2

Elliptic Curves and Modular Forms

We now describe basics of elliptic curves and modular curves in three steps:

1. as plane curves over a field;
2. as scheme/group functor over a ring;
3. modular forms as functorial rules on modular curves.

Elliptic curves and modular curves are perhaps the most important objects studied in number theory. The theory gives a base of the proof by Wiles (through Ribet's work) of Fermat's last theorem, it supplies us with the simplest (and perhaps the most beautiful) example of Shimura varieties (cf. [IAT] Chaps. 6 and 7), a fast prime factorization algorithm (cf. [REC] IV), and so on. We give a sketch of the theory of modular curves and modular forms and (a minimal amount of) notation and terminology for us to be able to state main themes in the next chapter. For graduate students just starting to learn elliptic curves and modular forms, this chapter hopefully serves as an introductory illustration of the theory. Experienced readers may skip this chapter, going directly to the Chap. 3.

2.1 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 the familiar one: $k = \mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C} = \Omega$.

2.1.1 Plane Curves

Let $\mathfrak{a}$ be a principal ideal of the polynomial ring $k[X, Y]$. Note that polynomial rings over a field are a unique factorization domain. We thus have the prime factorization $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ with principal primes $\mathfrak{p}$. We call $\mathfrak{a}$ *square-*

H. Hida, *Elliptic Curves and Arithmetic Invariants*, Springer Monographs in Mathematics, DOI 10.1007/978-1-4614-6657-4_2,

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* defined over k 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 and 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 f of generators and depends only on the ideal $\mathfrak{a}$; thus, it is more appropriate to write it as $V_{\mathfrak{a}}$. As an exceptional case, we note $V_{(0)}(A) = A^2$. Geometrically, if $\mathfrak{a} \neq \{0\}$, we think of $V_{\mathfrak{a}}(\Omega)$ as a curve in $\Omega^2 = V_{(0)}(\Omega)$. This is intuitively more geometric if we take $k \subset \Omega = \mathbb{C}$ (a "curve" is a two-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 $\overline{\mathfrak{a}}$ for the principal ideal of $\overline{k}[X,Y]$ generated by $\mathfrak{a}$, we have

$$\overline{\mathfrak{a}} = \left\{g(X,Y) \in \overline{k}[X,Y] \middle| g(x,y) = 0 \text{ for all } (x,y) \in V_{\mathfrak{a}}(\overline{k})\right\}. \tag{2.1.1}$$

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 $SETS$; see Sect. 4.1 for category and functor and Example 4.1 for a list of notations for categories). 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 a number-theoretic viewpoint (Diophantine problems), studying $V_{\mathfrak{a}}(A)$ for a small field (or even a ring, such as $\mathbb{Z}$) is important. Thus, it would often be better to regard $V_{\mathfrak{a}}$ as a functor.

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

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

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 have a finer nontrivial decomposition $V_{\mathfrak{p}} = V \cup W$ with plane curves V and W defined over k. A prime ideal $\mathfrak{p} \subset k[X,Y]$ generates an ideal in $\overline{\mathfrak{p}}$ in $\overline{k}[X,Y]$, which may decompose into a product of primes in $\overline{k}[X,Y]$. If the ideal $\overline{\mathfrak{p}}$ 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 curves defined over k. If $\mathbf{A}^1 = V_{\mathfrak{b}}$ is the *affine line*, that is, $V_{\mathfrak{b}}(A) \cong A$ 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 $V_{\mathfrak{a}}$; hence, $R_{\mathfrak{a}}$ is the ring of regular k-functions of $V_{\mathfrak{a}}$ defined over k. Let $\mathbf{A}^n = (\mathbf{A}^1)^n$.

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 $\phi_? \mod \mathfrak{a}$ $(? = X, Y)$ 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,

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

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 from $V_{\mathfrak{a}}$ into $V_{\mathfrak{b}}$ [we will see later that $\mathrm{Hom}_{COF}(V_{\mathfrak{a}}, V_{\mathfrak{b}})$ is a set].

The polynomials (ϕ_X, ϕ_Y) induce a k-algebra homomorphism $\underline{F}$ from $k[X,Y]$ into itself by pullback; 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 that is a special case of Yoneda's lemma:

Lemma 2.1 *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.

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

$$V_\mathfrak{a}(A) \ni (a,b) \leftrightarrow (\Phi(X,Y) \mapsto \Phi(a,b)) \in \mathrm{Hom}_{ALG_{/k}}(R_\mathfrak{a}, A).$$

Thus, for 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, clearly, if we start with $\underline{F}$, the above association leads to F.

Exercise 2.2 *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.*

Recall that $V_\mathfrak{a}$ is *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 2.3 *1. Prove that for any unique factorization domain R, $R[X]$ is a unique factorization domain.*
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 the morphism $F : V_\mathfrak{a} \to V_\mathfrak{b}$ of functors.*

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* and is written as $k(V_\mathfrak{a})$.

2.1.2 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 the corresponding linear space as $T_P = V_{\mathfrak{b}}$ for the principal ideal $\mathfrak{b}$ generated by $\frac{\partial f}{\partial X}(a,b)X + \frac{\partial f}{\partial Y}(a,b)Y$. We say that $V_{\mathfrak{a}}$ is *nonsingular* 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 words, if $(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P)) \neq (0,0)$.

Example 2.4 Let $\mathfrak{a} = (f)$ for $f(X,Y) = Y^2 - X^3$. Then for $(a,b) \in V_{\mathfrak{a}}(K)$, we have

$$\frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b) = -3a^2(X-a) + 2b(Y-b).$$

Thus, this curve is singular only at $(0,0)$.

Example 2.5 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 $g'(x_0) = 0$ and hence is 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. A 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 $R_{\mathfrak{a}}$. Then 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 2.6 *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 $\partial(\phi\varphi) = \varphi(P)\partial(\phi) + \phi(P)\partial(\varphi)$. Write $D_{V,P}$ for the space of

all K-derivations at P, which is a K-vector space. Clearly, for $\mathbf{A} := V_{(0)}$, $D_{\mathbf{A},P}$ is a two-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 $\Omega_{(a,b)} = (X-a, Y-b)/(X-a, Y-b)^2$ is a two-dimensional vector space over K generated by $X-a$ and $Y-b$. Thus, $D_{\mathbf{A},P}$ and $\Omega_{(a,b)}$ are dual to 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 we have

$$\phi(X,Y) \equiv \frac{\partial \phi}{\partial X}(a,b)(X-a) + \frac{\partial \phi}{\partial Y}(a,b)(Y-b) \mod (X-a, Y-b)^2.$$

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, $f\partial : \varphi \mapsto f \cdot \partial(\varphi)$ because $f \in R_\mathfrak{a}$ is again a k-derivation. The totality of the k-derivation $Der_{V_\mathfrak{a}/k}$ is therefore an $R_\mathfrak{a}$-module.

To make T_P explicit, first take $\mathfrak{a} = (0)$; thus, $V_\mathfrak{a} = \mathbf{A}^2$. We have

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

for $\partial \in Der_{\mathbf{A}^2/k}$; hence, ∂ 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; thus, 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 $R_\mathfrak{a}$-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 $(dY, \partial) = \partial Y$; hence, $\{dX, dY\}$ 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 and the right-hand sides have 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 the following:

Lemma 2.7 *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 2.8 If $V_\mathfrak{a}$ is irreducible (so that $R_\mathfrak{a}$ is an integral domain), the space $k(V_\mathfrak{a})\Omega_{V_\mathfrak{a}/k} = (k(V_\mathfrak{a})dX \oplus k(V_\mathfrak{a})dY)/k(V_\mathfrak{a})df$ has dimension 1, 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 nonconstant), 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 2.9 *The four following 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 $\dim P/P^2 = \dim \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$. Thus, by Nakayama's lemma (Lemma 10.8), $\mathfrak{m}_P$ is principal. Any nonzero prime ideal of $k[X,Y]$ is either principal 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.

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-defined 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 2.10 *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 discrete valuation ring if and only if $\mathcal{O}_{V_{\mathfrak{a}},P}$ is a discrete valuation ring.*

Write $\mathrm{Max}(R_{\mathfrak{a}})$ for the set of maximal ideals of $R_{\mathfrak{a}}$. Then, clearly, 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 say 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, no less).

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

Corollary 2.11 *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. Then $\mathcal{O}_{V,P}$ is a normal local domain with principal maximal ideal, which is a discrete valuation ring (cf. [CRT] Theorem 11.1).

Exercise 2.12 *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 $k \subset A$ that 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.*

2.1.3 Projective Space

Let A be a commutative ring. Write A_P for 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 $M_P = \left\{\frac{m}{s} \middle| s \in A \setminus P\right\}/\sim = A_P \otimes_A M$ is free over A_P. We call M locally free if M_P is free at all prime ideals P of A. If $\operatorname{rank}_{A_P} M_P$ is constant r independent of P, we write $\operatorname{rank}_A M = r$.

Write $ALG_{/B}$ for the category of B-algebras; hence, $\operatorname{Hom}_{ALG_{/B}}(A, A')$ is made up of B-algebra homomorphisms from A into A', sending the identity 1_A to the identity $1_{A'}$. Here B is a general base ring, and we write ALG for $ALG_{/\mathbb{Z}}$ (and ALG is the category of all commutative rings with identity). We consider a covariant functor $\mathbf{P}^n = \mathbf{P}^n_{/B} : ALG_{/B} \to SETS$ 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 (represented by the *projective space* $\mathbf{P}^n$ of dimension n). Indeed, if $\sigma : A \to A'$ is a B-algebra homomorphism, letting it act on A^{n+1} coordinatewise, $L \mapsto \sigma(L) \otimes_A A'$ [the A'-module generated by $\sigma(L)$] induces a map $\mathbf{P}^n(A) \to \mathbf{P}^n(A')$. If A is a field K, then $L \in \mathbf{P}^n(K)$ has to be free of dimension 1 generated by a nonzero vector $x = (x_0, x_1, \ldots, x_n)$. The vector x is unique up to multiplication by nonzero elements of K. Thus, we have proven the first statement (for a field) of the following:

Lemma 2.13 *Suppose that K is a local ring with maximal ideal $\mathfrak{m}$. Then $\mathbf{P}^n(K)$ is canonically in bijection to*

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

Moreover, writing $D_i : ALG_{/B} \to SETS$ for the subfunctor $D_i(A) \subset \mathbf{P}^n(A)$ made up of the classes L whose projection to the ith 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 B-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 ith coordinate.

Proof. Since $K = K_{\mathfrak{m}}$ for its maximal ideal $\mathfrak{m}$, L is 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. Taking a basis $\overline{v}_1, \ldots, \overline{v}_n$ of K^{n+1}/L, we 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 (by Nakayama's lemma; Lemma 10.8). Thus, $\underline{x} \not\equiv 0 \mod \mathfrak{m}$ for the maximal ideal $\mathfrak{m}$ of K. In particular, for an index i, $x_i \notin \mathfrak{m}$; hence, $x_i \in K^\times$. Since the projection of L to the ith 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.

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

Thus, L is free of rank 1 over A and hence has a generator $(x_0, \dots, x_n)$ with $x_i \in A^\times$. Then $(x_0, \dots, x_n) \mapsto (\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}) \in A^n$ 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 $(x_0, \dots, x_n)$, as only the ratio matters.

Exercise 2.14 *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 second coordinates 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, $\mathbf{P}^1(\mathbb{R})$ [resp., $\mathbf{P}^1(\mathbb{C})$] is isomorphic (topologically under Euclidean topology) to a circle (resp., a Riemann sphere).

We now assume that $n = 2$. Set $L = \{(x{:}y{:}0) \in \mathbf{P}^2(K)\}$. Then $\mathbf{P}^1 \cong L$ by $(x{:}y) \mapsto (x{:}y{:}0)$; hence, 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 algebraically closed fields K), $\mathbf{P}^2(K)$ is the union of the affine plane and a projective line $L \cong \mathbf{P}^1(K)$. We let $L = L_\infty$ (the line at ∞).

2.1.4 Projective Plane Curve

Return to our base field $B = k$. 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 have $L \in \mathbf{P}^2(K)$ sent its generator $(a, b, c) \in L$ to identify $\mathbf{P}^2(K)$ with the (classical) projective space with homogeneous coordinate. Since $F(L) = 0$ if and only if $F(a{:}b{:}c) = 0$, 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 general A), 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 at ∞: $\overline{V}_\mathfrak{a} \cap L_\infty$. Since in $D_j \cong \mathbf{A}^2$ $(j = 0, 1, 2)$, $\overline{V}_\mathfrak{a} \cap D_j$ 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 completion/compactification of the (open) affine curve $V_\mathfrak{a}$. 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 2.1, we define $\mathrm{Hom}_{\text{proj } k\text{-curves}}(\overline{V}_\mathfrak{a}, \overline{V}_\mathfrak{b}) := \mathrm{Hom}_{COF}(\overline{V}_\mathfrak{a}, \overline{V}_\mathfrak{b})$.

A projective plane curve $\overline{V}_\mathfrak{a}$ is nonsingular (or smooth) if $\overline{V}_\mathfrak{a} \cap D_j$ is a nonsingular 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 $D_j \cap V_\mathfrak{a}$.

Example 2.15 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). We call this point the origin $\mathbf{0}$ of the curve $\overline{V}_\mathfrak{a}$. If $\overline{V}_\mathfrak{a}$ is smooth, the pair $(\overline{V}_\mathfrak{a}, \mathbf{0})$ is called an elliptic curve.

Exercise 2.16 *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* $k(C)$ of C over k is the field of fractions of $\mathcal{O}_{C,P}$ for any $P \in C(\overline{k})$ hence, independent of $C \cap D_j$.

Lemma 2.17 *Take a nonzero $f \in k(C)$. Then there exist homogeneous polynomials $G(X,Y,Z), H(X,Y,Z) \in k[X,Y,Z]$ 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 $C \cap D_2$ $f(x,y,1) = \frac{h(x,y)}{g(x,y)}$. 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 2.18 Look at $\phi = cx + dy$ in $k(C)$ for $C = \overline{V}_\mathfrak{a}$ for $\mathfrak{a}$ generated by $y^2 - x^3 - ax - b$. Then C is defined by $Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$, and

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

Thus, ϕ has a 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 $C_{/k}$. Set $C_i = C \cap D_i$, 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. Obviously, the totality $T_{C/k}$ of global tangent vectors is a k-vector space. The k-dual of $T_{C/k}$ is called the space of k-differentials over k and written as $\Omega_{C/k}$. We will see that $\Omega_{C/k}$ is finite dimensional over k.

Corollary 2.19 *Suppose that C is nonsingular. Each $\phi \in k(C)$ induces $\phi \in \mathrm{Hom}_{\text{proj } k\text{-curves}}(C, \mathbf{P}^1)$. Indeed, we have $k(C) \sqcup \{\infty\} \cong \mathrm{Hom}_{\text{proj } k\text{-curves}}(C, \mathbf{P}^1)$, 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 $\phi(L) \in \mathbf{P}^1(A)$; thus, 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 2.13, L is generated by (a, b, c) with at least one unit coordinate. Then any $\ell \in L$ is of the form $\lambda(a, b, c)$ (for a scalar λ), 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 (see [CRT] Theorem 2.2–3 and Lemma 10.8 in the text), $A/\phi(L)$ 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 $\phi(L) \otimes_k \overline{k} \in \mathbf{P}^1(\overline{k})$ and hence $\phi(L) \otimes_A A/\mathfrak{m} \in \mathbf{P}^1(k)$, which implies $\phi(L) \in \mathbf{P}^1(A)$.

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, and so $\phi(L)$ and $A^2/\phi(L)$ are locally free of rank 1. Therefore, $\phi(L) \in \mathbf{P}^1(A)$; hence, $L \mapsto \phi(L)$ induces a natural transformation of functors.

Exercise 2.20 *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. $\mathrm{Hom}_{proj\ k\text{-}curves}(C, \mathbf{P}^1) \setminus \infty \cong k(C)$.

2.1.5 Divisors

Let C be a nonsingular projective geometrically irreducible plane curve. Since C is nonsingular, for any point $P \in C(\overline{k})$, $\mathcal{O}_{C,P}$ is a discrete valuation ring, and the rational function field $\overline{k}(C)$ is the quotient field of $\mathcal{O}_{C,P}$ (regarding C as defined over $\overline{k}$). Writing $v_P : \overline{k}(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ for the additive valuation of $\mathcal{O}_{C,P}$, we have a well-defined $v_P(f) \in \mathbb{Z}$ for any nonzero 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 $v_P(f) = \min(n : a_n(f) \neq 0)$. We start with Bézout's theorem:

Theorem 2.21 *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 $|C(\overline{k}) \cap C'(\overline{k})| = m \cdot n$.

Here we do not assume F and G are square-free. As is clear from the definition of multiplicity given below, for example, if $F = F_0^e$ with $\deg(F_0) = m_0$,

$$|C(\overline{k}) \cap C'(\overline{k})| = e|C_0(\overline{k}) \cap C'(\overline{k})| = em_0 \cdot n = m \cdot n$$

for the curve C_0 defined by $F_0 = 0$. Thus, for the proof of the theorem, we may assume that F and G are square-free.

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 a better definition of multiplicity in good textbooks on algebraic geometry (e.g., [ALG] Theorem I.7.7).

The *divisor group* $\mathrm{Div}(C)$ of a smooth 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 the *degree* of D by $\deg(D) = \sum_P m_P$.

Consider the space of *meromorphic differentials*:

$$\Omega_{C/k,\eta} = \{f \cdot \omega | f \in k(C), \omega \in \Omega_{C_i/k}\} \ (= k(C) \cdot \Omega_{C/k} \text{ if } \Omega_{C/k} \neq 0).$$

For $\omega \in \Omega_{C/\overline{k},\eta}$, we have its expansion $\sum_n a_n(\omega)t_P^n dt_P$ at each $P \in C(\overline{k})$; thus, we define $v_P(\omega) := \min(n : a_n(\omega) \neq 0)$.

Since there are only finitely many poles and zeros of f, 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 a meromorphic differential ω, we define again $\mathrm{div}(\omega) = \sum_P v_P(\omega)[P]$. By Lemma 2.17, we may write $f(x{:}y{:}z) = \frac{h(x:y:z)}{g(x:y:z)}$ for a homogeneous polynomial h, g in $\overline{k}[x,y,z]$ of equal 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 $-\sum_{P, v_P(f)<0} m_P = m\deg(g)$. Thus, we get the following:

Lemma 2.22 *Let C be a smooth projective plane curve. For any $f \in \overline{k}(C)$, $\deg(\mathrm{div}(f)) = 0$, and f is a constant in $\overline{k}$ if $f \in \overline{k}(C)$ is regular at all $P \in C$.*

Lemma 2.23 *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. Consider the curve C' defined by $H = 0$. Suppose C is defined by a homogeneous equation of degree m. Then by Bézout's theorem (applied to C and C'), $m \cdot n = \deg(\mathrm{div}_0(\phi)) = 1$. Thus, $m = n = 1$, and it is then clear 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 2.19, $\deg(\mathrm{div}_0(f))$ is the number of points over 0 (counting with multiplicity) of the regular map $f : C \to \mathbf{P}^1$. By taking a constant $\alpha \in k \subset \mathbf{P}^1$ away from f, $\deg(\mathrm{div}_0(f - \alpha)) = 1 = \deg(\mathrm{div}_\infty(f - \alpha))$, and $|f^{-1}(\alpha)| = \deg(\mathrm{div}_0(f - \alpha)) = 1$; hence, we find that f is one-to-one and onto. Thus, f is an isomorphism. □

Write $\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C_{/\overline{k}}) | \deg(D) = 0\}$. 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 say that D and D' are *algebraically equivalent* if $\deg(D) = \deg(D')$. The quotient groups

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

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).

2.1.6 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 $C_{\overline{k}}$,

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

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

Example 2.24 Let $C = \mathbf{P}^1$. Take a 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 ∞, $\mathrm{div}(f) + D \geq 0$ 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 a pole at ∞. Thus, $L(D) = \{g(x) | \deg(g(x)) \leq \deg(D)\}$, and we have $\ell(D) =$

$1+\deg(D)$. If C is a plane projective curve, we write $f = \frac{h(X,Y,Z)}{g(X,Y,Z)}$ as a reduced fraction by Lemma 2.17. Take $D = \sum_P m_P[P] \in \mathrm{Div}(C)$, 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 $D > 0$ (i.e., $m_P > 0$ for some P), we may assume that $V_{(g(X,Y,1))} \cap C$ contains $|D|$. In order not to have a pole in $C \setminus D_2$, $\deg(h)$ has to be bounded; thus, $\ell(D) < \infty$. Since $L(D) \subset L(D_+)$ in general, writing $D = D_+ + D_-$ so that $D_+ \geq 0$ and $-D_- \geq 0$, this shows that $\ell(D) < \infty$.

Exercise 2.25 *Give more details of the proof of* $\ell(D) < \infty$.

Theorem 2.26 (Riemann–Roch) *Let* $C = \overline{V}_{\mathfrak{a}}$ *be a smooth projective irreducible curve over a field* k. *Let* $K = \mathrm{div}(\omega)$ *for meromorphic* $0 \neq \omega \in \Omega_{C/\overline{k},\eta}$. *Then, for* $g = \dim_{\overline{k}} \Omega_{C/\overline{k}}$, *we have* $\ell(D) = 1 - g + \deg(D) + \ell(K - D)$ *for all divisors* D *on* $C(\overline{k})$. *If* $g = 1$, *we have* $K = 0$ *in* $\mathcal{J}(C)$.

The number g in the above theorem is called the *genus* of the curve C and is written as $g(C)$. 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 2.27 *If* $g(C) = 1$ *and* $\deg(D) > 0$, *then we have* $\ell(D) = \deg(D)$ *and* $\ell(-D) = 0$.

Proof. For a nonconstant $f \in \overline{k}(E)$, $\deg(\mathrm{div}(f)) = 0$ implies that f has a pole somewhere. If $D > 0$, $f \in L(-D)$ does not have pole and hence is constant. Since $D > 0$, f vanishes at $P \in |D|$. Thus, $f = 0$. More generally, if $\deg(D) > 0$ and $\phi \in L(-D)$, then $0 > \deg(-D) = \deg(\mathrm{div}(\phi)) - \deg(D) \geq 0$; thus, $\phi = 0$. Thus, if $\deg(D) > 0$, then $\ell(-D) = 0$. Since $K = 0$ if $K = \mathrm{div}(\omega)$ for $0 \neq \omega \in \Omega_{C/\overline{k}}$, we have by Theorem 2.26 that $\ell(D) = \deg(D) + \ell(0 - D) = \deg(D)$. □

Because $\deg(\mathrm{div}(f)) = 0$, if $D \gg 0$, $\ell(-D) = 0$ [as $f \in L(-D)$ has to vanish over D and regular everywhere outside D]. In particular, $\ell(K - D) = 0$ if $D \gg 0$. Thus, the above theorem implies what Riemann originally proved:

Corollary 2.28 (Riemann) *Let $C = \overline{V}_{\mathfrak{a}}$ be a nonsingular projective curve defined over a field k. Then there exists a nonnegative integer $g = g(C)$ such that $\ell(D) \geq 1 - g + \deg(D)$ for all divisors D on $C(\overline{k})$, and the equality holds for sufficiently positive divisors D.*

By Example 2.24, we conclude $g(\mathbf{P}^1) = 0$ from the corollary.

Exercise 2.29 *Prove $\Omega_{\mathbf{P}^1/\overline{k}} = 0$ (without using the Riemann–Roch theorem).*

2.1.7 Regular Maps from a Curve into a 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 a nontrivial common divisor.

Lemma 2.30 *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 $P \in C(\overline{k})$. For $L \in C(A) \subset \mathbf{P}^n(A)$, define $\phi_A(L)$ 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 basically the same as that of Corollary 2.19.

Exercise 2.31 *Prove the above lemma.*

2.2 Elliptic Curves

An *elliptic curve* $E_{/k}$ is a nonsingular, projective, geometrically irreducible plane curve of genus 1 with a point $\mathbf{0}_E$ specified. Here we define that the genus $g(E)$ regarding E is defined over $\overline{k}$. We will study elliptic curves in more detail in this section.

2.2.1 Abel's Theorem

When we consider $P \in E(k)$ as a divisor, we write $[P]$. So $3[P]$ is a divisor supported on P with multiplicity 3. We prove

Theorem 2.32 (Abel) *Let $E_{/k}$ be an elliptic curve with origin $\mathbf{0}_E$. The correspondence $P \mapsto [P] - [\mathbf{0}_E]$ induces a bijection $E(\overline{k}) \cong \mathcal{J}(E)$ (the Jacobian of 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 2.23, 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 2.27, $\ell(D+[\mathbf{0}_E])=1$, 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 nonnegative divisor with degree 1 is a single point $[P]$. Thus, $D+[\mathbf{0}_E]$ is linearly equivalent to $[P]$; hence, the map is surjective.

Corollary 2.33 *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 the curve 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 easily show that $\lambda(P)=1$ for all P (see Sect. 6.1.4). 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 2.34 *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 2.35 *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 2.36 If k is perfect, $\overline{k}/k$ is a Galois extension possibly of infinite degree; thus, by Galois theory (see Sect. 4.2.1), 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 Theorem 6.3).

2.2.2 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 $\mathbf{0} = \mathbf{0}_E$. Consider $L(n[\mathbf{0}])$, which has dimension n if $n > 0$ by Corollary 2.27. 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 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 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. This y is unique up to the transformation: $y \mapsto y + ax + b$ $(a, b \in k)$.

Proposition 2.37 *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*

$$y^2 = 4x^3 - g_2 x - g_3 \quad \textit{with} \quad g_2, g_3 \in k, \tag{2.2.1}$$

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 $4X^3 - g_2 X - g_3$ 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 (2.2.1) 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:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{with } a_j \in k, \tag{2.2.2}$$

because the poles of order 6 of y^2 and x^3 have to be canceled. We homogenize (2.2.2) 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 pullback 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; hence, $[k(E) : k(x)] = 2$. Similarly, $[k(E) : k(y)] = 3$. Since $[k(E) : k(C)]$ is a common factor of the two degrees $[k(E) : k(x)] = 2$ 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 (2.2.2).

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

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

As $\omega = (a + \text{higher-degree terms})dT$ 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 (and ω is said to be adapted to the parameter T). We normalize x so that $x = T^{-2} + \text{higher-degree terms}$. We now suppose that 2 is invertible in k. Then we 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 a 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 $a_1 = a_3 = 0$):

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

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 (2.2.1) (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 $g(x) = 0$ (see Example 2.5).

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 $(0,0)$, $v_P(y) = v_P(x)$; hence, P is neither a zero nor a pole of t. The function t never vanishes 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 zeros can be excluded similarly. Thus, we conclude $\Delta(E,\omega) \neq 0$ ($\Leftrightarrow C$ is smooth), and we have $E \cong C$ by ϕ.

Conversely, we have seen that any curve defined by (2.2.1) is smooth in Example 2.5 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 $\mathbf{P}^2$ (Example 2.15). 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 (2.2.1). If such an ω exists, all other holomorphic differentials ω' are of the form $f\omega$ with $\mathrm{div}(f) \geq 0$, which implies $f \in k$; hence, $g = \dim_k \Omega_{E/k} = 1$, 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 2.38 *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 each 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 $\mathbf{0} = \infty$.

2.2.3 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 $\varphi^*\omega' = \omega$ and $\varphi(\mathbf{0}_E) = \mathbf{0}_{E'}$. Here, for $\omega' = f dg$, $\varphi^*\omega' = (f \circ \varphi)d(g \circ \varphi)$; 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 $\mathbf{0}_{E'}$ 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 $\varphi^*\omega' = \omega$ and $\varphi(\mathbf{0}_E) = \mathbf{0}_{E'}$]. 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

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

where $[\cdot]$ indicates the set of isomorphism classes of the objects inside the brackets 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 2.39 *If k has characteristic 2, show that we cannot have any ring $\mathcal{R}$ such that*

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

for all field extensions K/k. Here the isomorphism is a natural transformation between 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: $(E,\omega) \bmod K^\times$ under the action of $\lambda \in K^\times$ given by $(E,\omega)_{/K} \mapsto (E,\lambda\omega)_{/K}$, 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

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

$$g_2(E,\lambda\omega) = \lambda^{-4}g_2(E,\omega) \quad \text{and} \quad g_3(E,\lambda\omega) = \lambda^{-6}g_3(E,\omega). \tag{2.2.3}$$

Thus, we have the following result:

Theorem 2.40 *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 $J(E) = \frac{(12g_2(E,\omega))^3}{\Delta(E,\omega)}$. Then J only depends on E (not the chosen differential ω). If $J(E) = J(E')$, then we have

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

for a 12th root λ of $\Delta(E,\omega)/\Delta(E',\omega')$. Note that the 12th 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

$$y^2 = 4x^3 - gx - g \quad \text{for} \quad g = \frac{27j}{j-1}$$

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's lemniscate). Thus, we have the following:

Corollary 2.41 *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 2.42 *1. Prove that $g_j(E',\omega') = \lambda^{-2j}g_j(E,\omega)$ for suitable ω and ω' and a suitable 12th 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.

2.3 Modular Forms

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

2.3.1 Elliptic Curves over General Rings

What we have done over fields can also be done over general noetherian rings A. We sketch the theory (see Chap. 6 for detailed proofs). 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 polynomial $\Phi(X,Y,Z) \in A[X,Y,Z]$, 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

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

Clearly, 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 2.43 *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 $C \subset \mathbf{P}^2_{/A}$. 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 $\phi : R_i \to K$; hence, $\mathrm{Ker}(\phi)$ is a maximal ideal of R_i.

Exercise 2.44 *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* $\mathrm{Ker}(\phi)$ *for some ϕ.*

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

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

where $\phi : R_i \to \overline{k}$ is the k-algebra homomorphism inducing the point P. 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 $\mathcal{O}_{C,P}/\mathfrak{m}_P \cong \mathrm{Im}(P) \subset K$.

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 sketch a general definition of smoothness, but before starting this subtle process of defining smoothness over a ring, we point out that—precise definitions 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 over rings, he or she can just admit this fact for a while to go through this section and the next (as we learn more about this in Chap. 4).

Here is a formal definition of smoothness. For A-algebras R and R', we define the R'-module of derivations $Der_A(R, R')$ by the R'-module of derivations trivial over A [hence, $(\partial : R \to R') \in Der_A(R, R')$ satisfies $\partial(\varphi\phi) = \varphi\partial(\phi) + \phi\partial(\varphi)$ and $\partial(a) = 0$ for all $a \in A$].

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

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

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 $\widehat{A}[[T]]$ for a variable $T \in \widehat{\mathcal{O}}_{C,P}$ and any adically continuous 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 Sect. 4.1.7 and Lemma 4.32). 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; see Sect. 4.1.8 for a more thorough discussion of étale/smooth morphisms).

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 2.45 *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.*

We recall the R_i-module of derivations $Der_{C_i/A} = Der_A(R_i, R_i)$, which is the R_i-module of $\partial : R_i \to R_i$ such that $\partial(\varphi\phi) = \varphi\partial(\phi) + \phi\partial(\varphi)$ 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

$\omega_P \in \Omega_{\mathcal{O}_{C,P}/A_P} := \mathrm{Hom}_{A_P}(Der_{\mathcal{O}_{C,P}/A_P}, \mathcal{O}_{C,P})$. If C_i is smooth over A, then the R_i-module $\Omega_{C_i/A}$ is a locally free R_i-module of rank 1. We define the *relative cotangent module* $\Omega_{C/A}$ 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, $\Omega_{C/A}$ is a locally free A-module of some rank g, and this number g is called the *genus* $g(C)$ of a curve 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 and ∂ is a derivation in $Der_{E/A}$, we define $\phi_*\partial \in Der_{E'/A}$ by $\phi_*\partial_{\phi(P)}(f) = \partial_P(f\circ\phi)$ for all P. By duality, 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 (although it is if ϕ is an isomorphism).

Exercise 2.46 *Let $A = \mathbb{F}_p$. Give an example of a nonconstant 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 $F(X,Y,Z) = \sum_{i,j,l} c_{i,j,l}X^iY^jZ^l$, the σ-transform $\sigma(F)(X,Y,Z) = \sum_{i,j,l}\sigma(c_{i,j,l})X^iY^jZ^l$ defines a plane projective A'-curve $\sigma(C)$. Note that the affine ring of $\sigma(C_i)$ is the ring $R_i \otimes_{A,\sigma} A'$; hence, 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 $Der_{C_i/A} \otimes_A A' = Der_{C_i\otimes A'/A'}$. 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 $\wp : ALG \to SETS$ given by $\wp(A) = \left[(E,\omega)_{/A}\right]$ a covariant functor from ALG into $SETS$. We again have the following result basically in the same way as in the case of fields (see Sect. 6.2.1 for a proof):

Theorem 2.47 *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 $SETS$:*

$$\wp(?) \cong \mathrm{Hom}_{ALG_{/\mathbb{Z}[\frac{1}{6}]}}(\mathcal{R}, ?).$$

In other words, 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 the following:

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 $\lambda \in A^\times$.

2.3.2 Geometric Modular Forms

Let A be an algebra over $\mathbb{Z}[\frac{1}{6}]$. We restrict the functor $\wp$ to $ALG_{/A}$ and write the restriction $\wp_{/A}$. Then, by Theorem 2.47, for $\mathcal{R}_A := A[g_2, g_3, \frac{1}{\Delta}]$,

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

A morphism of functors $\phi : \wp_{/A} \to \mathbf{A}^1_{/A}$ is, by definition, given by (a collection of) maps $\phi_R : \wp_{/A}(R) \to \mathbf{A}^1(R) = R$ 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,

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

Thus, $\phi_{\mathcal{R}_A}(\mathrm{id}_{\mathcal{R}_A}) \in \mathcal{R}_A$; hence, 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 2.48 *Any functor morphism $\phi : \wp_{/A} \to \mathbf{A}^1_{/A}$ 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 $\wp_{/A} \to \mathbf{A}^1_{/A}$ 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 2.49 *For a field K with $\frac{1}{6} \in K$, prove, for $0 < w \in 2\mathbb{Z}$,*

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

2.3.3 Archimedean Uniformization

In the following three sections, we would like to give a sketch of the classical theory of elliptic curves defined over the complex field $\mathbb{C}$ created by Weierstrass. By means of Weierstrass $\wp$-functions, we can identify $E(\mathbb{C})$ (for each elliptic curve $E_{/\mathbb{C}}$) with a quotient of $\mathbb{C}$ by a lattice L. In this way, we can identify $[(E,\omega)_{/\mathbb{C}}]$ with the space of lattices in $\mathbb{C}$. This method is analytic.

We can deduce from the analytic parameterization (combined with geometric technique of Weil–Shimura) many results on the moduli space of elliptic curves, such as the exact field of definition of the moduli, determination of the field of moduli (of each member), and so on (e.g., [IAT] Chap. 6). We have come here in a reverse way: Starting algebraically, mainly by the Riemann–Roch theorem, we have determined a unique Weierstrass equation over A for a given pair $(E,\omega)_{/A}$, and therefore, we know the exact shape of the moduli space before setting out to study the analytic method. After studying analytic theory over $\mathbb{C}$, combining these techniques, we start studying modular forms.

We start with classical homotopy theory for complex manifolds. A *path* γ on a complex manifold M is a piecewise smooth continuous map γ from the closed interval $[0,1]$ into a complex manifold M. We write the path as $(\gamma : x \to y)$ with $\gamma(0) = x$ and $\gamma(y) = 1$. Morally, we start the point x at time 0 and "walking" to reach y by the unit time 1. Two paths $(\alpha : x \to y)$ and $(\beta : x \to y)$ are homotopy equivalent (for which we write $\alpha \approx \beta$) if we have a bicontinuous map $\phi : [0,1] \times [0,1] \to M$ such that $\alpha(t) = \phi(0,t)$ and $\beta(t) = \phi(1,t)$ (i.e., we can fill the area encircled by α and β in M, intuitively). Consider the space $\mathcal{Z} = \mathcal{Z}(M)$ of homotopy classes of paths starting from a fixed point $x \in M$. An open neighborhood U of x is called *simply connected* if we have a bijection: $\mathcal{Z}(U) \cong U$ by projecting $(\gamma : x \to y)$ down to y [i.e., no holes in $\mathcal{Z}(U)$ so no path circling the hole]. Shrinking the neighborhood of x (to avoid holes), we can always find a simply connected open neighborhood of $x \in M$. For example, if U is diffeomorphic to an open disk with center x, it is simply connected (that is, every loop is equivalent to x). If $\gamma : x \to y$ and $\gamma' : y \to z$ are two paths, we define their composed path $\gamma\gamma' : x \to z$ by

$$\gamma\gamma'(t) = \begin{cases} \gamma(2t) & \text{if } 0 \le t \le 1/2 \\ \gamma'(2t-1) & \text{if } 1/2 \le t \le 1. \end{cases}$$

By this composition, $\pi_M = \pi_1^{\mathrm{top}}(M,x) = \{\gamma \in \mathcal{Z}(M) | \gamma : x \to x\}$ becomes a group called *the topological fundamental group* of M. Taking a system of

neighborhoods $\mathcal{U}_y$ of $y \in M$ made of simply connected open neighborhoods of y, we equip a topology with $\mathcal{Z}(M)$ so that a fundamental system of neighborhoods of $\gamma : x \to y$ is given by $\{\gamma U | U \in \mathcal{U}_x\}$. Then $\mathcal{Z}(M)$ becomes a complex manifold. Via composition, π_M acts on $\mathcal{Z}(M)$ freely without fixed points. We have a continuous map $\pi : \pi_M \backslash \mathcal{Z}(M) \to M$ given by $\pi(\gamma : x \to y) = y$, which is a local isomorphism, and $\pi : \pi_M \backslash \mathcal{Z}(M) \cong M$ is a homeomorphism. This space $\mathcal{Z}(M)$ is called a *universal covering* space of M.

We apply this general construction to an elliptic curve $(E, \omega)_{/\mathbb{C}}$ defined over $\mathbb{C}$ in the following way. We take as M the following zero set of the equation of E:

$$E(\mathbb{C}) = E(g_2, g_3)(\mathbb{C}) = \{(x{:}y{:}z) \in \mathbf{P}^2(\mathbb{C}) | y^2 z - 4x^3 + g_2 z^2 x + g_3 z^3 = 0\},$$

which is a compact Riemann surface of genus 1. Let $\mathcal{Z} = \mathcal{Z}(E(\mathbb{C}))$ be the set of all equivalence classes of paths emanating from $\mathbf{0}$. Write $\mathit{\Pi} = \pi_1^{\mathrm{top}}(E, \mathbf{0})$. Since $E(\mathbb{C})$ is a commutative group, writing its group multiplication additively, we define the sum $\gamma + \gamma'$ on $\mathcal{Z}$ by, noting that γ and γ' originate at the origin $\mathbf{0}$:

$$(\gamma + \gamma')(t) = \begin{cases} \gamma(2t) & \text{if } 0 \le t \le 1/2 \\ \gamma(1) + \gamma'(2t-1) & \text{if } 1/2 \le t \le 1. \end{cases}$$

Then $(\gamma + \gamma')(1) = \gamma(1) + \gamma'(1)$, and we claim that $\gamma + \gamma' \approx \gamma' + \gamma$. In fact, on the square $[0,1] \times [0,1]$, we consider the path α on the boundary connecting the origin $(0,0)$ and $(1,1)$ passing $(0,1)$, and write β the opposite path from $(0,0)$ to $(1,1)$ passing $(1,0)$. They are obviously homotopy equivalent. Thus, we have a continuous map $\phi : [0,1] \times [0,1] \to [0,1] \times [0,1]$ such that $\phi(0,t) = \alpha(t)$ and $\phi(1,t) = \beta(t)$. Define

$$f : [0,1] \times [0,1] \to E(\mathbb{C}) \text{ by } f(t,t') = \gamma(t) + \gamma'(t').$$

Then it is easy to see that $f \circ \phi(0,t) = (\gamma' + \gamma)(t)$ and $f \circ \phi(1,t) = (\gamma + \gamma')(t)$.

Via the addition induced from the group structure of $E(\mathbb{C})$ as above, $\mathcal{Z}$ becomes an additive complex Lie group. Since $\gamma + \gamma' = \gamma\gamma'$ if $\gamma \in \mathit{\Pi}$ and $\gamma' \in \mathcal{Z}$ by definition, $\mathit{\Pi}$ is an additive subgroup of $\mathcal{Z}$ and $\mathit{\Pi} \backslash \mathcal{Z} \cong E(\mathbb{C})$. Here we may regard the left-hand side as the quotient group of $\mathcal{Z}$ by the subgroup $\mathit{\Pi}$.

We claim to have an isomorphism $\mathcal{Z} \cong \mathbb{C}$ as additive Lie groups. Choose a nowhere vanishing differential form ω on E, and define a map $I : \mathcal{Z} \to \mathbb{C}$ by $\gamma \mapsto \int_\gamma \omega \in \mathbb{C}$. Since ω is holomorphic on $\mathcal{Z}$, the value of I is independent of the representative γ in the homotopy class $[\gamma]$ by Cauchy's integration theorem. Since ω is translation invariant on $E(\mathbb{C})$, it is translation invariant on $\mathcal{Z}$ and $I(\gamma + \gamma') = I(\gamma) + I(\gamma')$. In particular, I is a local homeomorphism because $E(\mathbb{C})$ is one-dimensional and for simply connected U, $\mathcal{Z}(U) \cong I(U)$. Thus, the pair $(E(\mathbb{C}), \omega)$ is isomorphic locally to the pair of the additive group $\mathbb{C}$ and du for the coordinate u on $\mathbb{C}$, because du is the unique translation-invariant differential (up to constant multiple). Since $I^{-1}([\mathbf{0}]) = \{\mathbf{0}\}$, I is a linear

isomorphism into $\mathbb{C}$. For an open neighborhood U of $\mathbf{0}$ with $U \cong \mathcal{Z}(U) \ni \gamma \mapsto I(\gamma) = \int_\gamma \omega \in \mathbb{C}$ giving an isomorphism onto a small open disk D in $\mathbb{C}$ centered at 0, we have two $\gamma_1, \gamma_2 \in U$ giving rise to two linearly independent $I(\gamma_j)$ $(j = 1, 2)$. Then $I(m\gamma_1 + n\gamma_2) = mI(\gamma_1) + nI(\gamma_2)$ for all $m, n \in \mathbb{Z}$. Replacing γ_j by $\frac{1}{a}\gamma_j \in \mathcal{Z}(U)$ such that $I(\frac{1}{a}\gamma_j) = \frac{I(\gamma_j)}{a}$ for any positive integer a, by the same argument, we find $I(m\gamma_1 + n\gamma_2) = mI(\gamma_1) + nI(\gamma_2)$ for all $m, n \in \mathbb{Q}$; hence, I is a surjective isomorphism.

In the same way, if $\alpha : E \to E$ is an endomorphism of E with $\alpha(\mathbf{0}_E) = \mathbf{0}_E$, α lifts an endomorphism of $\mathcal{Z}$, sending a path γ from $\mathbf{0}_E$ to $z \in \mathbb{C}$ to a path $\alpha(\gamma)$ from $\alpha(\mathbf{0}_E) = \mathbf{0}_E$ to $\alpha(z)$. In particular, $\alpha(\gamma + \gamma') = \alpha(\gamma) + \alpha(\gamma')$. Thus, α gives rise to a linear map from $\mathbb{C} = \mathcal{Z}$ to $\mathbb{C}$. Since α is holomorphic (as it is a polynomial map of the coordinates of $\mathbf{P}^2_{/\mathbb{C}}$), α is a $\mathbb{C}$-linear map. We thus get a natural inclusion:

$$\mathrm{End}(E_{/\mathbb{C}}) \hookrightarrow \mathbb{C}. \tag{2.3.1}$$

Writing $L = L_E$ for $I(\Pi)$, we can find a base w_1, w_2 of L over $\mathbb{Z}$. Thus, we have a map

$$\wp(\mathbb{C}) \ni (E, \omega) \longmapsto L_E \in \{L | L : \text{lattice in } \mathbb{C}\} =: Lat,$$

and we have $(E(\mathbb{C}), \omega) \cong (\mathbb{C}/L_E, du)$. Therefore, the map $\wp(\mathbb{C}) \to Lat$ is injective. We show its surjectivity in the next subsection.

By the above fact combined with (2.3.1), we get the following:

Proposition 2.50 *We have a ring embedding*

$$\mathrm{End}(E_{/\mathbb{C}}) \hookrightarrow \{u \in \mathbb{C} | u \cdot L_E \subset L_E\},$$

and hence $\mathrm{End}(E_{/\mathbb{C}})$ *is either* $\mathbb{Z}$ *or an order of an imaginary quadratic field.*

Proof. The first assertion follows from (2.3.1). Pick $\alpha \in \mathrm{End}(E_{/\mathbb{C}})$ corresponding to $u \in \mathbb{C}$ as above. Note that $L_E = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Then $uw_1 = aw_1 + bw_2$ and $uw_2 = cw_1 + dw_2$ for integers a, b, c, d. In short, writing $w = \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right)$ and $\rho(\alpha) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we get $uw = \rho(\alpha)w$; hence, $\rho : \mathrm{End}(E_{/\mathbb{C}}) \to M_2(\mathbb{Z})$ is a ring homomorphism. By the first assertion, the image has to be an order of imaginary quadratic field or just $\mathbb{Z}$.

When $\mathrm{End}(E_{/\mathbb{C}}) \neq \mathbb{Z}$, E is said to have *complex multiplication*. We also simply call E a *CM elliptic curve* if it has complex multiplication.

2.3.4 Weierstrass $\wp$-Function

For a given $L \in Lat$, Weierstrass defined his $\wp$-functions by

$$x_L(u) = \wp(u) = \frac{1}{u^2} + \sum_{\ell \in L - \{0\}} \left\{ \frac{1}{(u-\ell)^2} - \frac{1}{\ell^2} \right\} = \frac{1}{u^2} + \frac{g_2}{20}u^2 + \frac{g_3}{28}u^4 + \cdots$$

$$y_L(u) = \wp'(u) = \frac{\partial \wp}{\partial u}(u) = -\frac{2}{u^3} - 2 \sum_{\ell \in L - \{0\}} \frac{1}{(u-\ell)^3} = -2u^{-3} + \cdots,$$

where

$$g_2 = g_2(L) = 60 \sum_{\ell \in L - \{0\}} \frac{1}{\ell^4} \quad \text{and} \quad g_3 = g_3(L) = 140 \sum_{\ell \in L - \{0\}} \frac{1}{\ell^6}.$$

Equating poles, $\varphi = y_L^2 - 4x_L^3 + g_2 x_L + g_3$ is holomorphic everywhere. Since these functions factor through the compact space $\mathbb{C}/L$, φ is bounded and hence must be a constant. Since the constant terms of x_L and y_L both vanish, we conclude $\varphi = 0$. We obtain a holomorphic map $(x_L, y_L) : \mathbb{C}/L - \{0\} \to \mathbf{A}^2_{/\mathbb{C}}$. Counting the order of poles at $\mathbf{0}$, we check that the map (x_L, y_L) has degree 1, that is, an isomorphism onto its image and extends to

$$\Phi = (x_L{:}y_L{:}1) = (u^3 x_L{:}u^3 y_L{:}u^3) : \mathbb{C}/L \to \mathbf{P}^2_{/\mathbb{C}}.$$

Thus, we rediscover the elliptic curve $E_L = E(L) = \Phi(\mathbb{C}/L) = E(g_2(L), g_3(L))$ and the induced differential

$$\omega_L = \frac{dx_L}{y_L} = du.$$

This shows

Theorem 2.51 (Weierstrass) *We have* $\wp(\mathbb{C}) = [(E, \omega)_{/\mathbb{C}}] \cong Lat$.

We now relate the space Lat with the upper half-complex plane $\mathfrak{H}$. Two complex numbers $w_1, w_2 \in (\mathbb{C}^\times)^2$ span a lattice if and only if $\mathrm{Im}(w_1/w_2) \neq 0$. Recall that $\mathfrak{H} = \{z \in \mathbb{C} | \, \mathrm{Im}(z) > 0\}$. By changing the order of w_1 and w_2 without affecting their lattice, we may assume that $\mathrm{Im}(w_1/w_2) > 0$. Thus, we have a natural isomorphism of complex manifolds:

$$\mathcal{B} = \left\{ v = \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right) \in (\mathbb{C}^\times)^2 \,\middle|\, \mathrm{Im}(w_1/w_2) > 0 \right\} \cong \mathbb{C}^\times \times \mathfrak{H}$$

via $\left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right) \mapsto (w_2, w_1/w_2)$.

Two vectors v and v' span the same lattice L if and only if $v' = \alpha v$ for $\alpha \in SL_2(\mathbb{Z})$; hence,

$$Lat \cong SL_2(\mathbb{Z}) \backslash \mathcal{B}.$$

This action of $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ on $\mathcal{B}$ can be interpreted on $\mathbb{C}^\times \times \mathfrak{H}$ as follows:

$$\alpha(u, z) = (cu + d, \alpha(z)) \quad \text{for} \quad \alpha(z) = \frac{az + b}{cz + d}.$$

Exercise 2.52 *Check that the above action is well defined; that is, show that* $(\alpha\beta)(u, z) = \alpha(\beta(u, z))$ *for* $\alpha, \beta \in SL_2(\mathbb{Z})$.

2.3.5 Holomorphic Modular Forms

Since a geometric modular form $f \in G_w(\mathbb{C})$ is a function of $(E,\omega)_{/\mathbb{C}}$, it induces a function of $v \in \mathcal{B}$. Writing $L(v) = L(w_1, w_2)$ for the lattice spanned by $v \in \mathcal{B}$, therefore, we regard f as a holomorphic function on $\mathcal{B}$ by $f(v) = f(E_{L(v)}, \omega_{L(v)})$. Then conditions (G0–3) can be stated as

$$\begin{aligned}
&\text{(G0)} && f \in \mathbb{C}[g_2(v), g_3(v)];\\
&\text{(G1)} && f(\alpha v) = f(v) \text{ for all } \alpha \in SL_2(\mathbb{Z});\\
&\text{(G2)} && f \in \mathbb{C}[g_2(v), g_3(v), \Delta(v)^{-1}];\\
&\text{(G3)} && f(\lambda v) = \lambda^{-w} f(v)\ (\lambda \in \mathbb{C}^\times).
\end{aligned}$$

We may also think of $f \in G_w(\mathbb{C})$ as a function on $\mathfrak{H}$ by $f(z) = f(v(z))$ for $v(z) = 2\pi i \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$ $(z \in \mathfrak{H})$. Recall that multiplying $\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$ by $2\pi i$ is to adjust the rationality coming from q-expansion to the rationality coming from the universal ring $\mathbb{Z}[\frac{1}{6}][g_2, g_3]$. Indeed, we will see below that $(2\pi i^{-2j} g_j)(\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right))$ has Fourier expansion in $\mathbb{Q}[[q]]$ for $q = \exp(2\pi i z)$. Then we have the following interpretation:

$$\begin{aligned}
&\text{(G0)} && f \in \mathbb{C}[g_2(z), g_3(z)];\\
&\text{(G1,3)} && f(\alpha(z)) = f(z)(cz+d)^w \text{ for all } \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z});\\
&\text{(G2)} && f \in \mathbb{C}[g_2(z), g_3(z), \Delta(z)^{-1}].
\end{aligned}$$

Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)(z) = z+1$, any $f \in \mathbb{C}[g_2(z), g_3(z), \Delta^{-1}(z)]$ satisfies $f(z+1) = f(z)$. Defining $\mathbf{e}(z) = \exp(2\pi i z)$ for $i = \sqrt{-1}$, the function $\mathbf{e} : \mathbb{C} \to \mathbb{C}^\times$ induces an analytic isomorphism: $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^\times$. Let $q = \mathbf{e}(z)$ be the variable on $\mathbb{C}^\times$. Since f is translation invariant, f can be considered as a function of q. Thus, it has a Laurent expansion $f(q) = \sum_{n \gg -\infty} a(n,f) q^n$. We have the following examples (see (1.3.1), the following section, and [LFE] Chap. 5):

$$\begin{aligned}
12g_2 &= 1 + 240 \sum_{n=1}^{\infty} \left\{ \sum_{0<d|n} d^3 \right\} q^n \in \mathbb{Z}[[q]]^\times,\\
-6^3 g_3 &= 1 - 504 \sum_{n=1}^{\infty} \left\{ \sum_{0<d|n} d^5 \right\} q^n \in \mathbb{Z}[[q]]^\times,\\
\Delta &= q \prod_{n=1}^{\infty} (1-q^n)^{24} \in q(\mathbb{Z}[[q]]^\times).
\end{aligned} \tag{2.3.2}$$

The last expansion of Ramanujan's function tells us that Δ does not vanish on $\mathfrak{H}$ analytically although this is geometrically clear, as $\Delta(E,\omega) \neq 0$ for any elliptic curve (see [EEK] for a concise proof of the product expansion). In particular, we have

$$J = \frac{(12g_2)^3}{\Delta} = q^{-1} + \cdots \in q^{-1}(1 + \mathbb{Z}[[q]]).$$

By this adjustment (multiplying $2\pi i$), we regard g_2 and g_3 as elements of $\mathbb{Z}[\frac{1}{6}][[q]]$, and we consider the Weierstrass equation as a power series identity with coefficients in $\mathbb{Z}[\frac{1}{6}]$; namely, consider a projective plane curve $E_{\infty/\mathbb{Z}[[q]]}$ (called the Tate curve) defined over the power series ring $\mathbb{Z}[[q]]$ by the equation

$$Y^2Z = 4X^3 - g_2(q)XZ^2 - g_3(q)Z^3$$

and define $\omega_\infty = \frac{dX}{Y}$. Since Δ is a unit in $\mathbb{Z}[\frac{1}{6}]((q)) := \mathbb{Z}[\frac{1}{6}][[q]][\frac{1}{q}]$, we see that $(E_\infty, \omega_\infty)$ gives an elliptic curve over the Laurent series ring $\mathbb{Z}[1/6]((q))$ with nowhere vanishing differential ω_∞. For any $f \in G_w(A)$,

$$f(q) = f((E_\infty, \omega_\infty) \otimes_{\mathbb{Z}[\frac{1}{6}]((q))} A((q))) \in A[[q]]$$

is called the *q-expansion* of f. If $f \in G_w(\mathbb{C})$, the q-expansion $f(q)$ coincides with the analytic Fourier expansion via $q = \mathbf{e}(z)$, because by Theorem 2.48, f is an isobaric polynomial $\Phi(g_2, g_3)$ in g_2 and g_3 and by definition $g_2(q)$ and $g_3(q)$ are their analytic expansions.

Write $\mathbf{P}^1(J)_{/\mathbb{Z}[\frac{1}{6}]}$ for the projective line over $\mathbb{Z}[\frac{1}{6}]$ whose coordinate is given by J [in other words, $\mathbf{P}^1(J) = D_0 \cup D_1$ over local rings with $D_1 = \mathbf{A}^1$ defined by the affine ring $\mathbb{Z}[\frac{1}{6}][J]$. Since the coordinate at ∞ of $\mathbf{P}^1(J)$ can be given by J^{-1} ($J^{-1} \in q(1 + q\mathbb{Z}[[q]])$), we know that $\mathbb{Z}[[q]] = \mathbb{Z}[[J^{-1}]]$ and

$$\widehat{\mathcal{O}}_{\mathbf{P}^1(J),\infty} \cong \mathbb{Z}[1/6][[q]] \text{ via } q\text{-expansion}, \tag{2.3.3}$$

where $\widehat{\mathcal{O}}_{\mathbf{P}^1(J),\infty}$ is the (q)-adic completion of the local ring $\mathcal{O}_{\mathbf{P}^1(J),\infty}$ at ∞.

We note that

$$Lat/\mathbb{C}^\times = SL_2(\mathbb{Z})\backslash(\mathfrak{H} \times \mathbb{C}^\times)/\mathbb{C}^\times \cong SL_2(\mathbb{Z})\backslash\mathfrak{H},$$

which is isomorphic to $\mathbf{P}^1(J) - \{\infty\}$ by J. Thus, we see that (G0) over $\mathbb{C}$ is equivalent to

(G0′) f is a holomorphic function on $\mathfrak{H}$ satisfying the automorphic property (G1,3), and its analytic q-expansion $f(q)$ is contained in $\mathbb{C}[[q]]$.

More generally, for modular forms $f \in G_w(A)$, we can interpret (G0) as

(G0″) $f : \wp_{/A} \to \mathbf{A}^1_{/A}$ is a morphism of functors satisfying the automorphic property (G3) in Sect. 2.3.2, and its algebraic q-expansion $f(E_\infty, \omega_\infty)$ is contained in $A[[q]]$.

2.4 p-Adic Uniformization

We recall Tate's theory of p-adic uniformization of elliptic curves, following Tate's paper [T3] (dating back to 1959). The uniformization has been generalized to higher-dimensional abelian varieties by Mumford and Faltings–Chai [DAV] Chaps. II, III, which is the base of the theory of smooth toroidal compactification of Shimura varieties.

2.4.1 Explicit q-Expansion

As we learned from Weierstrass, every elliptic curve over $\mathbb{C}$ is isomorphic to E with $E(\mathbb{C}) = \mathbb{C}/L$ for a lattice $L = \mathbb{Z}(2\pi i) + \mathbb{Z}\log q$ for an element $q \in \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C})$ with $|q| < 1$. The covering map $\mathbb{C} \to E(\mathbb{C})$ factors through $\exp : \mathbb{C} \to \mathbb{C}^\times$ given by $\exp(x) = e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. Thus, $E(\mathbb{C}) = \mathbb{C}^\times/q^{\mathbb{Z}}$, where $q^{\mathbb{Z}} = \{q^m | m \in \mathbb{Z}\}$, which is a discrete subgroup of $\mathbb{C}^\times$. We see from the definition of Weierstrass functions in Sect. 2.3.4 that

$$\begin{aligned} g_2(L) &= \frac{1}{12} + 20\sum_{n=1}^{\infty}\left\{\sum_{0<d|n} d^3\right\} q^n = \frac{1}{12} + 20\sum_{n=1}^{\infty}\frac{n^3 q^n}{1-q^n}, \\ g_3(L) &= -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^{\infty}\left\{\sum_{0<d|n} d^5\right\} q^n = -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^{\infty}\frac{n^5 q^n}{1-q^n}, \\ \Delta(L) &= q\prod_{n=1}^{\infty}(1-q^n)^{24}, \\ J(L) &= q^{-1} + j'(q) \quad \text{with } j'(q) \in \mathbb{Z}[[q]]. \end{aligned} \tag{2.4.1}$$

These formulas follow from (1.3.1).

Setting $w = \exp(u) = e^u$ ($u = \log w$), we compute the (q, w)-expansion of $\wp_L(u)$: By (1.3.3), for w with $|q| < |w| < |q|^{-1}$, we obtain

$$\begin{aligned} \wp_L(u) &= \frac{1}{u^2} + \sum_{m=-\infty,\ m\neq 0}^{\infty}\left\{\frac{1}{(u+2\pi i m)^2} - \frac{1}{(2\pi i m)^2}\right\} \\ &\quad + \sum_{n=1}^{\infty}\left\{\sum_{m=-\infty}^{\infty}\frac{1}{(-u+2\pi i m + n\log q)^2} - \frac{1}{(2\pi i m + n\log q)^2}\right\} \\ &\quad + \sum_{n=1}^{\infty}\left\{\frac{1}{(u+2\pi i m + n\log q)^2} - \frac{1}{(2\pi i m + n\log q)^2}\right\} \\ &= \sum_{m=1}^{\infty} m w^m - \frac{2\zeta(2)}{(2\pi i)^2} + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\left\{m w^{-m} q^{mn} + m w^m q^{mn} - 2q^{mn}\right\}. \end{aligned}$$

Applying $\frac{d}{dw}$ to $\frac{1}{1-w} = \sum_{m=0}^{\infty} w^m$, we get

$$\frac{w}{(1-w)^2} = \sum_{m=1}^{\infty} m w^m.$$

Then, from the fact $\zeta(2) = \frac{\pi^2}{6}$ (see [LFE] Sect. 2.1), we see

$$x_L(u) = \wp_L(u) = t_L(w) + \frac{1}{12}, \tag{2.4.2}$$

where

$$t(q,w) = t_L(w) = \sum_{m=-\infty}^{\infty} \frac{q^m w}{(1-q^m w)^2} - 2\sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2}. \tag{2.4.3}$$

The same formula written in a slightly different way is

$$t(q,w) = \frac{w}{(1-w)^2} + \sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}(w^n + w^{-n} - 2).$$

This new formula confirms $t(q,w) \in \mathbb{Z}[w, w^{-1}, (1-w)^{-1}][[q]]$. Let $A_w = \mathbb{Z}[w, w^{-1}, (1-w)^{-1}]$ as a localized polynomial ring, which is plainly a finitely generated $\mathbb{Z}$-algebra. Thus, we have $t(q,w) \in A_w[[q]]$.

Again applying $w\frac{d}{dw} = \frac{d}{du}$ to x_L, we get

$$y_L(u) = \wp'(u) = t_L(w) + 2s_L(w), \tag{2.4.4}$$

where

$$s(q,w) = s_L(w) = \sum_{m=-\infty}^{\infty} \frac{(q^m w)^2}{(1-q^m w)^3} + \sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2}. \tag{2.4.5}$$

From the identity: $y_L^2 = 4x_L^3 - g_2(L)x_L - g_3(L)$, we get

$$s^2(q,w) + t(q,w)s(q,w) = t(q,w)^3 - b_2(q)t(q,w) - b_3(q), \tag{2.4.6}$$

where

$$b_2(q) = b_2(L) = \frac{1}{4}\left(g_2 - \frac{1}{12}\right) = 5\sum_{n=1}^{\infty} \frac{n^3 q}{1-q^n} \in q\mathbb{Z}[[q]]$$

$$b_3(q) = b_3(L) = \frac{1}{4}\left(g_3 + \frac{g_2}{12} - \frac{1}{432}\right) = \sum_{n=1}^{\infty}\left(\frac{7n^5 + 5n^3}{12}\right)\frac{q^n}{1-q^n} \in q\mathbb{Z}[[q]].$$

Note here that the identity is the algebraic identity in the power series ring $A_w[[q]]$, because the identity is valid over the open set $|q| < |w| < |q|^{-1}$ in $\mathbb{C}^2$. We recall the following identity in $A_w[[q]]$:

$$\begin{aligned}\Delta = g_2^3 - 27g_3^2 &= \left(4b_2 + \frac{1}{12}\right)^3 - 27\left(4b_3 - \frac{b_2}{3} - \frac{1}{216}\right)^2 \\ &= b_3 + b_2^2 + 72b_2b_3 - 432b_3^2 + 64b_2^3 = q\prod_{n=1}^{\infty}(1-q^n)^{24}.\end{aligned} \tag{2.4.7}$$

Since $w \mapsto (t(q,w), s(q,w))$ factors through $\mathbb{C}^\times/q^{\mathbb{Z}}$, we have

$$t(q,qw) = t(q,w) \quad \text{and} \quad s(q,qw) = s(q,w) \quad \text{in } A_w[[q]]. \tag{2.4.8}$$

We check the following identity by power series computation:

$$s(q, w^{-1}) + s(q, w) = -t(q, w) \quad \text{in } A_w[[q]]. \tag{2.4.9}$$

The canonical differential on $E(\mathbb{C})$ is given by

$$\frac{dw}{w} = du = \frac{dx}{\frac{dx}{du}} = \frac{dx}{y}.$$

Exercise 2.53 *1. Show that the projective plane curve C over a field k defined by $X^3 - XYZ - Y^2Z = 0$ is singular at (0:0:1), which is an ordinary double point.*

2. Show the function field of the curve C for $k = \mathbb{F}_p$ as above is isomorphic to $\mathbb{F}_p(w)$ with $x = \frac{X}{Z} = \frac{w}{(1-w)^2}$ and $y = \frac{Y}{Z} = \frac{w^2}{(1-w)^3}$.

2.4.2 Tate Curves

By the computation we have done in the previous section, the projective plane curve E_∞ is defined over $\mathbb{Z}[[q]]$ by the following new equation in $\mathbf{P}^2_{/\mathbb{Z}[[q]]}$ with homogeneous coordinate $(S{:}T{:}U)$:

$$S^2U + TSU - T^3 + b_2(q)TU^2 + b_3(q)U^3 = 0.$$

An important point is that the curve originally defined over $\mathbb{Z}[\frac{1}{6}][[q]]$ is extended to over $\mathbb{Z}[[q]]$. It has an integral point $\mathbf{0}$ given by $(S, T, U) = (1, 0, 0)$. More generally, we can think of a surjective homomorphism:

$$\mathbb{Z}[[q]][S, T, U]/(S^2U + TSU - T^3 + b_2(q)TU^2 + b_3(q)U^3) \to \mathbb{Z}[[q]][S]$$

taking (S, T, U) to $(S, 0, 0)$. To compute the tangent space at $\mathbf{0}$, we use the affine equation of $u = U/S$ and $t = T/S$ given by $u + tu = t^3 - b_2u^2t - b_3u^3$, and we have

$$\Omega_{\widehat{\mathcal{O}}_{E_\infty,\mathbf{0}}/\mathbb{Z}[[q]]} = \mathbb{Z}[[q, t]]dt.$$

This shows that $\widehat{\mathcal{O}}_{E_\infty,\mathbf{0}} = \mathbb{Z}[[q, u]]$ and $\mathbf{0}$ is a **smooth** point of E_∞.

Since $q|\Delta$ in $\mathbb{Z}[[q]]$ (and $\Delta/q \in \mathbb{Z}[[q]]^\times$), after inverting q, that is, over $\mathbb{Z}[[q]][q^{-1}]] = \mathbb{Z}((q))$, the curve $E_{\infty/\mathbb{Z}((q))}$ is an elliptic curve with an invariant differential $\omega_\infty = \frac{dx}{y} = \frac{dt}{t+2s} = \frac{dw}{w}$. The curve E_∞ over $\mathbb{Z}[[q]]$ (without inverting q) has one singular point, that is, $E_\infty \mod q$ is singular only at P with coordinate $(s, t) = (0, 0)$ (which is not the origin of $\overline{E}_\infty = E_\infty \mod q$), and the (completed) stalk $\widehat{\mathcal{O}}_{E_\infty,P}$ is isomorphic to $\mathbb{Z}[[q]][[t, s]]/(ts - q)$, which is a regular ring (cf. [CRT] Sect. 19). Thus, the local ring at every geometric point of $E_{\infty/\mathbb{Z}}$ is a regular ring of relative dimension 1 over $\mathbb{Z}[[q]]$ (we call such a curve a regular curve). The smooth locus of $\overline{E}_\infty$ is isomorphic to $\mathbf{P}^1$ removed two points, say 0 and ∞, which is $\mathbb{G}_m$ (here we may think $\mathbb{G}_m$ as a covariant functor sending a ring A to its multiplicative group $A^\times$). The description of

the singularity of $(E_\infty \mod q) = E_\infty \otimes_{\mathbb{Z}[[q]]} \mathbb{Z}[[q]]/(q)$ as above is clear from the equation of $\overline{E}_\infty$: $s^2 + st = t^3$, because $b_2(q) \equiv b_3(q) \equiv 0 \mod q$. Thus, $\overline{E}_{\infty/\mathbb{Z}}$ is a projective regular plane curve with a nowhere vanishing differential ω_∞.

Let K be a complete field with discrete valuation $|\ | = |\ |_K$ (for example, the p-adic field $\mathbb{Q}_p$ and its field extensions finite degree). Write A for the valuation ring of K. We pick $q_E \in K^\times$ with $|q_E| < 1$. The specialization of E_∞ under the algebra homomorphism $q \mapsto q_E$ gives rise to an elliptic curve $E_K = E_\infty \otimes_{\mathbb{Z}[[q]]} K$ defined over K. Let $P, Q, R \in E_K(K)$. By Abel's theorem (Theorem 2.32), we have

$$P + Q + R = \mathbf{0} \iff [P] + [Q] + [R] \sim 3[\mathbf{0}],$$

where "$\sim$" indicates the linear equivalence.

We explore the addition formula in terms of the coordinates s and t in order to understand well the group structure of $E(K)$. In other words, we want to express explicitly the coordinates of the sum $P+Q$ in terms of the coordinates of each P and Q. By the equation defining E_K, we get $3[\mathbf{0}] = E_K \cap L_\infty$ (see Example 2.18), where $L_\infty = \{U = 0\} \subset \mathbf{P}^2$ is the line at infinity. Since any two lines in $\mathbf{P}^2$ are linearly equivalent (that is, $L_\infty - L$ is the divisor of the function U/ϕ_L for the linear form ϕ_L defining L),

$$P + Q + R = \mathbf{0} \iff [P] + [Q] + [R] = L \cap E_K$$

for the line $L \subset \mathbf{P}^2$ passing through two of the three points P, Q, R, because if P and Q are on L (P and Q determine L), we find the third point $R \in L \cap E_K$ by the Bézout theorem. Here the line L is the tangent line at P if $P = Q$.

Write $P = (s, t)$, $Q = (s', t')$, and $R = (s'', t'')$. We suppose that P and Q are different from $\mathbf{0}$; so their coordinates are finite. Suppose that the line L (having P and Q on it) passes through $\mathbf{0}$ (thus, $R = \mathbf{0}$). If a line passes through $\mathbf{0} = (0, 1, 0)$, its equation $\phi(S, T, U) = aT + bS + cU = 0$ ($s = \frac{S}{U}$ and $t = \frac{T}{U}$) satisfies $\phi(1, 0, 0) = b = 0$; hence, L is parallel to the s-axis, and we conclude $t = t'$. Thus, by (2.4.6), assuming $P \neq Q$ (i.e., $s \neq s'$ or equivalently $2P \neq \mathbf{0}$), we have $s^2 + st = s'^2 + s't \iff s + s' = -t$. In short,

$$t = t' \quad \text{and} \quad s + s' = -t \iff P + Q = -R = \mathbf{0}. \tag{2.4.10}$$

If $P + Q \neq \mathbf{0}$, then the equation of L can be written as $s = \mu t + \nu$. Again by (2.4.6), we have

$$\mu = \frac{s - s'}{t - t'} = \frac{t^2 + tt' + t'^2 - b_2 - s'}{s + s' + t} \tag{2.4.11}$$
$$\nu = s - \mu t = s' - \mu t'.$$

Using the above equations, we find the third point in $L \cap E_\infty$. We get

$$t'' = \mu^2 + \mu - t - t' \quad \text{and} \quad s'' = -t'' - \mu t'' - \nu. \tag{2.4.12}$$

Here is a result in [T3] Theorem 1:

Theorem 2.54 (Tate) *Let $A = \varprojlim_m A/q^m A$ be a q-adically complete local $\mathbb{Z}[[q]]$-algebra. Then*

(1) *The map $w \mapsto (s(q,w), t(q,w), 1) \in \mathbf{P}^2(A)$ induces an injective homomorphism of $A^\times$ into $E_A(A)$ for $E_A = E_\infty \otimes_{\mathbb{Z}[[q]]} A$.*
(2) *If A is the integer ring of a local field K [that is, a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((q))$], then π extends to an isomorphism of $K^\times/q^{\mathbb{Z}} \cong E_A(K)$.*

If an elliptic curve E is isomorphic to E_A over $A[\frac{1}{q}]$, we say that E has *split multiplicative reduction* modulo (q).

Proof. We reproduce the proof [T3]) with some modification as in [GME] Sect. 2.5.2. The power series $t(q,w) - \frac{w}{(1-w)^2}$ and $s(q,w) - \frac{w^2}{(1-w)^3}$ are contained in $\mathbb{Z}[w, w^{-1}][[q]]$. Thus, if $w \in A^\times$, the series $((1-w)^3 s(q,w), (1-w)^3 t(q,w))$ converges in A^2 under the q-adic topology; hence, we get a point

$$\pi(w) = ((1-w)^3 s(q,w) : (1-w)^3 t(q,w) : (1-w)^3) \in E_A(A)$$

as long as one of the coordinates is nonzero. Since $(1-w)^3 s(q,w) \equiv w^2 \bmod qA$, we see $(1-w)^3 s(q,w) \in A^\times$ for all $w \in A^\times$. Thus, the map $\pi : A^\times \to E_A(A)$ is well defined. If $\pi(w) = \mathbf{0}_{E_A} = (1{:}0{:}0)$, we have $(1-w)^3 = 0$, and so $w = 1$. Thus, $\pi^{-1}(\mathbf{0}) = \{1\}$.

We do not give a detailed proof of "homomorphy" of π (i.e., π is a group homomorphism) here, but instead we just remark that the assertion (2) implies homomorphy because the addition and the inverse are basically power series identities. More precisely, taking parameters (w, w') on $E_\infty \times E_\infty$, we have a power series $\Phi(W, W') \in \mathbb{Z}[[q]][[W, W']]$ for $W = 1 + w$ and $W' = 1 + w'$ such that if $P \in E_\infty$ has coordinate w and $Q \in E_\infty$ has coordinate w', and then the w-coordinate of $P + Q \in E_\infty$ is given by $\Phi(W, W')$. This fact is valid by (2) after evaluating the variable q of the base ring $\mathbb{Z}[[q]]$ at many different $q_E \in A$, and so it should be valid as a power series identity.

We now prove (2). We first assume that K is of characteristic 0. We can easily check the convergence of

$$\pi(w) = (s(q,w) : t(q,w) : 1) \in \mathbf{P}^2(K) \quad \text{if } |q| < |w| < |q|^{-1}$$

for $q \in K^\times$ with $|q| < 1$. Here $|\cdot|$ is the absolute value of K, and convergence is under the topology of K. We simply put $\pi(w) = \mathbf{0} \in E_A(K)$ if $w \in q^{\mathbb{Z}}$. Thus, $\pi : K^\times/q^{\mathbb{Z}} \to E_A(K)$ is well defined by (2.4.8), and by the first assertion,

$$\pi^{-1}(\mathbf{0}) = q^{\mathbb{Z}}. \tag{2.4.13}$$

We take $u, v, w \in K^\times$ with $w = uv$. Since π depends only on the class modulo $q^{\mathbb{Z}}$ (2.4.8), we may assume $|q| < |u| \le 1$ and $1 \le |v| < |q|^{-1}$. Thus, $|q| < |w| < |q|^{-1}$, and $\pi(u), \pi(v)$ and $\pi(w)$ are well defined [that is, the power series $s(q, ?)$ and $t(q, ?)$ converge at these points]. Since $\pi(1) = \pi(q^0) = \mathbf{0}$ by definition, (2.4.9) and (2.4.10) shows the desired result when $uv = 1$. Thus,

we may assume that $\pi(u) = P$, $\pi(v) = Q$, and $\pi(w) = R$ are all different from $\mathbf{0}$ and that $P \neq Q$. Write $P = (s,t)$, $Q = (s',t')$, and $R = (s'',t'')$. By (2.4.10), (2.4.11), and (2.4.12), $\pi(u) + \pi(v) = \pi(w)$ is equivalent to the following simultaneous identities:

$$\begin{aligned}(t-t')^2t'' &= (s-s')^2 + (s-s')(t-t') - (t-t')^2(t+t'),\\ (t-t')s'' &= -(t-t')(s+t'') + (s-s')(t-t'').\end{aligned} \tag{2.4.14}$$

Assuming $w = uv$, we want to show that this identity (2.4.14) holds for $\pi(u) = P$, $\pi(v) = Q$, and $\pi(w) = R$. Since $w = uv$, (2.4.14) is the identity in

$$\mathbb{Z}[u, u^{-1}, v, v^{-1}, (1-u)^{-1}, (1-v)^{-1}, (1-uv)^{-1}][[q]].$$

Since $\mathbb{Z}[u, u^{-1}, v, v^{-1}, (1-u)^{-1}, (1-v)^{-1}, (1-uv)^{-1}]$ is finitely generated over $\mathbb{Z}$, we can embed this ring into $\mathbb{C}$. Then the identity holds, by extending this embedding to $K \hookrightarrow \mathbb{C}$; consider $E_{\mathbb{C}} = E_K \otimes_K \mathbb{C}$ over $\mathbb{C}$, since the identities (2.4.14) hold for elliptic curves defined over $\mathbb{C}$. We only verified homomorphy assuming $P \neq \pm Q$, but any map between infinite groups satisfying $\pi(uv) = \pi(u) + \pi(v)$ if $\pi(u) \neq \pm\pi(v)$ can be easily verified to be a homomorphism (see the exercise below and [T3] Lemma 1). This shows that $\pi : K^\times/q^{\mathbb{Z}} \to E_K(K)$ is a homomorphism, and so, as remarked already, the assertion (1) also holds for any q-adically complete A. In particular, π is also a homomorphism for local fields of characteristic p. Then the injectivity follows from (2.4.13).

We only give a sketch of a proof of the surjectivity when A is the integer ring of a finite extension $K/\mathbb{Q}_p$. Since a convergent power series gives an open map on a convergent open disk into an open disk under the p-adic topology (cf. [T3] Corollary 1), $\pi(K^\times)$ is an p-adic open subgroup of $E_A(K)$. Since $\mathbf{P}^2(K)$ is a compact p-adic set, $E_A(K)$ is a compact p-adically closed subset of $\mathbf{P}^2(K)$. Since $E_A(K) = \bigcup_{x\in E_A(K)}(x + \pi(K^\times))$, $E_A(K)$ is covered by finitely many open set of the form $x + \pi(K^\times)$. Thus, $\pi(K^\times)$ is a subgroup of $E_A(K)$ of finite index. Thus, $E_A(K)/\pi(K^\times)$ is a finite group. In other words, for any $x \in E_A(K)$, $Nx \in \pi(K^\times)$. Write $\overline{\mathbb{Q}}_p$ for an algebraic closure of $\mathbb{Q}_p$ containing K. Since $\overline{\mathbb{Q}}_p/q^{\mathbb{Z}}$ is divisible and all torsion points of E_A are contained in $\pi(\overline{\mathbb{Q}}_p^\times)$, we find that $Nx \in \pi(K^\times)$ implies $x \in \pi(\overline{\mathbb{Q}}_p^\times)$. Thus, $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}} \cong E_A(\overline{\mathbb{Q}}_p)$. By definition, $\pi(w^\sigma) = \pi(w)^\sigma$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$. If $\pi(w)^\sigma = \pi(w)$, we have $w^\sigma = q^m w$. Since $|q| < 1$ and $|w| = |w^\sigma|$, we find $w^\sigma = w$. Take $\mathfrak{G} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ invariants of the exact sequence: $1 \to q^{\mathbb{Z}} \to \overline{\mathbb{Q}}_p^\times \to \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}} \to 1$. Note that $H^1(\mathfrak{G}, q^{\mathbb{Z}}) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathfrak{G}, \mathbb{Z}) = 0$ (as $\mathbb{Z}$ does not have nontrivial compact subgroups). Thus, we have $H^0(\mathfrak{G}, \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}) = K^\times/q^{\mathbb{Z}}$ and $H^0(\mathfrak{G}, E(\overline{\mathbb{Q}}_p)) = E_A(K)$ by definition. From $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}} \cong E_A(\overline{\mathbb{Q}}_p)$, via a long exact sequence of the continuous cohomology, we get $K^\times/q^{\mathbb{Z}} \cong E_A(K)$ as desired.

Exercise 2.55 *Let $(G,\cdot)$ and $(H,+)$ be infinite abelian groups and let $\pi : G \to H$ be a map with infinite image sending the identity to the identity such that $\pi(v\cdot w) = \pi(v)+\pi(w)$ as long as $\pi(v) \neq \pm\pi(w)$. Show that π is a homomorphism.*

Corollary 2.56 *Let W be a complete discrete valuation ring finite flat over $\mathbb{Z}_p$ inside $\overline{\mathbb{Q}}_p$ and put K for its field of fractions. Let $q \in W$ with $|q|_p < 1$ and E_q be the elliptic curve over W with Tate period q. Then, for a prime l, we have $E[l^n] \cong \mu_{l^n} \times \mathbb{Z}/l^n\mathbb{Z}$ by the map sending $\zeta q^{m/l^n} \in E_q[l^n]$ with $\zeta \in \mu_{l^n}(\overline{\mathbb{Q}}_p)$ and $m \in \mathbb{Z}$ to $(\zeta, (m \mod l^n)) \in \mu_{l^n}(\overline{\mathbb{Q}}_p) \times \mathbb{Z}/l^n\mathbb{Z}$. On $T_l E_q = \varprojlim_n E_q[l^n] \cong \mathbb{Z}_l(1) \times \mathbb{Z}_l$, $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ acts by a nonsemisimple representation isomorphic to $\sigma \mapsto \left(\begin{smallmatrix} \mathcal{N}_l & u \\ 0 & 1 \end{smallmatrix}\right)$, where $\mathcal{N}_l$ is the l-adic cyclotomic character such that $\zeta^\sigma = \zeta^{\mathcal{N}_l(\sigma)}$ for $\zeta \in \mu_{l^\infty}(\overline{\mathbb{Q}}_p)$ and $\mathcal{N}_l(\sigma) \in {\mathbb{Z}_l}^\times$ and for a choice of $q^{1/l^n} \in \overline{\mathbb{Q}}_p$ and the primitive l^nth root $\zeta_{l^n} = i_p(i_\infty^{-1}(\mathbf{e}(\frac{1}{l^n}))) \in \mu_{l^n}(\overline{\mathbb{Q}}_p)$, we have $(q^{1/l^n})^\sigma = \zeta_{l^n}^{u(\sigma)} q^{1/q^n}$ (for all n) with $u(\sigma) \in \mathbb{Z}_l$. In particular, the l^n-torsion points of E_q for n sufficiently large generate a nonabelian soluble extension of K.*

Proof. By Theorem 2.54 (2), the field of rationality of $E_q[l^n]$ is the Kummer extension $K[\mu_{l^n}, q^{1/l^n}]$. Then the above form of representation is given by the Galois action on the basis $\{\zeta_{l^n}, q^{1/l^n}\}$ of $E_q[l^n](\overline{\mathbb{Q}}_p)$.

2.5 What We Study in This Book

We learned in this section that the isomorphism classes of (E,ω) over a field are in bijection to rational points of an affine algebraic variety $\mathrm{Spec}(\mathcal{R})$ for $\mathcal{R} = \mathbb{Z}[\frac{1}{6}, X, Y, \frac{1}{X^3-27Y^2}]$. Similarly, the set of isomorphism classes of elliptic curves over an algebraically closed field k is isomorphic to $\mathbf{P}^1(J)(k) - \infty = \mathrm{Spec}(\mathbb{Z}[J])(k) \cong k$. Generalizing this, we may look into the problem classifying pairs $(E,\phi_N)_{/A}$ of an elliptic curve E over a ring A with a level-N-structure for a positive integer N. The level structure ϕ_N can be an embedding of abelian group functors $\phi_N : \mu_N \hookrightarrow E$ defined over the category of A-algebras $ALG_{/A}$. Here we use the group structure of E. We prove later in Chap. 6 that this classification problem gives rise to an affine curve $Y_1(N)_{/\mathbb{Z}[\frac{1}{N}]} = \mathrm{Spec}(\mathcal{R}_0(\Gamma_1(N)))$ defined over the very small ring $\mathbb{Z}[\frac{1}{N}]$. In other words, if $N \geq 4$, the isomorphism classes of $(E,\phi_N)_{/A}$ over an $\mathbb{Z}[\frac{1}{N}]$-algebra A are in bijection with the set $Y_1(N)(A) = \mathrm{Hom}_{\mathrm{alg}}(\mathcal{R}_0(\Gamma_1(N)), A)$ (this is a theorem of Shimura and Igusa; Theorem 6.25). Adding finitely many points (called cusps) to $Y_1(N)$ using the theory of Tate curves, we construct a projective curve $X_1(N)$ canonically containing $Y_1(N)$ as we made $\mathbf{P}^1(J)$ out of $M_1 = \mathbf{P}^1(J) \setminus \{\infty\}$. Since $\phi_N|_{\mu_{N'}}$ for a factor $N'|N$ is a level-N'-structure, we naturally get morphisms $Y_1(N) \to Y_1(N')$ and $X_1(N) \to X_1(N')$. Thus, we get a tower of projective curves $\{X_1(N) \twoheadrightarrow X_1(N')\}_{N'|N}$ indexed by positive integers N under the

(reversed) order given by divisibility $N'|N$. The procurve $\varprojlim_N X_1(N)$ and also the proaffine curve $\varprojlim_N Y_1(N)$ are a quotient of the Shimura curve we study in Chap. 7. We study the arithmetic invariant via the theory of Shimura varieties and Hecke operators acting on it. In the following chapter, we present some of the results of this book without going deep into the proof; thus, even if readers do not fully understand the results, we suggest they try to get an overview of the book (the details will be supplied later, after we've given the basics of scheme theory and the relevant theory of modular forms/elliptic curves/Shimura variety).

http://www.springer.com/978-1-4614-6656-7

Elliptic Curves and Arithmetic Invariants
Hida, H.
2013, XVIII, 450 p., Hardcover
ISBN: 978-1-4614-6656-7