ARITHMETIC OF CURVES

HARUZO HIDA

In this course, we start with very basics of curves and try to reach the theory of their jacobians and at the end, we introduce modular Galois representation a la Eichler–Shimura:

(1) Plane curves over a field (elementary, up to Section 3);
(2) Scheme/group functor over a ring (a try-to-be easy introduction to scheme theory);
(3) Picard schemes and Jacobian of curves (more sophisticated hereafter);
(4) General theory of abelian varieties;
(5) Construction of modular Galois representation.

Elliptic curves and modular curves are one of the most important objects studied in number theory. As everybody knows, the theory is a base of the proof by Wiles (through Ribet's work) of Fermat's last theorem, is the main tool in the proof of Serre's mod p modularity conjecture (by Khare–Wintenberger), it supplies us with the simplest (and perhaps the most beautiful) example of Shimura varieties (cf. [IAT] Chapters 6 and 7), it supplies a fast prime factorization algorithm (cf. [REC] IV), and so on. Since this is a topic course, we give details of proofs in the first few weeks and later we try to introduce more up-to-date materials in a less strict manner though in this notes, detailed proofs of many theorems (which may not be touched in the lecture) are given.

Contents

Date: December 15, 2011.
The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949.

1. Curves over a Field

In this section, we describe basics of plane curves over a fixed field k. We also fix an algebraic closure $\overline{k}$ of k and a sufficiently big algebraically closed field Ω containing $\overline{k}$. Here we suppose that Ω has many transcendental elements over k. An example of this setting is a familiar one: $k = \mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C} = \Omega$.

1.1. **Plane curves.** Let $\mathfrak{a}$ be a principal ideal of the polynomial ring $k[X, Y]$. Note that polynomial rings over a field is a unique factorization domain. We thus have prime factorization $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ with principal primes $\mathfrak{p}$. We call $\mathfrak{a}$ *square free* if $0 \le e(\mathfrak{p}) \le 1$ for all principal primes $\mathfrak{p}$. Fix a square-free $\mathfrak{a}$. The set of A-rational points for any k-algebra A of a *plane curve* is given by the zero set

$$V_{\mathfrak{a}}(A) = \left\{(x, y) \in A^2 \middle| f(x, y) = 0 \text{ for all } f(X, Y) \in \mathfrak{a}\right\}.$$

It is common to take an intermediate field $\Omega/A/k$ classically, but the definition itself works well for any k-algebra A (here a k-algebra is a commutative ring containing k sharing identity with k). Often in mathematics, if one has more flexibility, proofs become easier; so, we just allow $V_{\mathfrak{a}}(A)$ for any k-algebras A. Obviously, for a generator $f(X, Y)$ of $\mathfrak{a}$, we could have defined

$$V_{\mathfrak{a}}(A) = V_f(A) = \left\{(x, y) \in A^2 \middle| f(x, y) = 0\right\},$$

but this does not depend on the choice of generators and depends only on the ideal $\mathfrak{a}$; so, it is more appropriate to write $V_{\mathfrak{a}}$. As an exceptional case, we note $V_{(0)}(A) = A^2$. Geometrically, we think of $V_{\mathfrak{a}}(\Omega)$ as a curve in $\Omega^2 = V_{(0)}(\Omega)$. This is more geometric if we take $k \subset \mathbb{C}$ (the 2-dimensional "plane" as a real manifold). In this sense, for any algebraically closed field K over k, a point $x \in V_{\mathfrak{a}}(K)$ is called a geometric point with coefficients in K, and $V_{(f)}(K) \subset V_{(0)}(K)$ is called the geometric curve in $V_{(0)}(K) = K^2$ defined by the equation $f(X, Y) = 0$.

By Hilbert's zero theorem (Nullstellensatz; see [CRT] Theorem 5.4 and [ALG] Theorem I.1.3A), writing $\overline{\mathfrak{a}}$ the principal ideal of $\overline{k}[X, Y]$ generated by $\mathfrak{a}$, we have

$$\overline{\mathfrak{a}} = \left\{g(X, Y) \in \overline{k}[X, Y] \middle| g(x, y) = 0 \text{ for all } (x, y) \in V_{\mathfrak{a}}(\overline{k})\right\}. \tag{1.1}$$

Thus we have a bijection

$$\{\text{square-free ideals of } \overline{k}[X, Y]\} \leftrightarrow \{\text{plane curves } V_{\mathfrak{a}}(\overline{k}) \subset V_{(0)}(\overline{k})\}.$$

The association $V_{\mathfrak{a}} : A \mapsto V_{\mathfrak{a}}(A)$ is a covariant functor from the category of k-algebras to the category of sets (denoted by $SETS$). Indeed, for any k-algebra homomorphism $\sigma : A \to A'$, we have an associated map: $V_{\mathfrak{a}}(A) \ni (x, y) \mapsto (\sigma(x), \sigma(y)) \in V_{\mathfrak{a}}(A')$ as $0 = \sigma(0) = \sigma(f(x, y)) = f(\sigma(x), \sigma(y))$. Thus $\mathfrak{a} = \overline{\mathfrak{a}} \cap k[X, Y]$ is determined uniquely by this functor, but the value $V_{\mathfrak{a}}(A)$ for an individual A may not determine $\mathfrak{a}$. From number theoretic view point, studying $V_{\mathfrak{a}}(A)$ for a small field (or even

a ring, such as $\mathbb{Z}$) is important. Thus it would be better regard $V_{\mathfrak{a}}$ as a functor in number theoretic setting.

If $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}$ for principal prime ideals $\mathfrak{p}$, by definition, we have

$$V_{\mathfrak{a}} = \bigcup_{\mathfrak{p}} V_{\mathfrak{p}}.$$

The plane curve $V_{\mathfrak{p}}$ (for each prime $\mathfrak{p}|\mathfrak{a}$) is called an *irreducible* component of $V_{\mathfrak{a}}$. Since $\mathfrak{p}$ is a principal prime, we cannot further have non-trivial decomposition $V_{\mathfrak{p}} = V \cup W$ with plane curves V and W. A prime ideal $\mathfrak{p} \subset k[X,Y]$ may decompose into a product of primes in $\overline{k}[X,Y]$. If $\mathfrak{p}$ remains prime in $\overline{k}[X,Y]$, we call $V_{\mathfrak{p}}$ *geometrically irreducible*.

Suppose that we have a map $F_A = F(\phi)_A : V_{\mathfrak{a}}(A) \to V_{\mathfrak{b}}(A)$ given by two polynomials

$$\phi_X(X,Y), \phi_Y(X,Y) \in k[X,Y]$$

(independent of A) such that $F_A(x,y) = (\phi_X(x), \phi_Y(y))$ for all $(x,y) \in V_{\mathfrak{a}}(A)$ and all k-algebras A. Such a map is called *a regular k-map* or *a k-morphism* from a plane k-curve $V_{\mathfrak{a}}$ into $V_{\mathfrak{b}}$. Here $V_{\mathfrak{a}}$ and $V_{\mathfrak{b}}$ are plane curve defined over k. If $\mathbf{A}^1 = V_{\mathfrak{b}}$ is the *affine line*, i.e., $V_{\mathfrak{b}}(A) \cong A$ for all A (taking for example $\mathfrak{b} = (y)$), a regular k-map $V_{\mathfrak{a}} \to \mathbf{A}^1$ is called a *regular k-function*. Regular k-functions are just functions induced by the polynomials in $k[x,y]$ on $V_{\mathfrak{a}}$; so, $R_{\mathfrak{a}}$ is the ring of regular k-functions of $V_{\mathfrak{a}}$ defined over k.

We write $\mathrm{Hom}_{k\text{-curves}}(V_{\mathfrak{a}}, V_{\mathfrak{b}})$ for the set of regular k-maps from $V_{\mathfrak{a}}$ into $V_{\mathfrak{b}}$. Obviously, only $\phi_?$ mod $\mathfrak{a}$ can possibly be unique. We have a commutative diagram for any k-algebra homomorphism $\sigma : A \to A'$:

$$\begin{array}{ccc} V_{\mathfrak{a}}(A) & \xrightarrow{F_A} & V_{\mathfrak{b}}(A) \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ V_{\mathfrak{a}}(A') & \xrightarrow[F_{A'}]{} & V_{\mathfrak{b}}(A'). \end{array}$$

Indeed,

$$\sigma(F_A((x,y))) = (\sigma(\phi_X(x,y)), \sigma(\phi_Y(x,y))) = (\phi_X(\sigma(x),\sigma(y)), \phi_Y(\sigma(x),\sigma(y)) = F_{A'}(\sigma(x),\sigma(y)).$$

Thus the k-morphism is a *natural transformation of functors* (or a *morphism of functors*) from $V_{\mathfrak{a}}$ into $V_{\mathfrak{b}}$. We write $\mathrm{Hom}_{COF}(V_{\mathfrak{a}}, V_{\mathfrak{b}})$ for the set of natural transformations (we will see later that $\mathrm{Hom}_{COF}(V_{\mathfrak{a}}, V_{\mathfrak{b}})$ is a set).

The polynomials (ϕ_X, ϕ_Y) induces a k-algebra homomorphism $\underline{F} : k[X,Y] \to k[X,Y]$ by pull-back, that is, $\underline{F}(\Phi(X,Y)) = \Phi(\phi_X(X,Y), \phi_Y(X,Y))$. Take a class $[\Phi]_{\mathfrak{b}} = \Phi + \mathfrak{b}$ in $B = k[X,Y]/\mathfrak{b}$. Then look at $\underline{F}(\Phi) \in k[X,Y]$ for $\Phi \in \mathfrak{b}$. Since $(\phi_X(x), \phi_Y(y)) \in V_{\mathfrak{b}}(\overline{k})$ for all $(x,y) \in V_{\mathfrak{a}}(\overline{k})$, $\Phi(\phi_X(x,y), \phi_Y(x,y)) = 0$ for all $(x,y) \in V_{\mathfrak{a}}(\overline{k})$. By Nullstellensatz, $\underline{F}(\Phi) \in \overline{\mathfrak{a}} \cap k[X,Y] = \mathfrak{a}$. Thus $\underline{F}(\mathfrak{b}) \subset \mathfrak{a}$, and $\underline{F}$ induces a (reverse) k-algebra homomorphism

$$\underline{F} : k[X,Y]/\mathfrak{b} \to k[X,Y]/\mathfrak{a}$$

making the following diagram commutative:

$$\begin{array}{ccc} k[X,Y] & \xrightarrow{\underline{F}} & k[X,Y] \\ \downarrow & & \downarrow \\ k[X,Y]/\mathfrak{b} & \xrightarrow[\underline{F}]{} & k[X,Y]/\mathfrak{a}. \end{array}$$

We write $R_{\mathfrak{a}} = k[X,Y]/\mathfrak{a}$ and call it the affine ring of $V_{\mathfrak{a}}$. Here is a useful (but tautological) lemma which is a special case of Yoneda's lemma:

Lemma 1.1. *We have a canonical isomorphism:*

$$\mathrm{Hom}_{COF}(V_{\mathfrak{a}}, V_{\mathfrak{b}}) \cong \mathrm{Hom}_{k\text{-}curves}(V_{\mathfrak{a}}, V_{\mathfrak{b}}) \cong \mathrm{Hom}_{k-alg}(R_{\mathfrak{b}}, R_{\mathfrak{a}}).$$

The first association is covariant and the second is contravariant. In particular, $\mathrm{Hom}_{COF}(V_{\mathfrak{a}}, V_{\mathfrak{b}})$ *is a set.*

Here is a sketch of the proof.

Proof. First we note $V_{\mathfrak{a}}(A) \cong \mathrm{Hom}_{ALG_{/k}}(R_{\mathfrak{a}}, A)$ via $(a,b) \leftrightarrow (\Phi(X,Y) \mapsto \Phi(a,b))$. Thus as functors, we have $V_{\mathfrak{a}}(?) \cong \mathrm{Hom}_{ALG_{/k}}(R_{\mathfrak{a}}, ?)$. We identify the two functors $A \mapsto V_{\mathfrak{a}}(A)$ and $A \mapsto \mathrm{Hom}(R_{\mathfrak{a}}, A)$ in this way. Then the main point of the proof of the lemma is to construct from a given natural transformation $F \in \mathrm{Hom}_{COF}(V_{\mathfrak{a}}, V_{\mathfrak{b}})$ a k-algebra homomorphism $\underline{F} : R_{\mathfrak{b}} \to R_{\mathfrak{a}}$ giving F by $V_{\mathfrak{a}}(A) = \mathrm{Hom}_{ALG_{/k}}(R_{\mathfrak{a}}, A) \ni \phi \overset{F_A}{\mapsto} \phi \circ \underline{F} \in \mathrm{Hom}_{ALG_{/k}}(R_{\mathfrak{b}}, A) = V_{\mathfrak{b}}(A)$. Then the following exercise finishes the proof, as plainly if we start with $\underline{F}$, the above association gives rise to F. □

Exercise 1.2. *Let $\underline{F} = F_{R_{\mathfrak{a}}}(\mathrm{id}_{R_{\mathfrak{a}}}) \in V_{R_{\mathfrak{b}}}(R_{\mathfrak{a}}) = \mathrm{Hom}_{ALG_{/k}}(R_{\mathfrak{b}}, R_{\mathfrak{a}})$, where $\mathrm{id}_{R_{\mathfrak{a}}} \in V_{\mathfrak{a}}(R_{\mathfrak{a}}) = \mathrm{Hom}_{ALG_{/k}}(R_{\mathfrak{a}}, R_{\mathfrak{a}})$ is the identity map. Then prove that $\underline{F}$ does the required job.*

We call $V_{\mathfrak{a}}$ *irreducible* (resp. *geometrically irreducible*) if $\mathfrak{a}$ is a prime ideal of $k[x,y]$ (resp. $\overline{\mathfrak{a}} = \mathfrak{a}\overline{k}[X,Y]$ is a prime ideal in $\overline{k}[X,Y]$).

Exercise 1.3.
(1) *Prove that for any UFD R, $R[X]$ is a UFD.*
(2) *Give an example of two distinct principal prime ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathbb{Q}[X,Y]$ with $V_{\mathfrak{a}}(\mathbb{Q}) = V_{\mathfrak{b}}(\mathbb{Q})$.*
(3) *If $\mathfrak{a}$ and $\mathfrak{b}$ are two distinct principal prime ideals of $\mathbb{Q}[X,Y]$, prove $V_{\mathfrak{a}}(\overline{\mathbb{Q}}) \neq V_{\mathfrak{b}}(\overline{\mathbb{Q}})$.*
(4) *For a principal ideal $\mathfrak{a} = (f) \subset k[X,Y]$, prove $\overline{\mathfrak{a}} \cap k[X,Y] = \mathfrak{a}$.*
(5) *Show that $\underline{F} : k[X,Y]/\mathfrak{b} \to k[X,Y]/\mathfrak{a}$ is uniquely determined by $F : V_{\mathfrak{a}} \to V_{\mathfrak{b}}$ independent of the choice of (ϕ_X, ϕ_Y), give an example that $\underline{F} : k[X,Y] \to k[X,Y]$ depends really on the choice of (ϕ_X, ϕ_Y).*

An element in the total quotient ring of $R_{\mathfrak{a}}$ is called a *rational k-function* on $V_{\mathfrak{a}}$. If $V_{\mathfrak{a}}$ is irreducible, then rational k-functions form a field. This field is called the *rational function field of $V_{\mathfrak{a}}$ over k.*

1.2. **Tangent space and local rings.** Suppose $\mathfrak{a} = (f(X,Y))$. Write $V = V_{\mathfrak{a}}$ and $R = R_{\mathfrak{a}}$. Let $P = (a,b) \in V_{\mathfrak{a}}(K)$. We consider partial derivatives

$$\frac{\partial f}{\partial X}(P) := \frac{\partial f}{\partial X}(a,b) \quad \text{and} \quad \frac{\partial f}{\partial Y}(P) := \frac{\partial f}{\partial Y}(a,b).$$

Then the line tangent to $V_{\mathfrak{a}}$ at (a,b) has equation

$$\frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b) = 0.$$

We write corresponding line as $T_P = V_{\mathfrak{b}}$ for the principal ideal $\mathfrak{b}$ generated by $\frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b)$. We call $V_{\mathfrak{a}}$ is *non-singular* or *smooth* at $P = (a,b) \in V_{\mathfrak{a}}(K)$ for a subfield $K \subset \Omega$ if this T_P is really a line; in other word, if $(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P)) \neq (0,0)$.

Example 1.4. *Let $\mathfrak{a} = (f)$ for $f(X,Y) = Y^2 - X^3$. Then $\frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b) = -3a^2(X-a) + 2b(Y-b)$ ($b^2 = a^3$). Thus this curve is singular only at $(0,0)$.*

Example 1.5. *Suppose that k has characteristic different from 2. Let $\mathfrak{a} = (Y^2 - g(X))$ for a cubic polynomial $g(X) = X^3 + aX + b$. Then the tangent line at (x_0, y_0) is given by $2y_0(X - x_0) - g'(x_0)(Y - y_0)$. This equation vanishes if $0 = y_0^2 = g(x_0)$ and $g'(x_0) = 0$; so, singular at only $(x_0, 0)$ for a multiple root x_0 of $g(X)$. Thus $V_{\mathfrak{a}}$ is a nonsingular curve if and only if $g(X)$ is separable if and only if its discriminant $-4a^3 - 27b^2 \neq 0$.*

Suppose that K/k is an algebraic field extension. Then $K[X,Y]/\mathfrak{a}K[X,Y]$ contains $R_{\mathfrak{a}}$ as a subring. The maximal ideal $(X-a, Y-b) \subset K[X,Y]/\mathfrak{a}K[X,Y]$ induces a maximal ideal $P = (X-a, Y-b) \cap R_{\mathfrak{a}}$ of $R_{\mathfrak{a}}$. The *local ring* $\mathcal{O}_{V,P}$ at P is the localization

$$\mathcal{O}_{V,P} = \left\{ \frac{a}{b} \middle| b \in R,\ b \in R \setminus P \right\},$$

where $\frac{a}{b} = \frac{a'}{b'}$ if there exists $s \in R \setminus P$ such that $s(ab' - a'b) = 0$. Write the maximal ideal of $\mathcal{O}_{V,P}$ as $\mathfrak{m}_P$. Then $\mathfrak{m}_P \cap R = P$.

Lemma 1.6. *The linear vector space $T_P(K)$ is the dual vector space of $P/P^2 = \mathfrak{m}_P/\mathfrak{m}_P^2$.*

Proof. Write $\mathfrak{a} = (f)$. Replacing $k[X,Y]/(f)$ by $K[X,Y]/(f)$, we may assume that $K = k$. A K-derivation $\partial : \mathcal{O}_{V,P} \to K$ (at P) is a K-linear map with $\partial(\phi\varphi) = \varphi(P)\partial(\phi) + \phi(P)\partial(\varphi)$. Writing $D_{V,P}$ for the space of K-derivations at P, which is a K-vector space. Plainly for $\mathbf{A} := V_{(0)}$, $D_{\mathbf{A},P}$ is a 2-dimensional vector space generated by $\partial_X : \phi \mapsto \frac{\partial \phi}{\partial X}(P)$ and $\partial_Y : \phi \mapsto \frac{\partial \phi}{\partial Y}(P)$. We have a natural injection $i : D_{V,P} \to D_{\mathbf{A},P}$ given by $i(\partial)(\phi) = \partial(\phi|_V)$. Note that $\Omega_{(a,b)} = (X-a, X-b)/(X-a, X-b)^2$ is a 2-dimensional vector space over K generated by $X-a$ and $Y-b$. Thus $D_{\mathbf{A},P}$ and $\Omega_{(a,b)}$ is dual each other under the pairing $(\alpha(X-a)+\beta(Y-b), \partial) = \partial(\alpha(X-a)+\beta(Y-b))$. The projection $k[X,Y] \twoheadrightarrow R$ induces a surjection

$$\Omega_{(a,b)} \to \Omega_{V,P} = P/P^2,$$

whose kernel is spanned by $f \mod (X-a, Y-b)^2 = \frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b)$ if $\mathfrak{a} = (f)$, since $\phi(X,Y) \equiv \frac{\partial \phi}{\partial X}(a,b)(X-a) + \frac{\partial \phi}{\partial Y}(a,b)(Y-b) \mod (X-a, Y-b)^2$. Thus the above duality between $\Omega_{(a,b)}$ and $D_{\mathbf{A},(a,b)}$ induces the duality $\Omega_{V,P} = P/P^2$ and $T_P(K)$ given by $(\omega, t) = t(\omega)$, where we regard t as a derivation $\mathcal{O}_{V,P} \to K$. □

We call T_P the *tangent* space at P and $\Omega_P = \Omega_{V,P}$ the *cotangent* space at P of V. More generally, a *k-derivation* $\partial : R_{\mathfrak{a}} \to R_{\mathfrak{a}}$ is a k-linear map satisfying the Leibniz condition $\partial(\phi\varphi) = \phi\partial(\varphi) + \varphi\partial(\phi)$ and $\partial(k) = 0$. For a k-derivation as above, $f\partial : \varphi \mapsto f \cdot \partial(\varphi)$ for $f \in R_{\mathfrak{a}}$ is again a k-derivation. The totality of k-derivation $Der_{V_{\mathfrak{a}}/k}$ is therefore an $R_{\mathfrak{a}}$-module.

First take $\mathfrak{a} = (0)$; so, $V_{\mathfrak{a}} = \mathbf{A}^2$. By the Leibniz relation,

$$\partial(X^n) = nX^{n-1}\partial X,\ \partial(Y^m) = mY^{m-1}\partial Y \ \text{ and } \ \partial(X^nY^m) = nX^{n-1}Y^m\partial X + mX^nY^{m-1}\partial Y$$

for $\partial \in Der_{\mathbf{A}^2/k}$; so, ∂ is determined by its value $\partial(X)$ and $\partial(Y)$. Note that $(\partial X)\frac{\partial}{\partial X} + (\partial Y)\frac{\partial}{\partial Y}$ in $Der_{\mathbf{A}^2/k}$ and the original ∂ has the same value at X and Y; so, we have

$$\partial = (\partial X)\frac{\partial}{\partial X} + (\partial Y)\frac{\partial}{\partial Y}.$$

Thus $\left\{\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}\right\}$ gives a basis of $Der_{\mathbf{A}^2/k}$.

Assuming $V_{\mathfrak{a}}$ nonsingular (including $\mathbf{A}^2 = V_{(0)}$), we write the dual as $\Omega_{V_{\mathfrak{a}}/k} := \mathrm{Hom}(Der_{V_{\mathfrak{a}}/k}, R_{\mathfrak{a}})$ (the *space of k-differentials*) with the duality pairing

$$(\cdot,\cdot) : \Omega_{V_{\mathfrak{a}}/k} \times Der_{V_{\mathfrak{a}}/k} \to R_{\mathfrak{a}}.$$

We have a natural map $d : R_{\mathfrak{a}} \to \Omega_{V_{\mathfrak{a}}/k}$ given by $\phi \mapsto (d\phi : \partial \mapsto \partial(\phi)) \in Der_{V_{\mathfrak{a}}/k}$. Note

$$(d(\phi\varphi), \partial) = \partial(\phi\varphi) = \phi\partial(\varphi) + \varphi\partial(\phi) = (\phi d\varphi + \varphi d\phi, \partial)$$

for all $\partial \in Der_{V_{\mathfrak{a}}/k}$. Thus we have $d(\phi\varphi) = \phi d\varphi + \varphi d\phi$, and d is a k-linear derivation with values in $\Omega_{V_{\mathfrak{a}}/k}$.

Again let us first look into $\Omega_{\mathbf{A}^2/k}$. Then by definition $(dX, \partial) = \partial X$ and $(dY, \partial) = \partial Y$; so, $\{dX, dY\}$ is the dual basis of $\left\{\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}\right\}$. We have $d\Phi = \frac{\partial \Phi}{\partial X}dX + \frac{\partial \Phi}{\partial Y}dY$ as we can check easily that the left hand side and right hand side as the same value on any $\partial \in Der_{\mathbf{A}^2/k}$.

If $\partial : R_{\mathfrak{a}} = k[X,Y]/(f) \to R_{\mathfrak{a}}$ is a k-derivation, we can apply it to any polynomial $\Phi(X,Y) \in k[X,Y]$ and hence regard it as $\partial : k[X,Y] \to R_{\mathfrak{a}}$. By the above argument, $Der_k(k[X,Y], R_{\mathfrak{a}})$ has a basis $\left\{\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}\right\}$ now over $R_{\mathfrak{a}}$. Since ∂ factors through the quotient $k[X,Y]/(f)$, it satisfies $\partial(f(X,Y)) = (df, \partial) = 0$. Thus we have

Lemma 1.7. *We have an inclusion $Der_{V_{\mathfrak{a}}/k} \hookrightarrow (R_{\mathfrak{a}}\frac{\partial}{\partial X} \oplus R_{\mathfrak{a}}\frac{\partial}{\partial Y})$ whose image is given by $\{\partial \in Der_k(k[X,Y], R_{\mathfrak{a}}) | \partial f = 0\}$. This implies*

$$\Omega_{V_{\mathfrak{a}}/k} = (R_{\mathfrak{a}}dX \oplus R_{\mathfrak{a}}dY)/R_{\mathfrak{a}}df$$

for $df = \frac{\partial f}{\partial X}dX + \frac{\partial}{\partial Y}dY$ by duality.

Remark 1.8. *If $V_{\mathfrak{a}}$ is an irreducible curve; so, $R_{\mathfrak{a}}$ is an integral domain, for its quotient field $k(V_{\mathfrak{a}})$, $k(V_{\mathfrak{a}})\Omega_{V_{\mathfrak{a}}/k} = (k(V_{\mathfrak{a}})dX \oplus k(V_{\mathfrak{a}})dY)/k(V_{\mathfrak{a}})df$ is 1 dimensional, as $df \neq 0$ in $\Omega_{\mathbf{A}^2/k}$. In particular, if we pick $\psi \in R_{\mathfrak{a}}$ with $d\psi \neq 0$ (i.e., a non-constant), any differential $\omega \in \Omega_{V_{\mathfrak{a}}/k}$ can be uniquely written as $\omega = \phi d\psi$ for $\phi \in k(V_{\mathfrak{a}})$.*

Lemma 1.9. *The following four conditions are equivalent:*

(1) *A point P of $V(\overline{k})$ is a smooth point.*
(2) *$\mathcal{O}_{V,P}$ is a local principal ideal domain, not a field.*
(3) *$\mathcal{O}_{V,P}$ is a discrete valuation ring with residue field $\overline{k}$.*
(4) *$\varprojlim_n \mathcal{O}_{V,P}/\mathfrak{m}_P^n \cong \overline{k}[[T]]$ (a formal power series ring of one variable).*

Proof. Let $K = \overline{k}$. By the above lemma, T_P is a line if and only if $\dim T_P(K) = 1$ if and only if $\dim P/P^2 = 1$. Thus by Nakayama's lemma (e.g., [MFG] Lemma 2.3), P is principal. Any prime ideal of $k[X,Y]$ is either minimal or maximal (i.e, the ring $k[X,Y]$ has Krull dimension 2). Thus any prime ideal of R and $\mathcal{O}_{V,P}$ is maximal. Thus (1) and (2) are equivalent. The equivalence of (2) and (3) follows from general ring theory (see [CRT] Theorem 11.2). We leave the equivalence (3) $\Leftrightarrow$ (4) as an exercise for the reader. □

Write x, y for the image of $X, Y \in k[X,Y]$ in $R_\mathfrak{a}$. Any $\omega \in \Omega_{V_\mathfrak{a}/k}$ can be written as $\phi dx + \varphi dy$. Suppose that $V_\mathfrak{a}$ is nonsingular. Since $\mathcal{O}_{V_\mathfrak{a},P} \hookrightarrow k[[T]]$ (for $P \in V_\mathfrak{a}(k)$) for a local parameter T as above, ϕ, φ, x, y have the "Taylor expansion" as an element of $k[[T]]$, for example, $x(T) = \sum_{n\geq 0} a_n(x)T^n$ with $a_n(x) \in k$. Thus dx, dy also have a well define expansion, say, $dx = d(\sum_{n\geq 0} a_n(x)T^n) = \sum_{n\geq 1} a_n(x)T^{n-1}dT$. Therefore we may expand

$$\omega = \phi dx + \varphi dy = \sum_{n\geq 0} a_n(\omega)T^n dT$$

once we choose a parameter T at P. This expansion is unique independent of the expression $\phi dx + \varphi dy$. Indeed, if we allow meromorphic functions Φ as coefficients, as we remarked already, we can uniquely write $\omega = \Phi dx$ and the above expansion coincides with the Taylor expansion of Φdx.

Exercise 1.10. *Let $P \in V_\mathfrak{a}(K)$ for a finite field extension K/k, and pull back P to a maximal ideal $(X-a, Y-b) \subset K[X,Y]$. Define $(X-a, Y-b) \cap k[X,Y]$, and project it down to a maximal ideal $p \subset R_\mathfrak{a} = k[X,Y]/\mathfrak{a}$. Write $\mathcal{O}_{V_\mathfrak{a},p}$ for the localization of $R_\mathfrak{a}$ at p. Prove the following facts:*

(1) *p is a maximal ideal and its residue field is isomorphic to the field $k(a,b)$ generated by a and b over k.*
(2) *$(p/p^2) \otimes_{k(a,b)} K \cong P/P^2$ as K-vector space.*
(3) *Any maximal ideal of $R_\mathfrak{a}$ is the restriction of $P \in V_\mathfrak{a}(K)$ for a suitable finite field extension K/k.*
(4) *$\mathcal{O}_{V_\mathfrak{a},p}$ is a DVR if and only if $\mathcal{O}_{V_\mathfrak{a},P}$ is a DVR.*

Write $\mathrm{Max}(R_\mathfrak{a})$ for the set of maximal ideals of $R_\mathfrak{a}$. Then plainly, we have a natural inclusion $V_\mathfrak{a}(k) \hookrightarrow \mathrm{Max}(R_\mathfrak{a})$ sending (a,b) to $(x-a, y-b)$ for the image x, y in $R_\mathfrak{a}$ of $X, Y \in k[X,Y]$. For $P \in \mathrm{Max}(R_\mathfrak{a})$, we call P is smooth on $V_\mathfrak{a}$ if $\mathcal{O}_{V,P}$ is a discrete valuation ring. By the above exercise, this is consistent with the earlier definition (no more and no less).

For any given affine plane irreducible curve $V_\mathfrak{a}$, we call $V_\mathfrak{a}$ is normal if $R_\mathfrak{a}$ is integrally closed in its field of fractions.

Corollary 1.11. *Any normal irreducible affine plane curve is smooth everywhere.*

Proof. By ring theory, any localization of a normal domain is normal. Thus $\mathcal{O}_{V,P}$ is a normal domain. By the exercise below, we may assume that $P \cap k[X,Y] \neq (0)$. Then P is a maximal ideal, and hence $K = k[X,Y]/P$ is an algebraic extension of k. In this case, $\mathcal{O}_{V,P}$ is a normal local domain with principal maximal ideal, which is a discrete valuation ring (cf. [CRT] Theorem 11.1). □

Exercise 1.12. (1) *Let $P = k[X,Y] \cap (X-a, Y-b)$ for $(a,b) \in V_\mathfrak{a}(\Omega)$, where $(X-a, Y-b)$ is the ideal of $\Omega[X,Y]$. Is it possible to have $P = (0) \subset k[X,Y]$ for a point $(a,b) \in V_\mathfrak{a}(\Omega)$.*
(2) *If $\mathfrak{a} = (XY)$, is the ring $\mathcal{O}_{V,O}$ for $O = (0,0)$ an integral domain? What is $\dim_k \mathfrak{m}_O/\mathfrak{m}_O^2$?*
(3) *For all points $P \in V_\mathfrak{a}(\Omega)$ with $R_\mathfrak{a} \cap P = (0)$ (regarding $P = (x-a, y-b)$ as an maximal ideal of $\Omega[X,Y]/\mathfrak{a}\Omega[X,Y]$), prove that V is smooth at P.*
(4) *If A is a discrete valuation ring containing a field $k \subset A$ which is naturally isomorphic to the residue field of A, prove $\widehat{A} = \varprojlim_n A/\mathfrak{m}_A^n \cong k[[T]]$, where $\mathfrak{m}_A$ is the maximal ideal of A.*

1.3. **Projective space.** Let A be a commutative ring. Write A_P be the localization at a prime ideal P of A. Thus

$$A_P = \left\{ \frac{b}{s} \middle| s \in A \setminus P \right\} / \sim,$$

where $\frac{b}{s} \sim \frac{b'}{s'}$ if there exists $s'' \in A \setminus P$ such that $s''(s'b - sb') = 0$. An A-module M is called *locally free* at P if

$$M_P = \{\frac{m}{s} | s \in A \setminus P\} / \sim = A_P \otimes_A M$$

is free over A_P. We call M locally free if it is free at all prime ideals of A. If $\mathrm{rank}_{A_P} M_P$ is constant r independent of P, we write $\mathrm{rank}_A M$ for r.

Write $ALG_{/k}$ for the category of k-algebras; so, $\mathrm{Hom}_{ALG_{/k}}(A, A')$ is made up of k-algebra homomorphisms from A into A' sending the identity 1_A to the identity $1_{A'}$. Here k is a general base ring, and we write ALG for $ALG_{/\mathbb{Z}}$ (as ALG is the category of all commutative rings with identity). We consider a covariant functor $\mathbf{P}^n = \mathbf{P}^n_{/k} : ALG_{/k} \to SETS$ given by

$$\mathbf{P}^n(A) = \left\{ L \subset A^{n+1} \middle| L \text{ (resp. } A^{n+1}/L) \text{ is locally } A\text{-free of rank 1 (resp. } n) \right\}.$$

This is a covariant functor. Indeed, if $\sigma : A \to A'$ is a k-algebra homomorphism, letting it act on A^{n+1} coordinate-wise, $L \mapsto \sigma(L)$ induces a map $\mathbf{P}^n(A) \to \mathbf{P}^n(A')$. If A is a field K, then X has to be free of dimension 1 generated by a non-zero vector $x = (x_0, x_1, \ldots, x_n)$. The vector x is unique up to multiplication by non-zero elements of K. Thus we have proven the first statement (for a field) of the following

Lemma 1.13. *Suppose that K is a local ring with maximal ideal $\mathfrak{m}$. Then we have*

$$\mathbf{P}^n(K) \cong \left\{ \underline{x} = (x_0, x_1, \ldots, x_n) \in K^{n+1} \middle| \underline{x} \not\equiv (0, \ldots, 0) \mod \mathfrak{m} \right\} / K^\times.$$

Moreover, writing $D_i : ALG_{/k} \to SETS$ for the subfunctor $D_i(A) \subset \mathbf{P}^n(A)$ made up of the classes L whose projection to the i-th component $A \subset A^{n+1}$ is surjective, we have $\mathbf{P}^n(K) = \bigcup_i D_i(K)$ and $D_i(A) \cong \mathbf{A}^n$ canonically for all k-algebras A. If A is a local ring K, $D_i \cong \mathbf{A}^n$ is given by sending $(x_0, \ldots, x_n)$ to $(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}) \in K^n$ removing the i-th coordinate.

Proof. Since $K = K_{\mathfrak{m}}$ for its maximal ideal $\mathfrak{m}$, L is K-free if it is locally free. Thus we have a generator $\underline{x} = (x_0, \ldots, x_n)$ of L over K. Since K^{n+1}/L is locally free of rank n, it has to be free of rank n over K as K is local. Take a basis $\overline{v}_1, \ldots, \overline{v}_n$ of K^{n+1}/L, we can lift them to $v_i \in K^{n+1}$ so that $\underline{x}, v_1, \ldots, v_n$ form a basis of K^{n+1} over K. Thus $\underline{x} \not\equiv 0 \mod \mathfrak{m}$ for the maximal ideal $\mathfrak{m}$ of K. In particular, for an index i, $x_i \notin \mathfrak{m}$; so, $x_i \in K^\times$. Since the projection of L to the i-th component is generated by $x_i \in K^\times$, it is equal to K, and hence $\underline{x} \in D_i(K)$. Thus $\mathbf{P}^n(K) = \bigcup_i D_i(K)$.

If $L \in D_i(A)$, we have the following commutative diagram

$$\begin{array}{ccc} L & \xrightarrow{\hookrightarrow} & A^{n+1} \\ \| \downarrow & & \downarrow i\text{-th proj} \\ L & \xrightarrow{\sim} & A \end{array}$$

Thus L is free of rank 1 over A; so, it has a generator $(x_0, \ldots, x_n)$ with $x_i \in A^\times$. Then $(x_0, \ldots, x_n) \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}) \in A^n$ gives rise to a natural transformation of D_i onto $\mathbf{A}^n$ (which is an isomorphism of functors). □

If K is local (in particular, a field), we write $(x_0 : x_1 : \cdots : x_n)$ for the point of $\mathbf{P}^n(K)$ represented by $(x_0, \ldots, x_n)$ as only the ratio matters.

Exercise 1.14. *Is there any example of a point in $X \in \mathbf{P}^1(A)$ (and a ring A) such that the projections to the first and the second coordinate are both not surjective?*

We assume that K is a field for a while. When $n = 1$, we see $\mathbf{P}^1(K) = K^\times \sqcup \{\infty\}$ by $(x : y) \mapsto \frac{x}{y} \in K \sqcup \{\infty\}$. Thus $\mathbf{P}^1(\mathbb{R})$ is isomorphic to a circle and $\mathbf{P}^1(\mathbb{C})$ is a Riemann sphere.

We now assume that $n = 2$. Writing $L = \{(x : y : 0) \in \mathbf{P}^2(K)\}$. Then $\mathbf{P}^1 \cong L$ by $(x : y) \mapsto (x : y : 0)$; so, L is isomorphic to the projective line. We have $\mathbf{P}^2(K) = D(K) \sqcup L$ for fields K, where $D = D_2$. Thus geometrically (i.e., over fields), $\mathbf{P}^2$ is the union of the affine plane added L. We call $L = L_\infty$ (the line at ∞).

1.4. **Projective plane curve.** For a plane curve defined by $\mathfrak{a} = (f(x,y))$ for $f(x,y)$ of degree m, we define $F(X,Y,Z) = Z^m f(\frac{X}{Z}, \frac{Y}{Z})$, which is a (square-free) homogeneous polynomial of degree m in $k[X,Y,Z]$. If $L \in \mathbf{P}^2(A)$, we can think of $F(\ell)$ for $\ell \in L$. We write $F(L) = 0$ if $F(\ell) = 0$ for all $\ell \in L$. Thus for any k-algebra A, we define the functor $\overline{V}_{\mathfrak{a}} : ALG_{/k} \to SETS$ by

$$\overline{V}_{\mathfrak{a}}(A) = \left\{ L \in \mathbf{P}^2(A) | F(L) = 0 \right\}.$$

If A is a field K, we sent $L \in \mathbf{P}^2(K)$ to its generator $(a : b : c) \in L$ when we identified $\mathbf{P}^2(K)$ with the (classical) projective space with homogeneous coordinate. Since $F(L) = 0$ if and only if $F(a : b : c) = 0$ in this circumstances, we have

$$\overline{V}_{\mathfrak{a}}(K) = \left\{ (a : b : c) \in \mathbf{P}^2(K) | F(a,b,c) = 0 \right\}$$

which is called a *projective plane k-curve*. Since $D_2 \cong \mathbf{A}^2$ canonically via $(x : y : 1) \mapsto (x, y)$ (and this coordinate is well defined even over A which is not a field), we have $\overline{V}_{\mathfrak{a}}(A) \cap D_2(A) = V_{\mathfrak{a}}(A)$. In this sense, we can think of $\overline{V}_{\mathfrak{a}}$ as a completion of $V_{\mathfrak{a}}$ adding the boundary $\overline{V}_{\mathfrak{a}} \cap L_\infty$. Since in $D_j \cong \mathbf{A}^2$ $(j = 0, 1)$, $\overline{V}_{\mathfrak{a}} \cap D_j$ is a plane affine curve (for example, $\overline{V}_{\mathfrak{a}} \cap D_0$ is defined by $F(1, y, z) = 0$), $(L_\infty \cap \overline{V}_{\mathfrak{a}})(\overline{k})$ is a finite set. Thus $\overline{V}_{\mathfrak{a}}$ is a sort of completion/compactification of the (open) affine curve $V_{\mathfrak{a}}$ (we sort out this point more rigorously later). Of course, we can start with a homogeneous polynomial $F(X,Y,Z)$ (or a homogeneous ideal of $k[X,Y,Z]$ generated by $F(X,Y,Z)$) to define a projective plane curve. Following Lemma 1.1, we define $\mathrm{Hom}_{k\text{-curves}}(\overline{V}_{\mathfrak{a}}, \overline{V}_{\mathfrak{b}}) := \mathrm{Hom}_{COF}(\overline{V}_{\mathfrak{a}}, \overline{V}_{\mathfrak{b}})$.

Example 1.15. *Suppose $\mathfrak{a} = (y^2 - f(x))$ for a cubic $f(x) = x^3 + ax + b$. Then $F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$. Since L_∞ is defined by $Z = 0$, we find $L_\infty \cap \overline{V}_{\mathfrak{a}} = \{(0 : 1 : 0)\}$ made of a single point (of $\overline{V}_{\mathfrak{a}}$ intersecting with L_∞ with multiplicity 3). This point we call the origin $\mathbf{0}$ of $V_{\mathfrak{a}}$.*

A projective plane curve $\overline{V}_{\mathfrak{a}}$ is non-singular (or smooth) if $\overline{V}_{\mathfrak{a}} \cap D_j$ is a non-singular plane curve for all $j = 0, 1, 2$. The tangent space at $P \in \overline{V}_{\mathfrak{a}}(K)$ is defined as before since P is in one of $D_j \cap V_{\mathfrak{a}}$.

Exercise 1.16. *Suppose $\overline{V}_{\mathfrak{a}}$ is defined by $F(X,Y,Z) = 0$. Let $f(x,y) = F(x,y,1)$ and $g(y,z) = F(1,y,z)$. Then the projective plane curve $\overline{V}_{\mathfrak{a}}$ for $\mathfrak{a} = (f(x,y))$ satisfies $\overline{V}_{\mathfrak{a}} \cap D_0 = V_{(g)}$. Show that $\mathcal{O}_{V_{\mathfrak{a}},P} \cong \mathcal{O}_{V_{(g)},P}$ canonically if $P \in \overline{V}_{\mathfrak{a}} \cap D_0 \cap D_2$.*

By the above exercise, the tangent space (the dual of $\mathfrak{m}_P/\mathfrak{m}_P^2$) at $P \in \overline{V}_{\mathfrak{a}}(K)$ does not depend on the choice of j with $P \in \overline{V}_{\mathfrak{a}} \cap D_j$. If a projective plane curve C is irreducible, the rational function field over k is the field of fraction of $\mathcal{O}_{C,P}$ for any $P \in C(\overline{k})$; so, independent of $C \cap D_j$.

Lemma 1.17. *Take a nonzero $f \in k(C)$. Then we find homogeneous polynomials $H(X,Y,Z)$ and $G(X,Y,Z) \neq 0$ in $k[X,Y,Z]$ with $\deg(G) = \deg(H)$ such that $f(x{:}y{:}z) = \frac{H(x,y,z)}{G(x,y,z)}$ for all $(x{:}y{:}z) \in C(\overline{k})$.*

Proof. We may write on $C \cap D_2$ $f(x,y,1) = \frac{h(x,y)}{g(x,y)}$. If $m = \deg(h) = \deg(g)$, we just define $H(X,Y,Z) = h(\frac{X}{Z}, \frac{Y}{Z})Z^m$ and $G(X,Y,Z) = g(\frac{X}{Z}, \frac{Y}{Z})Z^m$. If $\deg(h) > \deg(g)$, we define $H(X,Y,Z) = h(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(h)}$ and $G(X,Y,Z) = g(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(h)}$. If $\deg(h) < \deg(g)$, we define $H(X,Y,Z) = h(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(g)}$ and $G(X,Y,Z) = g(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(g)}$. Multiplying h or g by a power of Z does not change the above identity $f(x,y,1) = \frac{h(x,y)}{g(x,y)}$, because $Z = 1$ on $C \cap D_2$. Thus adjusting in this way, we get G and H. □

Example 1.18. *Consider the function $\phi = cx + dy$ in $k(C)$ for $C = \overline{V}_{\mathfrak{a}}$ with $\mathfrak{a} = (y^2 - x^3 - ax - b)$. Then C is defined by $Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$, and*

$$\phi(X{:}Y{:}Z) = c\frac{X}{Z} + d\frac{Y}{Z} = \frac{cX + dY}{Z}.$$

So ϕ has pole of order 3 at $Z = 0$ (as the infinity on C has multiplicity 3) and three zeros at the intersection of $L := \{cx + dy = 0\}$ and $C \cap D_2 \cap L$.

Take a projective nonsingular plane k-curve $C_{/k}$. Put $C_i = C \cap D_i$ which is an affine nonsingular plane curve. Then we have well defined global differentials $Der_{C_i/k}$. Since $\partial : Der_{C_i/k}$ induces $\partial_P : \mathcal{O}_{C_i,P} \to K$ for any $P \in C_i(K)$ by $f \mapsto \partial(f)(P)$, we have $\partial_P \in T_P$. If $\partial_i \in Der_{C_i/k}$ given for

each $i = 0, 1, 2$ satisfies $\partial_{i,P} = \partial_{j,P}$ for all (i, j) and all $P \in (D_i \cap D_j)(\overline{k})$, we call $\partial = \{\partial_i\}_i$ a global tangent vector defined on C. Plainly the totality $T_{C/k}$ of global tangent vectors are k-vector space. The k-dual of $T_{C/k}$ is called the space of k-differentials over k and written as $\Omega_{C/k}$. It is known that $\Omega_{C/k}$ is finite dimensional over k.

Corollary 1.19. *Suppose that C is non-singular. Each $\phi \in k(C)$ induces $\phi \in \mathrm{Hom}_{k\text{-}curves}(C, \mathbf{P}^1)$. Indeed, we have $k(C) \sqcup \{\infty\} \cong \mathrm{Hom}_{proj\ k\text{-}curves}(C, \mathbf{P}^1)$, where ∞ stands for the constant function sending all $P \in C(A)$ to the image of $\infty \in \mathbf{P}^1(k)$ in $\mathbf{P}^1(A)$.*

Proof. We prove only the first assertion. Suppose $k = \overline{k}$. Write $\phi(x{:}y{:}z) = \frac{h(x,y,z)}{g(x,y,z)}$ as a reduced fraction by the above lemma. For $L \in C(A) \subset \mathbf{P}^2(A)$, we consider the sub A-module $\phi(L)$ of A^2 generated by $\{(h(\ell), g(\ell)) \in A^2 | \ell \in L\}$. We now show that $\phi(L) \in \mathbf{P}^1(A)$; so, we will show that the map $C(A) \ni L \mapsto \phi(L) \in \mathbf{P}^1(A)$ induces the natural transformation of C into $\mathbf{P}^1$. If A is local, by Lemma 1.13, L is generated by (a, b, c) with at least one unit coordinate. Then any $\ell \in L$ is of the form $\lambda(a, b, c)$ and therefore $\phi(\ell) = \lambda^{\deg(h)}\phi(a, b, c)$. Thus $\phi(L) = A{\cdot}\phi(a, b, c)$. Since A is a k-algebra, k is naturally a subalgebra of the residue field $A/\mathfrak{m}$ of A. Since $\phi(P)$ for all $P \in C(k)$ is either a constant in k or ∞, we may assume that $(h(P), g(P)) \neq (0, 0)$ for all $P \in C(k)$. Since $(a, b, c) \not\equiv 0 \mod \mathfrak{m}$ as (a, b, c) generates a direct summand of A^3. Thus $(h(a, b, c), g(a, b, c)) \not\equiv (0, 0) \mod \mathfrak{m}$. After tensoring $A/\mathfrak{m}$ over A, $(A/\mathfrak{m})^2/(\phi(L)/\mathfrak{m}\phi(L))$ is one dimensional. Thus by Nakayama's lemma (e.g., [CRT] Theorem 2.2–3), $A/\phi(L)$ is generated by a single element and has to be a free module of rank 1 as $\phi(L)$ is a free A-module of rank 1. Thus $\phi(L) \in \mathbf{P}^1(A)$. If k is not algebraically closed, replacing A by $\overline{A} = A \otimes_k \overline{k}$, we find $\phi(L) \otimes_k \overline{k} \in \mathbf{P}^2(\overline{k})$ and hence $\phi(L) \otimes_A A/\mathfrak{m} \in \mathbf{P}^2(k)$, which implies $\phi(L) \in \mathbf{P}^2(A)$.

If A is not necessarily local, applying the above argument to the local ring A_P for any prime ideal P of A, we find that $\phi(L)_P = \phi(L_P)$ and $A_P^2/\phi(L_P)$ are free of rank 1; so, $\phi(L)$ and $A^2/\phi(L)$ are locally free of rank 1; therefore, $\phi(L) \in \mathbf{P}^2(A)$.

Now it is plain that $L \mapsto \phi(L)$ induces a natural transformation of functors. □

Exercise 1.20. *Prove the following facts:*

1. *If $L_\mathfrak{m}$ is free of finite rank r for a maximal ideal $\mathfrak{m}$ of A, L_P is free of rank r for any prime ideal $P \subset \mathfrak{m}$.*
2. *If $L \subset A^2$ is a free A-submodule of rank 1 and A^2/L is generated by one element over A, A^2/L is A-free of rank 1.*
3. $\mathrm{Hom}_{k\text{-}curves}(C, \mathbf{P}^1) \setminus \infty \cong k(C)$.

1.5. **Divisors.** The *divisor group* $\mathrm{Div}(C)$ of a non-singular projective geometrically irreducible plane curve C is a formal free $\mathbb{Z}$-module generated by points $P \in C(\overline{k})$. When we consider a point P as a divisor, we write it as $[P]$. For each divisor $D = \sum_P m_P[P]$, we define $\deg(D) = \sum_P m_P$. Since C is nonsingular, for any point $P \in C(\overline{k})$, $\mathcal{O}_{C,P}$ is a DVR, and the rational function field $\overline{k}(C)$ is the quotient field of $\mathcal{O}_{C,P}$ (regarding C as defined over $\overline{k}$). Thus if we write the valuation $v_P : \overline{k}(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ for the additive valuation of $\mathcal{O}_{C,P}$, we have a well defined $v_P(f) \in \mathbb{Z}$ for any non-zero rational $\overline{k}$-function $f \in \overline{k}(C)$. Since $\mathfrak{m}_P = (t_P)$ and $t_P^{v_P(f)} \| f$ in $\mathcal{O}_{C,P}$, f has a zero of order $v_p(f)$ at P if $v_P(f) > 0$ and a pole of order $|v_p(f)|$ if $v_P(f) < 0$. In other words, the Taylor expansion of f at P is given by $\sum_n a_n(f)t_P^n$ and $v_p(f) = \min(n : a_n(f) \neq 0)$. For a global differential $\omega \in \Omega_{C/\overline{k}}$, we have its Taylor expansion $\sum_n a_n(f)t_P^n dt_P$ at each $P \in C(\overline{k})$; so, we may also define $v_P(\omega) := \min(n : a_n(\omega) \neq 0)$. We extend this definition for meromorphic differentials $k(C) \cdot \Omega_{C/k} = \{f \cdot \omega | f \in k(C), \omega \in \Omega_{C/k}\}$. Here we quote Bézout's theorem:

Theorem 1.21. *Let C and C' be two plane projective k-curves inside $\mathbf{P}^2$ defined by relatively prime homogeneous equations*

$$F(X, Y, Z) = 0 \quad \textit{and} \quad G(X, Y, Z) = 0$$

of degree m and n respectively. Then counting with multiplicity, we have $|C(\overline{k}) \cap C'(\overline{k})| = m \cdot n$.

If C is smooth at $P \in C \cap C'$ in $C \cap D_2$, $\phi = \frac{G(X,Y,Z)}{Z^n}$ is a function vanishing at P. The multiplicity of P in $C \cap C'$ is just $v_P(\phi)$. More generally, if $P = (a, b)$ is not necessarily a smooth point, writing

$C \cap D_2 = V_{\mathfrak{a}}$ and $C' \cap D_2 = V_{\mathfrak{b}}$ for principal ideals $\mathfrak{a}, \mathfrak{b}$ in $\overline{k}[X,Y]$ and viewing P as an ideal

$$(X-a, Y-b) \subset \overline{k}[X,Y],$$

the multiplicity is given by the dimension of the localization $(\overline{k}[x,y]/\mathfrak{a}+\mathfrak{b})_P$ over $\overline{k}$. The same definition works well for any points in $C \cap D_0$ and $C \cap D_1$. One can find the proof of this theorem with (possibly more sophisticated) definition of multiplicity in a text of algebraic geometry (e.g. [ALG] Theorem I.7.7).

We define divisors $\mathrm{div}(f) = \sum_{P \in C(k)} v_P(f)[P]$, $\mathrm{div}_0(f) = \sum_{P \in C(k), v_P(f)>0} v_P(f)[P]$ (zero divisor) and $\mathrm{div}_\infty(f) = \sum_{P \in C(k), v_P(f)<0} v_P(f)[P]$ (polar divisor) of f. Similarly, for meromorphic differential ω, we define again $\mathrm{div}(\omega) = \sum_P v_P(\omega)[P]$. By Lemma 1.17, $f(x{:}y{:}z) = \frac{h(x:y:z)}{g(x:y:z)}$ for a homogeneous polynomial h, g in $\overline{k}[x,y,z]$ of the same degree. If the degree of equation defining C is m and C' is defined by $h(X,Y,Z)=0$, $\deg_0(\mathrm{div}(f)) = |C(\overline{k}) \cap C'(\overline{k})| = m\deg(h) = m\deg(g) = \deg_\infty(\mathrm{div}(f))$. This shows $\deg(\mathrm{div}(f)) = 0$ as $\sum_{P, v_P(f)>0} m_P = m\deg(h)$ and $-\sum_{P, v_P(f)<0} m_P = m\deg(g)$.

Lemma 1.22. *Let C be a nonsingular projective plane curve. For any $f \in \overline{k}(C)$, $\deg(\mathrm{div}(f)) = 0$, and if $f \in \overline{k}(C)$ is regular at every $P \in C$, f is a constant in $\overline{k}$.*

Lemma 1.23. *If $f \in k(C)$ satisfies $\deg(\mathrm{div}_0(f)) = \deg(\mathrm{div}_\infty(f)) = 1$, $f : C \to \mathbf{P}^1$ induces an isomorphism of projective plane curve over k.*

Proof. Write $\phi(x{:}y{:}z) = \frac{H(x,y,z)}{G(x,y,z)}$ as a reduced fraction of homogeneous polynomials $G, H \in k[X,Y,Z]$ of degree n. Suppose C is defined by a homogeneous equation of degree m. Then by Bézout's theorem, $m \cdot n = \deg(\mathrm{div}_0(\phi)) = 1$. Thus $m = n = 1$, and it is then plain that $(x{:}y{:}z) \mapsto (G(x,y,z){:}H(x,y,z))$ gives rise to an isomorphism $C \cong \mathbf{P}^1$.

Another proof: By the proof of Corollary 1.19, $\deg(\mathrm{div}_0(f))$ is the number of points over 0 (counting with multiplicity) of the regular map $f : C \to \mathbf{P}^1$. By taking off a constant $\alpha \in k \subset \mathbf{P}^1$ to f, $\deg(\mathrm{div}_0(f-\alpha)) = 1 = \deg(\mathrm{div}_\infty(f-\alpha))$, and $|f^{-1}(\alpha)| = \deg(\mathrm{div}_0(f-\alpha)) = 1$; so, we find that f is one-to-one and onto. Thus f is an isomorphism. □

Write $\mathrm{Div}^r(C) = \{D \in \mathrm{Div}(C_{/\overline{k}}) | \deg(D) = r\}$. Inside $\mathrm{Div}^0(C)$, we have the subgroup $\{\mathrm{div}(f) | f \in \overline{k}(C)^\times\}$. We call two divisors D, D' *linearly equivalent* if $D = \mathrm{div}(f) + D'$ for $f \in \overline{k}(C)$. We call that D and D' are *algebraically equivalent* if $\deg(D) = \deg(D')$. The quotient groups

$$\mathcal{J}(C) = \frac{\mathrm{Div}^0(C)}{\{\mathrm{div}(f) | f \in k(C)^\times\}} \quad \text{and} \quad \mathrm{Pic}(C) = \frac{\mathrm{Div}(C)}{\{\mathrm{div}(f) | f \in k(C)^\times\}}$$

are called the *jacobian* and the *Picard group* of C, respectively. Sometimes, $\mathcal{J}(C)$ is written as $\mathrm{Pic}^0(C)$ (the degree 0 Picard group).

1.6. **Riemann–Roch theorem.** We write $D = \sum_P m_P[P] \geq 0$ (resp. $D > 0$) for a divisor D on C if $m_P \geq 0$ for all P (resp. $D \geq 0$ and $D \neq 0$). For a divisor D on $C_{\overline{k}}$

$$L(D) = \{f \in \overline{k}(C) | \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

Plainly, $L(D)$ is a vector space over $\overline{k}$. It is known that $\ell(D) = \dim_{\overline{k}} L(D) < \infty$. For $\phi \in k(C)^\times$, $L(D) \ni f \mapsto f\phi \in L(D - \mathrm{div}(\phi))$ is an isomorphism. Thus $\ell(D)$ only depends on the class of D in $\mathrm{Pic}(C)$.

Example 1.24. Let $C = \mathbf{P}^1$. For a positive divisor $D = \sum_{a \in \overline{k}} m_a[a]$ with $m_a \geq 0$ and $m_a > 0$ for some a, regarding $a \in \overline{k}$ as a point $[a] \in \mathbf{P}^1(\overline{k}) = \overline{k} \sqcup \{\infty\}$. On $\mathbf{A}^1(\overline{k}) = \overline{k}$, forgetting about the infinity, $\mathrm{div}(f) + D \geq 0$ if $f = \frac{g(x)}{\prod_a (x-a)^{m_a}}$ for a polynomial $g(x)$. If $\deg(D) \geq \deg(g(x))$, the function f does not have pole at ∞. Thus $L(D) = \{g(x) | \deg(g(x)) \leq \deg(D)\}$ and we have $\ell(D) = 1 + \deg(D)$ if $D > 0$. If C is a plane projective curve, we can write $f = \frac{h(X,Y,Z)}{g(X,Y,Z)}$ as a reduced fraction by Lemma 1.17. Write $D = \sum_P m_P[P]$, and put $|D| = \{P | D = \sum_P m_P[P] \text{ with } m_P \neq 0\}$. If $|D|$ is inside $D_2 \cap C \subset \mathbf{A}^2$ and $D > 0$, we may assume that $V_{(g(X,Y,1))} \cap C$ contains $|D|$. Then not to have pole at $C \setminus D_2$, $\deg(h)$ has to be bounded; so, $\ell(D) < \infty$. Since $L(D) \subset L(D_+)$ in general, writing $D = D_+ + D_-$ so that $D_+ \geq 0$ and $-D_- \geq 0$, this shows $\ell(D) < \infty$.

Exercise 1.25. *Give more details of the proof of $\ell(D) < \infty$.*

Theorem 1.26 (Riemann-Roch)**.** *Let C be a non-singular projective curve defined over a field k. Then for $g = \dim_{\overline{k}} \Omega_{C/\overline{k}}$ and a divisor K of degree $2g-2$ of the form $\mathrm{div}(\omega)$ for a meromorphic differential ω on C such that $\ell(D) = 1 - g + \deg(D) + \ell(K - D)$ for all divisor D on $C(\overline{k})$. If $g = 1$, we have $K = 0$.*

This theorem applies to any smooth projective curve including non-singular projective curves of the form $\overline{V}_{\mathfrak{a}}$. We will study general curves and schemes later in Section 4. The divisor K is called a *canonical divisor* K (whose linear equivalence class is unique). Note that

$$L(K) = \{f \in \overline{k}(C) | \mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega) \geq 0\} \cong \Omega_{C/\overline{k}}$$

by $f \mapsto f\omega \in \Omega_{C/k}$. Then by the above theorem,

$$g(C) = \dim \Omega_{C/\overline{k}} = \ell(K) = 1 - g + \deg(K) + \ell(0) = 2 + \deg(K) - g(C),$$

and from this, we conclude $\deg(K) = 2g(C) - 2$. One can find a proof of this theorem in any introductory book of algebraic geometry (e.g., [ALG] IV.1 or [GME] Theorem 2.1.3).

Corollary 1.27. *If $g(C) = 1$, then $\ell(D) = \deg(D)$ and $\ell(-D) = 0$ if $\deg(D) > 0$.*

Proof. For a non-constant $f \in \overline{k}(E)$, $\deg(\mathrm{div}(f)) = 0$ implies that f has a pole somewhere. If $D > 0$, $f \in L(-D)$ does not have pole; so, constant. Since $D > 0$, f vanishes at $P \subset D$. Thus $f = 0$. More generally, if $\deg(D) > 0$ and $\phi \in L(-D)$, then $0 > \deg(-D) = \deg(\phi) - \deg(D) \geq 0$; so, $\phi = 0$. Thus if $\deg(D) > 0$, then $\ell(-D) = 0$. Since $K = 0$, we have by the Riemann-Roch theorem that $\ell(D) = \deg(D) + \ell(0 - D) = \deg(D)$ if $\deg(D) > 0$. □

Because of $\deg(\mathrm{div}(f)) = 0$, if $D \gg 0$, $\ell(-D) = 0$. In particular $\ell(K - D) = 0$ if $D \gg 0$. Thus the above theorem implies what Riemann originally proved:

Corollary 1.28 (Riemann)**.** *Let $C = \overline{V}_{\mathfrak{a}}$ be a non-singular projective curve defined over a field k. Then there exists a non-negative integer $g = g(C)$ such that $\ell(D) \geq 1 - g + \deg(D)$ for all divisor D on $C(\overline{k})$ and the equality holds for sufficiently positive divisor D.*

By the above example, we conclude $g(\mathbf{P}^1) = 0$ from the corollary.

Exercise 1.29. *Prove $\Omega_{\mathbf{P}^1/\overline{k}} = 0$.*

1.7. **Regular maps from a curve into projective space.** Take a divisor D on a nonsingular projective plane curve C. Suppose $\ell(D) = n > 0$. Take a basis $(f_1, f_2, \ldots, f_n)$ of $L(D)$. Thus we can write $f_j = \frac{h_j}{g_j}$ with homogeneous polynomials g_j, h_j having $\deg(g_j) = \deg(h_j)$. Replacing (g_j, h_j) by $(g_0' := g_1 g_2 \cdots g_n, h_j' := h_j g^{(j)})$ for $g^{(j)} = \prod_{i \neq j} g_i$, we may assume $\deg(g_j') = \deg(h_j')$ for all j, and further dividing them by the GCD of $(h_1', \ldots, h_n', g_0')$, we may assume that $f_j = \frac{h_j}{g_0}$ with $\deg(h_j) = \deg(g_0)$ for all j and $(g_0, h_1, \ldots, h_n)$ do not have nontrivial common divisor.

Lemma 1.30. *Let the assumptions on $(g_0, h_1, \ldots, h_n)$ be as above. Suppose that*

$$(g_0(P), h_1(P), \ldots, h_n(P)) \neq (0, 0, \ldots, 0)$$

for all $P \in C(\overline{k})$. Define $L \in C(A) \subset \mathbf{P}^n(A)$, $\phi_A(L)$ for an A-submodule of A^{n+1} generated by $\phi(\ell) = (g_0(\ell), h_1(\ell), \ldots, h_n(\ell)) \in A^{n+1}$ for all $\ell \in L$. Then $\phi = \{\phi_A\}_A : C \to \mathbf{P}^n$ is a k-morphism of the projective plane k-curve C into $\mathbf{P}^n_{/k}$.

The proof of the above lemma is the same as that of Corollary 1.19; so, we leave it to the reader:

Exercise 1.31. *Prove the above lemma.*

2. Elliptic Curves

An *elliptic curve* $E_{/k}$ is a non-singular projective geometrically irreducible plane curve with point $\mathbf{0}_E$ specified having $g(E) = 1$. Here we define $g(E)$, regarding E is defined over $\overline{k}$. We study elliptic curves in more details.

2.1. **Abel's theorem.** When we regard $P \in E(k)$ as a divisor, we just write $[P]$. So $3[P]$ is a divisor supported on P with multiplicity 3. We prove

Theorem 2.1 (Abel)**.** *Let $E_{/k}$ be an elliptic curve with origin $\mathbf{0}_E$. The correspondence $P \mapsto [P]-[\mathbf{0}_E]$ induces a bijection $E(\overline{k}) \cong \mathcal{J}(E)$. In particular, $E(\overline{k})$ is an abelian group.*

Proof. Injectivity: if $[P]-[Q] = [P]-[\mathbf{0}_E]-([Q]-[\mathbf{0}_E]) = \mathrm{div}(f)$ with $P \neq Q$ in $E(\overline{k})$, by Lemma 1.23, f is an isomorphism. This is wrong as $g(\mathbf{P}^1) = 0$ while $g(E) = 1$. Thus $P = Q$.

Surjectivity: Pick $D \in \mathrm{Div}^0(E)$. Then $D+[\mathbf{0}_E]$ has degree 1; so, by Corollary 1.27, $\ell(D+[\mathbf{0}_E]) = 1$, and we have $\phi \in L(D+[\mathbf{0}_E])$. Then $\mathrm{div}(\phi)+D+[\mathbf{0}_E] \geq 0$, and this divisor has degree 1. Any non-negative divisor with degree 1 is a single point $[P]$. Thus $D+[\mathbf{0}_E]$ is linearly equivalent to $[P]$; so, the map is surjective. □

Corollary 2.2. *If $0 \neq \omega \in \Omega_{E/\overline{k}}$, then $\mathrm{div}(\omega) = 0$.*

Proof. Since $E(\overline{k})$ is a group, for each $P \in E(\overline{k})$, $\mathcal{T}_P : Q \mapsto Q+P$ gives an automorphism of E. Thus $\omega \circ \mathcal{T}_P$ is another element in $\Omega_{E/\overline{k}}$. Since $\dim \Omega_{E/\overline{k}} = 1$, we find $\omega \circ \mathcal{T}_P = \lambda(P)\omega$ for $\lambda(P) \in \overline{k}^\times$. Since $\omega \neq 0$, at some point $P \in E(\overline{k})$, $v_P(\omega) = 0$. Since $v_Q(\omega \circ \mathcal{T}_P) = v_{P+Q}(\omega)$ and we can bring any point to P by translation, we have $v_P(\omega) = 0$ everywhere. Thus $\mathrm{div}(\omega) = 0$. □

We can show easily $\lambda(P) = 1$ for all P (see [GME] §2.2.3). Nonzero differentials ω in $\Omega_{E/k}$ are called *nowhere vanishing differentials* as $\mathrm{div}(\omega) = 0$. They are unique up to constant multiple.

Exercise 2.3. *Take a line L defined by $aX+bY+cZ$ on $\mathbf{P}^2$ and suppose its intersection with an elliptic curve $E \subset \mathbf{P}^2$ to be $\{P, Q, R\}$. Prove that $[P]+[Q]+[R] \sim 3[\mathbf{0}_E]$.*

A field k is called a *perfect* field if any finite field extension of k is separable (i.e., generated by θ over k whose minimal equation over k does not have multiple roots). Fields of characteristic 0 and finite fields are perfect.

Exercise 2.4. *Let C be an irreducible plane curve over a perfect field k. Let K be the integral closure of k in $k(C)$. Show*

1. *K/k is a finite field extension;*
2. *$K \otimes_k \overline{k} \cong \overbrace{\overline{k} \times \overline{k} \times \cdots \times \overline{k}}^{d}$ as k-algebras for $d = \dim_k K$;*
3. *C is geometrically irreducible if and only if $K = k$.*

Remark 2.5. If k is perfect, $\overline{k}/k$ is a Galois extension possibly infinite; so, by Galois theory, we have a bijection between open subgroups G of $\mathrm{Gal}(\overline{k}/k)$ and finite extensions K/k inside $\overline{k}$ by

$$G \mapsto \overline{k}^G = \{x \in \overline{k} | \sigma(x) = x \text{ for all } \sigma \in G\}$$

and $K \mapsto \mathrm{Gal}(\overline{k}/K)$. Since the isomorphism $E(\overline{k}) \cong \mathcal{J}(C)$ is Galois equivariant, we have

$$E(K) \cong \mathcal{J}(E)^{\mathrm{Gal}(\overline{k}/K)} = \{D \in \mathcal{J}(E) | \sigma(D) = D \text{ for all } \sigma \in G\},$$

where $\sigma \in \mathrm{Gal}(\overline{k}/k)$ acts on $D = \sum_P m_P[P]$ by $\sigma(D) = \sum_P m_P[\sigma(P)]$. Basically by definition, we have

$$\mathcal{J}(E)(K) := \mathcal{J}(E)^{\mathrm{Gal}(\overline{k}/K)} = \frac{\{D \in \mathrm{Pic}^0(E) | \sigma(D) = D\}}{\{\mathrm{div}(f) | f \in K(E)^\times\}}.$$

Since any subfield $K \subset \overline{k}$ is a union of finite extensions, the identity $E(K) \cong \mathcal{J}(E)(K)$ is also true for an infinite extension K/k inside $\overline{K}$. Actually we have a good definition of $\mathrm{Pic}(E)(A)$ for any k-algebra A, and we can generalize the identity $E(K) \cong \mathcal{J}(E)(K)$ to all k-algebras A in place of fields K inside $\overline{k}$ (see [GME] Theorem 2.2.1).

2.2. **Weierstrass equations of elliptic curves.** We now embed $E_{/k}$ into the two-dimensional projective space $\mathbf{P}^2_{/k}$ using a base of $L(3[\mathbf{0}])$ and determine the equation of the image in $\mathbf{P}^2_{/k}$. Choose a parameter $T = t_{\mathbf{0}}$ at the origin $\mathbf{0} = \mathbf{0}_E$. We first consider $L(n[\mathbf{0}])$ which has dimension n if $n > 0$. We have $L([\mathbf{0}]) = k$ and $L(2[\mathbf{0}]) = k1 + kx$. Since x has to have a pole of order 2 at $\mathbf{0}$, we may normalize x so that $x = T^{-2}(1 + \text{higher terms})$ in $k[[T]]$. Here x is unique up to translation: $x \mapsto x + a$ with $a \in k$. Then $L(3[\mathbf{0}]) = k1 + kx + ky$. We may then normalize y so that $y = -T^{-3}(1 + \text{higher terms})$. Following the tradition, we later rewrite y for $2y$; thus, the normalization will be $y = -2T^{-3}(1 + \text{higher terms})$ at the end. Then y is unique up to the affine transformation: $y \mapsto y + ax + b$ $(a, b \in k)$.

Proposition 2.6. *Suppose that the characteristic of the base field k is different from 2 and 3. Then for a given pair (E, ω) of an elliptic curve E and a nowhere-vanishing differential ω both defined over k, we can find a unique base $(1, x, y)$ of $L(3[\mathbf{0}])$ such that E is embedded into $\mathbf{P}^2_{/k}$ by $(1, x, y)$ whose image is defined by the affine equation*

$$y^2 = 4x^3 - g_2x - g_3 \quad \textit{with} \quad g_2, g_3 \in k, \tag{2.1}$$

and ω on the image is given by $\frac{dx}{y}$. Conversely, a projective algebraic curve defined by the above equation is an elliptic curve with a specific nowhere-vanishing differential $\frac{dx}{y}$ if and only if the discriminant $\Delta(E, \omega) = g_2^3 - 27g_3^2$ of $4X^3 - g_2X - g_3$ does not vanish.

The function $\Delta(E, \omega)$ is called the discriminant function and also *Ramanujan's Δ-function*. An equation of an elliptic curve E as in (2.1) is called a *Weierstrass equation* of E, which is determined by the pair (E, ω).

Proof. By the dimension formulas, counting the order of poles at $\mathbf{0}$ of monomials of x and y, we have

$$\begin{aligned} L(4[\mathbf{0}]) &= k + kx + ky + kx^2, \\ L(5[\mathbf{0}]) &= k + kx + ky + kx^2 + kxy \quad \text{and} \\ L(6[\mathbf{0}]) &= k + kx + ky + kx^2 + kxy + kx^3 \\ &= k + kx + ky + kx^2 + kxy + ky^2, \end{aligned}$$

from which the following relation results,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{with } a_j \in k, \tag{2.2}$$

because the poles of order 6 of y^2 and x^3 have to be canceled. We homogenize the equation (2.2) by putting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ (and multiplying by Z^3). Write C for the projective plane k-curve in $\mathbf{P}^2$ defined by the (homogenized) equation. Thus we have a k-regular map: $\phi : E \to C \subset \mathbf{P}^2$ given by $P \mapsto (x(P) : y(P) : 1)$. Thus the function field $k(E)$ contains the function field $k(C)$ by the pull back of ϕ. By definition, $k(C) = k(x, y)$. Since $\mathrm{div}_\infty(x) = 2[\mathbf{0}_E]$ for $x = \frac{X}{Z} : E \to \mathbf{P}^1$, this gives a covering of degree 2; so, $[k(E) : k(x)] = 2$. Similarly $[k(E) : k(y)] = 3$. Since $[k(E) : k(C)]$ is a common factor of $[k(E) : k(x)] = 2$ and $[k(E) : k(y)] = 3$, we get $k(E) = k(C)$. Thus if C is smooth, $E \cong C$ by ϕ as a smooth geometrically irreducible curve is determined by its function field. Therefore, assuming C is smooth, $E_{/k}$ can be embedded into $\mathbf{P}^2_{/k}$ via $P \mapsto (x(P), y(P))$. The image is defined by the equation (2.2).

Let T be a local parameter at $\mathbf{0}_E$ normalized so that

$$\omega = (1 + \text{higher degree terms})dT.$$

Anyway $\omega = (a + \text{higher degree terms})dT$ for $a \in k^\times$, and by replacing T by aT, we achieve this normalization. The parameter T normalized as above is called a parameter adapted to ω. Then we may normalize x so that $x = T^{-2} + \text{higher degree terms}$. We now suppose that 2 is invertible in k. Then we may further normalize y so that $y = -2T^{-3} + \text{higher degree terms}$ (which we will do soon but not yet; so, for the moment, we still assume $y = T^{-3} + \text{higher degree terms}$).

The above normalization is not affected by variable change of the form $y \mapsto y + ax + b$ and $x \mapsto x + a'$. Now we make a variable change $y \mapsto y + ax + b$ in order to remove the terms of xy and

y (i.e., we are going to make $a_1 = a_3 = 0$):

$$(y+ax+b)^2 + a_1x(y+ax+b) + a_3(y+ax+b) \\ = y^2 + (2a+a_1)xy + (2b+a_3)y + \text{polynomial in } x.$$

Assuming that 2 is invertible in k, we take $a = -\frac{a_1}{2}$ and $b = -\frac{a_3}{2}$. The resulting equation is of the form $y^2 = x^3 + b_2x^2 + b_4x + b_6$. We now make the change of variable $x \mapsto x + a'$ to make $b_2 = 0$:

$$y^2 = (x+a')^3 + b_2(x+a')^2 + b_4(x+a') + b_6 = x^3 + (3a'+b_2)x^2 + \cdots.$$

Assuming that 3 is invertible in k, we take $a' = -\frac{b_2}{3}$. We can rewrite the equation as in (2.1) (making a variable change $-2y \mapsto y$). By the variable change as above, we have $y = -2T^{-3}(1+\text{higher terms})$, and from this, we conclude $\omega = \frac{dx}{y}$. The numbers g_2 and g_3 are determined by T adapted to a given nowhere-vanishing differential form ω.

If the discriminant $\Delta(E,\omega)$ of $g(x) = 4x^3 - g_2x - g_3$ vanishes, C has only singularity at $(x_0 : 0 : 1)$ for a multiple root x_0 of $g(x) = 0$. If $g(x)$ has a double zero, C is isomorphic over $\overline{k}$ to the curve defined by $y^2 = x^2(x-a)$ for $a \neq 0$. Let $t = \frac{x}{y}$. Then for $P \in E(\overline{k})$ mapping to $(0,0)$, $v_P(y) = v_P(x)$; so, P is neither a zero nor a pole of t. The function t never vanish outside $\mathbf{0}_E$ (having a pole at $(a,0)$). It has a simple zero at $\mathbf{0}_E$ by the normalization of x and y. Thus $\deg(\mathrm{div}_0(t)) = 1$, and $\overline{k}(C) = \overline{k}(t)$, which is impossible as $k(C) = k(E)$ and $g(E) = 1$. The case of triple zero can be excluded similarly. Thus we conclude $\Delta(E,\omega) \neq 0$ ($\Leftrightarrow C$ is smooth: Example 1.15), and we have $E \cong C$ by ϕ.

Conversely, we have seen that any curve defined by equation (2.1) is smooth in Example 1.15 if the cubic polynomial $F(X) = 4X^3 - g_2X - g_3$ has three distinct roots in k. In other words, if the discriminant $\Delta(E,\omega)$ of $F(X)$ does not vanish, E is smooth.

For a given equation, $Y^2 = F(X)$, the algebraic curve E defined by the homogeneous equation $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ in $\mathbf{P}^2_{/k}$ has a rational point $\mathbf{0} = (0,1,0) \in E(k)$, which is ∞ in $\mathbf{P}^2$. Thus E is smooth over k if and only if $\Delta(E,\omega) \neq 0$ (an exercise following this proof).

We show that there is a canonical nowhere-vanishing differential $\omega \in \Omega_{E/k}$ if E is defined by (2.1). If such an ω exists, all other holomorphic differentials ω' are of the form $f\omega$ with $\mathrm{div}(f) \geq 0$, which implies $f \in k$; so, $g = \dim_k \Omega_{E/k} = 1$, and $E_{/k}$ is an elliptic curve. It is an easy exercise to show that $y^{-1}dx$ does not vanish on E (an exercise following this proof).

We summarize what we have seen. Returning to the starting elliptic curve $E_{/k}$, for the parameter T at the origin, we see by definition

$$x = T^{-2}(1 + \text{higher degree terms}) \quad \text{and} \quad y = -2T^{-3}(1 + \text{higher degree terms}).$$

This shows

$$\frac{dx}{y} = \frac{-2T^{-3}(1+\cdots)}{-2T^{-3}(1+\cdots)}dT = (1 + \text{higher degree terms})dT = \omega.$$

Thus the nowhere-vanishing differential form ω to which T is adapted is given by $\frac{dx}{y}$. Conversely, if $\Delta \neq 0$, the curve defined by $y^2 = 4x^3 - g_2x - g_3$ is an elliptic curve over k with origin $\mathbf{0} = \infty$ and a standard nowhere-vanishing differential form $\omega = \frac{dx}{y}$. This finishes the proof. □

Exercise 2.7. (1) *If C is defined by $y^2 = x^3$, prove $k(C) = k(t)$ for $t = \frac{x}{y}$.*

(2) *Compute $v_P(dx/y)$ explicitly at any point P on $E(\overline{k})$.*

(3) *Show that if $\Delta \neq 0$, the curve defined by $y^2 = 4x^3 - g_2x - g_3$ (over a field k of characteristic $\neq 2, 3$) is also smooth at $\mathbf{0} = \infty$.*

2.3. **Moduli of Weierstrass type.** We continue to assume that the characteristic of k is different from 2 and 3. Suppose that we are given two elliptic curves $(E,\omega)_{/k}$ and $(E',\omega')_{/k}$ with nowhere-vanishing differential forms ω and ω'. We call two pairs (E,ω) and (E',ω') isomorphic if we have an isomorphism $\varphi : E \to E'$ with $\varphi^*\omega' = \omega$. Here for $\omega' = fdg$, $\varphi^*\omega' = (f \circ \varphi)d(g \circ \varphi)$; in other words, if $\sigma : k(E') \to k(E)$ is the isomorphism of the function fields associated with φ, $\varphi^*\omega' = \sigma(f)d(\sigma(g))$. Let T' be the parameter at the origin $\mathbf{0}$ of E' adapted to ω'. If $\varphi : (E,\omega) \cong (E',\omega')$, then the parameter $T = \varphi^*T' \bmod T^2$ is adapted to ω (because $\varphi^*\omega' = \omega$). We choose coordinates (x,y) for E and (x',y') for E' relative to T and T' as above. By the uniqueness of the choice of (x,y)

and (x', y'), we know $\varphi^* x' = x$ and $\varphi^* y' = y$. Thus the Weierstrass equations of (E, ω) and (E', ω') coincide. We write $g_2(E, \omega)$ and $g_3(E, \omega)$ for the g_2 and g_3 of the coefficients of the Weierstrass equation of (E, ω). If a field K has characteristic different from 2 and 3, we have

$$\big[(E,\omega)_{/K}\big] \cong \big\{(g_2, g_3) \in K^2 \big| \Delta(E,\omega) \neq 0\big\} \cong \mathrm{Hom}_{ALG}(\mathbb{Z}[\frac{1}{6}, X, Y, \frac{1}{X^3 - 27Y^2}], K),$$

where $[\cdot]$ indicates the set of isomorphism classes of the objects inside the bracket and $\mathrm{Spec}(R)(K)$ for a ring R is the set of all algebra homomorphisms: $R \to K$. The last isomorphism sends (g_2, g_3) to the algebra homomorphism ϕ with $\phi(X) = g_2$ and $\phi(Y) = g_3$. We will see later this identity is actually valid any algebra A in $ALG_{/\mathbb{Z}[\frac{1}{6}]}$ in place of a field K.

Exercise 2.8. *If k has characteristic 2, show that we cannot have any ring $\mathcal{R}$ such that*

$$\big[(E,\omega)_{/K}\big] \cong \mathrm{Hom}_{ALG}(\mathcal{R}, K)$$

for all field extension K/k. Here the isomrophism is a natural transformation bewteen the functors $K \mapsto [(E,\omega)_{/K}]$ and $K \mapsto \mathrm{Hom}_{ALG}(\mathcal{R}, K)$ from the category of fields into SETS.

We now classify elliptic curves E eliminating the contribution of the differential from the pair (E, ω). If $\varphi : E \cong E'$ for (E, ω) and (E', ω'), we have $\varphi^* \omega' = \lambda\omega$ with $\lambda \in K^\times$, because $\varphi^*\omega'$ is another nowhere-vanishing differential. Therefore we study $K^\times$-orbit: $(E, \omega) \mod K^\times$ under the action of $\lambda \in K^\times$ given by $(E,\omega)_{/K} \longmapsto (E, \lambda\omega)_{/K}$, computing the dependence of $g_j(E, \lambda\omega)$ $(j = 2, 3)$ on λ for a given pair $(E, \omega)_{/K}$. Let T be the parameter adapted to ω. Then λT is adapted to $\lambda\omega$. We see

$$x(E,\omega) = \frac{(1 + T\phi(T))}{T^2} \Rightarrow x(E, \lambda\omega) = \frac{(1 + \text{higher terms})}{(\lambda T)^2} = \lambda^{-2} x(E, \omega),$$
$$y(E,\omega) = \frac{(-2 + T\psi(T))}{T^3} \Rightarrow y(E, \lambda\omega) = \frac{(-2 + \text{higher terms})}{(\lambda T)^3} = \lambda^{-3} y(E, \omega).$$

Since $y^2 = 4x^3 - g_2(E,\omega)x - g_3(E,\omega)$, we have

$$\begin{aligned}(\lambda^{-3}y)^2 &= 4\lambda^{-6}x^3 - g_2(E,\omega)\lambda^{-6}x - \lambda^{-6}g_3(E,\omega)\\ &= 4(\lambda^{-2}x)^3 - \lambda^{-4}g_2(E,\omega)(\lambda^{-2}x) - \lambda^{-6}g_3(E,\omega),\end{aligned}$$

$$g_2(E, \lambda\omega) = \lambda^{-4} g_2(E,\omega) \quad \text{and} \quad g_3(E, \lambda\omega) = \lambda^{-6} g_3(E,\omega). \tag{2.3}$$

Thus we have

Theorem 2.9. *If two elliptic curves $E_{/K}$ and $E'_{/K}$ are isomorphic, then choosing nowhere-vanishing differentials $\omega_{/E}$ and $\omega'_{/E'}$, we have $g_j(E', \omega') = \lambda^{-2j} g_j(E, \omega)$ for $\lambda \in K^\times$. The constant λ is given by $\varphi^*\omega' = \lambda\omega$.*

We define the J-invariant of E by $J(E) = \frac{(12 g_2(E,\omega))^3}{\Delta(E,\omega)}$. Then J only depends on E (not the chosen differential ω). If $J(E) = J(E')$, then we have

$$\frac{(12 g_2(E,\omega))^3}{\Delta(E,\omega)} = \frac{(12 g_2(E',\omega'))^3}{\Delta(E',\omega')} \iff g_j(E',\omega') = \lambda^{-2j} g_j(E,\omega)$$

for a twelfth root λ of $\Delta(E,\omega)/\Delta(E',\omega')$. Note that the twelfth root λ may not be in K if K is not algebraically closed.

Conversely, for a given $j \notin \{0, 1\}$, the elliptic curve defined by $y^2 = 4x^3 - gx - g$ for $g = \frac{27j}{j-1}$ has J-invariant $12^3 j$. If $j = 0$ or 1, we can take the following elliptic curve with $J = 0$ or 12^3. If $J = 0$, then $y^2 = 4x^3 - 1$ and if $J = 12^3$, then $y^2 = 4x^3 - 4x$ (Gauss' lemniscate). Thus we have

Corollary 2.10. *If K is algebraically closed, then $J(E) = J(E') \Leftrightarrow E \cong E'$ for two elliptic curves over K. Moreover, for any field K, there exists an elliptic curve E with a given $J(E) \in K$.*

Exercise 2.11.
(1) *Prove that $g_j(E', \omega') = \lambda^{-2j} g_j(E, \omega)$ for suitable ω and ω' and a suitable twelfth root λ of $\Delta(E,\omega)/\Delta(E',\omega')$ if $J(E) = J(E')$.*
(2) *Explain what happens if $J(E) = J(E')$ but $E \ncong E'$ over a field K not necessarily algebraically closed.*

3. Modular Forms

We give an algebraic definition of modular forms and then relate it to classical defintions.

3.1. **Elliptic curves over general rings.** What we have done over fields can be also done over general noetherian rings A. We sketch the theory without much proof. Here is a definition of a plain projective curve over a ring A as a subfunctor $C \subset \mathbf{P}^2$. Recall $L \in \mathbf{P}^2(R)$ for an A-algebra R is a locally free R-submodule of R^3 of rank 1 with locally free quotient R^3/L. For a given homogeneous plynomial $\Phi(X,Y,Z) \in A[X,Y,Z]$, we define $\Phi(L) = 0$ if $\Phi(\ell) = 0$ for all $\ell \in L$. Assume that $F(X,Y,Z)$ is not a zero-divisor in $A[X,Y,Z]$. Then a homogeneous polynomial $F(X,Y,Z) \in A[X,Y,Z]$ defines a subfunctor (called a plane projective A-curve) by

$$R \mapsto C(R) = \{L \in \mathbf{P}^2(R) | \Phi(L) = 0\}.$$

Plainly C is a covariant subfunctor of $\mathbf{P}^2$. If the residue ring $\frac{A[X,Y,Z]}{(F(X,Y,Z))}$ modulo its nilradical is an integral domain, we call C *irreducible*.

Exercise 3.1. *If A is a field k, verify that this definition is equivalent to the definition of irreducibility of the plane k-curve already given earlier.*

We define

$$\mathrm{Hom}_{A\text{-curves}}(C, C') := \mathrm{Hom}_{COF}(C, C'),$$

and in this way, we get the category of plane projective A-curves. Fix such a curve $C \subset \mathbf{P}^2_{/A}$. First suppose that A is a local ring with maximal ideal $\mathfrak{m}$. Write k for $A/\mathfrak{m}$. We then define

$$R_0 = \frac{A[Y,Z]}{(F(1,Y,Z))},\ R_1 = \frac{A[X,Z]}{(F(X,1,Z))},\ R_2 = \frac{A[X,Y]}{(F(X,Y,1))}.$$

Consider a covariant functor $C_i : R \mapsto \mathrm{Hom}_{ALG_{/A}}(R_j, R)$ from $ALG_{/A}$ to $SETS$. This functor can be identified with a subfunctor of C, for example, by

$$C_2(R) \ni \phi \mapsto L = R \cdot (\phi(X), \phi(Y), 1) \in C(R),$$

and C_2 can be identified with the functor sending R to the zero set of $F(X,Y,1)$ in R^2. If R is a local ring, we know $C(R) = C_0(R) \cup C_1(R) \cup C_2(R)$. For any finite field extension K of k, a point $P \in C_i(K)$ gives rise to an A-algebra homomorphism $\phi : R_i \to K$; so, $\mathrm{Ker}(\phi)$ is a maximal ideal of R_i.

Exercise 3.2. *Under the above setting, prove*

1. $\mathrm{Ker}(\phi)$ *is a maximal ideal of R_i if K/k is a finite field extension,*
2. *any maximal ideal of R_i is given in this way as* $\mathrm{Ker}(\phi)$.

The point $P \in C(\overline{k})$ is called a *maximal point* of C. We define

$$\mathcal{O}_{C,P} = \{\frac{a}{b} | b \in R_i \setminus \mathrm{Ker}(\phi)\}/\approx .$$

Again $\mathcal{O}_{C,P}$ is determined independent of the choice of i with $P \in C_i(K)$. Then $\mathcal{O}_{C,P}$ is a local ring with maximal ideal $\mathfrak{m}_P$ with $\mathcal{O}_{C,P}/\mathfrak{m}_P \cong \mathrm{Im}(\phi) \subset K$. The cotangent space at P is defined by P/P^2 and the tangent space at P over K is by definition its dual $\mathrm{Hom}_K(P/P^2, K)$. As before, the tangent space is isomorphic to the space of K-derivations $\partial : \mathcal{O}_{C,P} \to K$.

We are going to sketch a general definition of smoothness, but before starting this subtle process of defining smoothness over a ring, we point out that, general definition aside, an important point is that we can again prove that an elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$ is smooth over $A = \mathbb{Z}[\frac{1}{6}, g_2, g_3]$ if and only if $\Delta \in A^\times$. If the reader is not very familiar with the notion of smoothness/étaleness over rings, he or she can just admit this fact for a while to go through this section and the next (as he/she will understand details once scheme theory is learned).

Here is a formal definition of smoothness/étaleness. For an A–algebra R and R', we define the R'-module of derivations $Der_A(R, R')$ just by the R'-module of derivations trivial over A (so, $(\partial : R \to R') \in Der_A(R, R')$ satisfies $\partial(\varphi\phi) = \varphi\partial(\phi) + \phi\partial(\varphi)$ and $\partial(a) = 0$ for all $a \in A$).

Consider $\mathfrak{m}$-adic *completions*

$$\widehat{A} = \varprojlim_n A/\mathfrak{m}^n \text{ and } \widehat{\mathcal{O}}_{C,P} = \varprojlim_n \mathcal{O}_{C,P}/\mathfrak{m}_P^n.$$

Then $\widehat{\mathcal{O}}_{C,P}$ is naturally an algebra over $\widehat{A}$. Write $\widehat{\mathfrak{m}}_P$ for the maximal ideal of $\widehat{\mathcal{O}}_{C,P}$. We call $P \in C(K)$ *smooth* over A if $\widehat{\mathcal{O}}_{C,P}$ is free of finite positive rank over $\widehat{A}[[T]]$ (i.e., $\widehat{\mathcal{O}}_{C,P} \cong \widehat{A}[[T]]^r$ for $0 < r \in \mathbb{Z}$) for a variable $T \in \widehat{\mathcal{O}}_{C,P}$ and any derivation of $\widehat{A}[[T]]$ over $\widehat{A}$ with values in any artinian $\widehat{\mathcal{O}}_{C,P}$-algebra extends uniquely to $\widehat{\mathcal{O}}_{C,P}$; i.e., the ring theoretic tangent spaces of $\widehat{\mathcal{O}}_{C,P}$ and $\widehat{A}[[T]]$ are equal. This last point means that $\Omega_{\widehat{\mathcal{O}}_{C,P}/\widehat{A}[[T]]} = 0$ (see [GME] §1.9.2 for differentials). In short, $\widehat{\mathcal{O}}_{C,P}$ is an étale algebra over $\widehat{A}[[T]]$; i.e., $\mathrm{Spec}(\widehat{\mathcal{O}}_{C,P})$ and $\mathrm{Spec}(\widehat{A}[[T]])$ are locally isomorphic in the sense of algebraic geometry).

If C is smooth over A at all maximal points $P \in C(K)$, we call C *smooth* over A. Assuming that k is algebraically closed, C is smooth over A if and only if $\widehat{\mathcal{O}}_{C,P} \cong \widehat{A}[[T]]$ as $\widehat{A}$-algebras for all maximal points $P \in C$.

For general A not necessarily local, we call C *smooth* over A if C is smooth over the localization of A at every maximal ideal of A.

Exercise 3.3. *Prove that if C is a smooth plane projective curve over an integral local domain A with algebraically closed residue field, C is smooth over the quotient field of A, regarding C a plane projective curve over the quotient field.*

Suppose C is smooth over A. We can define the R_i-module of derivations $Der_{C_i/A} = Der_A(R_i, R_i)$ just by the R_i-module of derivations trivial over A (so, $(\partial : R_i \to R_i) \in Der_{C_i/A}$ satisfies $\partial(\varphi\phi) = \varphi\partial(\phi) + \phi\partial(\varphi)$ and $\partial(a) = 0$ for all $a \in A$). The R_i-dual $\Omega_{C_i/A}$ of $Der_{C_i/A}$ is called the R_i-module of 1-differentials over C_i. Each $\partial \in Der_{C_i/A}$ gives rise to an A_P-derivation $\partial_P : \mathcal{O}_{C,P} \to \mathcal{O}_{C,P}$ given by $\partial_P(\frac{a}{b}) = \frac{\partial(a)b - a\partial(b)}{b^2}$ for a maximal point $P \in C_i$, where A_P is the localization of A at $P \cap A$ (regarding P as a prime ideal of R_i). By duality, $\omega \in \Omega_{C_i/A}$ therefore gives rise to the cotangent vector $\omega_P \in \Omega_{\mathcal{O}_{C,P}/A_P} := \mathrm{Hom}_{A_P}(Der_{\mathcal{O}_{C,P}/A_P}, \mathcal{O}_{C,P})$. The R_i-module $\Omega_{C_i/A}$ is a locally-free R_i-module of rank 1. Then we define $\Omega_{C/A}$ to be the collection of all $\omega = (\omega_i \in \Omega_{C_i/A})_i$ such that $\omega_{i,P} = \omega_{j,P}$ for all $P \in (C_i \cap C_j)(\overline{k})$ $((i,j) = (0,1), (1,2), (0,2))$. If C is smooth over A, again $\Omega_{C/A}$ is a locally free A-module of some rank g, and this number g is called the genus $g(C)$ of C over A.

An elliptic curve over A is a plane projective smooth curve E of genus 1 with a specific point $\mathbf{0}_E \in E(A)$. If $\Omega_{E/A} = A\omega$, the differential ω is called a *nowhere vanishing differential*. If $\phi : E \to E'$ is a morphism of elliptic curve, we can pull back a nowhere vanishing differential ω' on E' by ϕ, which is written as $\phi^*\omega'$. Note here that $\phi^*\omega'$ may not be nowhere vanishing (though it is, if ϕ is an isomorphism).

Exercise 3.4. *Let $A = \mathbb{F}_p$. Give an example of a non-constant morphism $\phi : E \to E$ such that $\phi^*\omega = 0$ for a nowhere vanishing differential ω on E.*

If $A \xrightarrow{\sigma} A'$ is an algebra homomorphism and if a plane projective A-curve C is defined by an equation $F(X,Y,Z) = \sum_{i,j,l} c_{i,j,l} X^i Y^j Z^l$, the σ-transform $\sigma(F)(X,Y,Z) = \sum_{i,j,l} \sigma(c_{i,j,l}) X^i Y^j Z^l$ defines a plane projective A'-curve $\sigma(C)$. Note that $\sigma(C_i)$ is defined by the ring $R_i \otimes_{A,\sigma} A'$; so, often we write $C \otimes_A A'$ for $\sigma(C)$ and call it the base-change $C \otimes_A A'_{/A'}$ of $C_{/A}$. Similarly, if $\partial : R_i \to R_i$ is an A-derivation, $\partial \otimes 1 : R_i \otimes_A A' \to R_i \otimes_A A'$ given by $\partial \otimes 1(\phi \otimes a) = \sigma(a\partial(\phi))$ is an A'-derivation. This shows $Der_{C_i/A} \otimes_A A' = Der_{C_i \otimes A'/A'}$. Thus by duality, we also have $\Omega_{C_i/A} \otimes_A A' = \Omega_{C_i \otimes A'/A'}$. In particular, $\omega \in \Omega_{C/A}$ induces $\sigma_*(\omega) = \omega \otimes 1 \in \Omega_{C \otimes A'/A'}$. We write the pair $(E \otimes_A A', \sigma_*\omega)$ as $(E,\omega) \otimes_A A'$. This makes $\mathcal{P} : ALG \to SETS$ given by $\mathcal{P}(A) = \left[(E,\omega)_{/A}\right]$ a covariant functor from the category of algebras into sets. We again have the following result basically in the same way as in the case of fields (see [GME] §2.2.6 for a proof):

Theorem 3.5. *Let $\mathcal{R} = \mathbb{Z}[\frac{1}{6}, g_2, g_3, \frac{1}{\Delta}]$. Then we have a canonical equivalence of functors from $ALG_{/\mathbb{Z}[\frac{1}{6}]}$ to SETS: $\mathcal{P}(?) \cong \mathrm{Hom}_{ALG_{/\mathbb{Z}[\frac{1}{6}]}}(\mathcal{R}, ?)$.*

In other word, for a given pair $(E,\omega)_{/A}$ of an elliptic curve E over A and a nowhere vanishing differential ω, there exists unique $(g_2(E,\omega), g_3(E,\omega)) \in A^2$ such that E is canonically isomorphic to

an elliptic curve defined by

$$Y^2Z = 4X^3 - g_2(E,\omega)XZ^2 - g_3(E,\omega)Z^3$$

and ω induces the differential $\frac{dX}{Y}$ on $E_2 = E \cap D_2$ under this isomorphism. Thus we have

(1) If (E,ω) is defined over a $\mathbb{Z}[\frac{1}{6}]$-algebra A, we have $g_j(E,\omega) \in A$, which depends only on the isomorphism class of (E,ω) over A,
(2) $g_j((E,\omega) \otimes_A A') = \sigma(g_j(E,\omega))$ for each $\mathbb{Z}[\frac{1}{6}]$-algebra homomorphism $\sigma : A \to A'$,
(3) $g_j(E,\lambda\omega) = \lambda^{-2j} g_j(E,\omega)$ for all $\lambda \in A^\times$.

3.2. **Geometric modular forms.** Let A be an algebra over $\mathbb{Z}[\frac{1}{6}]$. We restrict the functor $\mathcal{P}$ to $ALG_{/A}$ and write the restriction $\mathcal{P}_{/A}$. Then by Theorem 3.5, for $\mathcal{R}_A := A[g_2, g_3, \frac{1}{\Delta}]$,

$$\mathcal{P}_{/A}(?) = \mathrm{Hom}_{ALG_{/A}}(\mathcal{R}_A, ?).$$

A morphism of functors $\phi : \mathcal{P}_{/A} \to \mathbf{A}^1_{/A}$ is given by maps $\phi_R : \mathcal{P}_{/A}(R) \to \mathbf{A}^1(R) = R$ indexed by $R \in ALG_{/A}$ such that for any $\sigma : R \to R'$ in $\mathrm{Hom}_{ALG_{/A}}(R, R')$, $\phi_{R'}((E,\omega)\otimes_R R') = \sigma(f((E,\omega)_{/R}))$. Note that $\mathbf{A}^1_{/A}(?) = \mathrm{Hom}_{ALG_{/A}}(A[X], ?)$ by $R \ni a \leftrightarrow (\varphi : A[X] \to R) \in \mathrm{Hom}_{ALG_{/A}}(A[X], ?)$ with $\varphi(X) = a$. In particular,

$$\phi_{\mathcal{R}_A} : \mathcal{P}(\mathcal{R}_A) = \mathrm{Hom}_{ALG_{/A}}(\mathcal{R}_A, \mathcal{R}_A) \to \mathbf{A}^1(A[X], \mathcal{R}_A) = \mathcal{R}_A.$$

Thus $\phi_{\mathcal{R}_A}(\mathrm{id}_{\mathcal{R}_A}) \in \mathcal{R}_A$; so, write $\phi_{\mathcal{R}_A}(\mathrm{id}_{\mathcal{R}_A}) = \Phi(g_2, g_3)$ for a two variable rational function $\Phi(x,y) \in A[x, y, \frac{1}{x^3 - 27y^2}]$. Let $\mathbf{E}_{/\mathcal{R}_A}$ be the universal elliptic curve over $\mathcal{R}_A$ defined by $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ with the universal differential $\boldsymbol{\omega} = \frac{dX}{Y}$. If we have $(E,\omega)_{/R}$, we have a unique A-algebra homomorphism $\sigma : \mathcal{R}_A \to R$ given by $\sigma(g_j) = g_j(E,\omega)$; in other words, $(E,\omega)_{/R} \cong (\mathbf{E},\omega)_{\mathcal{R}_A} \otimes_{\mathcal{R}_A} R$, and

$$\begin{aligned}\phi_R(E,\omega) = \phi_R((\mathbf{E},\omega) \otimes_{\mathcal{R}_A} R) &= \sigma(\phi_{\mathcal{R}_A}(\mathbf{E},\omega)) \\ &= \sigma(\phi_{\mathcal{R}_A}(\mathrm{id}_{\mathcal{R}_A})) = \Phi(\sigma(g_2), \sigma(g_3)) = \Phi(g_2(E,\omega), g_3(E,\omega)).\end{aligned}$$

Theorem 3.6. *Any functor morphism $\phi : \mathcal{P}_{/A} \to \mathbf{A}^1_{/A}$ is given by a rational function $\Phi \in \mathcal{R}_A$ of g_2 and g_3 so that $\phi(E,\omega) = \Phi(g_2(E,\omega), g_2(E,\omega))$ for every elliptic curve (E,ω) over an A-algebra.*

Define a weight function $w : A[g_2, g_3] \to \mathbb{Z}$ by $w(g_2^a g_3^b) = 4a + 6b$, and for general polynomials $\Phi = \sum_{a,b} c_{a,b} g_2^a g_3^b$, we put $w(\Phi) = \max(w(g_2^a g_3^b) | c_{a,b} \neq 0)$. A polynomial $\Phi = \sum_{a,b \geq 0} c_{a,b} g_2^a g_3^b$ of g_2 and g_3 is called *isobaric* if $c_{a,b} \neq 0 \Rightarrow 4a + 6b = w$.

A weight w modular form defined over A is a morphism of functors $\mathcal{P}_{/A} \to \mathbf{A}^1_{/A}$ given by an isobaric polynomial of g_2 and g_3 of weight w with coefficients in A. Write $G_w(A) = G_w(\Gamma_0(1); A)$ for the A-module of modular forms of weight w. Then $f \in G_w(A)$ is a functorial rule assigning each isomorphism class of $(E,\omega)_{/R}$ for an A-algebra R an element $f(E,\omega) \in R$ satisfying the following properties:

(G0) $f \in A[g_2, g_3]$,
(G1) If (E,ω) is defined over an A-algebra R, we have $f(E,\omega) \in R$, which depends only on the isomorphism class of (E,ω) over R,
(G2) $f((E,\omega) \otimes_R R') = \sigma(f(E,\omega))$ for each A-algebra homomorphism $\sigma : R \to R'$,
(G3) $f((E,\lambda\omega)_{/R}) = \lambda^{-w} f(E,\omega)$ for any $\lambda \in R^\times$.

Exercise 3.7. *For a field K with $\frac{1}{6} \in K$, prove, for $0 < w \in 2\mathbb{Z}$,*

$$\dim_K G_w(K) = \begin{cases} \left[\frac{w}{12}\right] & \text{if } w \equiv 2 \mod 12, \\ \left[\frac{w}{12}\right] + 1 & \text{otherwise.} \end{cases}$$

4. Functorial Algebraic Geometry

We recall here briefly definitions and results in functorial algebraic geometry as succinct as possible in a style suitable to deal with jacobian and abelian varieties (cf. [RAG] I.1). In order to make our exposition short and to reach fast to the core of the theory necessary to our later treatment, we define schemes as covariant functors outright, and in this sense our exposition is unconventional. Since the spectrum $\mathrm{Spec}(A)$ over the base ring B (or equivalently, over the base scheme $\mathrm{Spec}(B)$) is traditionally first defined as a local ringed space made up of prime ideals of A with Zariski topology, we write S_A for the associated covariant functor defined on the category of B-algebras $R \mapsto S_A(B) = \mathrm{Hom}_{B\text{-alg}}(A, R)$ only in this section (later we write this functor as $R \mapsto \mathrm{Spec}_B(A)(R)$, identifying the functor and the scheme). All rings R we consider are commutative, have the identity element 1_R, and we denote by 0_R the zero element of R.

4.1. **Affine variety.** Let k be an algebraically closed field. A Zariski closed subset V in k^n is defined by the zero set of finitely many polynomials $f_1, \ldots, f_m \in k[X] = k[X_1, \ldots, X_n]$; so, $V = \{(x = (x_1, \ldots, x_n) \in k^n | f_j(x) = 0 \ (j = 1, \ldots, m)\}$. The polynomials $f_1, \ldots, f_m$ generates an ideal $I = \sum_{j=1}^m k[X] f_j \subset k[X]$, and plainly,

$$V = V(I) = \{x \in k^n | f(x) = 0 \ \forall f \in I\}.$$

Thus we write this closed set as $V = V(I)$ for the ideal I. Since $k[X]$ is noetherian, an ideal I is generated by finitely many elements; hence, any Zariski closed subset has the form $V(I)$ with an ideal I.

Easy to verify $V(k[X]) = \emptyset$, $V((0)) = k^n$, $V(I \cap J) = V(I) \cup V(J)$ and $V(\sum_{i\in I} I_i) = \bigcap_{i\in I} V(I_i)$. Thus the family of subsets of the form $V(I)$ for ideals I satisfies the axiom of closed subsets of k^n giving the Zariski topology on k^n. By Hilbert's zero theorem (cf. [CRT] Section 5), $V(I) = V(\sqrt{I})$ for the radical $\sqrt{I} = \{f \in k[X] | f^n \in I\}$. Thus the association

$$\{\text{ideals of } k[X]\} \to \{\text{Zariski closed subsets of } k[X]\}$$

given by $I \mapsto V(I)$ is surjective but not injective.

For any k-algebra R, define

$$\mathcal{V}_I(R) = \{x = (x_1, \ldots, x_n) \in R^n | f(x) = 0 \ \forall f \in I\}.$$

Then $R \mapsto \mathcal{V}_I(R)$ is a covariant functor from the category of k-algebras into sets (see the following section for the definition of functors), as any k-algebra homomorphism $\phi \in \mathrm{Hom}_{k\text{-alg}}(R, R')$ induces a map $\mathcal{V}_I(\phi) : \mathcal{V}_I(R) \to \mathcal{V}_I(R')$ given by $(x_1, \ldots, x_n) \mapsto (\phi(x_1), \ldots, \phi(x_n))$, which satisfies $\mathcal{V}_I(\phi' \circ \phi) = \mathcal{V}_I(\phi') \circ \mathcal{V}_I(\phi)$. If $\alpha \in \mathcal{V}_I(R)$, we have a k-algebra homomorphism $\phi_\alpha : k[X] \to R$ given by $\phi_\alpha(f(X)) = f(\alpha)$ for $f(X) \in k[X] = k[X_1, \ldots, X_n]$. Since $f(\alpha) = 0$ for all $f \in I$, ϕ_α factors through $k[X]/I$. Thus we get a map $\phi_R : \mathcal{V}_I(R) \to \mathrm{Hom}_{k\text{-alg}}(k[X]/I, R)$ sending $\alpha \in \mathcal{V}_I(R)$ to ϕ_α. For any given $\varphi \in \mathrm{Hom}_{k\text{-alg}}(k[X]/I, R)$, it is plain that $\varphi_R = \phi_\alpha$ for $\alpha = (\varphi(X_1), \ldots, \varphi(X_n))$. Thus

$$\phi : \mathcal{V}_I(?) \to \mathrm{Hom}_{k\text{-alg}}(k[X]/I, ?) \text{ is an isomorphism of functors.} \tag{4.1}$$

Even if $V(I) = V(\sqrt{I})$, it is obvious that $\mathcal{V}_I \neq \mathcal{V}_{\sqrt{I}}$ as functors as easily checked

$$\mathrm{Hom}_{k\text{-alg}}(k[X]/\sqrt{I}, k[X]/I) \neq \mathrm{Hom}_{k\text{-alg}}(k[X]/I, k[X]/I)$$

if $I \neq \sqrt{I}$. We call the functor $\mathcal{V}_{\sqrt{I}}$ an affine variety, which is a reduced affine k-scheme (a general definition of k-schemes will be given in a following section).

If $W \subset k^r$ is another Zariski closed subset defined by an ideal $J \subset k[Y] = k[Y_1, \ldots, Y_r]$. A map $\varphi : V \to W$ is a regular map if there exists a set of polynomials $\varphi_1, \ldots, \varphi_r$ in $k[X]$ such that $\varphi(x) = (\varphi_1(x), \ldots, \varphi_r(x)) \in k^r$ for all $x \in V$. This induces a morphism of functors $\mathcal{V}_I \to \mathcal{V}_J$ given by $\varphi_R : \mathcal{V}_I(R) \to \mathcal{V}_J(R)$ with $\varphi_R(x) = (\varphi_1(x), \ldots, \varphi_r(x))$ for all $x \in \mathcal{V}_I(R) \subset R^n$. The set of polynomials $\varphi = (\varphi_1, \ldots, \varphi_r)$ gives rise to a k-algebra homomorphism $\underline{\varphi} : k[Y] \to k[X]$ given by $\underline{\varphi}(Y_j) = \varphi_j(X)$. It induces therefore a k-algebra homomorphism $\underline{\varphi} : k[Y] \to k[X]/I$ by composing the projection $k[X] \twoheadrightarrow k[X]/I$. If $f(Y) \in J$, then $\underline{\varphi}(f(Y)) = f(\varphi_1(X), \ldots, \varphi_r(X)) \mod I$. Since $\varphi(x) = (\varphi_1(x), \ldots, \varphi_r(x)) \in W$ for all $x \in V$, we get $\underline{\varphi}(f(Y))(x) = 0$; so, by Hilbert's zero theorem,

$\underline{\varphi}(f(Y)) \in \sqrt{I}$. Thus φ induces $\underline{\varphi} : k[Y]/\sqrt{J} \to k[X]/\sqrt{I}$. In particular, if $\sqrt{I} = I$ and $\sqrt{J} = J$, we get

$$\mathrm{Hom}_{\mathrm{functor}}(\mathcal{V}_I, \mathcal{V}_J) \ni \varphi \mapsto \underline{\varphi} \in \mathrm{Hom}_{k\text{-alg}}(k[Y]/J, k[X]/I).$$

As we will see in (4.5), this is an isomorphism. Thus basically, knowing the affine variety $\mathcal{V}_I$ is equivalent to knowing the algebra $k[X]/I$ (cf. Yoneda's lemma, see Lemma 4.16).

4.2. **Categories.** We give a brief outline of the definition of categories and examples. A category $\mathcal{C}$ consists of two data: objects of $\mathcal{C}$ and morphisms of $\mathcal{C}$. For any two objects X and Y of $\mathcal{C}$, we have a set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ of morphisms satisfying the following three rules:

(Ct1) *For three objects X, Y, Z, there is a composition map:*

$$\mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z) : (g, f) \mapsto g \circ f;$$

(Ct2) *(Associativity). For three morphisms: $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$, we have $h \circ (g \circ f) = (h \circ g) \circ f$;*

(Ct3) *For each object X, there is a specific element $1_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ such that $1_X \circ f = f$ and $g \circ 1_X = g$ for all $f : Y \to X$ and $g : X \to Z$.*

For two objects X and Y in $\mathcal{C}$, we write $X \cong Y$ if there exist morphisms $f : X \to Y$ and $g : Y \to X$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$. Often $\mathcal{C}$ is a subcategory of $SETS$, and in that case, 1_X is usually given by the identity map id_X; so, in such a case, we write id_X for 1_X.

Example 4.1. A list of examples of categories: In the table below, X denotes a given topological space (it is often the underlying toplogical space of a scheme). See [GME] Chapter 1 a brief outline of tradtional theory of schemes and its language (see [EGA] for real details). We will recall functorial definition of scheme in a couple of sections ahead.

Category	*Objects*	*Morphisms*
$SETS$	*sets*	*maps between sets*
AB	*Abelian groups*	*group homomorphisms*
ALG	*Algebras*	*Algebra homomorphisms*
$ALG_{/B}$	*B-algebras*	*B-algebra homomorphisms*
$\widehat{ALG}_{/B}$	*complete B-algebras*	*continuous B-algebra homomorphisms*
$O(X)$	*open subsets in X*	*inclusions*
$PS(X)$	*presheaves on X*	*morphisms of presheaves*
$S(X)$	*sheaves on X*	*morphisms of presheaves*
$QS(X)$	*quasi coherent sheaves*	*morphisms of presheaves*
$SCH_{/S}$	*S-Schemes*	*morphisms of local ringed spaces$_{/S}$*
$GSCH_{/S}$	*group S-Schemes*	*group morphisms of $SCH_{/S}$*
$BT_{/S}$	*Barsotti–Tate groups$_{/S}$*	*morphisms of $GSCH_{/S}$*
$ELL_{/SCH}$	*elliptic curves $E_{/S}$*	*morphisms of $GSCH_{/S}$*
$MOD_{/B}$	*B-modules*	*B-linear maps*

In the above table, $ELL_{/SCH}$ is actually a *fiber category* over the category SCH of schemes. This means that each elliptic curve E is defined over a scheme S, and $\mathrm{Hom}_{ELL}(E_{/S}, E'_{/S'})$ is made up of a commutative diagram

$$\begin{array}{ccc} E & \longrightarrow & E' \\ \downarrow & & \downarrow \\ S & \longrightarrow & S' \end{array}$$

with the top arrow sending the origin of E to that of E'.

A category $\mathcal{C}'$ is a *subcategory* of $\mathcal{C}$ if the following two conditions are satisfied:

(i) Each object of $\mathcal{C}'$ is an object of $\mathcal{C}$ and $\mathrm{Hom}_{\mathcal{C}'}(X, Y) \subset \mathrm{Hom}_{\mathcal{C}}(X, Y)$;
(ii) The composition of morphisms is the same in $\mathcal{C}$ and $\mathcal{C}'$.

A subcategory $\mathcal{C}'$ is called a *full subcategory* of $\mathcal{C}$ if the sets of homomorphisms are equal:

$$\mathrm{Hom}_{\mathcal{C}'}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(X,Y)$$

for any two objects X and Y in $\mathcal{C}'$.

4.3. **Functors.** A *covariant* (resp. *contravariant*) *functor* $F : \mathcal{C} \to \mathcal{C}'$ is a rule associating an object $F(X)$ of $\mathcal{C}'$ and a morphism $F(f) \in \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ (resp. $F(f) \in \mathrm{Hom}_{\mathcal{C}'}(F(Y), F(X))$) to each morphism $f : X \to Y$ of $\mathcal{C}$. We require $F(1_X) = 1_{F(X)}$ and

$$F(f \circ h) = F(f) \circ F(h) \text{ (resp. } F(f \circ h) = F(h) \circ F(f)). \tag{4.2}$$

Example 4.2. *Let X be a topological space. Then the category $O(X)$ of open sets consists of open subsets and inclusions:*

$$\mathrm{Hom}_{O(X)}(U,V) = \begin{cases} Inc : U \hookrightarrow V & \text{if } U \subset V \\ \emptyset & \text{otherwise.} \end{cases}$$

Then a presheaf $\mathcal{F}$ is a functor from $O(X)$ into AB.

A *morphism* f between two contravariant functors $F, G : \mathcal{C} \to \mathcal{C}'$ is a system of morphisms $\{\phi_X \in \mathrm{Hom}_{\mathcal{C}'}(F(X), G(X))\}_{X \in \mathcal{C}}$ making the following diagram commutative for all $u \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$:

$$\begin{array}{ccc} F(Y) & \xrightarrow{F(u)} & F(X) \\ {\scriptstyle \phi_Y}\downarrow & & \downarrow{\scriptstyle \phi_X} \\ G(Y) & \xrightarrow[G(u)]{} & G(X). \end{array} \tag{4.3}$$

In general, the totality of morphisms between two functors may not be a set; so, we cannot define the category of contravariant functors out-right by the collection of all functors from $\mathcal{C}$ to $\mathcal{C}'$. However we pretend to have the "category" of contravariant functors $CTF(\mathcal{C}, \mathcal{C}')$ using the above definition of morphisms between functors. Similarly, we have the "category" $COF(\mathcal{C}, \mathcal{C}')$ of covariant functors by reversing the direction of morphisms $F(u)$ and $G(u)$. In practice, we impose some conditions on functors in these "categories" to have well defined full subcategory (so, this does not pose any real problem).

If $F, G : \mathcal{C} \to SETS$ are functors, and $F(A) \subset G(A)$ for all $A \in Ob(\mathcal{C})$, we call F a subfunctor of G. Here, for $\phi \in \mathrm{Hom}_{\mathcal{C}}(A, A')$, $G(\phi)$ induces $F(\phi)$ (in other words, the inclusion $i_A : F(A) \hookrightarrow G(A)$ is a functor morphism). If $G_i \subset G$ are subfunctors indexed by an index set I, then plainly $A \mapsto \bigcap_{i \in I} G_i(A) \subset G(A)$ is a subfunctor of G. We call this functor the intersection of all G_i in G.

We can also define the product of two functors $F, G : \mathcal{C} \to SETS$ just putting $F \times G(A) := F(A) \times G(A)$ (the set theoretic product) with $(F \times G)(\phi) = F(\phi) \times G(\phi)$. If $f : F \to S$ and $g : G \to S$ are morphism of functors $F, G, S : \mathcal{C} \to SETS$, we define the *fibered product* $F \times_S G : \mathcal{C} \to SETS$ by

$$A \mapsto (F \times_S G)(A) = \{(x,y) \in F(A) \times G(A) | f_A(x) = g_A(y)\} \tag{4.4}$$

with $(F \times_S G)(\phi)(x,y) = (F(\phi)(x), G(\phi)(y))$. If further $f : F \hookrightarrow S$ and $g : G \hookrightarrow S$ are inclusions of functors, identifying F and G with subfunctors of S by f and g, it is plain that $F \times_S G(R) = F(R) \cap G(R)$ in S.

If $f : X \to Y$ is a morphism in $COF(\mathcal{C}, SETS)$ and $Y' \subset Y$ be a subfunctor, we define $f^{-1}(Y') \in COF(\mathcal{C}, SETS)$ by $f^{-1}(Y')(A) = f_A^{-1}(Y'(A))$. Plainly, $f^{-1}(Y')$ is a subfunctor of X.

4.4. **Affine schemes.** As we remarked, knowing the affine variety $\mathcal{V}_I$ is equivalent to knowing the algebra $A = k[X]/I$. So we may start with a k-algebra A in place of the zero set V to make a theory. Slightly more generally, writing B for a fixed base commutative ring B, we consider a B-algebra A. The *affine B-scheme* $S = S_A = \mathrm{Spec}_B(A)$ associated to A is a functorial rule of assigning to each B–algebra R the set given by $S(R) = \mathrm{Hom}_{B\text{-alg}}(A, R)$. When the underlying base algebra B is evident in the context, we simply write $\mathrm{Spec}(A)$ for $\mathrm{Spec}_B(A)$. Though $\mathrm{Spec}(A)$ has another aspect of a topological local ringed space as described in, for example, [GME] Section 1.2, here we concentrate on its functorial property. Since the category $SCH_{/B}$ of B-schemes is a full

subcatageory of $COF(ALG_{/B}, SETS)$, this is legitimate (see [GME] §1.4.3 and Lemma 4.16 in the text). Hereafter we write simply $\mathcal{C}_B$ for $COF(ALG_{/B}, SETS)$, which is the biggest "category" containing our geometric objects. As we remarked already, $COF(ALG_{/B}, SETS)$ may not be really a category in true sense (i.e., $\mathrm{Hom}_{COF}(F, G)$ may not be a set), but our category of schemes $SCH_{/B}$ is defined later imposing a sheaf condition to assure that it is a category by Yoneda's lemma (cf. Lemma 4.16).

The set $S_A(R)$ is called the set of R–rational points (or R–integral points) of S_A. A *B–morphism* $\phi : S_A \to S_C$ (or a morphism defined over B) is given by $\phi(P) = P \circ \underline{\phi}$ for an underlying B–algebra homomorphism $\underline{\phi} : C \to A$; in other words, we have the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{P} & R \\ {\scriptstyle \underline{\phi}}\uparrow & & \uparrow{\scriptstyle P\circ\underline{\phi}} \\ C & = & C \end{array}$$

By definition, we have the following properties of the functor S_A:

- (F1) If $R \xrightarrow{f} R' \xrightarrow{g} R''$ are B–algebra homomorphisms, then we have maps $f_* : S_A(R) \to S_A(R')$ and $g_* : S_A(R') \to S_A(R'')$ given by $f_*(P) = f \circ P$ and $g_*(Q) = g \circ Q$, and we have $(g \circ f)_* = g_* \circ f_*$.
- (F2) If $R' = R''$ and g as above is the identity map $\mathrm{id}_{R'} : R' \to R'$, we have $\mathrm{id}_{R',*} \circ f_* = f_*$. If $R = R'$ and f as above is the identity map $\mathrm{id}_R : R \to R$, we have $g_* \circ \mathrm{id}_{R,*} = g_*$.
- (F3) For the identity map $\mathrm{id}_R : R \to R$, $\mathrm{id}_{R,*} : S_A(R) \to S_A(R)$ is the identity map of the set $S_A(R)$.

In short, $R \mapsto S_A(R)$ is a covariant functor of B–algebras into sets; so, an object in $\mathcal{C}_B$. For two affine schemes S and T over B, a morphism $\phi : S \to T$ is a family of maps $\phi_R : S(R) \to T(R)$ indexed by B–algebras R such that the following diagram commutes for any B–algebra homomorphism $\alpha : R \to R'$:

$$\begin{array}{ccc} S(R) & \xrightarrow{\phi_R} & T(R) \\ {\scriptstyle \alpha_*}\downarrow & & \downarrow{\scriptstyle \alpha_*} \\ S(R') & \xrightarrow[\phi_{R'}]{} & T(R'). \end{array}$$

If confusion nis unlikely, we write $\mathrm{Hom}_B(S, T) = \mathrm{Hom}_{\mathcal{C}_B}(S, T)$ for the set of all morphisms from S into T.

By definition, we also have the following properties of affine schemes:

- (cf1) If $A \xleftarrow{\phi} C \xleftarrow{\psi} D$ are B–algebra homomorphisms, then we have morphisms of schemes $S_D \xrightarrow{\psi} S_C \xrightarrow{\phi} S_A$ such that $\phi \circ \psi$ is associated to $\underline{\psi} \circ \underline{\phi}$.
- (cf2) If $A = C$ and $\underline{\phi}$ in (cf1) is the identity map $\underline{\mathrm{id}}_A$ of A, we have $\mathrm{id}_A \circ \psi = \psi$. If $C = D$ and $\underline{\psi}$ in (cf1) is the identity map $\underline{\mathrm{id}}_C$ of C, we have $\phi \circ \mathrm{id}_C = \phi$.
- (cf3) For the identity map $\underline{\mathrm{id}}_A : A \to A$, $\mathrm{id}_A : S_A(R) \to S_A(R)$ is the identity map for all B–algebras R.

Thus the functor $A \mapsto S_A$ is a contravariant functor from B–algebras into $\mathcal{C}_B$. One of the most basic facts in functorial algebraic geometry is full-faithfullness of this functor (e.g. [GME] §1.4.3):

$$\mathrm{Hom}_{B\text{-alg}}(A', A) \cong \mathrm{Hom}_B(S_A, S_{A'}) \ \text{ via } \underline{\alpha} \leftrightarrow \alpha. \tag{4.5}$$

A main point of the proof of this fact is to construct from a given morphism $\phi \in \mathrm{Hom}_B(S_A, S_{A'})$ a B-algebra homomorphism $\varphi : A' \to A$ such that $\underline{\varphi} = \phi$.

Exercise 4.3. *Let $\varphi = \phi_A(\mathrm{id}_A) \in S_{A'}(A) = \mathrm{Hom}_{B\text{-}alg}(A', A)$, where $\mathrm{id}_A \in S_A(A) = \mathrm{Hom}_{B\text{-}alg}(A, A)$ is the identity map. Then prove that $\underline{\varphi} = \phi$.*

Here are some examples of affine schemes:

Example 4.4. Take $f(X,Y,Z) = X^p + Y^p - Z^p$ for a prime p, and let $B = \mathbb{Z}$. Then consider $A = \mathbb{Z}[X,Y,Z]/(f(X,Y,Z))$. For each algebra R, we claim

$$S_A(R) \cong \{(x,y,z) \in R^3 | x^p + y^p = z^p\}.$$

Indeed, for each solution $P = (x,y,z)$ of Fermat's equation in R, we define an algebra homomorphism $\underline{\phi} : B[X,Y,Z] \to R$ by sending polynomials $\Phi(X,Y,Z)$ to its value $\Phi(x,y,z) =: \underline{\phi}(\Phi) \in R$. Since $\Phi \in (f(X,Y,Z)) \Leftrightarrow \Phi = \Psi f$, we find that $\underline{\phi}(\Psi f) = \Psi(x,y,z) f(x,y,z) = 0$; so, $\underline{\phi}$ factors through the quotient A getting $\phi \in S_A(R)$. In this way, we get an injection from the right-hand-side to $S_A(R)$. If we start from $\underline{\phi} : A \to R$ in $S_A(R)$, we find

$$0 = \underline{\phi}(0) = \underline{\phi}(X^p + Y^p - Z^p) = \underline{\phi}(X)^p + \underline{\phi}(Y)^p - \underline{\phi}(Z)^p.$$

Thus $(x,y,z) := (\underline{\phi}(X), \underline{\phi}(Y), \underline{\phi}(Z))$ is an element in the right-hand-side, getting the isomorphism. By Fermat's last theorem, we have

$$S_A(\mathbb{Z}) \cong \{(a,0,a),(0,b,b),(c,-c,0) | a,b,c \in \mathbb{Z}\} \text{ if } p \text{ is a prime} \geq 3.$$

There is a simpler example: We have

$$S_{\mathbb{Z}[X_1,\ldots,X_n]}(R) = R^n \text{ via } \phi \mapsto (\underline{\phi}(X_1), \ldots, \underline{\phi}(X_n)).$$

Often $S_{\mathbb{Z}[X_1,\ldots,X_n]}$ is written as $\mathbf{A}^n$ or $\mathbb{G}_a^n$ and is called the affine space of dimension n. We write $\mathbb{G}_a$ for $\mathbb{G}_a^1$, though we have written it earlier as $\mathbb{A}^1$ (the affine line). We have an algebra homomorphism $B[X,Y,Z] \to A$ for A in Example 4.4 sending Φ to $(\Phi \mod f(X,Y,Z))$. This in turn induces a morphism $i : S_A \to \mathbb{G}_a^3$, which is visibly injective.

An A-algebra A' is called *finite type* over A if we can write $A' = A[X_1,\ldots,X_n]/\mathfrak{a}$ for the polynomial ring $A[X_1,\ldots,X_n]$ of finitely many variables modulo an ideal $\mathfrak{a}$. If further $\mathfrak{a}$ is generated by finitely many elements of $A[X_1,\ldots,X_n]$, we call A' *finitely presented* over A (cf. [EGA] IV.1.4). If A is noetherian, $A[X_1,\ldots,X_n]$ is noetherian; so, finite-presentation of $A[X]/\mathfrak{a}$ is automatic. However when we treat non-noetherian rings (for example, if we want to show that the classification functor of elliptic curves $E_{/R}$ given by $R \mapsto \{E_{/A}\}/\cong$ is (close to) a scheme), finite-presentation property guarantees that the number of equations defining affine scheme is finite (and hence the property is important technically). The corresponding morphism $S_{A'} \to S_A$ of affine schemes are also called *finite type* (resp. *finitely presented*) if A'/A is of finite type (resp. finitely presented).

A morphism $\phi : S_A \to S_{A'}$ is called *flat* if $M \mapsto M \otimes_{A',\underline{\phi}} A$ is a left exact functor from the category of A'-modules to the category of A-modules. Here the functor $M \mapsto M \otimes_{A',\underline{\phi}} A$ is *left exact* if it preserves injective morphisms of A-modules, that is,

$$\mathrm{Ker}(\iota \otimes 1 : M \otimes_{A',\underline{\phi}} A \to M' \otimes_{A',\underline{\phi}} A) = 0 \text{ if } \mathrm{Ker}(\iota : M \to M') = 0.$$

The morphism ϕ is *faithfully flat* if (i) it is flat and (ii) $0 \to M \to M' \to M'' \to 0$ is exact if $0 \to M \otimes_{A',\underline{\phi}} A \to M' \otimes_{A',\underline{\phi}} A \to M'' \otimes_{A',\underline{\phi}} A \to 0$ is exact for any sequence $M \to M' \to M''$ of A'-modules. The proof of the following fact is a bit demanding:

Proposition 4.5. *Suppose that A is noetherian B-algebra and A' is an A-algebra of finite type. Let M be an A'-module of finite type.*

1. $\{P \in \mathrm{Spec}(A') | M_P$ *is flat over* $A_P\}$ *is an open subscheme of* $S_{A'}$,
2. *If A' is A-flat, the morphism $S_{A'} \to S_A$ is an open map.*

We refer the proof to [CRT] Theorem 24.3 for (1), [CMA] page 48 or [EGA] IV.2.4.6 for (2).

A morphism $\phi : S_{A'} \to S_A$ is called *finite* if the A-module A' (via $\underline{\phi}$) is of finite type (that is, there exist a positive integer n and a surjective A-linear map $A^n \twoheadrightarrow A'$). If $S_{A'}$ is finite flat, localizations $A'_{\mathfrak{m}}$ at each prime ideal $\mathfrak{m}$ of A are free of finite rank over $A_{\mathfrak{m}}$, and therefore, $S_{A'}$ is also called locally free of finite rank over S_A if ϕ is finite flat.

For a maximal ideal $\mathfrak{m}$ of A', ϕ is *smooth* at $\mathfrak{m}$ if $A'_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$ and for any A-algebra R with a square-zero ideal I, $\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}^n A', R) \to \mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}^n A', R/I)$ is surjective for all positive integer n (that is, any A-algebra homomorphism $\phi_0 : A'/\mathfrak{m}^n A' \to R/I$ can be lifted to an A-algebra homomorphism $\phi_1 : A'/\mathfrak{m}^n A' \to R$ such that $\phi_1 \mod I = \phi_0$). Here $A'_{\mathfrak{m}}$ is the localization of A' at $\mathfrak{m}$ and $A_{\mathfrak{m}}$ is the localization of A at $\underline{\phi}^{-1}(\mathfrak{m})$. We call $\phi : S_{A'} \to S_A$ *smooth* if ϕ is smooth at all

maximal ideals $\mathfrak{m}$ of A. Since smoothness at $\mathfrak{m}$ is an infinitesimal property only depending modulo a power of the maximal ideal, it only depends on the adic completion of the maximal ideal.

Suppose that B is a perfect field k and that S_A is of finite type over S_k (so, $K = A/\mathfrak{m}$ is a finite separable extension of k for a maximal ideal $\mathfrak{m}$ of A), $S_A \to S_k$ is smooth at $\mathfrak{m}$ if and only if the $\mathfrak{m}$-adic completion $\widehat{A} = \varprojlim_n A/\mathfrak{m}^n$ is isomorphic to a power series ring $K[[X_1, \dots, X_n]]$ for $n = \dim A$ (cf. [BCM] IX.3.3). Thus if B is a perfect field k and A is noetherian of (Krull) dimension n, S_A is smooth over S_k if and only of the local ring of A at every maximal ideal $\mathfrak{m}$ has completion isomorphic to $(A/\mathfrak{m})[[X_1, \dots, X_n]]$.

Exercise 4.6. *Prove that $\mathbb{G}_a^n$ is smooth over $S_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z})$.*

For a maximal ideal $\mathfrak{m}$ of A', $\phi : S_{A'} \to S_A$ is *étale* at $\mathfrak{m}$ if $S_{A'_{\mathfrak{m}}}$ is flat over $S_{A_{\mathfrak{m}}}$ and for any A-algebra R with a square-zero ideal I, $\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}^n, R) \to \mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}^n, R/I)$ is bijective for all positive integers n.

Lemma 4.7. *If A' is a local ring étale finite over a local ring A having the same residue field k. Then $A/\mathfrak{m}_A^n = A'/\mathfrak{m}_{A'}^n$ for all n, in particular, we have*

$$\widehat{A} = \varprojlim_n A/\mathfrak{m}_A^n = \varprojlim_n A'/\mathfrak{m}_{A'}^n = \widehat{A}'.$$

Proof. By assumption, $A/\mathfrak{m}_A = A'/\mathfrak{m}_{A'} = k$ for maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_{A'}$. Since $\mathfrak{m}_A$ is square zero ideal of $A/\mathfrak{m}_A^2$, taking R to be $A/\mathfrak{m}_A^2$, we have

$$\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^2, A/\mathfrak{m}_A) \cong \mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^2, A/\mathfrak{m}_A^2),$$

whose left hand side is a singleton given by the projection $A'/\mathfrak{m}_{A'}^2 \twoheadrightarrow k$. Similarly, taking R to be $A'/\mathfrak{m}_{A'}^2$,

$$\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^2, A'/\mathfrak{m}_{A'}) \cong \mathrm{End}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^2),$$

whose left-hand-side is a singleton. Thus

$$\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^2, A/\mathfrak{m}_A^2) = \{\varphi_2\} \quad \text{and} \quad \mathrm{End}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^2) = \{\mathrm{id}_{A'/\mathfrak{m}_{A'}^2}\}$$

are both singletons. Since $A'/\mathfrak{m}_{A'}^2$ is an A-algebra, $\mathrm{Hom}_{A\text{-alg}}(A/\mathfrak{m}_A^2, A'/\mathfrak{m}_{A'}^2) = \{\phi_2 = \iota_A \mod \mathfrak{m}_{A'}^2\}$. Taking $A' = A$, we find $\mathrm{End}_{A\text{-alg}}(A/\mathfrak{m}_A^2) = \{\mathrm{id}_{A/\mathfrak{m}_A^2}\}$. Thus $\varphi_2 \circ \phi_2 = \mathrm{id}_{A/\mathfrak{m}_A^2}$ and $\phi_2 \circ \varphi_2 = \mathrm{id}_{A'/\mathfrak{m}_{A'}^2}$. Thus $A'/\mathfrak{m}_{A'}^2 = A/\mathfrak{m}_A^2$.

We now proceed by induction on n assuming $A/\mathfrak{m}_A^{n-1} = A'/\mathfrak{m}_{A'}^{n-1}$ and prove $A/\mathfrak{m}_A^n = A'/\mathfrak{m}_{A'}^n$. Since $\mathfrak{m}_{A'}^{n-1} \subset A'/\mathfrak{m}_{A'}^n$ and $\mathfrak{m}_A^{n-1} \subset A/\mathfrak{m}_A^n$ are square zero ideals, taking (R, I) to be $(A'/\mathfrak{m}_{A'}^n, \mathfrak{m}_{A'}^{n-1})$ and $(A'/\mathfrak{m}_{A'}^n, \mathfrak{m}_{A'}^{n-1})$, by the same argument as above, we find

$$\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^n, A/\mathfrak{m}_A^n) \cong \mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^n, A/\mathfrak{m}_A^{n-1}) = \{\varphi_n\}$$
$$\mathrm{Hom}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^n, A'/\mathfrak{m}_{A'}^{n-1}) \cong \mathrm{End}_{A\text{-alg}}(A'/\mathfrak{m}_{A'}^n) = \{\mathrm{id}_{A'/\mathfrak{m}_{A'}^2}\}.$$

Then for a unique A-algebra homomorphism $\phi_n = (\iota_A \mod \mathfrak{m}_{A'}^n) : A/\mathfrak{m}_A^n \to A'/\mathfrak{m}_{A'}^n$, we find $\varphi_n \circ \phi_n = \mathrm{id}_{A/\mathfrak{m}_A^n}$ and $\phi_n \circ \varphi_n = \mathrm{id}_{A'/\mathfrak{m}_{A'}^n}$, and we are done. □

We call $\phi : S_A \to S_{A'}$ *étale* if ϕ is étale at all maximal ideals of A'.

Exercise 4.8. *Suppose we have morphisms of B-schemes $S_{A''} \to S_{A'} \to S_A$. If $S_{A''}$ is étale over $S_{A'}$ and $S_{A'}$ is smooth over S_A, prove that $S_{A''}$ is smooth over S_A. How about, if $S_{A''}$ is smooth over S_A and $S_{A''}$ is étale over $S_{A'}$, is $S_{A'}$ smooth over S_A?*

4.5. **Zariski open covering.** When we have a morphism of affine schemes $\phi : S_A \to S_C$, and if $\underline{\phi} : C \to A$ is a surjective ring homomorphism, we call ϕ a *closed immersion*. Then ϕ_R is injective (for any B-algebra R), and we can identify $S_A \subset S_C$ all the time. In this case, S_A regarded as a subfunctor of S_C is called *B–closed* in S_C. As we will see in Exercise 4.15 (2), if $S_i \subset S_C$ is closed for a finite number of affine schemes S_i, the intersection $R \mapsto \bigcap_i S_i(R)$ is again an affine closed subscheme. Thus we can give a topology on $S_C(R)$ for each R so that closed sets are given by the empty set $\emptyset$ and those of the form $S_A(R)$ for closed immersion $S_A \hookrightarrow S_C$. This topology is called the *Zariski B-topology* of S_C. When B is obvious in the context, we call it Zariski topology on S_C. If B' is a B–algebra, we may regard $A' = B' \otimes_B A$ as a B'–algebra by $a' \mapsto a \otimes 1$. Then we get a new

scheme $S_{A'}$ over the ring B', which sometimes written as $S_{B'} \times_B S_A$ and is called the *fibered product* of S_A and $S_{B'}$ over B. Indeed as a functor, it is identical to $S_{B'} \times_{S_B} S_A$ (Exercise 4.15 (3–4)). If we have a point $\phi \in S_A(R)$ for a B'–algebra R, we can extend $\underline{\phi} : A \to R$ to $\underline{\phi}' : A' = B' \otimes_B A \to R$ by $\underline{\phi}'(a \otimes b) = a\underline{\phi}(b)$. Thus $\phi \mapsto \phi'$ gives the natural map $S_A(R) \to S_{A'}(R)$ for all B'–algebras R. This map is an isomorphism, because for any given $\phi' \in S_{A'}(R)$, $\underline{\phi}(b) = \underline{\phi}(1 \otimes b)$ gives a point $\phi \in S_A(R)$ as long as R is a B'–algebra (Exercise 4.15 (3)). However a B'–closed subset of $S_{A'}$ may not be B–closed; so, the Zariski topology depends on the base ring B.

Exercise 4.9. *Let $f : S_{A'} \to S_A$ be a morphism of affine scheme. If $S_{\overline{A}} \subset S_A$ is a closed subscheme, prove that $f^{-1}(S_{\overline{A}})$ is a closed subscheme (so, any morphism of affine schemes is "continuous" with respect to Zariski topology).*

Pick $0 \neq f \in A$. Then $\overline{A} = A/(f)$ is a surjective image of A. Thus $S_{\overline{A}} \subset S_A$ is a closed subscheme. For each point $\phi \in S_A(R)$, $f : \phi \mapsto \phi(f)$ gives rise to a map $f_R : S_A(R) \to \mathbb{G}_a(R) = R$. This collection of maps $\{f_R\}_R$ can be easily checked to be a morphism $S_A \to \mathbb{G}_a$ of functors, which we again call $f : S_A \to \mathbb{G}_a$. In this way, we regard $f \in A$ as a function (or more precisely, a functor morphism) defined on S_A with values in $\mathbb{G}_a$. Any B-algebra homomorphism $(P : A \to R) \in S_A(R)$ factoring through $\overline{A}$ satisfies $f(P) = P(f) = 0$. Thus $S_{\overline{A}}(R) = \{P \in S_A(R) | f(P) = 0\}$ (which is the zero-set of f). We consider the quotient ring $A_f = A[\frac{1}{f}]$. Then the natural map $b \mapsto \frac{b}{1}$ is a B-algebra homomorphism of A into A_f; so, $S_{A_f} \subset S_A$. If $P \in S_A(R)$ factors through A_f, we have $f(P) = P(f) \in R^\times$, as $f \in A$ is invertible in A_f. Thus $S_A \supset S_{\overline{A}} \sqcup S_{A_f}$, and $S_A(k) = S_{\overline{A}}(k) \sqcup S_{A_f}(k)$ for any field k (which is a B-algebra). Hence we call S_{A_f} an open subscheme of S_A, giving outside the zero set of the function f.

Exercise 4.10. *Prove that $S_A(k) = S_{\overline{A}}(k) \sqcup S_{A_f}(k)$ for any field k, and give an example of B-algebra R such that $S_A(R) \supsetneq S_{\overline{A}}(R) \sqcup S_{A_f}(R)$.*

More generally, a subfunctor $U \subset S_A$ is called an open subscheme if U is a subfunctor and there exists a subset $I \subset A$ such that

$$\begin{aligned} U(R) = U_I(R) &= \{P \in S_A(R) | \sum_{f \in I} f(P)R = R\} \\ &= \{P \in \mathrm{Hom}_{B\text{-alg}}(A, R) | \sum_{f \in I} P(f)R = R\}. \end{aligned} \tag{4.6}$$

Obviously, for the ideal generated (I) by I, $U_{(I)} = U_I$, and we may assume that I is an ideal. For $I = (0_A)$, $U_{(0)}(R) = \emptyset$ for any B-algebra R; so, $\emptyset$ is an open subscheme. Similarly, $U_A(R) = S_A(R)$ for all R; so, S_A itself is an open subscheme. If $\{I_i\}_{i \in I}$ is a family of ideals, we have $U_{\sum_{i \in I} I_i} \supset \bigcup_{i \in I} U_i$ and $U_{\sum_{i \in I} I_i}(k) = \bigcup_{i \in I} U_i(k)$ if k is a field.

Exercise 4.11. *Check that $R \mapsto U_I(R)$ is a subfunctor of S_A, and verify that $S_{A_f} = U$ if $I = \{f\}$.*

Exercise 4.12. *If a nonempty open subscheme $U \subset S_A$ is isomorphic to an affine scheme $S_{A'}$, prove that there exists a multiplicative set $S \subset A$ such that A' is isomorphic as B-algebras to the ring of fractions $S^{-1}A$.*

Exercise 4.13. *Let $B = \mathbb{C}$ and $A = \mathbb{C}[X, Y]$ (the polynomial ring of the indeterminates X and Y). Define a closed subscheme S_C of S_A for $C = A/(X, Y)$. Prove that there exists an open subscheme U of S_A such that $U(k) = S_A(k) - S_C(k)$ for any field extension $k/\mathbb{C}$ but U is not isomorphic to any affine $\mathbb{C}$-scheme.*

Lemma 4.14. *Let U, U' be open-subschemes of S_A. If $U(k) = U'(k)$ for any field k over B, $U = U'$.*

Proof. Let $U = U_I$ and $U' = U_J$ for ideals I and J. If $U \neq U'$, we can find a B-algebra R such that $P \in U(R)$ but $P \notin U'(R)$. Regarding $P \in S_A(R) = \mathrm{Hom}_{B\text{-alg}}(A, R)$, we find that $P(I)R = R$ and $P(J)R \subsetneq R$. Since $P(J)R$ is a proper ideal of R, we can find a maximal ideal $\mathfrak{m}$ of R such that $\mathfrak{m} \supset P(J)R$ (cf. [CRT] Theorem 1.1). Let $k = R/\mathfrak{m}$ and define $\overline{P} \in \mathrm{Hom}_{B\text{-alg}}(A, k)$ by composing P with the projection $R \twoheadrightarrow k$. Then $\overline{P} \in U(k)$ and $\overline{P} \notin U'(k)$. □

Exercise 4.15.

(1) *Prove that a closed immersion $i : S_A \hookrightarrow S_C$ gives rise to an injection $i_R : S_A(R) \hookrightarrow S_C(R)$ for any B–algebras R.*
(2) *Prove that if $i : S_A \subset S_C$ and $j : S_D \subset S_C$ are closed, then $R \mapsto S_A(R) \cap S_D(R)$ is closed in S_C and is isomorphic to S_E for $E = A \otimes_C D$, where the tensor product is taken with respect to the associated algebra homomorphisms $\underline{i} : C \to A$ and $\underline{j} : C \to D$.*
(3) *Prove $S_A(R) \cong S_{A'}(R)$ if $A' = B' \otimes_B A$ and R is a B'–algebra, where B' is another B–algebra. Here the left-hand side is regarded as an affine B-scheme and the right-hand side is regarded as an affine B'-scheme.*
(4) *For two B–algebras A and C, show that $S_{A\otimes_B C}(R) = S_A(R) \times S_C(R)$ for any B–algebra R. Hint: $\phi \in S_A(R)$ and $\psi \in S_C(R)$, we associate $\phi \otimes \psi \in S_{A\otimes_B C}(R)$ given by $(\phi \otimes \psi)(b \otimes c) = \phi(b)\psi(c)$. Thus a product of affine schemes is again an affine B-scheme. The scheme $S_{A\otimes_B C}$ is called the fibered product of S_A and S_C over B.*

Recall the simplified notation: $\mathcal{C}_B = COF(ALG_{/B}, SETS)$. We can generalize open/closed subschemes to open/closed subfunctors in the following way. A subfunctor $U \subset X$ is called *open* (resp. *closed*) *subfunctor* if for any affine B-scheme S_A and any morphism $f : S_A \to X$, the pullback $f^{-1}(U)$ is an open (resp. closed) subscheme. By Exercise 4.9, if $X \cong S_A$ is affine, the definition of closedness of U is the same as that of closed affine subscheme. An open subscheme of an affine scheme is determined by its value over fields (Lemma 4.14), and the value of an open subscheme at a field is the complement of a closed subscheme. This shows that if $X \cong S_A$ is affine, the definition of being open for U in X is the same as that of open affine subscheme.

Here is a slightly more general version of Yoneda's lemma than Exercise 4.3:

Lemma 4.16. *For any $X \in \mathcal{C}_B$, we have a canonical isomorphsm*

$$\iota : \mathrm{Hom}_B(S_A, X) \cong X(A)$$

given by $\iota(f) = f_A(\mathrm{id}_A)$ for the identity map $\mathrm{id}_A : A \cong A$.

Taking $R = A$ and $X = S_{A'}$, this proves (4.5).

Proof. We have ι well defined as above. Take a (variable) B-algebra R. Then for any $\phi \in \mathrm{Hom}_{B\text{-alg}}(A, R) = S_A(R)$, we have $X(\phi) \circ f_A = f_R \circ S_A(\phi)$ as f is a morphism of functors. Then writing $I_f = f_A(\mathrm{id}_A)$, we get $f_R(\phi) = X(\phi)(I_f)$ as $S_A(\phi)(\mathrm{id}_A) = \phi \circ \mathrm{id}_A = \alpha$. Since R is a variable, f is uniquely determined by I_f. Thus ι is injective. Conversely, for any $x \in X(A)$ and $\phi \in S_A(R) = \mathrm{Hom}_{B\text{-alg}}(A, R)$, we define $f_R(\phi) = X(\phi)(x)$, and we leave the reader to verify $\iota(f) = x$. In this way, we can recover f and hence ι is surjective. □

Lemma 4.17. *If $U, U' \subset X \in \mathcal{C}_B$ are open subfunctors, $U = U'$ if $U(k) = U'(k)$ for all fields k over B.*

Proof. Suppose that $U \neq U'$. Then we find a B-algebra A such that $U(A) \neq U'(A)$. Thus we find $P \in U(A)$ but $P \notin U'(A)$. By Lemma 4.16, we may regard $P \in \mathrm{Hom}_B(S_A, U) \subset \mathrm{Hom}_B(S_A, X)$. Then $P_A : S_A(A) \to X(A)$, and $\mathrm{id}_A \in P_A^{-1}(U(A))$ but $\mathrm{id}_A \notin P_A^{-1}(U'(A))$; so, $P^{-1}(U) \neq P^{-1}(U')$. Then by Lemma 4.14, we find a field k with $P^{-1}(U)(k) \neq P^{-1}(U')(k)$; so, $U(k) \neq U'(k)$. □

A family $\{U_i\}_{i\in I}$ of open subfunctors of X is called an *open covering* if $X(k) = \bigcup_{i\in I} U_i(k)$ for all fields k over B.

For a given $X \in \mathcal{C}_B$, we can think of the category $O(X)$ of open subfunctors of X, whose objects are made up of open subsubfuctors of X and $\mathrm{Hom}_{O(X)}(U, U')$ is either the inclusion $U \subset U'$ or the empty set according as U is a subfunctor of U' or not. By Lemma 4.17, the category $O(X)$ looks very close to the category of open subsets of a topological space.

4.6. **Zariski sheaves.** A functor $X \in \mathcal{C}_B$ is called *local* if it satisfies the following set theoretic exact sequence for any open covering $\{Y_i\}_{i\in I}$ of any object Y in $\mathcal{C}_B$:

$$\mathrm{Hom}_{\mathcal{C}_B}(Y, X) \to \prod_{i\in I} \mathrm{Hom}_{\mathcal{C}_B}(Y_i, X) \rightrightarrows \prod_{i,j\in I} \mathrm{Hom}_{\mathcal{C}_B}(Y_i \cap Y_j, X), \tag{4.7}$$

in other words, writing $\mathrm{Res}_i : \mathrm{Hom}_{\mathcal{C}_B}(Y, X) \to \mathrm{Hom}_{\mathcal{C}_B}(Y_i, X)$ for the restriction to Y_i and $\mathrm{Res}_{i,j} : \mathrm{Hom}_{\mathcal{C}_B}(Y_i, X) \to \mathrm{Hom}_{\mathcal{C}_B}(Y_i \cap Y_j, X)$ for the restriction to $Y_i \cap Y_j$, if $\mathrm{Res}_{i,j}(\alpha_i) = \mathrm{Res}_{j,i}(\alpha_j)$ for $(\alpha_i) \in$

$\mathrm{Hom}_{\mathcal{C}_B}(Y,X) \to \prod_{i\in I}\mathrm{Hom}_{\mathcal{C}_B}(Y_i,X)$, then $\alpha_i = \mathrm{Res}_i(\alpha)$ for all i for a *unique* $\alpha \in \mathrm{Hom}_{\mathcal{C}_B}(Y,X)$. Thus, any morphism from Y to X is determined by the local data α_i. This is the least requirement for X being a geometric object as a morphism from a geoemetric object must be determined by local data. A *B-scheme* is a local functor in $\mathcal{C}_B$ which has an open covering by affine B-schemes. For a B-scheme S, an S-scheme is a pair of a morphism $\iota_X : X \to S$ and X. We write $SCH_{/S}$ for the category of S-schemes. A morphism of S-schemes $\phi : X \to Y$ by definition satisfies $\iota_Y \circ \phi = \iota_X$. If $X_{/S}$ and $Y_{/S}$ are S-schemes, $X \times_S Y$ is plainly an S-scheme (so, $SCH_{/B}$ has fibered product; see [GME] §1.5.2). A morphism $X \to Y$ of B-scheme is *separated* if the diagonal subfunctor $\Delta_{X/Y}(R) = \{(x,x) \in X(R) \times_{Y(R)} X(R) | x \in X(R)\}$ is a closed subscheme of $X \times_Y X$. We define a morphism of scheme $f : X \to S$ to be *proper* if the following two conditions are satisfied by f:

(1) f is separated and of finite type;
(2) For any S–scheme T, the projection $f_T : X_T = X \times_S T \to T$ is a closed map.

A morphism $X \xrightarrow{f} Y$ of B-scheme is *quasi-compact* if for any open subscheme $U \subset Y$, the topological space of $f^{-1}(U)$ is quasi-compact (i.e., any open covering of $f^{-1}(U)$ has finite subcovering).

As expected, we have (cf. [RAG] 1.8):

Lemma 4.18. *An affine B-scheme is a B-scheme.*

Here is a sketch of a proof.

Proof. By Lemma 4.16 and (4.3), $X(A) = \mathrm{Hom}_{\mathcal{C}_B}(S_A, S_R) = \mathrm{Hom}_{B\text{-alg}}(R,A)$. Thus, for an open affine covering $\{S_{A_i}\}_{i\in I}$ (for fraction rings A_i) of S_A, we need to prove exactness of

$$\mathrm{Hom}_{\mathcal{C}_B}(S_A,X) \to \prod_{i\in I}\mathrm{Hom}_{\mathcal{C}_B}(S_{A_i},X) \rightrightarrows \prod_{i,j\in I}\mathrm{Hom}_{\mathcal{C}_B}(S_{A_i}\cap S_{A_j},X)$$

for $X = S_R$, which turns out to be

$$\mathrm{Hom}_{B\text{-alg}}(R,A) \to \prod_{i\in I}\mathrm{Hom}_{B\text{-alg}}(R,A_i) \rightrightarrows \prod_{i,j\in I}\mathrm{Hom}_{B\text{-alg}}(R, A_i \otimes_A A_j),$$

since $S_{A_i} \cap S_{A_j} = S_{A_i \otimes A_j}$ with $\mathrm{Res}_{i,j}$ corresponding to $A_i \ni a \mapsto a \otimes 1 \in A_i \otimes_A A_j$. The exactness of the above sequence is equivalent to the exactness of

$$A \to \prod_{i\in I} A_i \rightrightarrows \prod_{i,j\in I} A_i \otimes_A A_j.$$

Since $O(S_A)$ has a base of open subsets of the form S_{A_f}, we may assume $A_i = A_{f_i}$ for $\{f_i\}_{i\in I}$. Then $A_i \otimes_A A_j = A_{f_i f_j}$ by $a \otimes b \mapsto ab$, and the exactness of the above sequence follows from standard commutative ring theory (cf. [ALG] II.2.2 or [GME] §1.2.1). □

For $A \in ALG_{/B}$, we have the structure morphism $\underline{\iota}_A : B \to A$ given the B-algebra structure on A, and hence $\iota_A : S_A \to S_B$. Let X be a B-scheme; so, $X = \bigcup_{i\in I} S_{A_i}$ for open affine subschemes S_{A_i}. Since X is local, we have the exact sequence

$$\mathrm{Hom}_{\mathcal{C}_B}(X,S_B) \to \prod_{i\in I}\mathrm{Hom}_{\mathcal{C}_B}(S_{A_i},S_B) \rightrightarrows \prod_{i,j\in I}\mathrm{Hom}_{\mathcal{C}_B}(S_{A_i}\cap S_{A_j},S_B)$$

and $\{\iota_{A_i} : S_{A_i} \to S_B\}_i$ is in the kernel of the second double arrows; so, we have a unique *structure morphism* $\iota_X : X \to S_B$.

Let X be a B-scheme. A *presheaf* F on X is a contravariant functor from $O(X)$ to AB. A morphism of presheaves $F \to G$ is a morphism of contravariant group functors. A *sheaf* F is a presheaf which satisfies the following exact sequence (of abelian groups) for any open covering $\{Y_i\}_{i\in I}$ of any object Y in $\mathcal{C}_B$:

$$0 \to F(Y) \xrightarrow{\prod_i \mathrm{Res}_i} \prod_{i\in I} F(Y_i) \xrightarrow{\prod_{i,j}\mathrm{Res}_i - \mathrm{Res}_j} \prod_{i,j\in I} F(Y_i \cap Y_j),$$

where Res_i indicate the restriction map $F(Y) \to F(Y_i)$ and $\mathrm{Res}_i - \mathrm{Res}_j$ is taken in $F(Y_i \cap Y_j)$ after restricting to $Y_i \cap Y_j$. The category of sheaves $S(X)$ is a full subcategory of the category $PS(X)$ of preseaves. For a presheaf F and an open subscheme U, often we write $H^0(U,F)$ for $F(U)$ following

a tradition of cohomology theory. For any open subscheme $Y \subset X$ of a scheme and a sheaf F on X, F induces a sheaf on Y as any open subscheme of Y is open in X. We write $F|_Y$ for the induced sheaf.

The stalk at $P \in X(k)$ (for a field k) of a sheaf F is an abelian group given by $F_P = \varinjlim_U H^0(U, F)$, where U runs over affine open subscheme such that $P \in U(k)$ (such an open subscheme is called an open neighbourhood of P). We call P a *maximal point* if it has an affine open neighbourhood S_A with $P \in S_A(k) = \mathrm{Hom}_{B\text{-alg}}(A, k)$ surjecting down to k. A point $P \in X(k)$ is called a *geometric point* if k is an algebraically closed field. A geometric point may not be maximal as $P : A \to k$ may not be surjective for any open neighbourhood S_A of P. For any integral domain R, $P \in X(R)$ induces a geometric point $\overline{P} \in X(k)$ for an algebraic closure k of the field of fraction of R as we have a natural inclusion map $X(R) \hookrightarrow X(k)$. For a point $P \in X(k)$ as above, we write $k(P)$ for the coefficient field k. Since the stalk at P is determined by open affine neighbourhoods of P, any property of affine schemes determined by stalks can be extended to general schemes; so, for example, flatness, smoothness, étaleness, and so on is well defined for general scheme morphism $f : X \to Y$.

Since a sheaf has values in abelian groups, it has a natural structure of additive category. We call a sequence of sheaves $F \to G \to H$ exact if $F_P \to G_P \to H_P$ is exact for stalks at all maximal points P. Then the category of sheaves on X becomes an abelian category (see [GME] §1.4.4 for abelian/additive categories). If $f : X \to Y$ is a morphism of B-schemes and F is a sheaf on X, the *direct image* sheaf on Y, written as f_*F is defined by $f_*F(U) = F(f^{-1}(U))$ for open subschemes U of Y.

We have a unique sheaf $\mathcal{O}_S$ of "schematic functions" on S such that $\mathcal{O}_S(S_A) = H^0(S_A, \mathcal{O}_S) = A$ for any affine open subscheme $S_A \hookrightarrow S$. Indeed, for any open subscheme $U \subset S$, we have $H^0(U, \mathcal{O}_S) = \mathrm{Hom}_B(U, \mathbb{G}_a)$. This sheaf is called the *structure sheaf* of S. Since $\mathbb{G}_a$ is a ring scheme, $\mathcal{O}_S(U) = H^0(U, \mathcal{O}_S)$ is a ring. Thus $\mathcal{O}_S$ is a sheaf of rings. A sheaf F over a B-scheme S is called an $\mathcal{O}_S$-module if we have a functor morphism $\mathcal{O}_S \times F \to F$ which gives rise to an $\mathcal{O}_S(U)$-module structure on $F(U)$ for every open subscheme $U \subset S$. Consider a sheaf of rings $\mathcal{A}_{/S}$ which is at the same time an $\mathcal{O}_S$-module under the structure $\mathcal{O}_S$-algebra homomorphism $\iota_{\mathcal{A}} : \mathcal{O}_S \to \mathcal{A}$. Such a sheaf is called a sheaf of $\mathcal{O}_S$-algebras. We write the category of $\mathcal{O}_S$-algebras as $ALG_{/\mathcal{O}_S}$ whose morphism f are sheaf $\mathcal{O}_S$-algebra homomorphisms, that is, $f : \mathcal{A} \to \mathcal{A}'$ is a morphism of functors from $O(S)$ to AB and is at the same time $f_U : \mathcal{A}(U) \to \mathcal{A}'(U)$ is $\mathcal{O}_S(U)$-algebra homomorphism.

We may replace S_B by a general B-scheme S in the construction of B-schemes. Consider the category $\mathcal{C}_S = COF(ALG_{/\mathcal{O}_S}, SETS)$. Since $ALG_{/\mathcal{O}_S}$ is a subcategory of $ALG_{/B}$, we may restrict S_A for any $\mathcal{O}_S$-algebra A (which is also a B-algebra). A subfunctor U of $X \in \mathcal{C}_S$ is called open/closed if $f^{-1}(U)$ is open for any morphism $S_A \xrightarrow{f} X$ from an affine scheme S_A. An open covering $\{Y_i\}_i$ of $Y \in \mathcal{C}_S$ is made up of open subschemes $Y_i \subset Y$ such that $Y(k) = \bigcup_i Y_i(k)$ for any field k over the algebra $\mathcal{O}_S(U)$ for any affine subscheme $U \subset S$. Using this definition of open covering, we call $X \in \mathcal{C}_S$ local if it satisfies the sheaf exact sequence (4.7) (replacing $\mathcal{C}_B$ by $\mathcal{C}_S$) for open coverings $\{Y_i\}_i$ of Y. A functor $X \in \mathcal{C}_S$ is called *S-schemes* if it is local and covered by affine open subschemes. The functor $F \in \mathcal{C}_S = COF(SCH_{/S}, SETS)$ given by $F(f : X \to S) = \mathrm{Hom}_{\mathcal{O}_S\text{-algebra}}(\mathcal{A}, f_*\mathcal{O}_X)$. Here $f_*\mathcal{O}_X$ is a sheaf of $\mathcal{O}_S$-algebras given by $f_*\mathcal{O}_X(U) = \mathcal{O}_X(f^{-1}(U))$. Since $\mathcal{A}$ and $f_*\mathcal{O}_X$ are local as they are sheaves over S, the functor F is also local. Thus F is an S-scheme. We often write $F = Spec_S(\mathcal{A})$. A morphism $X \xrightarrow{f} S$ is called *affine relative to S* if $X = Spec_S(\mathcal{A})$ for a sheaf of $\mathcal{O}_S$-algebras. By definition, for any affine open subscheme $S_A \subset S$, $f^{-1}(S_A)$ is an affine scheme over A if and only if $X = Spec_S(\mathcal{A})$ (see [GME] §1.5.4).

An $\mathcal{O}_X$-module F on a scheme X is called *invertible* or a *line bundle* if there exists an open covering $\{Y_i\}_{i\in I}$ of X such that $F|_{Y_i} \cong \mathcal{O}_{Y_i}$ for each i. This is equivalent to $F_P \cong \mathcal{O}_{X,P}$ for all maximal points P. An $\mathcal{O}_X$-module F is called *quasi-coherent* if we have a sheaf exact sequence $\mathcal{O}_X^I \to \mathcal{O}_X^J \to F \to 0$, where $\mathcal{O}_X^I$ is the product of copies of $\mathcal{O}_X$ indexed by any set I. If we can take I and J finite, the $\mathcal{O}_X$-module F is called *coherent*.

Remark 4.19. *If $X = S_A$ is affine, for a quasi-coherent $\mathcal{O}_X$-module F, putting $M = F(X)$ we have $F(S_{A_f}) = M_f = A_f \otimes_A M$; thus, F is determined by M and sometimes written as $\widetilde{M}$. For any given*

A-module, we have a unique sheaf $\widetilde{M}$ such that $H^0(S_{A_f}, \widetilde{M}) = M_f$ (cf. [GME] *§1.2.3). Indeed, if we write $\mathbb{G}_a \otimes_A M$ for the A-module functor $R \mapsto R \otimes_A M$ in $\mathcal{C}_A$, we have $\widetilde{M}(U) = \mathrm{Hom}_{\mathcal{C}_A}(U, \mathbb{G}_a \otimes_A M)$.*

We write $QS(X)$ for the full subcategory in $S(X)$ of quasi-coherent $\mathcal{O}_X$-modules. The morphisms of this category are defined to be $\mathcal{O}_X$-linear morphisms in the category of (abelian) presheaves on X.

Exercise 4.20. *Let S be a scheme. Prove the following facts:*

1. *For a morphism of $\mathcal{O}_S$-modules $f : \mathcal{M} \to \mathcal{M}'$, $\mathrm{Ker}(f)(U) = \mathrm{Ker}(f : \mathcal{M}(U) \to \mathcal{M}'(U))$ is a $\mathcal{O}_S$-submodule of $\mathcal{M}$ (in particular, it is a sheaf).*
2. *For a set I of morphisms of $\mathcal{O}_S$-modules $f : \mathcal{M} \to \mathcal{M}'$, $\bigcap_{f \in I} \mathrm{Ker}(f)$ a a $\mathcal{O}_S$-submodule of $\mathcal{M}$ (in particular, it is a sheaf).*

If $X \xrightarrow{f} Y$ is a morphism of S-schemes, the direct image $F \mapsto f_*F$ gives a covariant functor from $QS(X)$ to $QS(Y)$. It has a left adjoint (contravariant) functor $f^* : QS(Y) \to QS(X)$. In other words, the cotravariant functor $G \mapsto \mathrm{Hom}_{QS(Y)}(G, f_*F)$ (for $F \in QS(X)$ and $G \in QS(Y)$)) is represented by a quasi-coherent sheaf f^*G over X; so, we have a canonical isomorphism (of bifunctors) $\mathrm{Hom}_{QS(Y)}(G, f_*F) \cong \mathrm{Hom}_{QS(X)}(f^*G, F)$. The sheaf f^*G is called the *inverse image* of G (see [GME] §1.5.3).

Exercise 4.21. *Using functoriality of "$\otimes$" and "Hom_A", check that if $X = S_{A'}$ and $Y = S_A$ and $G = \widetilde{M}$, we have $f^*G = (\widetilde{M \otimes_A A'})$.*

A morphism $X \xrightarrow{f} Y$ of B-schemes is a *finite* morphism if $f_*\mathcal{O}_X$ is a coherent $\mathcal{O}_Y$-module. If f is finite, for all field k over B, the fiber of the map $f_k : X(k) \to Y(k)$ is finite. If this property of finiteness of the fiber is satisfied for all fields k over B, f is called *quasi-finite morphism*.

Lemma 4.22. *If a B-morphism $X \xrightarrow{f} Y$ is finite, we have $X \cong Spec_Y(f_*\mathcal{O}_X)$; so, f is an affine morphism.*

Proof. Let $\mathcal{A} = f_*\mathcal{O}_X$. Then, $S_{\mathcal{A}}(T) = \mathrm{Hom}_{\mathcal{O}_Y\text{-alg}}(\mathcal{A}, g_*\mathcal{O}_T)$ for any Y-scheme $T \xrightarrow{g} Y$. In particular, $S_{\mathcal{A}}(X) = \mathrm{Hom}_{\mathcal{O}_Y\text{-alg}}(\mathcal{A}, \mathcal{A})$ has a canonical element $\mathrm{id}_{\mathcal{A}}$, which gives rise to a morphism $f' : X \to Spec_Y(\mathcal{A})$. For any maximal point $y \in Y(k)$, $\mathcal{A}_y$ is a $\mathcal{O}_{Y,y}$ module of finite type with $\mathcal{A}_y/\mathfrak{m}_y\mathcal{A}_y$ giving rise to $\mathcal{O}_{X,f^{-1}(y)}/\mathfrak{m}_y\mathcal{O}_{X,f^{-1}(y)}$. By Nakayama's lemma ([CRT] Theorem 2.2), we have $\mathcal{O}_{X,f^{-1}(y)} = \mathcal{A}_y$. Thus shows that f' gives rise to isomorphism of all stalks, and hence f' is an isomorphism. □

A scheme $X \in SCH_{/B}$ is *locally noetherian* if for any open affine subscheme S_A of X, A is a noetherian ring. If further the topological space of X is quasi compact, X is called *noetherian*. A morphism $X \xrightarrow{f} Y$ of B-schemes is *of finite type* if f is quasi compact and there exists an open covering $\{Y_i\}_i$ of Y such that $f^{-1}(Y_i)$ is covered with (finitely many) affine open subschemes S_{A_j} with A_j finitely generated over $\mathcal{O}_Y(Y_i)$. A B-morphism $X \xrightarrow{f} Y$ is called *proper* if (i) it is separated of finite type and (ii) for any Y-scheme T, the base-change $f_T : X \times_Y T \to T = Y \times_Y T$ is a closed map of the corresponding topological space. The valuative criterion of separatedness/properness is given as follows:

Proposition 4.23. *Suppose $f : X \to Y$ be a morphism of finite type with X noetherian in $SCH_{/B}$. Suppose we have a commutative diagram:*

$$\begin{array}{ccc} S_K & \xrightarrow{i_X} & X \\ \downarrow & & \downarrow \\ S_V & \xrightarrow[i_Y]{} & Y \end{array}$$

for valuation ring V with quotient field K in $ALG_{/B}$. Then f is separated (resp. proper) if and only if there exists at most one (resp. there exists a unique) morphism $i : S_V \to X$ making the above diagram commutative (after inserting diagonal arrow given by i).

See, for example, [ALG] II.4.7 for a proof.

Exercise 4.24. *Let $g : Y \to X$ and $f : X \to S$ be two morphisms. Prove that g is proper if $f \circ g$ is proper and f is separated.*

Corollary 4.25. *Let the notation be as in* Proposition 4.23. *If the morphism $f : X \to Y$ is finite, it is proper.*

Proof. We apply the above proposition. Since $\mathrm{Spec}(V)$ is irreducible reduced affine, we may assume that $X = \mathrm{Spec}(A')$ and $Y = \mathrm{Spec}(A)$ are irreducible and reduced. Since X is finite over Y, A' is integral over A. Then the diagram

$$\begin{array}{ccc} S_K & \xrightarrow{i_X} & X \\ \downarrow & & \downarrow \\ S_V & \xrightarrow[i_Y]{} & Y \end{array}$$

is equivalent to

$$\begin{array}{ccc} K & \xleftarrow{\underline{i}_X} & A' \\ \cup\uparrow & & \uparrow\cup \\ V & \xleftarrow[\underline{i}_Y]{} & A. \end{array}$$

Since the valuation ring is integrally closed in K, $\underline{i}_X$ maps A' into V and hence induces $S_V \to X$ with desired commutativity. □

4.7. **Sheaf of differential forms on schemes.** Let $S = S_A$ for a B-algebra A and R be an A–algebra. We have the structure morphism $X = S_R \to S$. For each R–module M, an A–derivation $\delta : R \to M$ is an A–linear map satisfying $\delta(fg) = f\delta(g) + g\delta(f)$ for all $f, g \in R$. We write $Der_A(R, M)$ for the R–module of A–derivations. Note that $\delta(1) = \delta(1 \times 1) = \delta(1) + \delta(1)$, and $\delta(1) = 0$. For $a \in A$, $\delta(a) = \delta(a1) = a\delta(1) = 0$ by the A–linearity of δ. Thus each A–derivation kills A. Conversely, if a derivation δ kills A, we see $\delta(ar) = a\delta(r) + r\delta(a) = a\delta(r)$, and δ is A–linear.

In algebraic geometry, there is no naive definition of differentiation. However we can think of derivations of the structure sheaf $\mathcal{O}_X = \widetilde{R}$ for each affine scheme $X = Spec(R)$. Thus if the covariant functor: $M \mapsto Der_A(R, M)$ from R–MOD to AB is representable by an R–module $\Omega_{X/S} = \Omega_{R/A}$, i.e. $Der_A(R, M) \cong \mathrm{Hom}_R(\Omega_{R/A}, M)$, we may think $\Omega_{R/A}$ as an analog of the cotangent bundle in Differential geometry. Indeed, we have

Proposition 4.26. *Let R be an A–algebra. The functor R–$MOD \ni M \mapsto Der_A(R, M) \in AB$ is representable by an R–module $\Omega_{R/A}$ with a universal derivation $d : R \to \Omega_{R/A}$, which is unique up to automorphisms of $\Omega_{R/A}$ over A. In other words, if $\delta : R \to M$ is an A–derivation, then there is a unique R–linear map $\phi : \Omega_{R/A} \to M$ such that $\delta = \phi \circ d$.*

Proof. Take the free R–module F generated by symbols $\{dr | r \in R\}$, and make a quotient by the R–submodule generated by $d(ar + a'r') - adr - a'dr'$ and $drr' - rdr' - r'dr$ for all $r, r' \in R$ and $a, a' \in A$. Then the resulted R–module $\Omega_{R/A}$ represents the functor.

There is another construction of $\Omega_{R/A}$. The multiplication $a \otimes b \mapsto ab$ induces an A–algebra homomorphism $m : R \otimes_A R \to R$ taking $a \otimes b$ to ab. We put $I = \mathrm{Ker}(m)$, which is an ideal of $R \otimes_A R$. Then we define $\Omega_{R/A} = I/I^2$. It is easy to check that the map $d : R \to \Omega_{R/A}$ given by $d(a) = a \otimes 1 - 1 \otimes a \mod I^2$ is a continuous A–derivation. Thus we have a morphism of functors: $\mathrm{Hom}_R(\Omega_{R/A}, ?) \to Der_A(R, ?)$ given by $\phi \mapsto \phi \circ d$. Since $\Omega_{R/A}$ is generated by $d(A)$ as A–modules, the above map is injective.

To show that $\Omega_{R/A}$ represents the functor, we need to show the surjectivity. Define $\phi : R \times R \to M$ by $(a, b) \mapsto a\delta(b)$ for $\delta \in Der_A(R, M)$. Then $\phi(ab, c) = ab\delta(c) = \phi(b, c)$ and $\phi(a, bc) = a\delta(bc) = ab\delta(c) = b\phi(a, c)$ for $a, c \in R$ and $b \in A$, and ϕ gives a continuous A–bilinear map. By the universality of the tensor product, $\phi : R \times R \to M$ extends to an A–linear map $\phi : R \otimes_A R \to M$. Now we see

that $\phi(a\otimes 1-1\otimes a)=a\delta(1)-\delta(a)=-\delta(a)$ and

$$\phi((a\otimes 1-1\otimes a)(b\otimes 1-1\otimes b))=\phi(ab\otimes 1-a\otimes b-b\otimes a+1\otimes ab)$$
$$=-a\delta(b)-b\delta(a)+\delta(ab)=0.$$

This shows that $\phi|_I$–factors through $I/I^2=\Omega_{R/A}$, and we have $\delta=\phi\circ d$, as desired. □

Let A' and R be A-algebras. Write $I=\mathrm{Ker}(R\otimes_A R\xrightarrow{a\otimes b\mapsto ab}R)$, $R'=A'\otimes_A A'$ and $I'=\mathrm{Ker}(R'\otimes_{A'}R'\xrightarrow{a\otimes b\mapsto ab}R')$. By the second construction of $\Omega_{R/A}$, we get

$$\Omega_{R/A}\otimes_R(A'\otimes_A R)\cong I/I^2\otimes_R R'\cong I'/I'^2\cong\Omega_{R'/A'}$$

canonically. Thus we get

Corollary 4.27. *Let $R\leftarrow A\to A'$ be morphisms of algebras. Then we have $\Omega_{R/A}\otimes_R(A'\otimes_A R)\cong\Omega_{A'\otimes_A R/A'}$.*

By the above proof of the proposition, any element of $\Omega_{R/A}$ can be written as $\sum_i f_i dr_i$ for some r_i and f_i in R. By Corollary 4.27, taking $A'=S^{-1}A$ for a multiplicative subset S in A, we get

$$S^{-1}\Omega_{R/A}=\Omega_{R/A}\otimes_R S^{-1}R=\Omega_{S^{-1}A\otimes_A R/S^{-1}A'}=\Omega_{S^{-1}R/S^{-1}A}. \tag{4.8}$$

Let S be a general scheme and $f:X\to S$ be a morphism of schemes. Let $S=\bigcup_i S_i$ ($S_i=Spec(A_i)$) be an open affine covering and $X=\bigcup_\alpha X_\alpha$ ($X_\alpha=Spec(R_\alpha)$) be an open affine covering of X so that f induces $f_\alpha:X_\alpha\to S_{i(\alpha)}$. Let Ω_α be the sheaf on X_α associated with the R–module $\Omega_{R_\alpha/A_{i(\alpha)}}$. Then by (4.8) and the universality, we have

$$\varphi_{\alpha\beta}:\Omega_\alpha|_{X_\alpha\cap X_\beta}\cong\Omega_\beta|_{X_\beta\cap X_\alpha}\quad\text{and}\quad\varphi_{\beta\gamma}\circ\varphi_{\alpha\beta}=\varphi_{\alpha\gamma}\quad\text{on}\quad X_\alpha\cap X_\beta\cap X_\gamma.$$

The sheaves Ω_α's glue together into a quasi-coherent sheaf $\Omega_{X/S}$. It is coherent if X is noetherian. This sheaf is called the sheaf of *differential* 1*–forms* on X over S. By this construction, Corollary 4.27 implies

Corollary 4.28. *Let $X\to Y\leftarrow Y'$ be morphism of schemes. Then we have $\Omega_{X/Y}\otimes_{\mathcal{O}_X}\mathcal{O}_{X\times_Y Y'}\cong\Omega_{X\times_Y Y'/Y'}$ canonically. In particular, for a point $y\in Y$, writing the fiber of X at y as X_y, we have $\Omega_{X/Y}\otimes_{\mathcal{O}_X}\mathcal{O}_{X_y}\cong\Omega_{X_y/y}$.*

Remark 4.29. Let $F:S(X)\to SETS$ or $SCH_{/X}\to SETS$ be a representable functor whenever X is affine. Here $SCH_{/X}$ is the category whose object is a pair (Y,f) made of a scheme Y and a morphism $f:Y\to X$ and whose morphisms are given by

$$\mathrm{Hom}_{SCH/X}((Y,f),(Z,g))=\left\{h\in\mathrm{Hom}_{SCH}(Y,Z)\middle|g\circ h=f\right\}.$$

Write C_X for the category of functors either from $S(X)$ or from $SCH_{/X}$ into $SETS$ depending on to which F belongs. We slightly generalize the notion of local functor from schemes to functors in C_X. A functor $F\in C_X$ is called *local* if it satisfies the following set theoretic exact sequence for any open covering $\{Y_i\}_{i\in I}$ of any object Y in C_X:

$$\mathrm{Hom}_{C_X}(Y,F)\to\prod_{i\in I}\mathrm{Hom}_{C_X}(Y_i,F)\rightrightarrows\prod_{i,j\in I}\mathrm{Hom}_{C_X}(Y_i\cap Y_j,F).$$

In other words, the functor F is local if F is determined by local data depending only on a (whatever) small neighbourhood of each point of X. If F is local and F restricted to $SCH_{/Y}$ or $S(Y)$ is a representable functor whenever the X-scheme Y is affine, then F is representable over $SCH_{/X}$ for an arbitrary scheme X. Indeed, taking an affine open covering $X=\bigcup_\alpha X_\alpha$, if W_α represents F restricted over X_α, we have a canonical isomorphism $\varphi_{\alpha\beta}:W_\alpha|_{X_\alpha\cap X_\beta}\cong W_\beta|_{X_\alpha\cap X_\beta}$ with $\varphi_{\beta\gamma}\circ\varphi_{\alpha\beta}=\varphi_{\alpha\gamma}$ on $X_\alpha\cap X_\beta\cap X_\gamma$ by the universality. Thus W_α glues together well into an object W which represents F over X.

In view of the above remark, the sheaf $\Omega_{X/S}$ represents a functor: $QS(X)\ni\mathcal{F}\mapsto Der_{\mathcal{O}_S}(\mathcal{O}_X,\mathcal{F})$, where $Der_{\mathcal{O}_S}(\mathcal{O}_X,\mathcal{F})$ is a sheaf generated by the presheaf $U\mapsto Der_{\mathcal{O}_S(f(U))}(\mathcal{O}_X(U),\mathcal{F}(U))$ for each open set U. Here $\mathcal{O}_S(f(U))=\varinjlim_{V\supset f(U)}\mathcal{O}_S(V)$. The $\mathcal{O}_X$-dual $\mathrm{Hom}_{\mathcal{O}_X}(\Omega_{X/Y},\mathcal{O}_X)$ is the *tangent sheaf* relative to X/Y. See [ALG] II.8 or [GME] §1.5.1 for more details.

Lemma 4.30. *For a finite flat S-morphism $f : X \to Y_{/S}$, f is étale if and only if $\Omega_{X/Y} = \mathrm{Coker}(f^* : f^*\Omega_{Y/S} \to \Omega_{X/S}) = 0$.*

Proof. Since f is affine by Lemma 4.22, we may assume that $S = \mathrm{Spec}(B)$, $X = \mathrm{Spec}(A')$ and $Y = \mathrm{Spec}(A)$. Suppose f is étale. Consider the exact sequence defining $\Omega_{A'/A}$:

$$0 \to I/I^2 \to A' \otimes_A A'/I^2 \xrightarrow{a\otimes b\mapsto ab} A' \to 0.$$

The map $A' \ni a \mapsto a \otimes 1 \in A' \otimes_A A'/I^2$ gives the section of multiplication $a \otimes b \mapsto ab$; so, we have $A' \otimes_A A'/I = A' \oplus I/I^2 = A' \oplus \Omega_{A'/A}$ with projection π to $\Omega_{A'/A}$. Note that $\mathrm{Hom}_{ALG_{/A}}(A', A' \otimes_A A'/I^2) \cong Der_A(A', \Omega_{A'/A})$ by $\phi \mapsto \pi \circ \phi$. Since I is a square 0 ideal of $A' \otimes_A A'/I^2$, by étaleness, $Der_A(A', \Omega_{A'/A}) = \{0\}$. Thus $\Omega_{A'/A} = 0$. The fact $\Omega_{X/Y} = \mathrm{Coker}(f^* : f^*\Omega_{Y/S} \to \Omega_{X/S})$ is a restatement of the fundamental exact sequence (e.g., [CRT] Theorem 25.1 or [GME] Proposition 1.5.4).

Conversely, assume that $\Omega_{A'/A} = 0$. We prove étaleness by supposing that we have A-algebra homomorphisms $\phi, \varphi : A' \to E$ extending an A-algebra homomorphism $A' \to E/J$ for a square 0 ideal J of an A-algebra E. This liftability basically follows comes from the natural map $A' = A' \otimes_A A' \to A' \otimes_A A' \otimes_A E = A' \otimes_A E$ which satisfies by $\Omega_{A'/A} = 0$ descent data for getting $A' \to E$ (see [CRT] §28 or [EGA] IV.22). Define an A-algebra homomorphism $\Phi : A' \otimes_A A' \to E$ by $\Phi(a \otimes b) = \phi(a)\varphi(b)$. Since $\phi \mod J = \varphi \mod J$, we have $\Phi(I) \subset J$ and $\Phi(d(a) \cdot d(a')) = 0$ for $d(a) = a \otimes 1 - 1 \otimes a$ by computation. Thus Φ induces $\Omega_{A'/A} = I/I^2 \to J$. Since $\Omega_{A'/A} = 0$, $\Phi|_I = 0$. Since $\phi(a) - \varphi(a) = \Phi(d(a)) = 0$, we get $\varphi = \phi$; so, A'/A is étale. □

4.8. **Scheme and variety.** In §4.6, we defined a B-scheme as a local functor in $\mathcal{C}_B$ covered by open affine subschemes. Here is a more down-to-earth definition. Let $f : S_1 \to S$ and $g : S_2 \to S$ be morphisms in $\mathcal{C}_B$. Recall

$$S_1 \times_S S_2(R) = \{(x, y) \in S_1(R) \times S_2(R) | f_R(x) = g_R(y)\},$$

as an object in $\mathcal{C}_B$. If T is the fourth functor with morphisms $f' : T \to S_1$ and $g' : T \to S_2$ such that $g \circ g' = f \circ f'$, we have a unique morphism $h : T \to S_1 \times_S S_2$ given by $h(x) = (f'(x), g'(x))$ such that $f \circ h = g' \circ h$. In this sense, $S_1 \times_S S_2$ satisfies the universality of the fibered product over S. Now a finitely presented quasi compact *B-scheme* $S_{/B}$ is a covariant functor from the category $ALG_{/B}$ of B-algebras into $SETS$ such that

(1) We have finitely many affine schemes $S_i = \mathrm{Spec}(B_i)$ for finitely presented B-algebras B_i with inclusion $S_i \hookrightarrow S$ such that $S = \bigcup_i S_i$ (i.e., $S(k) = \bigcup_i S_i(k)$ for all fields k over B);
(2) $S_i \cap S_j = S_i \times_S S_j$ is Zariski open in S_i and S_j for all pairs (i, j) of indices (so, $\{S_i\}$ is an open covering of S).

In practice, the scheme S is often constructed by gluing the affine schemes S_i, and each $\phi \in S(R)$ is determined by its "restriction" ϕ_i to S_i in the following way: For each B-algebra R, we require the local property that $\phi \in S(R)$ be determined by the tuple

$$\{\phi_i \in \mathrm{Hom}(S_R \times_S S_i, S_i)\}$$

such that ϕ_i and ϕ_j induce an identical morphism of $S_R \times_S S_i \times_S S_j \to S_i \times_S S_j$ (ignoring the indices i with $S_R \times_S S_i = \emptyset$); then, we may define

$$S(R) = \bigcup_i S_i := \left\{ (\phi_i)_i \middle| \begin{array}{l} \phi_i \in \mathrm{Hom}(S_R \times_S S_i, S_i), \text{ and} \\ \phi_i \text{ and } \phi_j \text{ coincide on } S_R \times_S S_i \times_S S_j \text{ for all } i, j \end{array} \right\}.$$

Thus S is a local functor covered with "finitely" many affine open subschemes (this finiteness is "quasi-compacity" as all affine schemes are quasi-compact; see [GME] §1.2.2).

A *B-morphism* $\phi : S \to T$ of schemes is a morphism in $\mathcal{C}_B$; so, the category of B-schemes $SCH_{/B}$ is a full subcategory of $\mathcal{C}_B$. The category $SCH_{/B}$ contains the category of affine B-schemes as a full subcategory (by Lemma 4.16).

Let $\phi : S \to T$ be a morphism of B-schemes. Covering T by affine schemes $\{S_{A'_i}\}_i$ for B-algebras A'_i, that is, $T = \bigcup_i S_{A'_i}$. Then $\phi^{-1}(S_{A'_i})$ can be covered again by suitable affine schemes $S_{A_{ij}}$ for A'_i-algebras A_{ij}. If $S_{A_{ij}}$ is smooth (resp. étale) over $S_{A'_i}$ for all i and j, we call S is *smooth* (resp. *étale*) over T.

A separated geometrically reduced scheme V of finite type over a field k is called a (algebraic) *variety* in this course. Here the word "geometrically reduced" means that $\overline{V} := V \times_k \overline{k}$ for an algebraic closure $\overline{k}$ of k is reduced (i.e., $\mathcal{O}_{\overline{V}}$ does not have nontrivial nilpotent elements). We do not include connectedness in the notion of "varieties". If $V_{/k}$ is an irreducible variety, for any dense affine open subscheme $S_A \subset V$, the Krull dimension $\dim A$ is independent of the choice of the affine open subscheme. We put $\dim V = \dim A$. A variety is equidimensional if all irreducible components have equal dimension, written as $\dim V$. As already remarked, a variety $V_{/k}$ (of equidimension n) over a perfect field k is smooth over k if and only if its stalk at all maximal point has completion isomorphic to $(\mathcal{O}_{V,x}/\mathfrak{m}_x)[[X_1, \ldots, X_n]]$ (hence, also, if and only if $\mathcal{O}_{V,x}$ is regular for all maximal points x). A *normal* variety is a variety V whose stalk $\mathcal{O}_{V,x}$ is integrally closed in its total quotient ring for any closed point (hence any point) of V. In particular, a smooth variety is normal (as power series rings over a field is normal). A dimension one variety is called a *curve*. Since any normal noetherian domain of dimension 1 is a discrete valuation ring (cf. [CRT] Theorem 11.2), a curve is smooth over a perfect field k if and only if it is normal.

4.9. **Projective schemes.** In order to give a typical example of non-affine schemes, we introduce graded algebras over a commutative algebra B. A graded algebra R over an algebra B is a direct sum $\bigoplus_d R_d$ for a B-subalgebra R_0 and R_0-modules R_d for integers d such that $R_n R_m \subset R_{m+n}$. A B-morphism $\phi : R \to R'$ of graded B-algebras R and R' is a B-algebra homomorphism with $\phi(R_d) \subset R'_d$ for all d. An element x of a graded algebra R is called homogeneous of degree d if $x \in R_d$. The polynomial ring $B[T]$ is a graded algebra with $B[T]_d = T^d B$ for $d \geq 0$ and $B_d = 0$ for negative d. More generally, the polynomial ring $B[T_1, \ldots, T_n]$ of n variables is a graded algebra such that each monomial of degree d is homogeneous of degree d.

If $x \in R$ is homogeneous of degree $d \neq 0$, then $R[\frac{1}{x}]$ is a graded ring by putting $R[\frac{1}{x}]_n = \sum_{jd+m=n} x^j R_m$ (in other words, for a homogeneous element $a \in R$, $\deg(\frac{a}{x^j}) = \deg(a) - jd$). Suppose that the base ring B is noetherian. If a graded algebra R is noetherian, then there are finitely many homogeneous elements $x_0, \ldots, x_n$ (of degree $d_0, \ldots, d_n$, respectively) in R which generate the B-algebra R. Thus the algebra homomorphism $B[T_0, \ldots, T_n] \to R$ sending a polynomial $P(T_0, \ldots, T_n)$ to $P(x_1, \ldots, x_n) \in R$ is a surjective algebra homomorphism.

Write $D_i = \mathrm{Spec}(B[T_0, \ldots, T_n][\frac{1}{T_i}]_0)$. Since we have

$$B[T_0, \ldots, T_n][T_i^{-1}]_0 \cap B[T_0, \ldots, T_n][T_j^{-1}]_0 = B[T_0, \ldots, T_n][(T_i T_j)^{-1}]_0$$

for $i \neq j$ (in $B[T_0, \ldots, T_n][\frac{1}{T_0}, \frac{1}{T_1}, \ldots, \frac{1}{T_n}]_0$), we identify $D_i \cap D_j$ with $\mathrm{Spec}(B[T_0, \ldots, T_n][(T_i T_j)^{-1}]_0)$ canonically. In this way, we can define the projective space of dimension n by $\mathbf{P}^n = \bigcup_{j=0}^n D_j$, which is not affine. If A is a B-algebra which is either a field or a valuation ring, by definition, we have

$$\mathbf{P}^n(A) \cong \{(x_0, \ldots, x_n) | x_j \in A^\times \text{ for at least one } j\}/A^\times.$$

If R is a general noetherian graded B-algebra, taking a finite set of homogeneous generators $x_0, \ldots, x_n$ of degree 1, taking the surjective B-algebra homomorphism $B[T_0, \ldots, T_n]$ sending T_j to x_j, the algebra homomorphism induces a surjection $B[T_0, \ldots, T_n][T_i^{-1}]_0 \to R[x_i^{-1}]_0$, which in turn gives rise to a subscheme $V_i = \mathrm{Spec}(R[x_i^{-1}]_0)$ of D_i. Then we define $\mathrm{Proj}(R) = \bigcup_i V_i$. We can generalize this definition to any graded B-algebra R generated by finitely many homogeneous elements (not necessarily of degree 1; see [GME] Section 1.3), because $\mathrm{Proj}(R) = \mathrm{Proj}(R^{(n)})$ for $R^{(n)} = \bigoplus_d R_{nd}$. If $R^\times$ contains a homogeneous element of nonzero degree, we have $\mathrm{Proj}(R) \cong \mathrm{Spec}(R_0)$ by definition (compare with [GME] Lemma 1.3.1); however, if R has no negative degree elements, $\mathrm{Proj}(R)$ is not affine.

If we can realize a B-scheme X as a closed subscheme of $\mathbf{P}^n$ (i.e., if we have a closed immersion $X \hookrightarrow \mathbf{P}^n_{/B}$), X is called B-projective. More generally, if we can realize a morphism $f : X \to Y$ so that it factors through $\mathbf{P}^n_Y = \mathbf{P}^n_{/B} \times_{S_B} Y$, f is called a *projective morphism*. This is equivalent to have an invertible sheaf $\mathcal{L}$ with generators $x_0, \ldots, x_n$ on X whose graded algebra $R = \bigoplus_{n \geq 0} H^0(X, \mathcal{L}^{\otimes n})$ has $\mathrm{Proj}(R)$ isomorphic to X, where $x_0, \ldots, x_n$ are regarded as homogeneous generators of R. The morphism $X \to \mathrm{Proj}(R)$ is the canonical one described in [GME] §1.5.5. If $(X, f : X \to Y)$ is

isomorphic in $SCH_{/Y}$ to an open subscheme $(U, g : U \to Y)$ of a closed subscheme $(C, h : C \to Y)$ of $\mathbf{P}^n_{/Y}$ (i.e., $U \xrightarrow[\subset]{\text{open}} C$ as Y-schemes), f is called *quasi projective*.

Exercise 4.31. *Prove that any projective morphism $X \to Y$ of B-schemes is a proper morphism* (hint: Use Proposition 4.23).

Exercise 4.32. *Suppose that B is an algebraically closed field k. Prove that for any k-morphism f from $\mathbf{P}^n_{/k}$ into an affine scheme S, $f_K : \mathbf{P}^n(K) \to S(K)$ has one point image for any field K/k. Using this fact, show further that $\mathbf{P}^n$ is not affine if $n \geq 1$.*

Similar to the relative spectrum $Spec_S(\mathcal{A})$ for a quasi-coherent $\mathcal{O}_S$-algebra, we can construct relative "Proj" for a quasi-coherent graded $\mathcal{O}_S$-algebras $\mathcal{A} = \bigoplus_n \mathcal{A}_n$. We assume that $\mathcal{A}$ is finitely generated over $\mathcal{A}_0$ and $\mathcal{A}_0$ is a coherent $\mathcal{O}_S$-algebras (so, $\mathcal{A}_n$ is also coherent). Then for any affine open $\mathrm{Spec}(R) \subset S$, $\mathcal{A}(\mathrm{Spec}(R))$ is a graded algbera of finite type over R, and we have $\mathrm{Proj}(\mathcal{A}(\mathrm{Spec}(R))$. Plainly if we cover S by affine open subscheme $\mathrm{Spec}(R_i)$, $\{\mathrm{Proj}(\mathcal{A}(\mathrm{Spec}(R_i)))\}_i$ glue naturally over S, giving rise to a projective S-scheme $Proj_S(\mathcal{A}) \to S$.

4.10. **Cartier divisors.** Let S be a locally noetherian scheme. We mean by a *projective smooth curve* of genus g over S a morphism of schemes $f : C \to S$ satisfying the following conditions:

(C0) f is projective of relative dimension 1 and is fiber by fiber connected;
(C1) f is smooth;
(C2) The sheaf $f_*\Omega_{C/S}$ is a locally free $\mathcal{O}_S$–module of rank g.

This means that for each geometric point $s \in S$, its fiber $C_s = f^{-1}(s)$ is reduced, connected, of dimension 1 and $\dim_{k(s)} H^0(\Omega_{C/S} \otimes k(s)) = g$. The number g in (C3) is called the *genus* of $C_{/S}$. When $C_{/S}$ is not smooth, the differential sheaf $\Omega_{C/S}$ is often not locally free.

Hereafter we always assume that $C_{/S}$ is a projective smooth curve of genus g. We recall the definition of invertible sheaves. A sheaf $\mathcal{L}$ is called *invertible*, if it is locally free of rank 1 over $\mathcal{O}_C$. We define a sheaf $Hom_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C)$ by $Hom_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C)(U) = \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{O}_U)$ for each open set U. It is easy to see that $Hom_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C)$ is a sheaf. In particular, $Hom_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C)$ is invertible if $\mathcal{L}$ is invertible. Now we see that

$$Hom_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C) \otimes \mathcal{L} \cong \mathcal{O}_C$$

via $\phi \otimes l \mapsto \phi(l)$. Thus the set $\mathrm{Pic}(C)$ of isomorphism classes of all invertible sheaves is a group under the tensor product, whose identity is given by the class of $\mathcal{O}_C$. In particular, we write $\mathcal{L}^{-1} = Hom_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C)$.

An effective *relative Cartier divisor* D in $C_{/S}$ ([AME] Chapter 1 and [EGA] IV.21.15) is a closed subscheme $D \overset{\iota}{\subset} C$ such that

(D1) $D_{/S}$ is flat ($\Rightarrow f_*(\mathcal{O}_D)$ is a locally free sheaf over $\mathcal{O}_S$);
(D2) The sheaf of ideals $I(D)$ defining D in $\mathcal{O}$ is invertible.

Then we have an exact sequence

$$0 \longrightarrow I(D) \longrightarrow \mathcal{O}_C \longrightarrow \mathcal{O}_D \longrightarrow 0. \tag{4.9}$$

By definition, $I(D)$ is an invertible sheaf. For each open $U \subset C$, we may regard $I(D)(U)$ as an ideal of $\mathcal{O}_C(U)$; so, we may take its inverse: $I(D)^{-1}$ (which is a fractional $\mathcal{O}_C(U)$–ideal in the function field of C). The sheaf $I(D)^{-1}$ is invertible. We have a natural morphism: $I(D)^{-1} \otimes I(D) \to \mathcal{O}_C$ and $I(D)^{-1}_x \otimes I(D)_x = I(D)_x \otimes Hom_{\mathcal{O}_C}(I(D)_x, \mathcal{O}_{C,x}) = \mathcal{O}_{C,x}$. Thus $I(D)^{-1} \otimes I(D) = \mathcal{O}_C$. Tensoring $I(D)^{-1}$ with the sequence (4.9), we have another exact sequence:

$$0 \longrightarrow \mathcal{O}_C \longrightarrow I(D)^{-1} \longrightarrow \mathcal{O}_D \otimes_{\mathcal{O}_C} I(D)^{-1} \longrightarrow 0.$$

Since $\mathcal{O}_D$ is flat over S, the sheaf $\mathcal{O}_D \otimes_{\mathcal{O}_C} I(D)^{-1}$ is again flat over S supported on D. If we are given an exact sequence of the above type:

$$0 \to \mathcal{O}_C \xrightarrow{\ell} \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{O}_C \to 0 \text{ with invertible } \mathcal{L} \text{ and } \mathcal{L}/\mathcal{O}_C \text{ flat over } S, \tag{4.10}$$

we have a global section $\ell \in \mathcal{L}$ as above; in other words multiplication: $x \mapsto \ell x$ by ℓ gives the inclusion $\mathcal{O}_C \hookrightarrow \mathcal{L}$.

Let $\mathrm{Supp}(\mathcal{L}/\mathcal{O}_C) = \{x \in C | (\mathcal{L}/\mathcal{O}_C)_x \neq 0\}$, which is a closed subset of C. We now try to recover the data of D out of (4.10). We put $|D| = \mathrm{Supp}(\mathcal{L}/\mathcal{O}_C)$, where $|D|$ indicates the underlying topological space. We have a local commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_{C,x} & \xrightarrow{\ell} & \mathcal{L}_x & \longrightarrow & \mathcal{L}_x/\mathcal{O}_{C,x} & \longrightarrow & 0 \\ & & \| & & \wr\| & & \wr\| & & \\ 0 & \longrightarrow & \mathcal{O}_{C,x} & \xrightarrow[\ell]{} & \mathcal{O}_{C,x} & \longrightarrow & \mathcal{O}_{C,x}/\ell\mathcal{O}_{C,x} & \longrightarrow & 0. \end{array}$$

Tensoring by $k(x) = \mathcal{O}_{C,x}/\mathfrak{m}_x$ for the maximal ideal $\mathfrak{m}_x$, we get

$$k(x) \xrightarrow{\ell} k(x) \longrightarrow \begin{Bmatrix} 0 & \text{if } x \notin |D| \\ k(x) & \text{if } x \in |D| \end{Bmatrix} \longrightarrow 0.$$

This shows $|D| = \{x \in C | \ell(x) = 0\}$. We know

$$I(D) = \mathcal{L}^{-1} \quad \text{and} \quad \mathcal{O}_D = (\mathcal{L}/\mathcal{O}_C) \otimes_{\mathcal{O}_C} \mathcal{L}^{-1}.$$

We can recover all the data defining the divisor D out of the pair $(\mathcal{L}, \ell)$. Therefore we have

$$\begin{aligned} (4.11) \quad &\{\text{Effective Cartier divisors on } C_{/S}\} \\ &\cong \left[(\mathcal{L}, \ell) \middle| \mathcal{L}\text{: invertible, } \ell \in \Gamma(C, \mathcal{L}),\ f_*(\mathcal{L}/\ell\mathcal{O}_C) \text{ is locally } \mathcal{O}_S\text{–free}\right], \end{aligned}$$

where $[\ \ ] = \{\ \ \}/\cong$: the set of isomorphism classes of pairs $(\mathcal{L}, \ell)$. Hereafter we identify the two sides of (4.11).

If $U = \mathrm{Spec}(A)$ is affine open in C, and if $\mathcal{L}|_U \cong \mathcal{O}_U$, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{O}_U & \xrightarrow{\ell} & \mathcal{L}|_U & \longrightarrow & (\mathcal{L}/\mathcal{O}_C)|_U & \to & 0 \\ & & \| & & \wr\| & & \wr\| & & \\ 0 & \to & \widetilde{A} & \xrightarrow[\ell]{} & \widetilde{A} & \longrightarrow & \widetilde{A}/\ell\widetilde{A} & \to & 0. \end{array}$$

Thus $D \cap U = \mathrm{Spec}(A/\ell A)$, and $A/\ell A$ is flat over B, where $\mathrm{Spec}(B)$ is affine open in S such that $f^{-1}(\mathrm{Spec}(B)) \supset U$.

If D and D' are effective Cartier divisors, we define $D + D'$ by one of the following equivalent conditions:

(a) $D \leftrightarrow (\mathcal{L}, \ell)$ and $D' \leftrightarrow (\mathcal{L}', \ell') \Rightarrow D + D' \leftrightarrow (\mathcal{L} \otimes \mathcal{L}', \ell \otimes \ell')$;
(b) $D \leftrightarrow I(D)$ and $D' \leftrightarrow I(D') \Rightarrow D + D' \leftrightarrow I(D) \otimes I(D') = I(D)I(D')$;
(c) $D \leftrightarrow (U_i = \mathrm{Spec}(A_i), \ell|_{U_i})$ and $D' \leftrightarrow (U_i = \mathrm{Spec}(A_i), \ell'|_{U_i}) \Rightarrow D + D' \leftrightarrow (U_i = \mathrm{Spec}(A_i), \ell\ell'|_{U_i})$,

where $C = \bigcup_i U_i$ is an affine open covering. For each effective divisor $D = (\mathcal{L}, \ell)$, we write $\mathcal{L}(D)$ for $\mathcal{L}$. Then $\mathcal{L}(D) \cong I(D)^{-1}$.

We now claim that for three effective divisors D, D' and D'',

$$(4.12) \qquad \textit{if } D + D' = D + D'', \textit{ then } D' = D''.$$

Proof. Since the assertion is local, we may assume that D, D' and D'' are on $\mathrm{Spec}(A)$ defined by non-zero-divisors $f, g, h \in A$. Thus $D = \mathrm{Spec}(A/fA)$, $D' = \mathrm{Spec}(A/gA)$ and $D'' = \mathrm{Spec}(A/hA)$. The assumption: $D + D' = D + D''$ implies $fg \equiv fh \mod A^\times$. By the flatness of A/fA, f is not a zero divisor. Dividing the above equation by f, we get the identity of principal ideals: $(g) = (h)$, which implies $D' = D''$. □

By (4.12), we can think of the group $\mathrm{Div}(C_{/S})$ formally generated by effective Cartier divisors relative to S. In other words, $\mathrm{Div}(C_{/S})$ is the quotient module of $\oplus_{D>0}\mathbb{Z}D$ by the submodule generated by

$$\{D - D' - D'' | D = D' + D'' \text{ as effective divisors}\}.$$

Each $D \in \mathrm{Div}(C_{/S})$ can be written as $D' - D''$ for two effective divisors D' and D''. Then we can define $\mathcal{L}(D)$ to be $\mathcal{L}(D') \otimes_{\mathcal{O}_C} \mathcal{L}(D'')^{-1}$. As easily seen, this is well defined independent of the choice of D' and D''. Then the map: $D \mapsto \mathcal{L}(D)$ gives rise to a group homomorphism: $\mathrm{Div}(C_{/S}) \longrightarrow \mathrm{Pic}(C)$, where $\mathrm{Pic}(C)$ is the group of isomorphism classes of invertible sheaves of C.

If $S = \mathrm{Spec}(k)$ for an algebraically closed field k, k-rational effective divisors can be identified with positive linear combinations of points on $C(k)$. We have $\deg(\sum_P m_P[P]) = \sum_P m_P$. We can thus think of the group $\mathrm{Div}(C/k)$ of all formal linear combinations (including negative coefficients) of points on C. Then $\deg : \mathrm{Div}(C/k) \to \mathbb{Z}$ is a well-defined homomorphism given by the above formula. In particular, for any divisor $D \in \mathrm{Div}(C/k)$, we have $\mathcal{L}(D) = \mathcal{L}(D_+) \otimes \mathcal{L}(D_-)^{-1}$ writing $D = D_+ - D_-$ for effective divisors D_+ and D_-, and we can verify $\deg(\mathcal{L}(D)) = \deg(D)$.

4.11. **Picard schemes.** For any scheme X, we define $\mathrm{Pic}(X)$ as the set of all isomorphism classes of invertible sheaves on X. The association $X \mapsto \mathrm{Pic}(X)$ is a contravariant functor by the pullback of invertible sheaves, and $\mathrm{Pic}(X)$ is actually a group by tensor product. In short, $\mathrm{Pic} : SCH \to AB$ is a contravariant group functor.

Let $(C, \mathbf{0}_C) \xrightarrow{f} S$ be a pointed curve. We define, for each S-scheme $\phi : T \to S$,

$$\mathrm{Pic}_{C/S}(T) = \mathrm{Pic}(C_T)/f_T^* \mathrm{Pic}(T).$$

Since $\mathbf{0}_C$ is a section of f, $\mathbf{0}_C^* : \mathrm{Pic}(C) \to \mathrm{Pic}(S)$ is a section of $f^* : \mathrm{Pic}(S) \to \mathrm{Pic}(C)$. Thus we have another expression:

$$\mathrm{Pic}_{C/S}(T) = \mathrm{Ker}(\mathbf{0}_{C_T}^* : \mathrm{Pic}(C_T) \to \mathrm{Pic}(T)).$$

Since invertible sheaves are determined by its restriction to open covering, the functor Pic is local (in the sense of (4.7)), and hence its subfunctor $\mathrm{Pic}_{C/S}$ is local, giving a local group functor from $SCH_{/S}$ into AB.

Lemma 4.33. *Suppose that C is smooth irreducible and $S = \mathrm{Spec}(k)$ for an algebraically closed field k. Then there is a canonical group isomorphism* $\mathrm{Div}(C/k)/\{\mathrm{div}(f) | f \in k(C)^\times\} \cong \mathrm{Pic}_{C/k}(k)$.

Proof. Then for any open affine subscheme $U \subset C$ and a divisor $D = \sum_P m_P[P] \in \mathrm{Div}(C/k)$, we can think of a sheaf $U \mapsto \{f \in \mathrm{Hom}_S(U, \mathbf{P}^1) | v_P(f) \geq -D\}$, which is the invertible sheaf $\mathcal{L}(D)$. Thus we have a group homomorphism $\mathrm{Div}(C/k) \to \mathrm{Pic}_{C/k}(k)$. Note that $\mathrm{Hom}_S(U, \mathbf{P}^1) = k(C)$ as long as $U \neq \emptyset$. Thus $U \mapsto \mathrm{Hom}_S(U, \mathbf{P}^1)$ is a constant sheaf $\underline{k(C)}$ with $\underline{k(C)}(U) = k(C)$. For any invertible sheaf $\mathcal{L}$, therefore $\mathcal{L} \otimes_{\mathcal{O}_C} \underline{k(C)} = \underline{k(C)}$, and hence $\mathcal{L}$ is a subsheaf of $\underline{k(C)}$. For each maximal P, $\mathcal{O}_{C,P}$ is a discrete valuation ring with uniformizer t_P (i.e., t_P generates the maximal ideal of $\mathcal{O}_{C,P}$) as C is smooth. Then $\mathcal{L}_P \subset k(C)_P = k(C)$ is of the form $\mathcal{L}_P = t_P^{-m_P}\mathcal{O}_{C,P}$ as $\mathcal{L}_P \cong \mathcal{O}_P$ as $\mathcal{O}_P$-module. Thus putting $D = \sum_P m_P[P]$, we have $\mathcal{L} \cong \mathcal{L}(D)$. In other words, $\mathrm{Div}(C/k) \to \mathrm{Pic}_{C/k}(k)$ is surjective. If $\mathcal{L}(D) \cong \mathcal{L}(D')$, then the isomorphism is induced by multiplication by an element of $k(C)^\times$, and hence we get the desired isomorphism. □

Suppose irreducibility of S. For $r \in \mathbb{Z}$, we put $\mathrm{Pic}^r_{C/S}(T) = \{\mathcal{L} \mathrm{Pic}_{C/S}(T) | \deg \mathcal{L}) = r\}$.

5. Jacobians of Stable Curves

In this section, we first construct Picard/Jacobian schemes for non-singular smooth curves over a field, though our statement and definition cover general case of over an integral scheme S. Then we generalize the construction, essentially, to stable curves, although we give details only for curves whose bad reduction at some fibers are union of two curves intersecting transversally. At the end, we study functorial properties of jacobians.

5.1. **Non-singular curves.** Let $f : C \to S$ be the smooth projective curve of genus $g \geq 2$. We suppose that $C(S) \neq \emptyset$. We follow Milne's treatment in [Mi1] in our construction of the jacobian of C over S. The method is to cover $\mathrm{Pic}^r_{C/S}$ by open subsets of a symmetric product of r copies of the curve and find a section of the covering for sufficiently large r, where $\mathrm{Pic}^r_{C/S}$ is the relative Picard functor of degree r line bundles over $C_{/S}$ defined as in Section 4.11:

$$\mathrm{Pic}^r_{C/S}(T) = \left\{\mathcal{L} \in \mathrm{Pic}(C \times_S T)/f_T^* \mathrm{Pic}(T) \middle| \deg(\mathcal{L}) = r\right\}$$

for $f_T : C \times_S T \to T$. An effective Cartier divisor D over $C_{/T} = C \times_S T$ is called *split* over $T_{/S}$ if $D = \sum_P m_P[P]$ for $P \in C(T)$. If $D = (\mathcal{L}, \ell)$ is an effective Cartier divisor on $C_{/S}$, then tensoring the exact sequence

$$0 \to \mathcal{O}_C \xrightarrow{\ell} \mathcal{L} \to \mathcal{O}_D \to 0$$

with $\mathcal{O}_T$ over $\mathcal{O}_S$, we get another exact sequence:

$$0 \to \mathcal{O}_{C/T} \xrightarrow{\ell\otimes 1} \mathcal{L}\otimes_{\mathcal{O}_S}\mathcal{O}_T \to \mathcal{O}_D\otimes_{\mathcal{O}_S}\mathcal{O}_T \to 0,$$

where the injectivity of $\ell\otimes 1$ follows from the local freeness of $\mathcal{O}_D$ over S (because $\mathcal{L}$ is then locally a direct sum of $\mathcal{O}_D$ and $\mathcal{O}_T$). The pullback divisor $D_T = (\mathcal{L}\otimes_{\mathcal{O}_S}\mathcal{O}_T, \ell\otimes 1)$ is an effective Cartier divisor on $C_{/T}$. This correspondence $D \mapsto D_T$ preserves the degree of divisors and makes an association $\mathrm{Div}^r_{C/S} : SCH_{/S} \to SETS$ (sending T to the set of all effective Cartier divisors on $C_{/T}$ of degree r) into a contravariant functor.

We consider the r–fold fiber product: $C^r = \overbrace{C\times_S C\times_S\cdots\times_S C}^{r}$. Permuting the factors, the symmetric group $\mathfrak{S} = \mathfrak{S}_r$ of degree r acts on C^r. The action obviously has fixed points, for example, the diagonal image of C. For any affine open $U \subset C$, U^r is an affine open in C^r stable under $\mathfrak{S}$. For a given finite set of geometric points $x_1,\dots,x_r$ in C, we can choose an affine open U of C containing all the points $x_1,\dots,x_r$, and affine open subsets of the form U^r covers C^r. Writing $U = \mathrm{Spec}(A)$, then $U^r = \mathrm{Spec}(A^{\otimes r})$ for $A^{\otimes r} := \overbrace{A\otimes_{\mathcal{O}_S} A\otimes\cdots\otimes_{\mathcal{O}_S} A}^{r}$. The symmetric group $\mathfrak{S}$ acts on $A^{\otimes r}$ by permuting factors. The quotient scheme $U^r/\mathfrak{S} = \mathrm{Spec}((A^{\otimes r})^{\mathfrak{S}})$ satisfies $U^r/\mathfrak{S}(k) = U(k)^r/\mathfrak{S}$ for all geometric points $\mathrm{Spec}(k) \hookrightarrow S$. Gluing together, $U^r/\mathfrak{S}$, we get the quotient scheme $C^{(r)} = C^r/\mathfrak{S}$. See [GME] Proposition 1.8.4 for a more theoretical treatment of quotient scheme by a group action. We call $C^{(r)}$ the symmetric r-th power of C.

We now claim that the formation of the quotient commutes with base-extension and that $C^{(r)}$ is actually a geometric quotient. Outside the fixed point of $\mathfrak{S}$, the covering $C^r \to C^{(r)}$ is étale, so the quotient process (outside the fixed points) commutes with base extension. We take a closed point of C^r which is fixed by non-trivial automorphism of $\mathfrak{S}$. Thus we assume that the point $x = (P_1,\dots,P_r)$ has several P_i's repeated. After shrinking S to an open affine subscheme and by an étale faithfully flat base extension of S, we may assume that $P_i \in C(S)$. We may assume further that $x = (\overbrace{P,P,\dots,P}^{j}, Q_{j+1},\dots,Q_r)$ with P and the Q_k's all distinct. Then the stabilizer of the point can be identified with $\mathfrak{S}_j$, and $\mathfrak{S}_j$ acts on the completed stalk: $\widehat{\mathcal{O}}_{C^r,x} = A[[T_1,\dots,T_j,T_{j+1},\dots,T_r]]$ $(A = \mathcal{O}_{S,f(x)})$ by permuting $T_1,\dots,T_j$. Writing $\pi : C^r \to C^{(r)}$ for the projection, we know from this that

$$\mathcal{O}_{C^{(r)},\pi(x)} = A[[\sigma_1,\dots,\sigma_j,T_{j+1},\dots,T_r]]$$

for the fundamental symmetric polynomials σ_j of j–variables $T_1,\dots,T_j$. This shows that the formation of $C^{(r)}$ commutes with base-extension, and π is locally-free of rank $r!$. Thus $C^{(r)}$ is truly the quotient of C^r by $\mathfrak{S}$ (such a quotient is called by Mumford a geometric quotient; see, [GME] §1.8.3). We note that the discriminant ideal $\mathfrak{d}_{X/Y}$ for $X = \widehat{\mathcal{O}}_{C^r,x}$ and $Y = \widehat{\mathcal{O}}_{C^{(r)},\pi(x)}$ is free, generated by

$$\prod_{0<m<n<j}(T_m - T_n)^2.$$

By this we can conclude that $C^r \twoheadrightarrow C^{(r)}$ is locally free of finite rank (i.e., is a finite flat morphism).

Proposition 5.1. *Assume $C(S) \neq \emptyset$. The functor $\mathrm{Div}^r_{C/S}$ is represented over $SCH_{/S}$ by $C^{(r)}_{/S}$, which is smooth of dimension r.*

If $S = \mathrm{Spec}(k)$ for an algebraically closed field k and K/k is an algebraicaaly closed field extension of k, it is plain that $\mathrm{Div}^r_{C/S}(K) = C^{(r)}_{/S}(K)$.

Proof. From the above computation of the stalk of $C^{(r)}$, we see that $C^{(r)}_{/S}$ is a smooth scheme over S. We now define a functorial map $\iota : \mathrm{Div}_{C/S} \to \underline{C}^{(r)}$. By the very definition of the fiber product, we have a functorial isomorphism: $\underline{C}^r(T) \cong \mathrm{Hom}_{SCH_{/S}}(T, C)^r$. For each split effective divisor $D = \sum_{j=1}^r [P_j]$ on $C_{/T}$, we define $\iota(D) = \pi\circ(P_1,\dots,P_r)$, which is by definition independent of the choice of ordering of P_j. When D is not split, taking a faithfully flat affine covering $f : T'_{/S} \to T_{/S}$, we get a point $h' = \iota_{T'}(D_{T'}) : T' \to C^{(r)}_{T'}$. Write $X = C^{(r)}_{T'}$ and $Y = C^{(r)}_T$ for simplicity. Then $X \to Y$

is affine faithfully flat. We have a closed immersion $h' : T' \to X$ giving rise to $\mathcal{O}_X/\mathcal{J}' = h'_*\mathcal{O}_{T'}$ for an ideal $\mathcal{J}'$. For projections $p_j : X' = X \times_Y X \to X$ and $p_{ij} : X'' = X \times_Y X \times_Y X \to X'$, we have the covering datum $p_1^*\mathcal{J}' \overset{\varphi}{\cong} p_2^*\mathcal{J}'$ and the descent datum $p_{23}^*\varphi \circ p_{12}^*\varphi = p_{13}^*\varphi$. By descent theory in [GME] §1.11, the sheaf of ideals $\mathcal{J}'$ descends to a sheaf of ideals $\mathcal{J} \subset \mathcal{O}_Y$ giving rise to a unique section $\iota(D) = h : T \to C_T^{(r)}$. This defines $\iota : \mathrm{Div}_{C/S} \to \underline{C}^{(r)}$. By this definition, injectivity of ι_T for all T is plain, because it is injective over split divisors.

To show the surjectivity of ι, first suppose that $T = \mathrm{Spec}(R)$ is affine. Pick a point $P \in C^{(r)}(R)$. Take the completed stalk $\widehat{\mathcal{O}}_{C^{(r)},P}$ of P. The infinitesimal neighborhood $\pi^{-1}(\mathrm{Spec}(\widehat{\mathcal{O}}_{C^{(r)},P}))$ of $\pi^{-1}(P)$ is stable under $\mathfrak{S}$. Thus (after a faithfully flat finite extension), we have, supposing the divisor P has s distinct points of C with multiplicities $j_1, j_2, \ldots, j_s$,

$$\widehat{\mathcal{O}}_{C^r,\pi^{-1}(P)} \cong R[[T_1, \ldots, T_r]]^n \quad (n = r!/j_1!j_2! \cdots j_s!)$$

for $\sum_k j_k = r$, on which $\mathfrak{S}$ acts by permuting components and the T_j's. Then P is given by an R–algebra homomorphism

$$\widehat{\mathcal{O}}_{C^{(r)},P} = R[[\sigma_1^{(1)}, \ldots, \sigma_{j_1}^{(1)}, \ldots, \sigma_1^{(s)}, \ldots, \sigma_{j_s}^{(s)}]] \to R$$

for the fundamental symmetric polynomials $\sigma_j^{(k)}$ of $T_1^{(k)}, \ldots, T_{j_k}^{(k)}$ of degree j. We want to lift ϕ to $\Phi : \widehat{\mathcal{O}}_{C^r,\pi^{-1}(U)} \to R'$ for a faithfully flat extension R'/R. It is enough to treat each connected component; so, we only need to lift an R–algebra homomorphism of $\phi : R[\sigma_1, \ldots, \sigma_r]] \to R$ to $R[[T_1, \ldots, T_r]]$ for $r > 1$. This may not be possible keeping R, but after a base-change to a faithfully flat extension R' again, we can lift it as follows: Let $f_0(X) = \sum_{j=0}^r \phi(\sigma_j) X_1^{r-j} \in R[X]$. We shall show the existence of an R–algebra R' free of finite rank over R such that $f_0(X)$ splits into a product of monic linear polynomials in $R'[X]$. What we need is to take $R' = R[[T_1, \ldots, T_r]] \otimes_{R[[\sigma_1,\ldots,\sigma_r]],\phi} R$. For the image t_i of T_i in R', we have $f_0(X) = \prod_{j=1}^r (X - t_i)$ in $R'[X]$. By defining $\Phi(T_j) = t_j$, we have an extension $\Phi : R'[[T_1, \ldots, T_r]] \to R'$ of ϕ. The morphism Φ gives rise to a point $(P_1, \ldots, P_r) \in C^r(T')$ for $T' = \mathrm{Spec}(R')$. Then we have $\iota_{T'}(D) \in C^{(r)}(T')$ for $D = \sum_j [P_j]$. The divisor D as a closed subscheme of $C_{T'}$ satisfies $p_1^*D \cong p_2^*D$ canonically by construction. Again by descent argument, we get a closed subscheme $D \subset C_{/T}$. Since $\mathcal{O}_D \otimes_{\mathcal{O}_T} \mathcal{O}_{T'}$ is $\mathcal{O}_{T'}$–flat, the faithfully flatness of R' over R tells us that D is locally-free over T, giving rise to a unique Cartier divisor such that $\iota_T(D) = P$. This solves the problem locally. Since the two functors are local, local construction glues well, yielding the desired map. □

In the above proof, we have used at many places that the (completed) local ring around a point in $C(A)$ is given by $A[[T]]$. Thus we need the smoothness of C for the validity of the proposition. However at this moment, we have not used projectivity (i.e., properness) of the curve.

Recall that we have assumed: $C(S) \neq \emptyset$. Taking $P \in C(S)$, we have

$$\mathrm{Pic}^r_{C/S}(T) \cong \mathrm{Pic}^{r+1}_{C/S}(T) \quad \text{by } \mathcal{L} \mapsto \mathcal{L} \otimes \mathcal{L}([P]).$$

Thus the representability of Pic^0 follows from the representability of Pic^r for sufficiently large r. Here we assume that $r > 2g$. We have a morphism of functors: $\pi : D \mapsto \mathcal{L}(D)$ from Div^r into Pic^r.

Lemma 5.2. *Let $F : SCH_{/S} \to SETS$ be a contravariant functor. Suppose that there exists a scheme $X_{/S}$ with a morphism of functors $\pi : \underline{X} \to F$ with a functorial section $s : F \to \underline{X}$ (that is, $\pi \circ s = 1_F$). Then F is representable by a closed subscheme Y of X.*

Proof. Let $\varphi = s \circ \pi$. Then $\varphi : \underline{X} \to \underline{X}$ is a morphism of functors; so, it induces by Key-lemma an endomorphism of the scheme X. Define $Y = X \times_{X \times X} X$ by the following Cartesian diagram:

$$\begin{array}{ccc} Y & \xrightarrow{i} & X \\ \downarrow & & \downarrow{\scriptstyle 1_X \times \varphi} \\ X & \xrightarrow[\Delta]{} & X \times_S X. \end{array}$$

Here Δ is the diagonal map. By the definition of fiber products, we have

$$\begin{aligned} Y(T) &= \big\{(a,b) \in X(T) \times X(T) \big| a = b \ \text{ and } \ a = \varphi \circ b\big\} \\ &= \big\{a \in X(T) \big| a = \varphi(a)\big\} \\ &= \big\{a \in X(T) \big| a = s(b)\ \exists b \in F(T)\big\} \cong F(T). \end{aligned}$$

Thus F is representable by Y. Since Δ is a closed immersion, $i : Y \hookrightarrow X$ is a closed immersion. □

We state a ring theoretic lemma, before constructing the jacobian variety. For an integral domain A with quotient field F and an A–module M of finite type, we write $\mathrm{rank}_A M$ for $\dim_F M \otimes_A F$.

Lemma 5.3. *Let A be an integral domain with quotient field F and M be an A–module of finite type. Let $d = \dim_F M \otimes_A F$. Then*

$$U = \big\{\mathfrak{p} \in \mathrm{Spec}(A) \big| \, \mathrm{rank}_{A/\mathfrak{p}} (M \otimes_A A/\mathfrak{p}) = d\big\}$$

is a dense open subset of $\mathrm{Spec}(A)$*, and for $\mathfrak{p} \notin U$, $\mathrm{rank}_{A/\mathfrak{p}} (M \otimes_A A/\mathfrak{p}) > d$.*

Proof. Since $\mathrm{Spec}(A)$ is irreducible, any non-empty open subset is dense; so, we shall prove the openness of U. Choose a maximal set of A–linearly independent elements $b = \{x_1, \ldots, x_d\}$ in M. Then for $L = Ax_1 + \cdots + Ax_d$, M/L is a torsion A–module of finite type. Thus $V_b = Supp(M/L) = \mathrm{Spec}(A/\mathfrak{a})$ for the annihilator $\mathfrak{a}$ of M/L is a proper closed subset of $\mathrm{Spec}(A)$ of positive codimension. Then obviously $U \supset \mathrm{Spec}(A) - \bigcap_b V_b$, where b runs over all maximal set of A–linearly independent elements of M. Pick $\mathfrak{p} \in \bigcap_b V_b$. If $r = \mathrm{rank}_{A/\mathfrak{p}}(M \otimes A/\mathfrak{p}) \le d$, then choosing a base $\overline{x}_1, \ldots, \overline{x}_r$ of $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ in the image of M and lifting them to elements $x_i \in M$ so that $x_i \equiv \overline{x}_i \mod \mathfrak{p}M_\mathfrak{p}$, we find that $x_1, \ldots, x_r$ generate $M_\mathfrak{p}$ by Nakayama's lemma. Thus further tensoring $M_\mathfrak{p}$ by F over $A_\mathfrak{p}$, we find that $r = d$ and $\mathfrak{p} \notin V_b$ for $b = \{x_1, \ldots, x_d\}$, a contradiction. Thus $r > d$ as desired. □

We now state

Theorem 5.4. *Let S be a scheme reduced and irreducible. Suppose that $f : C \to S$ is a smooth proper curve of positive genus g with $C(S) \neq \emptyset$. Then fixing $\mathbf{0} \in C(S)$, the group functor $\mathrm{Pic}^0_{C/S}$ is represented by an abelian scheme $J_{/S}$ of relative dimension g, and the map $P \mapsto \mathcal{L}([P] - [\mathbf{0}])$ induces an embedding of C into J taking $\mathbf{0}$ to the identity element in J.*

Here an *abelian scheme* over S means a proper smooth geometrically connected group scheme over S. An elliptic curve over S is nothing but an abelian scheme over S of relative dimension 1.

Proof. As before, fix an integer $r > 2g$. Our strategy of proving the representability of $\mathrm{Pic}^r_{C/S}$ is as follows: We try to find an open covering of $C^{(r)} = \bigcup_\delta C^\delta$ and $\mathrm{Pic}^r_{C/S} = \bigcup_\delta P^\delta$ such that for each piece of the covering C^δ, the functor $\pi : \underline{C}^\delta \to P^\delta$ has a section. Then plainly on $P^\delta \cap P^{\delta'}$, the schemes Y_δ and $Y_{\delta'}$, representing P^δ and $P^{\delta'}$ respectively, glue each other, and hence we get the representability of $\mathrm{Pic}^r_{C/S}$.

As in the proof of Theorem 2.1, the existence of the section $\mathbf{0} \in C(S)$ tells us that $\mathrm{Pic}^r_{C/S}$ is local with respect to the base S. If we can cover S by affine open subsets so that $\mathrm{Pic}_{C_U/U}$ is representable, the schemes $\mathrm{Pic}_{C_U/U}$ glue over S by the universality. Thus we may assume that $S = \mathrm{Spec}(A)$ for an integral domain A, and if necessary, we can shrink further S replacing $\mathrm{Spec}(A)$ by its localizations.

We pick an element $\delta \in \mathrm{Div}^{r-g}_{C/S}(C)$. For a relative Cartier divisor $\mathcal{D}$ on a smooth curve $\varphi : \mathcal{C} \to \mathcal{S}$ and for each geometric point $s \in \mathcal{S}$, writing $\mathcal{C}(s)$ for the fiber of $\mathcal{C}$ at s, we write $\ell(\mathcal{D}(s)) = \dim_{k(s)} H^0(\mathcal{C}(s), \mathcal{L}(\mathcal{D}(s)))$, where $\mathcal{D}(s) = \mathcal{D} \times_S k(s)$.

By the Riemann-Roch theorem, we have, for $D \in \mathrm{Div}^r_{C/S}(T)$ and $t \in T$,

$$\ell(D(t) - \delta_T(t)) = \dim_{k(t)}(H^0(C(t), (\mathcal{L}(-D(t) + \delta_T(t)) \otimes \Omega_{C(t)/k(t)})) + 1 \ge 1.$$

We define a subfunctor $C^\delta_{/S}$ of $\mathrm{Div}_{C/S}$ by

$$C^\delta_{/S}(T) = \Big\{D \in \mathrm{Div}^r_{C/S}(T) \Big| \ell(D(t) - \delta_T(t)) = 1 \ \forall t \in T\Big\}.$$

If S is a separably closed field, for a given $D \in \mathrm{Div}^r_{C/S}(S)$, $\ell(D) = r + 1 - g$. We know that $\mathcal{L}(D) \cong \mathcal{L}(D')$ for $D, D' \in \mathrm{Div}^r_{C/S}(S) \iff$ there exists $\phi \in H^0(C, \mathcal{L}(D))$ such that $D' = (\mathcal{L}(D), \phi)$

(or equivalently $(\phi) = D' - D$). Thus the fiber of $\pi : C^{(r)} \to \mathrm{Pic}^r_{C/S}$ over $\mathcal{L}(D)$ is as large as a $(r-g)$–dimensional projective space. If $H^0(C, \mathcal{L}(D-\delta)) \subset H^0(C, \mathcal{L}(D))$ is one-dimensional, the divisor $D' \in C^\delta$ with $D' > \delta$ and $\mathcal{L}(D') = \mathcal{L}(D)$ is uniquely determined by $\mathcal{L}(D)$, that is, $D' = (\mathcal{L}(D), \ell)$ for the unique $\ell \in H^0(C, \mathcal{L}(D-\delta))$ (up to scalar). Thus π induces a surjection with a canonical section from C^δ into a subfunctor of $\mathrm{Pic}^r_{C/S}$.

We admit the fact that that $C^\delta \subset C^{(r)}$ is a non-empty open subset (this is a bit technical cohomological computation; see, [GME] §4.1.1). We would like to show $C^{(r)} = \bigcup_\delta C^\delta$. What we need to show is that for any geometric point $x \in S$ and a sufficiently small affine open neighborhood $\mathrm{Spec}(A)$ of x, $C^\delta_{/\mathrm{Spec}(A)}$ is a non-empty open subset and moving δ around, they cover $C^{(r)}_{/\mathrm{Spec}(A)}$. We may assume that $S = \mathrm{Spec}(A)$ and $f_*\Omega_{C/A}$ is A–free of rank g.

For a given $D \in \mathrm{Div}^r_{C/S}(S)$, $f_*\mathcal{L}(D)$ is locally free of rank $r-g+1$ since $\deg D > 2g$. Thus for a closed point $s \in S$, we can find a sufficiently small affine neighborhood $U = \mathrm{Spec}(A)$ such that $H^0(U, f_*\mathcal{L}(D)|_U) = \bigoplus_{j=0}^{r-g} Ae_j$. The ring A is an integral domain by our assumption. Then write $\varphi : C_{/U} \hookrightarrow \mathbf{P}^{r-g}_{/U}$ for the projective embedding (associated to $(\mathcal{L}(P), e_0, \dots, e_{r-g})$) as in §4.9. By the construction of φ, $\varphi(e_i)$ gives the coordinate X_i of the projective space. If $\mathrm{Im}(\varphi)$ is contained in a hyper-plane $\sum_j a_j X_j = 0$, then $\sum_j a_j e_j = 0$ on $C_{/U}$, contradicting to our choice of e_j. Thus $\mathrm{Im}(\varphi)$ is not contained in any hyper-plane (defined over any flat extension of A). Then we can choose (after extending A to a locally free algebra of finite rank over A if necessary) $P_1, \dots, P_{r-g} \in C(A)$ such that the $(r-g) \times (r-g+1)$–matrix $(e_i(P_j)(s))_{i,j}$ has rank $r-g$ over $k(s)$. Then further shrinking $\mathrm{Spec}(A)$ (keeping $s \in \mathrm{Spec}(A)$), we have

$$H^0(C_{/U}, \mathcal{L}(D - \sum [P_j])) = \left\{ \sum a_i e_i \middle| \sum a_i e_i(P_j) = 0 (j = 1, \dots, r-g) \right\},$$

which has rank 1. This shows that for $\delta = \sum [P_j]$, we have $D \in C^\delta$, because of Lemma 5.3.

Since $C^{(r)}$ represents the functor $\mathrm{Div}^r_{C/S}$, we have a universal divisor $D_{univ} \in \mathrm{Div}^r_{C \times C^{(r)}/C^{(r)}}(C^{(r)})$ such that for any given $D \in \mathrm{Div}^r_{C/S}(T)$ on $C_T = C \times_S T$, there exists a unique $t \in C^{(r)}(T)$ such that $t^* D_{univ} = D$. Consider $\mathcal{D} = D_{univ} - p_1^*(\delta)$ for the projection $p_1 : C \times_S C^{(r)} \to C$. Then $\deg(\mathcal{D}) = g$ and $t^*\mathcal{D} = D - \delta_T$.

We consider the subfunctor P^δ of $\mathrm{Pic}^r_{C/S}$:

$$P^\delta(T) = \left\{ \mathcal{L} \in \mathrm{Pic}^r_{C/S}(T) | \ell(\mathcal{L}(t) \otimes \mathcal{L}(\delta_T(t))^{-1}) = 1 \ \forall t \in T \right\}.$$

We have a morphism of functors $\pi : \underline{C}^\delta \to P^\delta$ given by $\pi(D) = \mathcal{L}(D)$. For any $\mathcal{L} \in P^\delta(T)$, $\deg(\mathcal{L}) = r > 2g$. Under this condition, by Riemann-Roch and cohomological computation, we can show that $f_*\mathcal{L}$ is S–locally-free (see [GME] §4.1.1). After further shrinking S if necessary, we may assume that $f_*\mathcal{L}$ has a section ℓ so that $(\mathcal{L}, \ell) \in \mathrm{Div}^r_{C/S}(T)$. Thus $\mathcal{L}$ is in the image of $C^\delta(T)$, and the morphism of functors $C^\delta \to P^\delta$ is surjective and has a section. By Lemma 5.2, P^δ is representable by a closed subscheme J_δ of C^δ.

By the universality,

$$C^\delta \cap J_{\delta'} \cong P^\delta \cap P^{\delta'} \cong C^{\delta'} \cap J_\delta$$

canonically as functors. By the Key lemma, this induces gluing data to $\{J_\delta\}_\delta$, giving rise to a scheme $J_{/S}$ representing $\mathrm{Pic}^r_{C/S}$.

Since $\mathrm{Pic}^0_{C/S} \cong J$ by $\mathcal{L} \mapsto \mathcal{L} \otimes \mathcal{L}(\mathbf{0})^{\otimes r}$, J has a structure of a group scheme. Since J is a surjective image of the projective irreducible S–scheme $C^{(r)}$, it is proper and irreducible.

For each geometric point s of S, the fiber $J(s)$ at s is a proper group scheme over the separably closed field $k(s)$. In the construction of J, we could have assumed $r = g$. Then we still have a morphism $\pi : C(s)^{(g)} \to J(s)$. By the same argument, on an open subset of $C^{(g)}$, π is an isomorphism into an open subset of $J(s)$ whose complement is of positive codimension. Thus $J(s)$ has an open subset U which is smooth of dimension g over $k(s)$. Since $J(s) = \bigcup_{x \in J}(x + U)$ by the group action, and $x : U \to x + U$ is an isomorphism, $J(s)$ is smooth irreducible of dimension g. The above argument is still valid over a small open neighborhood of s, because we find U as above faithfully flat over the neighborhood. Therefore J is smooth irreducible over S.

We define a morphism of functors: $\underline{C} \to \mathrm{Pic}^0_{C/S} = \underline{J}$ by $P \mapsto \mathcal{L}([P]-[\mathbf{0}])$, which is injective, otherwise, we have an isomorphism $\phi : C \to \mathbf{P}^1$ (see the proof of Theorem 2.1). This induces an immersion $\iota : C \to J$, which is closed because $C_{/S}$ is proper. □

5.2. **Union of two curves.** In this section, first we assume that $S = \mathrm{Spec}(k)$ for a field k and $C = C_1 \cup C_2$ is a union of two smooth irreducible curves intersecting transversally at finite set of points. The word *"transversal"* means that for $x \in C_1 \cap C_2$, $\widehat{\mathcal{O}}_{C,x} \cong k[[X,Y]]/(XY)$. Thus the normalization $\pi : \widetilde{C} \to C$ is just the disjoint union $\widetilde{C} = C_1 \sqcup C_2$. Let $i_j : C_j \hookrightarrow C$ be the inclusion. Then for an invertible sheaf $\mathcal{L}$ on C, $i_j^*\mathcal{L}$ is an invertible sheaf on C_j. The correspondence: $\mathcal{L} \mapsto (i_1^*\mathcal{L}, i_2^*\mathcal{L})$ induces a functorial map

$$\iota : \mathrm{Pic}_{C/S} \to \mathrm{Pic}_{C_1/S} \times \mathrm{Pic}_{C_2/S} = \mathrm{Pic}_{\widetilde{C}/S}\,.$$

Let $\mathfrak{c} = C_1 \cap C_2 = C_1 \times_C C_2$, and put $C^\circ = C - \mathfrak{c}$ and $C_j^\circ = C_j - \mathfrak{c}$. We consider the following exact sequence: $0 \to \mathcal{O}_C \xrightarrow{\pi_*} \pi_*\mathcal{O}_{\widetilde{C}} \to \mathcal{O}_{\mathfrak{c}} \to 0$, where $\mathcal{O}_{\mathfrak{c}} \cong \bigoplus_{x\in\mathfrak{c}} \mathcal{O}_S$. This induces an exact sequence: $0 \to \mathcal{O}_C^\times \xrightarrow{\pi_*} \pi_*\mathcal{O}_{\widetilde{C}}^\times \to \mathcal{O}_{\mathfrak{c}}^\times \to 0$. Since the last term is $\mathcal{O}_S$–free, we get after tensoring $\mathcal{O}_T$ for an S–scheme T, we get another exact sequence

$$0 \to \mathcal{O}_{C_T}^\times \xrightarrow{\pi_*} \pi_*\mathcal{O}_{\widetilde{C}_T}^\times \to \bigoplus_{x\in\mathfrak{c}} \mathcal{O}_T^\times \to 0.$$

The associated long exact sequence is

$$0 \to \mathcal{O}_T^\times \xrightarrow{\Delta} (\mathcal{O}_{\widetilde{T}}^\times \times \mathcal{O}_{\widetilde{T}}^\times) \to \bigoplus_{x\in\mathfrak{c}} \mathcal{O}_T^\times \to H^1(C_T, \mathcal{O}_{C_T}^\times) \to H^1(\widetilde{C}_T, \mathcal{O}_{\widetilde{C}_T}^\times) \to H^1(\mathfrak{c}, \mathcal{O}_{\mathfrak{c}}^\times). \tag{5.1}$$

The last term vanishes, as $\dim \mathfrak{c} = 0$. Since each Čech 1-cocycle g_{ij} on $U_i \cap U_j$ for an open covering $\{U_i\}$ can be written as $g_{ij} = \frac{f_i}{f_j}$, that is, a Čech coboundary of f_j in the function field of $\widetilde{C}$, invertible sheaves $\mathcal{L}_i = f_i^{-1}\mathcal{O}_{U_i}$ glue into a global invertible sheaf $\mathcal{L}$ on $\widetilde{C}$, and we have $\mathrm{Pic}_{\widetilde{C}/S}(T) \cong H^1(\widetilde{C}_T, \mathcal{O}_{\widetilde{C}_T}^\times)$, whose identity connected component is given by the product $J_1 \times J_2$ of jacobians of C_j. Similarly we have $\mathrm{Pic}_{C/S}(T) \cong H^1(C_T, \mathcal{O}_{C_T}^\times)$. Taking the identity connected component (or more precisely, the kernel of the degree maps) of the sequence (5.1), we have the following exact sequence of fppf abelian sheaves:

$$0 \to \underline{\mathbb{G}_m}^{r-1} \to \mathrm{Pic}^0_{C/S} \to J_1 \times J_2 \to 0,$$

where $r = |\mathfrak{c}|$. For a given invertible sheaf $\mathcal{L}$ on $\widetilde{C}$, we consider $\pi_*\mathcal{L}$. Since $(\pi_*\mathcal{L})_x \cong (\mathcal{O}_{C_1,x} \oplus \mathcal{O}_{C_2,x})$ for $x \in \mathfrak{c}$, taking the kernel of $\mathcal{O}_{C_1,x} \oplus \mathcal{O}_{C_2,x} \to k(x)$ given by $(x \mod \mathfrak{m}_1) - (y \mod \mathfrak{m}_2)$ for the maximal ideals $\mathfrak{m}_j$ of $\mathcal{O}_{C_j,x}$, we can define an invertible sheaf $\mathcal{L}_C$ over C. This map $\mathcal{L} \mapsto \mathcal{L}_C$ plainly gives a section of $\mathrm{Pic}^0_{C/S} \to J_1 \times J_2$, and hence

$$\mathrm{Pic}^0_{C/S} \cong \underline{\mathbb{G}_m}^{r-1} \times J_1 \times J_2.$$

More generally, if C becomes $C_1 \cup C_2$ intersecting transversally after finite extension K of k, by a descent argument,

$$\mathrm{Pic}^0_{C/S} \cong \underline{T} \times J_1 \times J_2$$

for a linear algebraic group $T_{/k}$ with $T_{/K} \cong \mathbb{G}_m^{r-1}$. In any case, we have

Theorem 5.5. *Let k be a field, and $C = C_1 \cup C_2$ be a union of two proper smooth irreducible curves over k such that its components intersect transversally over a finite field extension K/k. Then $\mathrm{Pic}^0_{C/k}$ is representable by a smooth connected group scheme isomorphic to a product of a torus T and the jacobian of the normalization $\widetilde{C}$ of C. The torus T becomes isomorphic to $\mathbb{G}_m^{r-1}$ over K for $r = |C_1 \cap C_2|$.*

Suppose now that $S = \mathrm{Spec}(A)$ for a Dedekind domain A (such a scheme we call a Dedekind scheme). Let C/S be a proper flat curve fiber by fiber a smooth curve or a union of two proper smooth irreducible curves intersecting transversally. Suppose further that C is regular and that C is smooth over a dense open subset of S. Since two reduced components intersect transversally at a singular geometric point x of the curve C, we have $\widehat{\mathcal{O}}_{C,x} \cong W[[X,Y]]/(XY - \varpi^r)$ for a valuation

ring W with a prime element ϖ whose residue field is isomorphic to $k(x)$. By the regularity of the ring $\widehat{\mathcal{O}}_{C,x}$, the exponent r is equal to 1.

Let C° be the smooth locus of C. Then $\mathrm{Div}^g_{C^\circ/S}$ is representable by $X = (C^\circ)^{(g)}$ by the remark after Proposition 5.1. Let D^{univ} be the universal divisor on $C_X = C \times_S X$. For each point $t \in T$ and $T \to X$, we write D_t for $D^{univ} \times_{C_X} t$, which is a divisor on $C_t = C \times_X C_X$. Then by Riemann-Roch theorem, we have $\ell(D_t) \geq 1$. Let U be the open subset of X defined by

$$\underline{U}(T) = \{D \in \underline{X}(T) | \ell(D_t) = 1 \ \forall t \in T\}.$$

Then by the Riemann-Roch theorem and Lemma 5.3 for $C_{X/X}$, U is an open subscheme of X faithfully flat over S.

By the argument in the proof of Theorem 5.4, the natural map: $\underline{U}(T) \to \mathrm{Pic}^g_{C/S}(T)$ is an injection for all T. By Theorem 5.4 and Theorem 5.5, $U(s) = U \times_S s$ is an open dense subscheme of the jacobian J_s of C_s for all geometric point $s \in S$. We now identify $\mathrm{Pic}^g_{C/S}$ with $\mathrm{Pic}^0_{C/S}$ by using the smooth section $P : S \hookrightarrow C$. Since S is quasi compact (it is noetherian), $\mathrm{Pic}^0_{C/S}$ is covered by $g + \underline{U}$ for finitely many $g \in \mathrm{Pic}_{C/S}(T)$ for a faithfully flat covering $T \to S$. Fiber by fiber, $g + U \cap h + U$ for $g, h \in \mathrm{Pic}_{C/S}(T)$ is a non-trivial open subscheme of each. These schemes $\{g + U\}_g$ glue each other into a scheme $\mathrm{Pic}^0_{C_T/T}$ smooth over T of relative dimension g. By a standard descent argument, $\mathrm{Pic}^0_{C/S}$ is representable by a scheme smooth over S of relative dimension g.

Theorem 5.6. *Let S be a Dedekind scheme. Let C/S be a proper flat curve of genus g almost everywhere smooth and whose singular geometric fiber is a union of two proper smooth irreducible curves intersecting transversally. Suppose further that $C(S)$ is non-empty, having a smooth section $P : S \to C$ and that C is regular. Then the functor $\mathrm{Pic}^0_{C/S}$ is representable by a group scheme, fiber by fiber geometrically connected, smooth over S of relative dimension g.*

Results on the representability of $\mathrm{Pic}_{C/S}$ more general than this theorem can be found in [DeM] Theorem 2.5 and [NMD] Chapter 9.

Let $f : C \to S$ be a proper flat curve of genus g. Suppose that $\mathrm{Pic}^0_{C/S}$ is representable by the jacobian scheme $J_{/S}$, which is smooth over S of relative dimension g. As before, we suppose the origin $\mathbf{0}$ of J is actually a smooth point in $C(S)$. Then let $\mathcal{I} \subset \mathcal{O}_J$ be the sheaf of ideals defining the identity section $\mathbf{0}$ of J, that is, $\mathcal{I} = I(\mathbf{0})$. The cotangent space $\mathbf{0}^*\Omega_{J/S}$ of J along $\mathbf{0}$ is isomorphic to $\mathcal{I}/\mathcal{I}^2$, and the tangent space along the origin $\mathcal{T}_{J/S}$ is defined by the $\mathcal{O}_S$–dual of the cotangent space.

Theorem 5.7. *We have $\mathcal{T}_{J/S} \cong R^1 f_* \mathcal{O}_C$ and $\mathbf{0}^*\Omega_{J/S} \cong f_*\Omega^\circ_{C/S}$ canonically as $\mathcal{O}$–modules, where $\Omega^\circ_{C/S}$ is the dualizing sheaf of C/S.*

Proof. By construction, we have a canonical surjective homomorphism $\mathcal{I}/\mathcal{I}^2 \twoheadrightarrow \mathbf{0}^*\Omega_{J/S}$. Since J/S is smooth, over an affine open subset $U = \mathrm{Spec}(A) \subset S$, $\widehat{\mathcal{O}}_{U,\mathbf{0}} \cong A[[T_1, \ldots, T_g]]$, and thus $\mathcal{I} \otimes_S A/\mathcal{I}^2 \otimes_S A \cong A^g$. Thus the two locally free modules $\mathcal{I}/\mathcal{I}^2$ and $\mathbf{0}^*\Omega_{J/S}$ have the same rank. This shows that the morphism is an isomorphism.

Let $\mathcal{O}_S[\mathbf{e}] = \mathcal{O}_S[X]/(X^2)$, where $\mathbf{e}$ is the class of X modulo X^2. The scheme $T = \mathrm{Spec}_S(\mathcal{O}_S[\mathbf{e}])$ is an S–scheme, and we have a homomorphism

$$\pi : \underline{J}(T) = \mathrm{Pic}^0_{C/S}(T) \to \mathrm{Pic}^0_{C/S}(S).$$

Obviously,

$$\mathrm{Ker}(\pi) = \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_{J,\mathbf{0}}/\mathcal{I}^2, \mathcal{O}_S[\mathbf{e}]) \cong \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_S\mathbf{e}) \cong \mathcal{T}_{J/S}.$$

We can rewrite, when $S = \mathrm{Spec}(k)$ for a field k,

$$\pi : \underline{J}(T) \cong H^1(C, \mathcal{O}^\times_{C_T}) \to H^1(C, \mathcal{O}^\times_C) = \underline{J}(S),$$

by computing the cohomology groups using Čech cohomology groups.

Since $\mathcal{O}^\times_{C_T} \cong \mathcal{O}^\times_C \oplus \mathcal{O}_C\mathbf{e}$, we know that

$$\mathrm{Ker}(\pi) \cong H^1(C, \mathcal{O}_C\mathbf{e}) \cong H^1(C, \mathcal{O}_C).$$

Thus for all geometric points $s \in S$, $(R^1 f_* \mathcal{O}) \otimes k(s) \cong \mathcal{T}_{J/S} \otimes k(s)$. Since we have a natural map $(R^1 f_* \mathcal{O}) \to \mathcal{T}_{J/S}$ inducing the local isomorphism by the same (global) reasoning, the local freeness of the two sides shows the desired isomorphism.

By taking $\mathcal{O}_S$–dual, the Serre–Grothendieck duality theorem ([GME] §2.1.2) tells us the identity for the cotangent space. □

5.3. **Functorial properties of Jacobians.** Let $S = \mathrm{Spec}(A)$ for a Dedekind domain A of characteristic 0. We study functoriality of jacobian varieties for regular flat proper curves $C_{/S}$. For the moment, all curves C are supposed to be regular irreducible with smooth section $\mathbf{0} = \mathbf{0}_C : S \hookrightarrow C$. We also suppose the existence of the jacobian scheme $J = J(C)_{/S}$ representing $\mathrm{Pic}^0_{C/S}$. Let $f : C \to C'$ be an S–morphism between two curves taking $\mathbf{0}_C$ to $\mathbf{0}_{C'}$. Since $f_T^* : \mathrm{Pic}_{C'/S}(T) \to \mathrm{Pic}_{C/S}(T)$ is a morphism of group functors, it induces a homomorphism $J(f) : J_{C'} \to J_C$. This is the contravariant functoriality of the jacobian scheme. Since $f^*\mathcal{L}(D) = \mathcal{L}(f^*(D))$, we have $J(f)(\pi_{C'}(D)) = \pi_C(f^*(D))$ for $\pi_C : \mathrm{Div}^r_{C/S} \to \mathrm{Pic}^r_{C/S} \cong J$, where the last isomorphism is given by $\mathcal{L} \mapsto \mathcal{L} \otimes \mathcal{L}(-[\mathbf{0}])^{\otimes r}$.

Here is a useful ring theoretic lemma (see [GME] Lemma 2.8.1 for a proof):

Lemma 5.8. *Let $\varphi : (A, \mathfrak{m}) \to (B, \mathfrak{n})$ be a morphism of local rings (i.e. $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$). Suppose the following two conditions:* (i) *B is an A–module of finite type, and* (ii) *A and B are both regular of dimension n. Then B is A–free.*

Suppose that f is constant at one geometric fiber $f_s : C(s) \to C'(s)$. Since f is proper, the image $\mathrm{Im}(f)$ is a closed subscheme of C'. By the assumption, it is of positive codimension. Since $\dim S = 1$, we have $\dim C = 2$. Since f is an S–morphism taking $\mathbf{0}_C$ to $\mathbf{0}_{C'}$, $\dim \mathrm{Im}(f) \geq 1$. Thus $\dim \mathrm{Im}(f) = 1$. This shows that f is constant generically. We consider the graph $\Gamma_f \subset C \times_S C'$ of f, that is, $\Gamma_f = \mathrm{Im}(1 \times f)$. Since f is constant at the generic point η of S, $\Gamma_f \times_S \eta$ is open dense in Γ_f and Γ_f is of the form $\bigcup_j C \times P_j$ after finite locally free extension T of S. The closure of this set in $C \times_S C'$ is covered by $C \times_S D$ for a closed subscheme D of C' of relative dimension 0 over S; so, f is constant at every geometric fiber.

Suppose now that f is non-constant at one geometric fiber. Since f is proper non-constant fiber by fiber, it is universally surjective. Then by the above argument, f is quasi-finite (that is, its fiber at every geometric point is finite) with non-empty fiber everywhere. Thus for each geometric point $x \in C'$, f induces $f^\# : \mathcal{O}_{C',x} \hookrightarrow \mathcal{O}_{C,f^{-1}(x)}$. Since the two sides are regular rings of equal dimension ($= 2$), $f^\#$ is finite flat (see Lemma 5.8). Thus f is locally free. We write $\deg(f)$ for the rank of f, which is a well defined integer, since C and C' are irreducible.

Start with a morphism $f_\eta : C(\eta) \to C'(\eta)$ of generic fibers (so, $C(\eta) := C \times_S \eta$ for the generic point η of S). Let s be a closed point of S. Since S is $\mathrm{Spec}(A)$ for a Dedekind domain A, $A_s = \mathcal{O}_{S,s}$ is a discrete valuation ring (DVR). Let $C_s = C \times_S \mathrm{Spec}(A_s)$. Let x be a point of the generic fiber, that is, $x \in C \times_S \eta$ ($\eta = \mathrm{Spec}(K)$) for the quotient field K of A. Then by the valuative criterion of properness (Proposition 4.23), we have a unique point $x_s = \overline{x} \times_S s$ for the closure $\overline{x}$ in C. Similarly $f_\eta(x)_s$ is uniquely determined by $f_\eta(x)$. In other words, we have

$$\overline{\Gamma} \cap (x_s \times C') = \overline{\Gamma} \times_{C \times C'} (x_s \times C') = x_s \times f_\eta(x)_s$$

for the closure $\overline{\Gamma}$ of Γ_{f_η} in $C \times_S C'$. This shows that the projection $p : \overline{\Gamma} \to C$ is fiber by fiber an isomorphism, and therefore, locally free of rank 1 (see [EGA] IV.11.3.10). Thus p is an isomorphism. We put $f = p' \circ p^{-1}$ for the projection $p' : \overline{\Gamma} \to C'$. Then we see $\overline{\Gamma} = \Gamma_f$ for the morphism $f : C \to C'$. It is plain that f is determined uniquely by f_η.

We record what we have proven.

Lemma 5.9. *Let the notation and assumption be as above. Suppose that C and C' are regular irreducible curves. Then for an S–morphism $f : C \to C'$, if f is non-constant at one geometric fiber, then f is locally free of finite rank. If $f_\eta : C(\eta) \to C'(\eta)$ is a morphism of generic fibers, then there is a unique S–morphism $f : C \to C'$ inducing f_η. Writing $f_s : C(s) \to C'(s)$ for the morphism induced by f at a closed point $s \in S$, we have the reduction map:* $\mathrm{Hom}_S(C(\eta), C'(\eta)) \to \mathrm{Hom}_S(C(s), C'(s))$ *sending f_η to f_s.*

Let $f : C \to C'$ be a locally free S–morphism taking $\mathbf{0}_C$ to $\mathbf{0}_{C'}$. Then for $\mathcal{L} \in \mathrm{Pic}_{C/S}(T)$. We consider the functors

$$T_i : QS(T) \ni \mathcal{F} \mapsto R^i f_{T,*}(\mathcal{L} \otimes_{\mathcal{O}_{C_T}} f_T^*\mathcal{F}) \in QS(T).$$

Since C/C' is locally free of relative dimension 0, we can show that $f_{T,*}\mathcal{L}$ is locally free of rank $\deg(f)$ (Exercise 5.13). We then define

$$\mathrm{Pic}^t(f_T)(\mathcal{L}) = \bigwedge_{\mathcal{O}_S}^{\deg(f)} f_{T,*}\mathcal{L} \in \mathrm{Pic}_{C'/S}(T).$$

Obviously $\mathrm{Pic}^t(f)$ is a morphism of group functors; so, taking the identity connected component to the identity component, and hence it induces an S–morphism $J^t(f) : J \to J'$ of group schemes. When $f : C \to C'$ is not locally free, it has to be constant. In this case, we put $J^t(f)$ to be the zero-map.

Theorem 5.10. *Let the notation and assumption be as above. In particular, we assume that C and C' are regular. Then for an S–morphism $f : C \to C'$ taking $\mathbf{0}_C$ to $\mathbf{0}_{C'}$, $J(f) : J_{C'} \to J_C$ and $J^t(f) : J_C \to J_{C'}$ satisfy contravariant and covariant functoriality, respectively. This means $J(f \circ g) = J(g) \circ J(f)$ and $J^t(f \circ g) = J^t(f) \circ J^t(g)$ when all the morphisms above are well defined.*

We would like to prove the following *Albanese functoriality*:

Theorem 5.11. *We suppose that C is smooth over the spectrum S of a Dedekind domain. If $\phi : C \to A$ is an S–morphism into an abelian scheme $A_{/S}$ taking $\mathbf{0}$ to $\mathbf{0}_A$, then there exists a unique homomorphism $J(\phi) : J_C \to A$ such that $J(\phi)\circ\iota = \phi$ for the canonical closed immersion $\iota : C \hookrightarrow J$ in Theorem 5.4. In other words, J represents the covariant functor $A \mapsto \{\phi \in \mathrm{Hom}_S(C, A) | \phi(\mathbf{0}) = \mathbf{0}_A\}$ in the category of abelian schemes over S.*

Proof. Define $\Phi : \mathrm{Div}^g_{C/S}(T) \to \underline{A}(T)$ by $\Phi(\sum_j [P_j]) = \sum_j \phi(P_j)$. This is a well defined morphism of functors; so, it induces a morphism: $C^{(g)} \to A$ by Proposition 5.1 and the Key lemma. As we have shown in the proof of Theorem 5.6, we have a dense open subset $U \subset C^{(g)}$ such that $\sum_j [P_j] \mapsto \sum_j \iota(P_j)$ is an open immersion of U into J. Thus we define $J(\phi) = \Phi|_U$ on U. This Φ satisfies the desired property on U since $\mathrm{Pic}^r_{C/S} \cong \mathrm{Pic}^0_{C/S}$ by $\mathcal{L} \mapsto \mathcal{L} \otimes \mathcal{L}(-r[\mathbf{0}])$. Suppose $J - U$ contains an irreducible closed subscheme x of codimension 1. Since J is normal, $\mathcal{O}_{J,x}$ is a normal local ring of dimension 1 and hence is a discrete valuation ring (see [CRT] Theorem 11.2). Since the generic point $h \in \mathrm{Spec}(\mathcal{O}_{D,x})$ is contained in U, Φ is well defined on h. Then by the valuative criterion (Proposition 4.23) of properness, Φ extend uniquely to x. Thus, $J(\phi)$ extends uniquely to an open set $\widetilde{U} \subset J$ whose complement is of codimension ≥ 2.

By the lemma following this proof, we then know that $J(\phi)$ is actually defined over the entire J. □

We prove the following lemma used in the above proof:

Lemma 5.12 (A. Weil)**.** *Let the notation be as in* Theorem 5.11*. Let $G_{/S}$ be a group scheme over S and $V_{/S}$ be a smooth irreducible scheme. If $f : U \to G$ is an S–morphism defined over an open subset U of V with $\mathrm{codim}(V - U) \geq 2$, then f has a unique extension to V.*

Proof. We follow a proof by M. Artin in [A] 1.3. We prove that either f is defined on entire V or cannot be defined on a closed subset purely of codimension 1.

Write the group law of G as $m : G \times_S G \to G$; so, $m(x, y) = xy$ and $i : G \to G$ for the inverse. Define $F : V \times_S V \to G$ by $m \circ (\mathrm{id}_G \times i) \circ (f \times f)$ (on the points where the function is well defined). Thus $F(x, y) = f(x)f(y)^{-1}$. We claim that for any point $x \in V$,

$$F \text{ is defined on } (x, x) \iff f \text{ is defined at } x.$$

The direction: $\Leftarrow$ is obvious. Suppose F is defined on (x, x). If F cannot be defined at (a, b), F cannot be defined on any point in the closure of (a, b). Thus the set where F is defined is a non-empty open subset of $V \times_S V$. For the generic point η of V, $F(x, \eta)$ is well defined (since (x, x) is in the closure of (x, η)). Since f is defined on η, $f(x) = F(x, \eta)f(\eta)$ is well defined.

Now supposing that f is not defined on the entire V, we show that it cannot be defined on a closed subscheme of codimension 1. Let K be the function field of $V \times_S V$. We have $\phi = F^{\#} : \mathcal{O}_{G,e} \to K$, since $F(\eta, \eta) = e_\eta$ for the identity section $e : S \hookrightarrow G$. For each $\alpha \in K$, regarding $\alpha : V \times_S V \to \mathbf{P}^1_{/S}$, we put $(\alpha)_\infty = \alpha^{-1}(\infty)$. Since $V \times_S V$ is normal, $(\alpha)_\infty$ is a divisor on $V \times_S V$. Note that

$$\mathcal{O}_{V\times V,(x,x)} = \left\{\alpha \in K \middle| (x,x) \notin (\alpha)_\infty\right\}.$$

If F is not defined at (x,x), then there exists $\alpha \in \mathrm{Im}(\phi)$ such that $(x,x) \in (\alpha)_\infty$.

The diagonal image Δ is a complete intersection locally. Since $(\alpha)_\infty$ intersects with Δ at (x,x), it adds one more equation (because f is defined at (η,η)); so, the intersection has codimension 1 in Δ. Thus f cannot be defined on $C_\alpha = \Delta \cap (\alpha)_\infty$, which has purely of codimension 1. □

Exercise 5.13. (1) *Prove that $f_{T,*}\mathcal{L}$ is locally free of rank* $\deg(f)$ *for $\mathcal{L} \in \mathrm{Pic}_{C/S}(T)$ if $f : C \to C'$ is locally free of rank* $\deg(f)$.
(2) *Show that $\bigwedge^r_{\mathcal{O}_S} \mathcal{L}$ is invertible if $\mathcal{L}$ is a locally free sheaf of rank r over a scheme S.*
(3) *Under the notation of Theorem 5.10, verify $J(f\circ g) = J(g)\circ J(f)$ and $J^t(f\circ g) = J^t(f)\circ J^t(g)$.*

5.4. **Self-duality of Jacobian schemes.** Let A be a Dedekind domain. For all abelian schemes X defined over $S = \mathrm{Spec}(A)$, it is known that $\mathrm{Pic}_{X/S}$ is again representable by a group scheme whose identity component is an abelian scheme of the same dimension; so, we write X^* for the abelian scheme representing the connected component $\mathrm{Pic}^0_{A/S}$. It is called the *dual abelian scheme* of X. We admit this fact quoting [ABV] Section 13 (and [NMD] Section 8.2).

For each invertible sheaf $\mathcal{L}$ on J, we can pull it back to an invertible sheaf $\iota^*\mathcal{L}$ on C. This induces a morphism of group functors $\iota^* : \mathrm{Pic}_{J/S} \to \mathrm{Pic}_{C/S}$ and hence induces an S–homomorphism of the identity components $p : J^* \to J$.

We would like to prove the following self duality theorem for jacobians.

Theorem 5.14. *Let $S = \mathrm{Spec}(A)$ for a Dedekind domain A and $C_{/S}$ be a smooth proper curve over S of genus g. Then $J^* \cong J$ by $p = \iota^*$.*

Proof. We follow a proof given in [Mi1] Section 6. If ι^* induces an isomorphism fiber by fiber, it is locally free of rank 1, and hence globally an isomorphism. Thus we may assume that $S = \mathrm{Spec}(k)$ for an algebraically closed field k. We consider the natural map: $C^{(g-1)} = \mathrm{Div}^{g-1}_{C/S} \to \mathrm{Pic}^{g-1}_{C/S}$ taking D to $\mathcal{L}(D)$, and write Θ for the image of $C^{(g-1)}$ in J. Thus we have a morphism $f : C^{(g-1)} \to \Theta$. Choose a base $\omega_1, \ldots, \omega_g$ of $\Omega_{C/k}$, and embed $\Omega_{C/k}$ into $k(C)$ (regarded as the constant sheaf over C), where $k(C)$ is the function field of C. Write $e_1, \ldots, e_g$ for the image of ω_j. Let O be the open set of C on which e_j is a well defined morphism into $\mathbf{A}^1_{/k}$. Let $P_1, \ldots, P_r$ be r–points of C for $r \le g$. Consider the matrix $(e_i(P_j))$. Since e_j are linearly independent over k, on an open subset $U = U_r$ of $O^{(r)} \subset C^{(r)}$, one of the determinants of the $r \times r$-minors of the matrix does not vanish. Thus on $D \in U$, $\dim H^0(C, \Omega_{C/k} \otimes \mathcal{L}(-D)) = g - r$. By the Riemann-Roch theorem, $\dim H^0(C, \mathcal{L}(D)) = g - r + r - g + 1 = 1$.

Let $r = g - 1$. Then on U, the map $C^{(g-1)} \to \Theta$ is injective. Thus $\dim_k \Theta = g - 1$, and Θ is an effective divisor on J. Let us explain this fact in more details. For the generic point η of Θ, $A = \mathcal{O}_{U,\eta}$ is a discrete valuation ring. We have a morphism: $\mathrm{Spec}(A) \xrightarrow{v} J$. For a sufficiently small (non-empty) open subset $V \subset J$, the kernel of $\mathcal{O}_U(V) \xrightarrow{v^\#} A$ is generated by a single element f_V. Then the sheaf of ideals $I(\Theta)$ of the closed subscheme Θ is an invertible sheaf locally generated by f_V. We define $\mathcal{L}(\Theta) = I(\Theta)^{-1}$. By the same argument, to each closed subscheme $D \subset J$ of codimension 1, we can thus associate its sheaf of ideals $I(D)$ and an invertible sheaf $\mathcal{L}(D) = I(D)^{-1}$.

We define $i : C \to J^*$ by $i(a) = \mathcal{L}([\iota(a) + \Theta]) \otimes \mathcal{L}(-[\Theta])$, where $x + \Theta$ is the image of Θ under the translation $y \mapsto y + x$ in J. By the Albanese functoriality of the jacobian, i extends to $i : J \to J^*$ so that

$$i(d) = \mathcal{L}(\sum_j [\iota(P_j) + \Theta]) \otimes \mathcal{L}(-g[\Theta])$$

if d corresponds to $D = \sum_j P_j \in \mathrm{Div}^g_{C/S}(k)$.

Let $D \in \mathrm{Div}^g_{C/S}(S)$. Consider its image d in J. Let U' be the open subset of reduced divisors, that is, U' is obtained from U by removing divisors with multiplicity > 1. Then we claim that

$$\text{if } D \in U',\ \iota^*\mathcal{L}([d+\Theta]) = \mathcal{L}(D).$$

Writing $D = \sum_j [P_j]$, we consider the closed subset $\iota^{-1}([d+\Theta])$. For a point $Q \in C(k)$,

$$Q \in \iota^{-1}([d+\Theta]) \iff \exists Q_2, \dots, Q_g \text{ such that } \iota(Q) + \sum_j \iota(Q_j) = d.$$

This is equivalent to the linear equivalence of D to $D' = Q + \sum_j Q_j$, i.e., $\dim H^0(C, \mathcal{L}(D)) \geq 2$, which is impossible if D and D' are distinct. Thus $D = D'$ and hence, set theoretically $\iota^{-1}([d+\Theta]) = D$. To show that $\iota^*(\mathcal{L}([d+\Theta])) = \mathcal{L}(D)$, we need to show that $\deg(\iota^{-1}([d+\Theta])) = g$. The natural map $\pi : C^g \to C^{(g)}$ has degree $g!$ by definition. We shall compute the degree of the map $\psi : \Theta \times C \to J$ given by $(a, Q) \mapsto a + \iota(Q)$. The map π factors into a composite of three maps: $\pi : C^g \to C^{g-1} \times C \to \Theta \times C \xrightarrow{\psi} J$, and hence $g! = \deg(\pi) = (g-1)! \deg(\psi)$. This shows that $\deg(\psi) = g$. Since ψ is proper, it is finite over U'. Since divisors in U' are multiplicity free, we find $\deg(\iota^{-1}([d+\Theta])) = g$, which shows the claim.

By the claim, we find $\iota^* \circ i = \mathrm{id}_{U'}$ on U'. Since U' is dense, we find $p \circ i = \mathrm{id}_J$. Since J^* and J are irreducible of equal dimension, this implies that p and i are isomorphisms. □

Corollary 5.15. *Let J be the jacobian variety of a smooth proper algebraic curve over an algebraically closed field k. Then every effective divisor D on J algebraically equivalent to Θ is of the form $[a+\Theta]$ for $a \in J$. In particular, they are all irreducible.*

Proof. Since $J^* \cong J$, we have $\mathcal{L}(D) \cong \mathcal{L}(a+\Theta)$; so, we find a unique generator ϕ of $\mathcal{L}(-D) \otimes \mathcal{L}(a+\Theta)$ up to constant. We may regard ϕ as a morphism $\phi : J \to \mathbf{P}^1$. Then $\phi^{-1}(\infty) = a+\Theta$ and $\phi^{-1}(0) = D$. Restricting ϕ to C, we find $(\phi|_C)^{-1}(0) = D \cap C = D_C$, and from the above argument in the proof of the theorem, we conclude that $D = i(d) + \Theta$ for $d \in J$ corresponding to D_C (and thus $a = i(d)$). □

The above proof shows that $H^0(J, \mathcal{L}([a+\Theta])) = k$, and the linear equivalence class of $a + \Theta$ (in the set of effective divisors) is a singleton (that is, a one-element set). This fact also follows from the dimension formula of $H^0(J, \mathcal{L}([a+\Theta]))$ in [ABV] Section 16.

5.5. **Generality on abelian schemes.** We prepare some general results on abelian schemes X, which we apply to jacobian schemes at the end of this subsection.

Since X^* represents $\mathrm{Pic}^0_{X/S}$, we have a universal line bundle $\mathcal{P}_{/X \times_S X^*}$, called the *Poincaré bundle*, such that for any line bundle $\mathcal{L}$ over $X \times_S T$ trivial along the $\mathbf{0}$–section, we have a unique $\phi : T \to X^*$, $\phi_X^* \mathcal{P} \cong \mathcal{L}$, where $\phi_X : X \times_S T \to X \times_S X^*$. We then have a morphism of functors: $\underline{X}(T) \ni \phi \mapsto \phi_{X^*}^* \mathcal{P} \in \mathrm{Pic}_{X^*/S}(T)$. This induces an S–morphism $i : X \to (X^*)^*$. Since $\mathcal{P}$ is trivial over the zero-section, i takes $\mathbf{0}_X$ to $\mathbf{0}_{(X^*)^*}$. We would like to show that this map is an isomorphism of group schemes. This in particular shows that an abelian scheme is associated to a commutative group functor (so, the group $X(T)$ is an abelian group for all $T_{/S}$).

Lemma 5.16. (Rigidity) *Let X, Y and Z be reduced irreducible schemes over $S = \mathrm{Spec}(k)$ for an algebraically closed field k. Suppose that X is proper over S. Let $f : X \times_S Y \to Z$ be a morphism with $f(X \times y_0) = z_0$ for two closed points $y_0 \in Y$ and $z_0 \in Z$. Then there exists a morphism $g : Y \to Z$ such that $f = g \circ p$ for the projection $p : X \times_S Y \to Y$.*

Proof. We follow [ABV] Section 4. Since $X \times_S Y$ is irreducible and reduced, if we get a lemma on an open subscheme of $X \times_S Y$, the identity holds everywhere. Thus we choose an affine neighborhood $U = \mathrm{Spec}(A) \subset Z$ of z_0, and consider $f^{-1}(U)$. We write $F = Z - U$, which is closed. Since p is a closed map because of properness of X, we have $W = p(f^{-1}(F)) \subset Y$ is a closed subset (different from Y: $y_0 \notin W$). We put $V = Y - W$, which is an open neighborhood of y_0.

Choose a closed point x_0 of X. Then $Y \cong x_0 \times_S Y$, we define g by pulling back f through this isomorphism. For every closed point $y \in V$, f sends the proper irreducible scheme $X \times_S y$ into $U = \mathrm{Spec}(A)$; so, the image is a proper irreducible closed subscheme of U, which is $\mathrm{Spec}(A/\mathfrak{a})$ for an ideal $\mathfrak{a}$. The scheme $\mathrm{Spec}(A/\mathfrak{a})$ is proper irreducible and reduced only when $\mathfrak{a}$ is a maximal ideal; so, the image is a closed point. Thus $f(x, y) = f(x_0, y) = g \circ p(x, y)$, which was to be proven. □

Corollary 5.17. *Let S be an integral scheme (that is, reduced irreducible). Let X and Y be abelian schemes over S. If an S–morphism $f : X \to Y$ sends $\mathbf{0}_X$ to $\mathbf{0}_Y$, f is a morphism of group schemes, that is, a group homomorphism.*

By this fact, $i : X \to (X^*)^*$ is a morphism of group schemes.

Proof. Let $a_Z : Z \times_S Z \to Z$ be the addition of a general abelian scheme $Z_{/S}$. Define $\phi : X \times_S X \to Y$ by $f \circ a_X - a_Y \circ (f \times f)$. We need to show that ϕ is the zero map. Let $s \in S$ be any geometric point. By our assumption, $\phi(X(s) \times \mathbf{0}_{X(s)}) = \phi(\mathbf{0}_{X(s)} \times X(s)) = \mathbf{0}_{Y(s)}$ for the fibers at s. By the above lemma, ϕ is independent of right and left variables; so, a constant. This shows that ϕ is identically 0 fiber by fiber; so, it is identically 0 over $X \times_S X$. □

Lemma 5.18. *Let S be the spectrum of a discrete valuation ring A with quotient field K. Let $X_{/S}$ and $Y_{/S}$ be abelian schemes. Let $f_K : X_K \to Y_K$ be a K–homomorphism for $X_K = X \times_S \eta$ and $Y_K = Y \times_S \eta$ with $\eta = \mathrm{Spec}(K)$. If $f_K : X(\overline{K}) \to Y(\overline{K})$ is a surjection for an algebraically closed extension $\overline{K}$ of K, then there is a unique S–morphism $f : X \to Y$ inducing f_K. Moreover f is proper flat, and if X and Y have equal dimension, f is locally free of finite rank.*

Proof. Since $f_K : X(\overline{K}) \to Y(\overline{K})$ is surjective, f_K sends an open dense subset of X_K to a subset containing a dense open subset of Y_K. Thus f_K is flat over an open subset U of Y_K. If f_K is not flat at $x \in X(\overline{K})$, then we can find $x' \in X(\overline{K})$ such that $x \in -x' + f^{-1}(U)$. Since $f(x'+u) = f(x') + f(u)$, we can factor $f|_{x'+f^{-1}(U)}$ as

$$-x' + f^{-1}(U) \xrightarrow{T_{x'}} f^{-1}(U) \xrightarrow{f} U \xrightarrow{T_{f(-x')}} f(-x') + U,$$

where $T_{x'}(t) = t + x'$. Since $T_{x'}$ and $T_{f(-x')}$ are isomorphisms, we know that f is flat over $f(-x') + U$. Thus f_K is a flat morphism.

If $y \in Y(L)$ for an extension L of K, $f_K^{-1}(y)$ is a variety defined over L. By Hilbert's Nullstellensatz (Hilbert's zero theorem), it has a point rational over any algebraic closure of L. Thus we may assume that $\overline{K}$ is an algebraic closure of K.

If x_K is a closed point on $X_K(\overline{K})$, we have a finite extension L of K such that $x_K \in X(L)$. Take a valuation ring B of L over A, by the valuative criterion of properness (see Proposition 4.23), we have a unique $x \in X(B)$ giving rise to x_K at the generic fiber. Similarly, we have a unique $y \in Y(B)$ giving rise to $f(x)$. Thus f_K extends to an open set of X of codimension ≥ 2. Then by Lemma 5.12, it extends uniquely to X.

Let s be the closed point of S, and write $X(s)$ and $Y(s)$ for the special fibers at s. Let $k = k(s)$ be the residue field of A, and take a point $y_s \in Y(\overline{k})$ for an algebraic closure $\overline{k}$ of k. Since Y/S is smooth, we can find a valuation ring (unramified over A) such that y_s extends to a section $y \in Y(B)$. Since f is surjective, we can find $x_K \in X(\overline{K})$ such that $f_K(x_K) = y_K$. By extending B further if necessary, we may assume that x extends uniquely to $x \in X(B)$. Then by definition, $f(x) = y$, and hence $f_s : X(\overline{k}) \to Y(\overline{k})$ is surjective. This implies that f_s is flat by the argument at the beginning of the proof. Thus f is fiber by fiber flat, and hence f itself is flat (see [EGA] IV.11.3.10). By the surjectivity, f is faithfully flat. The morphism f is proper by Exercise 4.24.

If X and Y have equal dimension, wehave $\dim f^{-1}(y) = \dim X - \dim Y$ by [GME] Theorem 1.9.6, and $\dim f^{-1}(y) = 0$ for each geometric point $y \in Y$, and hence f is quasi finite. By the properness, $f_*(\mathcal{O}_X)$ is a coherent $\mathcal{O}_Y$–module (see [EGA] III.3.2.1) and hence, f is finite. Thus f is locally free of finite rank. □

We call a morphism of irreducible schemes *dominant* if the closure of the image is total.

Theorem 5.19. *Let A be a Dedekind domain, and write $S = \mathrm{Spec}(A)$. Let $X_{/S}$ and $Y_{/S}$ be abelian schemes over S. Then we have*

1. *If $f : X \to Y$ is a dominant S–homomorphism, then $\mathrm{Im}(f) = Y$, $\mathrm{Ker}(f) = X \times_{Y,\mathbf{0}_Y} S$ is a flat proper group scheme, and if f is generically smooth, it is an extension of an abelian scheme by a finite étale group scheme over an open dense subscheme of S.*
2. *If $f : X \to Y$ is a dominant S–homomorphism and $\dim_S X = \dim_S Y$, then $\mathrm{Ker}(f)$ is a finite flat group scheme over S, whose Cartier dual is given by $\mathrm{Ker}(f^t : Y^* \to X^*)$. Here X^* is the dual abelian scheme, and $f^t(\mathcal{L}) = f^*(\mathcal{L})$ for $\mathcal{L} \in \mathrm{Pic}_{Y/S}$.*

(3) *If $f : X \to Y$ is an S–homomorphism generically smooth, then there exists an abelian scheme W over a dense open subscheme O of S and S–homomorphisms $\pi : W_{/O} \to Y_{/O}$ and $\widetilde{f} : X_{/O} \to W_{/O}$ such that $f = \pi \circ \widetilde{f}$, π is finite over $\mathrm{Im}(\pi)$ and $\widetilde{f}$ is smooth and faithfully flat.*

Proof. Since f is proper, there exists a unique reduced closed subscheme $W = \mathrm{Im}(f)$ such that $|W_T| = |f_T(X_T)|$ set-theoretically for all S–schemes T. If f is dominant, its image W contains a generic point of Y, and $W = Y$ (because $\mathrm{Im}(f)$ is closed and Y is irreducible). The scheme W represents a group functor; so, it is a group subscheme of Y. Since X is irreducible, W is irreducible.

Suppose that f is dominant. We have the inclusion $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$. We take the integral closure $\mathcal{A}$ of $\mathcal{O}_Y$ in $f_*\mathcal{O}_X$, which is the sheaf of $\mathcal{O}_Y$–algebras. Consider the normalization $\pi : \widetilde{Y} = \mathrm{Spec}_Y \mathcal{A} \to Y$ in $\mathcal{O}_X$. Then $\widetilde{Y}$ is a normal scheme finite affine over Y, and hence proper over S. By definition, we have $\widetilde{f} : X \to \widetilde{Y}$ with $\pi \circ \widetilde{f} = f$. Since the morphism $X \times_S X \to \widetilde{Y} \times_S \widetilde{Y}$ is dominant, $\mathcal{O}_{\widetilde{Y}} \otimes_{\mathcal{O}_S} \mathcal{O}_{\widetilde{Y}}$ injects into $f_*\mathcal{O}_X \otimes_{\mathcal{O}_S} f_*\mathcal{O}_X$, which is a sheaf of integral domains (because $X_{/S}$ is smooth). It is known that for a field k and integrally closed k–algebras R and R' whose quotient fields are separable over k, $R \otimes_k R'$ is integrally closed as long as $R \otimes_k R'$ is an integral domain (see [BCM] V.1.7). Applying this fact to the quotient field k of $\mathcal{O}_S$ and replacing S by its dense open subset, we may assume that $\widetilde{Y} \times_S \widetilde{Y}$ is the normalization of $Y \times_S Y$ in $X \times_S X$. Consider the multiplication $m : X \times_S X \to X$. Since f is a homomorphism of group scheme, $m^{\#}$ takes $\mathcal{O}_Y$ into $\mathcal{O}_Y \otimes_{\mathcal{O}_S} \mathcal{O}_Y$ and hence induces a morphism $m_{\widetilde{Y}} : \widetilde{Y} \times_S \widetilde{Y} \to \widetilde{Y}$ to their normalizations. Similarly, the inverse $-1 : Y \to Y$ extends uniquely to $\widetilde{Y}$ by the uniqueness of the normalization. The scheme $\widetilde{Y}$ has the $\mathbf{0}$–section given by $\widetilde{f} \circ \mathbf{0}_X$. Thus $\widetilde{Y}$ is a group scheme, and $\widetilde{f} : X \to \widetilde{Y}$ and $\pi : \widetilde{Y} \to Y$ are homomorphisms. By our assumption, generically, the function field of X is a separable extension of the function field of $\widetilde{Y}$. Thus $\widetilde{f}$ is generically smooth.

Let $g : T \to S$ be an irreducible group scheme over an irreducible scheme S. Suppose that g is faithfully flat and that g is generically smooth, fiber by fiber. Since smoothness is a property of stalks, it is an open property; so, g is smooth over a dense open subset $U \subset T$. Since g is faithfully flat, we may assume that U is faithfully flat over an open subset $O = g(U) \subset S$. Let $x \in T$ be a non-smooth geometric point of g over O. Then we can find another geometric point $u \in T$ such that $x + u \in U$. Thus writing the translation by u as $T_u : T_{/O} \cong T_{/O}$, we find $g \circ T_u = g$. Since T_u is an isomorphism, g is smooth over $x \Leftrightarrow g$ is smooth over $T_u(x) = u + x$. This shows that g is everywhere smooth over O.

We apply the above argument to $g : \widetilde{Y} \to S$. Since the integral closure of $\mathcal{O}_S$ in $\mathcal{O}_X$ is equal to $\mathcal{O}_S$ (because X is proper smooth), the same is true in $\mathcal{O}_{\widetilde{Y}}$. Thus the quotient field of $\widetilde{Y}$ is a separable extension of k, and hence g is generically smooth. Since $\widetilde{Y}$ is an irreducible group scheme, the morphism g is smooth on a dense open subset of S. Thus again replacing S by its dense open subset if necessary, we may assume that $\widetilde{Y} \to S$ is smooth; so, $\widetilde{Y}$ is an abelian scheme over S.

Since $\widetilde{f}$ is generically smooth, $\widetilde{f}$ is smooth over an open subset $U \subset X$. Since fibers of X and $\widetilde{Y}$ are smooth, we may assume that U is faithfully flat over a dense open subset $O \subset S$. By Lemma 5.18, $\widetilde{f}$ is a flat morphism. Since flat morphisms are open maps, $\widetilde{f}(U)$ is open. Let $x \in X$ be a non-smooth geometric point of f over O. Then we can find another geometric point $u \in X$ such that $x + u \in U$. Then on a small neighborhood V of x, f factors as

$$\widetilde{f}_V : V \xrightarrow{T_{-u}} U \xrightarrow{\widetilde{f}} \widetilde{f}(U) \xrightarrow{T_{f(u)}} \widetilde{f}(V).$$

Since the translations are isomorphisms, $\widetilde{f}$ itself is smooth over O. This shows that $\mathrm{Ker}(\widetilde{f})$ is a smooth proper group scheme over O. Since it is noetherian, $\mathrm{Ker}(\widetilde{f})$ is a finite union of connected irreducible components over O. Write $G_{/O}$ for the identity component. Then G is proper smooth geometrically irreducible; so, it is an abelian scheme over O.

Since $f = \pi \circ \widetilde{f}$, $\mathrm{Ker}(f)$ contains $\mathrm{Ker}(\widetilde{f})$. Since $\widetilde{f}$ and f are both proper faithfully flat, and $\dim_S \widetilde{Y} = \dim_S Y$, we see that $\dim_S \mathrm{Ker}(\widetilde{f}) = \dim_S \mathrm{Ker}(f)$. Thus again $\mathrm{Ker}(f)$ is a finite disjoint union of the translation of G. This proves (1).

When $\dim_S X = \dim_S Y$, f is quasi finite. Since f is proper, it is locally free of finite rank by Lemma 5.8 (and hence affine). Thus $\mathrm{Ker}(f)$ is a locally free group scheme of finite rank.

We construct a non-degenerate pairing $\langle\ ,\ \rangle : \mathrm{Ker}(f) \times \mathrm{Ker}(f^t) \to \mathbb{G}_m$: Let $\mathcal{L} \in \mathrm{Ker}(f^t) \subset Y^*$. We may assume that $\mathbf{0}^*\mathcal{L} = \mathcal{O}_S$. Cover Y by affine open sets $U_i = \mathrm{Spec}(A_i)$ so that $\mathcal{L}|_{U_i} = \phi_i^{-1}\mathcal{O}_{U_i}$. Then $(\phi_i/\phi_j) \circ \mathbf{0}_Y = 1$ for all i and j, and $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, because f is affine. Then $f^*\mathcal{L}|_{f^{-1}(U_i)} = (\varphi_i)^{-1}\mathcal{O}_{f^{-1}(U_i)}$ for $\varphi_i = \phi_i \circ f$, and for every point $(P : T \to X) \in \mathrm{Ker}(f)(T)$, we have

$$(\varphi_i \circ P)/(\varphi_j \circ P) = (\phi_i \circ f \circ P)/(\phi_j \circ f \circ P) = (\phi_i \circ \mathbf{0}_Y)/(\phi_j \circ \mathbf{0}_Y) = 1.$$

This implies that $\{\varphi_i \circ P\}$ glues together giving rise to a section $\varphi \in \mathbb{G}_{m/S}(T)$. We then define $\langle P, \mathcal{L}\rangle = \varphi$. If $(\varphi_i|_{\mathrm{Ker}(f)})/(\varphi_j|_{\mathrm{Ker}(f)}) = 1$ for all i and j, then the sections ϕ_i glue to the constant function 1, and hence $\mathcal{L}$ has to be trivial. Thus $\mathrm{Ker}(f^t)(T)$ injects into $\mathrm{Hom}_{gp}(\mathrm{Ker}(f), \mathbb{G}_m) = (\mathrm{Ker}(f))^*(T)$ for all S–scheme T. By the Key lemma, we have an immersion $\mathrm{Ker}(f^t) \hookrightarrow (\mathrm{Ker}(f))^*$, which is a closed immersion, since $\mathrm{Ker}(f^t)$ is finite. By the first assertion already proven, f^t is locally free of finite rank, and hence $\mathrm{Ker}(f^t)$ is a locally-free group scheme. Thus $\deg(f^t) \le \deg(f)$.

Since X is a $\mathrm{Ker}(f)$–torsor over Y, we have $X \times_Y X \cong \mathrm{Ker}(f) \times_S Y$. Thus for any $\zeta \in \mathrm{Ker}(f)^*$, we can find a function $\phi : \mathrm{Ker}(f) \times_S Y \to \mathbf{P}^1$ such that $\phi(x + t) = \zeta(t)\phi(x)$ for $t \in \mathrm{Ker}(f)$. The function gives rise to a divisor D on $Y \times_S X$ such that $f_X^{-1}D$ is the divisor of ϕ. In other words, the invertible sheaf $\mathcal{L} = \mathcal{L}(D)$ over $Y \times_S X$ satisfies

$$\langle P, \mathcal{L}(D)\rangle = \zeta(P).$$

Since the choice of ζ is arbitrary, the pairing induces a surjection $\mathrm{Ker}(f^t)(T)$ onto $\mathrm{Ker}(f)^*(T)$ for all S–scheme T. Thus $\deg(f) \le \deg(f^t)$, and hence they are equal: $\deg(f) = \deg(f^t)$. This implies $\mathrm{Ker}(f^t) \cong \mathrm{Ker}(f)^*$. Since Cartier duality is perfect, we get $\mathrm{Ker}(f^t)^* \cong \mathrm{Ker}(f)$. This shows the second assertion.

We now prove (3). Since f is proper, the image of f in the topological space $|Y|$ is associated to a closed subscheme $\mathrm{Im}(f)$. The scheme structure of $\mathrm{Im}(f)$ is unique if we require it to be reduced. We write this scheme as W_0. By definition, f factors through W_0. Any point $P \in |W_0|$ comes from $Q \in |X|$. Thus $|W_0| + P = |\,\mathrm{Im}(f \circ T_Q)| = |W_0|$. By the uniqueness of the reduced structure, we find that the addition $m : Y \times_S Y \to Y$ induces an addition $m_0 : W_0 \times_S W_0 \to W_0$. Thus W_0 is an irreducible group subscheme of Y. Let W be the normalization of W_0 in X. Replacing S by its open subscheme, we can show that W is a group scheme and that $\pi : W \to W_0$ is a finite S–homomorphism, in the same manner as in the case $\widetilde{Y} \to Y$. By definition, we have an S–homomorphism $\widetilde{f} : X \to W$ with $f = \pi \circ \widetilde{f}$, which is generically smooth. Further shrinking S if necessary, we may assume that W is an abelian scheme over S. Then generic smoothness of $\widetilde{f}$ implies that $\widetilde{f}$ is smooth on a dense open subset of S, as desired. □

We assume to have an embedding $i_\infty : A \hookrightarrow \mathbb{C}$. Let $X_{/S}$ be an abelian scheme of relative dimension d. Since $X(\mathbb{C})$ is a commutative complex Lie group, the universal covering space H of $X(\mathbb{C})$ is a simply connected commutative Lie group of dimension d. It has to be a d–dimensional complex vector space. Then there exists a lattice $L = \pi_1(X(\mathbb{C}))$ in H, and $X(\mathbb{C}) \cong L\backslash H$. In particular, $X(\mathbb{C})$ is a divisible group. This implies the multiplication by a positive integer $[N] : X(\mathbb{C}) \to X(\mathbb{C})$ is surjective. Then by Lemma 5.18, $[N] : X \to X$ is locally free of finite rank.

Corollary 5.20. *Assume that $S = \mathrm{Spec}(A)$ with a Dedekind domain A, and let $X_{/S}$ be an abelian scheme of relative dimension d. Let $\mathrm{Spec}(k) \hookrightarrow S$ be a geometric point. Then we have*

1. *The multiplication by a positive integer N is a locally free morphism of degree N^{2d}.*
2. *If N is invertible over S, $X[N] = \mathrm{Ker}(N : X \to X)$ is an étale group scheme of rank N^{2d}. In general, $X[N]$ is a locally free group of rank N^{2d}; in particular, $X[p^\infty]$ is a Barsotti–Tate group over S.*
3. *The group $X(k)$ is divisible.*
4. *If $p > 0$ is the characteristic of a geometric point $s : \mathrm{Spec}(k) \hookrightarrow S$, then $X[p^n](k) \cong (\mathbb{Z}/p^n\mathbb{Z})^r$ with $0 \le r \le d$. The number r is called the p–rank of $X_{/S}$ at $s = \mathrm{Spec}(k)$.*

For simplicity, we shall prove the result only for Dedekind domains A inside $\mathbb{C}$ (this applies even to $\mathbb{Z}_p$ or its finite extension, since we can embed $\overline{\mathbb{Q}}_p$ into $\mathbb{C}$). The assertion in the corollary actually holds without assuming that A is inside $\mathbb{C}$. Only point we use this fact is the computation of $\deg[N]$. We refer the reader to Mumford's book [ABV] Sections 6 and 15 for a more general treatment.

The morphism $i : X \to (X^*)^*$ induces an isomorphism $X[N] \cong (X^*)^*[N]$ for all positive integer N by Theorem 5.19 (2). This shows in particular that $(f^t)^t = f$. Thus i has to be an isomorphism at the generic fiber, and hence by Theorem 5.19 (1), $X \cong (X^*)^*$ canonically. A more direct (and cohomological) proof of this fact can be found in [ABV] Section 13.

Proof. Since $N : X \to X$ is locally free, we can compute the rank, looking into the fiber over $\mathbb{C}$, and we get $\deg[N] = |\pi_1(X(\mathbb{C}))/N\pi_1(X(\mathbb{C}))| = N^{2d}$. This proves (1).

By (1) of Theorem 5.19, $X[N]$ is proper flat quasi-finite; so, it is a finite flat group scheme. Then by rank comparison of $X[p^n]$ and $X[p^{n+1}]$, we can verify that the group $X[p^\infty]$ is a Barsotti–Tate group. Let T_x be the translation by $x \in \underline{X}(T)$ for an S–scheme T. For each tangent vector ∂ at $\mathbf{0}$, we define $\mathcal{O}_S$–derivation $\widetilde{\partial}$ of $\mathcal{O}_X$ by $(\widetilde{\partial}\phi)(x) = \partial(\phi \circ T_{-x})$. Thus $\mathcal{T}_{X/S} = f^*(\mathbf{0}^*\mathcal{T}_{X/S})$ for the tangent bundle $\mathcal{T}_{/X}$. Write $f : X \to S$ for the structure morphism. In particular, $f_*\mathcal{T}_{/X}$ is a locally free $\mathcal{O}_S$–module of rank d. Taking the dual, $f_*\Omega_{X/S}$ is also a locally free $\mathcal{O}_S$–module. Take an open subscheme U of S such that over U, $f_*\Omega_{X/S}$ is free of rank d, and $f_*\Omega_{X/S}$ is made of translation invariant differentials. Choose a base $\omega_1, \ldots, \omega_d$ of $f_*\Omega_{X/S}|_U$, Let $\phi : X \to X$ be a locally free S–homomorphism. Then $\phi^*\omega_i$ is again a translation invariant differential; so, it is a linear combination of $\{\omega_j\}$. We then get a matrix $\lambda(\phi) \in M_d(\mathcal{O}_U)$ by $\phi^*(\omega_1, \ldots, \omega_d) = (\omega_1, \ldots, \omega_d)\lambda(\phi)$. We may assume $U = \mathrm{Spec}(B)$ for a localization B of A. We embed B into $\mathbb{C}$ and compute $\lambda(N)$. Since over $\mathbb{C}$, $X(\mathbb{C}) = L\backslash\mathbb{C}^d$ for a lattice L, and invariant differentials are given by du_i for the coordinate $(u_1, \ldots, u_d)$ of $\mathbb{C}^d$. This shows that $\lambda(N) = N$. In particular, $N : X \to X$ induces multiplication by N on $\Omega_{X/S}$. Thus if N is invertible on S, the pull back map of N is surjective on differentials, which shows that $N : X \to X$ is étale finite if N is invertible on S. This proves (2).

The assertion (3) follows from the locally freeness of $N : X \to X$, which implies $N : X(k) \to X(k)$ is surjective for an algebraically closed field k.

Let $p > 0$ be the characteristic of k. Consider $X[p]_{/k}$ as a group scheme. Then $\mathrm{rank}\, X[p] = p^{2d}$. Since $p : X \to X$ induces the zero map on $\Omega_{X/k}$, the cotangent space of $X[p]_{/k}$ at $\mathbf{0}$ is equal to $\Omega_{X/k}$ (see [GME] Proposition 1.5.4). Thus $\mathcal{O}_{X[p]_{/k}}$ covers surjectively $k[T_1, \ldots, T_d]/(T_1^2, \ldots, T_d^2)$, where T_j is the local parameters at $\mathbf{0}_X$. Since the rank of $X[p]$ is p^{2d}, $\mathcal{O}_{X[p]_{/k}}$ covers $k[T_1, \ldots, T_d]/(T_1^2, \ldots, T_d^2)$, and the rank of the connected component C of $X[p]$ is greater than or equal to p^d. Since the maximal étale quotient of $X[p]$ also have p–power order p^r, we find that $p^r \times \mathrm{rank}\, C = p^{2d}$. This combined with $\mathrm{rank}\, C = p^h$ with $h \geq d$ shows (4). □

Now assume that $S = \mathrm{Spec}(A)$ for a Dedekind domain A inside $\mathbb{C}$. We consider the complex torus $X(\mathbb{C}) = \mathbb{C}^d/L$ for $L = \pi_1(X(\mathbb{C}))$. We study the complex analytic cohomology group $H^1_{an}(X(\mathbb{C}), (\mathcal{O}_X^{an})^\times)$ for the sheaf $\mathcal{O}_X^{an}$ of complex analytic functions on $X(\mathbb{C})$, which classifies the complex analytic line bundles. We have an exact sequence of sheaves of analytic functions:

$$0 \to 2\pi i\mathbb{Z} \to \mathcal{O}_X^{an} \xrightarrow{\exp} (\mathcal{O}_X^{an})^\times \to 0.$$

The sheaf cohomology sequence attached to this short exact sequence gives another one:

$$0 \to 2\pi i\mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \to H^1_{an}(X(\mathbb{C}), 2\pi i\mathbb{Z}) \to H^1_{an}(X(\mathbb{C}), \mathcal{O}_X^{an}) \xrightarrow{\exp} H^1_{an}(X(\mathbb{C}), (\mathcal{O}_X^{an})^\times).$$

The image of the cohomological exponential map gives rise to $X^*(\mathbb{C})$, because all meromorphic function on $X(\mathbb{C})$ is algebraic (since $X(\mathbb{C})$ is projective: [ABV] Section 3). By using this, if $f : X \to Y$ is a finite homomorphism of abelian schemes, $\deg(f^t)$ is equal to the index of $H^1_{an}(X(\mathbb{C}), 2\pi i\mathbb{Z})$ in $H^1_{an}(Y(\mathbb{C}), 2\pi i\mathbb{Z})$. Since these lattices are dual of $\pi_1(X(\mathbb{C}))$ and $\pi_1(Y(\mathbb{C}))$, respectively, we rediscover $\deg(f) = \deg(f^t)$.

Now assume that $X = J$ is the jacobian scheme for a smooth curve $C_{/S}$. Since algebraic line bundles are automatically analytic line bundles, we have a natural map: $J(\mathbb{C}) \to H^1_{an}(C(\mathbb{C}), (\mathcal{O}_C^{an})^\times)$. This map is injective, because any meromorphic function on the compact Riemann surface $C(\mathbb{C})$ can be considered to be a holomorphic map from $C(\mathbb{C})$ to $\mathbf{P}^1(\mathbb{C})$, which is algebraic.

We have an exact sequence:

$$0 \to 2\pi i\mathbb{Z} \to \mathcal{O}_C^{an} \xrightarrow{\exp} (\mathcal{O}_C^{an})^\times \to 0.$$

The sheaf cohomology sequence attached to this short exact sequence gives another one:

$$0 \to 2\pi i\mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \to H^1_{an}(C(\mathbb{C}), 2\pi i\mathbb{Z}) \to H^1_{an}(C(\mathbb{C}), \mathcal{O}_C^{an}) \\ \to H^1_{an}(C(\mathbb{C}), (\mathcal{O}_C^{an})^\times) \xrightarrow{\deg} H^1_{an}(C(\mathbb{C}), 2\pi i\mathbb{Z}) \cong \mathbb{Z} \to 0.$$

Since we have the Hodge exact sequence:

$$0 \to H^0_{an}(C(\mathbb{C}), \Omega_C) \to H^1_{an}(C(\mathbb{C}), \mathbb{C}) \to H^1_{an}(C(\mathbb{C}), \mathcal{O}_C^{an}) \to 0,$$

$H^1_{an}(C(\mathbb{C}), \mathcal{O}_C^{an})$ is the dual of $H^0_{an}(C(\mathbb{C}), \Omega_C^{an})$ by the Poincaré duality; so, we have an isomorphism: $H^1_{an}(C(\mathbb{C}), \mathcal{O}_C^{an}) \cong \mathbb{C}^g$. Comparing complex dimension of the image of $J(\mathbb{C})$ in $H^1_{an}(C(\mathbb{C}), (\mathcal{O}_C^{an})^\times)$, we conclude

$$J(\mathbb{C}) \cong H^1_{an}(C(\mathbb{C}), \mathcal{O}_C^{an})/H^1_{an}(C(\mathbb{C}), 2\pi i\mathbb{Z}), \tag{5.2}$$

canonically.

There is a p–adic analog due to Tate of this Hodge decomposition. Let C be a smooth irreducible curve over $S = \mathrm{Spec}(W)$ for a p–adic valuation ring W finite flat over $\mathbb{Z}_p$. We write $\mathbb{C}_p$ for the p–adic completion of $\overline{\mathbb{Q}}_p$. By continuity, $\mathcal{G} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts continuously on $\mathbb{C}_p$. Then we have the following $\mathcal{G}$–linear isomorphism:

$$\mathrm{Hom}(T_p(X), \mathbb{C}_p) \cong H^1(J, \mathcal{O}_{J/\mathbb{C}_p}) \oplus \left(H^0(J, \Omega_{J/\mathbb{C}_p}) \otimes_{\mathbb{Q}_p} \mathrm{Hom}(\mathbb{Q}_p(1), \mathbb{C}_p)\right). \tag{5.3}$$

Here $\mathbb{Q}_p(1)$ is the Galois module $(\varprojlim_n \mu_{p^n}(\overline{\mathbb{Q}})) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and we regard these modules as $\mathcal{G}$–modules letting $\mathcal{G}$ act non-trivially on every term which has natural Galois action. Thus $\sigma\phi = \sigma \circ \phi \circ \sigma^{-1}$ for $\phi \in \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X), \mathbb{C}_p)$, and $\sigma(a \otimes \varphi) = \sigma(a) \otimes (\sigma \circ \varphi \circ \sigma^{-1})$ for $a \in H^0(J_{/\mathbb{C}_p}, \Omega_{J/\mathbb{C}_p})$ and $\varphi \in \mathrm{Hom}(\mathbb{Q}_p(1), \mathbb{C}_p)$. Actually Tate proved this type of p–adic Hodge decomposition for all abelian schemes over W and also for Barsotti–Tate groups over W in [T]. Since the proof is a bit involved, though elementary, we just quote this result for our later use. This type of decomposition, now called a Hodge-Tate decomposition, has been vastly generalized to general (geometric) p–adic Galois modules by Fontaine (see [PHT]).

5.6. **Endomorphism of abelian schemes.** In this subsection, we briefly recall the structure theory of endomorphism algebras of abelian schemes. More details can be found in Mumford's book [ABV] Chapter IV and for the theory of abelian varieties with complex multiplication, we refer to Shimura's book [ACM] Chapter II. Here an abelian scheme $X_{/S}$ is called *"of CM type"* or "with complex multiplication" if it has a commutative semi-simple subalgebra $M \subset \mathrm{End}_S^{\mathbb{Q}}(X)$ with $[M : \mathbb{Q}] = 2\dim_S(X)$. As shown by Tate (cf., Appendix I), an abelian variety X defined over a finite field does have complex multiplication. For an abelian variety E of dimension 1, that is, an elliptic curve, this fact follows from the existence of the Frobenius map $F \in \mathrm{End}(E)$, since F satisfies a quadratic equation with negative discriminant (see Hasse's Theorem in [GME] §2.6.3).

Let X and Y be an abelian scheme over $S = \mathrm{Spec}(A)$ for a Dedekind domain A. An S–morphism $f : X \to Y$ is called an S–*isogeny* if f is locally free of finite rank and is a group homomorphism. Suppose f is an S–isogeny. Then $\mathrm{Ker}(f)$ is a locally free group scheme of rank $N = \deg(f)$, and $\underline{\mathrm{Ker}(f)}(T)$ is always killed by N. In particular, for $x \in \underline{X}(T)$, Nx depends only on $f(x) \in \underline{Y}(T)$. Thus $f(x) \mapsto Nx$ is well defined at least on the image of f. For each $y \in \underline{Y}(T)$, we take a faithfully flat extension $T'_{/T}$ so that $y = f(x)$ with $x \in \underline{X}(T')$. Since the ambiguity of x falls in $\mathrm{Ker}(f)$, which is killed by N, by descent, we see $Nx \in \underline{X}(T)$, and hence the functorial map $f' : \underline{Y} \to \underline{X}$ taking y to Nx is well defined. This shows that we have an S–isogeny $f' : Y \to X$ such that $f' \circ f = [N]_X$. Since

$$f \circ f' \circ f - [N]_Y \circ f = f \circ f' \circ f - f \circ [N]_X = f \circ f' \circ f - f \circ f' \circ f = \mathbf{0}_Y,$$

the generic surjectivity of f tells us that $f \circ f' = [N]_Y$.

Now suppose for the moment that $S = \mathrm{Spec}(k)$ for a perfect field k. We consider a homomorphism $f : X \to Y$ of abelian schemes. Let $\pi' : W' = \mathrm{Im}(f) \to \mathrm{Spec}(k)$ with reduced scheme structure. Then W' is a proper, reduced and geometrically irreducible group scheme. Thus $\pi_*\mathcal{O}_{W'} = \widetilde{k}$ for the integral closure $\widetilde{k}$ of k in the function field of W'. Since W' is geometrically irreducible, we see that $\widetilde{k}/k$ is purely inseparable. Since k is perfect, we have $\widetilde{k} = k$; so, W' is generically smooth. Since W'

is a group scheme, it has to be an abelian variety (so it is smooth everywhere). By Theorem 5.19 applied to $f : X \to W'$, we find an abelian scheme W over k with a finite morphism $\pi : W \to W' \subset Y$ and a faithfully flat smooth homomorphism $\widetilde{f} : Y \to W$ such that $f = \pi \circ \widetilde{f}$.

Consider the kernel $\mathrm{Ker}(f)$, which is a proper flat group scheme over k. Again by Theorem 5.19, the identity component V of $\mathrm{Ker}(\widetilde{f})$ is an abelian variety, and $\mathrm{Ker}(\widetilde{f})$ is an extension of V by finite étale group scheme. Suppose that a positive integer N kills the quotient $\mathrm{Ker}(\widetilde{f})/V$. Then $[N] \circ \widetilde{f}$ induces a functorial map: $\underline{W} \to \underline{W}$ by an argument similar to the proof of the existence of f' as above, and hence a k–isogeny $[N] \circ \widetilde{f} : W \to W$.

Now assume that $X = Y$. Consider $[N] \circ \widetilde{f} : W \to W$. By definition, $\mathrm{Ker}(\widetilde{f}) \times_X W \subset \mathrm{Ker}([N] \circ \widetilde{f} : W \to W)$ which is a finite group. Thus $V \times_X W = V \cap W$ is a finite group. We consider the morphism $i : V \times_S W \to X$ given by $(v, w) \mapsto v + \pi(w)$. If $i(v, w) = 0$, then $v = -\pi(w) \in X$. Thus $\mathrm{Ker}(i) \cong V \times_X W$; so, i is an isogeny.

By this argument, any abelian scheme X over a field k is isogenous to a product $\prod_j X_j^{e_j}$ for simple abelian varieties X_j over k. Here an abelian scheme $X_{/k}$ is *k-simple* if $\mathrm{End}_S^{\mathbb{Q}}(X) = \mathrm{End}_S(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra. If k is algebraically closed, a k-simple abelian scheme is just called *simple*.

If X has an abelian subscheme $i : V \hookrightarrow X$, by taking the dual, we have a morphism $i^* : X^* \to V^*$. Since X and X^* are isogenous, having a quotient abelian scheme and having an abelian subscheme are equivalent. Thus $X_{/k}$ is simple if and only if it does not have non-trivial abelian scheme quotients or equivalently does not have non-trivial abelian subschemes.

Theorem 5.21. *Let $S = \mathrm{Spec}(A)$ for a Dedekind domain A whose residue fields are all perfect. For an abelian scheme $X_{/S}$, we let $O = \mathrm{End}_S(X)$ be the ring of S–endomorphisms of groups schemes. We put $\mathrm{End}_S^{\mathbb{Q}}(X) = \mathrm{End}_S(X) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $B = \mathrm{End}_S^{\mathbb{Q}}(X)$ is a semi-simple algebra of finite dimension over $\mathbb{Q}$, and O is an order of B (that is a subring which is a lattice of B). We have $\dim_{\mathbb{Q}} B \le 4d^2$ for $d = \dim_S X$.*

Proof. Take a geometric point $s = \mathrm{Spec}(k)$ of S, and choose a prime p so that it is different from the characteristic of k. Write $X(s)$ for the fiber of X at s. Then $X(s)[p^n]$ is a constant group scheme over the algebraically closed field k isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{2d}$, where $d = \dim_S X$. The module $T_p(X) = \varprojlim_n X[p^n](k)$ is a free $\mathbb{Z}_p$–module of rank $2d$ (see Corollary 5.20). By Lemma 5.18 (or Theorem 5.19), $\mathrm{End}_S(X)$ injects into $\mathrm{End}_s(X(s))$. Thus we only need to prove the assertion for $X(s)$.

We claim

$$O_s = \mathrm{End}_s(X(s)) \otimes_{\mathbb{Z}} \mathbb{Z}_p \text{ injects into } \mathrm{End}_{\mathbb{Z}_p}(T_p(X)). \tag{5.4}$$

Let us prove the claim. If $f \in O_s$ is mapped to $p^n T$ for $T \in \mathrm{End}_{\mathbb{Z}_p}(T_p(X))$. Then f kills $G = X(s)[p^n]$. Thus we have a commutative diagram for a morphism $g : X \to X$:

$$\begin{array}{ccc} X(s) & \xrightarrow{p^n} & X(s) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ X(s) & = & X(s), \end{array}$$

because X is the quotient of X by the constant finite group G under the translation action (see [GME] §1.8.3). Thus $f = p^n g$ in O_s. This shows that $O_s/p^n O_s$ injects into $\mathrm{End}_{\mathbb{Z}_p}(T_p(X)/p^n T_p(X))$. Taking the projective limit, we get the claim.

By the claim, we have

$$\mathrm{rank}_{\mathbb{Z}} O \le \mathrm{rank}_{\mathbb{Z}_p} O_s \le \mathrm{rank}_{\mathbb{Z}_p} \mathrm{End}_{\mathbb{Z}_p}(T_p(X)),$$

which proves the dimension inequality.

Write $B_s = \mathrm{End}_s^{\mathbb{Q}}(X(s))$ for a geometric point $s \in S$. As already seen before stating the theorem, $X(s)$ is isogenous to $\prod_j X_j^{e_j}$ for simple abelian varieties X_j over s; so, $B_s \cong \prod_j M_{e_j}(D_j)$ for an algebra $D_j = \mathrm{End}_s^{\mathbb{Q}}(X_j)$. Since X_j is simple, D_j is finite dimensional division algebra. Thus B_s is semi-simple.

Taking s to be the generic point η of S, by the above expression of B_η, we can find a base $\{f_1,\dots,f_r\}$ of B_η over $\mathbb{Q}$ so that $f_j : X(\eta) \to X(\eta)$ is surjective. By Lemma 5.18, f_j extends to an endomorphism of X, and $B = \mathrm{End}_S^{\mathbb{Q}}(X)$ coincides with B_η; so, B is semi-simple. □

For any given semi-simple algebra B over $\mathbb{Q}$, we have a number field K such that

$$B \otimes_{\mathbb{Q}} K \cong \bigoplus_i M_{n_i}(K)$$

for the $n \times n$ matrix algebra $M_n(K)$ (see [MFG] 2.1.4). We then define the (reduced) norm map $N_B : B \to K$ by $N_B(x_i) = \prod_i \det(x_i)$ for $x_i \in M_{n_i}(K)$. We may assume that $K/\mathbb{Q}$ is a Galois extension. Then an element $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$ acts on $B \otimes_{\mathbb{Q}} K$ on the right factor. By definition, $N_B(\sigma(x)) = \sigma(N_B(x))$. Since the image of B is fixed by this action, we conclude that the norm actually has values in $\mathbb{Q}$ on B.

Since $N_B : B \to \mathbb{Q}$ is a polynomial map (regarding B as a $\mathbb{Q}$-vector space), we can regard it as a morphism of $\mathbb{Q}$–schemes. In other words, defining functors $\underline{B}, \underline{\mathbb{Q}} : ALG_{/\mathbb{Q}} \to SETS$ by $\underline{B}(\mathcal{A}) = B \otimes_{\mathbb{A}} \mathcal{A}$ and $\underline{\mathbb{Q}}(\mathcal{A}) = \mathcal{A}$ for $\mathbb{Q}$–algebras $\mathcal{A}$, N_B induces a morphism of functors: $\underline{B} \to \underline{\mathbb{Q}}$. Thus we can think of $N_B : \underline{B}(\mathbb{Q}[T]) \to \mathbb{Q}[T]$. For each $\alpha \in B$, we define its characteristic polynomial $F_\alpha(T)$ by $N_B(T1_B - \alpha) \in \mathbb{Q}[T]$. By definition, we have $F_\alpha(\alpha) = 0$ in B. Since B is semi-simple, we can write $\alpha = \sigma + \nu$ for mutually commuting, a semi-simple σ and a nilpotent ν (Jordan decomposition). Taking a suitable semi-simple commutative subalgebra F of B of dimension $\sum_i n_i$ containing σ, we find

$$F_\alpha(T) = N_{F/\mathbb{Q}}(T - \sigma). \tag{5.5}$$

Now we apply this argument to $B = \mathrm{End}_S^{\mathbb{Q}}(X)$ for an abelian scheme $X_{/S}$. If $\alpha \in O = \mathrm{End}_S(X)$, α is integral over $\mathbb{Z}$, and hence $F_\alpha(T) \in \mathbb{Z}[T]$. Let us choose a geometric point $s \in S$. Then we regard B as a subalgebra of $E = \mathrm{End}_{\mathbb{Z}_p}(T_p(X(s))) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for a prime p different from the characteristic of s. Choose a commutative semi-simple $\mathbb{Q}$–subalgebra $F' \supset F \supset \mathbb{Q}(\sigma)$ of E with $\dim_{\mathbb{Q}} F' = 2d$ for $d = \dim_S X$. Then we have

$$P_\alpha(T) = N_{F'/\mathbb{Q}}(T - \sigma) = \det(T - \alpha) \tag{5.6}$$

regarding α as an element of E. On the other hand, by (5.5), $P_\alpha(T) = F_\alpha(T)^{[F':F]}$. This shows that $P_\alpha(T) \in \mathbb{Z}[T]$. Thus we have the following fact due to A. Weil:

Theorem 5.22. *Let the notation be as above. Then the characteristic polynomial $P_\alpha(T)$ of the matrix representation of $\alpha \in \mathrm{End}_S(X)$ on $T_p(X(s))$ is a monic polynomial in $\mathbb{Z}[T]$ of degree $2d$ with $d = \dim_S X$ and is independent of p and s as long as the characteristic of s is different from p. Inside $\mathrm{End}_S(X)$, we have $P_\alpha(\alpha) = 0$, and $P_\alpha(0) = \deg(\alpha)$.*

Proof. All the assertions follow from the last one, since $P_\alpha(T) = N(T1_B - \alpha) = \deg(T1_B - \alpha)$ and $N(\alpha) = P_\alpha(0)$. Suppose that $\deg(\alpha)$ is a p–power for a prime p. Suppose that p is not a zero-divisor on S. Writing $T_p(\alpha)$ for the endomorphism of $T_p(X(s))$ induced by α, we have $\mathrm{Ker}(\alpha) \cong T_p(X(s))/\alpha(T_p(X(s)))$, and hence $|\det(T_p(\alpha))|_p = |\deg(\alpha)|_p$. Since the two numbers are integers, we find $\det(T_p(\alpha)) = P_\alpha(0) = \pm\deg(\alpha)$. For general α, we can decompose $\alpha = \prod_p \alpha_p$ for p–isogenies. Thus if $\deg(\alpha)$ is prime to the characteristic of A, we have $\deg(\alpha) = \pm P_\alpha(0)$. This is enough to conclude the identity, because $\deg : B \to \mathbb{Q}$ is a polynomial map ([ABV] 18.2) and B is generated over $\mathbb{Q}$ by elements with deg prime to a given integer (see [ABV] Theorem 19.4 and [Mi] Section 12).

There is another argument showing $P_\alpha(0) = \deg(\alpha)$: B has a positive involution $\xi \mapsto {}^t\xi$ (the positivity means that $\xi \mapsto \mathrm{Tr}(\xi {}^t\xi)$ is positive definite; see Remark 5.25, [ABV] Section 21 and [ACM] Sections 1.3 and 5.1). Thus $\det(T_p(\alpha)) > 0$ if $\alpha \neq 0$, which shows the identity. □

Remark 5.23. Let $\mathbb{F}$ be a finite field of characteristic ℓ. If $X_{/\mathbb{F}}$ is a connected smooth group scheme such that $X \cong X_0 \times \mathbb{G}_m^r$ for an abelian scheme X_0 over a finite extension $\mathbb{F}'$, $\mathrm{End}_{\mathbb{F}'}(X) = \mathrm{End}_{\mathbb{F}'}(X_0) \times M_r(\mathbb{Z})$, because $\mathrm{End}_{\mathbb{F}}(\mathbb{G}_m) = \mathbb{Z}$. Thus the above argument still works well to produce $P_\alpha(T) \in \mathbb{Z}[T]$ for $\alpha \in \mathrm{End}_{\mathbb{F}}(X) (\subset \mathrm{End}_{\mathbb{F}'}(X))$. In this case, $P_\alpha(T)$ is of degree $2d_0 + r$ for $d_0 = \dim_{\mathbb{F}'} X_0$, because $\mathbb{G}_m[p^n] = \mu_{p^n}$ and hence $T_p(X) \cong \mathbb{Z}_p^{2d_0+r}$ if $p \neq \ell$. We still have $P_\alpha(0) = \deg(\alpha)$ if α is locally free of finite rank, and also $P_\alpha(\alpha) = 0$ in $\mathrm{End}_{\mathbb{F}'}(X)$.

There is a simple way of constructing homomorphisms between jacobian varieties by using covering of curves. We briefly explain the procedure. Let $C_{/S}$ and $C'_{/S}$ be a proper flat irreducible curves with jacobians $J_{/S}$ and $J'_{/S}$. We suppose that C and C' are regular. Another regular proper flat curve $C''_{/S}$ is called a correspondence if we have non-constant S–morphisms $\pi : C'' \to C$ and $\pi' : C'' \to C'$. Thus a correspondence is a triple: $T = (C'', \pi : C'' \to C, \pi' : C'' \to C')$. As we have seen, π and π' are locally free. For such a correspondence, we have an associated morphism: $T : J \to J'$ given by $T = J^t(\pi') \circ J(\pi) : J \to J'$. If $C = C'$ and $\pi = \pi'$, then $\pi_*\pi^*\mathcal{L} \cong \mathcal{L}^{\deg(\pi)}$ by definition (Exercise 5.24). Thus $T = [\deg(\pi)]$ in this case.

Define $T^t = (C'', \pi' : C'' \to C', \pi : C'' \to C)$ by interchanging the role of π and π'. Then $T^t = J^t(\pi) \circ J(\pi') : J' \to J$. Since $\pi_*\pi^*D = \deg(\pi)D$ and $\pi^*\pi_*D = \deg(\pi)D$ for divisors D, $J(\pi) \circ J^t(\pi) = [\deg(\pi)]$ and $J^t(\pi) \circ J(\pi) = [\deg(\pi)]$, where $[N]$ is the multiplication by $N \in \mathbb{Z}$ on the jacobian. $T \circ T^t = T^t \circ T = [\deg(\pi)\deg(\pi')]$.

Exercise 5.24. (1) *Prove* (5.5).

(2) *Give a detailed proof of* $\deg(\alpha) = P_\alpha(0)$ *for* $\alpha \in \mathrm{End}_S(X)$ *for an abelian scheme* X *over a Dedekind scheme* S. *Hint: First prove that a morphism:* $\mathrm{Res}_{F'/\mathbb{Q}}(\mathbb{G}_{m/F'}) \to \mathbb{G}_{m/\mathbb{Q}}$ *of group schemes is determined by its (complex or* p*–adic) absolute value, where* $G = \mathrm{Res}_{F'/\mathbb{Q}}(\mathbb{G}_{m/F'})$ *is a group scheme defined over* $\mathbb{Q}$ *given as a group functor:* $\underline{G}(A) = (A \otimes_{\mathbb{Q}} F')^\times$ *for* $\mathbb{Q}$*–algebras* A.

5.7. ℓ**–Adic Galois representations.** Let $\mathbb{F}$ be a finite field of characteristic p, and take an abelian variety $X_{/\mathbb{F}}$. Thus $\mathbb{F} = \mathbb{F}_q$ for $q = p^f$. We consider the relative Frobenius endomorphism $F : X \to X = X^{(q)}$ induced by $\phi : \mathcal{O}_X \to \mathcal{O}_X$ with $\phi(a) = a^q$. The morphism takes $\mathbf{0}_X$ to $\mathbf{0}_X$ because $\mathbf{0}_X$ is a section over $\mathbb{F}$. Therefore, by Corollary 5.17, F is an S–homomorphism. Since $\widehat{\mathcal{O}}_{X,\mathbf{0}} \cong \mathbb{F}[[T_1, \ldots, T_d]]$ for $d = \dim_{\mathbb{F}} X$ and ϕ induces an endomorphism $\widehat{\mathcal{O}}_{X,\mathbf{0}}$ taking T_j to T_j^q, the degree of F is given by q^d. We then have the characteristic polynomial $P_F(X) \in \mathbb{Z}[T]$. We pick a prime $\ell \neq p$ and consider $T_\ell(X)$. Since $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ acts on $X[\ell^n]$, the Galois group acts on $T_\ell(X)$. We write this representation as $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \to GL(T_\ell(X))$. Since the endomorphism ring also acts on $T_\ell(X)$, we write $\rho_\ell(\alpha)$ to indicate the operator on $T_\ell(X)$ associated to $\alpha \in \mathrm{End}_{\mathbb{F}}(X)$. The action of F on the $X[\ell^n]$ coincides with that of the Frobenius element ϕ in the Galois group. Thus the reciprocal characteristic polynomial of ϕ is given by $L(T) = T^{2d}P_F(T^{-1}) = \det(1 - \rho(\phi)T)$. Since we have $P_\alpha(0) = \det(\rho(\alpha)) = \deg(\alpha)$, we see $L(T) = \deg(1 - FT)$.

Remark 5.25. For an invertible sheaf $\mathcal{L}$ on $X_{/\mathbb{F}}$, the morphism $\varphi_{\mathcal{L}} : \underline{X} \to \mathrm{Pic}_{X/\mathbb{F}}$ given by $\varphi_{\mathcal{L}}(x) = (T_x^*\mathcal{L}) \otimes \mathcal{L}^{-1}$ (for the translation $T_x : X \to X$ by x) induces a morphism of functors, and hence a morphism of schemes: $X \to X^*$ which sends $\mathbf{0}_X$ to $\mathbf{0}_{X^*}$. Thus $\varphi_{\mathcal{L}}$ is a homomorphism (Corollary 5.17). If $\mathcal{L}$ is ample, it is known that $\varphi_{\mathcal{L}}$ is an isogeny (e.g. [ABV] Section 6 or [Mi] Sections 9–10). If further $\mathcal{L}$ is symmetric (that is, $\varphi_{\mathcal{L}} = \varphi_{\mathcal{L}}^t \iff (-1)^*\mathcal{L} \cong \mathcal{L}$), then $\xi^t = \varphi_{\mathcal{L}}^{-1}\xi\varphi_{\mathcal{L}}$ is an element in $B = \mathrm{End}_{\mathbb{F}}^{\mathbb{Q}}(X)$. Thus $\xi \mapsto \xi^t$ gives an involution of the semi-simple algebra B (this involution coincides with the transpose of endomorphisms in the case of jacobian, where we have taken $\mathcal{L} = \mathcal{L}(\Theta)$). An important point is that this is a positive involution, that is, the quadratic form $\xi \mapsto \mathrm{Tr}_{B/\mathbb{Q}}(\xi\xi^t)$ is positive definite (e.g. [ABV] Section 21). From this, as Weil did, one can prove that all roots of $P_F(T)$ has complex absolute value $q^{1/2}$. An algebraic integer whose Galois conjugates have equal complex absolute value $q^{1/2} = p^{f/2}$ is called a *Weil* p*-number of weight* f. Weil numbers have important arithmetic information as they appear as Frobenius eigenvalues of geometrically constructed Galois representations (see [Ho], [T2], [D1], [L] and [H11]).

If X is the jacobian scheme of a smooth curve $C_{/\mathbb{F}}$, the map F is induced by the Frobenius map $F_C : C \to C = C^{(q)}$, that is, $F = J^t(F_C)$. We put $V = J(F_C)$. Then $V^t = F$ and $F^t = V$ and $FV = VF = q$. Thus we have

$$\deg(1 - F_C^n) = \deg(1 - F^n) = |C(\mathbb{F}_{q^n})|.$$

Let $G = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F})$, and define the zeta function of C by

$$L_p(s, C) = \prod_{x \in C(\overline{\mathbb{F}})/G} (1 - N(x)^{-s})^{-1}, \tag{5.7}$$

where $N(x) = q^{[\mathbb{F}(x);\mathbb{F}]}$. Then, writing $L(t) = \deg(1 - Ft)$ again, we find a theorem of Weil (see [GME] §2.7.1):

$$L_p(s, C) = Z(q^{-s}) \text{ with } Z(t) = \frac{L(t)}{(1-t)(1-qt)}. \tag{5.8}$$

From this, $L_p(s, C)$ is a rational function of q^{-s} and hence is continued analytically to the whole s–plane with simple poles at 0 and 1. We also conclude the functional equation $L_p(s, C) = L_p(1-s, C)$ from Remark 5.25.

Now suppose that X is an abelian scheme defined over a Dedekind domain A whose quotient field is a number field K. We can perform the above construction at each point $v \in S = \mathrm{Spec}(A)$. If v is a closed point of characteristic p, writing $k(v) = \mathbb{F}_q$, we have $\rho_{v,\ell} : \mathrm{Gal}(\overline{k}(v)/k(v)) \to GL(T_\ell(X))$. Out of this, we get $L_v(T) = \det(1 - \rho_{v,\ell}(\phi)T) \in \mathbb{Z}[T]$ ($\ell \neq p$) which is the reciprocal polynomial of the characteristic polynomial of the Frobenius map F over $k(v)$.

Let $A_v = \mathcal{O}_{S,v}$ be the discrete valuation ring of A at v. For any finite extension L of K and a discrete valuation ring B in L over A_v, properness of X tells us $X(B) = X(L)$. Fixing a valuation ring $\overline{A}_v$ in an algebraic closure $\overline{K}$ over A_v, we have a reduction map:

$$X(\overline{K}) = X(\overline{A}_v) \to X(\overline{k}(v))$$

taking $x \in X(\overline{A}_v)$ to its special fiber. Since $X[\ell^n]$ is locally free over S, any point x_v at the special fiber $X[\ell^n]$ extends to a point $x \in X[p^n](B)$ for a finite extension $B = L \cap \overline{A}_v$. Thus the reduction map $\iota : X[\ell^n](\overline{K}) \to X[\ell^n](\overline{k}(v))$ is a surjective homomorphism. If $\ell \neq p$, counting the order of the two sides, we conclude that ι is an isomorphism. Taking the projective limit, we have an isomorphism $\iota : T_\ell(X_K) \cong T_\ell(X(v))$, where we have written $X_K = X \otimes_S K$. Let

$$\mathcal{D}_v = \{\sigma \in \mathrm{Gal}(\overline{K}/K) | \sigma(\overline{A}_v) \subset \overline{A}_v\}$$

be the decomposition group at v. Then we have the natural exact sequence:

$$1 \to \mathcal{I}_v \to \mathcal{D}_v \xrightarrow{\pi} \mathrm{Gal}(\overline{k}(v)/k(v)) \to 1.$$

By definition, $\pi(\sigma)((\iota(x)) = \iota(\sigma(x))$. This shows that the Galois representation $\rho_{K,\ell}$ on $T_\ell(X_K)$ is unramified at v, that is, $\rho_{K,\ell}(\mathcal{I}_v) = 1$, as long as $\ell \neq p$, and we have, for the Frobenius element ϕ_v of $\mathcal{D}_v$

$$\det(1 - \rho_{K,\ell}(\phi_v)T) = L_v(T) \in \mathbb{Z}[T], \tag{5.9}$$

which is independent of the choice of $\overline{A}_v$ (and of $\mathcal{D}_v$) as long as $p \neq \ell$.

A system of ℓ–adic Galois representations $\rho = \{\rho_\ell\}_\ell$ is called a *compatible system* of ℓ–adic Galois representations of weight $w \in \mathbb{Z}$ if the following conditions are satisfied:

(1) There is a finite set Σ of primes of K such that ρ_ℓ is unramified outside $\Sigma \cup \{\ell\}$;
(2) the characteristic polynomial of the Frobenius element at v is independent of ℓ as long as the prime $v \notin \Sigma$ and $v \nmid \ell$;
(3) All the roots of the characteristic polynomial of the Frobenius element have complex absolute value $|k(v)|^{w/2}$ for $v \notin \Sigma$ and $v \nmid \ell$ (i.e., Weil ℓ-number of weight wf if $|k(v)| = \ell^f$).

For a given abelian variety X_K defined over K, we embed X_K in the projective space $\mathbf{P}^N_{/K}$ (possible: see for example [ABV] Section 17 or [Mi] Section 7). Let O_K be the integer ring of K. Take a closure X of the image in $\mathbf{P}^N_{/O_K}$. Since smoothness is an open property (as it is defined via stalk), X is smooth over a dense open subscheme $S_1 = \mathrm{Spec}(A_1) \subset \mathrm{Spec}(O_K)$. The ring A_1 is given by removing primes in a finite subset Σ_1 of closed points of $\mathrm{Spec}(O_K)$. Since X is smooth over S_1, it is fiber by fiber irreducible. The multiplication $m : X_K \times X_K \to X_K$, the inverse $i : X_K \to X_K$ and the identity section $\mathbf{0} : \mathrm{Spec}(K) \to X_K$ extend to an open subscheme of $X \times_S X$, whose complement Z is of codimension at least 2, by the valuative criterion of properness. Since Z does not intersect X_K, its image in S_1 is a proper closed subset; so, consisting of another finite set of primes Σ_2. Remove again Σ_2 from S_1, we get $S = \mathrm{Spec}(A)$ for a localization A of O_K. Then $X_{/S}$ is an abelian scheme, and therefore, the system of ℓ–adic representations attached to X_K is a compatible system. There is a finer way to extend X to a smooth group scheme over $\mathrm{Spec}(O_K)$, which is called the

Néron model of X_K and gives the optimal result (see [NMD] for details of Néron models and [A] for a brief account).

More generally, let M be a number field. A system of continuous Galois representation $\rho = \{\rho_{\mathfrak{l}}\}$ of $\mathrm{Gal}(\overline{K}/K)$ indexed by primes of M on a vector space $V_{\mathfrak{l}}$ of (fixed) dimension d over the $\mathfrak{l}$–adic field $M_{\mathfrak{l}}$ is called a *strictly compatible system* of weight w if the following three conditions are satisfied:

(CP1) There is a finite set Σ of primes of K such that $\rho_{\mathfrak{l}}$ is unramified outside $\Sigma \cup \{\ell\}$, where $(\ell) = \mathfrak{l} \cap \mathbb{Z}$;

(CP2) the characteristic polynomial $L_{v,\rho}(T)$ of the Frobenius element at v on $H^0(\mathcal{I}_v, V_{\mathfrak{l}})$ is contained in $O_M[T]$ and is independent of $\mathfrak{l}$ as long as $v \nmid \ell$, where O_M is the integer ring of M.

(CP3) There exists an integer w called the weight of ρ such that all the reciprocal root α of $L_{v,\rho}(T)$ satisfies $|\alpha| = N(v)^{w/2}$ for almost all closed points $v \in S$, where $N(v) = |k(v)|$.

We define an imprimitive L–function of a compatible system ρ by

$$L(s,\rho) = \prod_{v \notin \Sigma} L_{v,\rho}(N(v)^{-s})^{-1},$$

where $N(v) = |k(v)|$. Here we regard $L_{v,\rho}(T) \in M[T]$ as an element of $M_{\mathbb{C}}[T]$ for $M_{\mathbb{C}} = M \otimes_{\mathbb{Q}} \mathbb{C}$ and have taken the product in $M_{\mathbb{C}}$. For a strictly compatible system, we can define the primitive L–function by

$$L(s,\rho) = \prod_{v} L_{v,\rho}(N(v)^{-s})^{-1}, \tag{5.10}$$

where v runs over all maximal ideals of O_K. When ρ is associated to the compatible system of ℓ–adic representation of the jacobian of a regular curve C, we write $L(s,C)$ for $L(s,\rho)$. Similarly if ρ is associated to an abelian scheme X, we write $L(s,X)$ for $L(s,\rho)$. When ρ is associated to an abelian scheme, by Remark 5.25, the weight of ρ is equal to 1. We can generalize the Hasse-Weil conjecture in this setting, although we do not make it very precise here, but just say that $L(s,\rho)$ should be continued to a meromorphic function on the whole complex plane, and when it is primitive of weight w, it should also satisfy a functional equation of the form: $s \leftrightarrow w+1-s$. By modularity theorems (finished by Khare–Wintenberger), the conjecture is now known for 2-dimensional systems of odd Galois representations.

We give an example of a compatible system with coefficients in a number field M. Start with an abelian scheme $X_{/S}$ over $S = \mathrm{Spec}(A)$ for a Dedekind domain $A \subset K$ as above. We suppose that X has a (big) commutative endomorphism subalgebra $O \subset \mathrm{End}_S(X)$ invariant under the involution $\xi \mapsto \xi^t$ such that $F + V \in O$ in $\mathrm{End}_v(X(v))$ for every special fiber $X(v)$, where F is the Frobenius map and V is its dual: $V = qF^{-1} = F^t$. Consider $L_{O,v}(T) = T^2 - (F+V)T + q \in O[T]$ for each special fiber v, where $q = |k(v)|$. Obviously, $L_{O,v}(F) = L_{O,v}(V) = 0$ in O. For simplicity, we assume that O is the integer ring of a number field M and that $[M:\mathbb{Q}] = \dim_S X$. We call such an abelian variety that "of $GL(2)$-type". The Tate module $T_\ell(X_K)$ is a torsion-free O–module such that $O_\ell = O \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ acts faithfully (cf. (5.4)). Thus $T_\ell(X_K)$ is a projective O_ℓ–module. Since K is a number field, O acts faithfully on $X(\mathbb{C})$ for an embedding $K \hookrightarrow \mathbb{C}$. Thus O acts faithfully on the lattice $\mathcal{L} = \pi_1(X(\mathbb{C})) = H^1(X(\mathbb{C}), 2\pi\mathbb{Z})$ in $H^1_{an}(X(\mathbb{C}), \mathcal{O}_X)$. The lattice $\mathcal{L}$ is a projective O–module. This shows that $2d = \mathrm{rank}_O \mathcal{L} = \dim_M(\mathcal{L} \otimes_O M)$ is divisible by $[M:\mathbb{Q}]$, that is, $2d = n[M:\mathbb{Q}]$. By our assumption: $[M:\mathbb{Q}] = \dim_S X$, n is equal to 2. Since $T_\ell(X(\mathbb{C})) \cong \varprojlim_m \mathcal{L}/\ell^m\mathcal{L} \cong O_\ell^n$, the isomorphism $\iota : T_\ell(X(\mathbb{C})) = T_\ell(X_K) \cong T_\ell(X(v))$ tells us that $T_\ell(X(v))$ is O_ℓ–free of rank 2. Thus we get a two-dimensional compatible system from X having values in $GL_2(M_{\mathfrak{l}})$ whose characteristic polynomial of the Frobenius element at v is given by $L_{O,v}(T)$. As remarked by Shimura in [IAT] Theorem 7.14, the jacobian variety $J_1(N)_{/\mathbb{Q}}$ of the modular curve $X_1(N)_{/\mathbb{Q}}$ is isogenous to a product of rational abelian varieties of $GL(2)$–type. By modularity theorems (in particular, the solution of Serre's mod p modularity conjecture by Khare–Wintenberger; see, Chapter 5 of [GME]), such an abelian variety is essentially a factor of $J_1(N)$ for a suitable N. Using étale cohomology groups $H^w(V, \mathbb{Z}_p)$ for a projective scheme $V_{/S}$, we can construct more compatible systems of weight w, although we will not touch this topic in this course (see [ECH]).

6. Modular Galois Representations

In this section, we construct Galois representations of cusp forms of weight 2 via the jacobian variety of modular curves. This is the method employed by Shimura in his book [IAT] and his earlier papers. Then we study its ramification. Although we have incorporated results obtained after Shimura's book was written, for example, those on ramifications of the Galois representation, our way of construction faithfully follows [IAT].

6.1. **Hecke correspondences.** We fix an integer $N > 0$ and consider the coarse moduli scheme $X = X_1(N)_{/\mathbb{Z}} = \overline{M}_{\Gamma_1(N)/\mathbb{Z}}$. The infinity cusp gives a smooth section in $X(\mathbb{Z})$ (by [GME] §2.9.4); so, we can apply the theory developed in the previous section. The non-singular model of $X_1(N)$ over $\mathbb{Q}$ is of genus 0 for all $N \le 10$. Thus we may assume $N \ge 4$ when we consider jacobians of $X_1(N)$. When $N \ge 4$, X is regular. Let $S = \mathrm{Spec}(\mathbb{Z}[\frac{1}{N}])$. Then X is a smooth irreducible curve over S. We write J for the jacobian variety of X over S. We look into the ℓ–adic Galois representations on $T_\ell(J)$.

Let p be a prime outside N. Since $Y = \overline{M}_{\Gamma_0(p),\Gamma_1(N)}$ classifies triples $(E, \phi_N, C)_{/T}$ for locally free subgroup C of rank p, we can think of an involution of moduli functors $\tau : (E, \phi_N, C)_{/T} \mapsto (E/C, \phi'_N, C^\perp)_{/T}$, where $C^\perp$ is the kernel of the dual map $E/C = (E/C)^* \to E^* = E$ of the projection $\pi : E \to E/C$, and $\phi'_N : \mu_N \hookrightarrow E/C$ is the one satisfying $\phi'_N = \pi \circ \phi_N$.

When C is an étale subgroup, the quotient E/C is well defined as a geometric quotient by the following reason: After an étale faithfully flat base change, C becomes a constant group, the quotient exists (cf. [GME] §1.8.3). Being geometric quotient is kept under étale base change, we know, from the uniqueness of the quotient, that the quotient carries a descent datum. By descent, E/C exists over S (actually the geometric quotient exists over S even if C is connected: see below and [ABV] Theorem 12.1). Therefore over $S[\frac{1}{p}]$ this involution is well defined, giving rise to an involution $\tau \in \mathrm{End}(Y_{S[\frac{1}{p}]})$ by the key lemma. We have two projections: $p_1, p_2 : Y_{/S[\frac{1}{p}]} \to X_{S[\frac{1}{p}]}$ such that $p_1(E, \phi_N, C) = (E, \phi_N)$ and $p_2(E, \phi_N, C) = (E/C, \phi'_N)$. In other words, $p_2 = p_1 \circ \tau$. We get a correspondence $(Y, p_1 : Y \to X, p_2 : Y \to X)$ in this way, which induces an endomorphism $T^t = T^t(p) = J^t(p_2) \circ J(p_1)$ and $T = T(p) = J^t(p_1) \circ J(p_2)$ (see the end of §5.6 for the definition of correspondences and their action on J). As seen in the proof of Theorem 5.21, we know $\mathrm{End}_{S[\frac{1}{p}]}(J) = \mathrm{End}_S(J)$ and hence f extends to the entire $J_{/S}$. Thus T and T^t extends to $J_{/S}$.

We now study the construction of T at the fiber at p. We write $X(p) = X \otimes_S \mathbb{F}_p$ and $Y(p) = Y \otimes_S \mathbb{F}_p$. By Eichler-Shimura congruence relation (see [GME] Theorem 2.9.13), $Y(p) = X(p) \cup X(p)^{(p)}$ with two components intersecting transversally at super singular points. By the description there, we still have quotient E/C for ordinary elliptic curves (E, ϕ_N, C). When C is étale, the quotient can be made as above. When $C \cong \mu_p$ étale locally, we can define E/C by the Frobenius map $F : E \to E^{(p)}$. Then $V : E \to E^{(\frac{1}{p})}$ is isomorphic to E/C for C étale. Thus we have well defined $\tau : Y(p)^\circ \to Y(p)^\circ$ for the smooth locus $Y(p)^\circ$ of $Y(p)$. This construction using F and V are well defined even for super-singular curves also. Thus the involution $\tau : Y(p) \to Y(p)$ is well defined everywhere. Anyway, as remarked already, the quotient E/C can be made over S; so, τ actually gives rise to the correspondence (Y, p_1, p_2) well defined over S. This gives another proof of extensibility of T and T^t to an endomorphism of $J_{/S}$.

We scrutinize more the maps p_j $(j = 1, 2)$. Suppose that $C \subset E$ is connected. Since $\phi_N : \mu_N \hookrightarrow E$, we have

$$\phi_N^{(p)} \circ F(x) = F \circ \phi_N(x) = p \cdot \phi_N(x) = \phi_N(px),$$

where $\phi_N^{(p)}$ is the conjugate of ϕ_N by the Frobenius automorphism on the base ring. Thus $\phi'_N = \tau(\phi_N) = p^{-1}\phi_N^{(p)}$ by our definition. On the modular curve $X(p)$, the association: $(E, \phi_N) \mapsto (E^{(p)}, \phi_N^{(p)})$ induces the Frobenius map on $X(p)$.

Suppose C is étale. Then $FV = p$; so, V acts trivially on ϕ_N. The first component $X(p)$ of $Y(p)$ as a correspondence over $X(p)$ gives rise to the map:

$$(E, \phi_N) \mapsto (E^{(p)}, p^{-1}\phi_N^{(p)})$$

and the second component gives rise to the map:

$$(E, \phi_N) \mapsto (E^{(1/p)}, \phi_N^{(1/p)}).$$

We find $T^t = F\langle p\rangle^{-1} + V$ on J, where $\langle p\rangle = \langle p\rangle_2$ is the automorphism of X sending (E, ϕ_N) to $(E, p\phi_N)$. By taking the dual, $T = F + V\langle p\rangle$ in $\mathrm{End}_{\mathbb{F}_p}(J(p))$. This relation is also called the *congruence relation* of Eichler-Shimura, which is equivalent to the splitting $Y = X(p) \cup X(p)^{(p)}$. Thus we have

Theorem 6.1 (G. Shimura)**.** *Let $S = \mathrm{Spec}(\mathbb{Z}[\frac{1}{N}])$ for $N \geq 4$. Let $X = X_1(N)$, and write $J = J_1(N)$ for the jacobian scheme of X over S. Let $J(p) = J \otimes_S \mathbb{F}_p$ for each prime p outside N. Then for each prime p outside N, we have an endomorphism $T(p), T^t(p) \in \mathrm{End}_S(J)$ such that $T(p) = F_p + V_p\langle p\rangle$ and $T^t(p) = F_p\langle p\rangle^{-1} + V_p$ in $\mathrm{End}_{\mathbb{F}_p}(J(p))$ for the Frobenius endomorphism F_p of $J(p)$ and its dual $V_p = F_p^t$. Since $F_pV_p = p$, F satisfies the quadratic equation:*

$$x^2 - T(p)x + p\langle p\rangle = 0$$

with coefficients in $\mathrm{End}_S(J)$.

Since $H^0(J, \Omega_{J/S}) \cong H^0(X, \Omega_{X/S})$ by Theorem 5.7, the operator $T(p)$ acts on $H^0(X, \Omega_{X/S})$ by $\omega|T(p) = T(p)^*\omega$. We can compute by using the Tate curve at ∞, the effect of the action on the q–expansion. The Frobenius element just acts by $q \mapsto q^p$ on the Tate curve, and V corresponds to (the sum in the jacobian of) p quotients of $E_{\infty/\mathbb{Z}[[q]]}$ by order p étale subgroups, which are $E_{0,p/\mathbb{Z}[[\zeta_p q^{1/p}]]}$ for each $\zeta_p \in \mu_p$. We then have for $\omega = f(q)\frac{dq}{q}$

$$a(n; f|T(p)) = a(np, f) + \sum_{\zeta \in \mu_p} \zeta^n a(\frac{n}{p}; f|\langle p\rangle) = a(np, f) + p \cdot a(\frac{n}{p}; f|\langle p\rangle),$$

where $a(\frac{n}{p}; f|\langle p\rangle) = 0$ if $p \nmid n$.

Now assume that $p|N$; so, we split $N = N_0p^r$ for N_0 prime to p. Let $\Gamma = \Gamma_0(p^{r+1}) \cap \Gamma_1(p^r)$. We still have $Y = \overline{M}_{\Gamma,\Gamma_1(N_0)}$ and the projection $p_1 : Y \to X$ well defined over $\mathbb{Z}$. The modular curve Y classifies over $S = \mathrm{Spec}(\mathbb{Z}[\frac{1}{N}])$ triples (E, ϕ_N, C) for a cyclic subgroup C of order p^{r+1} containing the image of $\phi_p = \phi_N|_{\mu_{p^r}}$. We can think of the quotient $E/(C[p])$. Since C is cyclic, the multiplication by p induces an isomorphism: $i : C/(C[p]) \cong pC = \mathrm{Im}(\phi_p)$. We then define the level Np^r–structure ϕ'_N on $E/(C[p])$ by

$$(\phi_p \circ i^{-1}) \times (\phi_N|_{\mu_{N_0}}).$$

Thus we find another projection: $p_2 : Y \to X$ induced by $(E, \phi_N, C) \mapsto (E/(C[p]), \phi'_N)$, getting a correspondence (Y, p_1, p_2), which induces $U(p) = J^t(p_1) \circ J(p_2)$ and $U^t(p) = J^t(p_2) \circ J(p_1)$. We verify

$$a(n; f|U(p)) = a(np; f).$$

Let $\mathbf{h}_k(\Gamma_1(N); A)$ denote the A–subalgebra of $\mathrm{End}_A(S_k(\Gamma_1(N); A))$ generated by Hecke operators $T(p)$, $U(p)$ and $\langle p\rangle$. The representation of $\mathrm{End}_{\mathbb{C}}(J(\mathbb{C}))$ on the cotangent space $H^0(J(\mathbb{C}), \Omega_{J/\mathbb{C}}) \cong S_2(\Gamma_1(N); \mathbb{C})$ (see Theorem 5.7) is faithful (because of (5.2)). Therefore we find an embedding $\theta : \mathbf{h}_2(\Gamma_1(N); \mathbb{Z}) \hookrightarrow \mathrm{End}_S(J_1(N))$ so that $\theta(h)^*\omega = \omega|h$ for $h \in \mathbf{h}_2(\Gamma_1(N); \mathbb{Z})$.

We have the Hodge exact sequence:

$$0 \to H^0_{an}(X(\mathbb{C}), \Omega_{X/\mathbb{C}}) \to H^1_{an}(X(\mathbb{C}), \mathbb{C}) \to H^1_{an}(X(\mathbb{C}), \mathcal{O}_X) \to 0.$$

by the well known pairing $(f, h) = a(1, f|h)$ for cusp forms f and Hecke operators h, we find

$$H^0_{an}(X(\mathbb{C}), \Omega_{X/\mathbb{C}}) \cong \mathrm{Hom}_{\mathbb{C}}(\mathbf{h}_2(\Gamma_1(N); \mathbb{C}), \mathbb{C})$$

as Hecke modules. Here the word "as Hecke modules" means the isomorphism is an isomorphism of modules over the Hecke algebra. By the duality of Serre–Grothendieck,

$$H^0_{an}(X(\mathbb{C}), \Omega_{X/\mathbb{C}}) \cong \mathrm{Hom}_{\mathbb{C}}(H^1_{an}(X(\mathbb{C}), \mathcal{O}_X), \mathbb{C})$$

as Hecke modules. Thus $H^1_{an}(X(\mathbb{C}), \mathcal{O}_X)$ is $\mathbf{h}_2(\Gamma_1(N); \mathbb{C})$–free of rank 1. We compute $H^1_{an}(X(\mathbb{C}), \mathbb{C})$ using harmonic analysis, and get

$$H^1(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{C} \cong H^1_{an}(X(\mathbb{C}), \mathbb{C}) \cong H^0_{an}(X(\mathbb{C}), \Omega_{X/\mathbb{C}}) \oplus H^0_{an}(X(\mathbb{C}), \overline{\Omega}_{X/\mathbb{C}})$$

as Hecke modules (the Hodge decomposition), where $\overline{\Omega}_{X/\mathbb{C}}$ is the sheaf of anti-holomorphic differentials. By the same argument, we find

$$H^0_{an}(X(\mathbb{C}),\overline{\Omega}_{X/\mathbb{C}}) \cong \mathrm{Hom}_{\mathbb{C}}(\mathbf{h}_2(\Gamma_1(N);\mathbb{C}),\mathbb{C})$$

as Hecke modules. This shows, for $A=\mathbb{C}$,

$$\mathbf{h}_2(\Gamma_1(N);A) \cong \mathrm{Hom}_A(\mathbf{h}_2(\Gamma_1(N);A),A) \tag{6.1}$$

$$H^1_{an}(X(\mathbb{C}),2\pi iA) \text{ is } \mathbf{h}_2(\Gamma_1(N);A)\text{–free of rank } 2. \tag{6.2}$$

Since $H^1_{an}(X(\mathbb{C}),2\pi i\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{C} \cong H^1_{an}(X(\mathbb{C}),\mathbb{C})$ canonically, the above fact descends to any $\mathbb{Q}$–algebra A. Since $T_\ell(J_{/\mathbb{Q}})\otimes\mathbb{Q} \cong H^1_{an}(X(\mathbb{C}),2\pi i\mathbb{Z})\otimes\mathbb{Q}_\ell$, we have

$$V_\ell = T_\ell(J_{/\mathbb{Q}})\otimes\mathbb{Q} \text{ is free of rank } 2 \text{ over } \mathbf{h}_2(\Gamma_1(N);\mathbb{Q}_\ell). \tag{6.3}$$

6.2. **Galois representations on modular Jacobians.** By the Galois action on V_ℓ, from (6.3), we get a two-dimensional Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbf{h}_2(\Gamma_1(N);\mathbb{Q}_\ell))$$

unramified outside $N\ell$. We would like to show

Theorem 6.2 (G. Shimura)**.** *The Galois representation ρ_ℓ is unramified outside $N\ell$, and the characteristic polynomial of $Frob_p$ for $p\nmid N\ell$ of ρ_ℓ is given by*

$$\det(T-\rho_\ell(Frob_p)) = T^2 - T(p)T + p\langle p\rangle.$$

This theorem and the following corollary are given in [IAT] Sections 7.5-6 in various different forms. The unramifiedness outside $N\ell$ is due to J. Igusa.

Proof. Unramifiedness follows from the fact that J is an abelian scheme over $\mathbb{Z}[\frac{1}{N}]$, as already explained in §5.7.

We follow [IAT] Section 7.5 to prove the rest. We fix a primitive root of unity $\zeta_N\in\mu_N$, and consider couples $(E,\phi_N:\mu_N\hookrightarrow E)$ classified by $X_1(N)$. We write $P=\phi_N(\zeta)$. Then we can find a unique $Q\in E$ modulo $\mathrm{Im}(\phi_N)$ such that $\langle P,Q\rangle=\zeta_N$. We define $\phi'_N:\mu_N\hookrightarrow E/\mathrm{Im}(\phi_N)$ by $\phi'_N(\zeta_N)=Q$. This gives an automorphism $\tau=\tau_{\zeta_N}$ of $X_1(N)$ (taking (E,ϕ_N) to $(E/\mathrm{Im}(\phi_N),\phi'_N)$) defined over $S[\zeta_N]$. Since F acts on $\mathrm{Im}(\phi_N)$ by multiplication by p,

$$\langle P,V(Q)\rangle = \langle F(P),Q\rangle = \langle pP,Q\rangle = \langle P,pQ\rangle.$$

This shows that $V(Q)=pQ$. Therefore, $\tau^{-1}T^t(p)\tau=T(p)$ and $\tau^{-1}V\tau=V\langle p\rangle$. We can also check $\tau^{-1}U^t(p)\tau=U(p)$ (see [MFM] Theorem 4.5.5). We recall the pairing

$$\langle\ ,\ \rangle : J[\ell^n]\times J[\ell^n]\to\mu_{\ell^n}$$

in Theorem 5.19 (2) (because $J^*\cong J$ canonically). Taking the projective limit with respect to n, we get a pairing $\langle\ ,\ \rangle : V_\ell\times V_\ell\to\mathbb{Q}_\ell(1)$ such that $\langle f(x),y\rangle=\langle x,f^t(y)\rangle$ for endomorphisms f of J, where $\mathbb{Q}_\ell(1)=\varprojlim_n \mu_{\ell^n}\otimes_{\mathbb{Z}}\mathbb{Q}$. We twist this pairing as $(x,y)=(x,\tau(y))$. Then $(h(x),y)=(x,h(y))$ for Hecke operators h. Write simply $\mathbf{h}=\mathbf{h}_2(\Gamma_1(N);\mathbb{Q}_\ell)$. Since $\mathrm{Hom}_{\mathbb{Q}_\ell}(\mathbf{h},\mathbb{Q}_\ell)\cong\mathbf{h}$ as we have already shown, we can lift this pairing to an $\mathbf{h}$–linear non-degenerate pairing $[\ ,\ ]:V_\ell\times V_\ell\to\mathbf{h}$ such that $L([x,y])=(x,y)$ for a generator $L\in\mathrm{Hom}_{\mathbb{Q}_\ell}(\mathbf{h},\mathbb{Q}_\ell)$ over $\mathbf{h}$. The adjoint of F under this new pairing is $V\langle p\rangle$; so, F and $V^*=V\langle p\rangle$ have equal characteristic polynomial over $\mathbf{h}$. Therefore $\det_{\mathbf{h}}(T-F)=\det_{\mathbf{h}}(T-V^*)$ in $\mathbf{h}[T]$. We have

$$(T-F)(T-V^*) = T^2 - T(p)T + p\langle p\rangle.$$

Taking the determinant on both sides, we get

$$\det_{\mathbf{h}}(T-F)^2 = (T^2 - T(p)T + p\langle p\rangle)^2.$$

Since this is the identity of the square of two monic polynomials in $\mathbf{h}[T]$, we get

$$\det(T-\rho_\ell(Frob_p)) = \det_{\mathbf{h}}(T-F) = T^2 - T(p)T + p\langle p\rangle.$$

□

Corollary 6.3. *Let $\lambda : \mathbf{h}_2(\Gamma_1(N);\mathbb{Z}) \to \overline{\mathbb{Q}}$ be an algebra homomorphism, and define a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ by $\chi(p) = \lambda(\langle p\rangle)$. Then for the finite extension $\mathbb{Q}[\lambda]$ generated over $\mathbb{Q}$ by $\lambda(T(n))$, there exists a unique compatible system with coefficients in $\mathbb{Q}[\lambda]$ of absolutely irreducible Galois representations $\rho_{\lambda,\mathfrak{l}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $GL_2(\mathbb{Q}_p[i_\mathfrak{l}\circ\lambda])$ (indexed by the embedding $i_\mathfrak{l} : \mathbb{Q}[\lambda] \hookrightarrow \overline{\mathbb{Q}}_\ell$ associated to the place $\mathfrak{l}$) such that*

1. *$\rho_{\lambda,\mathfrak{l}}$ is unramified outside $N\ell$ for the rational prime $\ell \in \mathfrak{l}$;*
2. *For a prime p outside $N\ell$,*
$$\det(1 - \rho_{\lambda,\mathfrak{l}}(Frob_p)T) = 1 - \lambda(T(p))T + p\chi(p)T^2;$$
3. *We have $\det(\rho_{\lambda,\mathfrak{l}}(c)) = -1$ for each complex conjugation c;*
4. *For the ℓ–adic cyclotomic character ν_ℓ, we have $\det\rho_{\lambda,\mathfrak{l}} = \chi\nu_\ell$, where we regard χ as a Galois character by $\chi(Frob_p) = \chi(p)$ for primes outside $N\ell$.*

Proof. The representation space of $\rho_{\lambda,\mathfrak{l}}$ is given by
$$V_\mathfrak{l} = T_\ell(J_1(N)) \otimes_{\mathbf{h},i_\mathfrak{l}\circ\lambda} \mathbb{Q}_\ell[i_\mathfrak{l}\circ\lambda],$$
where $\mathbb{Q}_\ell[i_\mathfrak{l}\circ\lambda]$ is the finite extension of $\mathbb{Q}_\ell$ generated by $i_\mathfrak{l}\circ\lambda(T(n))$ for all n. The assertions (1) and (2) follow from the above theorem. The cyclotomic character ν_ℓ is the unique ℓ–adic character (by class field theory) with $\nu_\ell(Frob_p) = p$ for primes p outside $N\ell$. This shows (4). Since each elliptic curve E has automorphism -1_E, the action of $\langle -1\rangle$ on each test object (E,ϕ_N) is trivial; so, as an automorphism of $X_1(N)$, $\langle -1\rangle$ is the identity. Through the identification: $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ given by $\sigma \mapsto n$ if $\zeta_N^\sigma = \zeta_N^n$, complex conjugation corresponds to -1. Thus $\chi(c) = \chi(-1) = \lambda(\langle -1\rangle) = 1$. This combined with (4) shows (3).

We shall give a sketch of two proofs of irreducibility. Suppose that $\rho_{\lambda,\mathfrak{l}}$ is reducible. For the moment, we assume that $\ell \nmid N$. Then we find two characters φ and ϕ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified outside $N\ell$ such that $\mathrm{Tr}\rho_{\lambda,\mathfrak{l}} = \varphi + \phi$ and $\varphi\phi = \nu_\ell\chi$ for the ℓ–adic cyclotomic character ν_ℓ. Write C for the ℓ–adic completion of $\overline{\mathbb{Q}}_\ell$, on which $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q})$ acts by continuity. Let K be a finite extension of $\mathbb{Q}_\ell$ in C and $\xi : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to K^\times$ be a continuous character. Let $\mathcal{G} = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K)$ act on C by $x \mapsto \xi(\sigma)\sigma(x)$, and write this Galois module as $C(\xi)$. By a theorem of Tate (see [T] Theorem 3.3.2), if $\xi|_{\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K_0)}$ gives an isomorphism of $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_\ell$ for a finite extension K_0/K and totally ramified extension K_∞/K_0, we have
$$H^0(\mathcal{G}, C(\xi)) = 0.$$
Again by another theorem of Tate (see (5.3) and [T] Corollary 3.3.2), if ℓ is outside N, then as $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$–modules
$$\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(J), C) \cong H^1(J_{/C}, \mathcal{O}_{J/C}) \oplus \left(H^0(J_{/C}, \Omega_{J/C}) \otimes \mathrm{Hom}(\mathbb{Q}_\ell(1), C)\right),$$
where $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q})$ acts on every term naturally, for example, $\sigma(\omega\otimes\phi) = \sigma(\omega)\otimes\sigma\circ\phi\circ\sigma^{-1}$ for $(\omega\otimes\phi) \in \left(H^0(J_{/C}, \Omega_{J/C}) \otimes \mathrm{Hom}(\mathbb{Q}_\ell(1), C)\right)$. Let $K = \mathbb{Q}_\ell[i_\mathfrak{l}\circ\lambda]$, taking the $\mathcal{G}$–invariants, we get
$$H^0(\mathcal{G}, \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(J), C)) \cong H^1(J_{/K}, \mathcal{O}_{J/K}).$$
Thus one of the two characters, say ϕ, has to be of finite order on the decomposition group at ℓ. We consider the restriction of ϕ to the inertia group of a prime $q|N$. By local class field theory, we may regard ϕ as a character of $\mathbb{Z}_q^\times$, which is almost q–profinite (that is, it has a q–profinite subgroup of finite index). Since ϕ has values in ℓ–profinite group, it has to be of finite order ([MFG] Lemma 2.19). Thus ϕ is unramified outside $N\ell$ and of finite order on the inertia group at primes dividing $N\ell$. Then by global class field theory, ϕ itself is of finite order. Thus $\varphi = \phi^{-1}\chi\nu_\ell$. Since ϕ and χ are of finite order, we may consider them as complex characters. Then $\lambda(T(p)) = \phi(p) + \chi\phi^{-1}(p)p$ for all primes outside $N\ell$. This is a contradiction, in two ways: one is that the L–function given by
$$L(s, \lambda\otimes\chi^{-1}\phi) = \sum_n \chi^{-1}\phi(n) i_\infty(\lambda(T(n)))n^{-s}$$
(for any complex embedding $i_\infty : \mathbb{Q}[\lambda] \hookrightarrow \mathbb{C}$) is known to be an entire function on the whole s–plane, but is equal to $\zeta(s-1)L(s,\chi^{-1}\phi^2)$, up to finite Euler factor, which has a pole at $s = 2$. The other contradiction is against the fact that the two roots of $X^2 - i_\infty(\lambda(T(p)))X + \chi(p)p$ has complex absolute value $p^{1/2}$.

If $\ell|N$, we need to use a result of Ribet affirming that if $\rho_{\lambda,\mathfrak{l}}$ is reducible for one $\mathfrak{l}$, every member of the compatible system is actually reducible ([R2] Corollary 1.6.1).

There is another way to show the irreducibility. For this, we need to assume that $\mathbb{Q}[\lambda]$ is generated by $\lambda(T(p))$ for p prime to N. This is satisfied when λ is primitive in the sense of [MFG] 3.2.1. If an endomorphism ϕ of $T_\ell(J)$ commutes with all Galois action, then it commutes with the action of $F = Frob_p$, and hence commutes with $T(p) \in \mathbb{Q}[F] \subset \mathrm{End}^{\mathbb{Q}}_{\mathbb{F}_p}(J)$. By a theorem of Faltings ([**?**] II.5), $\mathrm{End}_{\mathfrak{G}}(T_\ell(J)) = \mathrm{End}_{\mathbb{Q}}(J) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, where $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus on V_ℓ, we may assume that ϕ is induced by a $\mathbb{Q}$–rational endomorphism of the abelian variety $A = J \otimes_{\mathbf{h},\lambda} O$ for the integer ring O of $\mathbb{Q}[\lambda]$. Since $\mathbb{Q}[\lambda] \subset \mathrm{End}^{\mathbb{Q}}_{\mathbb{Q}}(A)$ is generated by $T(p)$ outside N, ϕ commutes with all elements in $\mathbb{Q}[\lambda]$. The algebra $\mathrm{End}^{\mathbb{Q}}_{\mathbb{Q}}(A)$ acts faithfully on $H^0(A, \Omega_{A/\mathbb{Q}})$ which is isomorphic to a $\mathbb{Q}[\lambda]$–vector space of dimension 1. Thus $\phi \in \mathbb{Q}[\lambda]$, and by Schur's lemma (cf. [MFG] Proposition 2.5), $\rho_{\lambda,\mathfrak{l}}$ is absolutely irreducible. □

Remark 6.4. Let the notation be as in the above corollary. Let O_λ be the integer ring of $\mathbb{Q}[\lambda]$. Since $\rho_{\lambda,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_\ell[i_{\mathfrak{l}} \circ \lambda])$ is continuous, it has values in the maximal compact subgroup $GL_2(\mathbb{Q}_\ell[i_{\mathfrak{l}} \circ \lambda])$. Such a compact subgroup can be brought into $GL_2(O_{\lambda,\mathfrak{l}})$ by conjugation, and we may assume that $\rho_{\lambda,\mathfrak{l}}$ has values in $GL_2(O_{\lambda,\mathfrak{l}})$. Thus we may consider $\overline{\rho}_{\lambda,\mathfrak{l}} = (\rho_{\lambda,\mathfrak{l}} \mod \mathfrak{l})$. It has been shown, mainly by Ribet, that $\overline{\rho}_{\lambda,\mathfrak{l}}$ is absolutely irreducible for almost all primes $\mathfrak{l}$ (and hence, by a result of Carayol and Serre, the isomorphism class of $\rho_{\lambda,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(O_{\lambda,\mathfrak{l}})$ for such $\mathfrak{l}$ is uniquely determined by λ; cf. [MFG] Proposition 2.13).

6.3. **Ramification at the level.** We keep the notation introduced in the previous section. We would like to prove the following theorem.

Theorem 6.5. *Let $\lambda : \mathbf{h}_2(\Gamma_1(N), \mathbb{Z}) \to \overline{\mathbb{Q}}^\times$ be an algebra homomorphism. Write $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ for the Dirichlet character given by $\chi(q) = \lambda(\langle q \rangle)$ for primes q. Let p be a prime factor of N, and write $N = N_0 p^e$ with $p \nmid N_0$. Suppose that $\mathfrak{l} \nmid p$ for a prime ideal $\mathfrak{l}$ of $\mathbb{Q}(\lambda)$. Then we have*

1. *Suppose that the conductor $\chi_p = \chi|_{(\mathbb{Z}/p^e\mathbb{Z})^\times}$ is equal to p^e, that is, χ_p restricted to $1+p^{e-1}\mathbb{Z}_p$ if $e > 1$ and to $\mathbb{Z}_p^\times$ if $e = 1$ is non-trivial. Then $\rho_{\lambda,\mathfrak{l}}$ restricted to the inertia group I_p at p is isomorphic to $\sigma \mapsto \left(\begin{smallmatrix} \chi_p(\sigma) & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where we have regarded χ_p as a character of the inertia group by local class field theory. Moreover on the one dimensional subspace of the representation space of $\rho_{\lambda,\mathfrak{l}}$ fixed by the inertia group I_p, the Frobenius element at p acts through the multiplication by $\lambda(U(p))$.*
2. *Suppose $\chi_p = 1$, $e = 1$ and that λ is primitive at p (that is, $\lambda(T(q))$ differs from the eigenvalues of the Hecke operator $T(q)$ occurring on $S_2(\Gamma_1(N_0); \mathbb{C})$ for infinitely many primes q). Then $\rho_{\lambda,\mathfrak{l}}$ restricted to the decomposition group at p is isomorphic to $\sigma \mapsto \left(\begin{smallmatrix} \nu_\ell(\sigma)\eta(\sigma) & * \\ 0 & \eta(\sigma) \end{smallmatrix}\right)$, where η is an unramified character with $\eta(Frob_p) = \pm\sqrt{\chi(p)} = \lambda(U(p))$, regarding χ as a character modulo N/p.*

This theorem for $e = 1$ was proven by Deligne and Rapoport (after some work by Shimura and Casselman). A proof under the assumption $e = 1$ is in [GME] §4.2.3 and see [AME] 14.5.1 for the general case of $e > 1$.

Exercise 6.6. *For a compatible system of $\mathfrak{l}$–adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, suppose that $\mathfrak{l} \nmid p$. Then, is the kernel $\mathrm{Ker}(\rho_{\mathfrak{l}}|_{I_p})$ independent of $\mathfrak{l}$?*

6.4. **Ramification of p–adic representations at p.** We now state the ordinarity (first proven by Deligne and later by Wiles) for $\rho_{\lambda,\mathfrak{p}}$ at p if $\lambda(T(p))$ or $\lambda(U(p))$ is a p–adic unit in $\mathbb{Q}_p[i_{\mathfrak{p}} \circ \lambda]$. Here $\mathfrak{p}|p$. The proof is in [GME] §4.2.4.

Theorem 6.7. *Let the notation be as in* Theorem 6.5*, p be a prime factor of $N = N_0 p^e$ ($p \nmid N_0$) and $\mathfrak{p}$ be a prime ideal over p of $\mathbb{Q}[\lambda]$.*

1. *If $\lambda(T(p))$, $\lambda(U(p))$ or $\lambda(U^t(p))$ is a $\mathfrak{p}$–adic unit, then the representation space $V(\rho_{\lambda,\mathfrak{p}})$, has one dimensional unramified quotient (that is, fixed by the inertia group at p) on which the Frobenius element $Frob_p$ acts through the multiplication by the unique $\mathfrak{p}$–adic unit root of*

$X^2-\lambda(T)X+p\chi(p^{(p)})=0$, *where* T *is given by either* $T(p)$ *or* $U(p)+U^t(p)\langle p^{(p)}\rangle$ *according as* $e=0$ *or* $e>0$.

(2) *If* χ_p *is trivial,* $e=1$ *and* λ *is primitive, then* $\rho_{\lambda,\mathfrak{p}}$ *restricted to the decomposition group of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *at* p *is isomorphic to* $\left(\begin{smallmatrix}\nu_p\eta & *\\ 0 & \eta\end{smallmatrix}\right)$ *for an unramified character* η *with* $\eta(Frob_p)=\pm\sqrt{\chi(p)}=\lambda(U(p))$.

References

Books

[AAG] S. S. Gelbart, *Automorphic Forms on Adele Groups*, Annals of Math. Studies **83**, Princeton University Press, Princeton, NJ, 1975.

[ABV] D. Mumford, *Abelian Varieties*, TIFR Studies in Mathematics, Oxford University Press, New York, 1994.

[ACM] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1998.

[ADT] J. S. Milne, *Arithmetic Duality Theorem*, Perspectives in Math. **1**, Academic Press, 1986

[ALF] K. Iwasawa, *Algebraic Functions*, Translation from the 1973 Japanese edition by Goro Kato. Translations of Mathematical Monographs, **118**, American Mathematical Society, Providence, RI, 1993.

[ALG] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[ALR] J.-P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, Benjamin, New York, 1968

[AME] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Math. Studies **108**, Princeton University Press, Princeton, NJ, 1985.

[ARG] G. Cornell and J. H. Silverman, editors, *Arithmetic Geometry*, Sp-ringer, New York, 1986.

[BAL] N. Bourbaki, *Algébre*, Hermann, Paris, 1958.

[BCM] N. Bourbaki, *Algébre Commutative*, Hermann, Paris, 1961–1998.

[BNT] A. Weil, *Basic Number Theory*, Springer, New York, 1974.

[CAL] L. Hörmander, *An Introduction to Complex Analysis in Several Variables*, North-Holland/American Elsevier, 1973

[CFN] J. Neukirch, *Class Field Theory*, Springer, 1986

[CFT] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York, 1968.

[CGP] K. S. Brown, *Cohomology of Groups*, Graduate Texts in Mathematics **87**, Springer, New York, 1982.

[CMA] H. Matsumura, *Commutative algebra*, 1970, Benjamin

[CPI] K. Iwasawa, *Collected Papers*, I, II, Springer, New York, 2001.

[CPS] G. Shimura, *Collected Papers*, I, II, III, IV, Springer, New York, 2002.

[CRT] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, New York, 1986.

[DAV] G. Faltings and C.-L. Chai, *Degeneration of Abelian Varieties*, Springer, New York, 1990.

[ECH] J. S. Milne, Étale Cohomology, Princeton University Press, Princeton, NJ, 1980.

[EEK] A. Weil, *Elliptic Functions according to Eisenstein and Kronecker*, Springer, 1976

[EGA] A. Grothendieck and J. Dieudonné, *Eléments de Géométrie Algébrique*, Publications IHES **4** (1960), **8** (1961), **11** (1961), **17** (1963), **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[FGA] A. Grothendieck, *Fondements de la Géométrie Algébrique*, Séminaire Bourbaki exp. no.149 (1956/57), 182 (1958/59), 190 (1959/60), 195 (1959/60), 212 (1960/61), 221 (1960/61), 232 (1961/62), Benjamin, New York, 1966.

[GCH] J.-P. Serre, *Galois Cohomology*, in Monographs in Mathematics, Sp-ringer, New York, 2002.

[GIT] D. Mumford, *Geometric Invariant Theory*, Ergebnisse **34**, Springer, New York, 1965.

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, second edition, World Scientific, Singapore, 2011.

[HAL] P. J. Hilton and U. Stammback, *A Course in Homological Algebra*, Graduate Texts in Mathematics **4**, Springer, New York, 1970.

[HMI] H. Hida, *Hilbert modular forms and Iwasawa theory*, Oxford University Press, 2006

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, and Iwanami Shoten, Tokyo, 1971.

[LAG] J. E. Humphreys, *Linear Algebraic Groups*, GTM **21**, Springer, 1987

[LFE] H. Hida, *Elementary Theory of L-Functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, England, 1993.

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000.

[MFM] T. Miyake, *Modular Forms*, Springer, New York-Tokyo, 1989.

[NMD] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Sp-ringer, New York, 1990.

[PAF] H. Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, 2004, Springer

[PHT] O. Brinon and B. Conrad, CMI Summer School notes on p-adic Hodge theory, 2009

[RAG] J. C. Jantzen, *Representations of Algebraic Groups*, Academic Press, Orlando, FL, 1987.

[REC] J. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, 1992, Springer-Verlag, New York

[SFT] G. E. Bredon, *Sheaf Theory*, McGraw-Hill, New York, 1967.

[SGA4$\frac{1}{2}$] P. Deligne, *Cohomologie Etale*, Séminaire de geometrie algébrique, Lecture Notes in Mathematics **569**, Springer, New York, 1977.

[SGL] H. Hida, *On the Search of Genuine p-Adic Modular L-Functions for $GL(n)$*, Mem. SMF **67**, 1996.

[TCF] M. Nagata, *Theory of Commutative Fields*, AMS, 1993

Articles

[A] M. Artin, Néron models, in [ARG], 213–230.

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$ or Wild 3-adic exercises, Journal AMS **14** (2001), 843–939.

[BDST] K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor, On icosahedral Artin representations, Duke Math. J. **109** (2001), 283–318.

[C] H. Carayol, Sur la mauvaise réduction des courbes de Shimura, Compositio Math. **59** (1986), 151–230

[C1] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, Ann. Sci. Ec. Norm. Sup. 4-th series, **19** (1986), 409–468

[Ca] H. Cartan, Formes modulaires, Sémeinaire H. Cartan, École Normale Sup. 1957/58, Exposé 4, 1958

[D] P. Deligne, Formes modulaires et représentations l–adiques, Sém. Bourbaki, exp. 335, 1969

[D1] P. Deligne, Variété abeliennes ordinaires sur un corps fini, Inventiones Math. **8** (1969), 238–243.

[D2] P. Deligne, Travaux de Shimura, Sem. Bourbaki, Exp. 389, Lecture Notes in Math. **244** (1971), 123–165.

[D3] P. Deligne, Variétés de Shimura: Interprétation modulaire, et techniques de construction de modéles canoniques, Proc. Symp. Pure Math. **33.2** (1979), 247–290.

[DeM] P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus, Publ. I.H.E.S. **36** (1969), 75–109.

[Di] F. Diamond, The refined conjecture of Serre, in "Elliptic Curves, Modular Forms & Fermat's Last Theorem," International Press, 1995, pages 22–37

[Dr] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abhandlungen Math. Sem. Hansischen Universität **14** (1941), 197–272.

[H81] H. Hida, On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves (Doctor's Thesis at Kyoto University, 1980), Amer. J. Math. **103** (1981), 727–776.

[H86] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones Math. **85** (1986), 545–613.

[H11] H. Hida, Hecke fields of analytic families of modular forms, J. Amer. Math. Soc. **24** (2011), 51-80

[Ho] T. Honda, Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan **20** (1968), 83–95

[I] J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. **81** (1959), 561–577.

[K] C. Khare, Serre's modularity conjecture: the level one case. Duke Math. J. **134** (2006), 557–589.

[K1] C. Khare, Serre's conjecture and its consequences. Jpn. J. Math. **5** (2010), 103–125.

[KW] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. I, II. I: Invent. Math. **178** (2009), 485–504; II. Invent. Math. **178** (2009), 505–586

[L] J. H. Loxton, On two problems of R. M. Robinson about sum of roots of unity, Acta Arithmetica **26** (1974), 159–174.

[Ma] B. Mazur, Modular curves and the Eisenstein ideal, Publ. IHES **47** (1977), 33–186

[Mi] J. Milne, Abelian varieties, in [ARG], 103–150.

[Mi1] J. Milne, Jacobian varieties, in [ARG], 167–212.

[Mi2] J. Milne, Canonical models of (mixed) Shimura varieties and automorphic vector bundles, Perspective Math. **10** (1990), 283–414.

[Mi3] J. Milne, Shimura varieties and motives, Proc. Symp. Pure Math. **55** (1994) ([MTV]) Part 2, 447–523.

[R] K. A. Ribet, P–adic interpolation via Hilbert modular forms, Proc. Symp. Pure Math. **29** (1975), 581–592

[R1] K.A. Ribet, On l-adic representations attached to modular forms. Inventiones Math. **28** (1975), 245–275

[R2] K. A. Ribet, Galois action on division points of abelian varieties with real multiplications, American J. Math. **98** (1976), 751–804.

[R3] K. A. Ribet, On l-adic representations attached to modular forms. II. Glasgow Math. J. **27** (1985), 185–194

[R4] K. A. Ribet, On modular representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Inventiones Math. **100** (1990), 431–476

[Se] J.-P. Serre, On modular representations of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Duke Math. J. **54** (1987), 179–230

[SeT] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. **88** (1968), 452–517

[Sh] G. Shimura, Correspondances modulaires et les fonctions ζ de courbes algébriques. J. Math. Soc. Japan **10** (1958) 1–28

[Sh1] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, Ann. of Math. **78** (1963), 149–192 ([63b] in [CPS] I).

[Sh2] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math. **85** (1967), 58–159 ([67b] in [CPS] II).

[Sh3] G. Shimura, On canonical models of arithmetic quotients of bounded symmetric domains, Ann. of Math. **91** (1970), 144–222; II, **92** (1970), 528–549 ([70a–b] in [CPS] II).
[T] J. Tate, p-divisible groups, Proc. Conf. on local fields, Driebergen 1966, Springer 1967, 158–183.
[T1] J. Tate, Endomorphisms of abelian varieties over finite fields, Inventiones Math. **2** (1966), 134–144
[T2] J. Tate, Class d'isogénies des variétés abéliennes sur un corps fini (d'après Honda), Séminaires Bourbaki 318, Novembre 1966
[T3] J. Tate, Conjectures on algebraic cycles in ℓ-adic cohomology, in [MTV] Part 1, Proc. Symp. Pure Math. **55** (1994), 71–82.
[Ta] R. Taylor, On Galois representations associated to Hilbert modular forms, Inventiones Math. **98** (1989), 265–280.
[Ta1] R. Taylor, l-adic representations associated to modular forms over imaginary quadratic fields. II. Invent. Math. **116** (1994), 619–643
[Ta2] R. Taylor, On Galois representations associated to Hilbert modular forms II, in Series in Number Theory **1** (1995): "Elliptic curves, Modular forms, & Fermat's last theorem", pp.185–191
[Ta3] R. Taylor, Icosahedral Galois representations, Pacific J. Math. (1997), Olga Tauski-Todd Memorial Issue 337–347.
[Ta4] R. Taylor, On icosahedral Artin representations II, Amer. J. Math. **125** (2003), 549–566.
[TaW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, Ann. of Math. **141** (1995), 553–572.
[We] A. Weil, Numbers of solutions of equations in finite fields, Bull. AMS **55** (1949), 497–508 (Œuvres I, [1949])
[Wi] A. Wiles, On ordinary Λ-adic representations associated to modular forms, Inventiones Math. **94** (1988), 529–573.
[Wi1] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551.

Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, U.S.A.
E-mail address: hida@math.ucla.edu