The extension of an elliptic curve by the multiplicative group over F_q

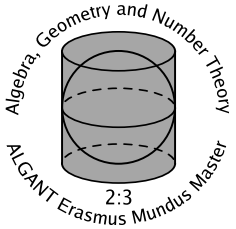
Zhao, H.

Heer Zhao

The extension group of elliptic curve E by $\mathbb{G}_m$ over $\mathbb{F}_q$

Master thesis, defended on June 21, 2007

Thesis advisor: Prof. Bas Edixhoven



Mathematisch Instituut, Universiteit Leiden

Acknowledgements

First of all I am grateful to my thesis supervisor Bas Edixhoven, for his guidance, discussions, and helpful suggestions.

I would like to thank the following people who have helped me during the past three years: Elisa Aghito, Francesco Baldassarri, Luca Barbieri-Viale, Alessandra Bertapelle, Franco Cardin, Bruno Chiarellotto, Andrea D'Agnolo, Albert Facchini, Adrian Iovita, Alessandro Languasco, Federico Menegazzo, Francis Sullivan, Giuseppe Zampieri from Padova, and Johan Bosman, Jan-Hendrik Evertse, Robin de Jong, Bart de Smit, Peter Stevenhagen from Leiden, Boas Erez from Bordeaux. I also thank King Fai Lai, Chuilei Liu, Daqing Wan.

Finally I thank the ALGANT program for funding me to study in Europe, and also thank University Padova and University Leiden.

Contents

1 Introduction

Let $\mathscr{C}$ be the category of abelian varieties over a field k, let G be the Galois group of $\bar{k}/k$, where $\bar{k}$ is a fixed algebraic closure of k, let $\mathscr{D}$ be the category of finitely generated $\mathbb{Z}_l$-modules with continuous G-action, and let l be a prime number which is different from $\mathrm{char}(k)$. Given two objects A and B in $\mathscr{C}$, take $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, f restricts to maps $f : A[l^n] \to B[l^n]$, for all $n \in \mathbb{Z}_{>0}$, and hence it induces a ($\mathbb{Z}_l$-linear) map $T_l(f) : T_l(A) \to T_l(B)$, where $T_l(A)$ and $T_l(B)$ are the corresponding Tate-modules of A and B respectively. We thus get an abelian group homomorphism $\mathrm{Hom}_{\mathscr{C}}(A, B) \to \mathrm{Hom}_{\mathscr{D}}(T_l(A), T_l(B))$. Moreover we have the following elegant theorem.

Theorem 1.1. (Tate, Faltings)Let k be a finite field or a number field, let A and B be abelian varieties over k. Then the map $\mathbb{Z}_l \otimes \mathrm{Hom}_{\mathscr{C}}(A, B) \to \mathrm{Hom}_{\mathscr{D}}(T_l(A), T_l(B))$ is bijective.

In the above theorem, we want to know what would happen if we replace the bifunctor $\mathrm{Hom}_{\mathscr{C}}(\cdot, \cdot)$ by another bifunctor $\mathrm{Ext}_{\mathscr{C}}(\cdot, \cdot)$. To make it easier, we replace A by an elliptic curve E over k, and replace B by the multiplicative group $\mathbb{G}_{m,k}$, also we restrict us to the case that k is a finite field. The fact is, the bijectivity still holds after we did these changes. We will see this in section 3.

2 Preparation

Through all this section, k will be a perfect field. Note that number fields and finite fields are perfect.

2.1 Algebraic Curves

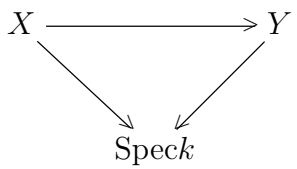
We begin with the definition of k-schemes, where k is a field.

Definition 2.1. An **affine k-scheme** $(X, \mathscr{O}_X)$ is a locally ringed space which is isomorphic to $(\mathrm{Spec}A, \mathscr{O}_{\mathrm{Spec}A})$ for some k-algebra A, together with a morphism of locally ringed spaces $c : X \to \mathrm{Spec}k$, called the structure morphism of $(X, \mathscr{O}_X)$. And the structure morphism c is given by the unique embedding of k-algebras from k into A.

A **k-scheme** is just a locally ringed space $(X, \mathscr{O}_X)$ in which every point has an open neighborhood U such that the induced space $(U, \mathscr{O}_X|_U)$ is isomorphic to some affine k-scheme. It's obvious that the structure morphisms on each affine piece agree on the intersections, hence gives rise to the structure morphism of $(X, \mathscr{O}_X)$. Simply, we will write X to denote the k-scheme $(X, \mathscr{O}_X)$.

Given a point $x \in X$, the **residue field** at x is defined to be $k(x) := \mathscr{O}_{X,x}/m_x$, where m_x is the unique maximal ideal of the local ring $\mathscr{O}_{X,x}$.

Definition 2.2. Given two k-schemes X and Y, a k-scheme morphism f from X to Y is just a morphism of locally ringed spaces f, such that:



commutes. Then we get a category of k-schemes actually, denoted by $k-\mathrm{Sch}$. Given a field K, we define $X(K) := \mathrm{Hom}_{k-\mathrm{Sch}}(\mathrm{Spec}K \to X)$, called the set of K-points of X. The name arises from the fact that to give an element of $X(K)$ is equivalent to give a point $x \in X$ and an inclusion map $k(x) \hookrightarrow K$.

A morphism of k-schemes $f : Y \to X$ is called a **closed immersion**, if it induces a homeomorphism between Y and a closed subset of X, and $f^\sharp : \mathscr{O}_X \to f_*\mathscr{O}_Y$ is surjective. If it is the case, Y is called a **closed subscheme** of X.

Example 2.3. Let k be the finite field $\mathbb{F}_q$, let X be a k-scheme, let $\{\mathrm{Spec}A_i\}_i$ be an open affine covering of X, where A_i's are k-algebras. Then we have ring homomorphisms $\mathrm{Frob}_{q,i} : A_i \to A_i$ by sending $a \in A_i$ to a^q. These give rise to k-scheme morphisms $\mathrm{Frob}_{q,i} : \mathrm{Spec}A_i \to \mathrm{Spec}A_i$, which is just the identity on the underlying topological space $|X|$. On the intersections $\mathrm{Spec}A_i \bigcap \mathrm{Spec}A_j$ the morphisms $\mathrm{Frob}_{q,i}$ and $\mathrm{Frob}_{q,j}$ agree, and by gluing we obtain the q-**Frobenius** morphism Frob_q of X.

Given an algebraic extension $K \supseteq k$, the Frobenius morphism on X induces a map : $X(K) \to X(K)$ by sending $\alpha \in X(K)$ to $\mathrm{Frob}_q \circ \alpha$, simply we still use the same symbol Frob_q to denote this induced map. At the same time, the Galois group $\mathrm{Gal}(K/\mathbb{F}_q)$ acts on $X(K)$ by $\sigma(\alpha) = \alpha \circ \sigma^*$, where $\alpha \in X(K)$, $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q)$, and σ^* is the induced $\mathbb{F}_q$-scheme morphism from the automorphism σ. Let σ_q be the q Frobenius automorphism of K, then we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Spec}K & \xrightarrow{\sigma_q^*} & \mathrm{Spec}K \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ X & \xrightarrow{\mathrm{Frob}_q} & X \end{array}$$

which can be checked locally on the affine pieces. Hence the induced map Frob_q gives the same action on $X(K)$ as $\sigma_q \in \mathrm{Gal}(K/\mathbb{F}_q)$.

Definition 2.4. Let X be an k-scheme, let $\bar{k}$ be a fixed algebraic closure of k.

The k-scheme X is called **irreducible**, if its topological space is irreducible. Moreover, it is called **geometrically irreducible**, if $X_{\bar{k}} = X \otimes_k \bar{k}$ is irreducible.

The k-scheme X is called **reduced**, if for any non-empty open subset

U of X, the ring $\mathscr{O}_X(U)$ has no nilpotent elements. Moreover, it is called **geometrically reduced**, if $X_{\bar{k}}$ is reduced.

The k-scheme X is called **integral**, if for any non-empty open subset U of X, the ring $\mathscr{O}_X(U)$ is an integral domain. X is called **geometrically integral**, if $X_{\bar{k}}$ is integral.

A morphism of k-schemes $f : X \to Y$ is called **of finite type**, if there exists a covering of Y by open affine subsets $\{V_i = \mathrm{Spec}B_i\}_i$, such that for each i, $f^{-1}(V_i)$ can be covered by finitely many open affine subsets $\{U_{i,j} = \mathrm{Spec}A_{i,j}\}$, and each $A_{i,j}$ is a finitely generated B_i-algebra. Moreover, if $f^{-1}(V_i) = \mathrm{Spec}A_i$ for some finite B_i-algebra, i.e. A_i is a finitely generated B_i-algebra and also a finitely generated B_i-module, then f is called a **finite morphism**. The morphism f is called **separated**, if the diagonal morphism $\Delta : X \to X \times_Y X$ is a closed immersion. The morphism f is called **proper**, if it is separated, of finite type, and universally closed. The morphism f is called universally closed, if f is closed, and for any morphism $Y' \to Y$, the morphism $f' : X \times_Y Y' \to Y'$ given by the base change is also closed.

Remark 2.5. In particular, in the above definition we choose f to be the structure morphism of a k-scheme X. Then if f is of finite type (resp. separated, proper), we will call X is of finite type (resp. separated, proper) over k. And X is of finite type, if it can be covered by finite number of open affine subsets $\mathrm{Spec}B_i$, where the B_i's are finitely generated k-algebras.

Definition 2.6. Let k be a field. A **curve** over k is an integral separated scheme X of finite type over k, geometrically irreducible, and of dimension 1. A curve X is called **complete** over k, if it is proper over k.

A curve X is called **regular**, if all the local rings of X are regular local rings. Moreover, X is called **geometrically regular**, if $X_{\bar{k}} = X \otimes_k \bar{k}$ is regular for a fixed algebraic closure $\bar{k}$ of k. Note that since we have assume that k is perfect in the beginning of this section, the regularity is equivalent to the geometrical regularity.

Take $x \in X$, X is called **smooth at** x, if at every point $\bar{x}$ of $X_{\bar{k}}$ lying over x the local ring $\mathscr{O}_{X_{\bar{k}},\bar{x}}$ is regular. We say X is **smooth** if it is smooth

at every point. In fact, this is equivalent to saying X geometrically regular.

Proposition-Definition 2.7. Given an integral k-scheme X, there exists a unique point η, such that the closure of $\{\eta\}$ is the whole space. This is called the **generic point** of X.

Proof. Since X is integral, it follows that X is irreducible and any non-empty open subset of X is dense. We can pick up an open affine subset $U = \mathrm{Spec}A$ of X, where A is an integral k-algebra. Let η be the point of X corresponding to the zero prime ideal of A, then we have $\{\eta\}$ is the unique point in U whose closure in $\mathrm{Spec}A$ is $\mathrm{Spec}A$. Moreover the closure of $\{\eta\}$ in X is X, since U is dense in X. If there is another point ξ with the same property, then $\overline{\{\xi\}} = X$ implies that $U \bigcap \{\xi\}$ is not empty. Then we have $\xi \in U$, which means ξ is also a generic point of the affine U. But there is only one generic point for U, so $\xi = \eta$. We are done. □

Definition 2.8. Let C be a curve over a field k. Then we define the **function field** of C to be the local ring $\mathscr{O}_\eta$ where η is the generic point of C , denoted by $K(C)$.

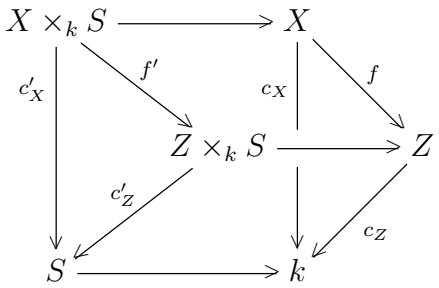
Proposition 2.9. Let X be a complete smooth curve over k, let Y be any curve over k, and let $f : X \to Y$ be a morphism. Then either (1) $f(X)$ consists of only one point, or (2) $f(X) = Y$. In case (2), f is a finite morphism, and Y is also complete.

To prove this, we need a lemma.

Lemma 2.10. Let $f : X \to Y$ be a morphism of separated k-schemes of finite type over k, with X proper over k. Then $f(X)$ is closed in Y, and $f(X)$ with its image k-subscheme structure is proper over k.

Proof. Let c_X and c_Y be the structure morphisms of X and Y respectively, then both c_X and c_Y are separated, and c_X is also proper. Since we have $c_X = c_Y \circ f$, it follows that f is proper (see Hartshorne's book [5, II Corollary 4.8]). Hence $f(X)$ is closed in Y.

Let $Z = f(X)$ and c_Z be the structure morphism of Z, then the closed immersion $i : Z \hookrightarrow Y$ is separable. Since Y is separable over k, i.e. c_Y is separable, $c_Z = c_Y \circ i$ is separable over k, hence Z is separable over k. From the fact that X is of finite type over k, we have that Z is also of finite type over k. To prove Z is proper over k, we are left to prove that c_Z is universally closed. Given a morphism of k-schemes $\alpha : S \to k$, we have the following commutative diagram:



where f', c'_X and c'_Z are the morphisms obtained by base change. Since f is surjective, f' is surjective. At the same time, c'_X is closed and $c'_Z = c'_Z \circ f'$, hence c'_Z is also closed. So we know c_Z is universally closed. □

Proof of proposition *(2.9):* Since X is complete, by the above lemma, $f(X)$ is closed in Y, and proper over k. On the other hand, $f(X)$ is irreducible. Thus either (1) $f(X) = pt$, or (2) $f(X) = Y$, and in case (2), Y is also complete.

In case (2), f will maps the generic point η of X to the generic point ξ of Y. Otherwise, if $f(\eta) = y$ is a closed point, then $\eta \in f^{-1}(y)$. Since f is continuous, it follows $f^{-1}(y)$ is closed. Then $X = \overline{\{\eta\}} \subseteq f^{-1}(y)$, which implies $X = f^{-1}(y)$. This contradicts that to the $f(X) = Y$. Then f induces a k-algebra morphism $f^\sharp : \mathscr{O}_{Y,\xi} \to \mathscr{O}_{X,\eta}$. This is just an inclusion of function fields, i.e., $K(Y) \to K(X)$. Since both fields are finitely generated extension fields of transcendence degree 1 of k, $K(X)$ must be a finite algebraic extension of $K(Y)$. To show that f is a finite morphism, let $V = \mathrm{Spec}B$ be any open affine subset of Y. Let A be the integral closure of B in $K(X)$. Then A is a finite B-module, and $\mathrm{Spec}A$ is isomorphic to some open subset U of X. Clearly $U = f^{-1}(V)$, so this means that f is a finite morphism. □

Definition 2.11. If $f : X \to Y$ is a finite morphism of curves, then the **degree** of f is defined to be the degree of the field extension $[K(X) : K(Y)]$.

2.2 Divisors

Let k be a field, let C be a complete smooth curve and C_0 be the subset of closed points of C.

Definition 2.12. The **divisor group** on C is the free $\mathbb{Z}$-module with basis C_0, denoted by $\mathrm{Div}(C)$. A element D of $\mathrm{Div}(C)$ is called a divisor on C, which is just a formal sum $D = \sum_{x \in C_0} n_x x$, with $n_x \in \mathbb{Z}$ and only finitely many $n_x \neq 0$

Since C is smooth, the local ring $\mathscr{O}_x$ at any point $x \in C$ is a DVR (discrete valuation ring). Then the function field $K(C)$ of C is equal to the fraction field of $\mathscr{O}_x$. It follows that we get a valuation $v_x : K(C)^\times \to \mathbb{Z}$, associated to x. Let $f \in K(C)^\times$,

Claim: Let $f \in K(C)^\times$, there are only finitely many x in C_0 such that $v_x(f) \neq 0$.

Proof of the claim: Take an open affine subset $U = \mathrm{Spec}B$ of C, with B an integral k-algebra of dimension 1. Then we have $f \in K(C) = \mathrm{Frac}(B)$. If $f \notin B$, we can replace U by a smaller non-empty open subset $V = \mathrm{Spec}B_1$ of U, such that $f \in B_1$. Then the zero set $V(f)$ inside V is a finite set. Also, since C is integral and of dimension 1, $C - V$ is a finite set. So there are only finitely many x in C_0 such that $v_x(f) \neq 0$. □

Now we can associate to every element $f \in K(C)^\times$ a divisor

$$(f) = \sum_{x \in C_0} v_x(f) \cdot x.$$

A **principal divisor** is a divisor of the form $\mathrm{div}(f)$ for some $f \in K(C)^\times$. Note that if $f, g \in K(C)^\times$, then $(f/g) = (f) - (g)$ because $v_x(f/g) = v_x(f) - v_x(g)$. So we get a group morphism $\mathrm{div} : K(C)^\times \to \mathrm{Div}(C)$, and all the principal divisors consist a subgroup of $\mathrm{Div}(C)$, denoted by $\mathrm{PDiv}(C)$. And we define the divisor class group of C to be the quotient $\mathrm{Div}(C)/\mathrm{PDiv}(C)$, denoted by $\mathrm{Cl}(C)$. Two divisors D and D' on C are called linearly equivalent, if $D - D'$ is a principal divisor, denoted by $D \sim D'$.

Definition 2.13. Let $D = \sum_{x \in C_0} n_x \cdot x$ be a divisor on C. The degree of D is defined by $\deg(D) := \sum_{x \in C_0} n_x \cdot \dim_k k(x)$, where $k(x)$ is the residue field at x.

Remark 2.14. Consider the base change $\alpha : \bar{C} \to C$, where $\bar{C} = C \times_k \bar{k}$. For $x \in C_0$, since k is perfect, $k \to k(x)$ is separable. It follows that $\alpha^{-1}(x)$ consists of $\dim_k k(x)$ reduced points of $\bar{C}$. In particular, if $k = \bar{k}$ (i.e. k is algebraically closed), then $k(x) = k$ for all closed points $x \in C_0$. Then $\deg(D) := \sum_{x \in C_0} n_x$, which coincides with the usual definition of degree of divisors on curves over an algebraically closed field.

In fact, the definition of degree of divisors gives rise a $\mathbb{Z}$-module morphism $\deg : \mathrm{Div}(C) \to \mathbb{Z}$. It follows that the kernel of deg is a subgroup of $\mathrm{Div}(C)$, denoted by $\mathrm{Div}^0(C)$.

After the definition of divisor group on a curve, we come to see how to construct a morphism between the divisor groups on curves, once we have a finite morphism of curves.

Definition 2.15. If $f : X \to Y$ is a finite morphism of smooth curves, we want to define a homomorphism $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$. It is enough to define it on the basis of $\mathrm{Div}(Y)$, i.e., on the subset of closed points of Y. For any closed point $Q \in Y$, let t be a uniformizer at Q ,i.e., t is an element of $K(Y)^\times$ such that $v_Q(t) = 1$, where v_Q is the valuation corresponding to the discrete valuation ring $\mathscr{O}_{Y,Q}$. We define $f^*(Q) = \sum_{f(P)=Q} v_P(t) \cdot P$. Since f is a finite morphism, this is a finite sum, so we get a divisor on X. Note that this definition is independent of the choice of the uniformizer t. In fact, if t' is another uniformizer at Q, then $t' = t \cdot u$ where u is a unit in $\mathscr{O}_Q$. Then for any point $P \in X$ with $f(P) = Q$, from the morphism on the stalks $f^\sharp : \mathscr{O}_{Y,Q} \to \mathscr{O}_{X,P}$, we know u is still a unit in $\mathscr{O}_{X,P}$, so $v_P(t) = v_P(t')$.

Remark 2.16. The map f^* preserves the principal divisors, this is because

for any $g \in K(Y)^\times$,

$$\begin{aligned} f^*((g)) &= f^*(\sum_{y \in Y_0} v_y(g) \cdot y) \\ &= \sum_{y \in Y_0} v_y(g) \cdot f^*(y) \\ &= \sum_{y \in Y_0} v_y(g) \sum_{f(x)=y} v_x(t_y) \cdot x \\ &= \sum_{y \in Y_0} \sum_{f(x)=y} v_y(g) v_x(t_y) \cdot x \\ &= \sum_{x \in X_0} v_x(f^\sharp g) \cdot x \\ &= (f^\sharp(g)) \end{aligned}$$

where t_y is the uniformizer of the local ring at y.

Proposition 2.17. Let $f : X \to Y$ be a finite morphism of regular curves. Then for any divisor D on Y, we have $\deg(f^*(D)) = \deg(f) \cdot \deg(D)$.

Proof. It suffices to prove that for any closed point $y \in Y$ we have $\deg(f^*(y)) = \deg(f)$. In fact, since $K(X)/K(Y)$ is a finite field extension, the proof is quite similar to the case in the finite extension of number fields. Take an affine open subset $V = \mathrm{Spec}B$ of Y containing y, then B is a Dedekind Domain from the fact that Y is regular curve. Let A be the integral closure of B in $K(X)$, A is again a Dedekind Domain. Then, $U := \mathrm{Spec}A$ is the open subset $f^{-1}(V)$ of X. Let $A' = A \otimes_B \mathscr{O}_{Y,y}$, then we get a ring extension$\mathscr{O}_{Y,y} \hookrightarrow A'$ inside the finite field extension $K(Y) \hookrightarrow K(X)$. $\mathscr{O}_{Y,y}$ is a DVR, in particular a PID. And all these ring are inside the field $K(X)$, so A' is torsion-free $\mathscr{O}_{Y,y}$-module, hence a free $\mathscr{O}_{Y,y}$-module and of rank $n := [K(X) : K(Y)] = \deg(f)$. Let t be the uniformizer of $\mathscr{O}_{Y,y}$, then A'/tA' is a $k(y)$-vector space of dimension n, where $k(y)$ is the residue field at y.

On the other hand, the points x_i of X such that $f(x_i) = y$ are in 1-1 correspondence with the maximal ideals m_i of A', and for each i, $A'_{m_i} = \mathscr{O}_{X,x_i}$. Clearly $tA' = \cap_i (tA'_{m_i} \cap A')$, so by the Chinese remainder theorem, $\dim_{k(x)} A'/tA' = \sum_i \dim_{k(x)} A'/(tA'_{m_i} \cap A')$. But $A'/(tA'_{m_i} \cap A') \cong$

$A'_{m_i}/(tA'_{m_i} = \mathscr{O}_{X,x_i}/t\mathscr{O}_{X,x_i}$, so the dimensions in the sum above are just equal to $v_{x_i}(t)$. But $f^*(y) = \sum v_{x_i}(t) \cdot x_i$, so we have shown that $\deg(f^*(y)) = \deg(f)$ as required. □

Corollary 2.18. Let C be a smooth complete curve. Then the map div : $K(C)^\times \to \mathrm{Div}(C)$ has kernel k^*, and has image inside $\mathrm{Div}^0(C)$.

Proof. Let's first prove it in case $C = \mathbb{P}^1_k$ which is smooth complete, then we generalize it to the general case. For any $f \in K(\mathbb{P}^1_k)^\times$ with $\mathrm{div}(f) = 0$, we have that f has no poles, it follows that f lies in $\mathscr{O}_{\mathbb{P}^1_k}(\mathbb{P}^1_k) = k$. On the other hand, $f \in k^\times$ implies $(f) = 0$. Hence $\ker(\mathrm{div}) = k^\times$. To prove $\mathrm{image}(\mathrm{div}) \subseteq \mathrm{Div}^0(C)$, since $\mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$ for any $f, g \in K(\mathbb{P}^1_k)^\times$ and $K(\mathbb{P}^1_k) = k(x)$, it suffices to prove it for f irreducible in $k[x]$. Let $U = \mathrm{Spec}k[x]$ and $V = \mathrm{Spec}k[y]$ be affine open subsets covering $\mathbb{P}^1_k$, and the coordinate change on $U \bigcap V$ is given by $x \mapsto y^{-1}$. Then on U, f does not have poles and has only one zero which is the point α associated to the prime ideal (f). Now we are left to investigate the situation at the only point outside U, which we denote by ∞. Let $g(y) = f(1/y)$, then $v_\infty(g) = -\deg(g) = -\deg(f)$. So the divisor associated to f is just $D = \alpha - \deg(f) \cdot \infty$, and $\deg(D) = \dim_k k(\alpha) - \deg(f) = 0$.

Now let's return to the general case. Let $f \in K(C)^\times$. If $f \in k$, then $(f) = 0$. Now assume $f \notin k$ with $\mathrm{div}(f) = 0$, we want to make a contradiction. Since C is geometrically irreducible, we must have f is transcendental over k. Otherwise, if f is algebraic over k, then let $F(y)$ be the minimal polynomial of f over k. Since C is geometrically regular, $F(y)$ cannot have multiple root in $\bar{k}$; C is geometrically irreducible, $F(y)$ must have only one root inside $\bar{k}$. Then $F(y)$ can only be a linear polynomial, and then $f \in k$, which gives rise to a contradiction. So $k(f) \subseteq K(C)$ is a finite field extension. This induces a finite morphism $\varphi : C \to \mathbb{P}^1_k$, which is surjective by proposition (2.9). Take $\beta \in \varphi^{-1}(0)$ (here 0 is used to denote the zero point of $\mathbb{P}^1_k$), then we must have $f(\beta) = 0$, i.e. $v_\beta(f) > 0$. This contradicts to $\mathrm{div}(f) = 0$, hence such f must be in k.

Let's now turn to prove that any principal divisor has degree 0. Let f be

in $K(C)^\times - k^\times$ and put $D := \mathrm{div}(f)$. As before, we still have the surjective finite morphism $\varphi : C \to \mathbb{P}^1_k$. Now since the principal divisor on $\mathbb{P}^1_k$ associated to x is just $\mathrm{div}(x) = 0 - \infty$, where x is the generator of the function field of the projective line over k. Then $\mathrm{div}(f) = \varphi^*(0 - \infty)$. Since $\deg(\mathrm{div}(x)) = 0$, by the previous proposition, we have $\deg(\mathrm{div}(f)) = \deg(f) \cdot \deg(\mathrm{div}(x)) = \deg(f) \cdot 0 = 0$. Hence the map div has its image inside $\mathrm{Div}^0(C)$. □

Definition 2.19. Let C be a smooth complete curve. Since the image of the map div is inside $\mathrm{Div}^0(C)$, we can define a quotient group $\mathrm{Cl}^0(C) := \mathrm{Div}^0(C)/\mathrm{PDiv}(C)$, called the divisor class group of degree zero.

Now we want to associate a line bundle to a given divisor. First we need to define line bundles.

Definition 2.20. Let $(X, \mathscr{O}_X)$ be a ringed space. A **sheaf of $\mathscr{O}_X$-module** (or simply an **$\mathscr{O}_X$-modules**) is a sheaf $\mathscr{F}$ on X, such that for each open set U of X, the group $\mathscr{F}(U)$ is an $\mathscr{O}_X(U)$-module, and for each $V \subset U$ the restriction homomorphism $\mathscr{F}(U) \to \mathscr{F}(V)$ is compatible with the module structures via the ring homomorphism $\mathscr{O}_X(U) \to \mathscr{O}_X(V)$. A morphism $\mathscr{F} \to \mathscr{G}$ of sheaves of $\mathscr{O}_X$-modules is a morphism of sheaves, such that for each open subset U of X, the map $\mathscr{F}(U) \to \mathscr{G}(U)$ is a homomorphism of $\mathscr{O}_X(U)$-modules.

The tensor product $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G}$ of two $\mathscr{O}_X$-modules is defined to be the sheaf associated to the presheaf $U \mapsto \mathscr{F}(U) \otimes_{\mathscr{O}_X(U)} \mathscr{G}(U)$. We will often write simply $\mathscr{F} \otimes \mathscr{G}$, with $\mathscr{O}_X$ understood.

An $\mathscr{O}_X$-module $\mathscr{F}$ is free if it is isomorphic to a direct sum of copies of $\mathscr{O}_X$. It is locally free if X can be covered by open subsets U for which $\mathscr{F}|_U$ is a free $\mathscr{F}|_U$-module. In that case the rank of $\mathscr{F}$ on such an open set is the number of copies of structure sheaf needed. If X is connected, then the rank of a locally free sheaf is the same everywhere. In particular, a locally free sheaf of rank 1 is called an **invertible sheaf**, also called a **line bundle**.

In fact, on a ringed space $(X, \mathscr{O}_X)$, the set of all invertible sheaves modulo isomorphisms forms a group under the operation $\otimes$, and the identity element

is just the class of the structure sheaf $\mathscr{O}_X$, the inverse of an invertible sheaf $\mathscr{L}$ is the dual sheaf $\mathcal{H}om(\mathscr{L}, \mathscr{O}_X)$. This group is called the **Picard group** of X, denoted by $\mathrm{Pic}(X)$.

Let C be a smooth curve, $D = \sum_{x \in C_0} n_x \cdot x \in \mathrm{Div}(C)$ a divisor on C. We can associate an invertible sheaf to D. First we define a presheaf $\mathscr{L}(D)$ on C by:

$$\mathscr{L}(D)(U) = \{f \in K(C) | \forall x \in U_0 : v_x(f) \geq -n_x\}$$

where U is any non-empty open affine subset of X and U_0 is the subset of closed points of U. Since for any $f, g \in K(C)$, $f|_U = g|_U$ for any non-empty open subset U implies $f = g$, it follows that $\mathscr{L}(D)$ is actually a sheaf that is an $\mathscr{O}_C$-module. Moreover it is an invertible $\mathscr{O}_C$-module. The reason is as follows: let $x \in C_0$, if $n_x = 0$, let U be the complement of $\mathrm{Supp}(D)$ (Here $\mathrm{Supp}(D)$ is the set consisting of the points y with $n_y \neq 0$), then $\mathscr{L}(D)|_U = \mathscr{O}|_U$. In general, let $U := \{x\} \cup (C - \mathrm{Supp}(D))$. Let t_x be an uniformizer at x. Let $U' \subseteq U$ be a neighborhood of x on which t_x is regular and has x as its only zero. Multiplication by $t_x^{-n_x}$ induces an isomorphism from $\mathscr{O}_C|_{U'}$ to $\mathscr{L}(D)|_{U'}$. So $\mathscr{L}(D)$ is an invertible sheaf.

Conversely, let $\mathscr{L}$ be an invertible sheaf on C, we can define a divisor D associated to $\mathscr{L}$. Let η be the generic point of C, then $\mathscr{L}_\eta$ is a $K(C)$-vector space of dimension one. Let s be a basis of this vector space, let $x \in C_0$ and s_x is a basis of the $\mathscr{O}_{C,x}$-module $\mathscr{L}_x$, we have $\mathscr{L}_\eta \cong K(C)s$, $\mathscr{L}_x \cong \mathscr{O}_{C,x} s_x$, and a morphism $\mathscr{L}_x \to \mathscr{L}_\eta$ between the stalks at η and x. This implies that there exists a unique $f_x \in K(C)^\times$ such that $s = f_x s_x$. We define $D := \sum_{x \in C_0} v_x(f_x)$ to be the divisor associated to $\mathscr{L}$ (note:$v_x(f_x)$ is independent of the choice of s_x). If we choose another basis $f \cdot s$ for $\mathscr{L}_\eta$ with $f \in K(C)^\times$, then we get another divisor $D' = \mathrm{div}(f) + D$, hence we actually get a unique divisor from $\mathscr{L}$ up to principal divisors. Then we have a morphism of $\mathscr{O}_C$-modules $\mathscr{L}(D) \to \mathscr{L}$ sending f to fs on each open subset U . Further, this map is an isomorphism.

Proposition 2.21. Let C be a curve, then we have an isomorphism $\mathrm{Cl}(C) \to \mathrm{Pic}(C)$, which sends divisor class $[D]$ to the invertible sheaf isomorphic class

$[\mathscr{L}(D)]$.

Proof. By the above construction, we have a map $\varphi : \mathrm{Div}(C) \to Pic(C)$. Since for any invertible sheaf $\mathscr{L}$, $\mathscr{L} \cong \mathscr{L}(D)$ where D is the divisor associated to $\mathscr{L}$, so this map is surjective. We still need to show this map is a group morphism and has kernel $\mathrm{PDiv}(C)$. It's obvious that $\mathscr{L}(\mathrm{div}(f)) \cong \mathscr{O}_C$ with the isomorphism given by multiplication by f, so $\varphi(0) = 0$ and $\mathrm{PDiv}(C)$ is contained in the kernel. Take two divisors $D = \sum_{x \in C_0} n_x x$ and $D' = \sum_{x \in C_0} n'_x x$. Then on an open subset of C,

$$\begin{aligned}
\mathscr{L}(D)(U) &= \{f \in K(C) | \forall x \in U_0 : v_x(f) \geq -n_x\}, \\
\mathscr{L}(-D')(U) &= \{f \in K(C) | \forall x \in U_0 : v_x(f) \geq n'_x\}, \\
\mathscr{L}(D - D')(U) &= \{f \in K(C) | \forall x \in U_0 : v_x(f) \geq n'_x - n_x\} \\
&= \{g \in K(C) | \forall x \in U_0 : v_x(f) \geq -n_x\} \cdot \{h \in K(C) | \forall x \in U_0 : v_x(f) \geq n'_x\} \\
&= \mathscr{L}(D)(U)\mathscr{L}(-D')(U) \\
&= \mathscr{L}(D)(U) \otimes_{\mathscr{O}_C(U)} \mathscr{L}(-D')(U), \\
\mathscr{O}_C(U) &= \mathscr{L}(0)(U) = \mathscr{L}(D - D)(U) = \mathscr{L}(D)(U) \otimes_{\mathscr{O}_C(U)} \mathscr{L}(-D)(U),
\end{aligned}$$

So $\mathscr{L}(D) = \mathscr{L}(-D)^\vee$, $\mathscr{L}(D - D') = \mathscr{L}(D) \otimes_{\mathscr{O}_C} \mathscr{L}(D')$, it follows that φ is a group morphism. To show that the kernel of φ is $\mathrm{PDiv}(C)$, we need to prove that $\mathscr{L}(D) \cong \mathscr{O}_C$ implies $D = \mathrm{div}(f)$ for some $f \in K(C)$. Let $\phi : \mathscr{O}_C \to \mathscr{L}(D)$ be an isomorphism, let $f := \phi(1)$. Since 1 is a basis of $\mathscr{O}_C$, f is a basis of $\mathscr{L}(D)$. Hence for any open subset U of C and $g \in K(C)^\times$ we have $gf \in \mathscr{L}(D)(U)$ if and only if $g \in \mathscr{O}_C(U)$. The first condition is equivalent to: $\mathrm{div}(g)|_U + \mathrm{div}(f)|_U \geq -D|_U$(the ordering is the partial ordering in which $\sum_x n_x x \geq \sum_x n'_x x$ if and only if $n_x \geq n'_x$ for all x, we will use it again later). The second condition is equivalent to: $\mathrm{div}(g)|_U \geq 0$. It follows that $\mathrm{div}(f) = -D$, which means $D \in \mathrm{PDiv}(C)$. So we have $Cl(C) \cong Pic(C)$.

□

2.3 Differentials

First, let's state the algebraic theory of differentials and give some proposition without proof. And for the proof, see Matsumura's book [11].

Let A be a ring (commutative with identity), let B be an A-algebra, let M be a B-module.

Definition 2.22. An A-derivation of B into M is a map $d : B \to M$ such that (1) d is A-linear, (2) $d(bb') = bd(b') + b'd(b)$ for any $b, b' \in B$.

Remark 2.23. In the above definition, we actually have $d(a) = 0$ for any $a \in A$. Because $d(a) = ad(1)$, and $d(1) = d(1 \cdot 1) = d(1) + d(1)$ implies $d(1) = 0$.

Definition 2.24. The module of relative differential forms of B over A is a B-module $\Omega_{B/A}$, together with an A-derivation $d : B \to \Omega_{B/A}$, which satisfies the following universal property: for any B-module M, and for any A-derivation d' of B into M, $\exists$ a unique B-module homomorphism $f : \Omega_{B/A} \to M$, such that $d' = f \circ d$.

Remark 2.25. By the universal property, if the module of relative differential forms of B over A exists, it is unique up to a unique isomorphism. A way to construct such a module is similar to the way to construct the tensor product of two modules over a ring. Take the free B-module generated by the symbols $\{db | b \in B\}$, then take the quotient by the submodule generated by the elements of the form $d(ab + a'b') - a(db) - a'(db')$ and $d(bb') - b(db') - b'(db)$, where b, b' are any elements in B. We denote this quotient B-module by $\Omega_{B/A}$, and define a map $d : B \to \Omega_{B/A}$ by sending b to db. Then $(\Omega_{B/A}, d)$ satisfies the universal property obviously, and is a module of relative differential forms of B over A.

Example 2.26. Let $B = A[x_1, \cdots, x_n]$ be the polynomial ring over a ring A, then by the above construction, $\Omega_{B/A}$ is just the free B-module with basis $(dx_1, \cdots, dx_n)$.

Proposition 2.27. (1) If A' and B are A-algebras, let $B' = B \otimes_A A'$. Then $\Omega_{B'/A'} \cong \Omega_{B/A} \otimes_B B'$.

(2) If S is a multiplicative system in B, then $\Omega_{S^{-1}B/A} \cong S^{-1}\Omega_{B/A}$.

(3) If B is an A-algebra, I is an ideal of B, and let $C = B/I$. Then there is a natural exact sequence of C-modules

$$I/I^2 \xrightarrow{\delta} \Omega_{B/A} \otimes_B C \longrightarrow \Omega_{C/A} \longrightarrow 0$$

where for any $b \in I$, if $\bar{b}$ is its image in I/I^2, then $\delta(\bar{b}) = d(b) \otimes 1$. Note in particular that I/I^2 has a natural C-module structure, and that δ is a C-linear map, even though it is defined via the derivation $d : B \to \Omega_{B/A}$.

Example 2.28. Let A be a field k, let $B = k[x_1, \cdots, x_n]$ and $I = (f_1, \cdots, f_r)$, where r, n are some positive integers and $f_1, \cdots, f_r$ are the polynomials in B, let $C = B/I$. Then by the previous example we have $\Omega_{B/k} = \oplus_{i=1}^n B \cdot dx_i$, and by the third part of the above proposition we have

$$I/I^2 \xrightarrow{\delta} \Omega_{B/k} \otimes_B C \longrightarrow \Omega_{C/k} \longrightarrow 0.$$

Since $\Omega_{B/k} \otimes_B C = \oplus_{i=1}^n B \cdot dx_i \otimes_B C = \oplus_n^{i=1} C \cdot dx_i$, and $im(\delta) = \sum_{i=1}^r C \cdot df_i$, it follows that $\Omega_{C/k} = \oplus_{i=1}^n C \cdot dx_i / \sum_r^{i=1} C \cdot df_i$.

Now we turn to define the sheaves of differentials on k-schemes. Let X be a k-scheme, for any open affine $U = \mathrm{Spec}B$, we associate a quasi-coherent $\mathscr{O}_X|_U$-module $\widetilde{\Omega_{B/k}}$. By the second part of the above proposition, we know $\Omega_{B/k}$ is compatible with localization, so we can glue the quasi-coherent $\mathscr{O}_X|_U$-modules $\widetilde{\Omega_{B/k}}$ on each affine piece into a quasi-coherent $\mathscr{O}_X$-module, denoted by $\Omega_{X/k}$ or simply by Ω_X. This is called the **sheaf of differentials** on X. At the same time, we also have an k-derivation $d : \mathscr{O}_X \to \Omega_X$, which is the universal k-derivation on $\mathscr{O}_X$.

Remark 2.29. Let C be a curve over a field k. By the compatibility of taking the module of differential with localization, we have $\Omega_{C,x} = \Omega_{\mathscr{O}_{C,x}/k}$ for any $x \in C$. In particular, if we take the generic point η of C, we have $\Omega_{C,\eta} = \Omega_{\mathscr{O}_{C,\eta}/k} = \Omega_{K(C)/k}$. Also, we have that $K(C) = \mathscr{O}_{C,x} \otimes_{\mathscr{O}_{C,x}} K(C)$

implies $\Omega_{K(C)/k} = \Omega_{\mathscr{O}_{C,x}/k} \otimes_{\mathscr{O}_{C,x}} K(C)$. Hence we get $\Omega_{C,\eta} = \Omega_{K(C)/k} = \Omega_{\mathscr{O}_{C,x}/k} \otimes_{\mathscr{O}_{C,x}} K(C) = \Omega_{C,x} \otimes_{\mathscr{O}_{C,x}} K(C)$.

Let's focus on curves to understand the k-derivations on them. Let C be a curve over a field k. Then C is smooth if and only if it's locally of the form Spec$B$, with $B = k[x_1, \cdots, x_n]/(f_1, \cdots, f_r)$, where $f_1, \cdots, f_r$ are in $k[x_1, \cdots, x_n]$ and n, r are some positive integers, such that $\text{rank}(\frac{\partial f_i}{\partial x_j}) = n-1$ at all $x \in C$.

Definition 2.30. Let C be a curve, and let η be the generic point of C. The **space of meromorphic differential forms** on C, denoted by $\mathcal{M}_C$, is the stalk $\Omega_{C,\eta}$ of the sheaf Ω_C at the generic point.

Let C be an complete smooth curve. By remark 2.29, $\mathcal{M}_C$ is a $K(C)$-vector space of dimension 1. Let $\omega \in \mathcal{M}_C$, let $x \in C$ be a closed point, let s be a generator of $\Omega_{C,x}$. Since $\mathcal{M}_C = \Omega_{C,\eta} = \Omega_{C,x} \otimes K(C)$, there exist an unique $f \in K(C)$ such that $\omega = f \cdot s$. Let $D_x := v_x(f)$, then this number is independent the choice of s_x. In fact if we choose another generator s'_x, then $s_x = s'_x \cdot u$ for some $u \in \mathscr{O}^\times_{C,x}$, it follows that $v_x(f) = v_x(fu)$. Now we can associate a divisor $\text{div}(\omega) := \sum_{x \in C_0} D_x \cdot x$ to the meromorphic differential ω. Since $\mathcal{M}_C$ is a $K(C)$-vector space of dimension 1, then the quotient of any two non-zero meromorphic differentials must be an element of $K(C)^\times$, hence the divisors associated to them are linearly equivalent. We will call anyone of them the **canonical divisor**, which is actually an class inside $\text{Cl}^0(C)$ (Here $\text{Cl}^0(C)$ is the divisor class group of degree zero).

2.4 The Riemann-Roch Theorem

In this section, we will give the Riemann-Roch theorem, which is one of the most beautiful and useful theorems for curves. It helps us describe the the functions on curves having given zeros and poles. First, we need some notations before giving the theorem.

In this section, C will always be a smooth complete curve over a field k. Then C is actually projective. We have seen that the sheaf of differentials

Ω_C on C is an invertible sheaf.

Definition 2.31. The genus $g(C)$ of C is defined to be the dimension of the k-vector space of $H^0(C,\Omega) = \Gamma(C,\Omega_C)$, which is the set of global sections of the curve.

Remark 2.32. From the definition, we always have $g(C) \geq 0$.

Definition 2.33. A divisor $D = \sum_{x\in C_0} n_x x$ is **effective** if all $n_x \geq 0$, denoted by $D \geq 0$.

From this, we can put a partial ordering on $\mathrm{Div}(C)$. Given two divisors $D, D' \in \mathrm{Div}(C)$, $D \geq D'$ if $D - D'$ is effective.

The k-vector space $L(D) := \{f \in K(C)^\times | \mathrm{div}(f) + D \geq 0\} \cup \{0\}$ This is nothing new, but the set of global sections $H^0(C,\mathscr{L}(D)) = \Gamma(C,\mathscr{L}(D))$ of the invertible sheaf associated to D. The number $l(D)$ is defined to be the dimension of $L(D)$. This is actually well-defined, later we will see $L(D)$ is a finite dimension k-vector space.

Proposition 2.34. Let $D \in \mathrm{Div}(C)$.
(1) If $\deg(D) < 0$, then $L(D) = \{0\}$ and $l(D) = 0$.
(2) The dimension of the k-vector space $L(D)$ is finite.
(3) If D' is linearly equivalent to D, then $L(D) \cong L(D')$, so $l(D) = l(D')$.

Proof. (1). If $f \neq 0$ and $f \in L(D)$, then $\mathrm{div}(f) + D \geq 0$, hence

$$0 \leq \deg(\mathrm{div}(f) + D) = \deg((f)) + \deg(D) = \deg(D) < 0.$$

This gives a contradiction. So $L(D) = \{0\}$ and $l(D) = 0$.

(2). Let $x \in C$ be a closed point, then the sheaf $\mathscr{L}(D-x)$ is a subsheaf of $\mathscr{L}(D)$ by the definition of such sheaves. Then we have a short exact sequence of sheaves:

$$0 \to \mathscr{L}(D-x) \to \mathscr{L}(D) \to \mathscr{L}(D)/\mathscr{L}(D-x) \to 0.$$

We can regard x as a closed k-subscheme, then the structure sheaf of x is just the constant sheaf $k(x)$, where $k(x)$ is the residue field at x. It's obvious that

$\mathscr{L}(D)/\mathscr{L}(D-x) \cong k(x)$, so $H^0(C, \mathscr{L}(D)/\mathscr{L}(D-x))$ is a finite dimensional k-vector space and $H^1(C, \mathscr{L}(D)/\mathscr{L}(D-x)) = 0$. Taking the long exact cohomology sequence of the above short exact sequence of sheaves, we get:

$$0 \to \Gamma(C, \mathscr{L}(D-x)) \to \Gamma(C, \mathscr{L}(D)) \to \Gamma(C, \mathscr{L}(D)/\mathscr{L}(D-x))$$
$$\to H^1(C, \mathscr{L}(D-x)) \to H^1(C, \mathscr{L}(D)) \to 0.$$

So $l(D) < \infty$ if and only if $l(D-x) < \infty$. Since we can subtract points from D to make $D < 0$ in finite steps, by using this procedure, it follows that $l(D) < \infty$ if and only if $l(D') < \infty$ for some $D' < 0$. Hence from (1), we know $l(D) < \infty$.

(3). Since $D - D' = \mathrm{div}(f)$ for some $f \in K(C)^\times$, $\mathscr{L}(D)$ is isomorphic to $\mathscr{L}(D')$ by multiplication by f^{-1}. So $L(D) \cong L(D')$, and $l(D) = l(D')$. □

Theorem 2.35 (Riemann-Roch Theorem)**.** Let C be a smooth complete curve of genus g over a field k, let K be a canonical divisor on C. Then

$$l(D) - l(K-D) = \deg(D) + 1 - g.$$

We will use Serre duality to prove it, so let's first state the Serre duality theorem without proof.

Lemma 2.36 (Serre's duality theorem for curves)**.** Let C be a smooth complete curve over a field k, let Ω_C be the invertible sheaf of differentials on C. Then for any locally free sheaf $\mathscr{F}$ on C there are natural isomorphisms:

$$H^i(C, \mathscr{F}) \cong H^{1-i}(C, \mathscr{F}^\vee \otimes \Omega_C)^\vee$$

for $i = 0, 1$. Note that the symbol $\vee$ outside denotes the dual k-vector space.

Proof. See Hartshorne's book [5, chapter 3, §7]. □

Proof of Riemann-Roch Theorem: The divisor $K - D$ corresponds to the invertible sheaf $\Omega_C \otimes \mathscr{L}(D)^\vee$. By Serre's duality theorem, we have that $H^1(C, \mathscr{L}(D)) \cong H^0(C, \Omega_C \otimes \mathscr{L}(D)^\vee) = L(K-D)$. So $l(D) - l(K-D)$ is equal to the Euler Characteristic of $\mathscr{L}(D)$

$$\chi(\mathscr{L}(D)) = \dim H^0(C, \mathscr{L}(D)) - \dim H^1(C, \mathscr{L}(D)).$$

So we need to show

$$\chi(\mathscr{L}(D)) = \deg(D) + 1 - g.$$

In the case $D = 0$, this just says that

$$\dim H^0(C, \mathscr{O}_C) - \dim H^1(C, \mathscr{O}_C) = 0 + 1 - g.$$

This is true, since our C is actually projective, it follows that $H^0(C, \mathscr{O}_C) = k$ and

$$\dim H^1(C, \mathscr{O}_C) = \dim H^0(C, \mathscr{O}_C^\vee \otimes \Omega_C) = \dim H^0(C, \Omega_C) = g.$$

For the general divisor D, we will reduce to the case $D = 0$. The method is to prove that the formula holds for D if and only if it holds for $D + x$ for x any closed point of C. Since any divisor can be reached from 0 in a finite number of steps by adding or subtracting a point each time, this will complete the general cases.

Similar to the case in the prove of proposition 2.34(2), we consider x as a closed subscheme of C and have a short exact sequence of sheaves:

$$0 \to \mathscr{L}(D) \to \mathscr{L}(D + x) \to k(x) \to 0.$$

Take the long exact sequence of cohomology, we have:

$$0 \to L(D) \to L(D + x) \to k(x) \to H^1(C, \mathscr{L}(D)) \to H^1(C, \mathscr{L}(D + x)) \to 0.$$

So we have:

$$l(D) - l(D + x) + \dim k(x) - \dim H^1(C, \mathscr{L}(D)) + \dim H^1(C, \mathscr{L}(D + x)) = 0.$$

This gives that $\chi(\mathscr{L}(D)) - \chi(\mathscr{L}(D + x)) = \dim k(x) = \deg(x)$. On the other hand, $\deg(D + x) = \deg(D) + \deg((x)) = \deg(D) + 1$, so the formula holds for D if and only if it holds for $D + x$, as required. □

Corollary 2.37. Let C be a smooth complete curve of genus g, let K be a canonical divisor on C.
(1) $\deg(K) = 2g - 2$.
(2) Let D be a divisor on C, if $\deg(D) > 2g - 2$, then $l(D) = \deg(D) - g + 1$.

Proof. (1). Take $D = K$ in Riemann-Roch formula, we get

$$l(K) - l(0) = \deg(K) + 1 - g.$$

Since $g = l(K)$ and $l(0) = 1$, we have $\deg(K) = 2g - 2$.
(2). Since $\deg(D) > 2g - 2$ and $\deg(K) = 2g - 2$, so $\deg(K - D) < 0$, it follows that $l(K - D) = 0$. Applying the Riemann-Roch theorem, we have

$$l(D) - 0 = \deg(D) + 1 - g,$$

hence $l(D) = \deg(D) + 1 - g$ □

2.5 Elliptic Curves

Now we will discuss a special kind of curves, the so-called elliptic curves. The elliptic curves have so nice properties that there are abundant theories and elegant results related to them.

Definition 2.38. An **elliptic curve** over a field k is a pair (E, O), where E is a smooth complete curve over k, of genus 1, and O is a k-rational point (the origin). Sometime, we just simply write E to denote (E, O).

A reason why elliptic curves are import is that we can put a group structure on it. Now we will assume that the base field k is algebraically closed to construct the group structure. If k is not algebraically closed, we just restrict the group structure of $E(\bar{k})$ to $E(k)$, where $E(k)$ can be regarded as the subset of $E(\bar{k})$ fixed by the Galois group of $\bar{k}/k$.

Lemma 2.39. Let C be a smooth complete curve over an algebraically closed field k, of genus 1. Let $P, Q \in C_0$, then $P \sim Q$, i.e. P is linearly equivalent to Q as divisors, if and only if $P = Q$.

Proof. Suppose $P - Q = \mathrm{div}(f)$ for some $f \in K(C)^\times$, then $f \in L(Q)$(here (Q). By Corollary 2.37 Part(2), we have $l(Q) = \deg(Q) + 1 - g = 1$. Since the constant functions are already in $L(Q)$, so we must have $L(Q) = k$ and $f \in k$. Hence $P = Q$. □

Proposition 2.40. Let (E,O) be an elliptic curve over an algebraically closed field k.
(1) For every divisor $D \in \mathrm{Div}^0(E)$, there exists a unique point $P \in E_0$ such that $D \sim P - O$.
Let $\sigma : \mathrm{Div}^0(E) \to E_0$ be the map given by the above association.
(2) The map σ is surjective.
(3) Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. Thus σ induces a bijection of sets (which we still denote as σ) $\sigma : \mathrm{Cl}^0 \to E_0$.
(4) The inverse to σ is the map

$$\kappa : E_0 \to \mathrm{Cl}^0(E), P \mapsto [P - O].$$

Proof. (1). Since $\deg(D+O) = 1 > 0 = 2g-2$, by Corollary 2.37 Part (2), it follows that $l(D+O) = \deg(D+O) + 1 - 1 = 1$. So $L(D+O) = k \cdot f$ for some $f \in K(C)^\times$, i.e., f is the generator of the 1-dimensional k-vector space $L(D+O)$. Then $\mathrm{div}(f) + D + O > 0$ and of degree 1, so it must be equal to a divisor P for some point $P \in E_0$. Hence $D = P - O - (f)$, $D \sim P - O$. In fact, such a point P is unique. If R is another point with such property, then $P - O \sim D \sim R - O$, so $P \sim R$, by the previous lemma, we have $P = R$.
(2). This is trivial, since $\sigma(P-O) \sim P - O$.
(3). Suppose that $\sigma(D_i) = P_i - O$ with $P_i \in E_0$ for $i = 1, 2$, then we have $D_i \sim P_i - O$ for $i = 1, 2$. So

$$\begin{aligned} D_1 \sim D_2 &\Leftrightarrow P_1 - O \sim P_2 - O \\ &\Leftrightarrow P_1 \sim P_2 \\ &\Leftrightarrow P_1 = P_2 \\ &\Leftrightarrow \sigma(D_1) = \sigma(D_2). \end{aligned}$$

(4). This is obvious. □

From the above proposition, we know there is a bijection between $\mathrm{Cl}^0(E)$ and E_0. Since Cl^0 is a group, we can just put the group structure of $\mathrm{Cl}^0(E)$ on E_0 to make it into an abstract group. In fact, this is also an algebraic group, i.e., the group operations are morphism of varieties after we treat the set E_0 of closed points of E as an algebraic variety. We will give a non-complete proof as follows.

Proposition 2.41. Under the group structure taken from the bijection $\mathrm{Cl}^0(E) \to E_0$, E_0 is an (commutative) algebraic group, i.e. the group operations are morphisms of varieties.

Proof. We only need to prove that the inverse map and the addition map are morphisms of algebraic varieties. We assume k is algebraically closed. First let's construct the inverse element $-P$ and the sum $P + Q$, where P and Q are two given point on E_0. By corollary 2.37, we know that $l(2O) = \mathrm{dim}L(2O) = 2$ and $l(3O) = \mathrm{dim}L(3O) = 3$. Then there exists functions

$x, y \in K(E)$, such that $L(2O) = k + kx$ and $L(3O) = k + kx + ky$. Note that x must have its only pole of order exact order 2 at O, and y must have its only pole of exact order 3 at O.

If $P = O$, then $-P = P = O$ and $P + Q = Q$. Assume $P \in E_0 - \{O\}$, then x is regular at P. Let $f = x - x(P)$, then f has a zero at P and $\mathrm{div}(f) = P + P' - 2O$, for some $P' \in E_0 - \{O\}$. Hence $-P$ is just P'.

If $Q = O$, then we have $P + Q = P$. Assume $Q \in E_0 - \{O\}$, and we consider the sysem of simultaneous linear equations:

$$\begin{cases} x(P)X + y(P)Y + Z = 0 \\ x(Q)X + y(Q)Y + Z = 0 \end{cases}$$

Take a nontrivial solution (a, b, c) of the above system, let $g = ax + by + c$. If $Q = -P$, we have $P + Q = O$. We assume $Q \neq -P$, then $b \neq 0$ (otherwise, by the above construction for $-P$ we have $Q = -P$). Thus g has a pole of order 3 at O, and $\mathrm{div}(g) = P + Q + R - 3O$ for some unique point R in $E_0 - \{O\}$. So we get $P + Q = -R$.

Now we give a geometric interpretation of the above construction, which shows that the group operations are morphism of varieties. Embed E_0 into $\mathbb{P}^2$ by $(x, y, 1)$, then the image of O in $\mathbb{P}^2$ is just the point $(0, 1, 0)$. Since $l(6O) = 6$ and $\{1, x, y, x^2, xy, y^2, x^3\} \in L(6O)$, $1, x, y, x^2, xy, y^2, x^3$ are k-linear dependent, i.e., there exist $a_0, \cdots, a_6 \in k$ such that

$$a_0 + a_1 x + a_2 y + a_3 x_2 + a_4 xy + a_5 y^2 + a_6 x^3 = 0. \tag{2.1}$$

We draw a line

$$aX + bY + cZ = 0 \tag{2.2}$$

passing through P, Q in $\mathbb{P}^2$, and another line

$$X - x(P)Z = 0 \tag{2.3}$$

passing through P and O, where (X, Y, Z) are the homogeneous coordinates of $\mathbb{P}^2$. Let $\phi(X, Y, Z) = (aX + bY + cZ)/Z$ and $\varphi(X, Y, Z) = (X - x(P)Z)/Z$, then ϕ and φ give rise to two elements in $K(E)$, and $\mathrm{div}(\phi) = P + Q + R$,

$\mathrm{div}(\varphi) = P + P' - 2O$. So R (resp. P') is one of the intersection points of (2.1) and (2.2) (resp. (2.3)), it follows that the coordinate of R (resp. P') is a rational function of the coordinates of P, Q (resp. P), which means the operations are not far from morphisms of algebraic groups. In fact, they are morphism of algebraic groups, we omit the long details of proof for this, see Silverman's book [18, chapter III, §3, Theorem 3.6].

After embedding E into $\mathbb{P}^2$, for any field automorphism σ of $\bar{k}$, we can apply σ to the coefficients of the equation of E. Then we get a new elliptic curve E^σ. Then E^σ is defined by

$$\sigma(a_0) + \sigma(a_1)x + \sigma(a_2)y + \sigma(a_3)x_2 + \sigma(a_4)xy + \sigma(a_5)y^2 + \sigma(a_6)x^3 = 0.$$

Since everything we have proved for E shifts to E^σ, the morphism $+ : E \times E \to E$ will be sent to $+ : E^\sigma \times E^\sigma \to E^\sigma$. If k is not algebraically closed, we can first regard E as an elliptic curve over $\bar{k}$. Since the rational functions of the coordinates of E giving rise to $+ : E \times E \to E$ are therefore invariant under $\sigma \in (\bar{k}/k)$, so they are actually rational functions with coefficients in k. Thus what we have said so far is valid for any elliptic curve defined over any perfect field. □

Remark 2.42. In (2.1), $a_5 a_6 \neq 0$, since otherwise every term would have a different order pole at O, and so all a_i's would vanish. Replacing x, y by $-a_5 a_6 x, a_5 a_6^2 y$ and dividing by $a_5^3 a_6^4$ gives a cubic equation of the form

$$y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6 \tag{2.4}$$

for some $b_1, \cdots, b_6 \in k$. The equations of such form are called the **Weierstrass equation**. In fact, every elliptic curve can be given by a smooth Weierstrass equation up to isomorphism, for details of this see Silverman's book [18, chapter III, §1, §2, §3].

Also from the proof of the above proposition, for any field extension $k' \supset k$, the k'-points $E(k')$ form a group.

Now we turn to study the maps between elliptic curves, especially isogenies.

Definition 2.43. Let (E, O) and (E', O) be elliptic curves over a field k. A **morphism** between (E, O) and (E', O) is a morphism of curves over k $\phi : E \to E'$ satisfying $\phi(O) = O$ (Here we use O to denote both of the zero points on E and E' with a little bit of ambiguity). An **isogeny** is a nonzero morphism of elliptic curves. And we say that E and E' are **isogenous** if there is an isogeny ϕ between them.

By proposition (2.9), a morphism ϕ satisfies either $\phi(E) = \{O\}$ or $\phi(E) = E'$. Thus except for the zero morphism, defined by $[0](P) = O$ for all $P \in E_0$, every other morphism is a finite morphism of curves, hence we can talk about the degree of ϕ. By convention, we set $\deg([0]) = 0$. We let $\mathrm{Hom}(E, E') = \{\text{morphisms } \phi : E \to E'\}$, then this is actually a group, since elliptic curves are groups. The addition law on $\mathrm{Hom}(E, E')$ is given by $(\phi+\varphi)(P) = \phi(P)+\varphi(P)$ for any $\phi, \varphi \in \mathrm{Hom}(E, E')$. We use $\mathrm{End}(E)$ to denote $\mathrm{Hom}(E, E)$.

Since we have a group structure on an elliptic curve E, we can define a morphism multiplication $[m] : E \to E$ for $m \in \mathbb{Z}$. For $P \in E_0$, if $m > 0$, $[m](P) := \underbrace{P + \cdots + P}_{m}$; if $m < 0$, $[m](P) := [-m](-P)$; and $[0](P) = O$. We write $E(k)[m]$ to denote the kernel of the morphism $[m]$ over a field k.

Given an isogeny $\phi : E \to E'$, we can define the dual isogeny to ϕ as follows. By definition (2.15), ϕ induces a map $\phi^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$. By remark (2.16) ϕ^* keeps the principal divisors, and by proposition (2.17) ϕ^* maps $\mathrm{Div}^0(E')$ into $\mathrm{Div}^0(E)$, hence we have a map $\phi^* : \mathrm{Cl}^0(E') \to \mathrm{Cl}^0(E)$. Assume $k = \bar{k}$, on the other hand, we have group isomorphisms

$$\kappa : E_0 \to \mathrm{Cl}^0(E), P \longmapsto [(P) - (O)]$$

and

$$\kappa' : E'_0 \to \mathrm{Cl}^0(E'), P' \longmapsto [(P') - (O)].$$

Hence we obtain a morphism going in the opposition direction to ϕ, namely the composition

$$E'_0 \xrightarrow{\kappa'} \mathrm{Cl}^0(E') \xrightarrow{\phi^*} \mathrm{Cl}^0(E) \xrightarrow{\kappa^{-1}} E_0.$$

Proposition 2.44. Let $\phi : E \to E'$ be an isogeny of degree m (hence $m > 0$).
(a) Let $\hat{\phi} = \kappa^{-1} \circ \phi^* \circ \kappa'$, then $\hat{\phi} : E' \to E$ is an isogeny. Moreover, it's the unique isogeny satisfying $\hat{\phi} \circ \phi = [m]$ on E. Symmetrically we also have $\phi \circ \hat{\phi} = [m]$ on E'.
(b) Let $\varphi : E \to E'$ be another isogeny. Then we have that $\widehat{\phi + \varphi} = \hat{\phi} + \hat{\varphi}$.
(c) For all $m \in \mathbb{Z}$, we have that $\widehat{[m]} = [m]$ and $\deg([m]) = m^2$ on E. We write $E(K)[m]$ to denote the kernel of the isogeny $[m]$ over some field K. If $\mathrm{char}(k) = 0$ or m is prime to $\mathrm{char}(k)$, then $E(\bar{k})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
(d) $\deg(\hat{\phi}) = \deg(\phi)$.
(e) $\hat{\hat{\phi}} = \phi$.

Proof. See Silverman's book [18, chapter III, §6]. □

3 Main theorem

Now we will give an answer to the problem mentioned in the introduction.

Through all this section, (E, O) will be an elliptic curve over a finite field $\mathbb{F}_q$, where q is a power of some prime p, G will be the Galois group of $\bar{\mathbb{F}}_q$ over $\mathbb{F}_q$, $\mathbb{G}_m$ will be the multiplicative group over $\mathbb{F}_q$, l will be a prime different from p, $T_l(E)$ and $T_l(\mathbb{G}_m)$ will be the corresponding (l-adic) Tate modules of E and $\mathbb{G}_m$ respectively. (For the definition of Tate modules, see Silverman's book [18, III § 7].)

Since the action of G on each $E(\bar{\mathbb{F}}_q)[l^n]$ commutes with the multiplications by l-powers used to construct the Tate module, G also acts on $T_l(E)$. Further, since the pro-finite group $G = \hat{\mathbb{Z}}$ acts continuously on each finite (discrete) group $E(\bar{\mathbb{F}}_q)[l^n]$, the resulting action on $T_l(E)$ is also continuous. By the same reason, we also have that the action of G on $T_l(\mathbb{G}_m)$ is continuous. Since $T_l(E) \cong \mathbb{Z}_l^2$ and $T_l(\mathbb{G}_m) \cong \mathbb{Z}_l$, after we choose $\mathbb{Z}_l$-bases for them, we get two continuous Galois representations $\rho : G \to GL_2(\mathbb{Z}_l)$ and $\chi : G \to GL_1(\mathbb{Z}_l) = \mathbb{Z}_l^\times$.

We will use $\mathscr{C}$ to denote the category of finitely generated $\mathbb{Z}_l$-modules with continuous G-action. From the above description, we get two objects $(T_l(E), \rho)$ and $(T_l(\mathbb{G}_m), \chi)$ in $\mathscr{C}$. Now we want to compare the two extension groups $\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m))$ and $\mathrm{Ext}(E, \mathbb{G}_m)$. Let

$$0 \to \mathbb{G}_m \xrightarrow{\alpha} M \xrightarrow{\beta} E \to 0 \tag{3.1}$$

be an extension in the category of algebraic groups, i.e., it gives an element in $\mathrm{Ext}(E, \mathbb{G}_m)$, then we have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & M & \longrightarrow & E & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle l^n\cdot} & & \downarrow{\scriptstyle l^n\cdot} & & \downarrow{\scriptstyle l^n\cdot} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & M & \longrightarrow & E & \longrightarrow & 0 \end{array} \tag{3.2}$$

where $l^n\cdot$ denotes the multiplication by l^n for some positive integer n. By the snake lemma, we have an exact sequence

$$0 \to \mathbb{G}_m(\bar{\mathbb{F}}_q)[l^n] \xrightarrow{\alpha} M(\bar{\mathbb{F}}_q)[l^n] \xrightarrow{\beta} E(\bar{\mathbb{F}}_q)[l^n] \to \mathrm{coker}(\mathbb{G}_m(\bar{\mathbb{F}}_q) \xrightarrow{l^n\cdot} \mathbb{G}_m(\bar{\mathbb{F}}_q)) \tag{3.3}$$

Since the map $\mathbb{G}_m(\bar{\mathbb{F}}_q) \xrightarrow{l^n\cdot} \mathbb{G}_m(\bar{\mathbb{F}}_q)$ is surjective,

$$\operatorname{coker}(\mathbb{G}_m(\bar{\mathbb{F}}_q) \xrightarrow{l^n\cdot} \mathbb{G}_m(\bar{\mathbb{F}}_q)) = 0$$

it follows that we get a short exact sequence of abelian groups

$$0 \to \mathbb{G}_m(\bar{\mathbb{F}}_q)[l^n] \xrightarrow{\alpha} M(\bar{\mathbb{F}}_q)[l^n] \xrightarrow{\beta} E(\bar{\mathbb{F}}_q)[l^n] \to 0 \tag{3.4}$$

Since $(\mathbb{G}_m(\bar{\mathbb{F}}_q)[l^n])_n$ satisfies the Mittag-Leffler condition, (i.e.

$$\mathbb{G}_m(\bar{\mathbb{F}}_q)[l^m] \xrightarrow{l^{m-n}\cdot} \mathbb{G}_m(\bar{\mathbb{F}}_q)[l^n]$$

is surjective for any $m \geq n$), we have the following exact sequence:

$$0 \to T_l(\mathbb{G}_m) \to T_l(M) \to T_l(E) \to 0. \tag{3.5}$$

Note this short exact sequence is compatible with the continuous G-action, hence we get an element of $\operatorname{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m))$. This gives rise to a map

$$\Phi : \operatorname{Ext}(E, \mathbb{G}_m) \longrightarrow \operatorname{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m)). \tag{3.6}$$

In fact, this is not only a map, but also a morphism of abelian groups. The reason is as follows.

If we have another extension $0 \to \mathbb{G}_m \to M' \to E \to 0$, then the sum of the two extensions M and M' is constructed by the following two steps:
Step (1):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m \times \mathbb{G}_m & \longrightarrow & M \times M' & \longrightarrow & E \times E & \longrightarrow & 0 \\ & & {\scriptstyle \nabla_{\mathbb{G}_m}}\downarrow & & \downarrow & & {\scriptstyle id}\downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & M_1 & \longrightarrow & E \times E & \longrightarrow & 0 \end{array} \tag{3.7}$$

where $\nabla_{\mathbb{G}_m}$is the codiagonal map (i.e. sending $(a, b) \in \mathbb{G}_m \times \mathbb{G}_m$ to $ab \in \mathbb{G}_m$), and M_1 is the push-out of $\mathbb{G}_m$ and $M \times M'$ in the above diagram.
Step (2):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & M_2 & \longrightarrow & E & \longrightarrow & 0 \\ & & {\scriptstyle id}\downarrow & & \downarrow & & {\scriptstyle \Delta_E}\downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & M_1 & \longrightarrow & E \times E & \longrightarrow & 0 \end{array} \tag{3.8}$$

where Δ_E is the diagonal map (i.e. sending $a \in E$ to $(a, a) \in E \times E$), and M_2 is the pull-back of M_1 and E in the above diagram.

Then the isomorphic class of the upper short exact sequence $0 \to \mathbb{G}_m \to M_2 \to E \to 0$ in the above diagram is just the sum of M and M' in $\mathrm{Ext}(E, \mathbb{G}_m)$ (Here we just use M to denote the corresponding extension of E by $\mathbb{G}_m$). For more details of the extensions of algebraic groups, see Serre's book [16].

Taking the corresponding Tate modules in the diagram (3.3), we get a commutative diagram compatible with the G-action on every Tate module:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_l(\mathbb{G}_m) \times T_l(\mathbb{G}_m) & \longrightarrow & T_l(M) \times T_l(M') & \longrightarrow & T_l(E) \times T_l(E) & \longrightarrow & 0 \\ & & {\scriptstyle \nabla_{T_l(\mathbb{G}_m)}}\downarrow & & \downarrow & & {\scriptstyle id}\downarrow & & \\ 0 & \longrightarrow & T_l(\mathbb{G}_m) & \longrightarrow & T_l(M_1) & \longrightarrow & T_l(E) \times T_l(E) & \longrightarrow & 0 \end{array} \tag{3.9}$$

By the same reason as in the statement of the exactness of (3.1), we have that the rows of (3.5) are exact. Similarly, from (3.4), we get another commutative diagram with exact rows which is compatible with the G-action:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_l(\mathbb{G}_m) & \longrightarrow & T_l(M_2) & \longrightarrow & T_l(E) & \longrightarrow & 0 \\ & & {\scriptstyle id}\downarrow & & \downarrow & & {\scriptstyle \Delta_{T_l(E)}}\downarrow & & \\ 0 & \longrightarrow & T_l(\mathbb{G}_m) & \longrightarrow & T_l(M_1) & \longrightarrow & T_l(E) \times T_l(E) & \longrightarrow & 0 \end{array} \tag{3.10}$$

By (3.5) and (3.6), we have that

$$\Phi(M + M') = \Phi(M_2) = T_l(M) + T_l(M') = \Phi(M) + \Phi(M').$$

This shows that $\Phi : \mathrm{Ext}(E, \mathbb{G}_m) \longrightarrow \mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m))$ is actually a abelian group morphism. Moreover, since $\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m))$ has a $\mathbb{Z}_l$-module structure, we get a $\mathbb{Z}_l$-module morphism:

$$\Phi : \mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Ext}(E, \mathbb{G}_m) \longrightarrow \mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m)).$$

Note here we still use the same symbol Φ to denote the $\mathbb{Z}_l$-module morphism. In fact, Φ is not only a morphism.

Theorem 3.1 (Main theorem)**.** As before, let (E, O) will be an elliptic curve over a finite field $\mathbb{F}_q$, where q is a power of some prime p, G will be the Galois group of $\bar{\mathbb{F}}_q$ over $\mathbb{F}_q$, $\mathbb{G}_m$ will be the multiplicative group over $\mathbb{F}_q$, l will be a prime different from p. Then Φ is an isomorphism.

To prove this theorem, we use three steps. Firstly, we will compute $\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m))$ explicitly in terms of ρ and χ. Secondly, we will compute $\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Ext}(E, \mathbb{G}_m)$ explicitly in terms of ρ and χ. After these computations, we will find that the two objects are finite abelian groups of the same order. At last, we will prove that Φ is injective, hence Φ is an isomorphism.

Theorem 3.2. Let $\rho : G \to GL_2(\mathbb{Z}_l)$ be the action on $\mathbb{Z}_l^2$ obtained by a choice of $\mathbb{Z}_l$-basis of $T_l(E)$, let $\chi : G \to \mathbb{Z}_l^\times$ be the action on $T_l(\mathbb{G}_m) \cong \mathbb{Z}_l$. Then $\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m)) \cong \mathrm{coker}(\mathbb{Z}_l^2 \xrightarrow{\rho(1)^t - q} \mathbb{Z}_l^2)$, where $\rho(1)^t$ is the transpose of the matrix corresponding to the Frobenius action on $T_l(E)$. Moreover, this is a finite l-group.

To prove this, we need some lemmas.

Lemma 3.3. Let M be a finitely generated $\mathbb{Z}_l$-module, then $\mathrm{Aut}_{\mathbb{Z}_l}(M) \cong \mathrm{Aut}_{\mathbb{Z}_l}(M_f) \oplus \mathrm{Aut}_{\mathbb{Z}_l}(M_t) \oplus \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)$, where M_t is the torsion part of M and M_f is the quotient M/M_t which is free. Moreover, $\mathrm{Aut}_{\mathbb{Z}_l}(M)$ has a profinite group structure.

Proof. Since $\mathbb{Z}_l$ is a principal ideal domain and M is a finitely generated $\mathbb{Z}_l$-module, we can decompose M into $M \cong M_f \oplus M_t$, with $M_f \cong \mathbb{Z}_l^r$ the free part of M, and $M_f \cong \mathbb{Z}/l^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/l^{r_s}\mathbb{Z}$ the torsion part of M, for some positive integers $r, r_1, \cdots, r_s$. Given an element $f \in \mathrm{End}_{\mathbb{Z}_l}(M)$, since f must map M_t into M_t, f restrict to a morphism $f_t : M_t \to M_t$. Since $M_f \cong M/M_t$, we get another morphism $f_f : M_f \to M_f$. Then we get a map $\Phi : \mathrm{End}_{\mathbb{Z}_l}(M) \to \mathrm{End}_{\mathbb{Z}_l}(M_f) \oplus \mathrm{End}_{\mathbb{Z}_l}(M_t)$ by sending f to (f_f, f_t), this is obviously an $\mathbb{Z}_l$-module epimorphism. To find the kernel of Φ, we consider

the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_t & \longrightarrow & M & \longrightarrow & M_f & \longrightarrow & 0 \\ & & {\scriptstyle f_t}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f_f}\downarrow & & \\ 0 & \longrightarrow & M_t & \longrightarrow & M & \longrightarrow & M_f & \longrightarrow & 0 \end{array}$$

If $f \in \ker(\Phi)$, then we have $\ker(f_f) = M_f$ and $\mathrm{coker}(f_t) = M_t$. By the snake lemma we get a morphism $f' : M_f \to M_t$ inside $\mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)$, which can be canonically embedded into $\mathrm{End}_{\mathbb{Z}_l}(M)$. Conversely, $\mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)$ is obviously inside the kernel of Φ. So we get a short exact sequence:

$$0 \to \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t) \to \mathrm{End}_{\mathbb{Z}_l}(M) \to \mathrm{End}_{\mathbb{Z}_l}(M_f) \oplus \mathrm{End}_{\mathbb{Z}_l}(M_t) \to 0$$

Since we have a canonical section:

$$\mathrm{End}_{\mathbb{Z}_l}(M_f) \oplus \mathrm{End}_{\mathbb{Z}_l}(M_t) \to \mathrm{End}_{\mathbb{Z}_l}(M)$$

by sending (f_1, f_2) to $f_1 \oplus f_2$, it follows that:

$$\mathrm{End}_{\mathbb{Z}_l}(M) \cong (\mathrm{End}_{\mathbb{Z}_l}(M_f) \oplus \mathrm{End}_{\mathbb{Z}_l}(M_t)) \oplus \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t).$$

If $f \in \mathrm{Aut}_{\mathbb{Z}_l}(M)$, then $f_f \in \mathrm{Aut}_{\mathbb{Z}_l}(M_f)$ and $f_t \in \mathrm{Aut}_{\mathbb{Z}_l}(M_t)$. Conversely, given $f_1 \in \mathrm{Aut}_{\mathbb{Z}_l}(M_f)$, $f_2 \in \mathrm{Aut}_{\mathbb{Z}_l}(M_t)$, and $f_3 \in \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)$, then $((f_1^{-1}, f_2^{-1}), -f_2^{-1} f_3 f_1^{-1})$ is just the inverse of $((f_1, f_2), f_3)$. Hence

$$\mathrm{Aut}_{\mathbb{Z}_l}(M) \cong \mathrm{Aut}_{\mathbb{Z}_l}(M_f) \oplus \mathrm{Aut}_{\mathbb{Z}_l}(M_t) \oplus \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t).$$

Since both $\mathrm{Aut}_{\mathbb{Z}_l}(M_t))$ and $\mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)$ are finite groups, and

$$\mathrm{Aut}_{\mathbb{Z}_l}(M_f) = GL_r(\mathbb{Z}_l) = \varprojlim_n GL_r(\mathbb{Z}/l^n\mathbb{Z})$$

is a profinite group, it follows that $\mathrm{Aut}_{\mathbb{Z}_l}(M_f)$ is a profinite group. □

Lemma 3.4. Let M be a finitely generated $\mathbb{Z}_l$-module, then there is a bijection between $\mathrm{Hom}_{\mathrm{GP}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M))$ and $\mathrm{Hom}_{\mathrm{TGp}}(\hat{\mathbb{Z}}, \mathrm{Aut}_{\mathbb{Z}_l}(M))$, where Gp denotes the category of groups and TGp denotes the category of topological groups.

Proof. From the morphisms $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ for every $n \in \mathbb{N}_{>0}$, we get a morphism $i : \mathbb{Z} \to \hat{\mathbb{Z}}$. This is injective, since $i(m) = 0$ for some $m \in \mathbb{Z}$ implies that $n|m$ for every $n \in \mathbb{Z}$, hence $m = 0$. Since $\hat{\mathbb{Z}} = \varprojlim_{n>0}(\mathbb{Z}/n\mathbb{Z})$, $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$.

Now let's assume M is free $\mathbb{Z}_l$-module of rank r. Let ρ be an element of $\mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M))$, let $g = \rho(1)$. Since $\mathrm{Aut}_{\mathbb{Z}_l}(M) \cong \mathrm{GL}_r(\mathbb{Z}_l)$, and we also have a short exact sequence

$$1 \to 1 + l^n \mathrm{Mat}_r(\mathbb{Z}_l) \to \mathrm{GL}_r(\mathbb{Z}_l) \to \mathrm{GL}_r(\mathbb{Z}_l/l^n\mathbb{Z}_l) \to 1$$

for every positive integer n, where $\mathrm{Mat}_r(\mathbb{Z}_l)$ is the $r \times r$-matrix ring over $\mathbb{Z}_l$. For any positive integer n_0, let $\bar{g}$ be the image of g in $\mathrm{GL}_r(\mathbb{Z}/l^{n_0}\mathbb{Z})$, let $m = \mathrm{order}(\bar{g})$, then we have that $g^m \in 1 + l^{n_0}\mathrm{Mat}_r(\mathbb{Z}_l)$, hence for any $k \in \mathbb{N}_{>0}$, $g^{km} \in 1 + l^{n_0}\mathrm{Mat}_r(\mathbb{Z}_l)$. This shows that ρ is actually continuous at 0, where $\mathbb{Z}$ is endowed with the topology induced from the embedding $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$. Further, since ρ is a group morphism, ρ is also a topological group morphism. Since $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$ and $\mathrm{GL}_r(\mathbb{Z}_l)$ is a profinite group, it follows that ρ can be extended to a unique topological morphism $\bar{\rho} : \hat{\mathbb{Z}} \to \mathrm{GL}_r(\mathbb{Z}_l)$. On the other hand, given a topological morphism $\eta : \hat{\mathbb{Z}} \to \mathrm{GL}_r(\mathbb{Z}_l)$, we can restrict it to a group morphism $\eta|_{\mathbb{Z}} : \mathbb{Z} \to \mathrm{GL}_r(\mathbb{Z}_l)$. To sum up, there is a bijection

$$\theta : \mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M)) \to \mathrm{Hom}_{\mathrm{TGp}}(\hat{\mathbb{Z}}, \mathrm{Aut}_{\mathbb{Z}_l}(M)),$$

such that $\theta(\rho) = \bar{\rho}$ and $\theta^{-1}(\eta) = \eta|_{\mathbb{Z}}$.

If M is not necessarily free, then by the above lemma we have that

$$\begin{aligned}\mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M)) \cong \mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M_f)) \oplus \mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M_t)) \\ \oplus \mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)) \quad (3.11)\end{aligned}$$

where the last two terms are finite, since $\mathrm{Aut}_{\mathbb{Z}_l}(M_t)$ and $\mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)$ are finite. The same situation holds for $\mathrm{Hom}_{\mathrm{TGp}}(\hat{\mathbb{Z}}, \mathrm{Aut}_{\mathbb{Z}_l}(M))$. Since we have that

$$\mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M_t)) \cong \mathrm{Hom}_{\mathrm{Gp}}(\hat{\mathbb{Z}}, \mathrm{Aut}_{\mathbb{Z}_l}(M_t))$$

and

$$\mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)) \cong \mathrm{Hom}_{\mathrm{TGp}}(\hat{\mathbb{Z}}, \mathrm{Hom}_{\mathbb{Z}_l}(M_f, M_t)).$$

So we still have a bijection

$$\theta : \mathrm{Hom}_{\mathrm{Gp}}(\mathbb{Z}, \mathrm{Aut}_{\mathbb{Z}_l}(M)) \to \mathrm{Hom}_{\mathrm{TGp}}(\hat{\mathbb{Z}}, \mathrm{Aut}_{\mathbb{Z}_l}(M))$$

giving by restriction and extension. □

Lemma 3.5. The category $\mathscr{C}$ of finitely generated $\mathbb{Z}_l$-modules with continuous G-action is equivalent to the category $\mathscr{D}$ of finitely generated $\mathbb{Z}_l$-modules with $\mathbb{Z}$-action.

Proof. Since G is the Galois group of $\bar{\mathbb{F}}_q$ over $\mathbb{F}_q$,

$$G = \varprojlim_{n>0} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \varprojlim_{n>0} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

Hence G is isomorphic to the profinite group $\hat{\mathbb{Z}}$ with topological generator the q Frobenius.

To give a group action on M is equivalent to give a group morphism from the group to $\mathrm{Aut}_{\mathbb{Z}_l}(M)$. By the above lemma, we have a bijection between $\mathrm{Ob}(\mathscr{C})$ and $\mathrm{Ob}(\mathscr{D})$. In fact the construction of the bijection in the above lemma given by restriction and extension is compatible with the $\mathbb{Z}_l$-module morphism inside $\mathscr{C}$ and $\mathscr{D}$, so this bijection actually gives a equivalence between $\mathscr{C}$ and $\mathscr{D}$. □

Let ρ (resp. χ) be the Galois representation on the Tate module of E (resp. $\mathbb{G}_m$). By lemma 3.5, we can consider $(T_l(E), \rho)$ and $(T_l(\mathbb{G}_m), \chi)$ as the objects in category $\mathscr{D}$.

Lemma 3.6. The category $\mathscr{D}$ is equivalent to the category of A-modules, where $A = \mathbb{Z}_l[t, t^{-1}]$ is the group ring $\mathbb{Z}_l[\mathbb{Z}]$.

Proof. Let M be a finitely generated $\mathbb{Z}_l$-module. To give M an A-module structure is equivalent to give the scalar multiplication on M by t, which is equivalent to give a $\mathbb{Z}$-action on M. Hence $\mathscr{D}$ is equivalent to the category of A-modules. □

Lemma 3.7. We have that:

$$\mathrm{Ext}_{\mathscr{D}}((T_l(E),\rho),(T_l(\mathbb{G}_m),\chi)) \cong \mathrm{coker}(\mathbb{Z}_l^2 \overset{\rho^t(1)-q}{\longrightarrow} \mathbb{Z}_l^2)$$

as abelian groups, where $\rho(1)^t$ is the transpose of the matrix of $\rho(1)$ under a selected basis, and q represents the scalar multiplication by q.

Proof. First let's construct some new objects in $\mathrm{Ob}(\mathscr{D})$, after giving an element $(\mathbb{Z}_l^r,\theta) \in \mathrm{Ob}(\mathscr{D})$. Define θ^{-1} to be the composition $\mathbb{Z} \overset{-}{\longrightarrow} \mathbb{Z} \overset{\theta}{\longrightarrow} \mathrm{GL}_r(\mathbb{Z}_l)$, where -1 is the inverse morphism on $\mathbb{Z}$. Since θ and -1 are continuous, so is θ^{-1}, hence $(\mathbb{Z}_l^r,\theta^{-1}) \in \mathrm{Ob}(\mathscr{D})$. We can give a natural $\mathbb{Z}$-action on $\mathbb{Z}_l^{r\vee} := \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l^r,\mathbb{Z}_l)$ from θ, by dualizing $\mathbb{Z}_l^r \overset{\theta(m)}{\longrightarrow} \mathbb{Z}_l^r$ to $\mathbb{Z}_l^{r\vee} \overset{\theta(m)^*}{\longrightarrow} \mathbb{Z}_l^{r\vee}$ for every $m \in \mathbb{Z}$. In fact, $\theta(m)^*$ is just the transpose of $\theta(m)$ after we choose the dual base for $\mathbb{Z}_l^{r\vee}$. We denote θ^t to be the composition $\mathbb{Z} \overset{\theta}{\longrightarrow} \mathrm{GL}_r(\mathbb{Z}_l) \overset{(\cdot)^t}{\to} \mathrm{GL}_r(\mathbb{Z}_l)$, which is a morphism even though $(\cdot)^t$ is an anti-morphism. And also $(\cdot)^t$ is continuous. Since $\mathbb{Z}_l^{r\vee} \cong \mathbb{Z}_l^r$, we get a new object $(\mathbb{Z}_l^r,\theta^t)$ in $\mathscr{D}$, and call θ^t the transposed action of θ on $\mathbb{Z}_l^r$.

After taking a basis for $T_l(E)$ (resp. $T_l(\mathbb{G}_m)$), the Frobenius actions $\rho(1)$ (resp. $\chi(1)$) can be expressed as a matrix over $\mathbb{Z}_l$ explicitly, and we still denote this matrix as $\rho(1)$ (reps. $\chi(1)$, in fact $\chi(1)=q$). Also we change to write $(\mathbb{Z}_l^2,\rho)$ (resp. $(\mathbb{Z}_l,\chi)$) as $(T_l(E),\rho)$ (resp. $(T_l(\mathbb{G}_m),\chi)$). Given an element $\mathbb{Z}_l \overset{\alpha}{\rightarrowtail} M \overset{\beta}{\twoheadrightarrow} \mathbb{Z}_l^2$ of $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l^2,\rho),(\mathbb{Z}_l,\chi))$, we take the dual sequence $\mathbb{Z}_l^\vee \overset{\alpha^*}{\twoheadleftarrow} M^\vee \overset{\beta^*}{\hookleftarrow} \mathbb{Z}_l^{2\vee}$. This is still exact as $\mathbb{Z}_l$-module sequence, and compatible with the transposed actions on each components, since the transposed action is defined by the $*$-operation. So $\mathbb{Z}_l \overset{\alpha^*}{\twoheadleftarrow} M \overset{\beta^*}{\hookleftarrow} \mathbb{Z}_l^2$ is an element of $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l,\chi^t),(\mathbb{Z}_l^2,\rho^t))$. Also the dual operation keeps the group law of $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l^2,\rho),(\mathbb{Z}_l,\chi))$ After taking the dual operation again, we go back to the original sequence, hence we have an isomorphism

$$\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l^2,\rho),(\mathbb{Z}_l,\chi)) \cong \mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l,\chi^t),(\mathbb{Z}_l^2,\rho^t)) \tag{3.12}$$

Now given an element $\mathbb{Z}_l^2 \overset{\alpha}{\rightarrowtail} M \overset{\beta}{\twoheadrightarrow} \mathbb{Z}_l$ of $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l,\chi^t),(\mathbb{Z}_l^2,\rho^t))$,using the functor $\_\otimes_{\mathbb{Z}_l}(\mathbb{Z}_l,\chi^{-1})$(note that $\chi^t=\chi$) on it, we get an element of $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l,1),(\mathbb{Z}_l^2,\chi^{-1}\rho^t))$(Here 1 refers to the zero morphism $\mathbb{Z} \to \mathbb{Z}_l^\times$).

Using the functor $\_\_ \otimes_{\mathbb{Z}_l} (\mathbb{Z}_l, \chi)$, we go back to the original sequence. Since the two functors keep the group law, hence we have an isomorphism

$$\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l, \chi^t), (\mathbb{Z}_l^2, \rho^t)) \cong \mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l, 1), (\mathbb{Z}_l^2, \chi^{-1}\rho^t)) \tag{3.13}$$

Hence $\mathrm{Ext}_{\mathscr{D}}((T_l(E), \rho), (T_l(\mathbb{G}_m), \chi)) \cong \mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l, 1), (\mathbb{Z}_l^2, \chi^{-1}\rho^t))$, we are left to compute the second object. By the above lemma, the category $\mathscr{D}$ can be regarded as the category of finitely generated $\mathbb{Z}_l$-modules which are also A-module. And in the category of A-modules, $\mathrm{Ext}(\cdot, (\mathbb{Z}_l^2, \chi^{-1}\rho^t))$ can be defined as the derived functor of $\mathrm{Hom}(\cdot, (\mathbb{Z}_l^2, \chi^{-1}\rho^t))$. So in order to complete the computation we take a projective resolution of $\mathbb{Z}_l$ as A-module. Consider the sequence of A-modules $A \overset{\kappa}{\rightarrowtail} A \overset{\mu}{\twoheadrightarrow} \mathbb{Z}_l$, where κ is the multiplication by $(t-1)$ and μ is given by mapping 1 to 1. This is obviously exact, hence gives rise to a projective resolution. Using the functor $\mathrm{Hom}_{A-\mathrm{mod}}(\cdot, (\mathbb{Z}_l^2, \chi^{-1}\rho^t))$ on this sequence, we get a complex:

$$0 \to \mathrm{Hom}_{A-\mathrm{mod}}(\mathbb{Z}_l, \mathbb{Z}_l^2) \overset{\mu^*}{\to} \mathrm{Hom}_{A-\mathrm{mod}}(A, \mathbb{Z}_l^2) \overset{\kappa^*}{\to} \mathrm{Hom}_{A-\mathrm{mod}}(A, \mathbb{Z}_l^2) \to 0.$$

So $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l, 1), (\mathbb{Z}_l^2, \chi^{-1}\rho^t)) = \mathrm{coker}\kappa^*$. Since $\mathrm{Hom}_{A-\mathrm{mod}}(A, \mathbb{Z}_l^2) \cong \mathbb{Z}_l^2$, if we regard κ^* as an endomorphism on $\mathbb{Z}_l^2$, it just the $\mathbb{Z}_l$-linear map given by the matrix $\chi^{-1}(1)\rho^t(1) - 1 = q^{-1}\rho^t(1) - 1$. Hence we have

$$\mathrm{coker}\kappa^* = \mathrm{coker}(q^{-1}\rho^t(1) - 1 : \mathbb{Z}_l^2 \to \mathbb{Z}_l^2) = \mathrm{coker}(\rho^t(1) - q).$$

So $\mathrm{Ext}_{\mathscr{D}}((\mathbb{Z}_l, 1), (\mathbb{Z}_l^2, \chi^{-1}\rho^t)) \cong \mathrm{coker}(\mathbb{Z}_l^2 \overset{\rho^t(1)-q}{\longrightarrow} \mathbb{Z}_l^2)$. □

After these preparations, now we can prove theorem 3.2.

Proof of Theorem 3.2: By lemma 3.5, we have that the category $\mathscr{C}$ is equivalent to $\mathscr{D}$, it follows that $\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m)) \cong \mathrm{Ext}_{\mathscr{D}}(T_l(E), T_l(\mathbb{G}_m))$. By lemma 3.7, $\mathrm{Ext}_{\mathscr{D}}(T_l(E), T_l(\mathbb{G}_m)) \cong \mathrm{coker}(\mathbb{Z}_l^2 \overset{\rho^t(1)-q}{\longrightarrow} \mathbb{Z}_l^2)$. So we get $\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m)) \cong \mathrm{coker}(\mathbb{Z}_l^2 \overset{\rho^t(1)-q}{\longrightarrow} \mathbb{Z}_l^2)$. In fact, this is a finite group, hence a finite l-group. This is because the characteristic polynomial of the Frobenius action on E has coefficients in $\mathbb{Z}$ (see Silverman's book [18, V, §2]), and the roots of this polynomial are of absolute value $\sqrt{q}$ which is different from q of course. Hence $\rho(1) - q$ has no zero characteristic root. Then

$\det(\rho(1)^t - q) = \det(\rho(1) - q)$ is not zero, and $\operatorname{coker}(\rho(1)^t - q)$ is a finite abelian l-group. □

Theorem 3.8. As before, (E, O) is an elliptic curve over $\mathbb{F}_q$ and $\mathbb{G}_m$ is the multiplicative group over $\mathbb{F}_q$. Then $\operatorname{Ext}(E, \mathbb{G}_m) \cong E^\vee(\mathbb{F}_q)$, i.e. it is isomorphic to the group of $\mathbb{F}_q$-points of the dual of E.

Proof. See Serre's book[16, page 183-184]. □

Theorem 3.9. As before, let (E, O) be an elliptic curve over $\mathbb{F}_q$ and $\mathbb{G}_m$ be the multiplicative group over $\mathbb{F}_q$.Then we have that:

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Ext}(E, \mathbb{G}_m) \cong \operatorname{coker}(\mathbb{Z}_l^2 \xrightarrow{\rho(1)-q} \mathbb{Z}_l^2)$$

as abelian groups. Moreover, they are finite l-groups.

Proof. By the above theorem $\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Ext}(E, \mathbb{G}_m) \cong E^\vee(\mathbb{F}_q)$, it is enough to express the $\mathbb{F}_q$-points group of $E^\vee$ as $\operatorname{coker}(\mathbb{Z}_l^2 \xrightarrow{\rho(1)-q} \mathbb{Z}_l^2)$. We know that the $\mathbb{F}_q$-points of an elliptic curve (E, O) are just the $\bar{\mathbb{F}}_q$-points fixed by the action of q Frobenius automorphism of $\bar{\mathbb{F}}_q/\mathbb{F}_q$, and by example 2.3 we also know the action of q Frobenius automorphism of $K/\mathbb{F}_q$ on $E(K)$ is the same as the action of the Frobenius morphism on $E(K)$ for any field $K \supset \mathbb{F}_q$. It follows that $E^\vee(\mathbb{F}_q) = E^\vee(\bar{\mathbb{F}}_q)[\operatorname{Frob}_{q,E^\vee} - 1]$, where $\operatorname{Frob}_{q,E^\vee}$ is just the q Frobenius morphism on $E^\vee$. Since $\sharp\, E^\vee(\mathbb{F}_q)$ is finite, it follows that $\operatorname{Frob}_{q,E^\vee} - 1$ is not zero, and that for some positive integer n big enough, we have

$$E^\vee(\mathbb{F}_q) \otimes_{\mathbb{Z}} \mathbb{Z}_l = E^\vee(\mathbb{F}_q)[l^n] = E^\vee(\bar{\mathbb{F}}_q)[l^n][\operatorname{Frob}_{q,E^\vee} - 1]. \tag{3.14}$$

We have the following exact sequence:

$$0 \to \ker(\operatorname{Frob}_{q,E^\vee} - 1) \to E^\vee(\bar{\mathbb{F}}_q)[l^n] \xrightarrow{\operatorname{Frob}_{q,E^\vee}-1} E^\vee(\bar{\mathbb{F}}_q)[l^n].$$

Since the Weil pairing $E(\bar{\mathbb{F}}_q)[l^n] \times E^\vee(\bar{\mathbb{F}}_q)[l^n] \longrightarrow \mu_{l^n}$ is a perfect pairing, where μ_{l^n} is the group of l^n-th roots of unity, taking the dual on the above sequence, we get another exact sequence

$$0 \leftarrow \ker(\operatorname{Frob}_{q,E^\vee} - 1)^D \leftarrow E(\bar{\mathbb{F}}_q)[l^n] \xleftarrow{\operatorname{Frob}^*_{q,E^\vee}-1} E(\bar{\mathbb{F}}_q)[l^n].$$

So we have $\ker(\mathrm{Frob}_{q,E^\vee}-1)\cong\ker(\mathrm{Frob}_{q,E^\vee}-1)^D\cong\mathrm{coker}(\mathrm{Frob}^*_{q,E^\vee}-1)$. In fact, the dual morphism $\mathrm{Frob}^*_{q,E^\vee}$ of $\mathrm{Frob}_{q,E^\vee}$ with respect to the Weil Pairing is just the dual isogeny $\widehat{\mathrm{Frob}_{q,E}}$ of the q Frobenius morphism $\mathrm{Frob}_{q,E}$ on E. Since $\mathrm{Frob}_{q,E}$ is an automorphism on the torsion group $E(\bar{\mathbb{F}}_q)[l^n]$, it follows that

$$\begin{aligned}\mathrm{coker}(\mathrm{Frob}^*_{q,E^\vee}-1)&\cong\mathrm{coker}(\widehat{\mathrm{Frob}_{q,E}}-1)\\&\cong\mathrm{coker}(\mathrm{Frob}_{q,E}\circ(\widehat{\mathrm{Frob}_{q,E}}-1))\\&=\mathrm{coker}(\mathrm{Frob}_{q,E}\circ\widehat{\mathrm{Frob}_{q,E}}-\mathrm{Frob}_{q,E})\\&=\mathrm{coker}(q-\mathrm{Frob}_{q,E})\end{aligned}$$

We almost proved the result, but this cokernel is taken on $E(\bar{\mathbb{F}}_q)[l^n]$, but not on $T_l(E)$. In fact, for n big enough, they give the same cokernel. This is because if we consider the following commutative diagram:

$$\begin{array}{ccccccccc}0&\longrightarrow&\mathbb{Z}_l^2&\xrightarrow{\mathrm{Frob}_{q,E}-q}&\mathbb{Z}_l^2&\longrightarrow&M&\longrightarrow&0\\&&\downarrow{\scriptstyle\cdot l^n}&&\downarrow{\scriptstyle\cdot l^n}&&\downarrow{\scriptstyle\cdot l^n}&&\\0&\longrightarrow&\mathbb{Z}_l^2&\xrightarrow{\mathrm{Frob}_{q,E}-q}&\mathbb{Z}_l^2&\longrightarrow&M&\longrightarrow&0\end{array}$$

where $\mathbb{Z}_l^2$ is regarded as the Tate module on E, $M:=\mathrm{coker}(\mathrm{Frob}_{q,E}-q)$ on $\mathbb{Z}_l^2$, and n is big enough such that $l^nM=0$ (We can do this, since $\mathrm{Frob}_{q,E}-q$ is a finite morphism implies that M is finite). Since both rows are exact in the above diagram, by the snake lemma, we get an exact sequence:

$$0\to0\to0\to M\to\mathbb{Z}/l^n\mathbb{Z}\xrightarrow{\mathrm{Frob}_{q,E}-q}\mathbb{Z}/l^n\mathbb{Z}\to M\to0.$$

So we get $\mathbb{Z}_l\otimes_{\mathbb{Z}}\mathrm{Ext}(E,\mathbb{G}_m)\cong\mathrm{coker}(\mathbb{Z}_l^2\xrightarrow{\mathrm{Frob}_{q,E}-q}\mathbb{Z}_l^2)$, and it's a finite l-group. Again by example 2.3, we can rewrite the above result as:

$$\mathbb{Z}_l\otimes_{\mathbb{Z}}\mathrm{Ext}(E,\mathbb{G}_m)\cong\mathrm{coker}(\mathbb{Z}_l^2\xrightarrow{\rho(1)-q}\mathbb{Z}_l^2)$$

where $\rho:\hat{\mathbb{Z}}\to\mathrm{GL}_2(\mathbb{Z}_l)$ is the Galois representation given before, and $\rho(1)$ corresponds to the q Frobenius action on $T_l(E)$. □

Theorem 3.10. The map Φ in the theorem 3.1 is injective.

To prove this, we need a lemma and some definition needed in the lemma.

Definition 3.11. An abelian variety A over a field k is a connected complete algebraic variety over k with a group law on it. The multiplication map and the inverse map are homomorphisms of algebraic groups. For example the elliptic curves are abelian varieties of dimension 1.

Let l be a prime which is different from $\mathrm{char}(k)$, let $A(k^s)[l^n]$ be the l^n-th torsion subgroups over a fixed separable closure k^s of k which is a finite group (the proof is similar to the case for elliptic curves, see Mumford's book [14]). Then $\{A(k^s)[l^n]\}_n$ with compatible Galois action forms a direct system naturally. Then the direct limit $\varinjlim_n A(k^s)[l^n]$ is called the **l-divisible group** on A, written as $A[l^\infty]$, which has a Galois action on itself. Note that we can also construct the l-divisible group on $\mathbb{G}_m$ using the same step.

In fact, we can get the l-divisible group on A (resp. $\mathbb{G}_m$) using the Tate module $T_l(A)$ (resp. $T_l(\mathbb{G}_m)$). We formulate as follows:

$$\begin{aligned}
\mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} T_l(A) &= (\varinjlim_n \mathbb{Z}/l^n\mathbb{Z}) \otimes_{\mathbb{Z}} T_l(A) \\
&= \varinjlim_n (\mathbb{Z}/l^n\mathbb{Z} \otimes_{\mathbb{Z}} T_l(A)) \\
&= \varinjlim_n T_l(A)/l^n T_l(A) \\
&= \varinjlim_n A(k^s)[l^n] \\
&= A[l^\infty]
\end{aligned}$$

From the above formulation, we have that the Galois action on $A[l^\infty]$ is the same as the action inherited from $T_l(A)$ by using the functor $\mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} \cdot$. By the same reason, we have that $\mathbb{G}_m[l^\infty] = \mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} T_l(\mathbb{G}_m)$. Further more, given a short exact sequence $B \overset{\kappa}{\rightarrowtail} M \twoheadrightarrow A$, where

$$A, B \in \{\text{abelian varieties over } k\} \cup \{\mathbb{G}_m \text{over } k\}.$$

Then we have a short exact sequence:

$$T_l(B) \overset{\kappa}{\rightarrowtail} T_l(M) \twoheadrightarrow T_l(A). \tag{3.15}$$

Applying the functor $\mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} \cdot$ on this sequence, we get a right exact sequence:

$$0 \to \mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} T_l(B) \to \mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} T_l(M) \to \mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} T_l(A) \to 0. \quad (3.16)$$

In fact, this is also left exact with the reason as follows. Assume that there exists $r \geq 0$ and $(b_i)_i \in T_l(B) - \{0\}$, such that $l^{-r} \otimes_{\mathbb{Z}} (\kappa(b_i))_i = 0$. Since $(b_i)_i \neq 0$ implies that $(\kappa(b_i))_i \neq 0$, hence $r = 0$. This shows that 3.16 is also right exact. Then we actually get a short exact sequence:

$$0 \to B[l^\infty] \to M[l^\infty] \to A[l^\infty] \to 0 \quad (3.17)$$

On the other hand, we also have $T_l(A) = \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, A[\infty])$, and the Galois action on $T_l(A)$ is induced by the Galois action on $A[\infty]$. Also the functor $\mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \cdot)$ is exact on $B[l^\infty] \rightarrowtail M[l^\infty] \twoheadrightarrow A[l^\infty]$. Hence we know that the l-Tate modules on A is equivalent to the l-divisible group on A (note A can be either an abelian variety over k or $\mathbb{G}_m$ over k). Moreover, the sequence 3.15 splits if and only if 3.16 splits.

Lemma 3.12. Let k be a field, A an abelian variety over k, l a prime number, and $\mathcal{E} = (\mathbb{G}_m \rightarrowtail E \twoheadrightarrow A)$ an extension whose class in $\mathrm{Ext}_{\mathscr{A}}(A, \mathbb{G}_m)$ is killed by $m = l^{n_0}$ for some integer $n_0 \geq 0$, where $\mathscr{A}$ is the category of commutative algebraic groups over k. If $\mathrm{Hom}(A[l^\infty], \mathbb{G}_m[l^\infty]) = 0$, and the induced extension on the corresponding l-divisible groups $\mathbb{G}_m[l^\infty] \rightarrowtail E[l^\infty] \twoheadrightarrow A[l^\infty]$ splits, then $\mathbb{G}_m \rightarrowtail E \twoheadrightarrow A$ splits.

Proof. First let's understand explicitly the meaning of $l^{n_0} \cdot \mathcal{E} = 0$. Given a morphism of abelian varieties $f : B \to A$, we have a morphism $f^* : \mathrm{Ext}_{\mathscr{A}}(\mathbb{G}_m, A) \to \mathrm{Ext}_{\mathscr{A}}(\mathbb{G}_m, B)$ given by pull-back, and this $*$-operation is additive, i.e. for $g : B \to A$, $(f+g)^* = f^* + g^*$, also $1_A^* = 1$. So we have $m \cdot \mathcal{E} = \underbrace{\mathcal{E} + \cdots + \mathcal{E}}_{m} = \underbrace{1_A^*\mathcal{E} + \cdots + 1_A^*\mathcal{E}}_{m} = (\underbrace{1_A + \cdots + 1_A}_{m})\mathcal{E} = ([m]_A)^*\mathcal{E}$, where $[m]_A$ denotes the multiplication map by m on A. And $([m]_A)^*\mathcal{E}$ is

given by the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & E' & \longrightarrow & A & \longrightarrow & 0 \\ & & \| & & {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle m\cdot} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \end{array} \tag{3.18}$$

where E' is the pull-back of A and E, $m\cdot$ denotes the multiplication by m, the two rows are exact. Since $m \cdot \mathcal{E} = ([m]_A)^*\mathcal{E} = 0$, the above row splits, hence $E' \cong \mathbb{G}_m \times A$, and there is a section $s : A \to \mathbb{G}_m \times A$. In fact such a section is unique, since the difference of two such sections must give an element of $\mathrm{Hom}_{\mathscr{A}}(A, \mathbb{G}_m)$ which is zero from the fact that A is complete. Again from 3.18, by using snake lemma we have $ker(p) \cong A[m]$. So we have a new commutative diagram

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & A(k^s)[m] & = & A(k^s)[m] & & \\ & & & & {\scriptstyle r}\downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_m(k^s) & \longrightarrow & \mathbb{G}_m(k^s) \times A(k^s) & \longrightarrow & A(k^s) & \longrightarrow 0 & \\ & & \| & & {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle m\cdot} & & \\ 0 & \longrightarrow & \mathbb{G}_m(k^s) & \longrightarrow & E(k^s) & \longrightarrow & A(k^s) & \longrightarrow 0 & \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array} \tag{3.19}$$

where we replace E' by $\mathbb{G}_m \times A$, but we still use p to denote the original morphism, and r corresponds to the embedding of $ker(p)$ in 3.18. Note that all the rows and columns are obviously exact. By the universal property of the direct product, the embedding $r : A(k^s)[m] \to \mathbb{G}_m(k^s) \times A(k^s)$ must send $a \in A(k^s)[m]$ to $(h(a), a) \in \mathbb{G}_m(k^s) \times A(k^s)$, where h is a morphism from $A(k^s)[m]$ to $\mathbb{G}_m(k^s)$. Taking the l-divisible group in the above diagram, we

get another commutative diagram with exact rows and columns

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & A(k^s)[m] & = & A(k^s)[m] & & \\
 & & & & {\scriptstyle r}\downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{G}_m[l^\infty] & \longrightarrow & \mathbb{G}_m[l^\infty]\times A[l^\infty] & \longrightarrow & A[l^\infty] & \longrightarrow & 0 \\
 & & \| & & {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle m\cdot} & & \\
0 & \longrightarrow & \mathbb{G}_m[l^\infty] & \longrightarrow & E[l^\infty] & \longrightarrow & A[l^\infty] & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \tag{3.20}$$

Since $\mathbb{G}_m[l^\infty] \rightarrowtail E[l^\infty] \twoheadrightarrow A[l^\infty]$ splits, there exists a section $t : A[l^\infty] \to E[l^\infty]$. Then there is a unique section $t' : A[l^\infty] \to \mathbb{G}_m[l^\infty] \times A[l^\infty]$, which lifts t. Also we have a section $t_0 : A[l^\infty] \to \mathbb{G}_m[l^\infty] \times A[l^\infty]$ by sending $a \in A[l^\infty]$ to $(1, a) \in \mathbb{G}_m[l^\infty] \times A[l^\infty]$. Then $t' - t_0$ is in $\mathrm{Hom}(A[l^\infty], \mathbb{G}_m[l^\infty]) = 0$ by assumption, hence $t' = t_0$. On the other hand, for $a \in A(k^s)[m]$, $p(t'(a)) = t(m \cdot a) = t(0) = 0$ implies that $t'(a) \in ker(p)$, hence equals to $(h(a'), a')$ for some $a' \in A(k^s)[m]$. Since t' is a section in the above diagram, we have $a = a'$, so $(1, a) = t_0(a) = t'(a) = (h(a), a)$. This shows that h is the trivial morphism, it follows that $E(k^s) \cong (\mathbb{G}_m(k^s) \times A(k^s))/(1 \times A(k^s)[m]) \cong \mathbb{G}_m(k^s) \times (A(k^s)/A(k^s)[m])$, and $\mathbb{G}_m \rightarrowtail E \twoheadrightarrow A$ splits. □

Proof of theorem *3.10:* Let $(\mathbb{G}_m \rightarrowtail M \twoheadrightarrow E) \in ker(\Phi)$. Note that this extension class is killed by some l-power. If moreover

$$\mathrm{Hom}(E[l^\infty], \mathbb{G}_m[l^\infty]) = 0 \tag{3.21}$$

and

$$\mathbb{G}_m[l^\infty] \rightarrowtail M[l^\infty] \twoheadrightarrow E[l^\infty] \tag{3.22}$$

splits, by the above lemma we have that $(\mathbb{G}_m \rightarrowtail M \twoheadrightarrow E)$ splits. So we are left to prove that 3.21 holds, and that 3.22 splits. Since the Frobenius

actions on $T_l(E)$ and $T_l(\mathbb{G}_m)$ don't have any common characteristic root, it follows that $\mathrm{Hom}(T_l(E), T_l(\mathbb{G}_m)) = 0$. Hence we get:

$$\mathrm{Hom}(E[l^\infty], \mathbb{G}_m[l^\infty]) = (\mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} \cdot)(\mathrm{Hom}(T_l(E), T_l(\mathbb{G}_m))) = 0.$$

Now we turn to prove that 3.22 splits. Since $(\mathbb{G}_m \rightarrowtail M \twoheadrightarrow E) \in ker(\Phi)$, the induced extension $T_l(\mathbb{G}_m) \rightarrowtail T_l(M) \twoheadrightarrow T_l(E)$ splits. Applying the functor $\mathbb{Q}_l/\mathbb{Z}_l \otimes_{\mathbb{Z}} \cdot$, we have that:

$$\mathbb{G}_m[l^\infty] \rightarrowtail M[l^\infty] \twoheadrightarrow E[l^\infty]$$

splits. □

At last, we can prove our main theorem.

Proof of the Main theorem: By theorem 3.2 and 3.9, we have

$$\mathrm{Ext}_{\mathscr{C}}(T_l(E), T_l(\mathbb{G}_m)) \cong \mathrm{coker}(\mathbb{Z}_l^2 \xrightarrow{\rho(1)^t - q} \mathbb{Z}_l^2)$$

and

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Ext}(E, \mathbb{G}_m) \cong \mathrm{coker}(\mathbb{Z}_l^2 \xrightarrow{\rho(1) - q} \mathbb{Z}_l^2).$$

Since $\rho(1) - q$ is a linear map of rank 2 on $\mathbb{Z}_l^2$, so

$$\det(\rho(1) - q) = \det(\rho(1)^t - q) \neq 0.$$

Then $\sharp(\mathrm{coker}(\rho(1) - q)) = \sharp(\mathrm{coker}(\rho(1)^t - q))$. By theorem 3.10, Φ is injective, it follows that Φ is actually an isomorphism. □

References

[1] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] Bas Edixhoven, *The Lecture Note of The National Course 2007: Algebraic curves*, unpublished.

[3] Bas Edixhoven, *Jacobian Varieties*, http://www.math.leidenuniv.nl/ edix/

[4] Gerard van der Geer and Ben Moonen, *Abelian Varieties*, http://staff.science.uva.nl/ bmoonen/boek/BookAV.html

[5] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[6] Haruzo Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer-Verlag, 2004.

[7] P.J. Higgins, *Introduction to Topological Groups*, Cambridge University Press, 1974.

[8] Peter Hilton and Urs Stammbach, *A Course in Homological Algebra*, Second Edition, Springer-verlag, 1997.

[9] Thomas W.Hungerford, *Algebra*, Springer-Verlag, 1974.

[10] Saunders Mac Lane, *Categories for the Working Mathematician*, Second Edition, Springer-Verlag, 1998.

[11] H. Matsumura, *Commutative Algebra*, W. A. Benjamin Co., New York, 1970.

[12] Patrick Morandi, *Field and Galois Theory*, Springer-Verlag, 1996.

[13] Carlos Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, 1991.

[14] David Mumford, *Abelian Varieties*, Second Edition, Oxford University Press, 1974.

[15] Jürgen Neukirch, *Algebraic Number Theory*, Translated from the German by Norbert Schappacher, Springer-Verlag, 1999.

[16] Jean-Pierre Serre, *Algebraic Groups and Class Fields*, Springer-Verlag, 1988.

[17] Igor R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, 1974.

[18] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.