

Geometric Reciprocity Laws

Since reciprocity laws play an important role in this book, we now describe several reciprocity laws appearing in number theory in terms of automorphism groups of a field fixing a given prime or a given point. Only this chapter contains (elementary) exercises.

To fix our idea, we describe here briefly a model reciprocity law. For a given field \mathfrak{K} , we consider the field automorphism group $\text{Aut}(\mathfrak{K})$ equipped with the Krull topology (which is described in Section 2.3). As is clear from the introduction, a geometric global reciprocity law gives a canonical description of $\text{Aut}(\mathfrak{K})$ by the adelic points of an algebraic (reductive) group G/\mathbb{Q} (modulo rational center $Z(\mathbb{Q})$): $\text{Aut}(\mathfrak{K}) \hookrightarrow \frac{G(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})}$ typically. If a local ring \mathcal{V} with quotient field \mathfrak{K} is given, we could define a decomposition subgroup D of $\text{Aut}(\mathfrak{K})$ (equipped with the Krull topology) by

$$D = \{ \sigma \in \text{Aut}(\mathfrak{K}) \mid \sigma(\mathcal{V}) = \mathcal{V} \},$$

and the local reciprocity law for \mathcal{V} describes D via a well-defined algebraic subgroup H of G . Often D is given by the image of adèle points, $H(\mathbb{A}^{(\infty)})$ (or \mathbb{Q}_p -points, $H(\mathbb{Q}_p)$), of H in $\frac{G(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})}$. This description may involve a subtle use of class field theory, and class field theory supplies us with one of the simplest examples of the reciprocity laws. The global reciprocity law is a particular case of the local one (taking $\mathcal{V} = \mathfrak{K}$). To have such reciprocity laws, the field \mathfrak{K} cannot be finitely generated over its prime subfield except for the case where G is finite. So for an algebraic group G of positive dimension, the reciprocity laws get more geometric flavor, and \mathfrak{K} is then realized as the function field of an infinite tower V of (geometrically irreducible) algebraic varieties defined over a tower of finite extensions over the prime field. Then if we have local reciprocity laws covering sufficiently many points of the tower V , the laws characterize a global model V of \mathfrak{K} (a model of a field K is an algebraic variety whose function field is isomorphic to K in a canonical way). Thus to have a coherent system of local reciprocity laws is almost equivalent to having a well-defined global model of a given function field (of infinite type). Similarly, if V

is minimal, the algebrogeometric automorphism group $\text{Aut}(V)$ of the variety V coincides with $\text{Aut}(\mathfrak{K})$, and hence the tower is realized as a collection of algebraic varieties $\{V_S|V/S\}_S$ for S running through open compact subgroups S of $\text{Aut}(\mathfrak{K})$, where V/S is the quotient variety of V by the action of S . Thus by the global reciprocity law, we can recover each member of the tower. This type of dichotomy appears in the theory of Shimura varieties.

In the later part of the book, we study more modern reciprocity laws (involving reductive groups of positive dimension) principally created by Shimura as an explicit description of automorphisms of Shimura varieties. In this beginning part of the book, we describe some reciprocity laws (including those relating finite groups G with the field automorphism groups) that only require minimal knowledge of algebraic geometry. Our requirement is reasonable knowledge of the theory of algebraic curves over number fields in this chapter. Some of the reciprocity laws are stated here without proof, though in the later chapters proofs are given in a more general setting. It would be a good exercise for the readers to deduce the results described in this chapter from the more elaborate versions in the later chapters. In the following chapter, we extend our scope in order to incorporate integral models of modular curves, and in the later chapters, we study Shimura varieties and their integral models via the language of schemes.

2.1 Sketch of Classical Reciprocity Laws

In this section, we sketch the classical reciprocity laws starting with the historic quadratic reciprocity invented by Euler (and proved by Gauss), and ending with a reciprocity law for a single rational elliptic curve. Here, primes p and q are always distinct odd primes.

2.1.1 Quadratic Reciprocity Law

For an integer n ($p \nmid n$), the Legendre symbol $\left(\frac{n}{p}\right)$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv n \pmod{p} \text{ has a solution,} \\ -1 & \text{otherwise.} \end{cases}$$

Since $x^2 \equiv n \pmod{p}$ has a solution if and only if $n \in (\mathbb{F}_p^\times)^2$ for $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $n \mapsto \left(\frac{n}{p}\right)$ gives an identification of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ with $\{\pm 1\}$; in particular, $n \mapsto \left(\frac{n}{p}\right)$ is a character of the finite multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.

The quadratic reciprocity law guessed by Euler and proven by Gauss,

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \quad (\text{Legendre, 1785}),$$

has an equivalent formulation due to Euler

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \quad (\text{Euler, 1744}),$$

where $p^* = (-1)^{(p-1)/2}p$. For a general odd positive integer n prime to p , define $\left(\frac{p^*}{n}\right) = \prod_q \left(\frac{p^*}{q}\right)^{e(q)}$ if the prime factorization of n is given by $\prod_q q^{e(q)}$. Thus $n \mapsto \left(\frac{p^*}{n}\right)$ is equal to the character: $n \mapsto \left(\frac{n}{p}\right)$.

This character decides how a prime decomposes in $\mathfrak{K} = \mathbb{Q}[\sqrt{p^*}]$. We look into the ring $R = \mathbb{Z}[\sqrt{p^*}] = \mathbb{Z}[X]/(X^2 - p^*)$. In R , a prime ideal (q) of \mathbb{Z} could remain prime or become a product of two prime ideals; that is, $(q) = \mathfrak{q}\mathfrak{q}'$ or $(q) = \mathfrak{q}$ for prime ideals $\mathfrak{q}, \mathfrak{q}'$ in R . Note that $R/(q) = \mathbb{F}_q[X]/(X^2 - p^*)$. The polynomial $X^2 - p^*$ is reducible in $\mathbb{F}_q[X]$ if and only if it has a solution in \mathbb{F}_q :

$$(q) = \mathfrak{q}\mathfrak{q}' \iff R/(q) \cong \mathbb{F}_q \oplus \mathbb{F}_q \iff \left(\frac{p^*}{q}\right) = 1,$$

where \mathfrak{q} is the kernel of the projection of R onto the first factor \mathbb{F}_q of $\mathbb{F}_q \oplus \mathbb{F}_q$.

The nontrivial automorphism σ of $\mathbb{Q}[\sqrt{p^*}]$ interchanges the roots of $X^2 - p^*$ and interchanges \mathfrak{q} and \mathfrak{q}' ; so, $\mathfrak{q}' = \sigma(\mathfrak{q})$. Identifying $\{\pm 1\}$ with $\text{Aut}(\mathfrak{K}) = \text{Gal}(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q})$, $\left(\frac{p^*}{q}\right)$ gives the generator of the subgroup of $\text{Aut}(\mathfrak{K})$ fixing a prime factor of (q) .

If $(q) = \mathfrak{q}$ remains prime, $\dim_{\mathbb{F}_q} R/(q) = 2$, and $\sigma(\mathfrak{q}) = \mathfrak{q}$. The stabilizer of \mathfrak{q} is the entire Galois group, and $\langle \left(\frac{p^*}{q}\right) \rangle = \{\pm 1\} \cong \text{Aut}(\mathfrak{K})$ gives the stabilizer.

In summary, identifying $\text{Aut}(\mathfrak{K})$ with $\{\pm 1\}$, the subgroup generated by $\left(\frac{p^*}{q}\right)$ gives the stabilizer of a prime ideal $\mathfrak{q}|q$ in R (in other words, the stabilizer of the \mathfrak{q} -adic valuation ring \mathcal{V} of \mathfrak{K}). The stabilizer is called the decomposition subgroup of q . The information of the decomposition group of q is equivalent to knowing how the prime (q) splits in R .

2.1.2 Cyclotomic Version

In the mid nineteenth century, Kummer extended the quadratic reciprocity law to cyclotomic fields (in his study of decomposition of prime numbers into a product of his “ideal” prime numbers). Let μ_p be the group of all p th roots of unity, and consider the extension $\mathfrak{K} = \mathbb{Q}[\mu_p]$ generated by p th roots of unity. Fixing one primitive root of unity, say, $\zeta = \zeta_p = \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$, μ_p is a cyclic group of order p generated by ζ_p . Each automorphism σ of μ_p takes ζ to another primitive root of unity ζ^m . Since ζ^m is primitive, $p \nmid m$ and hence, we have an identification $\text{Aut}(\mu_p) \cong \mathbb{F}_p^\times$ by $\chi_p : \sigma \mapsto m$. Actually the finite flat group scheme μ_p over \mathbb{Q} is the model of its function field $\mathfrak{K} = \mathbb{Q}[\mu_p]$, and $\text{Aut}(\mathfrak{K}) = \text{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q}) = \text{Aut}(\mu_p)$. Since $\sigma \in \text{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})$ induces an

element in $\text{Aut}(\mu_p)$ (and $[\mathbb{Q}[\mu_p] : \mathbb{Q}] = |\mathbb{F}_p^\times|$), we see that $\text{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q}) \cong \mathbb{F}_p^\times$ by χ_p . We write $\phi_q \in \text{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})$ with $\chi_p(\phi_q) = q$; so, $\phi_q(\zeta) = \zeta^q$.

Again we ask how a prime (q) decomposes in the ring $R = \mathbb{Z}[\mu_p]$. Pick a prime ideal $\mathfrak{q}|q$ in R ; we find that R/\mathfrak{q} is a finite extension of \mathbb{F}_q ; so, it is of the form \mathbb{F}_{q^f} for $f = \dim_{\mathbb{F}_q} R/\mathfrak{q}$. The Galois group $\text{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ is a cyclic group of order f generated by a canonical generator F taking $x \in \mathbb{F}_{q^f}$ to $x^q \in \mathbb{F}_{q^f}$; thus, the automorphism F of \mathbb{F}_{q^f} is induced by ϕ_q . In other words,

- The decomposition group of $\mathfrak{q}|q$ is given by $\langle \phi_q \rangle \cong \langle q \rangle \subset \mathbb{F}_p^\times$, and
- q is of order f in $\mathbb{F}_p^\times \iff (q) = \mathfrak{q}\sigma(\mathfrak{q}) \cdots \sigma^{g-1}(\mathfrak{q})$ in R for the integer $g = [\mathbb{Q}[\mu_p] : \mathbb{Q}]/f$,

where σ is the generator of $\text{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})/\langle \phi_q \rangle$. Thus one feature of the reciprocity law is the determination of the decomposition group of a given prime q in a given Galois extension K/\mathbb{Q} .

2.1.3 Geometric Interpretation

To further generalize the law, we need to ponder a philosophical reason why we have such an arithmetic way of describing the decomposition group. One feature of the cyclotomic version is the existence of a canonical generator ϕ_q (the *Frobenius element* at q) of the decomposition group, and another is the appearance of the exponential function $\exp(z)$, which has the following fundamental identity,

$$\exp\left(2\pi i \frac{1}{p}\right)^{\phi_q} = \phi_q(\zeta) = \zeta^q = \exp\left(2\pi i \frac{q}{p}\right).$$

So, roughly, the complex analytic function $\exp : \mathbb{C} \rightarrow \mathbb{C}^\times$ contains all the information of the reciprocity law, and $\exp\left(2\pi i \frac{1}{p}\right)$ gives a canonical generator ζ of the field $\mathbb{Q}[\mu_p]$ and behaves nicely under its Galois conjugation.

The function \exp gives rise to the following exact sequence,

$$0 \longrightarrow 2\pi i\mathbb{Z} \longrightarrow \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \rightarrow 1,$$

and thus we evaluated the function \exp at the fraction $2\pi i \frac{1}{p} \in \frac{1}{p}2\pi i\mathbb{Z}/2\pi i\mathbb{Z}$. The period $2\pi i$ of the exponential function “ \exp ” is important to ensure that the value of “ \exp ” on $2\pi i\mathbb{Q}$ is algebraic, and we have $2\pi i = \int_\gamma \frac{dt}{t}$ for the unit circle γ which generates the fundamental group $\pi_1(\mathbb{C}^\times) = H_1(\mathbb{C}^\times, \mathbb{Z})$.

Hilbert asked in his twelfth problem (of his famous lecture in 1900 at the International Congress of Mathematicians held in Paris; [H1]), for a given Galois extension (actually an abelian extension in his original setting),

Is there any complex analytic function which describes fully the reciprocity law of the extension?

2.1.4 Kronecker's Reciprocity Law

In the language of Poincaré, the fundamental group of \mathbb{C}^\times is given by \mathbb{Z} , and the universal covering of \mathbb{C}^\times is given by $\mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times$. We can create such a situation starting with an imaginary quadratic field $M = \mathbb{Q}[\sqrt{-D}]$ with discriminant $-D < 0$ in place of \mathbb{Q} . For any given ideal $\mathfrak{a} \subset R$ (for the integer ring $R \subset M$) and a period $\Omega \in \mathbb{C}^\times$, we consider an exact sequence:

$$0 \longrightarrow \Omega \mathfrak{a} \longrightarrow \mathbb{C} \xrightarrow{(\mathcal{P}, \mathcal{P}')} E(\mathbb{C}) \longrightarrow 0.$$

For the moment $E(\mathbb{C})$ is a quotient space \mathbb{C}/\mathfrak{a} , which is a Riemann surface of genus 1. The period Ω of the elliptic curve E is inserted here to ensure that the value on ΩM of the Weierstrass functions \mathcal{P} and \mathcal{P}' (as defined below) are algebraic. Writing ω for the (translation-) invariant differential on $E(\mathbb{C})$ induced by du for the variable u of \mathbb{C} , we have $\Omega = \int_\gamma \omega$ for the generator γ of $\pi_1(E(\mathbb{C})) = H_1(E(\mathbb{C}), \mathbb{Z}) = \mathfrak{a}\gamma$ just as before. Indeed, for an \mathbb{R} -base (w_1, w_2) of \mathbb{C} , we can think of $E_L(\mathbb{C}) = \mathbb{C}/L$ for $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ replacing \mathfrak{a} by L .

Weierstrass studied analysis and geometry of Riemann surfaces (transforming Riemann's marvelous but rather intuitive ideas into a rigorous mathematics). In particular, for the Riemann surface $E(\mathbb{C})$ of genus 1, he created the following function well-defined over $E(\mathbb{C})$,

$$x(u) = \mathcal{P}(u) = \frac{1}{u^2} + \sum_{\ell \in L - \{0\}} \left(\frac{1}{(u - \ell)^2} - \frac{1}{\ell^2} \right),$$

averaging the translations of $\frac{1}{u^2}$ over L , which is a two-dimensional analogue of the partial fraction expansion of the cotangent function (see [LFE] 2.1):

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left\{ \frac{1}{z+n} + \frac{1}{z-n} \right\}.$$

This function converges absolutely over $\mathbb{C} - L$ and gives a meromorphic function on $E(\mathbb{C})$. The Laurent expansion of \mathcal{P} and its derivative can be easily computed, and we have

$$x(u) = \mathcal{P}(u) = \frac{1}{u^2} + \frac{g_2}{20}u^2 + \frac{g_3}{28}u^4 + \cdots, \quad y(u) = \mathcal{P}'(u) = -\frac{2}{u^3} + \sum_{n \geq 1} a_n u^n,$$

where $g_2 = g_2(L) = 60 \sum_{\ell \neq 0} \ell^{-4}$ and $g_3 = g_3(L) = 140 \sum_{\ell \neq 0} \ell^{-6}$. The constants g_2 and g_3 are actually complex analytic functions of $w = (w_1, w_2)$.

Canceling the poles, we consider $\varphi = y^2 - 4x^3 + g_2x + g_3$ which is holomorphic everywhere on a compact Riemann surface $E(\mathbb{C})$; so, it has to be constant. The function φ has to be identically 0, because φ has no constant term. Thus $u \mapsto \mathbf{E}(u) = (u^3x(u), u^3y(u), u^3) \in \mathbf{P}^2$ embeds the Riemann surface into the projective space of dimension 2, whose image is an algebraic curve (called an *elliptic curve*) defined by the homogeneous equation:

$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ ($x = X/Z$ and $y = Y/Z$). We write $\Delta = g_2^3 - 27g_3^2$ for the discriminant of $4x^3 - g_2x - g_3$.

If we pick $\lambda \in \mathbb{C}^\times$, we have a biholomorphic isomorphism of Riemann surfaces: $u \mapsto \lambda u$ of $E_L(\mathbb{C}) \cong E_{\lambda L}(\mathbb{C})$. By definition, $g_i(\lambda L) = \lambda^{-2i}g_i(L)$ and $\Delta(\lambda L) = \lambda^{-12}\Delta(L)$. We have $j(\lambda L) = j(L)$ for the j -invariant defined by $j(w) = j(L) = \frac{g_2^3}{\Delta}$. The following facts are known from the general theory of algebraic curves and are proven in this chapter.

- If $\phi : E_L \rightarrow E_{L'}$ is a holomorphic homomorphism with $\phi(0) = 0$, then there exists $\lambda \in \mathbb{C}^\times$ such that $L' \supset \lambda L$ and $\phi(u+L) = (\lambda u + L')$ (Theorem 2.39);
- Write a morphism $\phi : E_L \rightarrow E_{L'}$ as $\phi(u) = (\phi_x(u), \phi_y(u), 1)$ using the coordinates of the projective space \mathbf{P}^2 . Then ϕ_x and ϕ_y are rational functions of x_L and y_L ; that is, $\phi_x = \frac{A(x,y,g_2,g_3)}{B(x,y,g_2,g_3)}$ and $\phi_y = \frac{\alpha(x,y,g_2,g_3)}{\beta(x,y,g_2,g_3)}$ for polynomials A, B, α, β with coefficients in \mathbb{Q} independent of L (Corollary 2.26);
- Every genus 1 Riemann surface is obtained as E_L for an L (Theorem 2.39);
- $E_{L/\mathbb{C}} \cong E_{L'/\mathbb{C}} \iff j(L) = j(L')$ (Corollary 2.35).

The function j is an example of a *modular function* and g_2 and g_3 are examples of *modular forms*. Modular forms are a special kind of automorphic forms defined on a more general complex domain.

For a given number field F , the maximal everywhere unramified abelian extension H/F is called the Hilbert class field. Kronecker studied the Hilbert class field H of the imaginary quadratic field M . Take a prime \mathfrak{p} of the integer ring R of M and its prime factor \mathfrak{P} in the integer ring O_H of H . The decomposition group $D_{\mathfrak{P}'} = \{\sigma \in \text{Gal}(H/M) \mid \sigma(\mathfrak{P}') = \mathfrak{P}'\}$ for any other prime factor $\mathfrak{P}' \mid \mathfrak{p}$ is a conjugate of $D_{\mathfrak{P}}$ (as is well known). Since $\text{Gal}(H/M)$ is abelian, the group $D_{\mathfrak{P}}$ is uniquely determined independently of the factor \mathfrak{P} of \mathfrak{p} ; so, we write $D_{\mathfrak{p}}$ for $D_{\mathfrak{P}}$. Since H/M is unramified (at \mathfrak{p}), $D_{\mathfrak{p}} \cong \text{Gal}(K/k)$ for the residue fields $K = O_H/\mathfrak{P}$ and $k = R/\mathfrak{p} = \mathbb{F}_q$ for a prime power q . The Frobenius automorphism $\phi_{\mathfrak{p}} \in D_{\mathfrak{p}}$ sending $x \in K$ to $x^q \in K$ gives a canonical generator of the Galois group $\text{Gal}(K/k)$. What Kronecker found is

Theorem (Kronecker–Weber) *Let H/M be the Hilbert class field of M . Then $H = M[j(\mathfrak{a})]$ for any ideal $0 \neq \mathfrak{a} \subset R$ and $j(\mathfrak{a})^{\phi_{\mathfrak{p}}} = j(\mathfrak{p}^{-1}\mathfrak{a})$. In particular, $\text{Gal}(H/M)$ is isomorphic to the ideal class group of M .*

Proof. We give a sketch of a proof. We first explain why $j(\mathfrak{a})$ is an algebraic number. If $\text{End}(E_L)$ contains the integer ring R of an imaginary quadratic field M , then $RL \subset L$; so, $L \subset \Omega M$ for $0 \neq \Omega \in L$. Via multiplication by Ω , $\mathbb{C}/\mathfrak{a} \cong \mathbb{C}/L$ for $\mathfrak{a} = \Omega^{-1}L$. Thus we may assume that L is an ideal \mathfrak{a} of M . Since the isomorphism class of $E_{\mathfrak{a}}$ only depends on \mathfrak{a} up to scalar multiplication, there are only countably many isomorphism classes of E_L with $\text{End}(E_L) \supset R$. Regard $E_{\mathfrak{a}}$ as a curve defined by the equation $y^2 = 4x^3 - g_2x - g_3$, and consider its conjugate $E_{\mathfrak{a}}^{\sigma}$ defined by $y^2 = 4x^3 - \sigma(g_2)x - \sigma(g_3)$ for any field automorphism σ of \mathbb{C} . Then $\text{End}(E_{\mathfrak{a}}^{\sigma})$ contains R because all endomorphisms are rational functions of (x, y, g_2, g_3) ; so, applying σ to their coefficients, we

get an endomorphism $\phi^\sigma \in \text{End}(E_a^\sigma)$ from $\phi \in \text{End}(E_a)$. The morphism $\phi \mapsto \phi^\sigma$ is an isomorphism of rings. Thus $E_a^\sigma = E_b$ for an ideal b in M and $j(a)^\sigma = j(b)$; so, $j(a)$ has only countably many conjugates. This implies that they are finitely many, because if $x \in \mathbb{C}$ is transcendental over \mathbb{Q} , one can embed $\mathbb{Q}(x)$ into \mathbb{C} in continuously many different ways (\mathbb{C} has continuously many transcendental numbers). Thus the number of conjugates of $j(a)$ is finite, and hence $j(a)$ is algebraic. Since $j(b) = j(a)$ if and only if $b = \alpha a$ for some $\alpha \in M^\times$, the fractional ideals of M modulo scalar multiplication are finitely many. For a given j , we can create a Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$ in $\mathbb{Q}(j)[x, y]$ with invariant j , for example, if $j \notin \{0, 1\}$, we put $g_2 = g_3 = \frac{27j}{j-1}$ (see just above Corollary 2.35 in the text or [IAT] 4.1). In other words, by choosing the period Ω as $\Omega = \int_\gamma \frac{dx}{y} = \int_\gamma \omega \in \mathbb{C}^\times$, we have

$$\Omega^{-4}g_2(a) = g_2(\Omega a) = \frac{27j}{j-1} = g_3(\Omega a) \in \overline{\mathbb{Q}}.$$

For almost all prime ideals \mathfrak{P} of $\mathbb{Q}(j(a))$, g_2 and g_3 are \mathfrak{P} -integral with $\Delta(a) \not\equiv 0 \pmod{\mathfrak{P}}$, and the equation modulo \mathfrak{P} gives rise to an elliptic curve \tilde{E}_a defined over a finite field \mathbb{F} . The relative Frobenius map $F : (x, y) \mapsto (x^p, y^p)$ sends \tilde{E}_a to another elliptic curve $\tilde{E}_a^{(p)}$ defined by $y^2 = 4x^3 - g_2^p x - g_3^p \in \mathbb{F}[x, y]$. Suppose that $(p) = \mathfrak{P} \cap \mathbb{Z}$ is split into $\mathfrak{p}\bar{\mathfrak{p}}$ in the imaginary quadratic field M . Then the group of p -torsion points $E_a[p]$ is the direct sum of the group of \mathfrak{p} -torsion points and that of $\bar{\mathfrak{p}}$: $E_a[p] = E_a[\mathfrak{p}] \oplus E_a[\bar{\mathfrak{p}}]$. As is well known (cf. [GME] 2.9.1), we can choose \mathfrak{p} uniquely so that $\tilde{E}_a[\mathfrak{p}] \cong R/\mathfrak{p}$ having p distinct points. Since $F : \tilde{E}_a \rightarrow \tilde{E}_a^{(p)}$ is a homomorphism of groups that is a zero map on the tangent space, it induces a group isomorphism $E_a(\overline{\mathbb{F}}) \cong E_a^{(p)}(\overline{\mathbb{F}})$ (though not a scheme isomorphism), and hence $\tilde{E}_a^{(p)} \cong \tilde{E}_{\mathfrak{p}^{-1}a}$, because $p : \tilde{E}_a \rightarrow \tilde{E}_a$ is an endomorphism (see [GME] 2.9.1) which factors $\tilde{E}_a \xrightarrow{F} \tilde{E}_a^{(p)} \xrightarrow{V} \tilde{E}_a$ with $\text{Ker}(V) = \tilde{E}_a^{(p)}[\mathfrak{p}] = \mathfrak{p}^{-1}a/a$. This shows that $j(a)^{\phi_p} = j(\mathfrak{p}^{-1}a)$. Since $j(a)$ characterizes the isomorphism class of E_a (over $\overline{\mathbb{Q}}$), we know that the $j(a)$ s indexed by $a \in Cl_M$ for the ideal class group Cl_M of M are all distinct. Since in each class of Cl_M , we can find split \mathfrak{p} outside a given finite set of primes of M (the Chebotarev density), we find that $\{j(a)\}_{a \in Cl_M}$ are all conjugates of each other over M ; so, they span the Hilbert class field H/M . This proves the above theorem (and finiteness of Cl_M).

By the theorem (or its proof), $\text{Gal}(H/M) \cong Cl_M$. This is the explicit class field theory for the imaginary quadratic field M . This type of result is generalized by Shimura, Taniyama, and Weil to *CM fields*, using a quotient \mathbb{C}^d/L for a lattice L of higher rank (theory of abelian varieties with complex multiplication; see Theorem 4.19 in the text, [IAT] Chapter 5, and [ACM]). A CM field means a totally imaginary quadratic extension of a totally real field.

2.1.5 Reciprocity Law for Elliptic Curves

We can slightly generalize the above construction. Let

$$E_L[p] = \{u \in E_L(\mathbb{C}) \mid pu = 0\} = \frac{1}{p}L/L \cong \mathbb{F}_p^2.$$

Note that $\mathbf{E}(0) = (0, -2, 0) \in \mathbf{P}^2(\mathbb{Q})$, and hence the point 0 of E_L does not move after applying $\sigma \in \text{Aut}(\mathbb{C})$. Then $\sigma \in \text{Aut}(\mathbb{C})$ brings $p : E_L \rightarrow E_L$ to $p : E_L^\sigma \rightarrow E_L^\sigma$ because they are rational functions of (x, y, g_2, g_3) ; so, if E_L is defined over a number field $M' = \mathbb{Q}[g_2(L), g_3(L)]$, $\sigma \in \text{Aut}(\mathbb{C}/M')$ induces a linear automorphism of $E_L[p]$. Taking a base $\mathbf{w} = (\frac{w_1}{p}, \frac{w_2}{p})$ of $E_L[p]$, we find $\sigma(\mathbf{w}) = \mathbf{w}\rho(\sigma)$ for a 2×2 matrix $\rho(\sigma) \in GL_2(\mathbb{F}_p)$, and so, we can identify $\text{Gal}(M'(E_L[p])/M')$ with a subgroup $\text{Im}(\rho)$ of $GL_2(\mathbb{F}_p)$. Here $M'(E_L[p])$ is the field generated by $x(\frac{w_i}{p})$ and $y(\frac{w_i}{p})$ ($i = 1, 2$) over M' . Thus identifying $E_L[p]$ with the column vector space \mathbb{F}_p^2 by ${}^t(a, b) \mapsto \mathbf{w}^t(a, b) \in E_L[p]$, we have

$$x(\rho(\sigma)v) = x(v)^\sigma \quad \text{and} \quad y(\rho(\sigma)v) = y(v)^\sigma.$$

This reciprocity law is still half baked, because we have not made explicit the form of $\rho(\phi_{\mathfrak{q}})$ for the canonical generator $\phi_{\mathfrak{q}}$ of the decomposition group of a prime \mathfrak{q} of M' . This can be done when L is a fractional ideal of an imaginary quadratic field, and the refined version is an example of Shimura's reciprocity laws (although the origin of this reciprocity goes back to Kronecker). When L is not in an imaginary quadratic field, $\text{Im}(\rho)$ is almost always full (by a result of Serre; see [ARE] and [Se2]), and we can (conjecturally for general $M' \neq \mathbb{Q}$) make explicit $\text{Tr}(\rho(\phi_{\mathfrak{q}}))$ and $\det(\rho(\phi_{\mathfrak{q}}))$ (see [GME] 5.2.4). However this information is still a bit short of completely determining the splitting of a prime \mathfrak{q} in $M'(E_L[p])$ (see [Sh2]), and the analysis of the Galois representation $\rho : \text{Gal}(M'(E_L[p])/M') \hookrightarrow GL_2(\mathbb{F}_p)$ is still a central subject today.

From what I said, it is clear that *the study of modular functions and modular forms (and their generalization, often called automorphic forms) is natural and crucial in algebraic number theory*, though they appear to be rather analytic and geometric objects.

2.2 Cyclotomic Reciprocity Laws and Adeles

We now give a more detailed description of the cyclotomic reciprocity laws and relate them to the idele class group of \mathbb{Q} . This fact was found basically by Kronecker and is one of the simplest examples of the reciprocity laws in class field theory.

2.2.1 Cyclotomic Fields

We look into the exponential function $\mathbf{e} : \mathbb{C} \rightarrow \mathbb{C}^\times$ given by $\mathbf{e}(z) = \exp(2\pi iz)$. For a positive integer N , we write $\zeta = \zeta_N = \mathbf{e}(\frac{1}{N})$. Then ζ is a primitive

N th root of unity. When N is a prime p , it satisfies the equation $X^p - 1 = (X - 1)\Phi_p(X) = 0$ for $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$. Since $\zeta \neq 1$, $\Phi_p(\zeta) = 0$.

Proposition 2.1 *The cyclotomic polynomial $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.*

Proof. The irreducibility of Φ_p and $\Psi(X) = \Phi_p(X + 1)$ is equivalent. We see easily that the constant term is given by $\Psi(0) = \Phi_p(1) = p$. Since $(X + 1)^p - 1 = X\Psi(X) \equiv X^p \pmod{p}$, by the Eisenstein criterion, $\Psi(X)$ is irreducible. \square

Corollary 2.2 *The equation $\Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}})$ for an integer $n \geq 1$ is irreducible in $\mathbb{Q}[X]$.*

The proof of this corollary is left to the reader as an exercise.

Corollary 2.3 *Let $N = p^n$ for a prime p . The cyclotomic field $\mathbb{Q}[\zeta_N]$ is a Galois extension of \mathbb{Q} whose Galois group is abelian. We have a canonical isomorphism of groups $\chi = \chi_N : \text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ given by $\sigma(\mathbf{e}(\frac{1}{N})) = \mathbf{e}(\frac{\chi(\sigma)}{N})$ for $\sigma \in \text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q})$.*

Proof. Let μ_N be the group of N th roots of unity. Then \mathbf{e} induces an isomorphism $\iota : \mathbb{Z}/N\mathbb{Z} \cong \mu_N$ of groups by $m \mapsto \mathbf{e}(\frac{m}{N})$. Since $\sigma(\zeta_N)$ is another primitive N th root for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ($\overline{\mathbb{Q}}$ is the algebraic closure of \mathbb{Q} in \mathbb{C}), σ induces an automorphism of the field $\mathbb{Q}[\zeta_N]$ because $\sigma(\zeta_N)$ is again a power of ζ_N . Thus $\mathbb{Q}[\zeta_N]/\mathbb{Q}$ is a Galois extension. Since $\text{Aut}(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^\times$ (multiplicative group) by $\phi \mapsto \phi(1)$, we find $\chi = \chi_N : \text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q}) \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$. If $\sigma \in \text{Ker}(\chi)$, σ fixes all N th roots of unity; so, χ is injective. Its p -component χ_{p^n} has to be surjective, since

$$|\text{Gal}(\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q})| = [\mathbb{Q}[\zeta_{p^n}] : \mathbb{Q}] = \deg(\Phi_{p^n}) = p^{n-1}(p-1) = |(\mathbb{Z}/p^n\mathbb{Z})^\times|. \quad \square$$

We show later the surjectivity of χ_N for general N (see Theorem 2.8).

Corollary 2.4 *Let $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \not\equiv 0 \pmod{p}\}$. Then the integral domain $\mathcal{V} = \mathbb{Z}_{(p)}[X]/(\Phi_{p^n}(X))$ is a discrete valuation ring whose maximal ideal is generated by $\varpi = \zeta_{p^n} - 1$, where ζ_{p^n} is the image of X in \mathcal{V} (so, it is a primitive p^n th root of unity which can be identified with $\mathbf{e}(\frac{1}{p^n})$). The valuation ring \mathcal{V} is fully ramified over $\mathbb{Z}_{(p)}$, that is, $(\varpi)^{[\mathcal{V}:\mathbb{Z}_{(p)}]} = (p)$.*

Proof. By the fundamental theorem of arithmetic, any $x = \frac{a}{b}$ can be written as $p^{v(x)}y$ for $y = \frac{d}{c}$ with $p \nmid c$ and $p \nmid d$; so, $y^{-1} \in \mathbb{Z}_{(p)}$. Thus $v : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}$ gives the valuation of \mathbb{Q} and $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v(x) \geq 0\}$; so, $\mathbb{Z}_{(p)}$ is a discrete valuation ring of \mathbb{Q} .

Let $\varpi = \zeta_p - 1$, and let $\mathcal{V} = \mathbb{Z}_{(p)}[X]/(\Phi_p(X))$. Since $\Psi(X) \equiv X^{p-1} \pmod{p}$, we see that $\mathcal{V}/(p) \cong \mathbb{F}_p[X]/(X^{p-1})$. Then

$$(1) \supset (X) \supset (X^2) \supset \cdots \supset (X^{p-1}) = (0)$$

are the only ideals of $\mathcal{V}/(p)$, because $(a_j X^j + a_{j+1} X^{j+1} + \dots + a_{p-1} X^{p-1}) = (X)^j$ if $a_j \neq 0$ in \mathbb{F}_p . Since $p = \Psi(0) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})} \sigma(\varpi)$, we find that $(\varpi) \supset (p)$. Then by the homomorphism theorem applied to $\mathcal{V} \twoheadrightarrow \mathcal{V}/(p)$, only ideals between (p) and (ϖ) are $(\varpi)^m$ for $m = 1, 2, \dots, p-1$. By induction on n , one can show that

$$(1) \supset (X) \supset (X^2) \supset \dots \supset (X^{n(p-1)}) = (0)$$

are the only ideals of $\mathcal{V}/(p^n)$. For a given ideal $\mathfrak{a} \subset \mathcal{V}$, $\mathfrak{a} \cap \mathbb{Z}_{(p)} = (p^\ell)$ because $\mathbb{Z}_{(p)}$ is a discrete valuation ring (DVR). Thus $\mathfrak{a} = (\varpi)^m$ for $0 \leq m \leq \ell(p-1)$. This shows that \mathcal{V} is a DVR with valuation w given by $w(x) = n \iff (x) = (\varpi)^n$. The same argument as above works well for $\mathcal{V} = \mathbb{Z}_{(p)}[X]/(\Phi_{p^n}(X))$ for $\varpi = \zeta_{p^n} - 1$, since $\Phi_{p^n}(X+1) \equiv X^{p^{n-1}(p-1)} \pmod{p}$. \square

Let \mathcal{V} be a DVR. Then we can extend the valuation v of \mathcal{V} to its field of fractions K by $v(\frac{a}{b}) = v(a) - v(b)$. In other words, $\mathcal{V} = \{x \in K \mid v(x) \geq 0\}$. For any $x \in K$, we have either $x \in \mathcal{V}$ or $x^{-1} \in \mathcal{V}$. In particular, if $x \in K$ is integral over \mathcal{V} , then x satisfies an equation

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \iff 1 = -a_1 x^{-1} - a_2 x^{-2} - \dots - a_n x^{-n}$$

with $a_j \in \mathcal{V}$. If $x \notin \mathcal{V}$, $v(x) < 0 \iff v(x^{-1}) > 0$, and

$$0 = v(1) = v(-a_1 x^{-1} - a_2 x^{-2} - \dots - a_n x^{-n}) \geq \min_j (v(a_j) + jv(x^{-1})) > 0,$$

which is a contradiction; so, $x \in \mathcal{V}$, and \mathcal{V} is integrally closed. In particular $\mathbb{Z}_{(p)}[\zeta_{p^n}]$ is the integral closure of $\mathbb{Z}_{(p)}$, and (p) fully ramifies in $\mathbb{Z}_{(p)}[\zeta_{p^n}]$.

2.2.2 Cyclotomic Reciprocity Laws

Let q be a prime different from p . We now look into $\mathcal{V}_q = \mathbb{Z}_{(q)}[X]/(\Phi_{p^n}(X)) = \mathbb{Z}_{(q)}[\zeta_{p^n}]$. We look into $\bar{\Phi}_{p^n}(X) = (\Phi_{p^n}(X) \pmod{q}) \in \mathbb{F}_q[X]$. Then $\mathcal{V}_q/q\mathcal{V}_q = \mathbb{F}_q[X]/(\bar{\Phi}_{p^n}(X))$ and $\dim_{\mathbb{F}_q} \mathcal{V}_q/q\mathcal{V}_q = \text{rank}_{\mathbb{Z}_{(q)}} \mathcal{V}_q = \deg(\Phi_{p^n}(X))$. Since we have $p^{n-1}(p-1)$ distinct primitive p^n th roots of unity in $\bar{\mathbb{F}}_q$, $\bar{\Phi}_{p^n}(X)$ does not have multiple roots, and we see $\mathcal{V}_q/q\mathcal{V}_q \cong \mathbb{F}_{q^{f_1}} \oplus \mathbb{F}_{q^{f_2}} \oplus \dots \oplus \mathbb{F}_{q^{f_g}}$. The image of X in $\mathbb{F}_{q^{f_j}}$ is a primitive p^n th root $\alpha = \alpha_j$ of unity in $\mathbb{F}_{q^{f_j}}$, and $\mathbb{F}_{q^{f_j}} = \mathbb{F}_q[\alpha]$. Thus $f = f_1 = f_2 = \dots = f_g$ is the minimal exponent so that \mathbb{F}_{q^f} contains a primitive p^n th root of unity. Since $\mathbb{F}_{q^f}^\times$ is made up of $(q^f - 1)$ th roots of unity, f is the minimal exponent such that $p^n \mid q^f - 1$. The ideal $\mathfrak{q}_j = \text{Ker}(\pi_j)$ for each projection $\pi_j : \mathcal{V}_q \twoheadrightarrow \mathcal{V}_q/q\mathcal{V}_q \twoheadrightarrow \mathbb{F}_{q^{f_j}}$ is a prime of \mathcal{V}_q , and we have

$$(q) = \prod_{j=1}^g \mathfrak{q}_j \quad \text{and} \quad fg = [\mathcal{V}_q/q\mathcal{V}_q : \mathbb{F}_q] = \deg(\Phi_{p^n}) = p^{n-1}(p-1).$$

Summing up, we get

Proposition 2.5 *Each prime $q \neq p$ decomposes into a product $(q) = \prod_{j=1}^g \mathfrak{q}_j$ of prime ideals \mathfrak{q}_j with $\mathcal{V}_q/\mathfrak{q}_j \cong \mathbb{F}_{q^f}$ for the minimal exponent f with $p^n | q^f - 1$. We also have $fg = p^{n-1}(p-1)$.*

Let $\mathfrak{q} = \mathfrak{q}_j$. Then $\mathcal{V}_q/\mathfrak{q}\mathcal{V}_q = \mathbb{F}_{q^f}$. Since $\text{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ is a cyclic group of order f generated by ϕ_q given by $\phi_q(x) = x^q$, it is induced by an element $\phi_q \in \text{Gal}(\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q})$ with $\chi_{p^n}(\phi_q) = q$. In other words, the stabilizer of \mathfrak{q} is given by $D_q = \langle \phi_q \rangle \subset G = \text{Gal}(\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q})$ generated by ϕ_q . We have an injection $G/D_q \hookrightarrow \{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$ by $\sigma D_q \mapsto \sigma(\mathfrak{q})$. Since $|D_q| = |\text{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)| = f$, the image has $[\mathbb{Q}[\zeta_{p^n}]:\mathbb{Q}]/f = g$ elements; so, we get

$$\text{Gal}(\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q})/D_q \cong \{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}.$$

We have proven:

Theorem 2.6 (Cyclotomic Reciprocity) *If $q \neq p$ is a prime, then for each prime factor \mathfrak{q} in $\mathbb{Z}_{(q)}[\zeta_{p^n}]$, the decomposition subgroup of \mathfrak{q} in $G = \text{Gal}(\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q})$: $D_q = \{\sigma \in G | \sigma(\mathfrak{q}) = \mathfrak{q}\}$ is given by the cyclic subgroup $\langle \phi_q \rangle$ generated by the Frobenius element ϕ_q with $\chi_{p^n}(\phi_q) = q$. In particular, $(q) = \prod_{\sigma \in G/D_q} \sigma(\mathfrak{q})$ and $\mathcal{V}_q/\mathfrak{q} \cong \mathbb{F}_{q^f}$ for the order f of q in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.*

Let \mathcal{V}_q be the localization of \mathcal{V}_q at \mathfrak{q} . Since $\prod_j \mathfrak{q}_j = (q)$ in \mathcal{V}_q , we find that $\mathfrak{q}\mathcal{V}_q = (q)$, which is a unique maximal ideal. Thus $\mathfrak{q}^m/\mathfrak{q}^{m+1} \cong \mathcal{V}_q/\mathfrak{q} = \mathbb{F}_{q^f}$ is a field; so, there is no ideal between \mathfrak{q}^m and \mathfrak{q}^{m+1} in \mathcal{V}_q . If \mathfrak{a} is an ideal of \mathcal{V}_q , $\mathfrak{a} \cap \mathbb{Z}_{(q)} = \mathfrak{q}^m$; so, $\mathfrak{a} = \mathfrak{q}^m$. In other words, all ideals of \mathcal{V}_q are given by

$$\mathcal{V}_q \supset \mathfrak{q} = (q) \supset \mathfrak{q}^2 = (q^2) \supset \mathfrak{q}^3 \supset \dots \supset (0).$$

Therefore \mathcal{V}_q is a discrete valuation ring. We have $\mathcal{V}_q \subset \cap_{\mathfrak{q}|q} \mathcal{V}_q$. If $\frac{b}{a} \in \mathbb{Q}[\zeta_{p^n}]$ for $a, b \in \mathcal{V}_q$ is in the intersection, then a is prime to \mathfrak{q} for all $\mathfrak{q}|q$; thus, a is prime to q . This implies $\mathcal{V}_q = \cap_{\mathfrak{q}|q} \mathcal{V}_q$, and \mathcal{V}_q is integrally closed (Exercise 3).

Since $\zeta = \zeta_{p^n}$ is defined by the relation

$$1 + \zeta^{p^{n-1}} + \zeta^{2p^{n-1}} + \dots + \zeta^{(p-1)p^{n-1}} = 0,$$

the $p^{n-1}(p-1)$ elements $1, \zeta, \dots, \zeta^{p^{n-1}(p-1)-1}$ form a base of $\mathbb{Z}[\zeta_{p^n}]$ over \mathbb{Z} . Then we have

$$\bigcap_{\mathfrak{q}} \mathcal{V}_q = \bigcap_{\mathfrak{q}} \mathcal{V}_q = (\cap_{\mathfrak{q}} \mathbb{Z}_{(q)})1 + (\cap_{\mathfrak{q}} \mathbb{Z}_{(q)})\zeta + \dots + (\cap_{\mathfrak{q}} \mathbb{Z}_{(q)})\zeta^{p^{n-1}(p-1)-1} = \mathbb{Z}[\zeta_{p^n}],$$

where \mathfrak{q} runs over all prime ideals of $O = \mathbb{Z}[\zeta_{p^n}]$ and q runs over all rational primes. This shows that $\mathbb{Z}[\zeta_{p^n}]$ is the integer ring of $\mathbb{Q}[\zeta_{p^n}]$; in other words, $\mathbb{Z}[\zeta_{p^n}]$ is the integral closure of \mathbb{Z} in $\mathbb{Q}[\zeta_{p^n}]$. Thus $O_{\mathfrak{q}} = \mathcal{V}_{\mathfrak{q}}$ for a prime ideal \mathfrak{q} of O , and we can restate the reciprocity law as follows:

Corollary 2.7 *The integer ring O of $\mathbb{Q}[\zeta_{p^n}]$ is generated by ζ_{p^n} over \mathbb{Z} . For a prime $q \neq p$ and a prime factor $\mathfrak{q}|q$, the decomposition group $D_{\mathfrak{q}}$ is independent*

of the choice of \mathfrak{q} and generated by the Frobenius element ϕ_q with $\chi_{p^n}(\phi_q) = q$. We have $(q) = \prod_{\sigma \in G/D_q} \sigma(\mathfrak{q})$ and $O/\mathfrak{q} = \mathbb{F}_{q^f}$ for the order f of q in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. The prime p is totally ramified in O , and the prime factor \mathfrak{p} of p is principal and is generated by $\zeta_{p^n} - 1$. In particular, $I_{\mathfrak{p}} = D_{\mathfrak{p}} = \text{Gal}(\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q})$ for the inertia subgroup $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$.

2.2.3 Adelic Reformulation

Recall that p and q are distinct primes, and put $N = p^m q^n$. Then we have a commutative diagram

$$\begin{array}{ccc} \mathbb{Q}[\zeta_N] & \longleftarrow & \mathbb{Q}[\zeta_{p^m}] \\ \uparrow & & \uparrow I_p \\ \mathbb{Q}[\zeta_{q^n}] & \xleftarrow{I_q} & \mathbb{Q}, \end{array}$$

where I_p denotes the inertia group at p . Since p is unramified in $\mathbb{Q}[\zeta_{q^n}]$, we find $I_p \cap I_q = \{1\}$. Since $I_p = \text{Gal}(\mathbb{Q}[\zeta_{p^m}]/\mathbb{Q})$ and $\text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q})$ is an abelian group (Corollary 2.3), we find that $\text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q}) = I_p \times I_q \cong (\mathbb{Z}/N\mathbb{Z})^\times$ by χ_N . Repeating this process for $N = \prod_p p^{e(p)}$, we find

Theorem 2.8 *The cyclotomic character χ_N induces an isomorphism*

$$\text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$$

of groups. The decomposition group of a prime $q \nmid N$ is cyclic and generated by the Frobenius element ϕ_q with $\chi_N(\phi_q) = q \in (\mathbb{Z}/N\mathbb{Z})^\times$. For a prime $p|N$, writing $N = p^e N'$ with $p \nmid N'$, the inertia group I_p of p is given by $\chi_N^{-1}((\mathbb{Z}/p^e\mathbb{Z})^\times)$, identifying $(\mathbb{Z}/N\mathbb{Z})^\times = (\mathbb{Z}/p^e\mathbb{Z})^\times \times (\mathbb{Z}/N'\mathbb{Z})^\times$. The decomposition group for $p|N$ is given by $I_p \times \langle \phi_p \rangle$, where $\chi_{N'}(\phi_p) = p \in (\mathbb{Z}/N'\mathbb{Z})^\times$.

By definition, if $M|N$, $\mathbb{Q}[\zeta_M] \subset \mathbb{Q}[\zeta_N]$ because $\zeta_M = \zeta_N^{N/M}$. Then it is easy to check that the following diagram commutes:

$$\begin{array}{ccc} \text{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q}) & \xrightarrow{\text{restriction}} & \text{Gal}(\mathbb{Q}[\zeta_M]/\mathbb{Q}) \\ \chi_N \downarrow & & \downarrow \chi_M \\ (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{(x \bmod N) \mapsto (x \bmod M)} & (\mathbb{Z}/M\mathbb{Z})^\times. \end{array} \quad (2.1)$$

Thus the composite (inside $\overline{\mathbb{Q}}$) of $\mathbb{Q}[\zeta_N]$ for all positive integers N is actually a union $\mathbb{Q}^{cyc} = \bigcup_N \mathbb{Q}[\zeta_N]$.

Taking the projective limit, we have

$$\chi : \text{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times = \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^\times. \quad (2.2)$$

We compute $\widehat{\mathbb{Z}} = \varprojlim_N (\mathbb{Z}/N\mathbb{Z})$. We recall that the p -adic integer ring $\mathbb{Z}_p = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})$ is formed by the formal series $\sum_{n \geq 0} c_n p^n$ with $0 \leq c_n \leq p-1$,

which is the valuation ring (and is the completion of $\mathbb{Z}_{(p)}$ with respect to the norm $|x|_p = p^{-v(x)}$). Since any integer can be expanded as above by p -adic expansion, $\mathbb{Z} \subset \mathbb{Z}_p$, and this inclusion is compatible with $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$. Writing the prime decomposition of N as $N = \prod_{p|N} p^{e(p)}$, we find by the Chinese remainder theorem

$$\widehat{\mathbb{Z}} = \varprojlim_N (\mathbb{Z}/N\mathbb{Z}) = \varprojlim_N \prod_{p|N} (\mathbb{Z}/p^{e(p)}\mathbb{Z}) = \prod_p \varprojlim_e (\mathbb{Z}/p^e\mathbb{Z}) = \prod_p \mathbb{Z}_p, \quad (2.3)$$

where p runs over all prime numbers in the last two products. We put the p -adic topology on \mathbb{Z}_p so that a system of neighborhoods of $x \in \mathbb{Z}_p$ is given by $\{x + p^n\mathbb{Z}_p\}_{n \geq 0}$. This makes \mathbb{Z}_p (resp. \mathbb{Z}_p^\times) a compact profinite ring (resp. group). We equip $\widehat{\mathbb{Z}}$ and $\widehat{\mathbb{Z}}^\times$ with the product topology of each component (\mathbb{Z}_p and \mathbb{Z}_p^\times). Then $\widehat{\mathbb{Z}}$ (resp. $\widehat{\mathbb{Z}}^\times$) is a compact profinite ring (resp. group).

We now want to prove: $\text{Gal}(\mathbb{Q}^{cy}/\mathbb{Q}) \cong \mathbb{A}^\times/\mathbb{Q}^\times \mathbb{R}_+^\times = GL_1(\mathbb{A}^{(\infty)})/\mathbb{Q}_+^\times$ for the adèle ring \mathbb{A} using the above expression of $\text{Gal}(\mathbb{Q}^{cy}/\mathbb{Q})$. The adèle ring \mathbb{A} is a rather complicated ring, but we find it very useful later, and it contains all arithmetic information of the field of rational numbers \mathbb{Q} .

Let us recall the definition of \mathbb{A} . We consider the product ring $\mathbb{R} \times \prod_p \mathbb{Q}_p$, where p runs over all positive prime numbers, and \mathbb{Q}_p is the field of fractions of \mathbb{Z}_p , and $\mathbb{Q} \subset \mathbb{Q}_p$, which is the completion of \mathbb{Q} under the p -adic norm $|\cdot|_p$ as above. Each p -adic number $x \in \mathbb{Q}_p$ has an expansion $\sum_{n \gg -\infty} c_n p^n$ ($c_n = 0$ if n is very negative). Since \mathbb{Z}_p^\times is made up of $\sum_{n=0}^\infty c_n p^n$ with $p \nmid c_0$, $\mathbb{Q}_p = \bigsqcup_n p^n \mathbb{Z}_p^\times \sqcup \{0\}$, where n runs over all integers. Regard \mathbb{Q} inside $\mathbb{R} \times \prod_p \mathbb{Q}_p$ by sending $\xi \in \mathbb{Q}$ to $(\xi, \xi, \dots, \overset{p}{\xi}, \dots) \in \mathbb{R} \times \prod_p \mathbb{Q}_p$. Let \mathbb{A} be the subring of $\mathbb{R} \times \prod_p \mathbb{Q}_p$ generated by \mathbb{Q} , $\widehat{\mathbb{Z}}$, and \mathbb{R} . We often write $x = (x_\infty, \dots, x_p, \dots)$ for an element $x \in \mathbb{R} \times \prod_p \mathbb{Q}_p$; so, $x_\infty \in \mathbb{R}$.

Proposition 2.9 *We have*

$$\mathbb{A} = \mathbb{A}' := \left\{ (x_p)_{p:\text{prime}, \infty} \in \mathbb{R} \times \prod_p \mathbb{Q}_p \mid x_p \in \mathbb{Z}_p \text{ for almost all } p \right\}$$

and $\mathbb{A} = (\mathbb{R} \times \widehat{\mathbb{Z}}) + \mathbb{Q}$. Here “almost all p ” means “except for finitely many p .”

Proof. The ring \mathbb{A}' is a subring of $\mathbb{R} \times \prod_p \mathbb{Q}_p$. For $\xi = \frac{a}{b} \in \mathbb{Q}$ ($a, b \in \mathbb{Z}$), if $p \nmid b$, we have $\xi \in \mathbb{Z}_p$. Thus $\xi \in \mathbb{A}'$, and $\mathbb{A} \subset \mathbb{A}'$. If $x \in \mathbb{A}'$, we expand $x_p = \sum_n c_n p^n$, and define $[x_p] = \sum_{n < 0} c_n p^n$, which is a fraction with a p -power denominator and is called the fraction p -part of x_p . Then $[x_p] = 0$ for almost all p , and $[x] = \sum_p [x_p] \in \mathbb{Q}$. Then we look into $x_p - [x] = x_p - [x_p] - \sum_{q \neq p} [x_q] \in \mathbb{Q}_p$. Since the denominator of $[x_q]$ is prime to p , we find $[x_q] \in \mathbb{Z}_p$. Thus $x_p - [x] = x_p - [x_p] - \sum_{q \neq p} [x_q] \in \mathbb{Z}_p$, and hence $x - [x] \in \widehat{\mathbb{Z}}$ inside \mathbb{A}' . In particular, $x = (x - [x]) + [x] \in (\mathbb{R} \times \widehat{\mathbb{Z}}) + \mathbb{Q} \subset \mathbb{A}$. This shows the last identity. \square

Writing the finite part $\mathbb{A}^{(\infty)} = \mathbb{A} \cap \prod_p \mathbb{Q}_p$, we thus have $\mathbb{A}^{(\infty)} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 2.10 *We have $\mathbb{A}^\times = \mathbb{Q}^\times (\mathbb{R}_+^\times \times \widehat{\mathbb{Z}}^\times)$ by $x \mapsto \langle x \rangle (x / \langle x \rangle)$, where $\mathbb{R}_+^\times = \{x \in \mathbb{R} | x > 0\}$.*

Proof. Since $\mathbb{Q}_p = \bigsqcup_n p^n \mathbb{Z}_p^\times \sqcup \{0\}$, we can write $x_p \in \mathbb{Q}_p$ as $x_p = p^{v(x_p)} u_p$ with $u_p \in \mathbb{Z}_p^\times$. Then for $x \in \mathbb{A}^\times$, $x^{-1} \in \mathbb{A}$, and hence $|x_p|_p = 1 \iff v(x_p) = 0$ for almost all p . In other words, $\langle x \rangle = \frac{x_\infty}{|x_\infty|} \prod_p p^{v(x_p)}$ is a rational number for $x \in \mathbb{A}^\times$, and $x \langle x \rangle^{-1} \in \mathbb{R}_+^\times \times \widehat{\mathbb{Z}}^\times$. \square

By translation, we extend the topology on $\widehat{\mathbb{Z}}$ to $\mathbb{A}^{(\infty)} = \mathbb{Q} + \widehat{\mathbb{Z}}$. Therefore \mathbb{A} and $\mathbb{A}^{(\infty)}$ are locally compact rings (and \mathbb{A}^\times is a locally compact group; see [MFG] 3.1, [LFE] 8.1-3 and [EPE] Chapter II for more about the adèle topology on the adèle points $G(\mathbb{A})$ of an algebraic group G over \mathbb{Q}).

Corollary 2.11 *We have $\mathbb{A}^\times / \mathbb{Q}^\times \mathbb{R}_+^\times \cong \widehat{\mathbb{Z}}^\times$. This isomorphism ι can be normalized so that it takes $p \in \mathbb{Q}_p \subset \mathbb{A}$ to $p^{(p^\infty)} = (p, p, \dots, p, \overset{p}{1}, p, \dots, p) \in \widehat{\mathbb{Z}}^\times$.*

Proof. We see that $\xi \in \mathbb{Q}^\times \cap (\widehat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times)$ means that $\xi = \xi_\infty > 0$ and the numerator and the denominator of $\xi = \xi_p$ is prime to p for all p ; so, $\xi = 1$. Thus we conclude $\mathbb{Q}^\times \cap (\widehat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times) = \{1\}$. By the isomorphism theorem:

$$\phi : \mathbb{A}^\times / \mathbb{Q}^\times \mathbb{R}_+^\times = \widehat{\mathbb{Z}}^\times \mathbb{Q}^\times \mathbb{R}_+^\times / \mathbb{Q}^\times \mathbb{R}_+^\times \cong \widehat{\mathbb{Z}}^\times / \mathbb{Q}^\times \cap (\widehat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times) = \widehat{\mathbb{Z}}^\times.$$

Since $p = p^{(p^\infty)} p_p p_\infty = 1$ in $\mathbb{A}^\times / \mathbb{Q}^\times \mathbb{R}_+^\times$ for $p_p = (1, \dots, 1, \overset{p}{p}, 1, \dots, 1) \in \mathbb{A}^\times$ and $p_\infty = (\overset{\infty}{p}, 1, \dots, 1) \in \mathbb{A}^\times$, the above isomorphism brings p_p in $\mathbb{Q}_p^\times \subset \mathbb{A}^\times$ to $(p^{(p^\infty)})^{-1}$. Defining $\iota(x) = \phi(x)^{-1}$, we get the desired isomorphism. \square

Combining this with Theorem 2.8, we get

Theorem 2.12 (Class Field Theory) *We have a canonical (reciprocity) isomorphism $\iota : GL_1(\mathbb{A}^{(\infty)}) / \mathbb{Q}_+^\times = \mathbb{A}^\times / \mathbb{Q}^\times \mathbb{R}_+^\times \cong \text{Gal}(\mathbb{Q}^{cyc} / \mathbb{Q})$ such that $p_p \in \mathbb{Q}_p$ is sent to a Frobenius element at p , and the decomposition group at p is given by the closure of the image of \mathbb{Q}_p^\times . Inside the decomposition group, the inertia group is given by the isomorphic image of \mathbb{Z}_p^\times .*

Class field theory says slightly more, namely that \mathbb{Q}^{cyc} is the maximal abelian extension \mathbb{Q}^{ab} of \mathbb{Q} . For more on this, see [FAN] Chapter 6. Often the above result is expressed as an exact sequence,

$$1 \rightarrow \mathbb{Q}^\times \mathbb{R}_+^\times \rightarrow \mathbb{A}^\times \xrightarrow{\iota} \text{Gal}(\mathbb{Q}^{ab} / \mathbb{Q}) \rightarrow 1,$$

and the map $\iota(x)$ is called the Artin reciprocity map and sometimes written as $\iota(x) = [x, \mathbb{Q}]$. The reciprocity map of the class field theory induces a locally compact (actually compact profinite) topology on the Galois group. This topology can be defined in a way intrinsic to Galois' theory, as we show in the following section.

Exercises

1. Prove that $\Phi_{p^n}(X)$ is irreducible in $\mathbb{Q}[X]$.
2. Give a detailed proof of Corollary 2.4.
3. Prove $\mathbb{Z}_{(q)}[\zeta_{p^n}]$ is integrally closed.
4. Prove that the integer ring O of $\mathbb{Q}[\zeta_N]$ is generated by ζ_N over \mathbb{Z} . Hint: First show that $\mathbb{Q}[\zeta_N] = \mathbb{Q}[\zeta_{p^m}] \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_{q^n}]$ if $N = p^m q^n$ for distinct primes p and q . Then show that $O = \mathbb{Z}[\zeta_{p^m}] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{q^n}]$ using the fact that no prime ramifies in the two fields $\mathbb{Q}[\zeta_{p^m}]$ and $\mathbb{Q}[\zeta_{q^n}]$ at the same time.
5. Give a detailed proof of Theorem 2.8.
6. Deduce the quadratic reciprocity law in the introduction either from Theorem 2.6 or Theorem 2.12.

2.3 A Generalization of Galois Theory

For our later use, we gather here some results from a generalization of Galois' theory given in [IAT] 6.3.

2.3.1 Infinite Galois Extensions

We study the Galois theory when $\dim_K L$ is infinite for a Galois extension L/K . First we recall Galois' fundamental theorem when L/K is finite.

Theorem 2.13 (E. Galois) *Suppose that L/K is a finite Galois extension. Taking an intermediate field $L/M/K$, L/M is a Galois extension and*

- (1) *There is one-to-one onto correspondence*

$$\{M : \text{intermediate field } L/M/K\} \leftrightarrow \{H : \text{subgroup of } \text{Gal}(L/K)\}$$

given by $M \mapsto \text{Gal}(L/M)$ and $H \mapsto L^H = \{x \in L \mid x = \sigma(x) \forall \sigma \in H\}$.

- (2) *For two intermediate fields M, M' , we have*
 - $M \supset M' \iff \text{Gal}(L/M) \subset \text{Gal}(L/M')$;
 - $\text{Gal}(M \cap M')$ *is the subgroup of* $\text{Gal}(L/K)$ *generated by the two subgroups* $\text{Gal}(L/M)$ *and* $\text{Gal}(L/M')$;
 - $\text{Gal}(L/MM') = \text{Gal}(L/M) \cap \text{Gal}(L/M')$;
 - *For* $\sigma \in \text{Gal}(L/K)$, $\text{Gal}(L/\sigma(M)) = \sigma \text{Gal}(L/M) \sigma^{-1}$.
- (3) *M/K is a Galois extension if and only if $\text{Gal}(L/M)$ is a normal subgroup in the Galois group $\text{Gal}(L/K)$. In particular, by $\sigma \mapsto \sigma|_M$, we have an isomorphism: $\text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Gal}(M/K)$.*

We admit this theorem, just referring the reader to any book on elementary Galois theory.

What we want to do in this subsection is to generalize the above theorem to an infinite Galois extension. Hereafter we suppose that L/K is an infinite Galois extension. Since each element $\xi \in L$ satisfies a polynomial equation of

finite degree with coefficients in K , there are only finitely many conjugates of ξ . Thus the Galois closure $K[\xi]^{gal}$ of $K[\xi]$ over K is a finite Galois extension of K , and we get from Theorem 2.13 (2),

$$L = \bigcup_{\xi \in L} K[\xi]^{gal} \Leftrightarrow \bigcap_{\xi \in L} \text{Gal}(L/K[\xi]^{gal}) = \{\text{id}\}. \quad (2.4)$$

We first generalize the third assertion of the above theorem.

Lemma 2.14 *Suppose M is an intermediate Galois extension of a Galois extension L/K . Then the group $\text{Gal}(L/M)$ is a normal subgroup of $\text{Gal}(L/K)$, and $\sigma \mapsto \sigma|_M$ induces an isomorphism $\text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Gal}(M/K)$. In particular, if M/K is a finite extension, then we have the equality $[\text{Gal}(L/K) : \text{Gal}(L/M)] = [M : K] < \infty$.*

Proof. If M/K is a finite extension, for any finite Galois extension L' with $L \supset L' \supset M$, we can extend $\sigma \in \text{Gal}(M/K)$ to $\tau \in \text{Gal}(L'/K)$ (assertion (3) of Theorem 2.13). Since L is a union of finite Galois extensions of L' , $\sigma \in \text{Gal}(L'/K)$ extends to $\tau \in \text{Gal}(L/K)$. If M/K is an infinite extension, writing M as a union of finite Galois extensions M'/K and applying the above fact to M'/K , we find that any $\sigma \in \text{Gal}(M/K)$ can be extended to $\tau \in \text{Gal}(L/K)$. Thus $\sigma \mapsto \sigma|_M$ is a surjective homomorphism of $\text{Gal}(L/K)$ onto $\text{Gal}(M/K)$. Its kernel is given by $\text{Gal}(L/M)$ which is normal. \square

Basically the same proof as above yields the following result which looks stronger than the lemma.

Corollary 2.15 *Let M be an intermediate extension of L/K . Then $\sigma \mapsto \sigma|_M$ induces an isomorphism $\text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Hom}_K(M, L)$, where the set $\text{Hom}_K(M, L)$ is the collection of K -linear field homomorphisms of M into L .*

The proof of this corollary is left to the reader as an exercise (Exercise 1).

We now give a topology on the group $\text{Gal}(L/K)$ in the following way. Define a fundamental system of open neighborhoods of the identity by the collection of subgroups of the form $\text{Gal}(L/M)$ for a finite extension M/K . If $H = \text{Gal}(L/M)$ for a finite extension M/K , the Galois closure M^{gal} is still a finite Galois extension of K ; so, we find a normal open subgroup $\text{Gal}(L/M^{gal})$ inside any open subgroup H . Thus we may define the system to be the set \mathfrak{U} of all normal subgroups $N = \text{Gal}(L/M)$ for finite Galois extensions M/K inside L . For each $\sigma \in \text{Gal}(L/K)$, we define the system of neighborhoods of σ to be $\sigma\mathfrak{U} = \mathfrak{U}\sigma = \{\sigma N = N\sigma \mid N \in \mathfrak{U}\}$. By this, if \mathfrak{U} satisfies the axiom of a fundamental system of open neighborhoods of a point, G becomes a topological group, that is, G is a group with a topology for which the multiplication $(a, b) \mapsto ab$ and inverse $a \mapsto a^{-1}$ are continuous. The axiom is checked by

Lemma 2.16 *We have*

- (1) *For $\sigma \neq 1$, there exists $N \in \mathfrak{U}$ with $\sigma \notin N$ (so, G is a Hausdorff group);*

(2) $N, H \in \mathfrak{U} \Rightarrow N \cap H \in \mathfrak{U}$.

Proof. By (2.4), $L = \bigcup_M M$ for finite Galois extensions M/K . If $\sigma \in \bigcap_M \text{Gal}(L/M)$, σ is the identity over all M ; so, $\sigma = 1$ in $\text{Gal}(L/K)$. Thus there exists a finite Galois extension M/K inside L such that $\sigma \notin N = \text{Gal}(L/M)$ if $\sigma \neq 1$. By definition, we have $N \in \mathfrak{U}$; so, assertion (1) follows.

Write $N = \text{Gal}(L/M)$ and $H = \text{Gal}(L/M')$. Then MM' is a composite of two finite Galois extensions; so, it is a finite Galois extension. By definition, σ is trivial over $MM' \iff \sigma$ is trivial over M and M' . Then by Lemma 2.14, we have $\text{Gal}(L/MM') = N \cap H$, and hence $N \cap H \in \mathfrak{U}$, which proves (2). \square

The topology we have defined was first introduced by Krull, and therefore it is called the Krull topology on $\text{Gal}(L/K)$.

Proposition 2.17 *For an infinite Galois extension L/K , $\text{Gal}(L/K)$ is a compact group under the Krull topology.*

Proof. Since $\text{Gal}(L/K)$ is Hausdorff, we need to show that for any given infinite subset Σ in $\text{Gal}(L/K)$, there exists an element $\sigma \in \text{Gal}(L/K)$ such that $\Sigma \cap H\sigma$ is infinite for all $H \in \mathfrak{U}$; that is, Σ has a limit point $\sigma \in \text{Gal}(L/K)$. Since $H = \text{Gal}(L/M)$ for a finite Galois extension M/K , there are finitely many automorphisms of M/K . Thus there exists an infinite subset Σ_H of Σ that induces a single automorphism σ_M on M . For any extension $\sigma' \in \Sigma_H$ of σ_M to L , the coset $H\sigma'$ is the collection of $\tau \in \text{Gal}(L/K)$ (by Lemma 2.14) with $\tau|_M = \sigma_M$. We make the construction of σ_M compatible with an increasing sequence of Galois extensions M_j of K inside L . In other words, we find a sequence of finite Galois extensions M_j/K ($j = 1, 2, \dots$) with $K \subset M_j \subset M_{j+1} \subset L$ and $\sigma_j = \sigma_{M_j} \in \text{Gal}(M_j/K)$ such that $L = \bigcup_j M_j$ and $\sigma_{j+1}|_{M_j} = \sigma_j$ for all j . We have found an element $\sigma \in \text{Gal}(L/K)$ such that $\sigma|_{M_j} = \sigma_{M_j}$ for all j . This σ is a limit point of Σ . \square

Corollary 2.18 *If M is an intermediate field of an infinite Galois extension L/K , $\text{Gal}(L/M)$ is a closed subgroup of $\text{Gal}(L/K)$.*

Proof. For any finite Galois extension M'/K inside L , we have by definition the following identity: $i^{-1}(\text{Gal}(L/MM')) = \text{Gal}(L/MM')$ for the inclusion map $i : \text{Gal}(L/M) \hookrightarrow \text{Gal}(L/K)$. For any $N \in \mathfrak{U}$, we find a finite Galois extension M'/K inside L such that $N = \text{Gal}(L/M')$. Since MM'/M is a finite Galois extension, $i^{-1}(N) = \text{Gal}(L/MM')$ is open in $\text{Gal}(L/M)$; so, i is continuous. The image of a compact set by a continuous map is compact; in particular, it is closed. \square

We now prove a generalization of Theorem 2.13.

Theorem 2.19 *Let L/K be an infinite Galois extension. We have the following canonical one-to-one onto correspondence,*

$$\{\text{intermediate fields } M \text{ of } L/K\} \leftrightarrow \{\text{closed subgroups } H \text{ of } \text{Gal}(L/K)\}$$

induced by $M \mapsto \text{Gal}(L/M)$ and $H \mapsto L^H$. Moreover,

- (1) Every open subgroup of $\text{Gal}(L/K)$ is closed, and open subgroups correspond to finite extensions L^H/K .
- (2) Let $\{N_i\}_{i \in I}$ for an index set I be a collection of closed subgroups of the Galois group $\text{Gal}(L/K)$. Writing $N_i = \text{Gal}(L/K_i)$, for the composite M of all $\{K_i\}_{i \in I}$, we have $\bigcap_{i \in I} N_i = \text{Gal}(L/M)$.
- (3) If $\{K_i\}_{i \in I}$ is a collection of intermediate fields of L/K , then the group $\text{Gal}(L/\bigcap_{i \in I} K_i)$ is the closure of the subgroup in $\text{Gal}(L/K)$ generated by $\text{Gal}(L/K_i)$ for all i .
- (4) For $\sigma \in \text{Gal}(L/K)$, we have $\text{Gal}(L/\sigma(M)) = \sigma \cdot \text{Gal}(L/M)\sigma^{-1}$.
- (5) If M/K is a Galois extension inside L , then $\text{Gal}(L/M)$ is a normal closed subgroup and $\text{Gal}(L/K)/\text{Gal}(L/M) \cong \text{Gal}(M/K)$ induced by $\sigma \mapsto \sigma|_M$ is an isomorphism of topological groups.

Proof. Let \mathfrak{M} be the set of all intermediate fields of L/K and \mathfrak{H} be the set of all closed subgroups of $\text{Gal}(L/K)$. For any $M \in \mathfrak{M}$, $\text{Gal}(L/M)$ is a closed subgroup of $\text{Gal}(L/K)$ by Corollary 2.18; so, $M \mapsto \text{Gal}(L/M)$ defines a map $\mathfrak{M} \rightarrow \mathfrak{H}$. We define a reverse map $\mathfrak{H} \rightarrow \mathfrak{M}$ by $H \mapsto L^H$.

We first prove that $\text{Gal}(L/L^H) = H$. Since $\text{Gal}(L/L^H) \subset \text{Gal}(L/K)$ is the collection of all automorphisms of L fixing L^H , we confirm that $H \subset \text{Gal}(L/L^H)$. Conversely, for each finite Galois extension M/L^H inside L , H acts on M nontrivially if $M \neq L^H$, and the image under $\sigma \mapsto \sigma|_M$ in $\text{Gal}(M/L^H)$ is a subgroup H' of $\text{Gal}(M/L^H)$ and $L^H = M^{H'}$. By Theorem 2.13 (1), $H' = \text{Gal}(M/L^H)$. In other words, for each $\sigma \in \text{Gal}(L/L^H)$, we find $h_M \in H$ such that $h_M|_M = \sigma|_M$. We consider the infinite set $\Sigma = \{h_M\}_M \subset H$ with M running through all finite Galois extensions M/L^H . Since H is a closed subgroup of a compact group $\text{Gal}(L/K)$, H itself is compact. Then Σ has a unique accumulation point h . Then for each finite Galois extension M/L^H , $\sigma|_M = h|_M$. Since $L = \bigcup_M M$ for finite Galois extensions of M/L^H , we find that $h = \sigma$ and $H = \text{Gal}(L/L^H)$.

We now prove $L^{\text{Gal}(L/M)} = M$. By Corollary 2.18, $H = \text{Gal}(L/M) \in \mathfrak{H}$. By definition, $M \subset L^H$. Supposing that $L^H \neq M$, we try to get a contradiction. Pick $\xi \in L^H - M$. Then $M[\xi]/M$ is a finite extension. Thus $M[\xi]^{gal} \subset L$ because L/K is normal. Since $\xi \notin M$, $\text{Gal}(M[\xi]^{gal}/M) \neq \{1\}$. Pick $\sigma \in \text{Gal}(M[\xi]^{gal}/M)$ with $\sigma(\xi) \neq \xi$. Then by Lemma 2.14, we find $\tau \in \text{Gal}(L/M) = H$ such that $\tau(\xi) = \sigma(\xi) \neq \xi$. This is wrong since $\sigma(\xi)$ has to be ξ because $\xi \in L^H$. Thus we find that $L^{\text{Gal}(L/M)} = M$, and the correspondence is one-to-one and onto.

For an open subgroup H , $\text{Gal}(L/K)/H$ is discrete and compact; so, it is finite (see Exercise 4). Since H is the kernel of the continuous map $\text{Gal}(L/K) \twoheadrightarrow \text{Gal}(L/K)/H$, H is closed. By $H = \text{Gal}(L/L^H)$, we see from Lemma 2.14 and Corollary 2.15 that $\text{Gal}(L/K)/H = \text{Hom}_K(L^H, L)$, and hence L^H/K is a finite extension by Corollary 2.15. This shows (1).

Assertion (2) follows from the fact: $\sigma \in \text{Gal}(L/K)$ is the identity on every K_i if and only if σ is the identity on the composite of all K_i (Exercise 2).

Let $\text{Gal}(L/\cap_{i \in I} K_i) = H'$. Then by definition, H' is a closed subgroup containing all $H_i = \text{Gal}(L/K_i)$, and it contains the closure H of the subgroup generated by H_i for all i . Since H is a closed subgroup (so in \mathfrak{H}) containing H_i , we see $L^H \subset K_i$ and hence $L^H \subset \cap_{i \in I} K_i$. Thus $H \supset H' = \text{Gal}(L/\cap_{i \in I} K_i)$. This shows $H = H'$.

Assertion (4) is plain from the definition of the Galois group, and the last assertion follows from Lemma 2.14. \square

2.3.2 Automorphism Group of a Field

We study $\text{Aut}(L/K)$ for an arbitrary extension L/K of fields. An intermediate extension M of L/K is called *of finite type* over K if there are finitely many elements x_1, \dots, x_n that generate M as a field over K . We define a fundamental system \mathfrak{U} of open neighborhoods of 1 on $\text{Aut}(L/K)$ by

$$\mathfrak{U} = \{H = \text{Aut}(L/M) \mid M/K \text{ is of finite type}\}. \quad (2.5)$$

Since a composite of two intermediate fields of finite type is again of finite type, \mathfrak{U} satisfies the axiom of the fundamental system of neighborhoods (see the proof of Lemma 2.16 and Exercise 3). Then define a system of neighborhoods of $\sigma \in \text{Aut}(L/K)$ by $\sigma\mathfrak{U} \cup \mathfrak{U}\sigma$. This topology gives a topological group structure on $\text{Aut}(L/K)$. Let \mathfrak{H} be the set of all compact subgroups of $\text{Aut}(L/K)$, and let \mathfrak{M} be the set of all intermediate fields M in L/K such that L/M is a Galois extension. Then we have

Proposition 2.20 (Jacobson) *We have a canonical bijective correspondence $\mathfrak{M} \cong \mathfrak{H}$ given by $M \mapsto \text{Gal}(L/M)$ and $H \mapsto L^H$.*

Proof. Pick a compact subgroup H of $\text{Aut}(L/K)$. Then for each $\xi \in L$, the topological group $\text{Aut}(L/K(\xi))$ is an open subgroup of $\text{Aut}(L/K)$. Thus $H' = H \cap \text{Gal}(L/K(\xi))$ is an open subgroup of H . In particular, H/H' is compact and discrete; so, it is finite (Exercise 4). Since $f(X) = \prod_{h \in H/H'} (X - h(\xi))$ has coefficients in L^H , ξ is algebraic over L^H . Since $h(\xi) = h'(\xi) \Leftrightarrow hH' = h'H'$, we find that the roots of $f(X)$ are all distinct; so $L^H(\xi)/L^H$ is a separable extension. Since $h(\xi) \in L$ for all $h \in H$, all the roots of $f(X)$ are in L . The Galois closure M of $L^H(\xi)$ over L^H is a Galois extension of L^H inside L . Since $L = \bigcup_{\xi \in L} L^H(\xi)$, we find that L/L^H is a Galois extension. Then by Theorem 2.19, we find that $H = \text{Gal}(L/L^H)$. Starting from $M \in \mathfrak{M}$, we find that $\text{Gal}(L/M) \in \mathfrak{H}$ and $M = L^{\text{Gal}(L/M)}$ by Theorem 2.19. \square

A field extension L/K is of finite type if L is generated over K by finitely many elements (as a field). Let \mathfrak{H}^o be the set of all open compact subgroups of $\text{Aut}(L/K)$ and \mathfrak{M}^o be the subset of \mathfrak{M} made up of fields M that are of finite type over K .

Corollary 2.21 *If \mathfrak{M}^o is nonempty, then $\text{Aut}(L/K)$ is locally compact, and the one-to-one onto correspondence in Proposition 2.20 induces $\mathfrak{M}^o \cong \mathfrak{H}^o$.*

Proof. If \mathfrak{M}° is nonempty, pick $M \in \mathfrak{M}^\circ$. Then the identity of $\text{Aut}(L/K)$ has an open neighborhood $\text{Gal}(L/M)$, which is also compact by Proposition 2.17. By translating this neighborhood to any point σ on $\text{Aut}(L/K)$ through multiplication by σ , every point has an open-compact neighborhood; so, $\text{Aut}(L/K)$ is locally compact. We need to show that L^H/K is of finite type over K if $H \in \mathfrak{H}^\circ$. Consider $F = ML^H$. Then L/F is a Galois extension; so, $H' = \text{Gal}(L/F)$ is a compact subgroup of $\text{Gal}(L/M)$. Since F/M is a finite extension, F is of finite type over M and hence over K . Thus the subfield L^H of a field F is of finite type over K . \square

Exercises

1. Prove Corollary 2.15.
2. Give a detailed proof of the assertions (2) and (4) of Theorem 2.19.
3. Prove that the Krull topology on $\text{Aut}(L/K)$ given by (2.5) is well-defined.
4. Prove that a compact and discrete set is a finite set.

2.4 Algebraic Curves over a Field

Here we give an exposition of classical theory of algebraic curves over a field from the viewpoint of the theory of discrete valuation. See [ALF] for a more detailed exposition on algebraic curves from this point of view. Under this setting, in the following section, we give a prototype of classification problems of abelian varieties (description of the moduli of elliptic curves over a field). To treat classification problems over rings, a more sophisticated language, for example, the language of schemes, is necessary. From the next chapter on, we treat the general case via the theory of schemes.

2.4.1 Algebraic Function Fields

Let K be a field of an arbitrary characteristic. An algebraic function field \mathfrak{K} of dimension 1 is a finitely generated nonalgebraic field extension \mathfrak{K}/K such that for any $x \in \mathfrak{K}$ transcendental over K , $\mathfrak{K}/K(x)$ is algebraic. We assume that the algebraic closure of K in \mathfrak{K} is K itself. In this case, we say that \mathfrak{K} is defined over K . Replacing K by its algebraic closure in \mathfrak{K} , we may always assume that \mathfrak{K} is defined over K .

We relate field theory to the geometric theory of projective algebraic curves by considering local coordinates. A prototypical example of algebraic function fields is given by the meromorphic function field over \mathbb{C} of a compact Riemann surface. Each point of a Riemann surface has a coordinate neighborhood, and the collection of all coordinate neighborhoods by definition determines the Riemann surface. Each meromorphic function has Laurent expansion at a given point, which gives a well-defined order of vanishing (or order of pole) of

the function at the given point. Associating the order at a point with meromorphic functions gives a valuation of the function field specific to the point. An idea of how to algebraize a Riemann surface is to consider the set of all valuations of its function field trivial over the base field and to replace coordinate neighborhoods by corresponding valuations. We recall here a formal definition of discrete valuation rings (DVR) inside an algebraic function field \mathfrak{K} over K . A *discrete valuation* v of \mathfrak{K} trivial on K is a surjective map $v : \mathfrak{K} \rightarrow \mathbb{Z} \sqcup \{\infty\}$ satisfying the following four conditions:

- (V0) $v(K^\times) = 0$ (triviality over the base field);
- (V1) $v(f) = \infty \Leftrightarrow f = 0$;
- (V2) $v(f + g) \geq \min(v(f), v(g))$ for all $f, g \in \mathfrak{K}$;
- (V3) $v(fg) = v(f) + v(g)$ for all $f, g \in \mathfrak{K}$.

Here we agree as a convention to have $a + \infty = \infty$ and $\infty > a$ for all $a \in \mathbb{Z}$. By the above properties, $\mathcal{V}_v = \{f \in \mathfrak{K} | v(f) \geq 0\}$ is a subring of \mathfrak{K} , and either $x \in \mathfrak{K}$ or $\frac{1}{x}$ belongs to \mathcal{V}_v . In particular, the field of fractions of \mathcal{V}_v is equal to \mathfrak{K} . The ring \mathcal{V}_v is called a *discrete valuation ring*, and $\mathfrak{m} = \{f \in \mathcal{V}_v | v(f) \geq 1\}$ is a unique maximal ideal of \mathcal{V}_v (so, \mathcal{V}_v is local). The field $\mathcal{V}_v/\mathfrak{m}$ is called the residue field of the valuation v and is a finite extension of the base field K . Moreover, every ideal of \mathcal{V}_v (except for the zero ideal) is a power of \mathfrak{m} , and $\mathfrak{m}^n = \{f \in \mathfrak{K} | v(f) \geq n\}$. See [CRT] Chapter 4 for more about valuation rings.

Our goal in this subsection is to create a space (a geometric object) from the purely algebraic notion of algebraic function fields \mathfrak{K} . The object is called the Zariski–Riemann space and is the collection of all valuations of \mathfrak{K} trivial over the base field K . The space is an algebraic replacement of the associated Riemann surface for $K = \mathbb{C}$.

Example 2.22 We start with the simplest Riemann surface: the Riemann sphere $\mathbf{P} = \mathbf{P}^1 = \mathbb{C} \cup \{\infty\}$. The meromorphic function field of the sphere \mathbf{P} is isomorphic to the rational function field $\mathfrak{K} = \mathbb{C}(x)$. Then the polynomial ring $\mathbb{C}[x]$ corresponds to the Riemann sphere \mathbf{P} with coordinate x in the following sense. The space \mathbf{P} is covered by two coordinate neighborhoods U_0 and U_∞ identical to \mathbb{C} , U_0 is centered at 0 with complex coordinate x , and the other U_∞ is centered at ∞ with coordinate $x' = \frac{1}{x}$. Then the field of meromorphic functions of \mathbf{P} is given by $\mathbb{C}(x)$, and the polynomial ring $\mathbb{C}[x]$ is the ring of functions with the only possible pole at ∞ . Each meromorphic function ϕ on U_0 finite at 0 has its Taylor expansion in the coordinate x : $\phi(x) = \sum_{n=0}^{\infty} a_n x^n$ whose radius of convergence is positive. If ϕ is not finite at 0, for some positive m , $x^m \phi(x)$ is finite at 0, and $\phi(x)$ therefore has its Laurent expansion $\sum_{n \geq -m} a_n x^n$. We can define a valuation v_0 on $\mathbb{C}(x)$ by assigning the exponent of the leading term of the Laurent expansion to a given meromorphic function $\phi \in \mathbb{C}(x)$. The valuation $v_0(\phi)$ is just the zero order of the function ϕ holomorphic at 0. For any other point $\alpha \in \mathbb{C} = U_0$ (resp. $\alpha = \infty \in U_\infty$), we can take $t_\alpha = x - \alpha$ (resp. $t_\infty = x^{-1}$) as a coordinate around α , and we can think of the valuation v_α giving the order of zero at α . In differential geometry or in complex analysis, local behavior of functions reflected by Taylor

expansion often determines in the aggregate global properties of the function. Partial fraction expansion determines elements in $\mathbb{C}(x)$; so, local knowledge of the valuation $v_\alpha(\phi)$ almost determines $\mathbb{C}(x)$. Thus it is natural to expect that the set Z of valuations $\{v_\alpha\}_\alpha$ determine \mathbf{P} . Indeed, at least set-theoretically, Z is in bijection with \mathbf{P} .

We choose a transcendental element $x \in \mathfrak{K}$ so that \mathfrak{K} is a finitely generated separable algebraic extension of $K(x)$. Then $\mathfrak{K}/K(x)$ is a simple extension; in other words, we can find a single generator $y \in \mathfrak{K}$ such that $\mathfrak{K} = K(x)[y]$. We may assume that y is integral over $K[x]$ (because some multiple of y by an element in $K[x]$ is integral over $K[x]$), and y satisfies an equation $y^m + a_1(x)y^{m-1} + \cdots + a_m(x) = 0$.

Suppose that $K = \mathbb{C}$. Take a general compact Riemann surface R . Then on the given Riemann surface R , choosing two generators (x, y) in its meromorphic function field, the relation of (x, y) gives a projective algebraic curve V in \mathbf{P}^2 . Moreover, defining the algebraic function field $\mathbb{C}(V)$ of V by the collection of nontrivial restriction to V of rational functions $P(x, y)/Q(x, y)$ (with two polynomials P and Q of equal degree), the meromorphic function field of R is isomorphic to the algebraic function field $\mathbb{C}(V)$ of V .

Here is another slightly more nontrivial example.

Example 2.23 Consider the function field $\mathfrak{K} = \mathbb{C}(x)[y]$ defined by the equation $y^2 = x(x-1)(x-\lambda)$ for $\lambda \in \mathbb{C}$ different from 0 and 1. We consider the square root $y(x) = \sqrt{x(x-1)(x-\lambda)}$ on U_0 . This function has two values on \mathbf{P} vanishing at $0, 1, \lambda$ and has a pole at ∞ ; in other words, its inverse vanishes at ∞ . Thus the locus of the point $(x, y, 1) \in \mathbf{P}^2$ is a two-sheet covering of \mathbf{P} that ramifies at $0, 1, \lambda, \infty$. Around $x = 0$, if a point circles around $(x, y) = (0, 0)$, for two values of $\pm y$, we have one value of x . In other words, cutting a line segment $[0, 1]$ and $[\lambda, \infty]$ from two copies of \mathbf{P} and gluing the two corresponding segments, we get the donut-shape Riemann surface R , on which the functions y and x both have single values. The field of meromorphic functions over R is given by $\mathbb{C}(x)[y]$. Moreover, we can embed R into \mathbf{P}^2 by $P \mapsto (x(P), y(P))$, which satisfies the given equation $y^2 = x(x-1)(x-\lambda)$. In other words,

$$R \cong V = \{(x, y) \in \mathbf{P}^2 \mid y^2 = x(x-1)(x-\lambda)\},$$

because x moves around all possible values in $\mathbf{P} = \mathbb{C} \cup \{\infty\}$.

For each point $\alpha \in \mathbb{C}$ different from $0, 1, \lambda$, pick a point P from the two points P, Q of R over α . Then P has an open neighborhood U with coordinate $t = x - \alpha$. Any meromorphic function f defined over U has a Laurent expansion $f(t) = \sum_{n \gg -\infty} a_n t^n$. We define a valuation $v_P : \mathbb{C}(V) \rightarrow \mathbb{Z} \cup \{\infty\}$ given by

$$v_P(f) = m \quad \text{if } a_m \neq 0 \text{ and } a_n = 0 \text{ if } n < m.$$

Thus we have (V0-3) for v_P and

$$\mathcal{V}_P = \{f \in \mathfrak{K} \mid v_P(x) \geq 0\} \quad (2.6)$$

is a valuation ring (Exercise 1) with $v_P(\mathbb{C}^\times) = 0$ (i.e., v_P is trivial on \mathbb{C}).

For P over one of the four ramified points $\alpha = 0, 1, \lambda, \infty$, for an open neighborhood O of α that does not contain any of $0, 1, \lambda, \infty$ different from α , $x^{-1}(O) = U$ is an open neighborhood of P and y gives a local coordinate t if $\alpha \neq \infty$ and y^{-1} gives a local coordinate t of U if $\alpha = \infty$. Then we define \mathcal{V}_P exactly in the same way. By definition, for each $x \in \mathfrak{K}$, either $v_P(x) \geq 0$ or $v_P(x) < 0$; in other words, x or x^{-1} is in \mathcal{V}_P . Thus we have $\mathfrak{K} = \text{Frac}(\mathcal{V}_P) = \{\frac{a}{b} \mid a \in \mathcal{V}_P, b \in \mathcal{V}_P - \{0\}\}$.

Start conversely with a discrete valuation $v : \mathfrak{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ with $v(\mathbb{C}^\times) = 0$. Then $\mathcal{V} = \{f \in \mathfrak{K} \mid v(f) \geq 0\}$ is a discrete valuation ring. Again for each $x \in \mathfrak{K}$, either $x \in \mathcal{V}$ or $x^{-1} \in \mathcal{V}$. First suppose that $x \in \mathcal{V}$. Then $\mathbb{C}[x] \subset \mathcal{V}$. Let $\mathfrak{m} = \{f \in \mathcal{V} \mid v(f) > 0\}$. Then \mathfrak{m} is the maximal ideal of \mathcal{V} , and \mathcal{V}/\mathfrak{m} is a field extension of \mathbb{C} . Since $\mathbb{C}[x]$ is a principal ideal domain, $\mathfrak{m} \cap \mathbb{C}[x]$ is either $(x - \alpha)$ for $\alpha \in \mathbb{C}$ or (0) . If $\mathfrak{m} \cap \mathbb{C}[x] = (0)$, we find that \mathcal{V}/\mathfrak{m} contains an isomorphic image of $\mathbb{C}[x]$. Thus the transcendental degree of \mathcal{V}/\mathfrak{m} , (i.e., $\dim(\mathcal{V}/\mathfrak{m})$) is larger than or equal to 1. Since \mathcal{V} has Krull dimension 1 (cf. [CRT] Section 5), this implies $\mathfrak{m} = (0)$, which is impossible. We find that $\mathfrak{m} \cap \mathbb{C}[x] = (x - \alpha)$. This implies that $\mathcal{V}/\mathfrak{m} = \mathbb{C}$ and $y \bmod \mathfrak{m} = \beta$ which satisfies $\beta^2 = \alpha(\alpha - 1)(\alpha - \lambda)$. In other words, taking the point P with coordinate $(\alpha, \beta) \in V$, we find $\mathcal{V} = \mathcal{V}_P$.

If $x \notin \mathcal{V}$, we find $z' = \frac{1}{x} \in \mathcal{V}$. Then we see easily that $\mathcal{V} = \mathcal{V}_\infty$. We have found the following fact:

$$R \cong \{\mathcal{V} \mid \mathcal{V} \text{ is a DVR with a valuation trivial on } \mathbb{C}\}.$$

This is an algebraic interpretation by Oscar Zariski of a Riemann surface as a space of all valuations trivial on \mathbb{C} , and the space at the right-hand side of the above identity is called a *Zariski–Riemann space*. It is intriguing that all rational primes correspond to discrete valuations of \mathbb{Q} , and we might want to think that \mathbb{Q} is an arithmetic analogue of a Riemann surface.

For a smooth projective curve V defined over a field K , we write $K(V)$ for its field of K -rational meromorphic functions, and $V(M)$ denotes the set of M -rational points of the curve V for an extension M/K . For a point P of V algebraic over K , we write $K(P)$ for the field generated over K by the coordinates of P .

Theorem 2.24 *For a given algebraic function field \mathfrak{K} defined over a field K , there exists a unique smooth projective curve V defined over K such that $\mathfrak{K} \cong K(V)$. We also have a canonical one-to-one onto correspondence:*

$$V(K) \cong \{\text{discrete valuations of } \mathfrak{K} \text{ trivial over } K^\times \text{ with residue field } K\}.$$

If $\mathfrak{K}'/\mathfrak{K}$ is an extension of algebraic function fields defined over K , the corresponding smooth projective algebraic curve gives rise to a covering $\pi : V' \rightarrow V$

such that $f \mapsto f \circ \pi$ gives the inclusion $\mathfrak{K} \hookrightarrow \mathfrak{K}'$. In particular $\mathcal{V}_P \cap \mathfrak{K} = \mathcal{V}_{\pi(P)}$ for the valuation ring \mathcal{V}_P corresponding to $P \in V'$.

Proof. We generalize the argument (in the two examples) of making a projective algebraic curve out of valuations of \mathfrak{K} for a general algebraic function field over a field K . We start with $K(\mathbf{P}^1) = K(x)$ with one transcendental element x . The main tool is the fact that $K[x]$ is a principal ideal domain. Pick a nonzero prime ideal P of $K[x]$. Pick $f \in P$, and factorize f into a product $f = c \prod_t t(x)^{e(t)}$ of irreducible monic polynomials $t(x)$ with a constant $c \in K^\times$. Since P is a prime, one of the irreducible factors $t(x)$ has to be in P . Then $K(P) = K[x]/P$ is covered by $K[x]/(t(x))$, which is a finite extension of K . We get a surjective field homomorphism $\pi : K[x]/(t(x)) \rightarrow K(P) = K[x]/P$. Since a field homomorphism is always injective (a field only has two ideals: (0) or itself), we find $K(P) = K[x]/(t(x))$ and $P = (t(x))$. So any nonzero prime ideal is a maximal ideal. We define the valuation $v_P : K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ by $v_P(f) = v_P(c \prod_t t(x)^{e(t)}) = e(t)$. Then the valuation ring $\mathcal{V}_P = \{f \in K(x) | v_P(f) \geq 0\}$ is associated with the point P by $\mathfrak{m}_P \cap K[x] = P$ for the maximal ideal $\mathfrak{m}_P = \{f \in \mathcal{V}_P | v_P(f) > 0\}$.

We study $\mathcal{V}_P/\mathfrak{m}_P^n \cong K[x]/P^n$, because $\mathfrak{m}_P^j/\mathfrak{m}_P^{j+1} = (K[x]/P)t(x)^j = P^j/P^{j+1}$. For a given $f \in K[x]$, by the division algorithm, we find a quotient $q \in K[x]$ and a remainder r such that $f = tq + r$ with $\deg(r) < \deg(t(x))$; so, we may regard r as a unique element in $K(P)$. We again apply the division algorithm to q , getting $q = tq_1 + r_1$; in other words, $f = r + r_1t + t^2q_1$. Repeating this process, we can expand f into: $f = r + r_1t + r_2t^2 + r_3t^3 + \dots$. This appears to be an infinite series, but is actually a finite sum by comparing the degrees of the both sides. We write $\widehat{\mathcal{V}}_P = K(P)[[t]]$, which is a formal power series ring, and embed \mathcal{V}_P into $\widehat{\mathcal{V}}_P$ by the above expansion; so, the image of \mathcal{V}_P is made up of polynomials in t with coefficients in $K(P)$. If one introduces the projective limit of $\mathcal{V}_P/\mathfrak{m}_P^n$, we find $\widehat{\mathcal{V}}_P = \varprojlim_n \mathcal{V}_P/\mathfrak{m}_P^n$.

For a given valuation ring $\mathcal{V} = \{f \in K(x) | v(f) \geq 0\}$ with $v(K^\times) = 0$ (but $v(K(x)) = \mathbb{Z} \cup \{\infty\}$), we find either $x \in \mathcal{V}$ or $x \notin \mathcal{V}$. If $x \in \mathcal{V}$, then $K[x] \subset \mathcal{V}$; so, v is a valuation on $K[x]$. Since v cannot be trivial over $K[x]$ (otherwise, it is trivial on $K(x)$), the intersection $\mathfrak{m} \cap K[x]$ is a prime ideal P of $K[x]$. Then $v = v_P$ because $v(f) \geq m \iff f \in \mathfrak{m}^m \cap K[x] = P^m$ because P is principal. If $x \notin \mathcal{V}$, then $x^{-1} \in \mathcal{V}$, and for the prime $Q = (x^{-1})$ in $K[x^{-1}]$, we have $K[x^{-1}]_Q = \mathcal{V}$, and \mathcal{V} corresponds to the point $\infty = Q$.

If K is algebraically closed, each nonzero prime ideal of $K[x]$ is the form of $(x - \alpha)$ with $\alpha \in K$, which tells us

$$\{\mathcal{V} | \text{valuation rings of } K(x) \text{ trivial on } K\} \cong K \cup \{\infty\} = \mathbf{P}(K) \quad (\text{canonically}).$$

If K is not algebraically closed, take an algebraic closure \overline{K} of K . Defining $\mathbf{P}(K)$ by the set of points in $\mathbf{P}(\overline{K})$ with coordinates in K , we have

$$\{\mathcal{V} | \text{valuation rings of } K(x) \text{ trivial on } K \text{ with } K(P) = K\} \cong \mathbf{P}(K).$$

The set $\{\mathcal{V} \mid \text{valuation rings of } K(x) \text{ trivial on } K\}$ is called the set of closed points of \mathbf{P} . They are associated with a maximal ideal of $K[x]$ or $K[x^{-1}]$. Of course, if \mathcal{V} is associated with $(t(x))$ and $t(x) \neq x$, then the same \mathcal{V} is associated with $x^{-\deg(t)}t(x) \in K[x^{-1}]$ because $v_P(x) = 0$ if $t(x) \neq x$. Thus we find

$$\begin{aligned} & \{\text{closed points of } \mathbf{P}/_K\} \\ &= \{\text{maximal ideals of } K[x]\} \cup \{\text{maximal ideals of } K[x^{-1}]\}. \end{aligned}$$

We now treat a general case of algebraic function fields not necessarily a rational function field $K(x)$. For a given valuation v , the *residue field* of v means the residue field of the valuation ring of v . Let \mathfrak{K} be an algebraic function field defined over K , and choose elements x and y so that $\mathfrak{K} = K(x, y)$ and y is separably integral over $K[x]$. Let R be the integral closure of $K[x]$ in \mathfrak{K} . Since $K[x]$ is a principal ideal domain and the quotient field of R (i.e., \mathfrak{K}) is a finite extension of $K(x)$, we find that R is free of rank $[\mathfrak{K} : K(x)]$ over $K[x]$. Since R is a finite integrally closed extension of the principal ideal domain $K[x]$, R is a Dedekind domain ([CRT] Section 11). So each nonzero fractional R -ideal \mathfrak{a} has a prime decomposition $\mathfrak{a} = \prod_P P^{e(P)}$ into a product of prime ideals P ($e(P) \in \mathbb{Z}$). With each prime ideal of R , we can associate a valuation $v_P : \mathfrak{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ by $v_P(f) = e(P)$ if $(f) = fR = \prod_P P^{e(P)}$. For any given valuation ring \mathcal{V} associated with a valuation $v : \mathfrak{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ with $v(K^\times) = 0$ but $v(\mathfrak{K}^\times) = \mathbb{Z}$, we find $x \in \mathfrak{K}$ transcendental over K such that $x \in \mathcal{V}$. Thus all valuations v as above are of the form v_P for a suitable choice of x and a prime ideal P of an integral closure R of $K[x]$. Thus we may identify

$$V(K) = \left\{ v : \text{discrete valuation} \mid \begin{array}{l} v(K^\times) = 0 \text{ and } v(\mathfrak{K}^\times) = \mathbb{Z} \\ \text{with residue field } K \end{array} \right\}.$$

Any prime ideal P of $K[x]$ is decomposed into a product of primes P_1, \dots, P_g in R . If K is algebraically closed, then there are g distinct points over a given point $P = (x - \alpha)$ of \mathbf{P} for $\alpha \in K$. If K is not algebraically closed, $K(P_i)$ for some i may be a nontrivial finite extension of K . In other words, in the algebraic closure \overline{K} of K , we have at most $[K(P_i) : K]$ (geometric) points coming out of P_i corresponding to embeddings of $K(P_i)$ into \overline{K} .

If furthermore, $R = K[x, y]$ for another element $y \in \mathfrak{K}$, we have an equation $f(X, Y) = Y^g + a_1(X)Y^{g-1} + \dots + a_g(X)$ satisfied by (x, y) . So for a given point $P = (x - \alpha) \in \mathbf{P}(K)$, the point $(\alpha, \beta) \in \overline{K}^2$ satisfying $f(\alpha, \beta) = 0$ gives rise to a point P_i over P in \mathbf{P}^2 . In this way, $P_i \mapsto (\alpha, \beta)$ supplies us with a projective embedding of $V(\overline{K})$ into $\mathbf{P}^2(\overline{K})$. The image is the projective algebraic curve defined by the equation $f(X, Y) = 0$ in \mathbf{P}^2 (or more precisely, using the homogeneous coordinate (X, Y, Z) , it is defined by $Z^g f(\frac{X}{Z}, \frac{Y}{Z}) = 0$). Thus except for finitely many points, there are really g distinct points in $V(\overline{K})$ over a given point $P \in \mathbf{P}(\overline{K})$. More generally, if $R = K[x, y_1, \dots, y_m]$, then $P \mapsto (x, y_1, \dots, y_m)$ gives an embedding of V into the $(m+1)$ -dimensional projective space \mathbf{P}^{m+1} .

If we take a proper subring $K[x, y] \subsetneq R$ such that $\mathfrak{K} = K(x, y)$, the ring $K[x, y]$ is not integrally closed. In other words, for $P \in V(K)$, x and y generate a subring \mathcal{V}'_P of the valuation ring. Since $\mathfrak{m}_P \cap K[x] = (t(x))$ for an irreducible polynomial $t(x)$, $\mathfrak{m}_P^e \subset \mathcal{V}'_P$ for some $e \leq g$ (since $P^g \subset (t(x))\mathcal{V}_P$).

Let $f(X, Y)$ be the equation of (x, y) . We can think of the projective algebraic curve $C \subset \mathbf{P}^2$ defined by this equation. Then if K is algebraically closed, $\alpha = (x \bmod P) \in K(P) = K$ and $\beta = (y \bmod P) \in K$ gives a point (α, β) of C in \mathbf{P}^2 . Even if V does not ramify, in $C(K)$, $P' = (\alpha, \beta)$ has extra ramification, and \mathcal{V}'_P is not a valuation ring.

We have a natural morphism $V \rightarrow C \rightarrow \mathbf{P}$ taking $P \mapsto (\alpha, \beta) \mapsto \alpha$. In this sense, V is the largest projective algebraic curve (over \mathbf{P} with coordinate x) giving rise to the algebraic function field \mathfrak{K} .

For a projective algebraic curve C , we consider its function field $K(C)$ and \mathcal{V}'_P made up of functions in $K(C)$ finite at $P \in C$. If \mathcal{V}'_P is a valuation ring, we call P a smooth point. The projective algebraic curve C giving rise to a given algebraic function field \mathfrak{K} is called a model of \mathfrak{K} . Among models of \mathfrak{K} , there is a unique model smooth everywhere, which is called the *smooth* or *non-singular* model of \mathfrak{K} . If $\mathfrak{K}'/\mathfrak{K}$ is a finite extension, by the above construction, we have a covering map $V' \rightarrow V$ as defined in the theorem. \square

For each point $P \in V(K)$ for V as in the theorem, $f \in \mathfrak{K}$ has an expansion $f(t) = \sum_{n \gg -\infty} a_n t^n$ with $a_n \in K(P)$ for a generator t of $P\mathcal{V}_P$. An element $t \in \mathfrak{K}$ giving rise to the generator t of P is called a *uniformizer* at P .

Corollary 2.25 *Let the notation and assumption be as in the theorem. Then the morphism $\pi : V' \rightarrow V$ is a polynomial map of the projective coordinates.*

Proof. Let R (resp. R') be the integral closure of $K[x]$ in \mathfrak{K} (resp. \mathfrak{K}'). Choose generators so that $R = K[x, y_1, \dots, y_m]$ and $R' = K[x, y'_1, \dots, y'_n]$. Since $R \subset R'$, we find $x = f_0(x, y'_1, \dots, y'_n)$ and $y_i = f_i(x, y'_1, \dots, y'_n)$. Then $\pi((x, y'_1, \dots, y'_n)) = (x, y_1, \dots, y_m)$, as desired. \square

Since any field embedding $\sigma : \mathfrak{K} \rightarrow \mathfrak{K}'$ brings \mathfrak{K} into a subfield $\sigma(\mathfrak{K})$, we have a morphism $\pi : V' \rightarrow V_\sigma$ of projective algebraic curves V' and V_σ corresponding to \mathfrak{K}' and $\sigma(\mathfrak{K})$ as long as σ leaves the field of definition stable (even if σ is nontrivial on K). If \mathfrak{K} is defined by $f(X, Y_1, \dots, Y_m)$, then $\sigma(\mathfrak{K})$ is obviously defined by the polynomial $\sigma(f)(X, Y_1, \dots, Y_m)$ obtained from f by applying σ to the coefficients in K of $f(X, Y_1, \dots, Y_m)$. Thus V_σ as above is actually given by the conjugate $\sigma(V)$ (i.e., $\sigma(V)(\overline{K}) = \sigma(V(\overline{K}))$) for any choice of extension of σ to \overline{K} . We have proven:

Corollary 2.26 *Let V/K and V'/K be smooth projective curves. Then we have a canonical isomorphism $\text{Hom}_K(V, V') \cong \text{Hom}_K(K(V'), K(V))$ given by $K(V') \ni \phi \mapsto \phi \circ f$ for a morphism $f : V \rightarrow V'$ of projective curves, where $\text{Hom}_K(V, V')$ is the collection of morphisms of projective curves defined over K and $\text{Hom}_K(K(V'), K(V))$ is the set of all field homomorphisms over K .*

For each $f \in \text{Hom}_K(V, V')$, taking the corresponding field homomorphism $\sigma : K(V') \hookrightarrow K(V)$, we define the degree of the morphism f by the field extension degree $[K(V) : \sigma(K(V'))]$. By definition, $\deg(f)$ also can be given by $\text{rank}_{\mathcal{V}_{P'}} (\oplus_{P \in f^{-1}(P')} \mathcal{V}_P)$ for any choice of a closed point $P' \in V'$.

Exercises

1. Prove the surjectivity of v_P so that \mathcal{V}_P in (2.6) is a DVR.
2. For a valuation ring \mathcal{V} of $K(x)$ of a valuation trivial on K but nontrivial on $K(x)$, if $x \notin \mathcal{V}$, show that $\mathcal{V} = K[z]_{(z)}$ for $z = x^{-1}$.
3. Describe the intersection in $\mathbf{P}(K)$:

$$\{\text{maximal ideals of } K[x]\} \cap \{\text{maximal ideals of } K[x^{-1}]\}.$$

4. Give a more detailed proof of Corollary 2.25.

2.4.2 Zariski Topology

Let \mathfrak{K} be an algebraic function field over an algebraically closed field K . We write V for its Zariski–Riemann space or equivalently the set of K -rational points of the associated smooth projective algebraic curve. We equip $V(K)$ with a topology in the following way. We cover V by “open” affine subvarieties. In the language of schemes, an open affine subvariety $U \subset V$ is given by the spectrum of an integral domain R ; that is, $U = \text{Spec}(R)$ and $V - U$ is a proper closed subset of V (i.e., heuristically, a subset defined by the zero set of polynomial equations whose meaning becomes clear later).

Recall that v_P is the valuation $v_P : \mathfrak{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ associated with each point $P \in V(K)$. We put

$$\begin{aligned} \mathcal{V}_P &= \{f \in \mathfrak{K} \mid v_P(f) \geq 0\} \quad (\text{the discrete valuation ring of } v_P), \\ \mathfrak{m}_P &= \{f \in \mathcal{V}_P \mid v_P(f) > 0\} \quad (\text{the maximal ideal of } \mathcal{V}_P), \text{ and} \\ K(P) &= \mathcal{V}_P / \mathfrak{m}_P \quad (\text{the residue field of } \mathcal{V}_P). \end{aligned} \tag{2.7}$$

For each nonconstant $x \in \mathfrak{K}$, we can think of

$$R_x = \bigcap_{\mathcal{V}_P \ni x} \mathcal{V}_P \subset \mathfrak{K}. \tag{2.8}$$

Then R_x is the integral closure of the polynomial ring $K[x]$ in \mathfrak{K} (Exercise 1), and \mathcal{V}_P is the localization of R_x at $P_x = P \cap R_x$ (Exercise 2). Then the set $\text{Spec}(R_x)(K)$ of all maximal ideals of R_x is in bijection with $V_x = \{P \in V \mid \mathcal{V}_P \ni x\}$ (see [GME] 1.2 and 1.4.3 for $\text{Spec}(R_x)$). We also have $V = \bigcup_{y \in \mathfrak{K} - K} V_y = V_x \cup V_{1/x}$. For each $P \in V$ and for $x \in \mathcal{V}_P$ (so, $P \in V_x$), V_x is called an open affine neighborhood of P . Any finite intersection $V_{x_1} \cap \cdots \cap V_{x_m}$ of $V_{x_j} \ni P$ ($j = 1, 2, \dots, m$) is also called an open affine neighborhood of P . Each open affine neighborhood U of x is in bijection with the set of maximal

ideals $\text{Spec}(R)(K)$ of a subring $R \subset \mathfrak{K}$ finitely generated over K . For example, $V_x \cong \text{Spec}(R_x)(K)$ and $V_x \cap V_y \cong \text{Spec}(R_x \cdot R_y)(K)$ ($R_x \cdot R_y$ is the composite ring of R_x and R_y in \mathfrak{K}), because $\mathcal{V}_P \supset R_x \cdot R_y \Leftrightarrow \mathcal{V}_P \supset R_x$ and $\mathcal{V}_P \supset R_y$. This topology we defined on V is called the *Zariski topology* on V .

2.4.3 Divisors

We now introduce divisors on an algebraic curve V . We start with interpreting elements in \mathfrak{K} as a function defined on V with values in the projective space \mathbf{P}^1 . Each $f \in \mathfrak{K} - K$ gives rise to an inclusion $K(f) \hookrightarrow \mathfrak{K}$ and hence gives rise to a (rational or meromorphic) function $f : V \rightarrow \mathbf{P}^1$ with

$$f(P) = \begin{cases} P \cap K[f] \in \mathbf{P}_f^1 & \text{if } P \in V_f, \\ P \cap K[\frac{1}{f}] \in \mathbf{P}_{1/f}^1 & \text{if } P \in V_{1/f}, \end{cases}$$

where $\mathbf{P}_f^1 = \{P \in \mathbf{P}^1 | P \ni g\}$. This is well-defined by the following. If $P \in V_f$, then $P \cap K[f] = (f - \alpha)$ for $\alpha \in K = \mathbf{P}_f^1$, and $\alpha = (f \bmod P) = f(P)$. If $P \in V_f \cap V_{1/f}$, then $P \cap K[\frac{1}{f}] = (\frac{1}{f} - \frac{1}{\alpha})$ and still $f(P) = \alpha$. If $P \notin V_f$, then $f(P) = \infty$. When $f(P) = 0$, we call P a zero of f and when $f(P) = \infty$, we call P a pole of f . For $f \in K$, we associate a constant function $f : V \rightarrow \mathbf{P}^1$ with value f everywhere. In this way, we can identify \mathfrak{K} with the set of all meromorphic functions on V .

For each $P \in V$, take $t = t_P$ with $v_P(t_P) = 1$ (such a t_P always exists because $v_P : \mathfrak{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ is surjective). By definition, $\mathfrak{m}_P = (t_P)$ in \mathcal{V}_P . Then we can expand $f \in \mathfrak{K}$ into a Laurent series of t_P as follows. First suppose that P is not a pole of f . Then $f - f(P)$ has zero at P ; so, $f_1 = (f - f(P))/t_P$ does not have a pole at P ; so, we have $f - (f(P) + f_1(P)t_P)$ is divisible by t_P^2 and so on. We thus have $f = \sum_{n \geq 0} c_n t_P^n \in K[[t_P]]$. If f has a pole at P , killing the pole by multiplying f by $t_P^{|v_P(f)|}$, $g = t_P^{|v_P(f)|} f$ does not have a pole at P ; so, we apply the above argument, and after expanding g into a power series of t_P , we divide the power series by $t_P^{|v_P(f)|}$ to get the Laurent expansion of f . We have $f = \sum_{n \geq v_P(f)} c_n t_P^n \in K((t_P)) = K[[t_P]][\frac{1}{t_P}]$. If we choose another t'_P with $v_P(t'_P) = 1$, we find that $t_P = t'_P(c_0 + c_1 t'_P + c_2 t'^2_P + \dots)$ with $c_0 \neq 0$. Thus $t'_P/t_P \in \mathcal{V}_P^\times$ and if we write the power series expansion of f with respect to t_P as $f(t_P)$, then we get $f(t'_P)$ by substituting $t_P(t'_P)$ for t_P (check that this substitution gives a well-defined power series in t'_P because $t_P(P) = 0$).

The divisor $\text{div}(f)$ of $f \neq 0$ is defined by a formal sum $\sum_P v_P(f)P$ (in some classical books in number theory, they use multiplicative notation, such as $\text{div}(f) = \prod_P P^{v_P(f)}$, because it corresponds to the prime decomposition of the ideal (f) , but we use additive symbols following the geometric tradition). Since f satisfies a polynomial equation of finite degree over $K[x]$ for a suitably chosen $x \in \mathfrak{K}$, f has only finitely many zeros and poles; thus the sum defining $\text{div}(f)$ is actually a finite sum (because $v_P(f) = 0$ except for finitely many points $P \in V$).

We define the *divisor* group $\text{Div}(V) = \text{Div}(\mathfrak{K})$ by the free abelian group of all formal finite sums $D = \sum_{P \in V} e_P P$, where $e_P = 0$ except for finitely many $P \in V$. We define the *degree* of a divisor $D = \sum_{P \in V} e_P P$ by $\deg(D) = \sum_P e_P$. We have a homomorphism $\deg : \text{Div}(V) \rightarrow \mathbb{Z}$, and we define $\text{Div}^0(V) = \text{Ker}(\deg)$.

Proposition 2.27 *If $f \in \mathfrak{K}$, then $\deg(\text{div}(f)) = 0$; so, $\text{div}(f) \in \text{Div}^0(V)$.*

Proof. We may assume that $f \in \mathfrak{K} - K$, because the assertion is clear for $f \in K^\times$. The inclusion $K(f) \hookrightarrow \mathfrak{K}$ induces a projection $f : V \rightarrow \mathbf{P}^1$. Then for each $p \in \mathbf{P}^1$, regarding it as a prime ideal of $K[f]$, we find $pR = \prod_P P^{e_P}$ with prime ideals P in the integral closure R of $K[f]$. Then by definition, we have $f(P) = 0 \Leftrightarrow e_P > 0$ and $\sum_P e_P = [R : K[f]] = [\mathfrak{K} : K(f)]$. In particular, writing $\infty = \prod_Q Q^{e'_Q}$ for the points Q with $f(Q) = \infty$, we find that

$$\deg(\text{div}(f)) = \sum_P e_P - \sum_Q e'_Q = [\mathfrak{K} : K(f)] - [\mathfrak{K} : K(f)] = 0$$

as desired. \square

Write $\mathcal{P}(V) = \{\text{div}(f) | f \in \mathfrak{K}^\times\}$. Then $\mathcal{P}(V)$ is a subgroup of $\text{Div}^0(V)$. The quotient group $\text{Pic}(V) = \text{Div}(V)/\mathcal{P}(V)$ (resp. $\text{Jac}(V) = \text{Pic}^0(V) = \text{Div}^0(V)/\mathcal{P}(V)$) is called the Picard group (resp. the Jacobian) of V . When $D - D' \in \mathcal{P}(V)$, we say that D is *linearly* equivalent to D' , and if $\deg(D) = \deg(D')$, we call D is *algebraically* equivalent to D' .

2.4.4 Differentials

We introduce a notion of differential forms on an algebraic curve V in a purely algebraic way. For the moment, until the end of the proof of Theorem 2.29, we suppose that K is algebraically closed.

For a given $f \in \mathfrak{K}$, we formally define df as a collection of power series $df(t_P) = \frac{df(t_P)}{dt_P} dt_P$. Here P runs through all points $P \in V$, and

$$\frac{d(\sum_n c_n t_P^n)}{dt_P} dt_P = \left(\sum_n c_n n t_P^{n-1} \right) dt_P.$$

In particular, df does not have the term $\frac{1}{t_P}$. If we change coordinate t_P into t'_P , the expression of df will change according to the chain rule:

$$df(t'_P) = \frac{df(t'_P)}{dt'_P} dt'_P = \frac{df(t'_P(t_P))}{dt'_P} \frac{dt'_P}{dt_P} dt_P.$$

We also think of $\omega = gdf$ as a collection of power series $\{g(t_P) \frac{df(t_P)}{dt_P} dt_P\}_{P \in V}$. In other words, if gdf and $g'df'$ give rise to the same power series at every $P \in V$, we identify $gdf = g'df'$. The totality of all differentials on V gives

rise to a vector space over \mathfrak{K} . We see $gdf/g'df' = \frac{g}{g'} \frac{df}{df'} \in \mathfrak{K}$, because f and f' satisfy the polynomial relation $F(f, f') = 0$ over K . In other words, if $F(X, Y) = \sum_{i,j} a_{i,j} X^i Y^j$, then taking a formal derivative of $F(f, f') = 0$, we have

$$0 = dF(f, f') = \sum_{i,j} \left(i a_{i,j} f^{i-1} f'^j df + j a_{i,j} f^i f'^{j-1} df' \right),$$

and df and df' are linearly dependent over \mathfrak{K} . Thus this vector space over \mathfrak{K} is one-dimensional.

We define $v_P(gdf) = v_P(g \frac{df(t_P)}{dt_P})$. Note here that $v_P\left(\frac{dt'_P}{dt_P}\right) = 0$ for two parameters t_P and t'_P at $P \in V$. By the chain rule, $\frac{df}{dt_P} = \frac{df}{dt'_P} \frac{dt'_P}{dt_P}$, we have

$$v_P\left(g \frac{df}{dt_P}\right) = v_P\left(g \frac{df}{dt'_P} \frac{dt'_P}{dt_P}\right) = v_P\left(g \frac{df}{dt'_P}\right) + v_P\left(\frac{dt'_P}{dt_P}\right) = v_P\left(g \frac{df}{dt'_P}\right).$$

Since the last expression of the above formula is the value $v_P(gdf)$ computed with respect to the coordinate t'_P , the value $v_P(gdf)$ is well-defined independently of the choice of the parameter t_P around P . In particular, we have

$$gdf = \left(g \frac{df(t_P)}{dt_P}\right) dt_P = \left(\sum_{n \geq v_P(gdf)} c_n t_P^n\right) dt_P.$$

We define $\text{div}(\omega) = \sum_P v_P(\omega)P$.

Since differentials form a one-dimensional vector space over \mathfrak{K} , for any two differentials ω and ω' , $\text{div}(\omega)$ and $\text{div}(\omega')$ are linearly equivalent. Thus $\deg(\text{div}(\omega))$ is independent of the choice of ω . Writing $\deg(\omega) = 2g - 2$, we define the genus $g = g(V)$ of V .

A differential ω is called *holomorphic* or *of the first kind* if $v_P(\omega) \geq 0$ for all $P \in V$. If ω' is holomorphic, writing $\omega' = f\omega$, we find $\text{div}(f) + \text{div}(\omega) = \text{div}(\omega') \geq 0$ (we write $D \geq 0$ for $D = \sum_P e_P P$ if $e_P \geq 0$ for all P). We have

$$f \in L(\text{div}(\omega)) = \{g \in \mathfrak{K} \mid \text{div}(g) \geq -\text{div}(\omega)\}.$$

The space $\Omega_{V/K}$ of all holomorphic differentials is isomorphic to $L(\text{div}(\omega))$ by $f\omega \leftrightarrow f$ for any choice ω of nonzero differentials, and $\dim_K L(\text{div}(\omega)) = \dim_K \Omega_{V/K}$ is finite and independent of the choice of ω (see Lemma 2.30). We later show (see Theorem 2.31) that this dimension is given by the genus g ; so, $g \geq 0$.

For a differential $\omega = gdf$, we expand it into a power series in t_P at $P \in V$, and write

$$\omega = \left(\sum_{n \geq v_P(\omega)} c_n t_P^n\right) dt_P.$$

Then we define $\text{Res}_P(\omega) = c_{-1}$.

Proposition 2.28 *The residue $\text{Res}_P(\omega)$ is well-defined independently of the choice of the parameter t_P .*

Since ω has only finitely many poles, $\text{Res}(\omega) = \sum_P \text{Res}_P(\omega) \in K$ is well-defined.

Proof. We give a proof valid only when K is of characteristic 0. See [ALF] Appendix and [ALG] Theorems III.7.14.1–2 for the proof valid for arbitrary characteristics. Choose two parameters $t = t_P$ and $t' = t'_P$, and expand $t' = a_1 t + a_2 t^2 + \cdots$ with $a_1 \neq 0$. If the expansion of $\omega = gdf$ with respect to t is given by $g \frac{df}{dt'} dt' = \sum_n c_n t'^n dt'$, the one with respect to t is given by

$$g \frac{df}{dt} dt = g \frac{df}{dt'} \frac{dt'}{dt} dt = \sum_n c_n (a_1 t + a_2 t^2 + \cdots)^n \left(\sum_j j a_j t^{j-1} \right) dt.$$

Let us look into the term involving t^{-1} :

$$c_{-1} (a_1 t + a_2 t^2 + \cdots)^{-1} \left(\sum_{j \geq 1} j a_j t^{j-1} \right) dt = \frac{c_{-1} a_1}{a_1} + \text{higher terms}.$$

We need to show that $c_n (a_1 t + a_2 t^2 + \cdots)^n \left(\sum_j j a_j t^{j-1} \right) = c_n t'^n \frac{dt'}{dt}$ for $n \neq -1$ does not involve the term t^{-1} . This follows from $t'^n \frac{dt'}{dt} = \frac{1}{n+1} \frac{dt'^{n+1}}{dt}$, since the Laurent series expansion of $\frac{d\phi}{dt}$ does not involve the term t^{-1} which is not a derivative of a power of t . This finishes the proof.

Since $\mathfrak{K}/K(x)$ is a separable finite extension for a nonconstant $x \in \mathfrak{K}$, we have the trace map $\text{Tr}_{\mathfrak{K}/K(x)} : \mathfrak{K} \rightarrow K(x)$ for any nonconstant function x . We study how the residue map behaves under field extensions using the trace map. The inclusion $K(x) \hookrightarrow \mathfrak{K}$ is induced by the projection $x : V \rightarrow \mathbf{P}^1$. For a prime ideal p of $K[x]$, we consider $x^{-1}(p) = \{P\}$; thus, $pR = \prod_P P^{e_P}$ for the integral closure R of $K[x]$ in \mathfrak{K} .

By the Chinese remainder theorem, $R/pR \cong \prod_P R/P^{e_P}$ and $R/p^n R \cong \prod_P R/P^{ne_P}$. Thus the completion of \mathfrak{K} with respect to p is given by $\mathfrak{K}_p = \prod_{P:x(P)=p} \mathfrak{K}_P$. In particular, we have $\text{Tr}_{\mathfrak{K}/K(x)}(f) = \sum_{P:x(P)=p} \text{Tr}_{\mathfrak{K}_P/K(x)_p}(f)$ for $f \in \mathfrak{K}$, because $\text{Tr}_{\mathfrak{K}/K(x)}(f)$ is $\text{Tr}(\rho(f))$ for the matrix $\rho(f) \in M_n(K(x))$ given by $(fg_1, fg_2, \dots, fg_d) = (g_1, \dots, g_d)\rho(f)$ for a base g_j of $\mathfrak{K}/K(x)$.

In $\mathfrak{K}_P = K[[t]]$ ($t = t_P$), we find $t^e = ut_p$ ($e = e_P$) for a unit power series $u = c_0 + c_1 t + c_2 t^2 + \cdots$ with $c_0 \neq 0$. We can take an e th root v of u in $K[[t]]$ because K is algebraically closed. Changing t by vt , we may assume that $K(x)_p = K((t^{e_P}))$ and $t_p = t^e$. Then we realize that $K((t))$ is a Galois extension of $K(x)_p = K((t^e))$ with the Galois group isomorphic to the group of e th roots of unity μ_e . Each $\zeta \in \mu_e$ acts on t by $t \mapsto \zeta t$. Then

$$\text{Tr}_{\mathfrak{K}_P/K(x)_p} t^n = \left(\sum_{\zeta \in \mu_e} \zeta^n \right) t^n = \begin{cases} 0 & e \nmid n, \\ et^n & \text{if } e \mid n. \end{cases}$$

We see that for $t^n \in \mathfrak{K}_P$, $\text{Res}_P(\text{Tr}_{\mathfrak{K}_P/K(x)_P}(t^n)d(t^e)) = e$ or 0 accordingly as $n = -e$ or not. On the other hand, we see $\text{Res}_P(t^n d(t^e)) = \text{Res}_P(et^{n+e-1}dt) = e$ or 0 accordingly as $n = -e$ or not, because $t^n \frac{dt^e}{dt} = et^{n+e-1}$. Thus $\text{Res}_P(\text{Tr}_{\mathfrak{K}/K(x)}(f)dt_P) = \sum_{P:x(P)=p} \text{Res}_P(fdt_P)$, and hence we get, for all $f \in \mathfrak{K}$,

$$\sum_{p \in \mathbf{P}^1} \text{Res}_p(\text{Tr}_{\mathfrak{K}/K(x)}(f)dx) = \sum_{P \in V} \text{Res}_P(fdx). \quad (2.9)$$

Theorem 2.29 (Residue Theorem) *For every differential ω on V , we have $\sum_{P \in V} \text{Res}_P(\omega) = 0$.*

Proof. Pick $x \in \mathfrak{K} - K$. Since the space of differentials is one-dimensional over \mathfrak{K} , we can write $\omega = fdx$ for $f \in \mathfrak{K}$. Then by (2.9), we may assume that $\mathfrak{K} = K(x)$. Since $\mathbf{P}^1 = K \cup \{\infty\}$, for each $\alpha \in K$, we take $t_\alpha = x - \alpha$ to be our parameter. At ∞ , we choose $t_\infty = \frac{1}{x}$ to be the parameter there. For each $f \in K(x)$, expand $f = \sum_n c_n t_\alpha^n$ and define $[f]_\alpha = \sum_{n < 0} c_n t_\alpha^n$. Then $[f]_\alpha = 0$ except for finitely many α and $\phi = f - \sum_{\alpha \in \mathbf{P}^1} [f]_\alpha \in K$, because $f - [f]_\alpha \in K[x]_{(x-\alpha)} = \mathcal{V}_\alpha$ and $\sum_{\beta \neq \alpha} [f]_\beta \in \mathcal{V}_\alpha$ (which implies the difference ϕ is a rational function without a pole; so, constant by $\deg(\phi) = 0$). We expand $f = \sum_{\alpha \in K, j} \frac{c_{\alpha,j}}{(x-\alpha)^j} + \sum_{j \geq 0} a_j x^j$. We only need to check the vanishing for $t_\alpha^{-j} dx = t_\alpha^{-j} dt_\alpha$ and $x^j dx$ for $j \geq 1$. By computation, we have $\text{Res}_\alpha(x^j dx) = 0$ for all $\alpha \in K \cup \{\infty\}$ because $x^j dx = -t_\infty^{-j-2} dt_\infty$. Similarly (Exercise 5),

$$\text{Res}_\beta(t_\alpha^{-j} dt_\alpha) = \begin{cases} 1 & \text{if } \beta = \alpha \text{ and } j = 1, \\ -1 & \text{if } \beta = \infty \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases} \quad (2.10)$$

This finishes the proof.

We now treat the general case; so, K is an arbitrary field inside its algebraic closure \overline{K} . We suppose that K is algebraically closed in \mathfrak{K} . The composite $\overline{K}\mathfrak{K} \cong \mathfrak{K} \otimes_K \overline{K}$ is an algebraic function field over \overline{K} . We write V (resp. \overline{V}) for the Zariski–Riemann space of $\mathfrak{K} = K(V)$ (resp. $\overline{K}\mathfrak{K} = \overline{K}(\overline{V})$). Then we have a natural inclusion $V(K) \hookrightarrow \overline{V}(\overline{K})$. Note here that $V(K) = \{P \in V \mid K(P) = K\}$. If $K(P) \supsetneq K$, then there are $[K(P) : K]$ points corresponding to P . In other words, for points P_1, \dots, P_d with $d = [K(P) : K]$ in $\overline{V}(\overline{K})$, $P_j \cap \mathfrak{K} = P \Leftrightarrow v_{P_j}|_{\mathfrak{K}} = v_P$ or, equivalently, P_j corresponds to each field embedding $K(P) \hookrightarrow \overline{K}$. We define $\text{Res}_P(\omega) = \sum_j \text{Res}_{P_j}(\overline{\omega})$, where $\overline{\omega}$ is the differential of $\overline{K}\mathfrak{K}$ corresponding to $\omega = gdf$. Since $\text{Res}_{P_j}(\overline{\omega})$ for different j are conjugates of each other, we find $\text{Res}_P(\omega) \in K$. Similarly, we send P to the sum $\sum_j P_j$ (trace of P_j) in $\text{Div}(\overline{V})$ and in this way, we embed $\text{Div}(V)$ into $\text{Div}(\overline{V})$. This embedding sends $\mathcal{P}(V)$ into $\mathcal{P}(\overline{V})$, and we have \deg on $\text{Div}(V)$ by pulling back \deg defined on $\text{Div}(\overline{V})$. In this way, everything we stated (in

particular, the residue theorem, Theorem 2.29) is valid over the general field K (not necessarily algebraically closed).

Similarly to $L(\operatorname{div}(\omega))$, we define for a general divisor D ,

$$L(D) = \{f \in \mathfrak{K} \mid \operatorname{div}(f) \geq -D\},$$

where for two divisors $D = \sum_P e_P P$ and $D' = \sum_P e'_P P$, we write $D \geq D'$ if $e_P \geq e'_P$ for all P . Plainly $L(D)$ is a K -vector space.

Lemma 2.30 *The dimension $\dim_K L(D)$ is finite. In particular, we have $L(0) = K$ and $\dim_K L(0) = 1$.*

Proof. If f is nonconstant, $\operatorname{div}(f)$ is nontrivial (in \bar{V}) and $\deg(\operatorname{div}(f)) = 0$. Thus $L(0) \subset \bar{K} \cap \mathfrak{K} = K$ (by the definition of algebraic function field, the integral closure in \mathfrak{K} of the base field is itself). For sufficiently positive D' , we see $L(D) \subset L(D')$. Writing $D' = \sum_P e'_P P$ and expanding $f \in L(D')$ into a Laurent series of t_P at $P \in D'$, we have e'_P linear forms taking $f \in L(D')$ to the coefficient of t_P^{-j} for $0 < j \leq e'_P$. If all such linear forms vanish at f , we see $f \in L(0)$ and hence f is a constant. Thus $\dim_K L(D') < \infty$, which proves the desired assertion. \square

Since $f \cdot L(D) = L(D - \operatorname{div}(f))$, the dimension $\dim_K L(D)$ depends only on the linear equivalence class of D . For the linear equivalence class Ω of differential divisors, we have a well-defined number $\dim_K L(\Omega - D)$.

We introduce the following Riemann–Roch theorem (see [BNT] Chapter VI, [FAN] 7.2 and [GME] 2.1.3 for different proofs).

Theorem 2.31 *We have for all $D \in \operatorname{Div}(V)$,*

$$\dim_K L(D) = \deg(D) - g + 1 + \dim_K L(\Omega - D),$$

where g is the genus of the curve V .

Applying this theorem to the trivial divisor 0, we find

$$1 = \dim_K L(0) = \deg(0) - g + 1 + \dim_K L(\Omega),$$

which shows that $g = \dim_K L(\Omega) = \dim_K \Omega_{V/K}$ as we claimed before.

Exercises

1. Prove that R_x in (2.8) is the integral closure of $K[x]$ in \mathfrak{K} .
2. Prove that \mathcal{V}_P is the localization of R_x at $P_x = P \cap R_x$.
3. Show that V is not a Hausdorff space under its Zariski topology.
4. Prove Theorem 2.28 for an algebraic function field of characteristic $p > 0$.
5. Give a detailed proof of (2.10).

2.4.5 Adele Rings of Algebraic Function Fields

We insert a brief interpretation of differentials by the language of adeles (due to A. Weil; see [ALF] Chapter 2). We write \mathfrak{K}_P for the Laurent series ring: $K(P)((t_P))$ and consider the product ring $\prod_{P \in V} \mathfrak{K}_P$, which we consider as a \mathfrak{K} -algebra by embedding \mathfrak{K} diagonally. We define the adele ring $\mathfrak{K}_{\mathbb{A}}$ of \mathfrak{K} by

$$\mathfrak{K}_{\mathbb{A}} = \mathfrak{K} + \widehat{\mathcal{V}} \subset \prod_{P \in V} \mathfrak{K}_P,$$

where $\widehat{\mathcal{V}} = \prod_{P \in V} \mathcal{V}_P$ for $\mathcal{V}_P = K(P)[[t_P]]$. Here we do not assume that K is algebraically closed. Similarly to the case of \mathbb{Q} , we can identify

$$\mathfrak{K}_{\mathbb{A}} = \{(f_P)_{P \in V} \mid f_P \in \mathcal{V}_P \text{ except for finitely many } P\}. \quad (2.11)$$

For a divisor $D = \sum_P e_P P$, we define $\widehat{\mathcal{V}}(D) = \{(f_P) \in \widehat{\mathcal{V}} \mid v_P(f_P) \geq -e_P\}$. We equip with $\mathfrak{K}_{\mathbb{A}}$ the topology whose system of neighborhoods of $f \in \mathfrak{K}_{\mathbb{A}}$ is given by $f + \widehat{\mathcal{V}}(D)$ for all negative divisors D . Here we call D negative if $e_P \leq 0$ for all P . By definition, $\mathfrak{K}_{\mathbb{A}}$ becomes a topological ring. For each $f = (f_P)_P \in \mathfrak{K}_{\mathbb{A}}^{\times}$, we define its divisor $\text{div}(f) = \sum_P v_P(f_P)P$. This is well-defined since $v_P(f_P) = 0$ for almost all P if $f \in \mathfrak{K}_{\mathbb{A}}^{\times}$. In particular, $\widehat{\mathcal{V}}^{\times} = \{f \in \mathfrak{K}_{\mathbb{A}} \mid \text{div}(f) = 0\}$. Thus we have $\text{Div}(\mathfrak{K}_{\mathbb{A}}^{\times}) = \text{Div}(V)$ and hence

$$\text{Pic}(V) = \mathfrak{K}_{\mathbb{A}}^{\times} / \mathfrak{K}^{\times} \widehat{\mathcal{V}}^{\times}. \quad (2.12)$$

For each differential ω on V (supposing K to be algebraically closed), we define a K -linear form $\tilde{\omega} : \mathfrak{K}_{\mathbb{A}} \rightarrow K$ by $f \mapsto \sum_P \text{Res}_P(f\omega)$. Since $f_P \in \mathcal{V}_P$ for almost all P , $\text{Res}_P(f\omega) = 0$ for almost all P ; so, the linear form $\tilde{\omega}$ is well-defined. By definition, if $\text{div}(f\omega) = \text{div}(f) + \text{div}(\omega) \geq 0$, then $\tilde{\omega}(f) = 0$. Thus $\tilde{\omega}(\widehat{\mathcal{V}}(\text{div}(\omega))) = 0$, and hence $\tilde{\omega}$ is a continuous linear form on $\mathfrak{K}_{\mathbb{A}}$ with respect to the discrete topology on K and vanishes over (the diagonal image) \mathfrak{K} by Theorem 2.29.

We consider the space \mathcal{L} of continuous linear forms $f : \mathfrak{K}_{\mathbb{A}}/\mathfrak{K} \rightarrow K$. We know that \mathcal{L} is a vector space over \mathfrak{K} . Actually \mathcal{L} is isomorphic to the space of differentials by $\omega \mapsto \tilde{\omega}$. We could have defined the differentials as K -linear forms on $\mathfrak{K}_{\mathbb{A}}/\mathfrak{K}$, and the proof of the Riemann–Roch theorem can be given from this point of view (see [BNT] Chapter VI and [ALF] Chapter 2).

Exercises

1. Give a detailed proof of (2.11).
2. Prove that $\mathfrak{K}_{\mathbb{A}}$ is locally compact if and only if K is a finite field.
3. Prove that $\widehat{\mathcal{V}}(D) + \widehat{\mathcal{V}}(D') = \widehat{\mathcal{V}}([D, D'])$ for the least common multiple $[D, D']$ of D and D' .
4. Prove that $\widehat{\mathcal{V}}(D) \cap \widehat{\mathcal{V}}(D') = \widehat{\mathcal{V}}((D, D'))$ for the greatest common divisor (D, D') of D and D' .

2.5 Elliptic Curves over a Field

An algebraic function field \mathfrak{K}/K is called *elliptic* if its genus is equal to 1. The corresponding algebraic curve E/K with one designated point $\mathbf{0} \in E(K)$ is called an elliptic curve. The elliptic curve is a pair $(E, \mathbf{0})/K$. The point $\mathbf{0}$ is called the origin of E , and two elliptic curves E and E' are isomorphic if we have an isomorphism $\phi : E \cong E'$ of algebraic curves that sends the origin to the origin. We study elliptic curves over a field in detail here. When we regard the point $\mathbf{0}$ as a divisor, we write $[\mathbf{0}]$ instead of $\mathbf{0}$.

2.5.1 Dimension Formulas

For divisors $m[\mathbf{0}]$, we study $L(m[\mathbf{0}])$. Since $0[\mathbf{0}]$ is the trivial divisor 0, we find $L(0[\mathbf{0}]) = K$. By definition, $\Omega_{E/K}$ is one-dimensional over K . Since $\deg(\omega) = 2g - 2 = 0$ for a differential ω on E , if ω has a zero, then ω has to have a pole. If ω is holomorphic nonzero, it vanishes nowhere. In other words, nowhere-vanishing differentials are all nonzero multiples of ω . In particular, $\text{div}(\omega) = 0$. Recall the linear equivalence class of $\text{div}(\omega')$ for all meromorphic differentials ω' on E . Then Ω is the linear equivalence class of all meromorphic functions in \mathfrak{K} , and $L(\Omega - D) \cong L(-D)$. If $D > 0$, then $\dim_K L(-D) = 0$ (Exercise 1).

We fix a nowhere-vanishing differential ω . If $f \in L([\mathbf{0}])$, then f has possibly only one simple pole at $\mathbf{0}$. Thus $\text{Res}_{\mathbf{0}}(f\omega) = \sum_{P \in E} \text{Res}_P(f\omega) = 0$ by Theorem 2.29. The function f is in $L(0)$ and is constant, and $\dim_K L([\mathbf{0}]) = \dim_K L(0) = 1$. By the Riemann–Roch theorem, we find

$$\dim_K L(m[\mathbf{0}]) = \deg(m[\mathbf{0}]) - g + 1 + \dim_K L(-m[\mathbf{0}]) = m \quad \text{if } m > 0. \quad (2.13)$$

More generally, by the same proof, we get

Proposition 2.32 *Let E be an elliptic curve over a field K . If $D > 0$ is a positive divisor, we have $\dim_K L(D) = \deg(D)$.*

We may normalize the uniformizing parameter at the origin $\mathbf{0}$ in terms of a holomorphic differential ω . Choose a parameter t at the origin. Since ω does not vanish at $\mathbf{0}$, we have $\omega = (c_0 + c_1t + c_2t^2 + \cdots)dt$ with $c_0 \neq 0$. Making a variable change $t = c_0^{-1}T$, we get $\omega = (1 + a_1T + a_2T^2 + \cdots)dT$. The parameter T with the above property is unique modulo T^2 in $K[[T]]$. Conversely, once we have chosen a formal parameter T modulo T^2 , there is a unique nowhere-vanishing differential ω of the above form because of $\dim_K \Omega_{E/K} = 1$ (Exercise 2). Such a T is called “ T adapted to ω .”

Exercises

1. Show that $\dim_K L(-D) = 0$ for an elliptic curve E if $D > 0$.
2. Show that for a given parameter t at $\mathbf{0}$, there exists a unique nowhere-vanishing differential ω so that its expansion in t has constant term 1.

2.5.2 Weierstrass Equations of Elliptic Curves

We now embed E/K into the two-dimensional projective space $\mathbf{P}_{/K}^2$ using a base of $L(3[\mathbf{0}])$ and determine the equation of the image in $\mathbf{P}_{/K}^2$. 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 2.33 *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 $\mathbf{P}_{/K}^2$ by $(1, x, y)$ whose image is defined by the affine equation*

$$y^2 = 4x^3 - g_2x - g_3 \quad \text{with} \quad g_2, g_3 \in K, \quad (2.14)$$

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

An equation of an elliptic curve E as in (2.14) is called a *Weierstrass equation* of E , which is determined by the pair (E, ω) .

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

$$\begin{aligned} L(4[\mathbf{0}]) &= K + Kx + Ky + Kx^2, \\ L(5[\mathbf{0}]) &= K + Kx + Ky + Kx^2 + Kxy \quad \text{and} \\ L(6[\mathbf{0}]) &= K + Kx + Ky + Kx^2 + Kxy + Kx^3 \\ &= K + Kx + Ky + Kx^2 + Kxy + Ky^2, \end{aligned}$$

from which the following relation results,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{with} \quad a_j \in K, \quad (2.15)$$

because the poles of order 6 of y^2 and x^3 have to be canceled. Therefore E/K can be embedded into $\mathbf{P}_{/K}^2$ via $P \mapsto (x(P), y(P))$. The image is defined by the equation (2.15).

Now we make a variable change $y \mapsto y + ax + b$ in order to remove the terms of xy and y (i.e., we are going to make $a_1 = a_3 = 0$):

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

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

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

Assuming that 3 is invertible in K , we take $a' = -\frac{b_2}{3}$. We can rewrite the equation as in (2.14) (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 .

Conversely, we have seen that any curve defined by equation (2.14) is smooth in Example 2.23 if the cubic polynomial $F(X) = 4X^3 - g_2X - g_3$ has three distinct roots in K . In other words, if the discriminant $\Delta(E, \omega)$ of $F(X)$ does not vanish, E is smooth.

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

We show that there is a canonical nowhere-vanishing differential $\omega \in \Omega_{E/K}$ if E is defined by (2.14). If such an ω exists, all other holomorphic differentials ω' are of the form $f\omega$ with $\text{div}(f) \geq 0$, 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 (Exercise 2).

We summarize what we have seen. Returning to the starting elliptic curve E/K , for the parameter T at the origin, we see by definition

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

This shows

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

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

Exercises

1. Show that dx/y does not vanish at any point on E .
2. Show that if $\Delta = 0$, the curve defined by $y^2 = 4x^3 - g_2x - g_3$ is not smooth at the multiple root α of $4x^3 - g_2x - g_3 = 0$.

2.5.3 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 $\varphi : E \rightarrow E'$ with $\varphi^*\omega' = \omega$. Here for $\omega' = f dg$, $\varphi^*\omega' = (f \circ \varphi)d(g \circ \varphi)$; in other words, if $\sigma : \mathfrak{K}' \rightarrow \mathfrak{K}$ 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) . Considering a polynomial ring $K[g_2, g_3]$ with variables g_2 and g_3 , if K has a characteristic different from 2 and 3, we have

$$[(E, \omega)_{/K}] \cong \{(g_2, g_3) \in K^2 \mid \Delta(E, \omega) \neq 0\} \cong \text{Spec}(\mathbb{Z}[X, Y, \frac{1}{X^3 - 27Y^2}](K)),$$

where $[\cdot]$ indicates the set of isomorphism classes of the objects inside the bracket and $\text{Spec}(R)(K)$ for a ring R is the set of all algebra homomorphisms: $R \rightarrow K$. The last isomorphism sends (g_2, g_3) to the algebra homomorphism ϕ with $\phi(X) = g_2$ and $\phi(Y) = g_3$.

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

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

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

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

This shows

$$g_2(E, \lambda\omega) = \lambda^{-4}g_2(E, \omega) \quad \text{and} \quad g_3(E, \lambda\omega) = \lambda^{-6}g_3(E, \omega). \quad (2.16)$$

Thus we have

Theorem 2.34 *If two elliptic curves E/K and E'/K are isomorphic, then choosing nowhere-vanishing differentials ω_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 $y^2 = 4x^3 - x$. Thus we have

Corollary 2.35 *If K is algebraically closed, then $J(E) = J(E') \iff E \cong E'$ for two elliptic curves over K . Moreover, for any field K , there exists an elliptic curve E with a given $J(E) \in K$.*

Exercises

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.

2.5.4 Group Structure on Elliptic Curves

We now introduce algebrogeometric group structure on elliptic curves. First assume that K is algebraically closed. We know that $L(2[0]) = K + Kx$. For a given point $P \in E - \{0\}$, x is finite at P . We put $f = x - x(P)$. The function f has a zero at P . Since $\deg(\operatorname{div}(f)) = 0$ and f has at most an order 2 pole at 0 , we have two possibilities: $\operatorname{div}(f) = P + P' - 2[0]$ or $\operatorname{div}(f) = P - [0]$. If the latter case happens, $[\mathfrak{K} : K(f)] = 1$ and hence $E \cong \mathbf{P}^1$, which is impossible since the genus of \mathbf{P}^1 is 0 (Exercise 1). Thus we find a unique P' from P , and we define $P' = -P$. When $P = 0$, the above argument just gives $P' = 0$; so, the definition of $P \mapsto -P$ is valid for all P .

Now we define addition of two points $P, Q \in E$. For $P, Q \in E - \{0\}$, we solve a system of simultaneous linear equations:

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

Here $(1, x, y)$ is a base of $L(3[0])$. Then for a nontrivial solution (a, b, c) of the above system, we define $g = ax + by + c$. We assume that $Q \neq -P$. Then $b \neq 0$ (because $b = 0 \Rightarrow Q = -P$ as is clear from the definition of $-P$). Thus g has a pole of order 3 at 0 . Since g is nonconstant with two zeros P, Q , we find a unique point R such that $\text{div}(g) = P + Q + R - 3[0]$. Then we define $P + Q$ to be $-R$. By Abel's theorem we prove in the following subsection, this addition gives rise to an abelian group structure on E . When $Q = -P$, we just define $P + Q = 0$.

Here is a geometric interpretation of the above definition of the addition. Embed E into \mathbf{P}^2 by $1, x, y$. Then we draw a line $aX + bY + cZ = 0$ passing through P, Q in \mathbf{P}^2 , where (X, Y, Z) is the homogeneous coordinate of \mathbf{P}^2 . Then we consider the function $\phi : E \rightarrow \mathbf{P}^1$ given by the equation $\phi(X, Y, Z) = (aX + bY + cZ)/Z$, which is an element in $\mathfrak{K} = K(E)$. We see that ϕ vanishes at two points P, Q , and the line intersects with E at a unique point R again. Then $\text{div}(\phi) = P + Q + R - 3[0]$. In particular, the coordinate of R is a rational function of the coordinates of P and Q ; so, $+: E \times E \rightarrow E$ is a morphism of algebraic geometry (in other words, it is induced from a field embedding $\mathfrak{K} \hookrightarrow \mathfrak{K} \otimes_K \mathfrak{K}$). Similarly, $P \mapsto -P$ is an automorphism of the elliptic curve (therefore of the algebraic function field \mathfrak{K}).

After embedding E into \mathbf{P}^2 , for any field automorphism σ of K , we can apply σ to the coordinate of E . Then we get a new elliptic curve E^σ . If E is defined, for example, by $F(X, Y) = \sum_{i,j} a_{i,j} X^i Y^j = 0$, then E^σ is defined by $F^\sigma(X, Y) = \sum_{i,j} \sigma(a_{i,j}) X^i Y^j = 0$. Since everything we have proved for E shifts to E^σ , the morphism $+: E \times E \rightarrow E$ will be sent to $+: E^\sigma \times E^\sigma \rightarrow E^\sigma$. If E is defined over a smaller field $k \subset \bar{k} = K$, the rational functions of the coordinates of E giving rise to $+: E \times E \rightarrow E$ are therefore invariant under σ ; so, it is a rational function with coefficients in k . Thus what we have said so far is valid for any elliptic curve defined over any perfect field (not necessarily over an algebraically closed field).

Exercises

1. Prove that \mathbf{P}^1 has genus 0.
2. Give a detailed argument why the morphism giving addition on E is well-defined over its field of definition.

2.5.5 Abel's Theorem

We now prove the following Abel's theorem for elliptic curves.

Theorem 2.36 *Let E be an elliptic curve with origin 0 defined over a perfect field K . Then $i : E(K) \rightarrow \text{Jac}(E)(K)$ given by $i(P) = P - [0]$ is an isomorphism of groups.*

By this theorem, we find that $P + Q + R \sim 3[0]$ (here \sim is the linear equivalence) if and only if $i(P) + i(Q) + i(R) = 0$ in $\text{Jac}(E)$; so, the group structure

we have defined in the previous subsection is induced from the group structure of the Jacobian $\text{Jac}(E)$.

Proof. By the same argument (as in the last part of the previous subsection) conjugating by automorphisms of K , everything we prove over an algebraically closed field K will be valid over any subfield k such that K/k is algebraic. Thus we may assume that K is algebraically closed. We first remark that

$$L(D) \neq \{0\} \Rightarrow \deg(D) \geq 0. \quad (2.17)$$

Indeed, if $0 \neq f \in L(D)$ implies that $\text{div}(f) + D \geq 0$; so, taking the degree, we have $\deg(D) \geq -\deg(\text{div}(f)) = 0$. This shows

$$\deg(D) < 0 \Rightarrow \dim_K L(D) = 0. \quad (2.18)$$

Take a degree 1 divisor $D = \sum_{i=1}^d P_i - \sum_{j=1}^{d-1} Q_j$. By the Riemann–Roch theorem, we have $\dim L(D) = \deg(D) + \dim L(-D) = \deg(D) = 1$ by (2.18). We find a nonconstant $f \in L(D)$. This f has to vanish at all Q_j . We have two possibilities:

- $\text{div}(f) = \sum_{j=1}^{d-1} Q_j - \sum_{i=1}^{d-1} P_i$ after renumbering P_i ; so, $D \sim P_d$;
- f has an extra zero R . Then $\text{div}(f) = \sum_{j=1}^{d-1} Q_j + R - \sum_{i=1}^d P_i$; so, $D \sim R$.

Thus D is linearly equivalent to one point. In other words, for any divisor D_0 of degree 0, $D_0 + [\mathbf{0}] \sim P$ for a point P , and hence, the class of D_0 is in the image of i ; so, i is surjective. If $i(P) = i(Q)$ for $P \neq Q$, then we have $P - Q \sim 0$, and hence $\dim L(P - Q) = \dim L(0) = 1$. Therefore we have a function f with a simple pole at P and a simple zero at Q . Thus $[\mathfrak{K} : K(f)] = 1$ and $E \cong \mathbf{P}^1$, a contradiction; so, i is injective. \square

2.5.6 Torsion Points on Elliptic Curves

Let T be a parameter of E over K at the origin $\mathbf{0}$. Then taking a copy S of T , we may think that S, T is a set of parameters of $E \times E$ at $(\mathbf{0}, \mathbf{0})$. Then $(P, Q) \mapsto f(P + Q)$ gives rise to a meromorphic function on $E \times E$. In other words, the function is a pullback of f by $+$. In particular, we have $T \circ + = \Phi \in K[[T, S]]$. For $f(T)$, we find $f \circ + (T, S) = f(\Phi(T, S))$, and by associativity, we get $\Phi(T, \Phi(S, U)) = \Phi(\Phi(T, S), U)$ (Exercise 1). In particular, sending $(T, S) \mapsto \Phi(T, S) = aT + bS \in (T, S)/(T, S)^2$, we get a new associative and commutative group law on K , which is linear with respect to K . Since such a group law is unique on the field K , we find that $\Phi(T, S) \equiv T + S \pmod{(T, S)^2}$ and, hence, the addition of the elliptic curve coincides with the usual addition on K in this sense.

Let N be a positive integer. Then $x \mapsto N \cdot x = \overbrace{x + x + \cdots + x}^N$ is a morphism of E into itself, and N induces on the vector space $(T)/(T^2)$ the multiplication by N . The morphism $x \mapsto N \cdot x$ induces an embedding N^* of the

function field $\mathfrak{K} = K(E)$ into itself. The degree $[\mathfrak{K} : N^*\mathfrak{K}] = \deg(N)$ is finite, because \mathfrak{K} is finitely generated over K and of transcendental degree 1. Thus we find that $N : E \rightarrow E$ is surjective for all positive integer N . In particular, $E(K)$ is an N -divisible group if K is algebraically closed, and we have proven this fact as long as N is prime to the characteristic of K .

A naive question is: What is $\deg(N) = [\mathfrak{K} : N^*(\mathfrak{K})]$? The following theorem gives us that information and slightly more.

Theorem 2.37 *Suppose that K is algebraically closed. Then $\deg(N) = N^2$. Moreover, if N is outside the characteristic of K , we have $E[N](K) \cong (\mathbb{Z}/N\mathbb{Z})^2$ as abelian groups, and if $p > 0$ is the characteristic of the field K , then $E[p]$ is either trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

We prove this theorem in the following subsection when K is a subfield of \mathbb{C} . See [GME] 2.6 for more general cases.

In the rest of this subsection, we explore consequences of the theorem. Start with an arbitrary field K and write \bar{K} for its algebraic closure. Take an elliptic curve E defined over K with function field \mathfrak{K} . We write the composite $\mathfrak{K}\bar{K}$ as $\bar{\mathfrak{K}}$, which gives rise to an elliptic curve \bar{E} over \bar{K} . As the algebraic curve inside \mathbf{P}^m (the integer m can be taken to be 2 as we have seen), E is just defined by equations giving relations among generators of \mathfrak{K} over K . Since $\bar{\mathfrak{K}}$ has the same generators (as \mathfrak{K}) over \bar{K} , they give rise to the same algebraic curve inside \mathbf{P}^m . For any extension F/K inside \bar{K} , we define $E(F)$ to be the set of points of \bar{E} with coordinates in F . Thus $E(F)$ is the subset of $\bar{E}(\bar{K})$ fixed by $\text{Gal}(\bar{K}/F)$.

Take two points P, Q in $E(\bar{K})$. Since $P + Q$ is determined by the third intersection with E of the line passing through P and Q , if we conjugate the coordinate by $\sigma \in \text{Gal}(\bar{K}/K)$, the resulting image goes to the third intersection with E of the line passing through $\sigma(P)$ and $\sigma(Q)$ (when $P = Q$, the line is the line tangent to $P \in E(\bar{K})$). This shows that $\sigma(P) + \sigma(Q) = \sigma(P + Q)$, and conjugation by Galois automorphism is compatible with the addition of E . In particular, $\sigma(N \cdot P) = N \cdot \sigma(P)$, so the Galois action preserves $E[N]$ (since $\sigma(\mathbf{0}) = \mathbf{0}$ because $\mathbf{0} \in E(K)$). In other words, $\sigma : E[N] \rightarrow E[N]$ is an injective group homomorphism. Since $E[N]$ is a finite group, σ induces an automorphism of the group $E[N]$.

Let P, Q be a base of $E[N]$ over $\mathbb{Z}/N\mathbb{Z}$. Then $\sigma(P), \sigma(Q)$ is another base. Write $\rho(\sigma)$ the base-change matrix:

$$\begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \begin{pmatrix} aP+bQ \\ cP+dQ \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

with $\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. By definition, we find $\rho(\sigma)\rho(\tau) = \rho(\sigma\tau)$ and $\rho(1) = 1_2$, where $1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Theorem 2.38 *Let E be an elliptic curve defined over K . Suppose that the integer N is outside the characteristic of K . Then $\sigma \mapsto \rho(\sigma)$ is a homomorphism $\rho : \text{Gal}(\bar{K}/K) \rightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$, where $GL_2(\mathbb{Z}/N\mathbb{Z})$ is the group*

of invertible two-by-two matrices with coefficients in the ring $\mathbb{Z}/N\mathbb{Z}$. Moreover, $\det \rho(\sigma) = \chi_N(\sigma)$, where $\chi_N(\sigma)$ is determined by $\sigma(\zeta_N) = \zeta_N^{\chi_N(\sigma)}$ for a primitive root of unity ζ_N .

By the above theorem, the field $F = K(E[N])$ generated by coordinates of all points of $E[N]$ is a Galois extension of K with $\text{Gal}(F/K) \cong \text{Im}(\rho) \subset GL_2(\mathbb{Z}/N\mathbb{Z})$, and F contains all N th roots of unity. We later explore some cases where ρ is surjective.

Proof. We only need to prove the last assertion about $\det \rho = \chi_N$ for the cyclotomic character χ_N . We construct a bilinear form $e = e_N : E[N] \times E[N] \rightarrow \mu_N$ for the group of N th roots of unity μ_N such that

- (P1) $e(x, x) = 1$ for all $x \in E[N]$ (alternating);
- (P2) $e(x, E[N]) = 1 \Rightarrow x = \mathbf{0}$ (nondegeneracy);
- (P3) $\sigma(e(x, y)) = e(\sigma(x), \sigma(y))$ (Galois equivariance).

If this is worked out, we find $e(P, Q) = \zeta_N$ is a primitive N th root (P2) and

$$\begin{aligned} \sigma(\zeta_N) &= \sigma(e(P, Q)) = e(\sigma(P), \sigma(Q)) \\ &= e(aP + bQ, cP + dQ) = e(P, Q)^{ad} e(Q, P)^{bc} = \zeta_N^{ad-bc} \end{aligned}$$

as desired (because $1 = e(P + Q, P + Q) = e(P, Q)e(Q, P)$). We need to construct e and to prove (P1–3) above. Here is a construction given by A. Weil: we need to consider a point $P \in E$ both as a geometric point and also a divisor; so, we write $[P]$ when we consider P as a divisor. By Abel's theorem,

- (div) if $\sum_i c_i x_i = \mathbf{0}$ for $x_i \in E(\bar{K})$ and $\sum_i c_i = 0$ for integers c_i , then $0 = \sum_i c_i ([x_i] - [\mathbf{0}]) = \sum_i c_i [x_i]$.

Pick $x \in E[N]$; so, $N[x] - N[\mathbf{0}] = \text{div}(f_x)$ for a function $f_x \in \bar{\mathcal{K}}$. Since $E(\bar{K})$ is divisible, we can pick $t \in E(\bar{K})$ such that $x = Nt$. We consider the divisor $D = \sum_{u \in E[N]} [t + u] - \sum_{u \in E[N]} [u]$. Then by (div), we find a function $g_x \in \bar{\mathcal{K}}$ such that $\text{div}(g_x) = D$. We see that $\text{div}(f_x \circ N)$ is made up of points that go to $\mathbf{0}$ and t with multiplicity N ; so, $\text{div}(f_x \circ N) = N \cdot \text{div}(g_x)$. Thus $g_x^N / f_x \circ N$ is a nonzero constant c , and $g_x(P + y)^N = c f_x(N(P + y)) = c f_x(NP) = g_x(P)^N$ for $y \in E[N]$. We then define $e(x, y) = g_x(P + y) / g_x(P)$ which is an N th roots of unity. By this construction, $g_{\sigma(x)} = c_1 \sigma(g_x)$ for a nonzero constant $c_1 \in \bar{K}$; so, we may choose $g_{\sigma(x)}$ to be $\sigma(g_x)$. Then Galois equivariance follows from

$$\begin{aligned} \sigma(e(x, y)) \sigma(g_x(P)) &= \sigma(g_x(P + y)) \\ &= \sigma(g_x)(\sigma(P) + \sigma(y)) = e(\sigma(x), \sigma(y)) \sigma(g_x(P)). \end{aligned}$$

For $y, y' \in E[N]$, $g_x(P + y + y') = e(x, y') g_x(P + y) = e(x, y) e(x, y') g_x(P)$; so, the pairing is linear with respect to the right variable. We now take care of the linearity for the left variable. Let $z = x + w$ for $x, w \in E[N]$. Since $x + w - z - \mathbf{0} = \mathbf{0}$, applying (div), we find $h \in \bar{\mathcal{K}}$ such that $\text{div}(h) = [x] + [w] - [z] - [\mathbf{0}]$. Then

$$\operatorname{div}(f_x f_w f_z^{-1}) = N([x] - [\mathbf{0}] + [w] - [\mathbf{0}] + [\mathbf{0}] - [z]) = N \cdot \operatorname{div}(h)$$

and $N \cdot \operatorname{div}(g_x g_w g_z^{-1}) = N \cdot \operatorname{div}(h \circ N)$. Thus $g_x g_w g_z^{-1} = c(h \circ N)$ for a nonzero constant $c \in K$. In other words,

$$\begin{aligned} e(x, y)^{-1} e(w, y)^{-1} e(z, y) g_x(P) g_w(P) g_z^{-1}(P) \\ = g_x(P + y) g_w(P + y) g_z^{-1}(P + y) = c \cdot h(P) = g_x(P) g_w(P) g_z^{-1}(P), \end{aligned}$$

which shows the desired left linearity.

If $e(x, y) = 1$ for all $y \in E[N]$, g_x factors through the image of N ; that is, $g_x = g' \circ N$, and hence $f_x = g'^N$ (so, $N \cdot \operatorname{div}(g') = \operatorname{div}(f_x)$) because $N : E \rightarrow E$ is surjective. We have $\operatorname{div}(g') = [x] - [\mathbf{0}]$, and by Abel's theorem $x = \mathbf{0}$. This proves the nondegeneracy.

We now prove (P1). Observe

$$\operatorname{div}\left(\prod_{n=0}^{N-1} f_x(P - nx)\right) = N \sum_{n=0}^{N-1} ([nx + x] - [nx]) = 0.$$

Then $\prod_{n=0}^{N-1} f_x(P - nx)$ is a constant. Since we have chosen t so that $Nt = x$, we have $g_x(P - nt) = f_x(N(P - nt))^N = f_x(NP - nx)^N$, and $\prod_{n=0}^{N-1} g_x(P - nt)$ has to be a constant. Now we plug $P - x$ in P , and we get

$$\begin{aligned} g_x(P) g_x(P - t) \cdots g_x(P - (N - 1)t) \\ = g_x(P - t) g_x(P - 2t) \cdots g_x(P - (N - 1)t) g_x(P - x). \end{aligned}$$

This shows that $g_x(P) = g_x(P - x)$ and hence $e(x, x) = 1$. \square

Exercises

1. Prove that $\Phi(T, \Phi(S, R)) = \Phi(\Phi(T, S), R)$ in the power series ring of three variables T, S, R over K .
2. Prove $\rho(\sigma)\rho(\tau) = \rho(\sigma\tau)$.

2.5.7 Classical Weierstrass Theory

Let $E_{/\mathbb{C}}$ be an elliptic curve over \mathbb{C} . Since E is of genus 1, it is a quotient of \mathbb{C} by a lattice $L \subset \mathbb{C}$. Here a lattice $L \subset \mathbb{C}$ is a \mathbb{Z} -submodule of \mathbb{C} generated by a base (w_1, w_2) of \mathbb{C} over \mathbb{R} . We write Lat for the set of all lattices in \mathbb{C} .

Taking a nowhere-vanishing differential ω on $E(\mathbb{C})$, we rediscover the lattice L of \mathbb{C} (associated with (E, ω)) by

$$L = \left\{ \int_{\gamma} \omega \mid \gamma \in H_1(E(\mathbb{C}), \mathbb{Z}) \right\}.$$

Abel's isomorphism is then given by $P \mapsto \int_0^P \omega \in \mathbb{C}/L = \text{Jac}(E)$. By Abel's theorem, we find that $E[N] = \frac{1}{N}L/L \cong (\mathbb{Z}/N\mathbb{Z})^2$, which gives a proof of Theorem 2.37 if $K = \mathbb{C}$. For a general field K of characteristic 0 inside \mathbb{C} and an elliptic curve E/K , the composite $\mathbb{C}\mathfrak{K}$ gives rise to the elliptic curve $E_{\mathbb{C}}$ over \mathbb{C} defined by the same equation; so, $E[N](\overline{K}) \cong E_{\mathbb{C}}[N]$, which proves the theorem basically for all fields of characteristic 0.

Conversely, for a given $L \in \text{Lat}$, 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 $\varphi = y_L^2 - 4x_L^3 + g_2x_L + g_3$ is holomorphic everywhere. Since these functions factor through the compact space \mathbb{C}/L , φ has to be constant, because any nonconstant 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 $(x_L, y_L) : \mathbb{C}/L - \{0\} \rightarrow \mathbb{C}_{\mathbb{C}}^2$. Looking at the order of poles at 0 , we know the above map is of degree 1, that is, an isomorphism onto its image. It also extends to the embedding $\Phi = (x_L, y_L, 1) = (u^3x_L, u^3y_L, u^3) : \mathbb{C}/L \rightarrow \mathbf{P}_{\mathbb{C}}^2$. Thus we get an elliptic curve $E_L = \Phi(\mathbb{C}/L) = E(g_2(L), g_3(L))$. We then have

$$\omega_L = \frac{dx_L}{y_L} = dx_L \left(\frac{dx_L}{du} \right)^{-1} = du.$$

This shows

Theorem 2.39 (Weierstrass) *We have*

$$\text{Lat} \cong \left[(E, \omega)_{/\mathbb{C}} \left| \begin{array}{l} E: \text{an elliptic curve over } \mathbb{C}, \\ \omega: \text{a nowhere-vanishing differential} \end{array} \right. \right],$$

where the straight brackets $[]$ indicate the set of all isomorphism classes of the objects inside.

We now make the space Lat more explicit. Two complex numbers w_1, w_2 span a lattice if and only if $\text{Im}(w_1/w_2) \neq 0$. Let $\mathfrak{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$. Interchanging w_1 and w_2 if necessary, we may assume that $\text{Im}(w_1/w_2) > 0$. So we get a natural isomorphism of complex manifolds via $\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \mapsto (w_2, w_1/w_2)$:

$$\mathcal{B} = \left\{ v = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \in (\mathbb{C}^\times)^2 \mid \operatorname{Im}(w_1/w_2) > 0 \right\} \cong \mathbb{C}^\times \times \mathfrak{H}.$$

Since v and v' span the same lattice L if and only if $v' = \alpha v$ for $\alpha \in SL_2(\mathbb{Z})$, we see that $Lat \cong SL_2(\mathbb{Z}) \backslash \mathcal{B}$. The action of $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ on \mathcal{B} is given on $\mathbb{C}^\times \times \mathfrak{H}$ by $\alpha(u, z) = (cu + d, \alpha(z))$ for $\alpha(z) = \frac{az+b}{cz+d}$.

We now consider the variables g_2 and g_3 and the J -invariant J defined below Theorem 2.34 as a function on the upper half complex plane \mathfrak{H} . In particular, by Corollary 2.35, J satisfies $J(\gamma(z)) = J(z)$ for $\gamma \in SL_2(\mathbb{Z})$.

2.6 Elliptic Modular Function Field

Combining the analytic consideration in the previous subsection with the algebraic study in the earlier ones, we now state and partially prove the first non-abelian global reciprocity law due to Shimura.

For a lattice L spanned by (w_1, w_2) with $\operatorname{Im}(w_1/w_2) > 0$, let $E(L)$ be the elliptic curve given by $E(\mathbb{C}) = \mathbb{C}/L$. Picking a point $u(a, b) = \frac{aw_1+bw_2}{N} \in E(L)[N]$ (for $0 \neq u = (a, b) \in (\mathbb{Z}/N\mathbb{Z})^2$), we define a function $f_u : Lat \rightarrow \mathbb{C}$ by

$$f_u(w) = \frac{g_2(w)g_3(w)}{\Delta(w)} x_L(u(a, b)) \text{ and } x_u(w) = x_L(u(a, b))$$

for $w = {}^t(w_1, w_2)$ and $\Delta = g_2^3 - 27g_3^2$. Then for $\alpha \in SL_2(\mathbb{Z})$,

$$f_u(\alpha w) = f_u(w) \text{ for } 0 \neq \forall u = (a, b) \in (\mathbb{Z}/N\mathbb{Z})^2 \Leftrightarrow \alpha \equiv \pm 1_2 \pmod{N}. \quad (2.19)$$

Also we see easily that $x_u(\lambda w) = \lambda^{-2} x_u(w)$ for nonzero scalar $\lambda \in \mathbb{C}^\times$. We call a meromorphic function f on \mathcal{B} a modular form of weight k on $\Gamma(N)$ if f satisfies $f(\gamma w) = f(w)$ for all $\gamma \in SL_2(\mathbb{Z})$ with $\gamma - 1_2 \in NM_2(\mathbb{Z})$ and $f(\lambda w) = \lambda^{-k} f(w)$ for $\lambda \in \mathbb{C}^\times$. In particular, if $k = 0$, they are called modular functions on $\Gamma(N)$. Thus f_u is a modular function on $\Gamma(N)$, and x_u is a modular form of weight 2 on $\Gamma(N)$. We often let $\Gamma(N)$ denote the subgroup of $SL_2(\mathbb{Z})$ made of matrices congruent to 1_2 modulo N . We have the following exact sequence,

$$1 \rightarrow \Gamma(N) \rightarrow SL_2(\mathbb{Z}) \xrightarrow{\text{mod } N} SL_2(\mathbb{Z}/N\mathbb{Z}) \rightarrow 1.$$

The surjectivity of the last “mod N ” map is nontrivial (Exercise 1).

Since $\mathcal{B} = \mathfrak{H} \times \mathbb{C}^\times$, one may regard a modular form as a meromorphic function on the upper half complex plane \mathfrak{H} by putting $f(z) = f(2\pi i(\frac{z}{i}))$. Since $\alpha(\frac{z}{i}) = (cz + d)(\frac{\alpha(z)}{i})$ for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we find that $f : \mathfrak{H} \rightarrow \mathbb{C}$ is a modular form of weight k on $\Gamma(N)$ if the following conditions are satisfied,

$$(G1) \quad f(\alpha(z)) = f(z)(cz + d)^k \text{ for all } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N).$$

If f is a modular form on $\Gamma(N)$, $f(z + N) = f(z)$; so, f is a function on $\mathfrak{H}/N\mathbb{Z}$, where $N\mathbb{Z}$ acts by translation. By the variable change, $q = q_N = \exp(\frac{2\pi iz}{N})$,

we may identify $\mathfrak{H}/N\mathbb{Z}$ with the open unit disk $\{q \in \mathbb{C} \mid |q| < 1\}$ punctured at 0 (0 corresponds to ∞), and we may regard f as a function of q defined over the punctured disk. It has a Laurent expansion around 0: $f(q) = \sum_n a_n q^n$, which is called the q -expansion of f . We assume that $f(q)$ is finite tailed; that is, there exists $N > 0$ such that $a_n = 0$ as long as $n < -N$.

We can compute explicitly the q -expansion of g_2 , g_3 and Δ for $q = q_1$:

$$\begin{aligned} 12g_2 &= 1 + 240 \sum_{n=1}^{\infty} \left\{ \sum_{0 < d|n} d^3 \right\} q^n \\ -6^3 g_3 &= 1 - 504 \sum_{n=1}^{\infty} \left\{ \sum_{0 < d|n} d^5 \right\} q^n \\ \Delta &= q \prod_{n=1}^{\infty} (1 - q^n)^{24}. \end{aligned} \tag{2.20}$$

From this we can conclude $J \in q^{-1}\mathbb{Z}[[q]]$ (cf. [IAT] Section 4.6).

We consider the Riemann surface $Y(N) = \Gamma(N) \backslash \mathfrak{H}$. Regarding $J = 12^3 j$ as a variable, and considering the elliptic curve $E : y^2 = 4x^3 - gx - g$ for $g = \frac{27j}{j-1}$ defined over $\mathbb{Q}(J)$, we can think of $\mathbb{Q}(J)(E[N])$. This is a Galois extension of $\mathbb{Q}(J)$ with

$$\text{Gal}(\mathbb{Q}(J)(E[N])/\mathbb{Q}(J)) \subset GL_2(\mathbb{Z}/N\mathbb{Z}).$$

We also consider the field \mathfrak{K}_N generated over $\mathbb{Q}(J)$ (now J is a function on \mathfrak{H}) by f_u for all $u \in (\mathbb{Z}/N\mathbb{Z})^2$. Since f_u is the x -coordinate of the point corresponding to $u = u(a, b) \in E[N]$ (up to the factor $g^2/g^3 - 27g^2$ in $\mathbb{Q}(J)$), we may regard $\mathfrak{K}_N \subset \mathbb{Q}(J)(E[N])$ and $\mathfrak{K}_N \subset \mathbb{C}(Y(N))$. It is easy to see that $\alpha \in SL_2(\mathbb{Z})$ acts on $Y(N)$ by $z \mapsto \alpha(z)$; so, it induces an automorphism of $\mathbb{C}(Y(N))/\mathbb{C}(J)$.

Theorem 2.40 *We have $\text{Gal}(\mathfrak{K}_N/\mathbb{Q}(J)) \cong GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, and $\alpha \in SL_2(\mathbb{Z})$ acts on $f \in \mathfrak{K}_N$ by $f \mapsto f \circ \alpha$. This action of $SL_2(\mathbb{Z})$ factors through $PSL_2(\mathbb{Z}/N\mathbb{Z})$, which is the subgroup of $\text{Gal}(\mathfrak{K}_N/\mathbb{Q}(J))$.*

Proof. We check $f_u \circ \alpha = f_{u\alpha}$. Since $f_{u\alpha} = f_u$ for all u implies that $u\alpha = \pm u$ by definition, we find that $\text{Gal}(\mathbb{C}(Y(N))/\mathbb{C}(J))$ contains $PSL_2(\mathbb{Z}/N\mathbb{Z})$. Since $Y(N)$ is the covering of degree $|PSL_2(\mathbb{Z}/N\mathbb{Z})|$ of $\mathbf{P}^1(J)$, we find that

$$\mathbb{C}(Y(N)) = \mathbb{C}(J)(f_u \mid 0 \neq u \in (\mathbb{Z}/N\mathbb{Z})^2).$$

By computing the q -expansion of f_u , we find that $f_u \in \mathbb{Q}[\zeta_N]((q))$:

$$x_u = \frac{1}{12} - 2 \sum_{n=1}^{\infty} \frac{nq^{Nn}}{1 - q^{Nn}} + \frac{\zeta_N^b q^a}{(1 - \zeta_N^b q_N^a)^2} + \sum_{n=1}^{\infty} \frac{(\zeta_N^{bn} q^{an} + \zeta_N^{-bn} q^{-an}) n q^n}{1 - q^n}$$

for $u = (a, b)$ and $q = \exp(2\pi iz/N)$. By Theorem 2.38, we know that $\mathfrak{K}_N \supset \mathbb{Q}[\zeta_N]$; so, $\mathbb{C} \cap \mathfrak{K}_N = \mathbb{C} \cap \mathbb{Q}[\zeta_N](q) = \mathbb{Q}[\zeta_N]$. Since $\text{Gal}(\mathfrak{K}_N/\mathbb{Q}(J))$ contains all $PSL_2(\mathbb{Z}/N\mathbb{Z})$ and also matrices with any given determinant modulo N , we find

$$\text{Gal}(\mathfrak{K}_N/\mathbb{Q}(J)) = GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

This finishes the proof.

By the above proof, q gives a parameter at ∞ of $Y(N)$ defined over $\mathbb{Q}(\zeta_N)$; so, we have

$$\mathfrak{K}_N = \mathbb{C}(Y(N)) \cap \mathbb{Q}[\zeta_N](q) \quad (q = \exp\left(\frac{2\pi iz}{N}\right)). \quad (2.21)$$

This shows

Corollary 2.41 *The curve $Y(N)_{/\mathbb{C}}$ is actually defined over $\mathbb{Q}[\zeta_N]$, and*

$$\mathbb{Q}[\zeta_N](Y(N)_{/\mathbb{Q}[\zeta_N]}) = \mathfrak{K}_N.$$

We consider the union $\mathfrak{K} = \bigcup_N \mathfrak{K}_N$ (note here that $\mathfrak{K}_N \subset \mathfrak{K}_M$ if $N|M$); so, \mathfrak{K} is a field.

Corollary 2.42 *We have $\text{Gal}(\mathfrak{K}/\mathbb{Q}(J)) \cong GL_2(\widehat{\mathbb{Z}})/\{\pm 1\}$ and $\mathfrak{K} \cap \mathbb{C} = \mathbb{Q}^{cyc}$. Moreover, each matrix $g \in GL_2(\widehat{\mathbb{Z}})$ acts on \mathbb{Q}^{cyc} by the action of $\det(g)$ under the identification $\text{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) = \widehat{\mathbb{Z}}^\times$.*

For $\alpha \in M_2(\mathbb{Z})$ with $\det(\alpha) > 0$, we can always write by elementary divisor theory, $\alpha = \gamma \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix} \gamma'$ with $\gamma, \gamma' \in SL_2(\mathbb{Z})$. We write $\delta = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}$. Since the effect of $f \mapsto f \circ \delta$ on q -expansion is $q \mapsto q^{m/n}$, the action $f \mapsto f \circ \alpha$ preserves the coefficient field $\mathbb{Q}[\zeta_N]$. Since $\delta^{-1}\Gamma(N)\delta \supset \Gamma(mnN)$ (Exercise 2), $\mathfrak{K}_N \circ \delta \subset \mathfrak{K}_{mnN}$. Since $\gamma, \gamma' \in SL_2(\mathbb{Z})$ preserve \mathfrak{K}_N , we see that $\mathfrak{K}_N \circ \alpha \subset \mathfrak{K}_{mnN}$ and hence $f \mapsto f \circ \alpha$ is an automorphism $\tau(\alpha)$ of \mathfrak{K} . For any $\alpha \in GL_2(\mathbb{Q})_+$, its integer multiple is in $M_2(\mathbb{Z})$. Thus the linear transformation $z \mapsto \alpha(z)$ is induced by an integer matrix; so, $\tau(\alpha) \in \text{Aut}(\mathfrak{K})$ is well defined on \mathfrak{K} ; that is, $GL_2(\mathbb{Q})_+$ acts on \mathfrak{K} by $f \mapsto f \circ \alpha$. We can check (e.g., [IAT] 6.4 or [MFG] Corollary 3.3):

- (A1) $GL_2(\mathbb{Q})_+ GL_2(\widehat{\mathbb{Z}}) GL_2(\mathbb{R})_+ = GL_2(\mathbb{A})_+$, where $+$ indicates the positivity of the determinant (at ∞);
- (A2) $GL_2(\widehat{\mathbb{Z}} \times \mathbb{R})_+ \cap \mathbb{Q}^\times = \{\pm 1\}$.

Thus we can let $GL_2(\mathbb{A})_+$ act on \mathfrak{K} . Here is a theorem of Shimura.

Theorem 2.43 (Elliptic Reciprocity Law) *We have an exact sequence*

$$1 \rightarrow \mathbb{Q}^\times GL_2(\mathbb{R})_+ \rightarrow GL_2(\mathbb{A})_+ \xrightarrow{\tau} \text{Aut}(\mathfrak{K}) \rightarrow 1.$$

The action of $GL_2(\mathbb{A})_+$ on \mathfrak{K} is as given above. The difficult part of the proof is the surjectivity of τ for which we refer the reader to [IAT] Theorem 6.23. We later give a sketch of a proof in a more general setting, Theorem 4.14.

For each open compact subgroup S of $GL_2(\mathbb{A})_+/\mathbb{Q}^\times GL_2(\mathbb{R})_+$, we have an algebraic function field \mathfrak{K}^S , which gives rise to a projective curve V_S defined over the fixed subfield k_S of \mathbb{Q}^{cyc} by $\det(S) \subset \mathbb{A}^\times/\mathbb{Q}^\times \mathbb{R}_+^\times = \text{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q})$. This curve is the modular curve of level S , and $V_S(\mathbb{C}) = \Gamma_S \backslash \mathfrak{H}$ (forgetting the points above $\infty \in \mathbf{P}^1(J)$). Here $\Gamma_S = S \cap SL_2(\mathbb{Q})$. In particular, $Y(N)$ corresponds to $\{u \in GL_2(\widehat{\mathbb{Z}}) | u \equiv 1_2 \pmod{N}\}$, and we have the following identity,

$$[(E, \phi : (\mathbb{Z}/N\mathbb{Z})^2 \cong E[N])_{/K} | e_N(\phi(1, 0), \phi(0, 1)) = \zeta_N] \cong Y(N)(K),$$

where K is any field extension of $\mathbb{Q}[\zeta_N]$ for a specific primitive N th root of unity ζ_N , and $[\cdot]$ indicates the set of isomorphism classes of the pairs (E, ϕ) . We have $(E, \phi)_{/K} \cong (E', \phi')_{/K}$ if there exists an isomorphism $f : E \rightarrow E'$ defined over K such that $f \circ \phi = \phi'$.

Since $\mathbb{A} = \mathbb{A}^{(\infty)} \times \mathbb{R}$, we have $GL_2(\mathbb{A})_+/\mathbb{Q}^\times GL_2(\mathbb{R})_+ = \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})}$, writing $Z(\mathbb{Q})$ for the center of $GL_2(\mathbb{Q})$ isomorphic to \mathbb{Q}^\times . Consider τ giving the isomorphism

$$\tau : \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} \cong \text{Aut}(\mathfrak{K}).$$

The fixed field \mathfrak{K}^S of $\tau(S)$ is an algebraic function field; so, it is the function field of a unique smooth projective curve V_S defined over $k_S = \mathfrak{K}^S \cap \overline{\mathbb{Q}}$ (which is the fixed field of $\iota(\det(S))$ for ι in Theorem 2.12). Therefore the isomorphism τ in Theorem 2.43 gives rise to a tower of algebraic curves $\{V_S\}_S$ defined over k_S indexed by open compact subgroups $S \subset \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})}$. The tower $\{V_S\}_S$ is called Shimura's canonical model of the tower of modular curves (or simply just the tower of modular curves), which classifies elliptic curves with additional structures and is the simplest example of the Shimura varieties we study in the rest of the book. We write $Y_S(\mathbb{C})$ for the image of $\Gamma_S \backslash \mathfrak{H}$ in $V_S(\mathbb{C})$ for $\Gamma_S = PGL_2(\mathbb{Q}) \cap S$ in $\frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})}$. Then $V_S - Y_S$ is a set of finite points (called cusps of V_S), and Y_S is an open algebraic curve (a quasi-projective curve) defined over k_S . In other words, V_{S/k_S} is the unique smooth compactification of Y_{S/k_S} .

We may regard V_S as defined over \mathbb{Q} forgetting the requirement of the field of definition to be the algebraic closure of \mathbb{Q} in the function field $k_S(V_S)$. By the strong approximation theorem (i.e., the density of $SL_2(\mathbb{Q})$ in $SL_2(\mathbb{A}^{(\infty)})$; e.g., [MFG] 3.1.2), $GL_2(\mathbb{Q}) \backslash GL_2(\mathbb{A}^{(\infty)})/Z(\mathbb{Q})S$ is in bijection with $\text{Gal}(k_S/\mathbb{Q})$ by $g \leftrightarrow \iota(\det(g))$. We write gS for the conjugate $g \cdot S \cdot g^{-1}$. Since $k_S \otimes_{\mathbb{Q}} \mathbb{C} = \prod_{\sigma \in \text{Gal}(k_S/\mathbb{Q})} \mathbb{C}$ by $k \otimes x \mapsto (\sigma(k)x)_\sigma$, we have

$$\mathfrak{K}^S \otimes_{\mathbb{Q}} \mathbb{C} = \prod_{g \in GL_2(\mathbb{Q}) \backslash \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} / S} \mathbb{C} \mathfrak{K}^{gS},$$

which implies

$$\begin{aligned} V_S \times_{\mathbb{Q}} \mathbb{C} &= \bigsqcup_{\sigma \in \text{Gal}(k_S/\mathbb{Q})} V_{S/\mathbb{C}}^{\sigma} = \bigsqcup_{g \in GL_2(\mathbb{Q}) \backslash \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} / S} V_{gS/\mathbb{C}} \\ V_{S/\mathbb{Q}}(\mathbb{C}) &= \bigsqcup_{g \in GL_2(\mathbb{Q}) \backslash \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} / S} V_{gS/\mathbb{C}}(\mathbb{C}), \end{aligned} \quad (2.22)$$

where each $V_{gS/\mathbb{C}}(\mathbb{C}) = V_{gS/k_S}(\mathbb{C})$ gives one connected component of $V_{S/\mathbb{Q}}(\mathbb{C})$. Since $V_S(\mathbb{C})$ with finitely many points above ∞ (called cusps) removed is exactly the quotient $Y_S = \Gamma_S \backslash \mathfrak{H}$, we find

$$GL_2(\mathbb{Q})_+ \backslash \left(\frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} \times \mathfrak{H} \right) / S = \bigsqcup_{g \in GL_2(\mathbb{Q}) \backslash \frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} / S} Y_{gS}(\mathbb{C}) = Y_{S/\mathbb{Q}}(\mathbb{C})$$

by $(g, z) \mapsto (z \bmod \Gamma_{gS})$. Thus we get the following expression:

$$\begin{aligned} &GL_2(\mathbb{Q})_+ \backslash \left(GL_2(\mathbb{A}^{(\infty)}) \times \mathfrak{H} \right) / Z(\mathbb{Q}) \\ &= \varprojlim_S GL_2(\mathbb{Q})_+ \backslash \left(\frac{GL_2(\mathbb{A}^{(\infty)})}{Z(\mathbb{Q})} \times \mathfrak{H} \right) / S = \varprojlim_S Y_{S/\mathbb{Q}}(\mathbb{C}). \end{aligned} \quad (2.23)$$

We may think of the proalgebraic curve $Y = \varprojlim_S Y_{S/\mathbb{Q}}$ as a model of the pro-Riemann surface $GL_2(\mathbb{Q})_+ \backslash (GL_2(\mathbb{A}^{(\infty)}) \times \mathfrak{H}) / Z(\mathbb{Q})$. This is the point of view of Deligne ([D1] and [D2]). Then $\varprojlim_S V_S$ is the smooth compactification of the open proalgebraic curve Y . In the rest of this book, we replace the algebraic group $GL(2)_{/\mathbb{Q}}$ by a more general reductive group $G_{/\mathbb{Q}}$ and study the canonical models of $G(\mathbb{Q}) \backslash (G(\mathbb{A}^{(\infty)}) \times X) / \overline{Z(\mathbb{Q})}$ for the symmetric space X of $G(\mathbb{R})$ and their (smooth and minimal) compactifications. Here $\overline{Z(\mathbb{Q})}$ is the topological closure of the center $Z(\mathbb{Q})$ of $G(\mathbb{Q})$ in $G(\mathbb{A}^{(\infty)})$. In the case of $G = GL(2)_{/\mathbb{Q}}$, we have $\overline{Z(\mathbb{Q})} = Z(\mathbb{Q})$; so, our formulation is consistent. In our study of p -adic automorphic forms on G , the two formulations, one due to Deligne and the other due to Shimura, both play fundamental roles.

Exercises

1. Prove the surjectivity of the mod N map from $SL_2(\mathbb{Z})$ to $SL_2(\mathbb{Z}/N\mathbb{Z})$.
2. Let $\delta = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}$. Prove that $\delta^{-1} \Gamma(N) \delta \supset \Gamma(mnN)$.
3. Prove (A1) and (A2).

<http://www.springer.com/978-0-387-20711-7>

p-Adic Automorphic Forms on Shimura Varieties

Hida, H.

2004, XI, 390 p., Hardcover

ISBN: 978-0-387-20711-7