $p > 2$, f has the inverse f^{-1} over K : $\mathbb{F}_p(\sqrt{d})[x,y]/(x^2 - dy^2 - 1) \xrightarrow{\cong} \mathbb{F}_p[s,t]/(st-1)$, $\overline{x} \mapsto \frac{1}{2}(\overline{s} + \overline{t})$, $\overline{y} \mapsto \frac{1}{2\sqrt{d}}(\overline{s} - \overline{t})$. Take the element 1 in $\mathbb{Z}/m\mathbb{Z}$, then $1 \cdot \sqrt{d} = -\sqrt{d}$. So $f^{-1} \circ {}^1f(\overline{s}) = f^{-1}(\overline{x} - \sqrt{d}\overline{y}) = \frac{1}{2}(\overline{s}+\overline{t}) - \frac{1}{2}(\overline{s}-\overline{t}) = \overline{t}$ and $f^{-1} \circ {}^1f(\overline{t}) = f^{-1}(\overline{x} + \sqrt{d}\overline{y}) = \overline{s}$. Hence f corresponds to the element -1 in $H^1(\mathbb{Z}/m\mathbb{Z}, \mathrm{GL}_1(\mathbb{Z}))$. Hence we have the following result:

Proposition 5.4.2. *Suppose $\mathbb{G}_m = \operatorname{Spec} \mathbb{F}_p[x,y]/(xy-1)$ for some prime number $p \neq 2$, then any non-trivial form of $\mathbb{G}_m$ over $\mathbb{F}_p$ is $\operatorname{Spec} \mathbb{F}_p[x,y]/(x^2 - dy^2 - 1)$ for some $d \in \mathbb{F}_p^\times$ with $d \not\equiv 1 (\mathrm{mod}\ (\mathbb{F}_p^\times)^2)$.*

5.5 Grassmann Varieties

Fix a field k. Let V be a vector space of finite dimension n over k. The Grassmannian $G(d,n)$ is defined as

$$G(d,n) = \{W \big| W \text{ is a subspace of } V,\ \dim V = d\}.$$

Given a basis $e_1, e_2, \ldots, e_n$ for V, $\bigwedge^d V$ has the following canonical basis:

$$\{e_{i_1} \wedge e_{i_2} \wedge \ldots \wedge e_{i_d} \big| 1 \leq i_1 < i_2 < \ldots < i_d \leq n\}. \tag{5.6}$$

For any d-dimensional subspace W of V, let a basis of W be $w_1, w_2, \ldots, w_d$, then $w_1 \wedge w_2 \wedge \ldots \wedge w_d$ can be uniquely expressed as a linear combination of the basis (5.6), i.e.

$$w_1 \wedge w_2 \wedge \ldots \wedge w_d = \sum_{1 \leq i_1 < i_2 < \ldots < i_d \leq n} a_{i_1 i_2 \ldots i_d} e_{i_1} \wedge e_{i_2} \wedge \ldots \wedge e_{i_d}.$$

So we can map W to the coordinates $(a_{i_1 i_2 \ldots i_d})_{1 \leq i_1 < i_2 < \ldots < i_d \leq n}$, this map is called Plücker map. One can prove such map is well-defined up to a constant ([15]) and consequently $G(d,n)$ can be embedded in the projective space $\mathbb{P}(\bigwedge^d V)$ using Plücker map. After such an embedding, $G(d,n)$ can be regarded as a projective algebraic variety and $\dim\,(G(d,n)) = d(n-d)$.

For the number of points $|G(d,n)(\mathbb{F}_q)|$ of $G(d,n)$ over the finite field $k = \mathbb{F}_q$, we have the following result ([15], p.17):

$$|G(d,n)(\mathbb{F}_q)| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{q^{d(n-d)}|\mathrm{GL}_d(\mathbb{F}_q)||\mathrm{GL}_{n-d}(\mathbb{F}_q)|}.$$

Since for any positive integer u,

$$|\mathrm{GL}_u(\mathbb{F}_q)| = \prod_{i=1}^{u}(q^u - q^{i-1}),$$

we have

$$|G(d,n)(\mathbb{F}_q)| = \frac{\prod_{i=1}^{n}(q^n - q^{i-1})}{q^{d(n-d)}\prod_{i=1}^{d}(q^d - q^{i-1})\prod_{i=1}^{n-d}(q^{n-d} - q^{i-1})}.$$

Now it is easy to calculate zeta functions of Grassmannian varieties.

Example 5.5.1. *For $G(3,5)$ defined over $\mathbb{F}_q$, we have*

$$\begin{aligned}|G(3,5)(\mathbb{F}_q)| &= \frac{(q^5-1)(q^5-q)(q^5-q^2)(q^5-q^3)(q^5-q^4)}{q^6(q^3-1)(q^3-q)(q^3-q^2)(q^2-1)(q^2-q)} \\ &= 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6,\end{aligned}$$

hence

$$|G(3,5)(\mathbb{F}_{q^r})| = 1 + q^r + 2q^{2r} + 2q^{3r} + 2q^{4r} + q^{5r} + q^{6r}$$

for any positive integer r. So

$$\begin{aligned}Z(G(3,5),T) &= \exp(\sum_{i=1}^{\infty}(1 + q^r + 2q^{2r} + 2q^{3r} + 2q^{4r} + q^{5r} + q^{6r})\frac{T^r}{r}) \\ &= \frac{1}{(1-T)(1-qT)(1-q^2T)^2(1-q^3T)^2(1-q^4T)^2(1-q^5T)(1-q^6T)}.\end{aligned}$$

For the automorphism group of $G(d,n)$ over a algebraically closed field L, we have the following result ([10], p.122, [29])[1] : When $n \neq 2d$ or $2d = n = 2$, $\mathrm{Aut}_L(G(d,n)) = \mathrm{PGL}_n(L)$. When $n = 2d$ and $n \neq 2$, $[\mathrm{Aut}_L(G(d,n)) : \mathrm{PGL}_n(L)] = 2$ and so $\mathrm{PGL}_n(L)$ is a normal subgroup of $\mathrm{Aut}_L(G(d,n))$ with index 2. In our case, from (5.5) we conclude that for $n \neq 2d$ or $2d = n = 2$, there are no non-trivial forms of $G(d,n)$.

[1] In the proof ([10], p.122), the author ignors the special case $n = 2d = 2$, in which $G(d-1,n) = G(0,2) = \{0\}$.

When $n = 2d$ and $n \neq 2$, we have the following exact sequence:

$$1 \to \mathrm{PGL}_n(\overline{k}) \to \mathrm{Aut}_{\overline{k}}(G(d,n)) \to \mathrm{Aut}_{\overline{k}}(G(d,n))/\mathrm{PGL}_n(\overline{k}) \cong \mathbb{Z}/2\mathbb{Z} \to 0.$$

Let $G_k = \mathrm{Gal}(\overline{k}/k)$, then the sequence,

$$1 = H^1(G_k, \mathrm{PGL}_n(\overline{k})) \to H^1(G_k, \mathrm{Aut}_{\overline{k}}(G(d,n))) \to H^1(G_k, \mathbb{Z}/2\mathbb{Z}),$$

is exact. Since $H^1(G_k, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, $G(d,n)$ has at most one non-trivial form.

5.6 Fermat Hypersurfaces

A Fermat hypersurface $\mathfrak{F}_n^r$ over a field k is a smooth projective variety defined by

$$X_1^r + X_2^r + \ldots + X_n^r = 0,$$

for some positive integers $n, r \geq 2$. Clearly smoothness requires $\mathrm{char}(k) \nmid r$. It is obvious that

$$\mu_r \wr S_n \leq \mathrm{Aut}_{\overline{k}}(\mathfrak{F}_n^r),$$

where $\mu_r \wr S_n$ is the wreath product of the group μ_r of r-th roots of unity in $\overline{k}$ and symmetry group S_n ([3]). So all forms of $\mathfrak{F}_n^r$ over k is classified by $H^1(G_k, \mu_r \wr S_n)$, where $G_k = \mathrm{Gal}(\overline{k}/k)$.

Brünjes proves the following two results (for the definition of étale algebra, see the Appendix):

Proposition 5.6.1 ([3], p.116)**.** *$H^1(G_k, \mu_r \wr S_n)$ can be identified by the following set:*

$$\{(L,x) \,\big|\, L \text{ is an étale algebra of degree } n \text{ over } k,\ x \in L^\times\}/\sim,$$

where $\sim$ is an equivalence relation defined as follows: $(L,x) \sim (L',x')$ if and only if there is a k-isomorphism $\phi : L \xrightarrow{\cong} L$, an element $y \in L^\times$ and an element $\varphi \in Aut_k(L)$ such that

$$x' = \phi(\varphi(xy^r)).$$

Proposition 5.6.2 ([3], p.123)**.** *Let $c \in H^1(G_k, \mu_r \wr S_n)$ which by proposition 5.6.1 corresponds to a pair (L,x) for some étale algebra of degree n over k and some element $x \in L^\times$. Let $L = \prod_{i=1}^{m} L_i$ for some finite field extension L_i of k in $\overline{k}$ with degree n_i, $i = 1,2,\ldots,m$. Also let $x = (x_1, x_2, \ldots, x_m)$ with $x_i \in L_i^\times$, $i = 1,2,\ldots,m$. For each L_i $(i = 1,2,\ldots,m)$, choose a k-basis $e_{1,i}, e_{2,i}, \ldots, e_{n_i,i}$ of L_i, then the $\mathfrak{F}_n^r(c)$, the Fermat equation $\mathfrak{F}_n^r$ twisted by c is given by*

$$\mathfrak{F}_n^r(b) = \sum_{i=1}^{m} \mathrm{Tr}_{L_i/k}\Big(\frac{1}{x_i}\Big(\sum_{j=1}^{n_i} e_{j,i}X_{j,i}\Big)^r\Big),$$

where $\mathrm{Tr}_{L_i/k} :\ L_i[X_{1,i}, X_{2,i}, \ldots, X_{n_i,i}] \to L_i[X_{1,i}, X_{2,i}, \ldots, X_{n_i,i}]$ is the k-linear map sending constants in L_i to their traces in k.

As an example, we give the forms of $\mathfrak{F}_2^3$ over $k = \mathbb{F}_q$. Let ν be any generator of $\mathbb{F}_{q^2}^\times$. Let $\iota = \nu^{\frac{q+1}{2}}$ and $\delta = \iota^2$. Define

$$L_\delta = \begin{cases} \mathbb{F}_q \times \mathbb{F}_q & \delta \in (k^\times)^2, \\ \mathbb{F}_q(\sqrt{\delta}) & \delta \notin (k^\times)^2. \end{cases}$$

Then there are two possibilities ($\mathrm{char}(k) \neq 3$ because of smoothness):

1. k has has the third root of unity, i.e. $q \equiv 1 (\text{mod } 3)$, then $\overline{\mathbb{F}}_q/\mathbb{F}_q$-forms are exactly the following twisted equations:

   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (1,1))) = X_1^3 + X_2^3$,
   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (1,\delta))) = X_1^3 + \delta X_2^3$,
   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (1,\delta^2))) = X_1^3 + \delta^2 X_2^3$,
   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (\delta,\delta))) = \delta X_1^3 + \delta X_2^3$,
   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (\delta,\delta^2))) = \delta X_1^3 + \delta^2 X_2^3$,
   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (\delta^2,\delta^2))) = \delta^2 X_1^3 + \delta^2 X_2^3$,
   - $\mathfrak{F}_2^3((L_\delta, 1)) = 2X_1^3 + 6\delta X_1 X_2^2$,
   - $\mathfrak{F}_2^3((L_\delta, \nu)) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu) X_1^3 + 3\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu\iota) X_1^2 X_2 + 3\delta \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu) X_1 X_2^2 + \delta \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu\iota) X_2^3$,
   - $\mathfrak{F}_2^3((L_\delta, \nu^2)) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu^2) X_1^3 + 3\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu^2\iota) X_1^2 X_2 + 3\delta \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu^2) X_1 X_2^2 + \delta \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu^2\iota) X_2^3$.

2. k does not contain the third root of unity, i.e. $q \equiv 2 (\text{mod } 3)$, then $\overline{\mathbb{F}}_q/\mathbb{F}_q$-forms are exactly the following twisted equations:

   - $\mathfrak{F}_2^3((\mathbb{F}_q \times \mathbb{F}_q, (1,1))) = X_1^3 + X_2^3$,
   - $\mathfrak{F}_2^3((L_\delta, 1)) = 2X_1^3 + 6\delta X_1 X_2^2$,
   - $\mathfrak{F}_2^3((L_\delta, \nu)) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu) X_1^3 + 3\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu\iota) X_1^2 X_2 + 3\delta \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu) X_1 X_2^2 + \delta \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\nu\iota) X_2^3$.

[3] also gives some examples on how to calculate the zeta functions of twisted Fermat equations in the case of $\mathbb{F}_q$ contains the r-th root of unity. The calculation is based on the fact that for hypersurfaces, only middle cohomology is non-trivial.

Lemma 5.6.3 (Hard Lefschetz theorem (Deligne) [2]))**.** *Let X be a smooth projective hypersurface X of dimension $n-2$ over a finite field k, then for any $d \in \{0, 1, \dots n-3, n-1, n, \dots, 2(n-2)\}$,*

$$H^d_{\acute{e}t}(\overline{X}, \mathbb{Q}_\ell) = \begin{cases} 0 & d \equiv 1(mod\ 2), \\ \mathbb{Q}_\ell(-\frac{d}{2}) & d \equiv 0(mod\ 2). \end{cases}$$

So we have

$$\det(1 - \mathrm{Fr}_r^* T \big| H^d_{\acute{e}t}(\overline{X}, \mathbb{Q}_\ell)) = \begin{cases} 1 & d \equiv 1(\mathrm{mod}\ 2), \\ 1 - q^{\frac{d}{2}} T & d \equiv 0(\mathrm{mod}\ 2), \end{cases}$$

for any $d \in \{0, 1, \dots n-3, n-1, n, \dots, 2(n-2)\}$. Hence

$$Z(X, T) = Q(T)^{((-1)^{n+1})} \prod_{\substack{d \in \{0,1,\dots,n-2\} \\ d \neq \frac{n-2}{2}}} \frac{1}{1 - q^d T},$$

where $Q(T) = \det(1 - \mathrm{Fr}_r^* T \big| H^{n-2}_{\acute{e}t}(\overline{X}, \mathbb{Q}_\ell))$.

[2] Deligne proved it in general case.

CHAPTER 6
Schemes

6.1 Zeta Functions

According to D. Eisenbud and J. Harris ([7], p.81), an arithmetic scheme X is a scheme isomorphic to $\operatorname{Spec} A$ for some commutative ring A that is finitely generated (as a ring) over $\mathbb{Z}$. When X is an arithmetic scheme, the zeta function attached to X is defined as (2.4) and converges absolutely when the real part of s in (2.4) satisfies:

$$\operatorname{Re}(s) > \dim X.$$

We have the following result ([22], p.84):

Theorem 6.1.1. *$\zeta(X, s)$ can be analytically continued in $\operatorname{Re}(s) > \dim X - \frac{1}{2}$ as a meromorphic function. Suppose further X to be irreducible with a generic point x and let $\kappa(x)$ be the residue field of x. Then*

- *If $\operatorname{char}(\kappa(x)) = 0$, the only pole of $\zeta(X, s)$ in $\operatorname{Re}(s) > \dim X - \frac{1}{2}$ is at $s = \dim X$ and it is a simple pole.*
- *Suppose $\operatorname{char}(\kappa(x)) = p$ for some prime number p. Let q be the highest power of p such that $\mathbb{F}_q \subset \kappa(x)$, then all poles of $\zeta(X, s)$ in $\operatorname{Re}(s) > \dim X - \frac{1}{2}$ are the points*

$$\dim X + \frac{2n\pi i}{\log q}, \qquad n \in \mathbb{Z},$$

and all such poles are simple.

The following result is important([22], p.85):

Theorem 6.1.2. *Suppose X and Y are schemes of finite type over $\mathbb{Z}$ and $f: X \to Y$ is a morphism. Denote the set of closed points in Y by $\widetilde{Y}$ and the fibre $X \times_Y \kappa(y)$ of f over $y \in Y$ by X_y. Then*

$$\zeta(X, s) = \prod_{y \in \widetilde{Y}} \zeta(X_y, s).$$

In particular, if X is a smooth scheme of finite type over the ring of integers $\mathcal{O}$ of a number field, $\mathcal{O}$ is a Dedekind domain and so every non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}$ is a closed point in Spec $\mathcal{O}$, hence

$$\zeta(X, s) = \prod_{\mathfrak{p} \in \mathrm{Spec}\ \mathcal{O},\ \mathfrak{p} \neq 0} \zeta(X_{\mathfrak{p}}, s).$$

[6] shows that if X is proper and flat over $\mathrm{Spec}\,\mathbb{Z}$ and its generic fibre $X \times_{\mathbb{Z}} \mathbb{Q}$ is smooth, then X has good reduction at all but a finite number of prime numbers, and the factor for the primes of the good reduction in the zeta function attached to X is

$$\prod_{i=0}^{2d} \prod_{\substack{\text{good} \\ \text{reduction} \\ \text{at } p}} \det(1 - p^{-s}\mathrm{Fr}_p^* | H^i_{\acute{e}t}(X \times_{\mathbb{Z}} \overline{\mathbb{Q}}_p, \mathbb{Q}_\ell))^{(-1)^{i+1}},$$

where d is the dimension of X.

Example 6.1.3. *Let k be a number field, and E/k be an elliptic curve. For any finite place v at which E has good reduction, the reduction of E at v, $\overline{E}_v$ can be*

considered defined over k_v, the residue field of k at v, which is finite. Hence the zeta function of $\overline{E}_v/k_v$ is

$$Z(\overline{E}_v, T) = \exp(\sum_{n=1}^{\infty} \#\overline{E}_v(k_{v,n})\frac{T^n}{n}),$$

where $k_{v,n}$ is the field extension of k_v with degree n in a fixed algebraic closure of k_v. This zeta function is a rational function:

$$Z(\overline{E}_v, T) = \frac{1 - a_v T + q_v T^2}{(1-T)(1-q_v T)},$$

where q_v is the order of k_v, and $a_v = q_v + 1 - \#\overline{E}_v(k_v)$.

Let $L_v(T) = 1 - a_v T + q_v T^2$. Extend $L_v(T)$ to the case of bad reduction by ([25], p.360)

$$L_v(T) = \begin{cases} 1 - T & E \text{ has split multiplicative reductive reduction at } v \\ 1 + T & E \text{ has non-split multiplicative reduction at } v \\ 1 & E \text{ has additive reduction at } v. \end{cases}$$

Then for any kind of finite place v, define the Hasse-Weil zeta function at v of $\overline{E}_v$ is

$$Z(\overline{E}_v, T) = \frac{L_v(T)}{(1-T)(1-q_v T)}.$$

Define the L-series of E/K to be

$$L_{E/k}(s) = \prod_{\text{finite place } v} L_v(q_v^{-s})^{-1}.$$

Define the global zeta function $\zeta(E/k, s)$ to be

$$\zeta(E/k, s) = \prod_{\text{finite place } v} Z(\overline{E}_v, q_v^{-s})$$

Then it is easy to see $\zeta(E/k, s)$ can be expressed by Dedekind's zeta function of k and L-series of E/k:

$$\zeta(E/k, s) = \frac{L_{E/k}(s)}{\zeta_k(s)\zeta_k(1-s)},$$

where $\zeta_k(s)$ is the Dedekind's zeta function of k given by

$$\zeta_k(s) = \prod_{\text{finite place } v} (1 - q_v^{-s})^{-1}.$$

6.2 Forms

Based on the definition of an étale form of an X-scheme Y, where X is a fixed scheme, the main results in this section are the Theorem 6.2.4 and Theorem 6.2.5, which assert that when both X and Y are affine, there exists an injective map from the set of equivalence classes of affine étale forms of Y into the Čech cohomology $H^1(X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -))$, and when $X = \operatorname{Spec} k$ for some perfect field k, and Y is any (not necessarily affine) scheme, $H^1(G_k, \mathrm{Aut}(Y \times_k \overline{k})) \cong \check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(Y \times_k -))$.

6.2.1 Étale Forms

This section uses concepts like flatness, faithful flatness, and étale morphism. See the Appendix for their definitions and general references.

In the language of schemes, a variety V defined over k implies V is a $\operatorname{Spec} k$-scheme.

A variety V' defined over k is a K/k-form of V means $V' \times_k K \cong V \times_k K$ as K-schemes for some finite separable field extension K/k, i.e. V and V' are isomorphic over some base extension. Such point of view leads to the concept of forms of a scheme.

As an example, consider the two affine $\operatorname{Spec}\mathbb{Z}$-schemes $\operatorname{Spec}\mathbb{Z}[x,y]/(y^2-x^2)$ and $\operatorname{Spec}\mathbb{Z}[x,y]/(y^2+x^2)$. As $\mathbb{Z}$-algebras, $\mathbb{Z}[x,y]/(y^2+x^2) \ncong \mathbb{Z}[x,y]/(y^2-x^2)$ because y^2-x^2 is reducible in $\mathbb{Z}[x,y]$ while y^2+x^2 is irreducible in $\mathbb{Z}[x,y]$. But clearly $(\mathbb{Z}[i])[x,y]/(x^2-y^2) \cong (\mathbb{Z}[i])[x,y]/(x^2+y^2)$ over $\mathbb{Z}[i]$. On the other hand, as $\mathbb{Z}[i]$-algebras,

$$(\mathbb{Z}[i])[x,y]/(x^2-y^2) \cong \mathbb{Z}[x,y]/(x^2-y^2) \otimes \mathbb{Z}[i],$$

and

$$(\mathbb{Z}[i])[x,y]/(x^2+y^2) \cong \mathbb{Z}[x,y]/(x^2+y^2) \otimes \mathbb{Z}[i].$$

Hence as $\operatorname{Spec}\mathbb{Z}[i]$-schemes,

$$\operatorname{Spec}\mathbb{Z}[x,y]/(y^2-x^2) \times \operatorname{Spec}\mathbb{Z}[i] \cong \operatorname{Spec}\mathbb{Z}[x,y]/(y^2+x^2) \times \operatorname{Spec}\mathbb{Z}[i].$$

Since $\mathbb{Z}[i]$ is a free $\mathbb{Z}$-module, $\mathbb{Z}[i]$ is a flat $\mathbb{Z}$-module. Hence for any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[i]$, $\mathbb{Z}[i]_{\mathfrak{p}}$ is a flat $\mathbb{Z}_{\mathfrak{p}\cap\mathbb{Z}}$-module. Here $\mathfrak{p} \cap \mathbb{Z} = j^{-1}(\mathfrak{p})$, where j is the canonical inclusion map $j : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. So the induced map $j^* : \operatorname{Spec}\mathbb{Z}[i] \to \operatorname{Spec}\mathbb{Z}$ is a flat morphism (Theorem 3 in the Appendix). Clearly j^* is surjective.

It is a well-known fact in algebraic number theory that for any number field K, there exists at least one prime number p, such that (p) in $\mathbb{Z}$ is ramified in the ring of integers $\mathcal{O}_K$ of K. So j^* is not an unramified morphism because $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$. Finally it is natural that a form of a scheme should be defined locally as usually happened in schemes. For a variety V defined over a field L, a

form of V looks like to be defined globally, but this is because $\operatorname{Spec} L$ contains only one point as a topological space. The discussion above provides a motivation to the following definition:

Definition 6.2.1. ([7], p.204) *Let S be s scheme and let X be a scheme over S. A scheme Y over S is a form of X if for any point $s \in S$, we can find an open neighborhood U_s of s in S, a scheme T_s and a flat surjective morphism $f_s : T_s \to U_s$ such that as T_s-schemes,*

$$X \times_S T_s \cong Y \times_S T_s,$$

where the morphism from T_s to S is the composition of f_s and the canonical open embedding of U_s into S.

From the definition, to prove an X-scheme Y' is a form of an X-scheme Y, we first have to find an open covering $\{U_i \,|\, i \in I,\ U_i \text{ is an open set of } X\}$ of X, where I is an index set and for each $i \in I$, a scheme T_i and a flat surjective morphism $f_i : T_i \to U_i$. Compared to the definition of a manifold M of dimension n, in which M locally looks like $\mathbb{R}^n$, it is natural to require T_i be "similar" to U_i in some sense. One way to see the similarity is to look at a morphism $f : X \to Y$, where X and Y are two smooth varieties defined over a algebraically closed field F. For the similarity of the two varieties, we at least should require f induce an isomorphism on tangent spaces for any closed point of X. This is equivalent to f being an étale morphism ([19], p.32). Another point is that in the definition 6.2.1, f_s maps T_s (which itself is open) onto an open subset U_s of S, and an étale morphism automatically satisfies this condition because any étale morphism is an open map ([19], p.14). Such requirement of similarity leads us to a special case of a Grothendieck topology, the étale site $X_{\acute{e}t}$ over X. That is, we add an extra condition of unramification on each f_i, i.e. that

each f_i besides being flat must also be unramified and locally of finite type, then to prove Y' is a form of Y over X, it is enough to find a covering

$$\mathscr{C} = \{T_i \to X \,\big|\, i \in I\} \tag{6.1}$$

in $X_{\acute{e}t}$, such that $Y \times_X T_i \cong Y' \times_X T_i$ as T_i-schemes for each $i \in I$.

Based on the discussion above, I give a restricted definition of a form of X-scheme Y, which I call an étale form.

Definition 6.2.2. *Let X be a scheme and $X_{\acute{e}t}$ be the étale site in the sense of Grothendieck. Let Y be an X-scheme. Then an X-scheme Y' is an étale form of Y if there exists a covering $\{T_i \xrightarrow{\delta_i} X \,\big|\, i \in I\}$ in $X_{\acute{e}t}$, where I is some index set, such that for each $i \in I$,*

$$Y \times_X T_i \cong Y' \times_X T_i$$

as T_i-schemes. If Y' is affine, Y' is also called an affine étale form of Y (over X).

6.2.2 Forms and Čech cohomology

From now on, forms and affine forms mean étale forms and affine étale forms respectively. Our aim is to relate forms with Čech cohomology. The following standard result is needed in the sequel and its proof can be found in e.g. [27], p.104.

Theorem 6.2.3. *If $\varphi : A \to B$ is a faithfully flat ring homomorphism and M is an A-module, then the following sequence is exact:*

$$0 \to M \xrightarrow{\alpha} M \otimes_A B \xrightarrow{\beta} M \otimes_A B \otimes_A B,$$

where $\alpha(m) = m \otimes 1$ for any $m \in M$ and $\beta(m \otimes b) = m \otimes b \otimes 1 - m \otimes 1 \otimes b$ for any $m \in M$ and $b \in B$.

Similar to the definition of non-abelian Galois cohomology, Milne defines the first Čech cohomology for sheaves of (not necessarily commutative) groups on $X_{\acute{e}t}$([19], p.122). I will extend Milne's idea to define directly the Čech cohomology $\check{H}^1(X_{\acute{e}t}, \mathscr{F})$ for any contravariant functor $\mathscr{F}$ from $X_{\acute{e}t}$ to the category of groups $\mathbb{G}$. This is done as follows:

First, for any open set $U \xrightarrow{\vartheta} X$ in $X_{\acute{e}t}$, denote $\mathscr{F}(U \xrightarrow{\vartheta} X)$ by just $\mathscr{F}(U)$ for convenience. Let

$$\mathscr{C} = \{U_j \xrightarrow{\vartheta_j} X \,\big|\, j \in J\}$$

be an étale covering of X, where J is some index set. Define $U_{ij} = U_i \times_X U_j$ for any $i, j \in J$. Under this fixed $\mathscr{C}$, a cocycle (c_{ij}) is defined as $c_{ij} \in \mathscr{F}(U_{ij})$ such that

$$c_{ij}c_{jk} = c_{ik}$$

on U_{ijk} for any $i, j, k \in J$ via the built-in maps $\mathscr{F}(U_{ij}) \to \mathscr{F}(U_{ijk})$, $\mathscr{F}(U_{jk}) \to \mathscr{F}(U_{ijk})$ and $\mathscr{F}(U_{ik}) \to \mathscr{F}(U_{ijk})$.

Let $Z(\mathscr{C}/X, \mathscr{F})$ be the set of all cocycles defined above. Define a relation "$\sim$" in $Z(\mathscr{C}/X, \mathscr{F})$ as follows: for any (c_{ij}) and (d_{ij}) in $Z(\mathscr{C}/X, \mathscr{F})$, $(c_{ij}) \sim (d_{ij})$ if and only if there exists $\omega_i \in \mathscr{F}(U_i)$, such that $d_{ij} = \omega_i c_{ij} \omega_j^{-1}$ on U_{ij}. Clearly $(c_{ij}) \sim (c_{ij})$

and $(c_{ij}) \sim (d_{ij})$ implies $(d_{ij}) \sim (c_{ij})$. Suppose $(c_{ij}) \sim (d_{ij})$ and $(d_{ij}) \sim (e_{ij})$ in $Z(\mathscr{C}/X, \mathscr{F})$, then there exist $\omega_i, \psi_i \in \mathscr{F}(U_i)$ such that

$$d_{ij} = \omega_i c_{ij} \omega_j^{-1}$$

and

$$e_{ij} = \psi_i \circ d_{ij} \psi_j^{-1}.$$

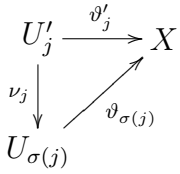
So

$$e_{ij} = \psi_i \omega_i c_{ij} \omega_j^{-1} \psi_j^{-1} = (\psi_i \omega_i) c_{ij} (\psi_j \omega_j)^{-1},$$

i.e. $(c_{ij}) \sim (e_{ij})$. Hence "$\sim$" is an equivalence relation. Consequently, we can define the first Čech cohomology $\check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathscr{F})$ with respect to a given étale covering $\mathscr{C}$ to be

$$\check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathscr{F}) = Z(\mathscr{C}/X_{\acute{e}t}, \mathscr{F})/\sim .$$

Let $\mathscr{C}' = \{U_j' \xrightarrow{\vartheta_j'} X \,\big|\, j \in J\}$, where J is an index set, be another covering in $X_{\acute{e}t}$. Define $\mathscr{C} < \mathscr{C}'$ if there is a map $\sigma : J \to I$ and a map $\nu_j : U_j' \to U_{\sigma(j)}$ for each $j \in J$, such that $\vartheta_j' = \vartheta_{\sigma(j)} \circ \nu_j$, i.e. the following diagram is commutative:



The partial order $<$ defined above is directed. This is because according to the properties of $X_{\acute{e}t}$, $\mathscr{C} \times_X \mathscr{C}' \stackrel{\text{def}}{=} \{S \times_X T \,\big|\, S \in \mathscr{C},\, T \in \mathscr{C}'\}$ is also a covering and clearly $\mathscr{C} < \mathscr{C} \times_X \mathscr{C}'$ and $\mathscr{C}' < \mathscr{C} \times_X \mathscr{C}'$.

With respect to this partial order, the first Čech cohomology $\check{H}^1(X_{\acute{e}t}, \mathscr{F})$ is defined

to be

$$\check{H}^1(X_{\acute{e}t}, \mathscr{F}) = \varinjlim_{\mathscr{C},<} \check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathscr{F}),$$

where $\mathscr{C}$ runs through all coverings in $X_{\acute{e}t}$.

Let Y be an X-scheme. Define a contravariant group functor $\mathrm{Aut}(Y \times_X -)$ from $X_{\acute{e}t}$ to the category of groups as follows: for any open set $U \xrightarrow{\alpha} X$ in $X_{\acute{e}t}$, $\mathrm{Aut}(Y \times_X -)$ maps U to $\mathrm{Aut}(Y \times_X U)$, the automorphism group of $Y \times_X U$ as U-schemes, and for any morphism $U \xrightarrow{h} V$ in $X_{\acute{e}t}$, $\mathrm{Aut}(Y \times_X -)$ maps h to $\mathrm{Aut}(Y \times_X h) : \mathrm{Aut}(Y \times_X V) \to \mathrm{Aut}(Y \times_X U)$ induced by the composition $U \xrightarrow{h} V \to X$: for any $\nu \in \mathrm{Aut}(Y \times_X V)$, we have an automorphism $\nu^{\#}$ induced by ν:

$$\nu^{\#} : Y \times_X V \times_V U \to Y \times_X V \times_V U,\ \nu^{\#} = \nu \times 1_U,$$

where 1_U is the identity map on U, and note that $V \times_V U \cong U$. In particular, suppose h is an isomorphism $h : U \xrightarrow{\cong} V$ over X, then for any $\nu \in \mathrm{Aut}(Y \times_X V)$,

$$\nu^{\#} : Y \times_X U \xrightarrow[\cong]{1\times h} Y \times_X V \xrightarrow[\cong]{\nu} Y \times_X V \xrightarrow[\cong]{(1\times h)^{-1}} Y \times_X U,$$

and hence

$$\nu^{\#} = (1 \times h)^{-1} \circ \nu \circ (1 \times h),$$

i.e.

$$\nu^{\#} = {}^h\nu. \tag{6.2}$$

(6.2) will be used to prove Theorem 6.2.5.

Define an equivalence relation $\sim$ as follows: let X be a scheme and Y be an X-scheme. Let X-schemes Y_1 and Y_2 be forms of Y, then define $Y_1 \sim Y_2$ if there is an isomorphism $f : Y_1 \xrightarrow{\cong} Y_2$ as X-schemes. It is obvious $\sim$ is an equivalence relation.

Now we will prove the two main results of this section:

Theorem 6.2.4. *Let X be an affine scheme and let Y be an affine scheme over X. Let $\mathscr{Y}$ be the equivalence classes of affine X-forms of Y with respect to the equivalence relation $\sim$ defined above, then there is an injective map*

$$\eta : \mathscr{Y} \hookrightarrow \check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -)), \tag{6.3}$$

where $\check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -))$ is induced by taking the direct limit of (6.4) *with respect to all étale coverings $\mathscr{C}$.*

Proof. Suppose we are given an affine X-form Y' of Y relative to a cover

$$\mathscr{C} = \{T_i \xrightarrow{\vartheta_i} X \,\big|\, i \in I\},$$

where I is an index set. Then for each i, we have an isomorphism ψ_i over T_i:

$$\psi_i : Y \times_X T_i \xrightarrow{\cong} Y' \times_X T_i.$$

Hence for any $i, j \in I$, $\psi_i^{-1} \circ \psi_j$ is an isomorphism of $Y \times_X T_{ij}$ over T_{ij}, where $T_{ij} = T_i \times_X T_j$. Denote $\psi_i^{-1} \circ \psi_j$ by c_{ij}.

For any $i, j, k \in I$, let $T_{ijk} = T_i \times_X T_j \times_X T_k$. Then via canonical projection maps $p_{ij} : T_{ijk} \to T_{ij}$, $p_{ik} : T_{ijk} \to T_{ik}$ and $p_{jk} : T_{ijk} \to T_{jk}$, clearly $c_{jk} \circ c_{ij} = c_{ik}$ in T_{ijk}. Hence (c_{ij}) is a cocycle in $\check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -))$.

Suppose there is another isomorphism $\psi_i' : Y \times_X T_i \xrightarrow{\cong} Y' \times_X T_i$ for each $i \in I$, then let $\lambda_i = \psi_i'^{-1} \circ \psi_i$, which is an automorphism of $Y \times_X T_i$, i.e. $\lambda_i \in \mathrm{Aut}(Y \times_X T_i)$,

and $\psi_i = \psi_i' \circ \lambda_i$. Let $c_{ij}' = \psi_i'^{-1} \circ \psi_j'$. We have

$$\begin{aligned} c_{ij} &= \psi_i^{-1} \circ \psi_j \\ &= (\psi_i' \circ \lambda_i)^{-1} \circ (\psi_j' \circ \lambda_j) \\ &= \lambda_i^{-1} \circ \psi_i'^{-1} \circ \psi_j' \circ \lambda_j \\ &= \lambda_i^{-1} \circ c_{ij}' \circ \lambda_j. \end{aligned}$$

Hence $[(c_{ij})] = [(c_{ij}')]$ which implies (c_{ij}) does not depend on the choice of ψ_i.

A similar argument shows that $[c_{ij}]$ is also independent of the choice of Y' up to isomorphism. Let $\Upsilon/\mathscr{C}$ be the set of equivalence classes of affine forms of Y over $X_{\acute{e}t}$ with respect to the fixed cover $\mathscr{C}$ in $X_{\acute{e}t}$, then we have a well-defined map:

$$\eta_{\mathscr{C}} : \Upsilon/\mathscr{C} \to \check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -)),\ Y' \mapsto [(c_{ij})]. \tag{6.4}$$

Let Y_1 and Y_2 be two affine forms of Y with respect to the same given cover $\mathscr{C}$ such that Y_1 and Y_2 give the same class of cocycles. This means we have isomorphisms as T_i-schemes $\varphi_i : Y \times_X T_i \xrightarrow{\cong} Y_1 \times_X T_i$ and $\phi_i : Y \times_X T_i \xrightarrow{\cong} Y_2 \times_X T_i$ for each $i \in I$ such that $[(\varphi_i^{-1} \circ \varphi_j)] = [(\phi_i^{-1} \circ \phi_j)]$. Then there exists $h_i \in \mathrm{Aut}(Y \times_X T_i)$ such that

$$\varphi_i^{-1} \circ \varphi_j = h_i^{-1} \circ \phi_i^{-1} \circ \phi_j \circ h_j,$$

hence

$$\phi_i \circ h_i \circ \varphi_i^{-1} = \phi_j \circ h_j \circ \varphi_j^{-1}. \tag{6.5}$$

Each $\phi_i \circ h_i \circ \varphi_i^{-1}$, denoted by β_i, gives an isomorphism as T_i-schemes:

$$\beta_i : Y_1 \times_X T_i \xrightarrow{\cong} Y_2 \times_X T_i. \tag{6.6}$$

(6.5) shows

$$\beta_i\big|_{Y_1 \times_X T_{ij}} = \beta_j\big|_{Y_1 \times_X T_{ij}}, \tag{6.7}$$

which is true even if $i = j$. Hence we have a set of isomorphisms

$$\{\, Y_1 \times_X T_i \xrightarrow{\beta_i} Y_2 \times_X T_i \,\big|\, i \in I\},$$

such that (6.7) holds for any $i, j \in I$.

Since each scheme can be covered by open affine subscheme in the usual sense, any open immersion is étale and the composition of any two étale morphisms is étale, as a result, we can assume each T_i is affine, i.e. $T_i = \operatorname{Spec} B_i$ for some ring B_i.

Since Y_1, Y_2 and X are all affine, we can let $Y_1 = \operatorname{Spec} A_1$, $Y_2 = \operatorname{Spec} A_2$ and $X = \operatorname{Spec} B$ for some rings A_1, A_2 and B respectively. So $Y_1 \times_X T_i = \operatorname{Spec}(A_1 \otimes_B B_i)$ and $Y_2 \times_X T_i = \operatorname{Spec}(A_2 \otimes_B B_i)$ for each $i \in I$. Also, since X is an affine scheme, and any affine scheme is quasi-compact and any étale homomorphism is an open map, we can assume I is a finite set.

Since the morphism $\beta_i : Y_1 \times_X T_i \to Y_2 \times_X T_i$ is an isomorphism as T_i-schemes, we have the following commutative diagram:

$$\begin{array}{ccc} \operatorname{Spec}(A_1 \otimes_B B_i) & \xrightarrow[\cong]{\beta_i} & \operatorname{Spec}(A_2 \otimes_B B_i) \\ & \searrow \quad \swarrow & \\ & \operatorname{Spec}(B_i) & \end{array}$$

which is equivalent to the following commutative diagram:

$$\begin{array}{ccc} A_1 \otimes_B B_i & \xleftarrow{\beta_i^{\#}} & A_2 \otimes_B B_i \\ {\scriptstyle b_i \mapsto 1 \otimes b_i} \uparrow & & \uparrow {\scriptstyle b_i \mapsto 1 \otimes b_i} \\ & B_i & \end{array} \tag{6.8}$$

where $\beta_i^{\#}$ is the corresponding ring homomorphism which induces the scheme morphism $\beta_i : Y_1 \times_X T_i \to Y_2 \times_X T_i$.

Let the ring homomorphism $\delta_i^{\#} : B \to B_i$ correspond to the morphism $\delta_i : \operatorname{Spec} B_i \to \operatorname{Spec} B$. Because of (6.8), we have for any $b \in B$,

$$\beta_i^{\#}(1 \otimes \delta_i^{\#}(b_i)) = 1 \otimes \delta_i^{\#}(b_i).$$

This implies $\beta_i^{\#}$ is a B-algebra isomorphism if $A_1 \otimes_B B_i$ and $A_2 \otimes_B B_i$ are regarded as B-algebras and consequently, we have a B-algebra isomorphism

$$(\beta_i^{\#})_{i\in I} : A_2 \otimes_B (\prod_{i\in I} B_i) \xrightarrow{\cong} A_1 \otimes_B (\prod_{i\in I} B_i),$$

where B-algebra structure of $\prod_{i\in I} B_i$ is defined by

$$(\delta_i^{\#})_{i\in I} : B \to \prod_{i\in I} B_i.$$

Both $A_1 \otimes_B B_i$ and $A_2 \otimes_B B_i$ are also B_i-algebras and (6.8) gives for any $b_i \in B_i$,

$$\beta_i^{\#}(1 \otimes b_i) = 1 \otimes b_i.$$

Hence $\beta_i^{\#}$ is also a B_i-algebra homomorphism.

Since the set $\{\operatorname{Spec} B_i \xrightarrow{\delta_i} \operatorname{Spec} B \,\big|\, i \in I\}$ is an étale covering of $X = \operatorname{Spec} B$, as sets, we have

$$\underset{i\in I}{\cup} \operatorname{Spec} B_i = \operatorname{Spec} B.$$

This implies the map $\operatorname{Spec}(\prod_{i\in I} B_i) \to \operatorname{Spec} B = X$ induced by $(\delta_i)_{i\in I}$ is surjective, hence the corresponding ring homomorphism $(\delta_i^{\#})_{i\in I} : B \to \prod_{i\in I} B_i$ is faithfully flat. Consequently, by base extension, we have the faithfully flat ring homomorphism:

$$1 \otimes (\delta_i^{\#})_{i\in I} : A_2 \otimes_B B \to A_2 \otimes_B (\prod_{i\in I} B_i).$$

This implies $1 \otimes (\delta_i^{\#})_{i\in I}$ is injective. Hence it can be regarded that

$$A_2 \otimes_B B \subset A_2 \otimes_B (\prod_{i\in I} B_i).$$

1°. Assume $\#I = 1$. Then (6.7) gives

$$\beta_1\big|_{\mathrm{Spec}\,(A_1\otimes_B B_1\otimes_B B_1)} = \beta_1\big|_{\mathrm{Spec}\,(A_1\otimes_B B_1\otimes_B B_1)}, \tag{6.9}$$

where the β_1 at the left hand side arises from the base change $A_1 \otimes_B B_1$ to $A_1 \otimes_B B_1 \otimes_B B_1$ via $a \otimes b \mapsto a \otimes b \otimes 1$, while the β_1 at the right hand side arises from the base change $A_1 \otimes_B B_1$ to $A_1 \otimes_B B_1 \otimes_B B_1$ via $a \otimes b \mapsto a \otimes 1 \otimes b$.

(6.9) implies for any $a_2 \in A_2$, let $\beta_1^{\#}(a_2 \otimes 1) = \sum_{l=1}^{n} a_{1l} \otimes b_{1l}$ for some $a_{11}, a_{12}, \ldots, a_{1n}$ in A_1 and some $b_{11}, b_{12}, \ldots, b_{1l}$ in B_1, then

$$\sum_{l=1}^{n} a_{1l} \otimes b_{1l} \otimes 1 = \sum_{l=1}^{n} a_{1l} \otimes 1 \otimes b_{1l},$$

i.e.

$$\sum_{l=1}^{n} (a_{1l} \otimes b_{1l} \otimes 1 - a_{1l} \otimes 1 \otimes b_{1l}) = 0.$$

We have already shown the ring homomorphism $\delta_1^{\#} : B \to B_1$ is faithfully flat, hence from Theorem 6.2.3,

$$\sum_{l=1}^{n} a_{1l} \otimes b_{1l} \in A_1 \otimes_B 1,$$

where $A_1 \otimes_B 1$ is defined to be the set $\{a \otimes 1 \,\big|\, a \in A_1\}$. So

$$\beta_1^{\#}(A_2 \otimes_B 1) \subset A_1 \otimes_B 1.$$

2°. Let $\#I = 2$. Then we have isomophism:

$$\beta_1^{\#} \times \beta_2^{\#} : A_2 \otimes_B (B_1 \times B_2) \cong (A_2 \otimes_B B_1) \times (A_2 \otimes_B B_2) \xrightarrow{\cong}$$
$$(A_1 \otimes_B B_1) \times (A_1 \otimes_B B_2) \cong A_1 \otimes_B (B_1 \times B_2).$$

Similarly, (6.7) gives

$$\beta_1 \times \beta_2\big|_{\mathrm{Spec}\,(A_1 \otimes_B (B_1 \times B_2) \otimes_B (B_1 \times B_2))} = \beta_1 \times \beta_2\big|_{\mathrm{Spec}\,(A_1 \otimes_B (B_1 \times B_1) \otimes_B (B_1 \times B_1))}, \tag{6.10}$$

where $\beta_1 \times \beta_2$ on the two sides has the similar interpretation as that given to β_1 in (6.9). (6.10) implies for any $a_2 \in A_2$, let $\beta_1^{\#} \times \beta_2^{\#}(a_2 \otimes (1,1)) = \sum_{l=1}^{n} a_{1l} \otimes (b_{1l}, b_{2l})$ for some $a_{11}, a_{12}, \ldots, a_{1n}$ in A_1 and some $(b_{11}, b_{21}), (b_{12}, b_{22}), \ldots, (b_{1n}, b_{2n})$ in $B_1 \times B_2$, then (6.7) gives

$$\sum_{l=1}^{n} a_{1l} \otimes (b_{1l}, b_{2l}) \otimes (1,1) = \sum_{l=1}^{n} a_{1l} \otimes (1,1) \otimes (b_{1l}, b_{2l}),$$

i.e.

$$\sum_{l=1}^{n} (a_{1l} \otimes (b_{1l}, b_{2l}) \otimes (1,1) - a_{1l} \otimes (1,1) \otimes (b_{1l}, b_{2l})) = 0.$$

Since $(\delta_1^{\#}, \delta_2^{\#}) : B \to B_1 \times B_2$ is faithfully flat, from Theorem 6.2.3,

$$\sum_{l=1}^{n} a_{1l} \otimes (b_{1l}, b_{2l}) \in A_1 \otimes_B (1,1) = \{a \otimes (1,1) \,\big|\, a \in A_1\},$$

i.e.

$$(\beta_1^{\#} \times \beta_2^{\#})(A_2 \otimes_B (1,1)) \subset A_1 \otimes_B (1,1).$$

3°. For any finite set I with $\#I = m$, since the ring homomorphism

$$(\delta^{\#})_{i \in I} : B \to \prod_{i \in I} B_i$$

is faithfully flat and

$$\big(\beta_i\big)_{i\in I}\big|_{\mathrm{Spec}\,(A_1\otimes_B(\prod_{i\in I}B_i)\otimes_B(\prod_{i\in I}B_i))}=\big(\beta_i\big)_{i\in I}\big|_{\mathrm{Spec}\,(A_1\otimes_B(\prod_{i\in I}B_i)\otimes_B(\prod_{i\in I}B_i))},$$

with the similar interpretation as that given to (6.9) and (6.10). Similar to 1° and 2°, we can prove the isomorphism

$$(\beta_i^{\#})_{i\in I}:\ A_2\otimes_B\prod_{i\in I}B_i\overset{\cong}{\longrightarrow}A_1\otimes_B\prod_{i\in I}B_i$$

satisfies

$$\big(\beta_i^{\#}\big)_{i\in I}\big(A_2\otimes_B(\underbrace{1,1,\dots 1}_{\#I=m})\big)\subset A_1\otimes_B(\underbrace{1,1,\dots 1}_{\#I=m}).$$

Since $(\beta_i^{\#})_{i\in I}$ is also a B-algebra isomorphism, we have

$$(\beta_i^{\#})_{i\in I}(A_2\otimes_B B)\subset A_1\otimes_B B.$$

Hence we have an injective ring homomorphism

$$(\beta_i^{\#})_{i\in I}:\ A_2\hookrightarrow A_1.$$

By symmetry, we also have an injective ring homomorphism

$$(\beta_i^{\#})_{i\in I}^{-1}:\ A_1\hookrightarrow A_2.$$

Hence

$$A_1\cong A_2.$$

So the $\eta_{\mathscr{C}}$ in (6.4) is injective. Let $\mathscr{C}'=\{T_j'\overset{\vartheta_j'}{\longrightarrow}X\,\big|\,j\in J\}$, where J is an index set, be another covering in $X_{\acute{e}t}$ such that $\mathscr{C}<\mathscr{C}'$. Hence there is a map $\sigma:\ J\to I$ and a map $\nu_j:T_j'\to T_{\sigma(j)}$ for each $j\in J$, such that

$$\vartheta_j'=\vartheta_{\sigma(j)}\circ\nu_j. \tag{6.11}$$

Suppose we are given an X-form $\mathcal{Y}$ of Y with respect to $\mathscr{C}$, i.e. $\mathcal{Y} \times_X T_i \cong Y \times_X T_i$ as T_i-schemes for each $i \in I$. Because of (6.11), we have for any $j \in J$,

$$\mathcal{Y} \times_X T'_j \cong \mathcal{Y} \times_X T'_j \times_{T_{\sigma(j)}} T_{\sigma(j)} \cong Y \times_X T'_j \times_{T_{\sigma(j)}} T_{\sigma(j)} \cong Y \times_X T'_j$$

as T'_j schemes. So $\mathcal{Y}$ is also an X-form of Y with respect to $\mathscr{C}'$. So we have

$$\mathscr{Y} = \varinjlim_{\mathscr{C},<} \Upsilon/\mathscr{C}. \tag{6.12}$$

Since for each covering $\mathscr{C}$ in $X_{\acute{e}t}$, $\eta_{\mathscr{C}} : \Upsilon/\mathscr{C} \to \check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -))$ is injective, we have an injective map η induced by $\eta_{\mathscr{C}}$:

$$\eta : \mathscr{Y} = \varinjlim_{\mathscr{C},<} \Upsilon/\mathscr{C} \to \varinjlim_{\mathscr{C},<} \check{H}^1(\mathscr{C}/X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -)) = \check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(Y \times_X -)). \tag{6.13}$$

□

We can obtain more results if X in Theorem 6.2.4 is $\operatorname{Spec} k$, where k is a perfect field (e.g. a number field or a finite field) and E be a scheme (not necessarily affine, e.g. an elliptic curve) over k. Note that $\operatorname{Spec} k$ has only one point as a topological space, and hence E' is a form of E over $X_{\acute{e}t}$ if and only if we have an étale covering $\{T \xrightarrow{\gamma} \operatorname{Spec} k\}$ such that $E \times_k T \cong E' \times_k T$. From Theorem 8 in the Appendix, we can assume that $T = \operatorname{Spec} K'$, where K' is a finite separable field extension of k. So if E' is a form of E over $\operatorname{Spec} k$, there is a finite separable field extension K'/k, such that $E' \times_k K' \cong E \times_k K'$ as K'-schemes. But since k is perfect and K'/k is a finite separable extension, there exists a field K such that $K \supset K' \supset k$ and K/k is a finite Galois extension. Clearly the following diagram is commutative:

$$\begin{array}{ccc} K' & \xhookrightarrow{h} & K \\ {\scriptstyle h}\uparrow & \nearrow_{h} & \\ k & & \end{array} \tag{6.14}$$

where h is the canonical inclusion map. This in turn gives the following commutative diagram:

$$\begin{array}{ccc} \operatorname{Spec} K & \xrightarrow{h^{\#}} & \operatorname{Spec} K' \\ {\scriptstyle h^{\#}}\downarrow & \swarrow_{h^{\#}} & \\ \operatorname{Spec} k & & \end{array} \tag{6.15}$$

where each $h^{\#}$ is induced by the corresponding h in (6.14). Clearly each $h^{\#}$ is étale because all field extensions K'/k, K/k and K/K' are finite and separable. Because of (6.15), we have $E' \times_k K \cong E \times_k K$ as K-schemes. Conversely, suppose we have a k-scheme E' and a finite Galois field extension K/k such that $E' \times_k K \cong E \times_k K$ as K-schemes, then since K/k is a finite Galois field extension, the morphism $\operatorname{Spec} K \to \operatorname{Spec} k$ induced by the inclusion map from k to K is étale. Hence E' is a form of E over $\operatorname{Spec} k$. So E' is a form of E over $\operatorname{Spec} k$ if and only if there exists a finite Galois field extension K/k such that $E' \times_k K \cong E \times_k K$ as K-schemes.

Now let E be a scheme (e.g. a quasi-projective variety) over k and K/k be a finite Galois field extension with Galois group $G = \operatorname{Gal}(K/k)$. By abuse of notation, write $\check{H}^1(K/X_{\acute{e}t}, \operatorname{Aut}(E \times_k -)$ to denote $\check{H}^1(\operatorname{Spec} K/X_{\acute{e}t}, \operatorname{Aut}(E \times_k -))$. Recall that here $X = \operatorname{Spec} k$ for some perfect field k. We have ([2]):

$$K \otimes_k K \cong \prod_{g \in G} K_g \tag{6.16}$$

as K-algebras, where K_g is an isomorphic copy of K for each $g \in G$. Hence there exists an isomorphism σ:

$$\sigma : \coprod_{g \in G} \operatorname{Spec} K_g \xrightarrow{\cong} \operatorname{Spec} K \times_{\operatorname{Spec} k} \operatorname{Spec} K.$$

Since K/k is a finite Galois extension, $\operatorname{Spec} K$ is an étale covering of $X = \operatorname{Spec} k$. Let $[(c)]$ be an element in $\check{H}^1(K/X_{\acute{e}t}, \operatorname{Aut}(E \times_k -))$ with a representative $(c) \in$

$Z(K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -))$, then $c \in \mathrm{Aut}(E \times_k K \times_k K)$. From (6.16),

$$\begin{aligned} E \times_k K \times_k K &\cong E \times_k \mathrm{Spec}\,(\prod_{g\in G} K_g) \\ &\cong E \times_k (\coprod_{g\in G} \mathrm{Spec}\, K_g) \\ &\cong \coprod_{g\in G} E \times_k K_g, \end{aligned} \tag{6.17}$$

where $\coprod$ means disjoint union. So

$$\mathrm{Aut}(E \times_k K \times_k K) \cong \prod_{g\in G} \mathrm{Aut}(E \times_k K_g). \tag{6.18}$$

Hence c can canonically be identified with the map $c^{\#} : G \to \mathrm{Aut}(E \times_k K)$ defined by $c^{\#}(g) = c\big|_{\mathrm{Aut}(E\times_k K_g)}$, $\forall g \in G$. By definition, the element c also satisfies the condition

$$c \circ c = c, \tag{6.19}$$

on $E\times_k K\times_k K\times_k K$, where the second c on the left hand side acts on $E\times_k K\times_k K\times_k K$ via the projection from $E \times_k K \times_k K \times_k K$ to the first, third and forth component; the second c on the left hand side acts via the projection from $E \times_k K \times_k K \times_k K$ to the first, second and third component; and the c on the right hand side acts via the projection from $E \times_k K \times_k K \times_k K$ to the first, second and forth component. From (6.16), as K-algebras,

$$K \otimes_k K \otimes_k K \cong K \otimes_k (\prod_{g\in G} K_g) \cong \prod_{g,h\in G} K_{(g,h)},$$

where $K_{(g,h)} = K$. Hence by abuse of notation, there also exists an isomorphism σ:

$$\sigma : \coprod_{g,h\in G} \mathrm{Spec}\, K_{(g,h)} \xrightarrow{\cong} \mathrm{Spec}\, K \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, K \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, K,$$

and similarly we have:

$$E \times_k K \times_k K \times_k K \cong \coprod_{g,h \in G} E \times_k K_{(g,h)}. \tag{6.20}$$

Consider the following diagram:

$$\begin{array}{ccc} \coprod_{g,h\in G} \operatorname{Spec} K_{(g,h)} & \xrightarrow[d_1]{d_0} \\ & \xrightarrow[d_2]{} & \coprod_{g\in G} \operatorname{Spec} K_g \\ \cong \downarrow \sigma & & \cong \downarrow \sigma \\ \operatorname{Spec} K \times_{\operatorname{Spec} k} \operatorname{Spec} K \times_{\operatorname{Spec} k} \operatorname{Spec} K & \xrightarrow[p_2]{p_0 \atop p_1} & \operatorname{Spec} K \times_{\operatorname{Spec} k} \operatorname{Spec} K \end{array} \tag{6.21}$$

where $p_l\,(l = 0, 1, 2)$ is defined as follows: let $K_1, K_2 \ldots, K_n$ be some field extensions of field k, then $p_i\,(i = 0, 1, \ldots, n-1)$ is defined to be the standard projection map:

$$p_i : \operatorname{Spec} K_1 \times_{\operatorname{Spec} k} \operatorname{Spec} K_2 \times_{\operatorname{Spec} k} \ldots \times_{\operatorname{Spec} k} \operatorname{Spec} K_{i+1} \times_{\operatorname{Spec} k} \ldots \times_{\operatorname{Spec} k} \operatorname{Spec} K_n \to$$
$$\operatorname{Spec} K_1 \times_{\operatorname{Spec} k} \operatorname{Spec} K_2 \times_{\operatorname{Spec} k} \ldots \times_{\operatorname{Spec} k} \widehat{\operatorname{Spec} K_{i+1}} \times_{\operatorname{Spec} k} \ldots \times_{\operatorname{Spec} k} \operatorname{Spec} K_n,$$

where $\widehat{\operatorname{Spec} K_{i+1}}$ means to omit $\operatorname{Spec} K_{i+1}$; d_0, d_1 and d_2 are defined as follows: for each $(g, h) \in G \times G$,

$$d_0 = g^* : \operatorname{Spec} K_{(g,h)} \to \operatorname{Spec} K_h,$$

where g^* is the isomorphism $\operatorname{Spec} K \to \operatorname{Spec} K$ induced by the ring isomorphism $g : K \to K$, d_1 is the identity map from $\operatorname{Spec} K_{(g,h)}$ to $\operatorname{Spec} K_{gh}$, and d_2 is the identity map from $\operatorname{Spec} K_{(g,h)}$ to $\operatorname{Spec} K_g$.

It is shown in [19], p.100, that the diagram in (6.21) is commutative for each pair (d_i, p_i), $i = 0, 1, 2$. Apply $\operatorname{Aut}(E \times_k -)$ to (6.21). Consider the pair (p_0, d_0). As we have discussed, any element $f \in \operatorname{Aut}(E \times_k \coprod_{g\in G} \operatorname{Spec} K_g) \cong \prod_{g\in G} \operatorname{Aut}(E \times_k \operatorname{Spec} K_g)$ can be identified with the (continuous) map $f^{\#} : G \to \operatorname{Aut}(E \times_k \operatorname{Spec} K)$ by $f^{\#}(g) = f\big|_{\operatorname{Aut}(E \times_k K_g)}$. Fix any $g \in G$, then for any $h \in G$, since d_0 is an isomorphism

from $\operatorname{Spec} K_{(g,h)}$ to $\operatorname{Spec} K_h$, from (6.2) we see that for each $f^{\#}(h)$, d_0 induces an element $d_0^* f^{\#}(g,h)$ in $\operatorname{Aut}(E \times_k K_{(g,h)})$ by $d_0^* f^{\#}(g,h) = {}^{g^*}f^{\#}(h)$, which is, by our convention, denoted by ${}^{g}f^{\#}(h)$. Similarly, we have that $d_1^* f^{\#}(g,h) = f^{\#}(gh)$ and $d_2^* f^{\#}(g,h) = f^{\#}(g)$.

Hence the first c on the left hand side of (6.19) acts on $\coprod_{g,h\in G} E \times_k K_{(g,h)}$ by $(c^{\#}(g))_{g,h\in G}$, the second c on the left hand side of (6.19) acts on $\coprod_{g,h\in G} E \times_k K_{(g,h)}$ by ${}^{g}c^{\#}(h)$, and the c on the right hand side of (6.19) acts on $\coprod_{g,h\in G} E \times_k K_{(g,h)}$ by $(c^{\#}(gh))_{g,h\in G}$. Hence (6.19) gives

$$c^{\#}(gh) = c^{\#}(g) \circ {}^{g}c^{\#}(h). \tag{6.22}$$

So $c^{\#} \in Z^1(G, \operatorname{Aut}(E \times_k K))$. Suppose we have $[(c)]$ has another representative (c') in $Z^1(\operatorname{Spec} K/X_{\acute{e}t}, \operatorname{Aut}(E \times_k -))$, then $c \sim c'$, i.e. there is $\omega \in \operatorname{Aut}(E \times_k K)$, such that on $E \times_k K \times_k K$,

$$c' = \omega^{-1} \circ c \circ \omega, \tag{6.23}$$

where the second ω on the right hand side acts on $E \times_k K \times_k K$ via the projection of $E \times_k K \times_k K$ to the first and third component, and the first ω acts via the projection of $E \times_k K \times_k K$ to the first and second component. As expected, the following diagram is commutative ([19], p.100):

$$\begin{array}{ccc} \coprod_{g\in G} \operatorname{Spec} K_g & \overset{d_0}{\underset{d_1}{\rightrightarrows}} & \operatorname{Spec} K \\ \cong \downarrow \sigma & & \cong \downarrow \sigma \\ \operatorname{Spec} K \times_{\operatorname{Spec} k} \operatorname{Spec} K & \overset{p_0}{\underset{p_1}{\rightrightarrows}} & \operatorname{Spec} K \end{array} \tag{6.24}$$

for each pair (d_0, p_0), where for each $g \in G$,

$$d_0 = g^* : \operatorname{Spec} K_g \to \operatorname{Spec} K,$$

and d_1 is the identity map from Spec K_g to Spec K. Using similar argument as above one can easily see that the first ω on the right hand side of (6.23) is $(\omega)_{g\in G}$ and the second ω in (6.23) is $({}^g\omega)_{g\in G}$. So (6.23) implies

$$c'^{\#}(g) = \omega^{-1} \circ c^{\#}(g) \circ {}^g\omega,$$

which is equivalent to say $c'^{\#} \sim c^{\#}$. Clearly the above argument can be reversed because c' and $c'^{\#}$ can be canonically identified. Hence we have a well-defined injective map $\mathfrak{f}$:

$$\mathfrak{f} : \check{H}^1(K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -)) \to H^1(G, \mathrm{Aut}(E \times_k K)),\ [(c)] \mapsto [c^{\#}].$$

Now we prove the surjectivity of $\mathfrak{f}$. Let $[f]$ is an element in $G^1(G, \mathrm{Aut}(E \times_k K))$ with representative $f \in Z^1(G, \mathrm{Aut}(E \times_k K))$, then f can be identified with $(f(g))_{g\in G}$. Since (6.18) is an isomorphism, f canonically corresponds to a unique element $\tilde{f}$ in $\mathrm{Aut}(E \times_k K \times_k K)$. If we can prove $\tilde{f} \in Z(\mathrm{Spec}\, K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -))$, then clearly $\mathfrak{f}(\tilde{f}) = f$. But since (6.17) and (6.20) are isomorphisms and diagrams in (6.21) and (6.24) are commutative, reversing the argument used to prove (6.22) gives

$$\tilde{f} \circ \tilde{f} = \tilde{f},$$

on $E \times_k K \times_k K \times_k K$, hence $\tilde{f} \in Z(\mathrm{Spec}\, K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -))$. From the isomorphism in (6.18), which maps the identity map on $E \times_k K \times_k K$ to identity map on each $E \times_k K_g$, it is obvious that $\mathfrak{f}$ maps the neutral element in $\check{H}^1(K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -))$ to the neutral element $H^1(G, \mathrm{Aut}(E \times_k -))$. Hence

$$\check{H}^1(K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -)) \overset{\mathfrak{f}}{\cong} G^1(G, \mathrm{Aut}(E \times_k K))$$

as pointed sets.

For any finite separable field extension F/k, since k is a perfect field, there always exists a finite Galois extension K/k such that $k \subset F \subset K$, therefore we have

$$\begin{aligned}
\check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(E \times_k K)) &= \varinjlim_{\substack{F/k \text{ finite} \\ \text{separable}}} \check{H}^1(F/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -)) \\
&= \varinjlim_{\substack{K/k \text{ finite} \\ \text{Galois}}} \check{H}^1(K/X_{\acute{e}t}, \mathrm{Aut}(E \times_k -)) \\
&\cong \varinjlim_{\substack{K/k \text{ finite} \\ \text{Galois}}} H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(E \times_k K)) \\
&= \varinjlim_{\substack{K/k \text{ finite} \\ \text{Galois}}} H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(E \times_k \overline{k})^{\mathrm{Gal}(\overline{k}/K)}) \\
&= H^1(G_k, \mathrm{Aut}(E \times_k \overline{k})),
\end{aligned}$$

where $G_k = \mathrm{Gal}(\overline{k}/k)$. In particular, if E is a quasi-projective variety over k which is perfect, the set of equivalence classes of $\overline{k}/k$-forms of E is classified by $H^1(G_k, \mathrm{Aut}(E \times_k \overline{k}))$, so we have a bijection between the set of equivalence classes of $\overline{k}/k$-forms of E and $\check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(E \times_k -))$. The conclusion of the above argument is the following result:

Theorem 6.2.5. *Let E be a scheme over a perfect field k and let $X = \operatorname{Spec} k$. Then we have that E' is a form of E over $X_{\acute{e}t}$ if and only if there exists a finite Galois extension K of k such that*

$$E \times_k K \cong E' \times_k K,$$

and

$$H^1(G_k, \mathrm{Aut}(E \times_k \overline{k})) \cong \check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(E \times_k -)).$$

If E is a quasi-projective variety over k, there exists a bijection between the set of equivalence classes of forms of E over $X_{\acute{e}t}$ and $\check{H}^1(X_{\acute{e}t}, \mathrm{Aut}(E \times_k -))$.

Hence for a variety E over a perfect field k, the definition of forms of E based on étale site coincides that given in the previous chapters.

Example 6.2.6. *Let $X = \operatorname{Spec} A$ for some ring A and $\mathbb{G}_a^n$ be the additive group scheme over X. Let GL_n be the covariant functor $S \mapsto \mathrm{GL}_n(\Gamma(S, \mathcal{O}_S))$ for any scheme S. Then $\mathrm{Aut}(\mathbb{G}_a^n \times_X -) = \mathrm{GL}_n$.*

When A is a local ring, $\check{H}^1(X_{\acute{e}t}, \mathrm{GL}_n) = 0$ ([19], p.124). This implies there are no non-trivial affine forms of $\mathbb{G}_a^n$ over X.

Another special case is $n = 1$, then $\mathrm{GL}_1 = \mathbb{G}_m$, which is the multiplicative group scheme. A version of Hilbert's Theorem 90 ([19], p.124) *gives:*

$$\check{H}^1(X_{\acute{e}t}, \mathbb{G}_m) = \mathrm{Pic}(X),$$

where $\mathrm{Pic}(X)$ is the Picard group of X. For the general discussion of Picard group, see e.g. [11], II.6. *If A is a unique factorization domain, $\mathrm{PicX} = 0$* ([16], p.273)*, and consequently there are no non-trivial affine forms of $\mathbb{G}_a$ over X.*

Example 6.2.7. *Given a scheme S, the set of isomorphic classes of S-forms of the projective space $\mathbb{P}_S^n$ for ALL positive integers n is characterized by the Brauer group of S, denoted by $\mathrm{Br}(S)$* ([7], p.205). *$\mathrm{Br}(S)$ is the generalization of the Brauer group of a field L. When $S = \operatorname{Spec} L$, $\mathrm{Br}(S) = Br(L) \cong H^2(\mathrm{Gal}(L^s/L), (L^s)^\times)$, where L^s is the separable closure of L. For the details of Brauer group of a scheme, see* [19], chapter IV.

Let S be $\operatorname{Spec} L$ *for some field L. We have shown that if L is a finite field, then* $\mathrm{Br}(L)$ *is trivial. It can also be shown the following cases:* ([23], p.162-163)

- $\mathrm{Br}(\mathbb{Q}^{ab})$ *is trivial.*
- *The Brauer group of any field extension of transcendence degree* 1 *over any algebraically closed field is trivial.*
- *$L = \mathbb{R}$, the field of real numbers, we have* $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$*, where the non-zero element in* $\mathbb{Z}/2\mathbb{Z}$ *corresponds to variety*

$$X^2 + Y^2 + Z^2 = 0$$

- *L is a local field (complete with finite residue field), then* $\mathrm{Br}(L) \cong \mathbb{Q}/\mathbb{Z}$.

Appendix A

1. Flatness and faithful flatness

The reference is [17], p.17-26.

Definition 1. *Let B be an A-module. B is called a flat A-module if for any injective A-module homomorphism $f : M \to N$, the induced B-module homomorphism*

$$f \otimes \mathrm{id}_B : M \otimes_A B \to N \otimes_A B,$$

is also injective, where id_B is the identity map on B.

Theorem 2. *Let A and B be rings with ring homomorphism $f : A \to B$, then B is flat over A if and only if $B_{\mathfrak{p}}$ is flat over $A_{f^{-1}(\mathfrak{p})}$ for any $\mathfrak{p} \in \operatorname{Spec} B$.*

Theorem 3. *Let $\varphi : A \to B$ be a flat ring homomorphism, then the followings are equivalent:*

a) $M \xrightarrow{m \mapsto m \otimes 1} M \otimes_A B$ *is injective for any A-module M.*

b) If $N \otimes_A B = 0$ for some A-module N, then $N = 0$.

c) Let $f : M \to N$ be a map of A-modules. Then if $f \otimes \mathrm{id}_B : M \otimes_A B \to N \otimes_A B$ is injective, f is also injective.

Definition 4. *Let $\varphi : A \to B$ be a flat ring homomorphism. We say φ is faithfully flat if φ satisfies the equivalent conditions of Theorem* 3*.*

2. Étale morphisms

The reference is ([19], chapter I). Let S be a scheme. Denote by $\mathcal{O}_{S,s}$ the stalk at point $s \in S$ and denote by $\mathfrak{m}_s$ the maximal ideal of $\mathcal{O}_{S,s}$.

Definition 5. *Let X and Y be schemes and let $f : Y \to X$ be a morphism which is locally of finite-type. Let $y \in Y$ and $x = f(y)$. f is said to be unramified at y if $\mathfrak{m}_x \cdot \mathcal{O}_{Y,y} = \mathfrak{m}_y$ and $\mathcal{O}_{Y,y}/\mathfrak{m}_y$ is a finite separable field extension of $\mathcal{O}_{X,x}/\mathfrak{m}_x$. f is said to be unramified if it is unramified at all points in Y. Here $\mathfrak{m}_x \cdot \mathcal{O}_{Y,y}$ is defined by the map $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ induced by f.*

Definition 6. *Let X and Y be schemes and $f : Y \to X$ be a morphism. f is said to be flat if for any point $y \in Y$, the induced map $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.*

Definition 7. *Let X and Y be schemes and $f : Y \to X$ be a morphism which is locally of finite-type. f is called to be étale if it is flat and unramified.*

Theorem 8 ([1], p.115)**.** *Let k be a field and X be a scheme. Then a morphism $f : X \to \operatorname{Spec} k$ is an étale morphism if and only if $X = \coprod_{i=1}^{n} \operatorname{Spec} k_i$ for some finite separable field extensions $k_1, k_2, \ldots k_n$ of k. Here $\coprod$ means disjoint union.*

Definition 9. *Let F be a field. An étale F-algebra L is an F-algebra and is isomorphic to a finite product $F_1 \times F_2 \times \ldots \times F_m$ as F-algebras, where $F_i\,(i = 1, 2, \ldots, m)$ is a finite separable field extension of k. The degree of L is its dimension $\dim_F L$ as an F-vector space, i.e.*

$$\dim_F L = [F_1 : F] + [F_2 : F] + \ldots + [F_m : F].$$

It is clear the definition of étale algebra is consistent with that of étale morphism.

3. Étale Site

A good introduction to site is [26], Chapter I, II. A site is a generalization of the notion of a topological space.

Definition 10 (Grothendieck)**.** *A Site $\mathfrak{T}$ is a category $\mathcal{T}$ and a set $\mathcal{C}$ each element of which is called a covering and is a set of morphisms in $\mathcal{T}$:*

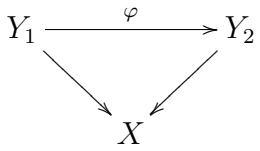
$$\{U_i \xrightarrow{\varphi_i} U \,\big|\, i \in I\},$$

where I is some index set, such that for any morphism $\varphi : V \to U$ in $\mathcal{T}$, the fiber product $U_i \times_U V$ exists in $\mathcal{T}$ for any $i \in I$. $\mathcal{C}$ must also satisfy the following conditions:

- *For any isomorphism $X \xrightarrow{\lambda} Y$ in $\mathcal{T}$, $\{X \xrightarrow{\lambda} Y\} \in \mathcal{C}$.*
- *For any element $\{U_i \xrightarrow{\varphi_i} U \,\big|\, i \in I\} \in \mathcal{C}$ and any morphism $\varphi : V \to U$ in $\mathcal{T}$, $\{U_i \times_U V \to V \,\big|\, i \in I\} \in \mathcal{C}$.*

- *Let* $\{U_i \xrightarrow{\varphi_i} U \,\big|\, i \in I\}$ *be an element in* $\mathcal{C}$*. For each* $i \in I$*, let* $\{V_{ij} \xrightarrow{\phi_{ij}} U_i \,\big|\, j \in I_i\}$ *be a covering. Then* $\{V_{ij} \xrightarrow{\varphi_i \circ \phi_{ij}} U \,\big|\, i \in I, j \in I_i\} \in \mathcal{C}$*.*

Definition 11 ([26], p.86)**.** *Let* X *be a scheme. Denote by* $\acute{E}t/X$ *the category of* X*-schemes in which an object (also called an open set) is an étale morphism* $Y \to X$ *for some scheme* Y*, and a morphism between two objects* $Y_1 \to X$ *and* $Y_2 \to X$ *is a morphism* $\varphi : Y_1 \to Y_2$ *such that the following diagram is commutative:*



Define a site $X_{\acute{e}t}$*, called the étale site of* X*, as follows:*

- *The underlying category* $\mathcal{T}$ *of* $X_{\acute{e}t}$ *is* $\acute{E}t/X$*.*
- *A covering is a set of morphisms* $\{Y_i \xrightarrow{\varphi_i} Y \,\big|\, i \in I\}$ *over* X *in* $\mathcal{T}$ *such that* $Y = \cup_{i \in I} \varphi_i(Y_i)$*.*

Definition 12. *Let* $\mathfrak{T}$ *be a site with underlying category* $\mathcal{T}$*. Let* $\mathcal{A}b$ *be the category of abelian groups. A presheaf on* $\mathfrak{T}$ *with values in* $\mathcal{A}b$ *is a contravariant functor* $\mathscr{F} : \mathcal{T} \to \mathcal{A}b$*.*

Definition 13. *Using notations in Definition* 12*,* $\mathscr{F}$ *is called a sheaf if* $\mathscr{F}$ *is a presheaf and for every covering* $\{U_i \xrightarrow{\varphi_i} U \,\big|\, i \in I\}$ *in* $\mathfrak{T}$*, the following sequence is exact:*

$$\mathscr{F}(U) \to \prod_{i \in I} \mathscr{F}(U_i) \rightrightarrows \prod_{i,j \in I} \mathscr{F}(U_i \times_U U_j).$$

References

[1] A. Altman and S. Kleiman. *Introduction to Grothendieck Duality Theory* (*Lecture Notes in Mathematics 146*). Springer-Verlag, 1970.

[2] S. A. Amitsur. Simple algebras and cohomology groups of arbitrary fields. *Trans. Amer. Math. Soc.*, 90:73–112, 1959.

[3] L. Brünjes. *Forms of Fermat Equations and Their Zeta Functions*. World Scientific, 2004.

[4] G. Chênevert. Some remarks on frobenius and lefschetz in étale cohomology (http://www.math.mcgill.ca/goren/seminaroncohomology/frobenius.pdf).

[5] C. Cid and T. Schulz. Computation of five- and six-dimensional bieberbach groups. *Experimental Mathematics*, 10:109–115, 2001.

[6] A. Deitmar. Panorama of zeta functions. *arXiv:math.NT/0210060v4*, 29 Sep 2005.

[7] D. Eisenbud and J. Harris. *The Geometry of Schemes*. Springer-Verlag, 2000.

[8] E. Freitag and R. Kiehl. *Etale Cohomology and the Weil Conjecture*. Springer-Verlag, 1988.

[9] E. Goren. *Lectures on Hilbert Modular Varieties and Modular Forms (CRM Monograph Series Vol. 14)*. Americal Mathematical Society, 2001.

[10] J. Harris. *Algebraic Geometry: A First Course*.

[11] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1997.

[12] D. Husemöller. *Elliptic Curves*. Springer-Verlag, 1987.

[13] J. Jahnel. The brauer-severi variety associated with a central simple algebra: A survey (www.math.uni-bielefeld.de/lag/man/052.pdf).

[14] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag, 1993.

[15] R. Kolhatkar. *Grassmann Varieties*. http://www.math.mcgill.ca/goren/Students/KolhatkarThesis.pdf.

[16] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Science Publications, 2002.

[17] H. Matsumura. *Commutative Algebra*. W.A. Benjamin,Inc., 1970.

[18] J. S. Milne. *Lectures on Etale Cohomology*. http://www.jmilne.org/math/CourseNotes/math732.pdf.

[19] J. S. Milne. *Étale Cohomology*. Princeton University Press, 1980.

[20] M.-H. Nicole. *Weil Cohomology*. http://www.math.mcgill.ca/goren/SeminarOnCohomology/Weilcohomology.pdf.

[21] L. Ribes. *Introduction of Profinite Groups and Galois Cohomology*. Queen's University, Kingston, Ontario, Canada, 1970.

[22] J.-P. Serre. Zeta and l functions. *Arithematical Algebraic Geometry (Proceeding of a Conference Held at Purdue University/1963), Harper & Row* 1965, p.83-92.

[23] J.-P. Serre. *Local Fields*. Springer-Verlag, 1979.

[24] J.-P. Serre. *Galois Cohomology*. Springer-Verlag, 2002.

[25] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[26] G. Tamme. *Introduction to Étale Cohomology*. Springer-Verlag, 1994.

[27] W. Waterhouse. *Introduction to Affine Group Schemes*. Springer-Verlag, 1979.

[28] A. Weil. The field of definition of a variety. *Amer. J. Math*, 78:509–524, 1956.

[29] R. Westwick. Linear transformations on grassmann spaces. *Pacific Journal of Mathematics*, 14:1123–1127, 1964.