ELLIPTIC CURVES AND MODULAR FORMS

HARUZO HIDA

Contents

In this notes, we hope to go through basics of elliptic curves and modular curves in three steps:

(1) As plane curves over a field (first 3 to 4 weeks);
(2) As scheme/group functor over a ring (next 3 weeks);
(3) Modular forms on modular curves.

Elliptic curves and modular curves are one of the most important objects studied in number theory. As everybody knows, the theory is a base of the proof by Wiles (through Ribet's work) of Fermat's last theorem, it supplies a fast prime factorization algorithm (cf. [REC] IV), and so on.

1. Curves over a field

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

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

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

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

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

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

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

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

Thus we have a bijection

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

The association $V_{\mathfrak{a}} : A \mapsto V_{\mathfrak{a}}(A)$ is a covariant functor from the category of k-algebras to the category of sets (denoted by $SETS$). Indeed, for any k-algebra homomorphism $\sigma : A \to A'$, $V_{\mathfrak{a}}(A) \ni (x, y) \mapsto (\sigma(x), \sigma(y)) \in V_{\mathfrak{a}}(A')$ 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 $\mathfrak{a}$.

Form number theoretic view point, studying $V_\mathfrak{a}(A)$ for a small field (or even a ring, such as $\mathbb{Z}$) is important. Thus it would be better regard $V_\mathfrak{a}$ as a functor in some number theoretic setting.

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

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

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

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

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

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

Indeed,

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

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

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

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

making the following diagram commutative:

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

We write $R_{\mathfrak{a}} = k[X,Y]/\mathfrak{a}$ and call it the affine ring of $V_{\mathfrak{a}}$. Here is a useful (but tautological) lemma which is a special case of Yoneda's lemma (in Math 210 series):

Lemma 1.1. *We have a canonical isomorphism:*

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

The first association is covariant and the second is contravariant.

Here is a sketch of the proof.

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

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

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

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

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

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

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

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

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

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

Example 1.1. Let $\mathfrak{a} = (f)$ for $f(X, Y) = Y^2 - X^3$. Then $\frac{\partial f}{\partial X}(a, b)(X - a) + \frac{\partial f}{\partial Y}(a, b)(Y - b) = -3a^2(X - a) + 2b(Y - b)$ $(b^2 = a^3)$. Thus this curve is singular only at $(0, 0)$.

Example 1.2. Suppose that k has characteristic different from 2. Let $\mathfrak{a} = (Y^2 - g(X))$ for a cubic polynomial $g(X) = X^3 + aX + b$. Then the tangent line at (x_0, y_0) is given by $2y_0(X - x_0) - g'(x_0)(Y - y_0)$. This equation vanishes if $0 = y_0^2 = g(x_0)$ and $g'(x_0) = 0$; so, singular at only $(x_0, 0)$ for a multiple root x_0 of $g(X)$. Thus $V_{\mathfrak{a}}$ is a nonsingular curve if and only if $g(X)$ is separable if and only if its discriminant $4a^3 - 27b^2 \neq 0$.

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

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

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

Lemma 1.4. *The linear vector space $T_P(K)$ is the dual vector space of $P/P^2 = \mathfrak{m}_P/\mathfrak{m}_P^2$.*

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

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

whose kernel is spanned by $f \mod (X-a, Y-b)^2 = \frac{\partial f}{\partial X}(a,b)(X-a) + \frac{\partial f}{\partial Y}(a,b)(Y-b)$
if $\mathfrak{a} = (f)$, since $\phi(X,Y) \equiv \frac{\partial \phi}{\partial X}(a,b)(X-a) + \frac{\partial \phi}{\partial Y}(a,b)(Y-b) \mod (X-a, Y-b)^2$.
Thus the above duality between $\Omega_{(a,b)}$ and $D_{\mathbb{A},(a,b)}$ 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 $\mathcal{O}_{V,P} \to K$. $\qquad \square$

We call T_P the *tangent* space at P and $\Omega_P = \Omega_{V,P}$ the *cotangent* space at P of
V. More generally, a k-derivation $\partial : R_{\mathfrak{a}} \to R_{\mathfrak{a}}$ is a k-linear map satisfying the
Leibniz condition $\partial(\phi\varphi) = \phi\partial(\varphi) + \varphi\partial(\phi)$ and $\partial(k) = 0$. For a k-derivation as above,
$f\partial : \varphi \mapsto f \cdot \partial(\varphi)$ for $f \in R_{\mathfrak{a}}$ is again a k-derivation. The totality of k-derivation
$Der_{V_{\mathfrak{a}}/k}$ is therefore an $R_{\mathfrak{a}}$-module.
First take $\mathfrak{a} = (0)$; so, $V_{\mathfrak{a}} = \mathbb{A}^2$. By the Leibniz relation, $\partial(X^n) = nX^{n-1}\partial X$,
$\partial(Y^m) = mY^{m-1}\partial Y$ and $\partial(X^n Y^m) = nX^{n-1}Y^m\partial X + mX^n Y^{m-1}\partial Y$ for $\partial \in Der_{\mathbb{A}^2/k}$;
so, ∂ is determined by its value $\partial(X)$ and $\partial(Y)$. Note that $(\partial X)\frac{\partial}{\partial X} + (\partial Y)\frac{\partial}{\partial Y}$ in
$Der_{\mathbb{A}^2/k}$ and the original ∂ has the same value at X and Y; so, we have

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

Thus $\left\{\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}\right\}$ gives a basis of $Der_{\mathbb{A}^2/k}$.
Assuming $V_{\mathfrak{a}}$ nonsingular (including $\mathbb{A}^2 = V_{(0)}$), 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 $\Omega_{\mathbb{A}^2/k}$. Then by definition $(dX, \partial) = \partial X$ and $(dY, \partial) = \partial Y$; so, $\{dX, dY\}$ is the dual basis of $\left\{\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}\right\}$. We have $d\Phi = \frac{\partial \Phi}{\partial X}dX + \frac{\partial \Phi}{\partial Y}dY$ as we
can check easily that the left hand side and right hand side as the same value on any
$\partial \in Der_{\mathbb{A}^2/k}$.
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 ∂ factor through the
quotient $k[X,Y]/(f)$, it satisfies $\partial(f(X,Y)) = (df, \partial) = 0$. Thus we have

Lemma 1.5. *We have an inclusion $Der_{V_{\mathfrak{a}}/k} \hookrightarrow (R_{\mathfrak{a}}\frac{\partial}{\partial X} \oplus R_{\mathfrak{a}}\frac{\partial}{\partial Y})$ whose image is given
by $\{\partial \in Der_k(k[X,Y], R_{\mathfrak{a}})|\partial f = 0\}$. This implies $\Omega_{V_{\mathfrak{a}}/k} = (R_{\mathfrak{a}}dX \oplus R_{\mathfrak{a}}dY)/R_{\mathfrak{a}}df$ for
$df = \frac{\partial f}{\partial X}dX + \frac{\partial}{\partial Y}dY$ by duality.*

Remark 1.1. If $V_{\mathfrak{a}}$ is an irreducible curve; so, $R_{\mathfrak{a}}$ is an integral domain, for its quotient
field $k(V_{\mathfrak{a}})$, $k(V_{\mathfrak{a}})\Omega_{V_{\mathfrak{a}}/k} = (k(V_{\mathfrak{a}})dX \oplus k(V_{\mathfrak{a}})dY)/k(V_{\mathfrak{a}})df$ is 1 dimensional, as $df \neq 0$
in $\Omega_{\mathbb{A}^2/k}$. In particular, if we pick $\psi \in R_{\mathfrak{a}}$ with $d\psi \neq 0$ (i.e., a non-constant), any
differential $\omega \in \Omega_{V_{\mathfrak{a}}/k}$ can be uniquely written as $\omega = \phi d\psi$ for $\phi \in k(V_{\mathfrak{a}})$.

Lemma 1.6. *The following four conditions are equivalent:*

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

Proof. Let $K = \overline{k}$. By the above lemma, T_P is a line if and only if $\dim T_P(K) = 1$ if and only if $\dim P/P^2 = 1$. Thus by Nakayama's lemma, P is principal. Any prime ideal of $k[X,Y]$ is either minimal or maximal (i.e, the ring $k[X,Y]$ has Krull dimension 2). Thus any prime ideal of R and $\mathcal{O}_{V,P}$ is maximal. Thus (1) and (2) are equivalent. The equivalence of (2) and (3) follows from general ring theory covered by Math 210 (see [CRT] Theorem 11.2). We leave the equivalence (3) $\Leftrightarrow$ (4) as an exercise. $\qquad\square$

Write x, y for the image of $X, Y \in k[X,Y]$ in $R_{\mathfrak{a}}$. Any $\omega \in \Omega_{V_{\mathfrak{a}}/k}$ can be written as $\phi dx + \varphi dy$. Suppose that $V_{\mathfrak{a}}$ is nonsingular. Since $\mathcal{O}_{V_{\mathfrak{a}},P} \hookrightarrow k[[T]]$ (for $P \in V_{\mathfrak{a}}(k)$) for a local parameter T as above, ϕ, φ, x, y have the "Taylor expansion" as an element of $k[[T]]$, for example, $x(T) = \sum_{n \geq 0} a_n(x)T^n$ with $a_n(x) \in k$. Thus dx, dy also have a well define expansion, say, $dx = d(\sum_{n \geq 0} a_n(x)T^n) = \sum_{n \geq 1} a_n(x)T^{n-1}dT$. Thus we may expand $\omega = \phi dx + \varphi dy = \sum_{n \geq 0} a_n(\omega)T^n dT$ once we choose a parameter T at P. This expansion is unique independent of the expression $\phi dx + \varphi dy$. Indeed, if we allow meromorphic functions Φ as coefficients, as we remarked already, we can uniquely write $\omega = \Phi dx$ and the above expansion coincides with the Taylor expansion of Φdx.

Exercise 1.7. *Let $P \in V_{\mathfrak{a}}(K)$ for a finite field extension K/k, and pull back P to a maximal ideal $(X - a, Y - b) \subset K[X,Y]$. Define $(X - a, Y - b) \cap k[X,Y]$, and project it down to a maximal ideal $p \subset R_{\mathfrak{a}} = k[X,Y]/\mathfrak{a}$. Write $\mathcal{O}_{V_{\mathfrak{A}},p}$ for the localization of $R_{\mathfrak{a}}$ at p. Prove the following facts:*

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

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

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

Corollary 1.8. *Any normal irreducible affine plane curve is smooth everywhere.*

Proof. By ring theory, any localization of a normal domain is normal. Thus $\mathcal{O}_{V,P}$ is a normal domain. By the exercise below, we may assume that $P \cap k[X,Y] \neq (0)$.

Then P is a maximal ideal, and hence $K = k[X,Y]/P$ is an algebraic extension of k. In this case, $\mathcal{O}_{V,P}$ is a normal local domain with principal maximal ideal, which is a discrete valuation ring (cf. [CRT] Theorem 11.1). $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Exercise 1.9.   (1) *Let $P = k[X,Y] \cap (X - a, Y - b)$ for $(a,b) \in V_\mathfrak{a}(\Omega)$, where $(X - a, Y - b)$ is the ideal of $\Omega[X,Y]$. Is it possible to have $P = (0) \subset k[X,Y]$ for a point $(a,b) \in V_\mathfrak{a}(\Omega)$.*
   (2) *If $\mathfrak{a} = (XY)$, is the ring $\mathcal{O}_{V,O}$ for $O = (0,0)$ an integral domain? What is $\dim_k \mathfrak{m}_O/\mathfrak{m}_O^2$?*
   (3) *For all points $P \in V_\mathfrak{a}(\Omega)$ with $R_\mathfrak{a} \cap P = (0)$ (regarding $P = (x - a, y - b)$ as an maximal ideal of $\Omega[X,Y]/\mathfrak{a}\Omega[X,Y]$), prove that V is smooth at P.*
   (4) *If A is a discrete valuation ring containing a field $k \subset A$ which is naturally isomorphic to the residue field of A, prove $\widehat{A} = \varprojlim_n A/\mathfrak{m}_A^n \cong k[[T]]$, where $\mathfrak{m}_A$ is the maximal ideal of A.*

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

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

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

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

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

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

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

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

Lemma 1.10. *Suppose that K is a local ring with maximal ideal $\mathfrak{m}$. Then we have*

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

Moreover, writing $D_i : ALG_{/k} \to SETS$ for the subfunctor $D_i(A) \subset \mathbf{P}^n(A)$ made up of the classes L whose projection to the i-th component $A \subset A^{n+1}$ is surjective, we have $\mathbf{P}^n(K) = \bigcup_i D_i(K)$ and $D_i(A) \cong \mathbb{A}^n$ canonically for all k-algebras A. If A is a

local ring K, $D_i \cong \mathbb{A}^n$ is given by sending $(x_0, \ldots, x_n)$ to $(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}) \in K^n$ removing the i-th coordinate.

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

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

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

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

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

Exercise 1.11. *Is there any example of a point in $X \in \mathbf{P}^1(A)$ (and a ring A) such that the projections to the first and the second coordinate are both not surjective?*

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

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

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

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

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

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

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

Example 1.3. Suppose $\mathfrak{a} = (y^2 - f(x))$ for a cubic $f(x) = x^3 + ax + b$. Then $F(X, Y, Z) = Y^2 Z - X^3 - aXZ^2 - bZ^3$. Since L_∞ is defined by $Z = 0$, we find $L_\infty \cap \overline{V}_\mathfrak{a} = \{(0 : 1 : 0)\}$ made of a single point (with multiplicity 3). This point we call the origin $\mathbf{0}$ of $V_\mathfrak{a}$.

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

Exercise 1.12. *Suppose $\overline{V}_\mathfrak{a}$ is defined by $F(X, Y, Z) = 0$. Let $f(x, y) = F(x, y, 1)$ and $g(y, z) = F(1, y, z)$. Then the projective plane curve $\overline{V}_\mathfrak{a}$ for $\mathfrak{a} = (f(x, y))$ satisfies $\overline{V}_\mathfrak{a} \cap D_0 = V_{(g)}$. Show that $\mathcal{O}_{V_\mathfrak{a}, P} \cong \mathcal{O}_{V_{(g)}, P}$ canonically if $P \in \overline{V}_\mathfrak{a} \cap D_0 \cap D_2$.*

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

Lemma 1.13. *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 on $C \cap D_2$ $f(x, y, 1) = \frac{h(x, y)}{g(x, y)}$. If $m = \deg(h) = \deg(g)$, we just define $H(X, Y, Z) = h(\frac{X}{Z}, \frac{Y}{Z})Z^m$ and $G(X, Y, Z) = g(\frac{X}{Z}, \frac{Y}{Z})Z^m$. If $\deg(h) > \deg(g)$, we define $H(X, Y, Z) = h(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(h)}$ and $G(X, Y, Z) = g(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(h)}$. If $\deg(h) < \deg(g)$, we define $H(X, Y, Z) = h(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(g)}$ and $G(X, Y, Z) = g(\frac{X}{Z}, \frac{Y}{Z})Z^{\deg(g)}$. Multiplying h or g by a power of Z does not change the above identity $f(x, y, 1) = \frac{h(x, y)}{g(x, y)}$, because $Z = 1$ on $C \cap D_2$. Thus by adjusting in this way, we get G and H. $\square$

Example 1.4. Consider the function $\phi = cx + dy$ in $k(C)$ for $C = \overline{V}_\mathfrak{a}$ with $\mathfrak{a} = (y^2 - x^3 - ax - b)$. Then C is defined by $Y^2 Z - X^3 - aXZ^2 - bZ^3 = 0$, and

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

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

Take a projective nonsingular plane k-curve $C_{/k}$. Put $C_i = C \cap D_i$ which is an affine nonsingular plane curve. Then we have well defined global differentials $Der_{C_i/k}$. Since $\partial : Der_{C_i/k}$ induces $\partial_P : \mathcal{O}_{C_i,P} \to K$ for any $P \in C_i(K)$ by $f \mapsto \partial(f)(P)$, we have $\partial_P \in T_P$. If $\partial_i \in Der_{C_i/k}$ given for each $i = 0, 1, 2$ satisfies $\partial_{i,P} = \partial_{j,P}$ for all (i,j) and all $P \in (D_i \cap D_j)(\overline{k})$, we call $\partial = \{\partial_i\}_i$ a global tangent vector defined on C. Plainly the totality $T_{C/k}$ of global tangent vectors are k-vector space. The k-dual of $T_{C/k}$ is called the space of k-differentials over k and written as $\Omega_{C/k}$. It is known that $\Omega_{C/k}$ is finite dimensional over k.

Corollary 1.14. *Suppose that C is non-singular. Each $\phi \in k(C)$ induces $\phi \in \mathrm{Hom}_{proj\ k\text{-}curves}(C, \mathbf{P}^1)$. Indeed, we have $k(C) \sqcup \{\infty\} \cong \mathrm{Hom}_{proj\ k\text{-}curves}(C, \mathbf{P}^1)$, where ∞ stands for the constant function sending all $P \in C(A)$ to the image of $\infty \in \mathbf{P}^1(k)$ in $\mathbf{P}^1(A)$.*

Proof. We prove only the first assertion. Suppose $k = \overline{k}$. Write $\phi(x : y : z) = \frac{h(x,y,z)}{g(x,y,z)}$ as a reduced fraction by the above lemma. For $L \in C(A) \subset \mathbf{P}^2(A)$, we consider the sub A-module $\phi(L)$ of A^2 generated by $\{(h(\ell), g(\ell)) \in A^2 | \ell \in L\}$. We now show that $\phi(L) \in \mathbf{P}^1(A)$; so, we will show that the map $C(A) \ni L \mapsto \phi(L) \in \mathbf{P}^1(A)$ induces the natural transformation of C into $\mathbf{P}^1$. If A is local, by Lemma 1.10, L is generated by (a, b, c) with at least one unit coordinate. Then any $\ell \in L$ is of the form $\lambda(a, b, c)$ and therefore $\phi(\ell) = \lambda^{\deg(h)}\phi(a, b, c)$. Thus $\phi(L) = A \cdot \phi(a, b, c)$. Since A is a k-algebra, k is naturally a subalgebra of the residue field $A/\mathfrak{m}$ of A. Since $\phi(P)$ for all $P \in C(k)$ is either a constant in k or ∞, we may assume that $(h(P), g(P)) \neq (0,0)$ for all $P \in C(k)$. Since $(a, b, c) \not\equiv 0 \mod \mathfrak{m}$ as (a, b, c) generates a direct summand of A^3. Thus $(h(a, b, c), g(a, b, c)) \not\equiv (0, 0) \mod \mathfrak{m}$. After tensoring $A/\mathfrak{m}$ over A, $(A/\mathfrak{m})^2/(\phi(L)/\mathfrak{m}\phi(L))$ is one dimensional. Thus by Nakayama's lemma (e.g., [CRT] Theorem 2.2–3), $A/\phi(L)$ is generated by a single element and has to be a free module of rank 1 as $\phi(L)$ is a free A-module of rank 1. Thus $\phi(L) \in \mathbf{P}^1(A)$. If k is not algebraically closed, replacing A by $\overline{A} = A \otimes_k \overline{k}$, we find $\phi(L) \otimes_k \overline{k} \in \mathbf{P}^2(\overline{k})$ and hence $\phi(L) \otimes_A A/\mathfrak{m} \in \mathbf{P}^2(k)$, which implies $\phi(L) \in \mathbf{P}^2(A)$.

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

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

Exercise 1.15. *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) $\mathrm{Hom}_{proj\ k\text{-}curves}(C, \mathbf{P}^1) \setminus \infty \cong k(C)$.

1.5. **Divisors.** The divisor group $\mathrm{Div}(C)$ of a non-singular projective geometrically irreducible plane curve C is a formal free $\mathbb{Z}$-module generated by points $P \in C(\overline{k})$. When we consider a point P as a divisor, we write it as $[P]$. For each divisor $D = \sum_P m_P[P]$, we define $\deg(D) = \sum_P m_P$. Since C is nonsingular, for any point $P \in$

$C(\overline{k})$, $\mathcal{O}_{C,P}$ is a DVR, and the rational function field $\overline{k}(C)$ is the quotient field of $\mathcal{O}_{C,P}$ (regarding C as defined over $\overline{k}$). Thus if we write the valuation $v_P : \overline{k}(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ for the additive valuation of $\mathcal{O}_{C,P}$, we have a well defined $v_P(f) \in \mathbb{Z}$ for any non-zero rational $\overline{k}$-function $f \in \overline{k}(C)$. Since $\mathfrak{m}_P = (t_P)$ and $t_P^{v_P(f)} \| f$ in $\mathcal{O}_{C,P}$, f has a zero of order $v_p(f)$ at P if $v_P(f) > 0$ and a pole of order $|v_p(f)|$ if $v_P(f) < 0$. In other words, the Taylor expansion of f at P is given by $\sum_n a_n(f)t_P^n$ and $v_p(f) = \min(n : a_n(f) \neq 0)$. For a global doifferential $\omega \in \Omega_{C/\overline{k}}$, we have its Taylor expansion $\sum_n a_n(f)t_P^n dt_P$ at each $P \in C(\overline{k})$; so, we may also define $v_P(\omega) := \min(n : a_n(\omega) \neq 0)$. We extend this definition for meromorphic differentials $k(C) \cdot \Omega_{C/k} = \{f \cdot \omega | f \in k(C), \omega \in \Omega_{C/k}\}$. Here we quote Bézout's theorem:

Theorem 1.16. *Let C and C' be two plane projective k-curves inside $\mathbf{P}^2$ defined by relatively prime homogeneous equations $F(X, Y, Z) = 0$ and $G(X, Y, Z) = 0$ of degree m and n respectively. Then counting with multiplicity, $|C(\overline{k}) \cap C'(\overline{k})| = m \cdot n$.*

If C is smooth at $P \in C \cap C'$ in $C \cap D_2$, $\phi = \frac{G(X,Y,Z)}{Z^n}$ is a function vanishing at P. The multiplicity of P in $C \cap C'$ is just $v_P(\phi)$. More generally, if $P = (a, b)$ is not necessarily a smooth point, writing $C \cap D_2 = V_{\mathfrak{a}}$ and $C' \cap D_2 = V_{\mathfrak{b}}$ for principal ideals $\mathfrak{a}, \mathfrak{b}$ in $\overline{k}[X, Y]$ and regarding P as an ideal $(X - a, Y - b) \subset \overline{k}[X, Y]$, the multiplicity is given by the dimension of the localization $(\overline{k}[x, y]/\mathfrak{a} + \mathfrak{b})_P$ over $\overline{k}$. The same definition works well for any points in $C \cap D_0$ and $C \cap D_1$. One can find the proof of this theorem with (possibly more sophisticated) definition of multiplicity in a text of algebraic geometry (e.g. [ALG] Theorem I.7.7).

Since there are only finitely many poles and zeros of f, we can define the divisors $\operatorname{div}(f) = \sum_{P \in C(k)} v_P(f)[P]$, $\operatorname{div}_0(f) = \sum_{P \in C(k), v_P(f) > 0} v_P(f)[P]$ and $\operatorname{div}_\infty(f) = \sum_{P \in C(k), v_P(f) < 0} v_P(f)[P]$ of f. Similarly, for meromorphic differential ω, we define again $\operatorname{div}(\omega) = \sum_P v_P(\omega)[P]$. By Lemma 1.13, $f(x : y : z) = \frac{h(x:y:z)}{g(x:y:z)}$ for a homogeneous polynomial h, g in $\overline{k}[x, y, z]$ of the same degree. If the degree of equation defining C is m and C' is defined by $h(X, Y, Z) = 0$, $\deg_0(\operatorname{div}(f)) = |C(\overline{k}) \cap C'(\overline{k})| = m \deg(h) = m \deg(g) = \deg_\infty(\operatorname{div}(f))$. This shows $\deg(\operatorname{div}(f)) = 0$ as $\sum_{P, v_P(f) > 0} m_P = m \deg(h)$ and $-\sum_{P, v_P(f) < 0} m_P = m \deg(g)$.

Lemma 1.17. *Let C be a nonsingular projective plane curve. For any $f \in \overline{k}(C)$, $\deg(\operatorname{div}(f)) = 0$, and if $f \in \overline{k}(C)$ is regular at every $P \in C$, f is a constant in $\overline{k}$.*

Lemma 1.18. *If $f \in k(C)$ satisfies $\deg(\operatorname{div}_0(f)) = \deg(\operatorname{div}_\infty(f)) = 1$, $f : C \to \mathbf{P}^1$ induces an isomorphism of projective plane curve over k.*

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

Another proof: By the proof of Corollary 1.14, $\deg(\operatorname{div}_0(f))$ is the number of points over 0 (counting with multiplicity) of the regular map $f : C \to \mathbf{P}^1$. By taking

off a constant $\alpha \in k \subset \mathbf{P}^1$ to f, $\deg(\mathrm{div}_0(f - \alpha)) = 1 = \deg(\mathrm{div}_\infty(f - \alpha))$, and $|f^{-1}(\alpha)| = \deg(\mathrm{div}_0(f - \alpha)) = 1$; so, we find that f is 1-1 onto. Thus f is an isomorphism. $\square$

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 call that D and D' are *algebraically equivalent* if $\deg(D) = \deg(D')$. The quotient groups $J(C) = \mathrm{Div}^0(C)/\{\mathrm{div}(f)|f \in k(C)^\times\}$ and $\mathrm{Pic}(C) = \mathrm{Div}(C)/\{\mathrm{div}(f)|f \in k(C)^\times\}$ are called the jacobian and the Picard group of C, respectively. Sometimes, $J(C)$ is written as $\mathrm{Pic}^0(C)$ (the degree 0 Picard group).

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

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

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

Example 1.5. Let $C = \mathbf{P}^1$. For a positive divisor $D = \sum_{a \in \overline{k}} m_a[a]$ with $m_a \geq 0$ and $m_a > 0$ for some a, regarding $a \in \overline{k}$ as a point $[a] \in \mathbf{P}^1(\overline{k}) = \overline{k} \sqcup \{\infty\}$. On $\mathbb{A}^1(\overline{k}) = \overline{k}$, forgetting about the infinity, $\mathrm{div}(f) + D \geq 0$ if $f = \frac{g(x)}{\prod_a (x-a)^{m_a}}$ for a polynomial $g(x)$. If $\deg(D) \geq \deg(g(x))$, the function f does not have pole at ∞. Thus $L(D) = \{g(x)| \deg(g(x)) \leq \deg(D)\}$ and we have $\ell(D) = 1 + \deg(D)$ if $D > 0$. If C is a plane projective curve, we can write $f = \frac{h(X,Y,Z)}{g(X,Y,Z)}$ as a reduced fraction by Lemma 1.13. Write $D = \sum_P m_P[P]$, and put $|D| = \{P|D = \sum_P m_P[P] \text{ with } m_P \neq 0\}$. If $|D|$ is inside $D_2 \cap C \subset \mathbb{A}^2$ and $D > 0$, we may assume that $V_{(g(X,Y,1))} \cap C$ contains $|D|$. Then not to have pole at $C \setminus D_2$, $\deg(h)$ has to be bounded; so, $\ell(D) < \infty$. Since $L(D) \subset L(D_+)$ in general, writing $D = D_+ + D_-$ so that $D_+ \geq 0$ and $-D_- \geq 0$, this shows $\ell(D) < \infty$.

Exercise 1.19. *Give the details of the proof of $\ell(D) < \infty$.*

Theorem 1.20 (Riemann-Roch). *Let $C = \overline{V}_\mathfrak{a}$ be a non-singular projective curve defined over a field k. Then for $g = \dim_{\overline{k}} \Omega_{C/k}$ and a divisor K of degree $2g - 2$ of the form $\mathrm{div}(\omega)$ for a meromorphic differential ω on C such that $\ell(D) = 1 - g + \deg(D) + \ell(K - D)$ for all divisor D on $C(\overline{k})$ and the equality holds for sufficiently positive divisor D. If $g = 1$, $K = 0$.*

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 algebraic geometry book (e.g., [ALG] IV.1 or [GME] Theorem 2.1.3).

Corollary 1.21. *If $g(C) = 1$, then $\ell(D) = \deg(D)$ if $\deg(D) > 0$.*

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

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

Corollary 1.22 (Riemann). *Let $C = \overline{V}_{\mathfrak{a}}$ be a non-singular projective curve defined over a field k. Then there exists a non-negative integer $g = g(C)$ such that $\ell(D) \geq 1 - g + \deg(D)$ for all divisor D on $C(\overline{k})$ and the equality holds for sufficiently positive divisor D.*

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

Exercise 1.23. *Prove $\Omega_{\mathbf{P}^1/\overline{k}} = 0$.*

1.7. **Regular maps from a curve into projective space.** Tak a divisor D on a nonsingular projective plane curve C. Suppose $\ell(D) = n > 0$. Take a basis $(f_1, f_2, \ldots, f_n)$ of $L(D)$. Thus we can write $f_j = \frac{h_j}{g_j}$ with homogeneous polynomials g_j, h_j having $\deg(g_j) = \deg(h_j)$. Replacing (g_j, h_j) by $(g'_0 := g_1 g_2 \cdots g_n, h'_j := h_j g^{(j)})$ for $g^{(j)} = \prod_{i \neq j} g_i$, we may assume $\deg(g'_j) = \deg(h'_j)$ for all j, and further dividing them by the GCD of $(h'_1, \ldots, h'_n, g'_0)$, we may assume that $f_j = \frac{h_j}{g_0}$ with $\deg(h_j) = \deg(g_0)$ for all j and $(g_0, h_1, \ldots, h_n)$ do not have nontrivial common divisor.

Lemma 1.24. *Let the assumptions on $(g_0, h_1, \ldots, h_n)$ be as above. Suppose that $(g_0(P), h_1(P), \ldots, h_n(P)) \neq (0, 0, \ldots, 0)$ for all $P \in C(\overline{k})$. Define $L \in C(A) \subset \mathbf{P}^n(A)$, $\phi_A(L)$ for an A-submodule of A^3 generated by $\phi(\ell) = (g_0(\ell), h_1(\ell), \ldots, h_n(\ell)) \in A^{n+1}$ for all $\ell \in L$. Then $\phi = \{\phi_A\}_A : C \to \mathbf{P}^n$ is a k-morphism of the projective plane k-curve C into $\mathbf{P}^n_{/k}$.*

The proof of the above lemma is the same as that of Corollary 1.14; so, we leave it to the reader:

Exercise 1.25. *Prove the above lemma.*

2. Elliptic curves

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

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

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

Proof. Injectivity: if $[P] - [Q] = [P] - [\mathbf{0}_E] - ([Q] - [\mathbf{0}_E]) = \operatorname{div}(f)$ with $P \neq Q$ in $E(\overline{k})$, by Lemma 1.18, f is an isomorphism. This is wrong as $g(\mathbf{P}^1) = 0$ while $g(E) = 1$. Thus $P = Q$.

Surjectivity: Pick $D \in \operatorname{Div}^0(E)$. Then $D + [\mathbf{0}_E]$ has degree 1; so, $\ell(D + [\mathbf{0}_E]) = 1$ by Corollary 1.21, and we have $\phi \in L(D + [\mathbf{0}_E])$. Then $\operatorname{div}(\phi) + D + [\mathbf{0}_E] \geq 0$ and has degree 1. Any non-negative divisor with degree 1 is a single point $[P]$. Thus $D + [\mathbf{0}_E]$ is linearly equivalent to $[P]$; so, the map is surjective. $\square$

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

Proof. Since $E(\overline{k})$ is a group, for each $P \in E(\overline{k})$, $\mathcal{T}_P : Q \mapsto Q + P$ gives an automorphism of E. Thus $\omega \circ \mathcal{T}_P$ is another element in $\Omega_{E/\overline{k}}$. Since $\dim \Omega_{E/\overline{k}} = 1$, we find $\omega \circ \mathcal{T}_P = \lambda(P)\omega$ for $\lambda \in \overline{k}$. 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 $\operatorname{div}(\omega) = 0$. $\square$

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

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

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

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

(1) *K/k is a finite field extension;*

(2) *$K \otimes_k \overline{k} \cong \overbrace{\overline{k} \times \overline{k} \times \cdots \times \overline{k}}^{d}$ as k-algebras for $d = \dim_k K$;*

(3) *C is geometrically irreducible if and only if $K = k$.*

Remark 2.1. If k is perfect, $\overline{k}/k$ is possibly an infinite Galois extension; so, by Galois theory, we have a bijection between open subgroups G of $\operatorname{Gal}(\overline{k}/k)$ 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 $K \mapsto \operatorname{Gal}(\overline{k}/K)$. Since the isomorphicm $E(\overline{k}) \cong J(C)$ is Galois equivariant, we have

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

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

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

Since any subfield $K \subset \overline{k}$ is a union of finite extensions, the identity $E(K) \cong J(E)(K)$ 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 $E(K) \cong J(E)(K)$ to all k-algebras A in place of fields K inside $\overline{k}$.

2.2. Weierstrass Equations of Elliptic Curves.

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

Proposition 2.5. *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*

(2.1) $$y^2 = 4x^3 - g_2 x - g_3 \quad \text{with} \quad g_2, g_3 \in k,$$

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.

An equation of an elliptic curve E as in (2.1) is called a *Weierstrass equation* of E, which is determined by the pair (E, ω).

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

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

from which the following relation results,

(2.2) $$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad \text{with } a_j \in k,$$

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

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

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

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

The above normalization is not affected by variable change of the form $y \mapsto y + ax + b$ and $x \mapsto x + a'$. Now we make a variable change $y \mapsto y + ax + b$ in order to remove the terms of xy and y (i.e., we are going to make $a_1 = a_3 = 0$):

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

Assuming that 2 is invertible in k, we take $a = -\frac{a_1}{2}$ and $b = -\frac{a_3}{2}$. The resulting equation is of the form $y^2 = x^3 + b_2 x^2 + b_4 x + b_6$. We now make the change of variable $x \mapsto x + a'$ to make $b_2 = 0$:

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

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

If the discriminant $\Delta(E, \omega)$ of $g(x) = 4x^3 - g_2 x - g_3$ vanishes, C has only singularity at $(x_0 : 0 : 1)$ for a multiple root x_0 of $g(x) = 0$. If $g(x)$ has a double zero, C is isomorphic over $\overline{k}$ to the curve defined by $y^2 = x^2(x - a)$ for $a \neq 0$. Let $t = \frac{x}{y}$. Then for $P \in E(\overline{k})$ mapping to $(0, 0)$, $v_P(y) = v_P(x)$; so, P is neither a zero nor a pole of t. The function t never vanish outside $\mathbf{0}_E$ (having a pole at $(a, 0)$). It has a simple zero at $\mathbf{0}_E$ by the normalization of x and y. Thus $\deg(\mathrm{div}_0(t)) = 1$, and $\overline{k}(C) = \overline{k}(t)$, which is impossible as $k(C) = k(E)$ and $g(E) = 1$. The case of triple zero can be

excluded similarly. Thus we conclude $\Delta(E, \omega) \neq 0$ ($\Leftrightarrow C$ is smooth: Example 1.3), and we have $E \cong C$ by ϕ.

Conversely, we have seen that any curve defined by equation (2.1) is smooth in Example 1.3 if the cubic polynomial $F(X) = 4X^3 - g_2 X - g_3$ 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 $Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$ in $\mathbf{P}^2_{/k}$ has a rational point $\mathbf{0} = (0, 1, 0) \in E(k)$, which is ∞ in $\mathbf{P}^2$. Thus E is smooth over k if and only if $\Delta(E, \omega) \neq 0$ (an exercise following this proof).

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

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

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

This shows

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

Thus the nowhere-vanishing differential form ω to which T is adapted is given by $\frac{dx}{y}$. Conversely, if $\Delta \neq 0$, the curve defined by $y^2 = 4x^3 - g_2 x - g_3$ 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. $\qquad\square$

Exercise 2.6. (1) *If C is defined by $y^2 = x^3$, prove $k(C) = k(t)$ for $t = \frac{x}{y}$.*

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

    (3) *Show that if $\Delta \neq 0$, the curve defined by $y^2 = 4x^3 - g_2 x - g_3$ is also smooth at $\mathbf{0} = \infty$.*

2.3. **Moduli of Weierstrass Type.** We continue to assume that the characteristic of k is different from 2 and 3. Suppose that we are given two elliptic curves $(E, \omega)_{/k}$ and $(E', \omega')_{/k}$ with nowhere-vanishing differential forms ω and ω'. We call two pairs (E, ω) and (E', ω') isomorphic if we have an isomorphism $\varphi : E \to E'$ with $\varphi^* \omega' = \omega$. Here for $\omega' = f dg$, $\varphi^* \omega' = (f \circ \varphi) d(g \circ \varphi)$; 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 $\mathbf{0}$ of E' adapted to ω'. If $\varphi : (E, \omega) \cong (E', \omega')$, then the parameter $T = \varphi^* T' \bmod T^2$ is adapted to ω (because $\varphi^* \omega' = \omega$). We choose coordinates (x, y) for E and (x', y') for E' relative to T and T' as above. By the uniqueness of the choice of (x, y) and (x', y'), we know $\varphi^* x' = x$ and $\varphi^* y' = y$. Thus the Weierstrass equations of (E, ω) and (E', ω') coincide. We write $g_2(E, \omega)$ and $g_3(E, \omega)$ for the g_2 and g_3 of the coefficients of the Weierstrass equation of (E, ω). If

a field K has characteristic different from 2 and 3, we have

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

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

Exercise 2.7. *If k has characteristic 2, show that we cannot have any ring $\mathcal{R}$ such that*

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

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

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

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

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

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

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

This shows

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

Thus we have

Theorem 2.8. *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 twelfth root λ of $\Delta(E,\omega)/\Delta(E',\omega')$. Note that the twelfth root λ may not be in K if K is not algebraically closed.

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

Corollary 2.9. *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 2.10.   (1) *Prove that $g_j(E',\omega') = \lambda^{-2j} g_j(E,\omega)$ for suitable ω and ω' and a suitable twelfth root λ of $\Delta(E,\omega)/\Delta(E',\omega')$ if $J(E) = J(E')$.*
   (2) *Explain what happens if $J(E) = J(E')$ but $E \not\cong E'$ over a field K not necessarily algebraically closed.*

3. Modular forms

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

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

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

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

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

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

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

Then 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, $P \in C_i(K)$ therefore gives rise to an A-algebra homomorphism $\phi : R_i \to K$; so, $\mathrm{Ker}(\phi)$ is a maximal ideal of R_i.

Exercise 3.2. *Under the above setting, prove*

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

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

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

Again $\mathcal{O}_{C,P}$ is determined independent of the choice of i with $P \in C_i(K)$. Then $\mathcal{O}_{C,P}$ is a local ring with maximal ideal $\mathfrak{m}_P$ with $\mathcal{O}_{C,P}/\mathfrak{m}_P \cong \mathrm{Im}(\phi) \subset K$. The cotangent space at P is defined by P/P^2 and the tangent space at P over K is by definition its dual $\mathrm{Hom}_K(P/P^2, K)$. Again the tangent space is isomorphic to the space of K-derivations $\partial : \mathcal{O}_{C,P} \to K$. Consider 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 $\widehat{A}$. We call $P \in C(K)$ *smooth* over A if $\widehat{\mathcal{O}}_{C,P} \cong \widehat{A}[[T]]$ for a variable T (the variable T is again called the local parameter at P). If C is smooth over A at all maximal point $P \in C$, we call C *smooth* over A.

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

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.

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

An elliptic curve over A is a plane projective smooth curve E of genus 1 with a specific point $\mathbf{0}_E \in E(A)$. If $\Omega_{E/A} = A\omega$, the differential ω is called a *nowhere vanishing differential*. If $\phi : E \to E'$ is a morphism of elliptic curve, we can pull back a nowhere vanishing differential ω' on E' by ϕ, which is written as $\phi^*\omega'$. Note here

that $\phi^*\omega'$ may not be nowhere vanishing (though it is, if ϕ is an isomorphism). If $A \xrightarrow{\sigma} A'$ is an algebra homomorphism and if a plane projective A-curve C is defined by an equation $F(X, Y, Z) = \sum_{i,j,l} c_{i,j,l} X^i Y^j Z^l$, the σ-transform $\sigma(F)(X, Y, Z) = \sum_{i,j,l} \sigma(c_{i,j,l}) X^i Y^j Z^l$ defines a plane projective A'-curve $\sigma(C)$. Note that $\sigma(C_i)$ is defined by the ring $R_i \otimes_{A,\sigma} A'$; so, often we write $C \otimes_A A'$ for $\sigma(C)$ and call it the base-change $C \otimes_A A'_{/A'}$ of $C_{/A}$. Similarly, if $\partial : R_i \to R_i$ is an A-derivation, $\partial \otimes 1 : R_i \otimes_A A' \to R_i \otimes_A A'$ given by $\partial \otimes 1(\phi \otimes a) = \sigma(a\partial(\phi))$ is an A'-derivation. This shows $Der_{C_i/A} \otimes_A A' = Der_{C_i \otimes A'/A'}$. Thus by duality, we also have $\Omega_{C_i/A} \otimes_A A' = \Omega_{C_i \otimes A'/A'}$. In particular, $\omega \in \Omega_{C/A}$ induces $\sigma_*(\omega) = \omega \otimes 1 \in \Omega_{C \otimes A'/A'}$. We write the pair $(E \otimes_A A', \sigma_*\omega)$ as $(E, \omega) \otimes_A A'$. This makes $\mathcal{P} : ALG \to SETS$ given by $\mathcal{P}(A) = [(E, \omega)_{/A}]$ a covariant functor from the category of algebras into sets. We again have the following result basically in the same way as in the case of fields (see [GME] §2.2.6 for a proof):

Theorem 3.4. *Let* $\mathcal{R} = \mathbb{Z}[\frac{1}{6}, g_2, g_3, \frac{1}{\Delta}]$. *Then we have a canonical equivalence of functors from* $ALG_{/\mathbb{Z}[\frac{1}{6}]}$ *to* $SETS$:

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

In other word, for a given pair $(E, \omega)_{/A}$ of an elliptic curve E over A and a nowhere vanishing differential ω, there exists unique coordinate $(g_2(E, \omega), g_3(E, \omega)) \in A^2$ such that E is defined by $Y^2 Z = 4X^3 - g_2(E, \omega) X Z^2 - g_3(E, \omega) Z^3$ and ω is given by $\frac{dX}{Y}$ on D_2. We also have

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

3.2. **Geometric modular forms.** Let A be an algebra over $\mathbb{Z}[\frac{1}{6}]$. We restrict the functor $\mathcal{P}$ to $ALG_{/A}$ and write the restriction $\mathcal{P}_{/A}$. Then by Theorem 3.4, for $\mathcal{R}_A := A[g_2, g_3, \frac{1}{\Delta}]$,

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

A morphism of functors $\phi : \mathcal{P}_{/A} \to \mathbb{A}^1_{/A}$ is by definition given by maps $\phi_R : \mathcal{P}_{/A}(R) \to \mathbb{A}^1(R) = R$ 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 $\mathbb{A}^1_{/A}(?) = \mathrm{Hom}_{ALG_{/A}}(A[X], ?)$ by $R \ni a \leftrightarrow (\varphi : A[X] \to R) \in \mathrm{Hom}_{ALG_{/A}}(A[X], ?)$ with $\varphi(X) = a$. Thus in particular,

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

Thus $\phi_{\mathcal{R}_A}(\mathrm{id}_{\mathcal{R}_A}) \in \mathcal{R}_A$; so, write $\phi_{\mathcal{R}_A}(\mathrm{id}_{\mathcal{R}_A}) = \Phi(g_2, g_3)$ for a two variable rational function $\Phi(x, y) \in A[x, y, \frac{1}{x^3 - 27y^2}]$. Let $\mathbf{E}_{/\mathcal{R}_A}$ be the universal elliptic curve over $\mathcal{R}_A$ defined by $Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$ 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, $(E, \omega)_{/R} \cong (\mathbf{E}, \omega)_{\mathcal{R}_A} \otimes_{\mathcal{R}_A} R$. Thus

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

Theorem 3.5. *Any functor morphism $\phi : \mathcal{P}_{/A} \to \mathbb{A}^1_{/A}$ 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 eliiptic 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 $\Phi = \sum_{a,b} c_{a,b} g_2^a g_3^b$ of g_2 and g_3 is called *isobaric* if $c_{a,b} \neq 0 \Rightarrow 4a + 6b = w$.

A weight w modular form defined over A is a morphism of functors $\mathcal{P}_{/A} \to \mathbb{A}^1_{/A}$ given by an isobaric polynomial of g_2 and g_3 of weight w with coefficients in A. Write $G_w(A)$ 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 A-algebra homomorphism $\sigma : R \to R'$,
(G3) $f((E, \lambda\omega)_{/R}) = \lambda^{-w} f(E, \omega)$ for any $\lambda \in R^\times$.

Exercise 3.6. *For a field K with $\frac{1}{6} \in K$, prove for $0 < w \in 2\mathbb{Z}$,*

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

3.3. **Topological Fundamental Groups.** In the following three sections, we would like to give a sketch of Weierstrass' theory of elliptic curves defined over the complex field $\mathbb{C}$. By means of Weierstrass $\mathcal{P}$–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 (combining with geometric technique of Weil-Shimura) many results on the moduli space of elliptic curves, like, the exact field of definition of the moduli, determination of the field of moduli (of each member), and so on (e.g., [IAT] Chapter 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 in studying analytic method. After studying analytic theory over $\mathbb{C}$, combining these techniques, we start studying modular forms.

Let $(E, \omega)_{/\mathbb{C}}$ be an elliptic curve over $\mathbb{C}$. Then

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

and $E(\mathbb{C})$ is a compact Riemann surface of genus 1. A path $\gamma : y \to x$ on $E(\mathbb{C})$ is a piecewise smooth continuous map γ from the interval $[0,1]$ into $E(\mathbb{C})$ (under the Euclidean topology on $E(\mathbb{C})$) such that $\gamma(0) = y$ and $\gamma(1) = x$. Two paths $\gamma, \gamma' : x \to x$ are homotopy equivalent (for which we write $\gamma \approx \gamma'$) if there is a bi-continuous map $\varphi : [0,1] \times [0,1] \to E(\mathbb{C})$ such that $\varphi(0,t) = \gamma(t)$ and $\varphi(1,t) = \gamma'(t)$. Let $\mathcal{Z}$ be the set of all equivalence classes of paths emanating from $\mathbf{0}$.

More generally, for each complex manifold M, we can think of the space $\mathcal{Z} = \mathcal{Z}(M)$ of homotopy classes of paths emanating from a fixed point $x \in M$. An open neighborhood U of x is called *simply connected* if $\mathcal{Z}(U) \cong U$ by projecting $(\gamma : x \to y)$ down to y. 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 product 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 multiplication, $\pi_M = \pi(M,x) = \{\gamma \in \mathcal{Z}(M) | \gamma : x \to x\}$ becomes a group called *the topological fundamental group* of M. Taking a fundamental system of neighborhoods $\mathcal{U}_y$ of $y \in M$ made of simply connected open neighborhoods of y, we define a topology on $\mathcal{Z}(M)$ so that a fundamental system of neighborhoods of $\gamma : x \to y$ is given by $\{\gamma U | U \in \mathcal{U}_x\}$. Then π_M acts on $\mathcal{Z}(M)$ freely without fixed points. By definition, 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. Since $\pi^{-1}(x) = \{x\}$, $\pi : \pi_M \backslash \mathcal{Z}(M) \cong M$ is a homeomorphism. Since $\pi : \mathcal{Z}(M) \to M$ is local isomorphism, we can regard $\mathcal{Z}(M)$ as a complex manifold. This space $\mathcal{Z}(M)$ is called a universal covering space of M.

We now return to the original setting: $\mathcal{Z} = \mathcal{Z}(E(\mathbb{C}))$, and write $\Pi = \pi(E, \mathbf{0})$. 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 visibly 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 $f \circ \phi(0,t) = (\gamma' + \gamma)(t)$ and $f \circ \phi(1,t) = (\gamma + \gamma')(t)$.

By the above addition, $\mathcal{Z}$ is an additive complex Lie group. Since $\gamma + \gamma' = \gamma\gamma'$ if $\gamma \in \Pi$ and $\gamma' \in \mathcal{Z}$ by definition, Π is an additive subgroup of $\mathcal{Z}$ and $\Pi \backslash \mathcal{Z} \cong E(\mathbb{C})$, where the quotient is made through the group action.

Now we define, choosing a C^∞–path $[\gamma]$ in each class of $\gamma \in \mathcal{Z}$ modulo Π and a nowhere vanishing differential form ω on E, 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 choice of the representative $[\gamma]$ 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, $\mathcal{Z}(U) \cong I(U)$. 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 a 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 $m, n \in \mathbb{Q}$; so, I is a surjective isomorphism.

This also shows that 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 induces 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:

$$(3.1) \qquad\qquad \operatorname{End}(E_{/\mathbb{C}}) \hookrightarrow \mathbb{C}.$$

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

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

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

By the above fact combined with (3.1), we get

Proposition 3.7. *We have a ring embedding* $\operatorname{End}(E_{/\mathbb{C}}) \hookrightarrow \{u \in \mathbb{C} | u \cdot L_E \subset L_E\}$, *and hence* $\operatorname{End}(E_{/\mathbb{C}})$ *is either* $\mathbb{Z}$ *or an order of an imaginary quadratic field.*

Proof. The first assertion follows from (3.1). Pick $\alpha \in \operatorname{End}(E_{/\mathbb{C}})$ corresponding $u \in \mathbb{C}$ 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 $uw = \rho(\alpha)w$; so, $\rho : \operatorname{End}(E_{/\mathbb{C}}) \to M_2(\mathbb{Z})$ is a ring homomorphism. By the first assertion, the image has to be an order of imaginary quadratic field or just $\mathbb{Z}$. $\qquad\square$

When $\operatorname{End}(E_{/\mathbb{C}}) \neq \mathbb{Z}$, E is said to have *complex multiplication*.

3.4. **Classical Weierstrass Theory.** Conversely, for a given $L \in Lat$, we define the Weierstrass $\mathcal{P}$–functions by

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

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

where

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

Then $\varphi = y_L^2 - 4x_L^3 + g_2 x_L + g_3$ is holomorphic everywhere. Since these functions factors through the compact space $\mathbb{C}/L$, φ has to be constant, because any non-constant holomorphic function is an open map (the existence of power series expansion and the implicit function theorem). Since x_L and y_L do not have constant terms, we conclude $\varphi = 0$. We have obtained a holomorphic map $(x_L, y_L) : \mathbb{C}/L - \{0\} \to \mathbf{A}^2_{/\mathbb{C}}$. Looking at the order of poles at $\mathbf{0}$, we know the above map is of 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 have an elliptic curve $E_L = \Phi(\mathbb{C}/L) = E(g_2(L), g_3(L))$. We then have

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

This shows

Theorem 3.8. (Weierstrass) *We have* $[(E, \omega)_{/\mathbb{C}}] \cong Lat$.

We would like to make the space Lat a little more explicit. We see easily that $w_1, w_2 \in (\mathbb{C}^\times)^2$ span a lattice if and only if $\mathrm{Im}(w_1/w_2) \neq 0$. Let $\mathfrak{H} = \{z \in \mathbb{C} | \, \mathrm{Im}(z) > 0\}$. 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:

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

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

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

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:

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

3.5. **Complex Modular Forms.** We want to write down definitions of modular forms over $\mathbb{C}$. We consider $f \in G_w(\mathbb{C})$. Writing $L(v) = L(w_1, w_2)$ for the lattice spanned by $v \in \mathcal{B}$, we can regard f as a holomorphic function on $\mathcal{B}$ by $f(v) = f(E_{L(v)}, \omega_{L(v)})$. Then the conditions (G0–3) can be interpreted as

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

We may also regard $f \in G_w(\mathbb{C})$ as a function on $\mathfrak{H}$ by $f(z) = f(v(z))$ for $v(z) = 2\pi i \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix} \right) (z \in \mathfrak{H})$. Here 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 $\mathbb{Z}[\frac{1}{6}][g_2, g_3]$, as we will

see later $(2\pi i)^{-j}g((\begin{smallmatrix} z \\ 1 \end{smallmatrix}))$ has Fourier expansion in $\mathbb{Q}[[q]]$ for $q = \exp(2\pi i z)$. Then we have the following interpretation:

(G0) $\qquad\qquad\qquad\qquad f \in \mathbb{C}[g_2(z), g_3(z)];$

(G1,3) $\qquad\qquad\quad f(\alpha(z)) = f(z)(cz + d)^w$ for all $\alpha = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in SL_2(\mathbb{Z});$

(G2) $\qquad\qquad\qquad\quad f \in \mathbb{C}[g_2(z), g_3(z), \Delta(z)^{-1}].$

Since $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})(z) = z + 1$, any $f \in \mathbb{C}[g_2(z), g_3(z), \Delta^{-1}(z)]$ is translation invariant. 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 the following section and [LFE] Chapter 5):

$$12g_2 = 1 + 240 \sum_{n=1}^{\infty} \left\{ \sum_{0 < d | n} d^3 \right\} q^n \in \mathbb{Z}[[q]]^\times,$$

(3.2) $$-6^3 g_3 = 1 - 504 \sum_{n=1}^{\infty} \left\{ \sum_{0 < d | n} d^5 \right\} q^n \in \mathbb{Z}[[q]]^\times,$$

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \in q(\mathbb{Z}[[q]]^\times).$$

This shows that

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

In particular, we may regard g_2 and g_3 as elements of $\mathbb{Z}[\frac{1}{6}][[q]]$.

We 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 $Y^2 Z = 4X^3 - g_2(q)XZ^2 - g_3(q)Z^3$ 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 $\mathbb{Z}[1/6]((q))$ 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. In particular, if $f \in G_w(\mathbb{C})$, the q–expansion $f(q)$ coincides with the analytic Fourier expansion via $q = \mathbf{e}(z)$, because f is an isobaric polynomial 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 $D_1 = \mathbb{A}^1$ 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

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

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 ∞.

Since we have

$$M_1(\mathbb{C}) = Lat/\mathbb{C}^\times = \mathfrak{H} \times \mathbb{C}^\times/(SL_2(\mathbb{Z}) \times \mathbb{C}^\times) \cong SL_2(\mathbb{Z})\backslash\mathfrak{H},$$

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″) $f : \mathcal{P}_{/A} \to \mathbb{A}^1_{/A}$ is a morphism of functors satisfying the automorphic property (G3) in §3.2, and its algebraic q–expansion $f(E_\infty, \omega_\infty)$ is contained in $A[[q]]$.

3.6. **Hurwitz's theorem, an application.** In 1897, Hurwitz studied an analogue of the Riemann zeta function:

$$L(4k) = \sum_{a+bi \in \mathbb{Z}[i] - \{0\}} \frac{1}{(a+bi)^{4k}}$$

for Gaussian integers $\mathbb{Z}[i]$ and showed that for positive integer k,

$$\frac{L(4k)}{\Omega^{4k}} \in \mathbb{Q} \quad (\Omega = 2 \int_0^1 \frac{dx}{\sqrt{1-x^4}} = \int_\gamma \frac{dx}{y} : \text{period of the lemniscate}).$$

Nowadays, we regard this value as a special value of a Hecke L-function:

$$L(s, \lambda) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) N(\mathfrak{a})^{-s} \quad \text{of the Gaussian field } \mathbb{Q}[i] \ (i = \sqrt{-1}).$$

Here $\lambda = \lambda_{4k}$ is a Hecke ideal character of $\mathbb{Q}[i]$ with $\lambda_{4k}((\alpha)) = \alpha^{-4k}$ and $L(4k) = 4L(0, \lambda)$ and $\mathfrak{a}$ runs over all nonzero ideals of the Gaussian integer ring $\mathbb{Z}[i]$.

   The plane affine curve $y^2 = 1 - x^4$ was first studied by Gauss around the same time when he finished his first major treatise "Disquisitiones Arithmeticae" in 1978 when he was 21 years old (though unpublished, he claimed that he can extend his theory of drawing regular polygon in a circle to this lemniscate or more general curves). This Gauss' lemniscate is equivalent to $Y^2 = 4X^3 - 4X$ by $Y = \frac{(4+4i)y}{((i-1)x+(1-i))^2}$ and $X = \frac{(1+i)x+1+i}{(i-1)x+1-i}$; so, it is an elliptic curve $(\mathcal{E}, \omega_\mathcal{E} := \frac{dX}{Y})_{/\mathbb{C}}$ with a given nowhere vanishing differential $\omega_\mathcal{E}$. We have $X = 0 \Leftrightarrow x = -1$ and $X = \infty \Leftrightarrow x = 1$. Since $\int_{-1}^1 \frac{dx}{\sqrt{1-x^4}} = 2 \int_0^1 \frac{dx}{\sqrt{1-x^4}}$, we get

$$\Omega = 2 \int_0^1 \frac{dx}{\sqrt{1-x^4}} = \int_0^\infty \frac{dX}{\sqrt{4X^3 - 4X}}.$$

Here, writing the path $\gamma := [0, \infty] = -[0, \mathbf{0}_\mathcal{E}] \in \pi_1(\mathcal{E}(\mathbb{C}), \mathbf{0}_\mathcal{E})$, we have the "period" Ω in the lattice $L_\mathcal{E} \in Lat$ of $\mathcal{E}$, which is a part of a $\mathbb{Z}$-basis of $L_\mathcal{E}$.

   Gauss' curve has an automorphism $[i] : (x, y) \mapsto (ix, y)$. This corresponds to the automorphism $[i] : (X, Y) \mapsto (iX, -Y)$ of the elliptic curve $\mathcal{E}$. Note that $[i](\mathbf{0}_\mathcal{E}) = \mathbf{0}_\mathcal{E}$. By Abel's theorem, we have a commutative diagram:

$$\begin{array}{ccc}
\mathcal{E}(\mathbb{C}) & \xrightarrow{\ \sim\ } & J(\mathcal{E}) \\
{\scriptstyle [i]}\downarrow & & \downarrow{\scriptstyle [i]_*} \\
\mathcal{E}(\mathbb{C}) & \xrightarrow{\ \sim\ } & J(\mathcal{E}),
\end{array}$$

where at the divisor level

$$[i]_*(\sum_P m_P[P]) = \sum_P m_P[[i](P)].$$

Thus $[i]$ is a group endomorphism of $\mathcal{E}$.

We can verify this fact differently. Any curve endomorphism $\alpha : E \to E$ sending $\mathbf{0}_E$ to $\mathbf{0}_E$ induces an endomorphism of the universal covering $\alpha : \mathcal{Z}(E(\mathbb{C})) \to \mathcal{Z}(E(\mathbb{C}))$ by sending a path $\gamma : \mathbf{0}_E \to z$ to $\alpha(\gamma) : \mathbf{0}_E = \alpha(\mathbf{0}_E) \to \alpha(\gamma)$ (the image of γ under α). Then by the definition of composition of paths, we have $\alpha(\gamma\gamma') = \alpha(\gamma)\alpha(\gamma')$. The group structure on $\mathcal{Z}(E(\mathbb{C})) = \mathbb{C}$ is given by this product structure (up to translation), $\alpha : \mathbb{C} \to \mathbb{C}$ is an additive group endomorphism. Since α is holomorphic (as it is a polynomial map in coordinates of $\mathbf{P}^2_{/\mathbb{C}}$ containing E), α has to be a $\mathbb{C}$-linear map; so, the original $\alpha : \mathbb{C}/L_E \to \mathbb{C}/L_E$ is a group homomorphism.

Now the vertical line L_{Y_0} defined by $Y = Y_0$ intersects with $E(\mathbb{C})$ at $[i]^2(X_0, Y_0) = (-X_0, Y_0)$ and (X_0, Y_0) and the infinity $\mathbf{0}_E$. Thus in $\mathrm{End}(E_{/\mathbb{C}})$, $[i]$ satisfies $[i]^2 = -1$. In other words, we have an embedding $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(\mathcal{E}_{/\mathbb{C}})$ given by $a + bi \mapsto a + b[i]$. Therefore $[i]$ acts on $\pi_1(\mathcal{E}(\mathbb{C}), \mathbf{0}_{\mathcal{E}}) \cong L_{\mathcal{E}}$ by $[i]$ on the left-hand-side and via multiplication by i on the right-hand-side. In short, $\mathcal{E}$ has complex multiplication by the Gaussian integers $\mathbb{Z}[i]$. Since the path $[-1, 1]$ is one of the generators of $H_1(R, \mathbb{Z})$ for the Riemann surface R associated to $y^2 = 1 - x^4$, we find that $L_{\mathcal{E}} = \mathbb{Z}[i] \cdot \Omega \subset \mathbb{C}$.

Hurwitz's formulation is modular: For any lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2 \subset \mathbb{C}$, we can think about

$$E_{2k}(L) = \frac{1}{2} \sum_{aw_1+bw_2 \in L} \frac{1}{(aw_1 + bw_2)^{2k}} \quad \text{(Eisenstein series, 1847)},$$

which is a function of lattices satisfying $E_{2k}(\alpha L) = \alpha^{-2k} E_{2k}(L)$. The quotient $\mathbb{C}/L$ gives rise to an elliptic curve $X(L) \subset \mathbf{P}^2$ by Weierstrass theory. Since $X(L)$ has a unique nowhere vanishing differential du for the variable u of $\mathbb{C}$ and we can recover out of $(X(L), du)$ the lattice L as $\{\int_\gamma du | \gamma \in \pi_1(X(L))\}$, we can think of E_{2k} as a function of the pairs (E, ω) of an elliptic curve E and a nowhere vanishing differential ω satisfying $E_{2k}(E, \alpha\omega) = \alpha^{-2k} E_{2k}(E, \omega)$. Note that $E_4(E, \omega) = \frac{1}{120}g_2(E, \omega)$ and $E_6(E, \omega) = \frac{1}{280}g_3(E, \omega)$. More generally, E_{2k} is a rational isobaric polynomial of g_2 and g_3. Thus E_{2k} is a modular form f of weight $2k$.

Since Weierstrass' function has the following Laurent expansion

(3.4) $$x_L(u) = u^{-2} + 6E_4(E, \omega)u^2 + \cdots + 2(2k + 1)E_{2k+2}(E, \omega)u^{2k} + \cdots.$$

Taking the derivative, we get

(3.5) $$y_L(u) = -2u^{-3} + 12E_4(E, \omega)u + \cdots + 4k(2k + 1)E_{2k}(E, \omega)u^{2k-1} + \cdots.$$

Plug this into the relation $y_L^2 = 4x_L^3 - g_2(E, \omega)x_L - g_3(E, \omega)$, we get a recurrence relation of E_{2k}, and solving the recurrence relation, we can compute the exact form of the isobaric polynomial $\Phi_{2k}(X, Y) \in \mathbb{Q}[X, Y]$ with $E_{2k}(E, \omega) = \Phi_{2k}(g_2(E, \omega), g_3(E, \omega))$.

Returning to Gauss's curve $(\mathcal{E}, \omega_{\mathcal{E}})$ defined by $y^2 = 4x^3 - 4x$, we have $L_{\mathcal{E}} = \mathbb{Z}[i] \cdot \Omega$. Thus

$$E_{2k}(\mathcal{E}, \omega_{\mathcal{E}}) = E_{2k}(\mathbb{Z}[i] \cdot \Omega) = \Omega^{-2k} E_{2k}(\mathbb{Z}i + \mathbb{Z}) = \Omega^{-2k} E_{2k}(i),$$

where at the extreme right, we regard E_{2k} as a function on $\mathfrak{H}$ by $E_{2k}(z) = E_{2k}(\mathbb{Z}z+\mathbb{Z})$. On the other hand,

$$E_{2k}(\mathcal{E}, \omega_{\mathcal{E}}) = \Phi_{2k}(g_2(\mathcal{E}, \omega_{\mathcal{E}}), g_3(\mathcal{E}, \omega_{\mathcal{E}})) = \Phi_{2k}(4, 0) \in \mathbb{Q}.$$

Note that $E_{2k}(i) = L(0, \lambda_{2k})$. Thus we get

Theorem 3.9 (Hurwitz [Hz], 1897). *We have $\frac{L(0,\lambda_{4k})}{\Omega^{4k}} \in \mathbb{Q}$ for all $0 < k \in \mathbb{Z}$.*

We can apply the same technique to the curve defined by $y^2 = x^3 - 1$ which has complex multiplication by the field $\mathbb{Q}[\sqrt{-3}]$, as a cubic root of unity ζ acts on the curve by $(x, y) \mapsto (\zeta x, y)$.

This is an obvious analogue of the rationality of Riemann zeta values by Euler/Bernoulli:

$$\frac{\zeta(2k)}{(2\pi i)^{2k}} = \frac{1}{(2\pi i)^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \in \mathbb{Q}.$$

Indeed, $2\pi i$ is the integral $\oint_{|z|=1} \frac{dz}{z}$ of the invariant differential of the multiplicative group $\mathbb{G}_{m/\mathbb{Z}}$ sending a ring A to its multiplicative group $A^{\times}$, and also note $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^{\times} \xleftarrow[\exp]{\sim} \mathbb{C}/2\pi i\mathbb{Z}$, while $\mathcal{E}(\mathbb{C}) \cong \mathbb{C}/\Omega \cdot \mathbb{Z}[i]$.

The rationality results of Hurwitz is now generalized to all imaginary quadratic fields M and L-values of the form $L(0, \lambda_{k,j})$ with integers $j < 0 \leq k$ for characters of the form $\lambda_{k,j}(\alpha) = \alpha^k \overline{\alpha}^j$ by the effort of many outstanding mathematicians, notably, Damerell, Manin, Mazur, Weil, Shimura and Katz, and the value is algebraic up to a power of the period $\Omega(E, \omega)$ and a power of $2\pi i$. Here $\Omega(E, \omega)$ is given by $\int_{\gamma} \omega$ for a pair (E, ω) defined over a number field with complex multiplication by the integer ring of M. Probably the most elementary treatment of this generalization is in Weil's book [EEK].

We can further ask

(Q1) Is there a good expression by an L-value of the value of a non-Eisenstein series $f \in G_w(\overline{\mathbb{Q}})$ at $(\mathcal{E}, \omega_{\mathcal{E}})$ (or at more general elliptic curves with complex multiplication)?

(Q2) What happens? if we evaluate a modular form in $G_w(\overline{\mathbb{Q}})$ at a rational elliptic curve $(E, \omega)_{/\mathbb{Q}}$ without complex multiplication.

To get a reasonable answer, we need to assume that the modular form in question is an eigenvector of all Hecke operators (as Eisenstein series are examples of such eigenforms). Under this assumption, as for (Q1), there are good answers by Waldspürger [Wa] and also by Gross–Zagier [GZ] (which promoted much progress towards solution of the Birch-Swinnerton Dyer conjecture). As for (Q2), not much is known yet.

4. ELLIPTIC CURVES OVER p–ADIC FIELDS

In this section, we recall the theory of Tate curves, following Tate's original paper [T1] (dating back to 1959, although it was published in 1995). This fact has been generalized to higher dimensional abelian varieties by Mumford and Faltings-Chai [DAV] II, III.

4.1. **Power series identities.** By Weierstrass theory, every elliptic curve over $\mathbb{C}$ is isomorphic to E with $E(\mathbb{C}) = \mathbb{C}/L$ for $L = \mathbb{Z}(2\pi i) + \mathbb{Z}\log q$ 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 Subsection 3.4 that

$$g_2(L) = \frac{1}{12} + 20\sum_{n=1}^\infty \left\{\sum_{0<d|n} d^3\right\} q^n = \frac{1}{12} + 20\sum_{n=1}^\infty \frac{n^3 q^n}{1-q^n},$$

$$(4.1) \qquad g_3(L) = -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^\infty \left\{\sum_{0<d|n} d^5\right\} q^n = -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^\infty \frac{n^5 q^n}{1-q^n},$$

$$\Delta(L) = q\prod_{n=1}^\infty (1-q^n)^{24}.$$

The first two formulas follow from the following partial fraction expansion of the cotangent function for $z = \frac{\log q}{2\pi i}$:

$$(4.2) \qquad \frac{1}{z} + \sum_{n=1}^\infty \left\{\frac{1}{(z+n)} + \frac{1}{(z+n)}\right\} = \pi\cot(\pi z) = \pi i\left\{-1 - 2\sum_{n=1}^\infty q^n\right\},$$

and its derivatives by $\left((2\pi i)^{-1}\frac{d}{dz}\right)^k = \left(q\frac{d}{dq}\right)^k$:

$$(4.3) \qquad \sum_{n=-\infty}^\infty \frac{1}{(z+n)^k} = \frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^\infty n^{k-1} q^n.$$

To obtain the product expansion of Δ, one need to work a little more (see [EEK], IV, (36)).

Write $w = \exp(u) = e^u$ ($u = \log w$). We now compute q–expansion of the Weierstrass function $\mathcal{P}_L(u)$: By (4.3), we get for w with $|q| < |w| < |q|^{-1}$

$$\mathcal{P}_L(u) = \frac{1}{u^2} + \sum_{m=-\infty,\ m\neq 0}^\infty \left\{\frac{1}{(u+2\pi i m)^2} - \frac{1}{(2\pi i m)^2}\right\}$$

$$+ \sum_{n=1}^\infty \left\{\sum_{m=-\infty}^\infty \frac{1}{(-u+2\pi i m + n\log q)^2} - \frac{1}{(2\pi i m + n\log q)^2}\right\}$$

$$+ \sum_{n=1}^\infty \left\{\frac{1}{(u+2\pi i m + n\log q)^2} - \frac{1}{(2\pi i m + n\log q)^2}\right\}$$

$$= \sum_{m=1}^\infty m w^m - \frac{2\zeta(2)}{(2\pi i)^2} + \sum_{n=1}^\infty\sum_{m=1}^\infty \left\{m w^{-m} q^{mn} + m w^m q^{mn} - 2q^{mn}\right\}.$$

Differentiating $\frac{1}{1-w} = \sum_{m=0}^{\infty} w^m$, we have

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

Then from the fact: $\zeta(2) = \frac{\pi^2}{6}$, we see

(4.4) $$x_L(u) = \mathcal{P}_L(u) = t_L(w) + \frac{1}{12},$$

where

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

We can rewrite

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

This shows that $t(q, w) \in \mathbb{Z}[w, w^{-1}, (1 - w)^{-1}][[q]]$. Regarding w as an indeterminate, we write A_w for $\mathbb{Z}[w, w^{-1}, (1 - w)^{-1}]$, which is a finitely generated $\mathbb{Z}$–algebra. We have seen that $t(q, w) \in A_w[[q]]$.

Differentiating with $w \frac{d}{dw} = \frac{d}{du}$, we get

(4.6) $$y_L(u) = \mathcal{P}'(u) = t_L(w) + 2 s_L(w),$$

where

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

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

(4.8) $$s^2(q, w) + t(q, w) s(q, w) = t(q, w)^3 - b_2(q) t(q, w) - b_3(q),$$

where

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

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

Although we computed the above identity using function theory, we note that all the functions in (4.8) have power series expansion in $A_w[[q]]$ and the identity is the algebraic identity in the power series ring, because the identity is valid over the open

set $|q| < |w| < |q|^{-1}$ in $\mathbb{C}^2$. We note one more identity in $A_w[[q]]$:

$$(4.9) \quad \Delta = g_2^3 - 27g_3^2 = \left(4b_2 + \frac{1}{12}\right)^3 - 27\left(4b_3 - \frac{b_2}{3} - \frac{1}{216}\right)^2$$

$$= b_3 + b_2^2 + 72b_2b_3 - 432b_3^2 + 64b_2^3 = q\prod_{n=1}^{\infty}(1 - q^n)^{24}.$$

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

$$(4.10) \qquad t(q, qw) = t(q, w) \quad \text{and} \quad s(q, qw) = s(q, w) \quad \text{in } A_w[[q]].$$

Of course, this can be verified by computation using only power series expansions of the functions involved. We can easily check by power series computation the following identity:

$$(4.11) \qquad\qquad s(q, w^{-1}) + s(q, w) = -t(q, w) \quad \text{in } A_w[[q]].$$

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

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

Exercise 4.1. (1) *Show that the projective plane curve over C 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 $\mathbb{F}_p(w)$ by $x = \frac{X}{Z} = \frac{w}{(1-w)^2}$ and $y = \frac{Y}{Z} = \frac{w^2}{(1-w)^3}$.*

4.2. **Tate curves.** By the computation above, we get the following projective plane curve E_∞ defined over $\mathbb{Z}[[q]]$ By the equation

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

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 $t = T/S$. Then the equation becomes

$$u + tu = t^3 - b_2u^2t - b_3u^3,$$

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 Δ is a product of q and a unit in $\mathbb{Z}[[q]][q^{-1}]] = \mathbb{Z}((q))$, the curve defines an elliptic curve E_∞ over $\mathbb{Z}((q))$ 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_∞ mod q is singular only at $(s, t) = (0, 0)$ (which is not the origin of $\overline{E}_\infty = E_\infty$ mod q), and the (completed) stalk $\widehat{\mathcal{O}}_{\overline{E}_\infty, P}$ is isomorphic to $\mathbb{Z}[[t, s]]/(ts)$, which is a regular ring (cf.

[CRT] §19; for example, a Dedekind domain and a power series ring over a Dedekind domain are regular). Thus the local ring at every geometric point of $\overline{E}_{\infty/\mathbb{Z}}$ is a regular ring of dimension two (we call such a curve a regular curve). The smooth locus of $\overline{E}_\infty$ is isomorphic to $\mathbf{P}^1$ removed 2 points, that 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 fact that $E_\infty \mod q = E_\infty \otimes_{\mathbb{Z}[[q]]} \mathbb{Z}[[q]]/(q)$ is as above is obvious 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_∞. The argument computing the Weierstrass equation of elliptic curve does not require full smoothness over the base but only smoothness at the origin and the existence of nowhere vanishing differential (see Subsection 2.2). Thus $E_{\infty/\mathbb{Z}[\frac{1}{6}]}[[q]]$ with the above ω_∞ is determined by a unique Weierstrass equation $y^2 = 4x^3 - g_2(q)x - g_3(q)$ in $\mathbb{Z}[\frac{1}{6}][[q]][x,y]$. By the computation as above, the equation in s,t is even well defined over $\mathbb{Z}[[q]]$.

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 2.1),

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

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

We are going 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, $3[\mathbf{0}] = E_K \cap L_\infty$, 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 (this condition of course determines 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 $\phi(1, 0, 0) = b = 0$; so, L is parallel to s–axis, we have $t = t'$. Thus by the equation (4.8), then assuming $P \neq Q$ (i.e., $s \neq s'$ or equivalently $2P \neq \mathbf{0}$),

$$s^2 + st = s'^2 + s't \iff s + s' = -t.$$

The line L is parallel to s–axis in the (s, t)–plane,

(4.12) $t = t'$ and $s + s' = -t \iff P + Q = -R = \mathbf{0}.$

If $P+Q \neq \mathbf{0}$, then the equation of L can be written as $s = \mu t + \nu$. Again by equation (4.8), we have

$$(4.13) \qquad \mu = \frac{s-s'}{t-t'} = \frac{t^2 + tt' + t'^2 - b_2 - s'}{s + s' + t}$$
$$\nu = s - \mu t = s' - \mu t'.$$

Now we solve, using the above equations, the third solution of $L \cap E_\infty$. We get

$$(4.14) \qquad t'' = \mu^2 + \mu - t - t' \quad \text{and} \quad s'' = -t'' - \mu t'' - \nu.$$

Here is a result in [T1] Theorem 1:

Theorem 4.2 (J. 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 $K^\times/q^\mathbb{Z} \cong E_K(K)$.*

Proof. By definition, we see $t(q,w) - \frac{w}{(1-w)^2}$ 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. In particular, it gives 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 non-zero. Since $(1-w)^3 s(q,w) \equiv w^2 \mod qA$, $(1-w)^3 s(q,w) \in A^\times$ 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 $(1-w)^3 = 0$; 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 is 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', 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 $q_E \in A$; so, it should be valid as 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 $|q| < 1$. 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 (4.10), and by the first assertion,

$$(4.15) \qquad \pi^{-1}(\mathbf{0}) = q^\mathbb{Z}.$$

We take $u, v, w \in K^\times$ with $w = uv$. Since π depends only on the class modulo $q^\mathbb{Z}$ (4.10), we may assume $|q| < |u| \leq 1$ and $1 \leq |v| < |q|^{-1}$. 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, (4.11) and (4.12)

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 (4.12), (4.13) and (4.14), $\pi(u) + \pi(v) = \pi(w)$ is equivalent to the following simultaneous identities:

$$(4.16) \qquad (t - t')^2 t'' = (s - s')^2 + (s - s')(t - t') - (t - t')^2(t + t')$$
$$(t - t')s'' = -(t - t')(s + t'') + (s - s')(t - t'').$$

Assuming $w = uv$, we want to show this identity (4.16) holds for $\pi(u) = P$, $\pi(v) = Q$ and $\pi(w) = R$. Since $w = uv$, (4.16) 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 $K \hookrightarrow \mathbb{C}$ and consider $E_{\mathbb{C}} = E_K \otimes_K \mathbb{C}$ over $\mathbb{C}$, since the identities (4.16) 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 (cf. [T1] Lemma 1). This shows that $\pi : K^{\times}/q^{\mathbb{Z}} \to E_K(K)$ is a homomorphism; 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 (4.15).

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. [T1] 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 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 is 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 $w^{\sigma} = w$. Thus taking $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ invariant of $\overline{\mathbb{Q}}_p^{\times}/q^{\mathbb{Z}} \cong E_A(\overline{\mathbb{Q}}_p)$, we get $K^{\times}/q^{\mathbb{Z}} \cong E_A(K)$ as desired. $\qquad\square$

References

[ALG]   R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[AME]   N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Ann. of Math. Studies, **108**, Princeton University Press, 1985

[BCM]   N. Bourbaki, *Commutative algebra*, Hermann, Paris, 1961-89

[CLC]   J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962

[CRT]   H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, New York, 1986.

[DAV]   G. Faltings and C.-L. Chai, *Degeneration of Abelian Varieties*, Sp-ringer, New York, 1990.

[EEK]   A. Weil, *Elliptic Functions according to Eisenstein and Kronecker*, Springer, 1976

[GME]   H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, Singapore, 2000.

[GZ]   B. Gross and D. Zagier, Heegner points and derivatives of L-series, Inventiones Math. **84** (1986), 225–320

[HAL]   P. J. Hilton and U. Stammback, *A Course in Homological Algebra*, Graduate Text in Math. **4**, Springer, Berlin-Heiderberg-New York-Tokyo, 1970

[Hz]   A. Hurwitz, Ueber die Entwicklungscoefficienten der lemniscatischen Functionen, Göttingen Nachrichten, 1987, 273–276

[IAT]   G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, and Iwanami Shoten, Tokyo, 1971.

[LFE]   H. Hida, *Elementary Theory of L-Functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, England, 1993.

[MFG]   H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000.

[REC]   J. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, 1992, Springer-Verlag, New York

[T]   J. Tate, p-divisible groups, Proc. Conf. on local filds, Driebergen 1966, Springer 1967, 158–183.

[T1]   J. Tate, A review of non-archimedean elliptic functions, in "*Elliptic Curves, Modular Forms, & Fermat's last Theorem*" Series in Number Theory I, International Press, 1995, pp. 162–184

[Wa]   J.-L. Waldspürger, Sur les valeurs de certaines fonctions L-automorphes en leur centre de symétrie. Compositio Mathematica, **54** (1985), 173–242