P-adic Uniformisation of Curves

Chris Williams

Part III Essay

Abstract

In the classical theory of elliptic curves over $\mathbb{C}$, we prove that every complex elliptic curve is the quotient of the plane by a lattice. In this essay, a corresponding theory over p-adic fields - due to Tate - is discussed, using the theory of p-adic analysis to show that every p-adic elliptic curve with non-integral j-invariant can be uniformised as a quotient of K^* by a multiplicative subgroup. We then look at beginning to generalise this result to higher genera using automorphic forms, proving that for a Schottky group Γ, there is a space $\Omega \subset \mathbb{P}^1_{\mathbb{C}_p}$ on which Γ acts discontinuously, giving rise to a smooth, irreducible algebraic curve Ω/Γ.

Contents

Introduction

In the classical theory of elliptic curves over $\mathbb{C}$, it is proved that every complex elliptic curve is the quotient of the plane by a lattice. Such a property is incredibly useful; for example, it allows us to describe the torsion of the curve, and it forms a basis for the study of complex multiplication. In this essay, we give an analogue for p-adic fields due to John Tate, and discuss David Mumford's generalisation to higher genera.

Part I is largely preliminary. In Chapter 1, relevant definitions and results on elliptic curves are stated, before some results about more general curves and their function fields - including a correspondence between points on the curve and places of its function field - are given. The crucial result for the remaining work is Theorem 1.18, which says that for an algebraically closed field K and a function field L of one variable and genus g over K, there is a smooth, irreducible curve V with $L = K(V)$.

Chapter 2 focuses on the complex case, considering an alternative approach using the exponential function. We also obtain formulae that are used in Part II to calculate invariants of a uniformised curve, and thus find necessary and sufficient conditions for uniformisation.

In Part II, we prove Tate's uniformisation theorem for elliptic curves: namely, that for any elliptic curve E over a p-adic field K with split multiplicative reduction and non-integral j-invariant, $\exists q \in K^*$ such that $E \cong K^*/q^{\mathbb{Z}}$. Thus for any elliptic curve E/K there is (at worst) a quadratic extension L/K with $E \cong K^*/q^{\mathbb{Z}}$ over L.

In Chapter 3, the theory of p-adic analysis is developed. We quote Schnirelmann's structure theorem, that says any meromorphic function on K^* can be described (up to a multiplicative constant) entirely in terms of its zeros and poles. We then prove that the field of q-periodic meromorphic functions is a function field of one variable and genus 1, and thus prove that $K^*/q^{\mathbb{Z}}$ is an elliptic curve. In Chapter 4, this curve is shown to satisfy the equation $E_q : Y^2 + XY = X^3 + BX + C$, with non-integral j-invariant and trivial Hasse invariant. We then collate these results in Chapter 5 to prove the uniformisation theorem.

The generalisation of this work to higher genera was described by Tate himself as 'far from obvious', and it indeed it required a very different approach by Mumford to give an answer to the problem. His work used the language of schemes and rigid analysis to prove that for any curve with split degenerate reduction, there is a Schottky group Γ (a finitely generated discontinuous subgroup of $PGL_2(K)$ with no elements of finite order) and a space $\Omega \subset \mathbb{P}^1_{\mathbb{C}_p}$ on which Γ acts discontinuously, with Ω/Γ an algebraic curve. It turns out we can take $\Omega = \mathbb{P}^1_{\mathbb{C}_p} \backslash \mathcal{L}$, where $\mathcal{L}$ is the set of limit points of Γ.

In Part III, a partial account of Mumford's work is given in a more down-to-earth setting - in which we can draw parallels with the work done in Part II. We will show that, for Ω and Γ as above, that Ω/Γ is an algebraic curve of genus g (where g is the number of generators of Γ, which is necessarily free; see Chapter 7). To do so, we consider $\mathbb{C}_p(\Omega/\Gamma)$, the field of Γ-invariant meromorphic functions on Ω, and show that it is a function field of one variable and genus g over $\mathbb{C}_p$, giving the result.

Chapter 6 defines the tree of a compact subset of $\mathbb{P}^1_K$. We associate to such a set a locally finite tree $\mathcal{T}(X)$ and show that there is a bijection between halflines in $\mathcal{T}(X)$ and limit points of X. Chapter 7 then introduces Schottky groups. We prove that, for suitable X, Γ acts on the tree $\mathcal{T}(X)$ and that $\mathcal{T}(X)/\Gamma$ is finite with universal cover $\mathcal{T}(X)$ and group of covering translations Γ. Thus any such group is free on g generators, say. We then construct a good fundamental domain F for Γ by cutting $2g$ disjoint discs out of the projective line, demanding that they satisfy suitable properties in relation to the generators.

Importantly, this gives us a workable notion of Ω as the union

$$\bigcup_{\gamma\in\Gamma} \gamma(F),$$

and shows that Γ acts discontinuously on Ω.

Chapter 8 then focuses on holomorphic/meromorphic functions on Ω, before constructing automorphic forms

$$\theta(a,b;z) = \prod_{\gamma\in\Gamma} \frac{z-\gamma(a)}{z-\gamma(b)}$$

for Γ, where $a, b \in \Omega$. A structure theorem for such automorphic forms is proved, that says any automorphic form for Γ is (up to a multiplicative constant) a finite product of the $\theta(a,b;z)$.

We then conclude in Chapter 9 that the field of Γ-invariant meromorphic functions is a function field of one variable and genus g (the number of generators of Γ). To do so, we construct a *single* non constant Γ-invariant meromorphic function h and show that $\mathbb{C}_p(\Omega/\Gamma)$ is an algebraic extension of $\mathbb{C}_p(h)$. The result on the genus is stated via a version of the Riemann-Roch theorem. Thus Ω/Γ is a smooth irreducible algebraic curve of genus g.

As mentioned before, whilst we are able to give a complete account of the uniformisation theorem in the genus 1 case, we can merely scratch the surface of the generalisation to higher genera. Mumford's results were part of a body of work that were to earn him the Fields Medal in 1974.

Acknowledgments

I would like to thank several people for their help in researching and writing this essay. Professor A.J. Scholl gave me invaluable guidance in first source selection and later on in helping me decide on further topics of study. I also talked informally with Valentijn Karemaker about suitable books for the content, attending her Part III seminar on the same subject. Finally, many thanks to Dominic Yeo, who kindly proofread the final draft before submission.

Part I: Motivation and Prerequisites

1. Preliminaries on Curves

1.1. Elliptic Curves

In this brief introductory section, we discuss the theory of elliptic curves and state some of the fundamental properties that we will later use throughout Part II.

Definition 1.1. An *elliptic curve* E/K is a smooth projective curve of genus 1 over a field K, together with a K-rational point $\mathcal{O}$.

Theorem 1.2. *(i) Let $(E, \mathcal{O})$ be an elliptic curve. Then there exist constants a_1, a_2, a_3, a_4 and $a_6 \in K$ and an isomorphism*

$$\phi : E \longrightarrow E(K) = \{[X : Y : Z] \in \mathbb{P}^2_K : F(X, Y, Z) = 0\} \subset \mathbb{P}^2_K$$

with $\phi(\mathcal{O}) = [0 : 1 : 0]$, and where

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3).$$

We say that a curve of this form is in Weierstrass form*.*

(ii) Conversely, any equation in the form F above gives rise to an elliptic curve over K, with K-rational point $[0 : 1 : 0]$.

Proof. This is a consequence of Riemann-Roch. For further details, see [6], III.3. □

It is convenient to pass to an affine piece via the change of variables $x = X/Z$, $y = Y/Z$. In the case where the characteristic of K is not 2 or 3, via simple substitutions (i.e. completing the square and cube), we obtain:

Corollary 1.3. *Let E/K be an elliptic curve over a field K of characteristic not equal to 2 or 3. Then the set of K-rational points can be described as*

$$E(K) = \{(x, y) \in K^2 : f(x, y) = 0\} \cup \mathcal{O},$$

where $f(x, y) = y^2 + xy - x^3 - Bx - C$ and $B, C \in K$.

Remark 1.4: We could also remove the xy term as well; however, in future chapters we will work with curves defined by equations *including* such a term, so it is convenient to develop the theory whilst incorporating it.

It is natural to ask the question of when two Weierstrass cubics, as above, give rise to isomorphic elliptic curves. It turns out we can characterise different Weierstrass forms of a given curve E by a simple change of variables.

Proposition 1.5. *Any two Weierstrass equations for E can be related by a linear change of variables*

$$x' = u^2x + r, y' = u^3y + u^2sx + t,$$

where $u \in K^*$ and $r, s, t \in K$.

Proof. See [6], III.3.1. □

From now on, we assume that K has characteristic 0, i.e. we are in the case above (this certainly includes $\mathbb{C}$ and the p-adic fields, which are the ones we are interested in). We now assign three fundamental constants to an elliptic curve of the form given in Corollary 1.3:

Definition 1.6. Suppose E/K is an elliptic curve given in general Weierstrass form. Define quantities

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Define the *discriminant* of E to be

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

the *j-invariant* of E to be

$$j(E) = c_4^3/\Delta,$$

and the *Hasse invariant* of E to be

$$\gamma(E/K) = -\frac{c_4}{c_6}$$

Lemma 1.7. *Up to a different choice of Weierstrass form:*

(i) The j-invariant $j(E)$ is well-defined,

(ii) The Hasse invariant $\gamma(E/K)$ is well-defined up to squares (i.e. it gives a well-defined element of $K^*/(K^*)^2$).

Proof. See [6], III.1, Table 3.1. □

Remark 1.8: For a curve in the form given in Corollary 1.3, it is easily checked that these quantities satisfy

$$\Delta = B^2 - C - 64B^3 + 72BC - 432C^2,$$
$$j = \frac{(1-48B)^3}{\Delta}.$$

We conclude this section by stating a fundamental result that we will require in later chapters to complete the uniformisation theorem.

Theorem 1.9. *(i) A curve given in Weierstrass form is nonsingular if and only if $\Delta \neq 0$.*

(ii) Two elliptic curves with j-invariant $\neq 0, 1728$ are isomorphic over K if and only if they have the same j-invariant and Hasse invariant.

(iii) If K is algebraically closed, then two elliptic curves are isomorphic over K if and only if they have the same j-invariant.

Proof. For (i), (iii) see [6], III.1.4. For (ii), see [7], V.5.2. □

1.2. Algebraic Curves

In this section, we state some results on the theory of algebraic curves (algebraic varieties whose function fields have transcendence degree 1 over the base field). The main result we require is that for any such function field L/K, there is a smooth irreducible curve V with $L = K(V)$ its function field. We construct V by considering the set of normalised discrete valuations and showing it has the required algebraic structure.

Recall that if V is an algebraic variety, then $P \in V$ is smooth if and only if the local ring of V at P, $\mathcal{O}_{V,P}$, is a regular local ring. So, in the case where V is an algebraic curve, as the transcendence degree of $K(V)$ over K is 1, we have that the maximal ideal is generated by 1 element; thus $\mathcal{O}_{V,P}$ is a discrete valuation ring, and we obtain a discrete valuation on $K(V)/K$, centred at P. It turns out that when V is an irreducible *smooth* curve, this accounts for *all* normalised discrete valuations on $K(V)/K$, as summarised in:

Theorem 1.10. *Let V be an irreducible smooth curve. There is a bijection*

$$\{\text{Points on } V\} \longleftrightarrow \{\text{Normalised discrete valuations on } K(V)/K\}.$$

In particular, every such valuation on $K(V)/K$ is centred at a point of V.

Proof. See [3], I.1.18. □

We now turn to another invariant of a function field, namely the genus. This is characterised by the Riemann-Roch theorem, which we will state in its most relevant form. First, we must define the notion of a divisor on a function field. Throughout, L will be a function field over K with transcendence degree 1, with K algebraically closed, and A the set of normalised discrete valuations on L/K.

Definition 1.11. A *divisor* on A is a formal finite sum of points of A, i.e. it has form

$$\underline{d} = \sum_{v \in A} n_v(v), \quad n_v \in \mathbb{Z},$$

with all but finitely many of the $n_v = 0$. We define the *degree* of a divisor to be

$$\deg(\underline{d}) = \sum_{v \in A} n_v.$$

Denote the group of divisors on A (under the operation of addition) by $\mathrm{Div}(A)$.

Definition 1.12. Let

$$\underline{d} = \sum_{v \in A} n_v(v), \quad \underline{d'} = \sum_{v \in A} n'_v(v)$$

be divisors on A. We say that $\underline{d} \leq \underline{d'}$ if $n_v \leq n'_v \ \forall v \in A$. We say $\underline{d}$ is *effective* if $\underline{d} \geq 0$.

Definition 1.13. Let $f \in L$. Define the principal divisor associated to f to be

$$\mathrm{div}(f) = \sum_{v \in A} v(f)(v).$$

It is a simple check to show that this is well-defined (see [2], I.6.5).

Definition 1.14. Let $\underline{d} \in \mathrm{Div}(A)$. Define

$$L(\underline{d}) = \{f \in L : \mathrm{div}(f) \geq -\underline{d}\},$$

a K-vector space.

We have the tools in place to state a version the Riemann-Roch theorem:

Theorem 1.15 (Riemann-Roch)**.** *Let $\underline{d} \in Div(A)$. Then there is a constant $g \in \mathbb{N}$ such that if $deg(\underline{d}) > 2g - 2$,*

$$\dim_K L(\underline{d}) = \deg(\underline{d}) - g + 1.$$

Definition 1.16. We call this g the *genus* of the function field.

Remark 1.17: If V is a plane curve, the correspondence in Theorem 1.10 shows that the definitions of divisors on V and $K(V)$ (and hence genus) coincide.

We can now state the main result we need:

Theorem 1.18. *Let L/K be a function field of one variable. Then there is an irreducible smooth projective curve V such that $L = K(V)$. Furthermore, the genus of L/K = the genus of V.*

Proof. For the existence of V, see [2], I.6. The result on the genus follows from Remark 1.17. □

Remark: In particular, if L/K is a function field of one variable and genus 1, then it is the function field of some elliptic curve. For a direct proof of this fact, see [3], II.2.17.

2. Complex Uniformisation: A Review

In this chapter, we review the theory of complex uniformisation. We recall results from the study of Riemann surfaces, before explaining why this approach immediately fails over p-adic fields. We then consider uniformising complex elliptic curves over $\mathbb{C}^*$ via the exponential map, and derive series expansions to describe an explicit map for this new approach - which will then carry over to the p-adic case, as required.

2.1. Complex Tori & Elliptic Curves

We begin by stating results about the Weierstrass $\wp$-function.

Definition 2.1. Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function with respect to Λ is defined to be

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Proposition 2.2. *$\wp$ is elliptic with period Λ and is holomorphic on $\mathbb{C}\setminus\Lambda$, with a double pole at each $z \in \Lambda$.*

Proposition 2.3. *$\wp$ satisfies the equation*

$$(\wp')^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3(\Lambda),$$

with g_2, g_3 constants that depend only on Λ.

This leads to the idea of complex uniformisation; define

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

and note we have a well defined map

$$\mathbb{C}/\Lambda \longrightarrow E_\Lambda,$$

$$z \mapsto (\wp(z;\Lambda), \wp'(z;\Lambda)).$$

It turns out that this is an isomorphism of groups (and a complex analytic isomorphism of Riemann surfaces). The complex uniformisation theorem now states:

Theorem 2.4 (Complex Uniformisation)**.** *Let $E : y^2 = x^3 + Ax + B$ with $27B^2 + 4A^3 \neq 0$. Then there exists a lattice $\Lambda \subset \mathbb{C}$ such that $E \cong E_\Lambda$; that is to say,*

$$g_2(\Lambda) = -4A, g_3(\Lambda) = -4B,$$

and the map

$$\mathbb{C}/\Lambda \longrightarrow E, z \mapsto (\wp(z;\Lambda), \frac{1}{2}\wp'(z;\Lambda))$$

is a complex analytic isomorphism.

Proof. See [7], I.4.3. □

Thus every complex elliptic curve is isomorphic to the quotient of $\mathbb{C}$ by a lattice.

2.2. q-Expansions of Elliptic Curves

We would like to develop this theory for p-adic fields. Unfortunately, we are forced to abandon this idea immediately; indeed, let $\Lambda \subset \mathbb{Q}_p$ be a discrete additive subgroup, and suppose $0 \neq x \in \Lambda$. Then $px, p^2x, p^3x, ...$ is a sequence in Λ tending to 0; that is, there are *no* non-trivial discrete subgroups of $\mathbb{Q}_p$. So we must change our approach. We return to the complex case.

A consequence of the theory above ([6], VI.4.1.1) is that homothetic lattices give the same elliptic curve. Thus we can normalise our lattice $\Lambda = \langle 1, \tau \rangle$, with imaginary part $\Im(\tau) > 0$. Write $\wp(z, \tau) = \wp(z, \Lambda)$; then

$$\wp(z+1;\tau) = \wp(z;\tau),$$

that is, we can consider $\wp$ as a function of $u = e^{2\pi i z}$. We also have

$$\wp(z, \tau+1) = \wp(z;\tau),$$

so we can consider $q = e^{2\pi i \tau}$, and find a Fourier expansion of $\wp$ in terms of u and q. Note $|q| < 1$. This consideration induces an isomorphism

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{C}^*/q^{\mathbb{Z}},$$

$$z \mapsto e^{2\pi i z}.$$

Our main task now is to determine an explicit formula for $\wp$ in this new context. We want a function $F(u;q)$ that satisfies

(i) $F(qu;q) = F(u;q)$, and

(ii) F has a double pole at each $u \in q^{\mathbb{Z}}$, but is holomorphic outside of this.

The main idea in constructing such a function is to find a suitable function satisfing (ii) at 1 and then "averaging," adjusting where necessary to ensure convergence. The most basic function with a double pole at 1 is $\frac{1}{(1-X)^2}$, which leads us to consider the series

$$\sum_{n\in\mathbb{Z}} \frac{1}{(1-q^n u)^2}.$$

Unfortunately this does not converge as $n \to -\infty$. We need instead to consider $\frac{X}{(1-X)^2}$ to ensure convergence; it can be shown ([7], I.6.1) that

$$F(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2}$$

converges absolutely and uniformly on compact subsets of $\mathbb{C}^* \backslash q^{\mathbb{Z}}$, and satisfies (i) and (ii).

We now relate this function back to $\wp$. By considering the start of the Laurent series of $\wp$, we obtain

$$\frac{1}{(2\pi i)^2}\wp(u;q) = F(u;q) + \frac{1}{12} - 2\sum_{n\in\mathbb{Z}} \frac{q^n}{(1-q^n)^2},$$

as their difference is holomorphic and elliptic (hence constant), and is thus identically zero since it vanishes at 0. We also require a q-expansion for $\wp'$. We use $\frac{d}{dz} = \frac{d}{du}\frac{du}{dz} = 2\pi i u \frac{d}{du}$, and obtain

$$\frac{1}{(2\pi i)^3}\wp'(u;q) = \sum_{n\in\mathbb{Z}} \frac{q^n u(1+q^n u)}{(1-q^n u)^3}.$$

We now make a change of variables, removing the powers of $(2\pi i)^3$ and the term $1/12$:

$$\frac{1}{(2\pi i)^2}x = x' + \frac{1}{12},$$

$$\frac{1}{(2\pi i)^3}y = 2y' + x.$$

Under this substitution, the equation $y^2 = 4x^3 - g_2x - g_3$ becomes

$$y'^2 + x'y' = x'^3 + B(q)x' + C(q),$$

for B, C functions of q (see Remark 1.4). Note that Proposition 1.5 says that this change induces an isomorphism of the corresponding curves.

We conclude:

Theorem 2.5. *Define series*

$$X(u;q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{q^n}{1-q^n},$$

$$Y(u;q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + \sum_{n\geq 1}\frac{q^n}{1-q^n}.$$

Then the map

$$\mathbb{C}^*/q^{\mathbb{Z}} \longrightarrow E_q : y^2 + xy = x^3 + B(q)x + C(q),$$

$$u \mapsto \begin{cases} (X(u;q), Y(u;q)) & : u \notin q^{\mathbb{Z}} \\ \mathcal{O} & : u \in q^{\mathbb{Z}} \end{cases}$$

is an isomorphism.

Part II: The Uniformisation Theorem

3. p-adic Analysis

Most of the preliminary work we have done so far is over arbitrary fields. We now specialise to the p-adic fields, i.e. finite extensions of $\mathbb{Q}_p$ for a prime p. In this chapter, we will develop the theory of p-adic analysis, including holomorphic/meromorphic functions over a p-adic field K, and quote Schnirelmann's structure theorem for convergent Laurent series. We will then focus on the field of q-periodic meromorphic functions for some $q \in K, |q| < 1$, and show that it is an elliptic function field, i.e. that it is a function field in one variable of genus 1 over K (and all finite extensions of K). We shall thus obtain an elliptic curve using Theorem 1.18, and show that $E_q \cong K^*/q^{\mathbb{Z}}$.

3.1. Definitions and Schnirelmann's Theorem

In what follows, $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$. Note that this is itself algebraically closed (see [3], II.4.16).

Definition 3.1. (i) A *holomorphic function on K* is defined by a Laurent series

$$\sum_{n\in\mathbb{Z}} a_n X^n, a_n \in K,$$

that converges for all $x \in \mathbb{C}_p$. We write H_K for the domain of holomorphic functions on K.

(ii) Let $M_K = \mathrm{Frac}(H_K)$, and say the elements of M_K are *meromorphic functions on K*.

Lev Schnirelmann proved a fundamental result about the structure of these functions, the proof of which we omit:

Theorem 3.2 (Schnirelmann)**.** *Let $f(X) = \sum_{n\in\mathbb{Z}} a_n X^n$, $a_n \in K$, be a Laurent series that converges $\forall x \in \mathbb{C}_p^*$. Then f can be written in the form*

$$f(X) = cX^k \prod_{|\alpha|<1} (1 - \frac{\alpha}{X}) \prod_{|\alpha|\geq 1} (1 - \frac{X}{\alpha}),$$

where the product is over $\{\alpha : f(\alpha) = 0\}$.

Proof. See [3], II.4.16. □

Remark 3.3: The non-archimedean property of the valuation on K makes the theory of series considerably easier than the corresponding case over $\mathbb{C}$. In particular, $|f(x)| = |\sum a_n x^n| \leq \max\{|a_n x^n|\}$, with equality if there is a *strict* maximum. We see that in particular, f can only be zero on *critical spheres* $|x| = r$, where there exists $m, n \in \mathbb{Z}$ such that $|a_m r^m| = |a_n r^n| = \max_i(|a_i x^i|)$. It can be shown that there is a finite, non-empty set of zeros on each of these critical spheres (see the proof of Schnirelmann). In particular, Schnirelmann says that any meromorphic function has form

$$f(X) = cX^k \prod_{|\alpha|<1} (1 - \frac{\alpha}{X})^{m_\alpha} \prod_{|\alpha|\geq 1} (1 - \frac{X}{\alpha})^{m_\alpha},$$

where the product is over all $\alpha \in \mathbb{C}_p^*$, and the m_α satisfy

(i) Only finitely many $m_\alpha \neq 0$ in an annulus $0 < r \leq |\alpha| \leq r' < \infty$;

(ii) $m_\alpha = m_{\sigma(\alpha)} \quad \forall \sigma \in \mathrm{Gal}(\overline{K}/K)$.

Definition 3.4. Let $q \in K$ with $|q| < 1$. A meromorphic function $f \in M_K$ is said to be *q-periodic* if it satisfies

$$f(q^{-1}X) = f(X).$$

Denote the space of q-periodic functions on K by $L_K(q)$.

3.2. Divisors and Theta functions

Every point $\alpha \in K^*$ gives rise to a discrete normalised valuation on M_K/K, namely ord_α, the *order of vanishing* at α. Such a set of valuations leads to a natural definition of the *divisor* of a meromorphic function f.

Definition 3.5. Let $f \in M_K$. Then define

$$\mathrm{div}(f) = \sum_{\alpha \in \mathbb{C}_p^*} m_\alpha(\alpha),$$

where $m_\alpha = \mathrm{ord}_\alpha(f)$.

Remark: The integers m_α satisfy conditions (i), (ii) of remark 3.3. In general, we say any such collection of integers

$$\{m_\alpha : \alpha \in \mathbb{C}_p^*\}$$

that satisfy these conditions is a *divisor over K*. Call the space of such divisors $\mathrm{Div}(K^*)$.

Note that the definitions of 'effective divisor' and the vector space $L(\underline{d})$ carry over directly from Chapter 1.2.

Proposition 3.6. *Let $\underline{d}$ be a divisor over K. Then $\exists \ 0 \neq f \in M_K$ such that $\underline{d} = \mathrm{div}(f)$.*

Proof. (sketch). Construct such a function using Schnirelmann. (See [4], p11). □

The following are two crucial definitions on the subsequent theory.

Definition 3.7. We say a divisor is *q-periodic* if

$$m_{q^{-1}\alpha} = m_\alpha \quad \forall \alpha \in \mathbb{C}_p^*,$$

and write $\mathrm{Div}(K^*/q^{\mathbb{Z}})$ for the space of q-periodic divisors over K.

Definition 3.8. A *theta function* for q is a meromorphic function with a q-periodic divisor.

Remark: Suppose θ is a theta function for 1 with divisor $\underline{d}$. Then let $\theta'(X) = \theta(q^{-1}X)$. θ and θ' have the same zeros and poles, so by Schnirelmann,

$$\theta'(X) = c^{-1}(-X)^d\theta(X).$$

Proposition 3.9. *There are well defined homomorphisms*

$$d_q : \mathrm{Div}(K^*/q^{\mathbb{Z}}) \longrightarrow \mathbb{Z}$$
$$\underline{d} \mapsto d,$$
$$\phi_q : \mathrm{Div}(K^*/q^{\mathbb{Z}}) \longrightarrow K^*/q^{\mathbb{Z}}$$
$$\underline{d} \mapsto c \pmod{q^{\mathbb{Z}}}.$$

Proof. Schnirelmann tells us that if θ'' is a general function with divisor $\underline{\mathrm{d}}$, then

$$\theta''(X) = bX^k\theta(X).$$

Thus we have

$$\begin{aligned}\theta''(X) &= bq^{-k}X^k c^{-1}(-X)^d\theta(X)\\ &= (cq^k)^{-1}(-X)^d\theta''(X),\end{aligned}$$

i.e. we see that we can associate to $\underline{d}$ a well-defined integer d and a well-defined value of $c \pmod{q^{\mathbb{Z}}}$. The maps we obtain are clearly homomorphisms. □

We can describe these homomorphisms more explicity:

Lemma 3.10. *(i) The map d_q is the* degree homomorphism *that maps*

$$\underline{d} \mapsto \sum_{|q|<|\alpha|\leq 1} m_\alpha.$$

(ii) The map ϕ_q is the Abel-Jacobi homomorphism *that maps*

$$\underline{d} \mapsto \prod_{|q|<|\alpha|\leq 1} \alpha^{m_\alpha}.$$

[Note that these are finite by condition (i) of 3.3.]

Proof. Consider the most basic theta function, namely

$$\theta_0(X) = \prod_{n\leq 0}(1-q^nX^{-1})\prod_{n>0}(1-q^{-n}X),$$

with $\mathrm{div}(\theta_0) = (1)$. A simple check shows that $\theta_0(q^{-1}X) = -X\theta_0(X)$, i.e.

$$d_q((1)) = 1, \quad \phi_q((1)) \equiv 1 \pmod{q^{\mathbb{Z}}}.$$

Now put $\theta_\alpha(X) = \theta_0(\alpha^{-1}X)$, i.e. $\mathrm{div}(\theta_\alpha) = (\alpha)$. Now

$$\theta_\alpha(q^{-1}X) = (\alpha q)^{-1}(-X)\theta_\alpha(X),$$
$$\text{hence} \quad d_q((\alpha)) = 1, \quad \phi_q((\alpha)) \equiv \alpha \pmod{q^{\mathbb{Z}}}.$$

Now take a general divisor $\underline{d} = \sum m_\alpha(\alpha)$. We easily see that $\prod(\theta_\alpha)^{m_\alpha}$ is a theta function for $\underline{d}$. Then

$$d_q(\underline{d}) = \sum m_\alpha = \deg(\underline{d}),$$
$$\phi_q(\underline{d}) = \prod \alpha^{m_\alpha},$$

over suitable limits, as required. □

Corollary 3.11. *A q-periodic divisor $\underline{d} = \sum m_\alpha(\alpha) \in \mathrm{Div}(K^*/q^{\mathbb{Z}})$ is the divisor of a q-periodic function*

$$\iff \deg(\underline{d}) = 0, \quad \prod \alpha^{m_\alpha} \equiv 1 \pmod{q^{\mathbb{Z}}}.$$

3.3. Constructing the Curve

Thus far we have constructed the field $L_K(q)$ of q-periodic meromorphic functions on K^*, and shown that their divisors satisfy a fairly strong condition. We are in a position to describe the genus of $L_K(q)$, using Riemann-Roch and the following:

Lemma 3.12. *Let $\underline{d} \in \mathrm{Div}(K^*/q^{\mathbb{Z}})$ be a q-periodic divisor over K, with $\deg(\underline{d}) > 0$. Then*

$$\dim_K L(\underline{d}) = \deg(\underline{d}).$$

Proof. Induct on $\deg(\underline{d})$. We see that we can, in fact, adapt the statement to expand it to $\deg(\underline{d}) = 0$; Corollary 3.11 tells us that we have proved

$$\dim_K L(\underline{d}) = \deg(\underline{d}) = 0,$$

provided $\phi_q(\underline{d}) \not\equiv 1 \pmod{q^{\mathbb{Z}}}$.

Now suppose $\deg(\underline{d}) = d$, and we have proved the result for all divisors of degree $d-1$. Let $a = \phi_q(\underline{d})$, and pick $b \not\equiv 1, a \pmod{q^{\mathbb{Z}}}$. Then

$$\deg(\underline{d} - (b)) = d - 1 \Rightarrow \dim_K L(\underline{d} - (b)) = d - 1.$$

(Note induction holds at d = 1 since $\phi_q(\underline{d} - (b)) \not\equiv 1 \pmod{q^{\mathbb{Z}}}$.) We see that $L(\underline{d} - (b))$ is the kernel of the linear map

$$L(\underline{d}) \longrightarrow K, \quad f \mapsto f(b).$$

Rank-nullity implies we need only prove surjectivity to complete the proof. But

$$(d-1)(1) + (a) - \underline{d}$$

is a principal divisor whose associated function f does not vanish at b; hence f has non-zero image in K, i.e. the map is surjective. □

We'd like to conclude that $L_K(q)$ has genus 1 over K. But Riemann-Roch is a statement about *algebraically closed* fields. We must show that the lemma holds for any enlargement of the field of constants, as then it holds over the algebraic closure (the union of all finite extensions).

Proposition 3.13. *Let F/K be a finite extension. Then $L_K(q) \cdot F = L_F(q)$. (i.e. if we extend the field of constants via a finite extension F of K, we obtain the q-periodic functions on F).*

Proof. Pick $u_1, ..., u_n$ a basis for F/K. Then the u_j also give a basis of H_F/H_K and M_F/M_K. If $f \in M_F$, write

$$f = \sum_i u_i f_i, \quad f_i \in M_K.$$

Then linear independence of the u_j gives that f q-periodic if and only if f_i q-periodic for all i. Thus the u_j also give a basis of $L_F(q)/L_K(q)$, that is, $L_F(q) = L_K(q) \cdot F$, as required. □

Corollary 3.14. *$L_K(q)$ has genus 1 over K.*

We've now proved that there is some elliptic curve, say E_q, such that $L_K(q) \cong K(E_q)$. We need to show that $E_q \cong K^*/q^{\mathbb{Z}}$. To do so, we recall the correspondence

$$\{\text{Points on } E_q\} \longleftrightarrow \{\text{normalised discrete valuations on } L_K(q)\} = A(L_K(q)).$$

Lemma 3.15. *There is an isomorphism*

$$\overline{K}^*/q^{\mathbb{Z}} \longrightarrow A(L_{\overline{K}}(q)) \longrightarrow E_q(\overline{K}),$$

$$\alpha \longmapsto \text{ord}_\alpha \longmapsto P_\alpha,$$

where ord_α *is centred at* P_α.

Proof. The second map, and hence the composite, is injective, since E_q is smooth (the first map is clearly injective).

Surjectivity: take a point Q in $E_q(\overline{K})$. Then take a function

$$f \in L(2Q)\backslash K,$$

where we note $2Q$ is a divisor in the usual sense on the curve. Such a function exists by 3.12. Schnirelmann says that such a function must have a pole in $\overline{K}^*/q^{\mathbb{Z}}$. But if Q is *not* in the image, then there is no point of $\overline{K}^*/q^{\mathbb{Z}}$ that gives rise to a valuation centred at Q, i.e. there is no pole in $\overline{K}^*/q^{\mathbb{Z}}$, contradiction. Thus the map is bijective and we obtain the required isomorphism. □

Corollary 3.16. $E_q(K) = K^*/q^{\mathbb{Z}}$.

Proof. Take $\text{Gal}(\overline{K}/K)$ invariants in 3.15. □

4. Invariant Calculations

The remaining work in the uniformisation theorem comes in determining which p-adic elliptic curves can be written in the form $K^*/q^{\mathbb{Z}}$. In this (somewhat technical) chapter, we will use formulae from complex uniformisation (see chapter 2) to define the 'Tate map', an explicit isomorphism $K^*/q^{\mathbb{Z}} \longrightarrow E_q(K)$, and use it to determine the j-invariant and Hasse invariant of E_q. We thus obtain the *necessary* condition that any p-adic elliptic curve that can be uniformised in this way has non-integral j-invariant and trivial Hasse invariant (we see in chapter 5 that these conditions are in fact sufficient).

4.1. The Tate Map

Recall 2.5; we defined series

$$X(u;q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{q^n}{1-q^n},$$

$$Y(u;q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + \sum_{n\geq 1}\frac{q^n}{1-q^n},$$

and obtained an isomorphism

$$\mathbb{C}^*/q^{\mathbb{Z}} \longrightarrow E_q(\mathbb{C}) : y^2 + xy = x^3 + B(q)x + C(q),$$

$$u \mapsto \begin{cases} (X(u;q), Y(u;q)) & : u \notin q^{\mathbb{Z}} \\ \mathcal{O} & : u \in q^{\mathbb{Z}} \end{cases}$$

Recall also Theorem 1.18, which says that a genus 1 function field L of one variable over an algebraically closed field K is the function field of some elliptic curve. In the proof, we take an arbitrary principal divisor (say $\underline{d} = (1)$) and consider

$$x \in L(2\underline{d})\backslash K, \quad y \in L(3\underline{d})\backslash L(2\underline{d}),$$

obtaining that $L = K(x,y)$. Details of this approach are in [3], II.2.17.

Now $X(u;q)$ has a pole of order 2 at 1 (mod $q^{\mathbb{Z}}$), and $Y(u;q)$ a pole of order 3. It follows that

$$L_{\overline{K}}(q) = \overline{K}(X,Y),$$

with the relation

$$Y^2 + XY = X^3 + B(q)X + C(q) \quad \text{(see 2.5)}.$$

Note that as $|q| < 1$, the series for X, Y obviously converge to a limit in the complete field $K(u,q)$ (a finite extension of K). So we see that the equation above is satisfied p-adically by considering it as an identity of formal power series (and using the complex case). We conclude:

Theorem 4.1 (Tate)**.** *Let K be a p-adic field, and let $X(u;q)$ and $Y(u;q)$ be as above. Then the map*

$$K^*/q^{\mathbb{Z}} \longrightarrow E_q(K) : y^2 + xy = x^3 + B(q)x + C(q),$$

$$u \mapsto \begin{cases} (X(u;q), Y(u;q)) & : u \notin q^{\mathbb{Z}} \\ \mathcal{O} & : u \in q^{\mathbb{Z}} \end{cases}$$

is an isomorphism.

4.2. Calculating the j-invariant

To calculate the j-invariant, we need to find explicit formulae for $B(q), C(q)$ in 4.1; then we can use Remark 1.8 to conclude.

Definition 4.2. Let $s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}$.

Lemma 4.3. *We have the equalities:*

(i) $B(q) = -5s_3(q)$,

(ii) $C(q) = -\frac{1}{12}[5s_3(q) + 7s_5(q)]$.

Proof. Define $D = u\frac{d}{du}$, a differential operator. Note (via a simple check) that

$$Y = \frac{1}{2}(DX - X),$$

that is,

$$(DX)^2 - X^2 = 4(X^3 + BX + C). \tag{1}$$

Observe that

$$\frac{q^n u}{(1-q^n u)^2} = u\frac{d}{du}\left(\frac{1}{1-q^n u}\right) = \sum_{m\geq 1} mq^{mn}u^m,$$

and also that

$$\frac{q^n u}{(1-q^n u)^2} = \frac{q^{-n}u^{-1}}{(1-q^{-n}u^{-1})^2},$$

so that

$$X(u;q) = \sum_{n\in\mathbb{Z}}\sum_{m\geq 1} mq^{mn}u^m - 2s_1$$

$$= \frac{u}{(1-u)^2} + \sum_{n\geq 1}\sum_{m\geq 1}\frac{mq^n}{1-q^n}(u^m + u^{-m}) - 2s_1.$$

We can consider q as an indeterminate, and thus consider the above series to have coefficients in the field $\mathbb{Q}((q))$. To ease the calculation, we make the change of variables, setting

$$T = \log u = -\sum_{n\geq 1}\frac{(1-u)^n}{n}.$$

This means

$$D = u\frac{d}{du} = \frac{d}{dT}.$$

The idea of such a substitution is to give a suitable Laurent expansion in T that we can then differentiate normally to substitute into the equation (1) above. We first define a set of important constants, the *Bernoulli numbers*.

Definition 4.4. The *Bernoulli numbers* B_k are defined to be the constants satisfying the following expression:

$$\frac{T}{e^T - 1} = \sum_{k=0}^{\infty} B_k \frac{T^k}{k!}.$$

We can calculate the Bernoulli numbers for small examples, and find

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_3 = B_5 = 0.$$

Using this, we can expand the first term in the above as

$$\frac{e^T}{(1-e^T)^2} = \frac{d}{dT}\left(\frac{1}{1-e^T}\right) = \frac{d}{dT}\left(\frac{1}{T}\frac{T}{1-e^T}\right) = -\frac{d}{dT}\left(\frac{1}{T}\sum_{k\geq 0} B_k \frac{T^k}{k!}\right)$$

$$= \frac{1}{T^2} - \sum_{k\geq 0} \frac{B_{k+2}}{k!}\frac{T^k}{k+2}.$$

Thus we can rewrite X (after expanding the second term) as

$$X(T;q) = \frac{1}{T^2} - \sum_{k\geq 0} \frac{B_{k+2}}{k+2}\frac{T^k}{k!} + 2\sum_{\substack{n>0 \\ n \text{ even}}} s_{n+1}\frac{T^n}{n!}. \tag{2}$$

Applying D to (1), as $DX \neq 0$, we obtain

$$D^2X - 2X = 6X^2 + 2B. \tag{3}$$

Substituting (2) into (3) and considering the constant term gives

$$B(q) = -5s_3(q).$$

Now using this and substituting (2) into (1), it follows (again by considering the constant term) that

$$C(q) = -\frac{1}{12}[5s_3(q) + 7s_5(q)],$$

as required. □

Corollary 4.5. *The coefficients B and C have integral coeffiecients, that is, they lie in $\mathbb{Z}[[q]]$.*

Proof. We have $n^3 \equiv n^5 (\text{mod } 12)$, so $5s_3 + 7s_5 \equiv 0 (\text{mod } 12)$, so the coefficients lie in $\mathbb{Z}$. □

Proposition 4.6. *(i) The discriminant of E_q satisfies $\Delta(E_q) \equiv q \pmod{q^2}$.*

(ii) There exists $R(q) \in \mathbb{Z}[[q]]$ such that $j(E_q) = \frac{1}{q} + R(q)$.

Proof. Recall Remark 1.8, which said that

$$\Delta = B^2 - C - 64B^3 + 72BC - 432C^2,$$

$$j = \frac{(1-48B)^3}{\Delta}.$$

(i) Now $s_3 \equiv s_5 \pmod{q^2}$, that is,

$$5s_3 + 7s_5 \equiv 12s_3 \pmod{12q^2},$$

proving that

$$C(q) \equiv -s_3 \equiv -q \pmod{q^2}.$$

Also, B(q) $\equiv -5q \pmod{q^2}$, so it follows that

$$\Delta \equiv -C(q) \equiv q \pmod{q^2}.$$

(ii) From (i),

$$j(E_q) = \frac{1}{q}h(q), \quad h(q) = \alpha(q)/\beta(q)$$

(where $\alpha, \beta \in \mathbb{Z}[[q]]$ with $\alpha, \beta \equiv 1 \pmod{q}$). Therefore we see easily that

$$h \in \mathbb{Z}[[q]], \;\; h \equiv 1 \pmod{q}$$

giving $j(E_q) = \frac{1}{q} + R(q)$ with $R(q) \in \mathbb{Z}[[q]]$ as required.

□

4.3. Calculating the Hasse invariant

Recall: $\gamma(E_q/K) = -c_4/c_6$, well-defined up to squares. Simple calculation gives, for E_q in the form of 4.1,

$$c_4(q) = 1 - 48B(q) = 1 + 240s_3(q),$$
$$c_6(q) = -1 + 72B(q) - 864C(q) = -1 + 504s_5(q).$$

Lemma 4.7. *Let $\alpha \in K^*$, with $|\alpha| < 1$. Then $1+4\alpha$ is a square in K.*

Proof. We consider the binomial coefficients

$$\binom{-1/2}{n} = \frac{(-1)^n}{4^n}\binom{2n}{n} \in \frac{1}{4^n}\mathbb{Z}.$$

Thus

$$(1+4\alpha)^{-1/2} = \sum_{n\geq 0}\binom{-1/2}{n}(4\alpha)^n = \sum_{n\geq 0}(-1)^n\binom{2n}{n}\alpha^n$$

is a power series in α with integer coefficients. As $|\alpha| < 1$, this series converges, so $(1+4\alpha)^{-1}$ is a square, which implies that $1 + 4\alpha$ is a square. □

Corollary 4.8. *We have $\gamma(E_q/K) \equiv 1 \pmod{K^*}$.*

Proof. As c_4 and $-c_6$ are squares in K, we know $-c_4/c_6$ is a square in K. □

Corollary 4.9. *For any choice of $q \in K$ with $|q| < 1$, we have $|j(E_q)| > 1$ and $\gamma(E_q/K) = 1$. In particular, a necessary condition for a p-adic curve to be uniformised in this way is that it has non-integral j-invariant and trivial Hasse invariant.*

Proof. The j-invariant and Hasse invariant of an elliptic curve are preserved by isomorphism. □

5. Tate's Uniformisation Theorem

To conclude our work with elliptic curves, we will show that the necessary conditions of Chapter 4 (i.e. Corollary 4.9) are in fact sufficient. We will also prove that for a p-adic elliptic curve E with non-integral j-invariant,

$$\gamma(E/K) \equiv 1 \pmod{(K^*)^2} \text{ if and only if } E \text{ has split multiplicative reduction,}$$

and thus obtain an alternate necessary and sufficient condition.

First, a lemma on power series.

Lemma 5.1. *Let $R(X) = \sum a_i X^i$ be a power series with integral coefficients in K. Then the function*

$$\phi : \{q \in K : 0 < |q| < 1\} \longrightarrow \{r \in K : |r| > 1\},$$
$$q \longmapsto \frac{1}{q} + R(q),$$

is a bijection.

Proof. Firstly it's clear that ϕ maps into the correct set, as

$$\left|\frac{1}{q} + R(q)\right| = \left|\frac{1}{q}\right| > 1.$$

It is injective: if $\phi(q_1) = \phi(q_2)$, then

$$\frac{|q_1 - q_2|}{|q_1 q_2|} = \left|\frac{1}{q_1} - \frac{1}{q_2}\right| = |R(q_1) - R(q_2)|$$
$$= |a_1(q_1 - q_2) + a_2(q_1^2 - q_2^2) + \cdots|$$
$$= |q_1 - q_2| \cdot |a_1 + a_2(q_1 + q_2) + \cdots|.$$

But $1/|q_1 q_2| > 1$, and $|a_1 + a_2(q_1 + q_2) + \cdots| \leq 1$ (as $a_i \in \mathcal{O}_K$), so we conclude that

$$|q_1 - q_2| = 0 \Rightarrow q_1 = q_2.$$

It is surjective: given $r \in K$ with $|r| > 1$, construct q by setting

$$q_0 = \frac{1}{r}, \quad q_{i+1} = \frac{1}{r}(1 + q_i R(q_i)),$$
$$q = \lim_{i \to \infty} q_i.$$

A simple check shows that $\phi(q) = r$. □

Corollary 5.2. *Let E/K be an elliptic curve with $|j(E)| > 1$. Then there exists some $q \in K$, with $|q| < 1$, such that $E \cong E_q$ over $\overline{K}$.*

Proof. In 4.6, we proved that

$$j(E_q) = \frac{1}{q} + R(q), \quad R \in \mathbb{Z}[[q]]$$

(for some integral power series R). Take this R in the lemma. Pick q such that $\phi(q) = j(E)$; then $j(E) = j(E_q)$, so 1.9 (iii) gives $E \cong E_q$ over an algebraic closure of K. □

Recall the set-up: K is a p-adic field, with ring of integers $\mathcal{O}_K$, uniformiser π and residue field k, and E/K is an elliptic curve. We can consider reduction (mod π) to obtain a curve $\tilde{E}(k)$. The curve has *good reduction* if $\tilde{E}$ is smooth, or *bad reduction* otherwise. We say a curve has *split multiplicative reduction* if $\tilde{E}$ has a node and the tangent slopes lie in k (recall that a curve in Weierstrass form has a node if and only if $\Delta = 0$ and $c_4 \neq 0$). For more on reduction, see [6], VII.5.

Theorem 5.3 (Tate's Uniformisation Theorem)**.** *Let E/K be an elliptic curve with $|j(E)| > 1$, and pick $q \in K$ such that $E \cong E_q$ over $\overline{K}$. The following are equivalent:*

(i) $E \cong E_q$ over K;

(ii) $\gamma(E/K) \equiv 1 \pmod{(K^*)^2}$;

(ii) E has split multiplicative reduction.

Proof. (i) $\iff$ (ii) follows from Theorem 1.9 (ii) and 4.8.

(i) $\Rightarrow$ (iii): it suffices to show that E_q has split multiplicative reduction. Now $|s_3(q)| < 1$, $|s_5(q)| < 1$, so the reduced curve has form

$$y^2 + xy = x^3.$$

The singular point is at $(0, 0)$; we can write the curve as the locus of

$$f(x, y) = (y + x)y - x^3,$$

i.e. the tangent slopes at the singular point are 0 and $1 \in k$. As $0 \neq 1$, the singular point is a node, so we have split multiplicative reduction.

(iii) $\Rightarrow$ (ii): take E a curve with split multiplicative reduction, and a minimal Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that the singular point is at $(0, 0)$.

We know $(0, 0)$ is on the curve, so $a_6 \equiv 0 \pmod{\pi}$, and it is singular, so $a_3 \equiv a_4 \equiv 0 \pmod{\pi}$. Thus

$$b_4 = a_1a_3 + 2a_4 \equiv 0 \pmod{\pi}, \quad b_6 = a_3^2 + 4a_6 \equiv 0 \pmod{\pi},$$

$$c_4 = b_2^2 - 24b_4 \equiv b_2^2 \pmod{\pi}.$$

Now $\tilde{E}$ has a node, so $c_4 \neq 0$, that is, b_2 is a unit in k. Now

$$\gamma(E/K) = -\frac{c_4}{c_6} = \frac{1}{b_2}\left(\frac{1 - 24\frac{b_4}{b_2^2}}{1 - 36\frac{b_4}{b_2^2} + 216\frac{b_6}{b_2^3}}\right).$$

By Lemma 4.7, the numerator and denominator of the bracket are both squares, so this is

$$\equiv \frac{1}{b_2} \equiv b_2 \pmod{(k^*)^2}.$$

It remains to prove that $b_2 = a_1^2 + 4a_2$ is a square in K^*. We've shown that the reduced curve has form

$$y^2 + \tilde{a_1}xy = x^3 + \tilde{a_2}x^2,$$

and we can factorise over the algebraic closure $\overline{k}$ to get

$$(y - \tilde{\alpha}x)(y - \tilde{\beta}x) = y^2 + \tilde{a_1}xy - \tilde{a_2}x^2.$$

In fact, note that as the reduction is split, $\tilde{\alpha}$ and $\tilde{\beta}$ lie in k; hence we can use Hensel's lemma to lift to $\alpha, \beta \in K$ with $\alpha \neq \beta$ and

$$(y - \alpha x)(y - \beta x) = y^2 + a_1xy - a_2x^2.$$

Thus

$$a_1 = -(\alpha + \beta), \quad a_2 = -\alpha\beta$$
$$\Rightarrow b_2 = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2 \in (K^*)^2,$$

i.e. $\gamma(E_q/K) \equiv 1 \pmod{(K^*)^2}$.

Thus (ii) $\iff$ (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii), and we are done. □

Corollary 5.4. *Let E/K be an elliptic curve with $|j(E)| > 1$, and take q such that $E \cong E_q$ over $\overline{K}$. Then there is (at worst) a quadratic extension L/K such that $E \cong E_q$ over L.*

Proof. Take $L = K(\sqrt{\gamma(E/K)})$. □

Remark: Corollary 5.4 allows us to describe $E(K)$ explicitly as

$$\{u \in L^*/q^{\mathbb{Z}} : N_{L/K}(u) \in q^{\mathbb{Z}}/q^{2\mathbb{Z}}\}.$$

For details, see [7], V.5.4.

This concludes our work with Tate's uniformisation theorem.

Part III: Mumford Curves

6. The Tree of a Compact Subset of $\mathbb{P}^1_K$

In the sequel, we will define Schottky groups - certain subgroups of $\mathrm{PGL}_2(K)$ - and prove that any such group Γ is free. To do so, we will associate to Γ a *tree* $\mathcal{T}(X)$ (for suitable compact $X \subset \mathbb{P}^1_K$) and hence a finite graph $\mathcal{T}(X)/\Gamma$ upon which Γ acts freely.

In this chapter, we will use the notion of reduction to define an equivalence relation on distinct triples of points in $\mathbb{P}^1_K$ (or, subsequently, $X \subset \mathbb{P}^1_K$). We then take for our vertices the equivalence classes and study the images of reductions to add edges. We will eventually conclude that the resulting graph is a locally finite tree, and prove a useful result connecting limit points of X to halflines in $\mathcal{T}(X)$.

First, we gather some relevant definitions:

Definition 6.1. A *tree* $\mathcal{T}$ is a connected graph with no cycles. A tree $\mathcal{T}$ is said to be *locally finite* if for a vertex v there are a finite number of vertices u connected to v by a single edge.

Definition 6.2. A *halfline* in a tree is an infinite chain of consecutive edges, with no repeated vertices, and with a specified endpoint.

6.1. Reductions of $\mathbb{P}^1_K$

Let $a = (a_0, a_1, a_\infty)$ be a triple of distinct points in $\mathbb{P}^1_K$. Then there is a unique automorphism γ_a of $\mathbb{P}^1_K$ mapping $a_0 \mapsto 0, a_1 \mapsto 1$, and $a_\infty \mapsto \infty$.

Definition 6.3. Define the *reduction of* $\mathbb{P}^1_K$ *at* a by

$$R_a : \mathbb{P}^1_K \xrightarrow{\gamma_a} \mathbb{P}^1_K \xrightarrow{R} \mathbb{P}^1_k,$$

where R is the standard reduction (mod π) for a uniformiser π.

Definition 6.4. Define, for a, b two distinct triples in $\mathbb{P}^1_K$,

$$R_{a,b} : \mathbb{P}^1_K \xrightarrow{\gamma_a \times \gamma_b} \mathbb{P}^1_K \times \mathbb{P}^1_K \xrightarrow{R \times R} \mathbb{P}^1_k \times \mathbb{P}^1_k.$$

$R_a, R_{a,b}$ are both clearly continuous (where $\mathbb{P}^1_k$ has the discrete topology).

Proposition 6.5. *Let a and b be triples of distinct points in $\mathbb{P}^1_K$.*

(i) If $\gamma_a \gamma_b^{-1} \in \mathrm{PGL}_2(\mathcal{O}_K)$, then $R_{a,b}(\mathbb{P}^1_K) \cong \mathbb{P}^1_k$.

(ii) If $\gamma_a \gamma_b^{-1} \notin \mathrm{PGL}_2(\mathcal{O}_K)$, then $R_{a,b}(\mathbb{P}^1_K) \subseteq \{\alpha\} \times \mathbb{P}^1_k \cup \mathbb{P}^1_k \times \{\beta\}, \quad \alpha, \beta \in \mathbb{P}^1_k$.

Note that equivalently, this says that if the reduction of $\gamma_a \gamma_b^{-1}$ to an endomorphism of $\mathbb{P}^1_k$ is invertible, then the image of $R_{a,b}$ is isomorphic to a single copy of $\mathbb{P}^1_k$; otherwise, it is a subset of two intersecting copies of $\mathbb{P}^1_k$.

Proof. (i) We have the commutative diagram

$$\begin{array}{ccccc} \mathbb{P}^1_K & \xrightarrow{\gamma_b} & \mathbb{P}^1_K & \xrightarrow{\gamma_a \gamma_b^{-1} \times \mathrm{id}} & \mathbb{P}^1_K \times \mathbb{P}^1_K \\ & & \downarrow R & & \downarrow R \times R \\ & & \mathbb{P}^1_k & \xrightarrow{A \times \mathrm{id}} & \mathbb{P}^1_k \times \mathbb{P}^1_k, \end{array}$$

where A denotes the reduction $\overline{\gamma_a\gamma_b^{-1}}$. Clearly the composite of the two top maps with the right hand map is $R_{a,b}$. Now $\gamma_a\gamma_b^{-1} \in \mathrm{PGL}_2(\mathcal{O}_K)$, so A is invertible, i.e.

$$\mathrm{Im}(R_{a,b}) = \mathrm{Im}(A \times \mathrm{id}) \cong \mathbb{P}^1_k$$

(since $R \circ \gamma_b$ is surjective).

(ii) Write

$$\gamma_a\gamma_b^{-1} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Then we see that the image of $\gamma_a \times \gamma_b$ lies in the zero set of the polynomial

$$F = -y_0(a_{21}x_1 + a_{22}x_0) + y_1(a_{11}x_1 + a_{12}x_0),$$

since

$$\mathrm{Im}(\gamma_a \times \gamma_b) = \mathrm{Im}((\gamma_a\gamma_b^{-1} \times \mathrm{id}) \circ \gamma_b) = \mathrm{Im}(\gamma_a\gamma_b^{-1} \times \mathrm{id})$$

(as γ_b is surjective). Here we have used the notation $([x_0 : x_1], [y_0 : y_1]) \in \mathbb{P}^1_K \times \mathbb{P}^1_K$.

Now if A is not invertible, then the reduction $F \pmod{\pi}$ factorises as

$$\overline{F} = (Ax_0 + Bx_1)(Cy_0 + Dy_1),$$

that is, the zero set of $\overline{F}$ is

$$Z(\overline{F}) = \{\alpha\} \times \mathbb{P}^1_k \cup \mathbb{P}^1_k \times \{\beta\},$$

some $(\alpha, \beta) \in \mathbb{P}^1_k \times \mathbb{P}^1_k$. The result follows since $\mathrm{Im}(R_{a,b}) \subseteq Z(\overline{F})$. □

6.2. The Tree of $X \subset \mathbb{P}^1_K$

Let $X \subset \mathbb{P}^1_K$ be a compact set.

Definition 6.6. Write $X^{(3)} \subset X^3$ for the set of all distinct triples in X. Given $a, b \in X^{(3)}$, we say a and b are *equivalent* if $\gamma_a\gamma_b^{-1} \in \mathrm{PGL}_2(\mathcal{O}_K)$.

This clearly defines an equivalence relation on $X^{(3)}$.

Definition 6.7. Suppose a and b are inequivalent points in $X^{(3)}$. We say a and b are *connected* if $(\alpha, \beta) \notin R_{a,b}(X)$ (where α, β are as in Proposition 6.5 (ii)). That is, a and b are connected if and only if $R_{a,b}(X)$ is the union of two lines and their intersection is not contained in this image.

Remark: Being connected is clearly a well-defined notion for equivalence classes of points in $X^{(3)}$; if $a \sim a'$, and a connected with b, then as $\gamma_a\gamma_a'^{-1}$ is an automorphism, $R_{a,b}(X)$ contains the intersection point if and only if $R_{a',b}(X)$ does.

Definition 6.8. The *tree of* X, denoted $\mathcal{T}(X)$, is the graph obtained by taking as vertices the equivalence classes of points in $X^{(3)}$ and saying $[a]$ and $[b]$ are joined by an edge if and only if a and b are connected.

Note that $R_a(X)$ is finite, say $= \{\alpha_1, ..., \alpha_n\}$. Then for each $a \in X^{(3)}$ we obtain a finite partition of X into (open, compact) disjoint sets $X_i = R_a^{-1}(\alpha_i)$. These partitions entirely determine $\mathcal{T}(X)$, as seen by:

Lemma 6.9. *Let $a, b \in X^{(3)}$. Then*

(i) $a \sim b$ *if and only if* a *and* b *define the same partitions of* X*.*

(ii) a *is connected to* b *if and only if for the corresponding partitions* $\{X_1, ..., X_m\}$ *and* $\{Y_1, ..., Y_n\}$ *we can reorder such that*

$$X_1 = Y_2 \cup \cdots \cup Y_n,$$

$$Y_1 = X_2 \cup \cdots \cup X_m.$$

Proof. (i) Suppose $a \sim b$. We have bijective projection maps

$$\pi_1 : R_{a,b}(X) \longrightarrow R_a(X),$$

$$\pi_2 : R_{a,b}(X) \longrightarrow R_b(X),$$

where bijectivity follows since if $\alpha \in R_a(X)$, pick some $\beta \in R_b(X)$ such that $(\alpha, \beta) \in R_{a,b}(X)$; then this choice of β is unique since (α, β) lies in the image of the (bijective) map

$$\mathbb{P}^1_k \xrightarrow{A \times \mathrm{id}} \mathbb{P}^1_k \times \mathbb{P}^1_k$$

(where A is invertible as $a \sim b$). Thus for $\alpha \in R_a(X)$, pick β as above, then

$$R_a^{-1}(\alpha) = R_{a,b}^{-1}\pi_1^{-1}(\alpha) = R_{a,b}^{-1}\pi_2^{-1}(\beta) = R_b^{-1}(\beta).$$

Thus for each X_i, there exists some Y_j such that $X_i = Y_j$. This process is clearly reversible. Thus the Y_j reorder the X_i and the partitions are the same.

Conversely, suppose the partitions are the same. Then for each $\alpha \in R_a(X)$, there is a unique β such that $R_a^{-1}(\alpha) = R_b^{-1}(\beta)$. Hence it's clear that $R_{a,b}(X)$ is not a subset of $\{\alpha'\} \times \mathbb{P}^1_k \cup \mathbb{P}^1_k \times \{\beta'\}$ for some $\alpha', \beta' \in \mathbb{P}^1_k$, that is, $a \sim b$.

(ii) Suppose a and b are connected. Put

$$X_1 = R_a^{-1}(\alpha), \quad Y_1 = R_b^{-1}(\beta),$$

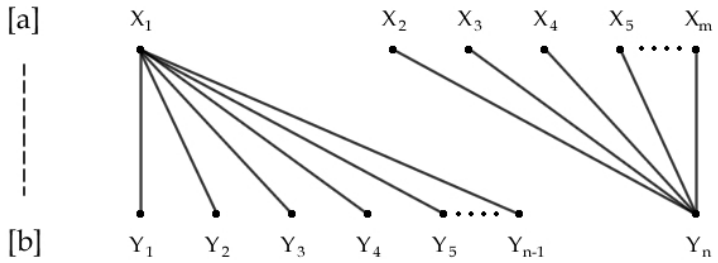
where (α, β) is the intersection point (which does not lie in $R_{a,b}(X)$, since a and b are connected). Then $X_1 \cup Y_1 = X$, and $X_1 \cap Y_1 = \varnothing$ since $(\alpha, \beta) \notin R_{a,b}(X)$, hence it follows that the decomposition has the required form.

Conversely if we have a decomposition of this form, put $\alpha = R_a(X_1), \beta = R_b(Y_1)$. It's clear that $R_{a,b}(X) \subseteq \{\alpha\} \times \mathbb{P}^1_k \cup \mathbb{P}^1_k \times \{\beta\}$ with $(\alpha, \beta) \notin R_{a,b}(X)$. □

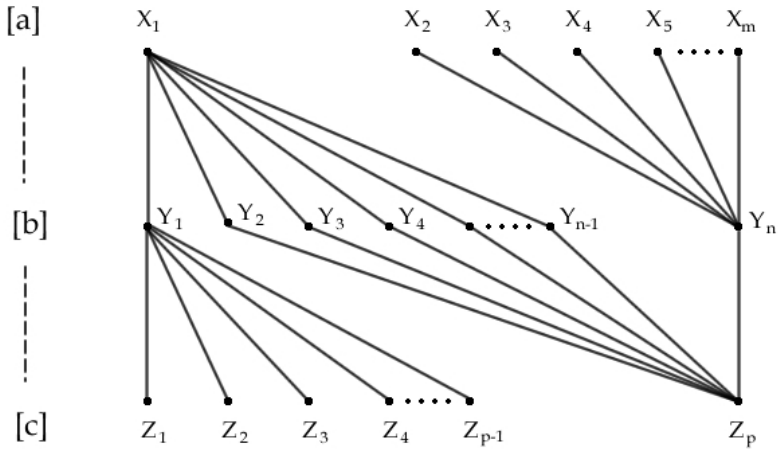
We now quote a lemma that completely describes the edges through a point $[a] \in \mathcal{T}(X)$.

Lemma 6.10. *Let* $[a] \in \mathcal{T}(X)$*, with* $R_a(X) = \{\alpha_1, ..., \alpha_n\}$*. Then if* $|R_a^{-1}(\alpha_i)| > 1$*, there exists a unique* $[b_i] \in \mathcal{T}(X)$ *such that there is a single edge between* $[a]$ *and* $[b_i]$*. Furthermore, all the edges through* $[a]$ *are obtained in this way.*

Lemmas 6.9 and 6.10 allow us to examine chains in $\mathcal{T}(X)$ by looking at the partitions they give rise to. In particular, Lemma 6.9 (ii) means that if $[a]$ is connected to $[b]$, we can (for a certain example) write the partitions like



where here the lines represent inclusions (i.e. $X_1 = Y_1 \cup \cdots \cup Y_{n-1}$). Then for $[b]$ connected to $[c]$, Lemma 6.10 implies that we can do the same, with a necessarily *different* choice of Y_i (i.e. if $Y_n = X_2 \cup \cdots \cup X_m$, we can't write $Y_n = Z_2 \cup \cdots \cup Z_p$), as shown below:



We see that we obtain a sequence of strictly decreasing nested subsets

$$X_1 \supsetneq Y_1 \supsetneq Z_1 \supsetneq \cdots .$$

Corollary 6.11. *There are no cycles (non-trivial finite chains with the same start and end point) in $\mathcal{T}(X)$.*

Proof. Take a cycle, and break it up as $[a] - [b] - [c] - \cdots - [a]$. We obtain

$$X_1 \supsetneq Y_1 \supsetneq Z_1 \supsetneq \cdots \supsetneq X_1',$$

but then $X_1' \in \{X_2, ...X_m\}$. This is a contradiction as the X_i are disjoint. □

Proposition 6.12. *There is a bijection*

$$\{\textit{halflines that start at } [a]\} \longleftrightarrow \{\textit{limit points of } X\}.$$

Proof. Take a halfline $[a_1] - [a_2] - \cdots$. We obtain a sequence

$$X_1^1 \supsetneq X_1^2 \supsetneq X_1^3 \supsetneq \cdots$$

of compact subsets of X. We have

$$\bigcap_{i=1}^{\infty} X_1^i \neq \varnothing,$$

since the X_1^i are closed. Without loss of generality, take $0 \in X_1^i$ for all i. Also without loss of generality $\infty \notin X_1^1$. Thus for each i, we can take a well-defined real number

$$\delta_i = \sup\{|x| : x \in X_1^i\}.$$

As the R_{a_i} are continuous, the X_1^i are open and contain a neighbourhood of 0; disjointness of each partition means

$$X_1^i = \{x \in X_1^1 : |x| \leq \delta_i\},$$

and $\lim_{i\to\infty} \delta_i = 0$, since the valuation on K is discrete and the inclusions $X_1^i \supsetneq X_1^{i+1}$ are strict. Thus

$$\bigcap_{i=1}^{\infty} X_1^i = \{0\},$$

and this is a limit point (as the intersection of an infinite family of open sets).

Conversely, if we take a limit point $\alpha \in X$, and $[a] \in \mathcal{T}(X)$, then we can define a halfline by:

(i) $[a_1] = [a]$,

(ii) $[a_{n+1}]$ is the point connected to $[a_n]$ corresponding to $R_{a_n}(\alpha)$.

Here we note that $|R_{a_n}^{-1}(R_{a_n}(\alpha))| > 1$ since α is a limit point and by continuity of R_{a_n}. □

We collect our results in the following:

Theorem 6.13. *$\mathcal{T}(X)$ is a locally finite tree.*

Proof. All that remains is to show $\mathcal{T}(X)$ connected. Take $[a] \neq [b]$ in $\mathcal{T}(X)$. If they are not connected, then there is some $\alpha \in X$ with $R_{a,b}(\alpha)$ lying on the intersection of the two lines in $R_{a,b}(X)$. Then $R_a^{-1}(R_a(\alpha))$ clearly contains more than one point (since it contains all points corresponding to the second line in the image). So define $[a_1]$ to be the point connected to $[a]$ over $R_a(\alpha)$. Then we continue inductively to define a chain

$$[a] - [a_1] - [a_2] - \cdots$$

in the direction of $[b]$. Such a chain must be finite by our results on halflines, so it defines a path from $[a]$ to $[b]$. □

7. Schottky Groups

We now consider Schottky groups, finitely generated discontinuous subgroups of $\mathrm{PGL}_2(K)$ with no elements of finite order. Such groups give an analogue of the group $q^{\mathbb{Z}}$ studied in the genus 1 case. In this section, we review some properties of general discontinuous groups, and then specialise to prove a structure theorem for Schottky groups, namely that every Schottky group is free. We will conclude by quoting a result that every Schottky group has a good fundamental domain, that is, a subset of $\mathbb{P}^1_K$ with suitable properties. Such domains will be used to define a space Ω with Ω/Γ an algebraic curve.

7.1. Discontinuous Groups

Recall that $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^*$ is the automorphism group of $\mathbb{P}^1_K$. If $\gamma \in \mathbb{P}^1_K$,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then γ acts on $q \in \mathbb{P}^1_K$ by $\gamma(q) = \frac{aq+b}{cq+d}$.

Definition 7.1. Let $\Gamma \leq \mathrm{PGL}_2(K)$ be a subgroup. We say that $\alpha \in \mathbb{P}^1_K$ is a *limit point of* Γ if there is an infinite sequence $(\gamma_n)_{n=1}^{\infty} \subset \Gamma$, with $\gamma_m \neq \gamma_n$ for $m \neq n$, and some $\beta \in \mathbb{P}^1_K$ such that

$$\lim_{n\to\infty} \gamma_n(\beta) = \alpha.$$

We write $\mathcal{L} = \mathcal{L}(\Gamma)$ for the set of limit points of Γ.

Definition 7.2. Let F be a field. We say that a subgroup $\Gamma \leq \mathrm{PGL}_2(F)$ is *discontinuous* if

(i) $\mathcal{L}(\Gamma) \neq \mathbb{P}^1_F$,

(ii) for any $\alpha \in \mathbb{P}^1_F$, the closure $\overline{\Gamma(\alpha)}$ of the orbit of α is compact.

Remarks: (i) Note that if F is locally compact, the second condition is automatic. So when $F = K$ is a p-adic field, Γ is discontinuous if and only if $\mathcal{L}(\Gamma) \neq \mathbb{P}^1_K$. From now on, we assume that we are in this situation.

(ii) If a group Γ is discontinuous, then it is discrete. Indeed, suppose there is some sequence $(\gamma_n)_{n=1}^{\infty} \subset \Gamma$ tending to some $\gamma \in \Gamma$ as n tends to infinity. Then the sequence $(\gamma^{-1}\gamma_n)_{n=1}^{\infty}$ tends to the identity, and hence every point of $\mathbb{P}^1_K$ is a limit point, contradicting the assumption that Γ is discontinuous.

Definition 7.3. Let $\gamma \in \mathrm{PGL}_2(K)$, with eigenvalues λ, μ. We say that γ is

(i) *hyperbolic* if $|\lambda| \neq |\mu|$,

(ii) *parabolic* if $\lambda = \mu$, or

(iii) *elliptic* if $|\lambda| = |\mu|$ but $\lambda \neq \mu$.

Lemma 7.4. *Let $\gamma \in \mathrm{PGL}_2(K)$.*

(i) γ is hyperbolic if and only if γ is conjugate in $\mathrm{PGL}_2(K)$ to an element of the form

$$\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}, \quad 0 < |q| < 1.$$

(ii) γ is elliptic or parabolic if and only if a conjugate of γ^2 lies in $\mathrm{PGL}_2(\mathcal{O}_K)$.

Proof. Omitted. See [1], I.1.4 for details. □

Proposition 7.5. *(i) Suppose $\gamma \in \mathrm{PGL}_2(K)$ is hyperbolic. Then $\langle\gamma\rangle$ is discontinuous.*

(ii) If Γ is a discontinuous group, and $\gamma \in \Gamma$ is elliptic or parabolic, then γ has finite order.

Proof. (i) The group $\langle\gamma\rangle$ has two limit points, corresponding to the eigenvectors of γ. So $\mathcal{L}(\langle\gamma\rangle) \neq \mathbb{P}^1_K$, and hence $\langle\gamma\rangle$ is discontinuous.

(ii) As γ is elliptic or parabolic, it is conjugate in $\mathrm{PGL}_2(K)$ to an element of form

$$\text{(a)} \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, \ |\lambda| = 1, \quad \text{or (b)} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix},$$

where here we write elements of $\mathrm{GL}_2(K)$ representing the corresponding classes in $\mathrm{PGL}_2(K)$. Let $\Gamma' = \langle\gamma\rangle$; then Γ' is discontinuous, and hence discrete. In case (a), the group $\{\lambda^n : n \in \mathbb{Z}\}$ is this a discrete subgroup of the unit group $\mathcal{O}_K^\times$ of $\mathcal{O}_K$, and thus is finite, forcing λ to be a root of unity, proving the claim.

In case (b), we have

$$\langle\gamma\rangle \cong \{n\mu : n \in \mathbb{Z}\},$$

and for a p-adic field this cannot be discrete unless $\mu = 0$. □

We want to investigate the limit points of discontinuous groups. Suppose Γ is discontinuous, with (without loss of generality) $\infty \notin \mathcal{L}$, and $(\gamma_n)_{n=1}^\infty \subset \Gamma$ is an infinite sequence. Write

$$\gamma_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}.$$

Then, by compactness of $\mathbb{P}^1_K$, there is a subsequence such that $a_n/c_n = \gamma_n(\infty)$ tends to some limit, then a subsequence of this such that $b_n/d_n = \gamma_n(0)$ tends to some limit, and yet a further subsequence such that $d_n/c_n = -\gamma_n^{-1}(\infty)$ tends to a limit. From now on, when we refer to (γ_n) we implicitly mean this subsequence.

Since $\infty \notin \mathcal{L}$, we have

$$\lim_{n\to\infty} \begin{pmatrix} \frac{a_n}{c_n} & \frac{b_n}{c_n} \\ 1 & \frac{d_n}{c_n} \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & d \end{pmatrix} \in M_2(K),$$

where the matrices on the left hand side define the same elements (under equivalence in $\mathrm{GL}_2(K)$) as the γ_n in $\mathrm{PGL}_2(K)$.

Now, since Γ is discontinuous, it is discrete; thus the limit does not lie in $\mathrm{GL}_2(K)$, that is it has determinant $ad - b = 0$, forcing $ad = b$. Thus

$$\lim_{n\to\infty} \gamma_n(q) = \frac{aq + b}{q + d} = \frac{a(q + d)}{q + d} = a,$$

unless $q = -d \in \mathcal{L}$ and d_n/c_n is a constant sequence.

Definition 7.6. Let $\alpha \in \mathbb{P}^1_K$. Then define $\mathcal{L}(\alpha) \subseteq \mathcal{L}$ to be the set of limit points β of Γ for which there is an infinite sequence (γ_n) such that

$$\lim_{n\to\infty} \gamma_n(\alpha) = \beta.$$

Lemma 7.7. *(i) If $x \notin \mathcal{L}$, then $\mathcal{L}(x) = \mathcal{L}$.*

(ii) For any three distinct points $A = \{x, y, z\} \subset \mathbb{P}^1_K$, there is some $w \in A$ with $\mathcal{L}(w) = \mathcal{L}$.

Proof. (i) In our discussion above, we showed that $\lim_{n\to\infty} \gamma_n(x)$ is independent of x when $x \neq -d := \lim_{n\to\infty} -\gamma_n^{-1}(\infty)$. But $-d$ is a limit point. So as x is not a limit point, we have $\mathcal{L} = \mathcal{L}(x)$.

(ii) From (i), we need only consider the case where $x, y, z \in \mathcal{L}$. If x and y are distinct, then $\mathcal{L}(x) \cup \mathcal{L}(y) = \mathcal{L}$, since if β is a limit point with corresponding sequence γ_n, either x or y is not equal to $-\lim_{n\to\infty} \gamma_n^{-1}(\infty)$, so $\beta = \lim_{n\to\infty} \gamma_n(x)$ (without loss of generality).

Thus $z \in \mathcal{L}(x) \cup \mathcal{L}(y)$. Without loss of generality $z \in \mathcal{L}(x)$. Continuity gives $\mathcal{L}(z) \subseteq \mathcal{L}(x)$; indeed, if $z = \lim_{n\to\infty} \gamma_n(z)$ for some sequence (γ_n), and $w = \lim_{m\to\infty} \phi_m(z) \in \mathcal{L}(w)$ for some sequence (ϕ_m), we have $w = \lim_{m,n\to\infty} \phi_m\gamma_n(x) \in \mathcal{L}(x)$. Thus

$$\mathcal{L} = [\mathcal{L}(z) \cup \mathcal{L}(x)] \subseteq \mathcal{L}(x) \subseteq \mathcal{L},$$

that is, $\mathcal{L}(x) = \mathcal{L}$, as required. □

Corollary 7.8. *$\mathcal{L}$ is compact. If $|\mathcal{L}| > 2$, then $\mathcal{L}$ is perfect (equal to its set of limit points).*

Proof. If $|\mathcal{L}| \leq 2$, it is clearly compact. Suppose $|\mathcal{L}| > 2$. Pick a limit point $x \in \mathcal{L}$ such that $\mathcal{L} = \mathcal{L}(x)$ using Lemma 7.7 (ii). Note that as $x = \lim_{n\to\infty} \gamma_n(x)$ is a limit point for Γ, we have $\Gamma(x) \subset \mathcal{L}$; indeed, for any $\phi \in \Gamma$, we see that $\phi(x) = \lim_{n\to\infty} \phi\gamma_n(x)$. It is thus easy to see that $\mathcal{L}$ is nothing but the closure $\overline{\Gamma(x)}$. Then

$$\overline{\Gamma(x)} = \mathcal{L}(x) = \mathcal{L},$$

that is, $\mathcal{L}$ is compact and perfect. □

7.2. Schottky Groups

Definition 7.9. A subgroup $\Gamma \leq \mathrm{PGL}_2(K)$ is said to be a *Schottky group* if

(i) it is finitely generated,

(ii) it is discontinuous, and

(iii) every non-trivial element is hyperbolic (which happens if and only if it has no non-trivial elements of finite order).

Proposition 7.10. *Let Γ be a Schottky group with at most 2 limit points. Then $\Gamma = \langle\gamma\rangle$ for some $\gamma \in \Gamma$.*

Proof. Note that there must be exactly 2 limit points (see Lemma 7.5 (i)). Without loss of generality $\mathcal{L} = \{0, \infty\}$. Then every element has form $x \mapsto qx, q \in K^*$. The subgroup $\{q : (x \mapsto qx) \in \Gamma)\}$ is a discrete subgroup of K^* with no elements of finite order, hence is generated by some q_0. This corresponds to some hyperbolic γ with $\Gamma = \langle\gamma\rangle$. □

Remarks: (i) It follows that any Schottky group with 2 limit points is free. Henceforth we focus on the case where there are more than 2 limit points.

(ii) Let X be a compact subset of $\mathbb{P}^1_K$ with $\Gamma(X) = X$. Then note that $\mathcal{L}(\Gamma) \subset X$, since $\mathcal{L}$ is perfect, and for any distinct triple of points in X, we can take one of them, say x, such that $\mathcal{L} = \mathcal{L}(x)$. For any such X we have a tree $\mathcal{T}(X)$.

Proposition 7.11. *Take X as above. Then Γ acts on $\mathcal{T}(X)$ by*

$$\gamma \cdot [(a_0, a_1, a_\infty)] = [\gamma(a_0), \gamma(a_1), \gamma(a_\infty)].$$

Proof. It suffices to show that the natural action of Γ on $X^{(3)}$ respects equivalence and connectedness of points. Note that if $a = (a_0, a_1, a_\infty) \in X^{(3)}$, and $\phi \in \Gamma$, then

$$\gamma_a \cdot \phi^{-1} : \phi(a) \mapsto (0, 1, \infty),$$

that is, $\gamma_a \phi^{-1} = \gamma_{\phi(a)}$. Thus

$$\gamma_{\phi(a)} \gamma_{\phi(b)}^{-1} = \gamma_a \cdot \phi^{-1} \cdot \phi \cdot \gamma_b^{-1} = \gamma_a \gamma_b^{-1},$$

i.e. the action of Γ on $X^{(3)}$ preserves equivalence and connectedness. □

We're now in a position to prove the main result of this section, namely that any Schottky group Γ is free. To do so, we note that Γ acts freely on $\mathcal{T}(X)/\Gamma$; so the result follows immediately from:

Lemma 7.12. *Let Γ be a Schottky group, and let $\mathcal{T}(X)$ be the tree of a compact Γ-invariant $X \subset \mathbb{P}^1_K$. Then $\mathcal{T}(X)/\Gamma$ is finite.*

Proof. First, some notation. If $\mathcal{T}$ is a locally finite tree, and α is a vertex of $\mathcal{T}$, then

$$\mathcal{T} \backslash \{\alpha\} = \mathcal{S}_1 \sqcup \cdots \sqcup \mathcal{S}_m \sqcup \mathcal{T}_1 \sqcup \cdots \sqcup \mathcal{T}_n,$$

a union of disjoint locally finite trees, where each $\mathcal{S}_i$ is finite and each $\mathcal{T}_j$ is infinite. We say that $\mathrm{fin}(\alpha) := \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_m$ is the *finite side* of α, and that α is n-sided (where n is the number of *infinite* components of this disjoint union).

Take any vertex α of $\mathcal{T}(X)$, and take $\Gamma' \subset \Gamma$ a finite generating set (containing inverses and the identity). We pick a finite subtree $\mathcal{U} \subset \mathcal{T}(X)$ to be the minimal tree such that:

(i) For all $\gamma \in \Gamma'$, we have $\gamma(\alpha) \in \mathcal{U}$, and

(ii) If $\beta \in \mathcal{U}$, then $\mathrm{fin}(\beta) \subset \mathcal{U}$.

Then define a subtree $\mathcal{V}$ of $\mathcal{T}(X)$ by

$$\mathcal{V} = \bigcup_{\gamma \in \Gamma} \gamma(\mathcal{U}).$$

Note that since $\mathcal{U}$ contains the finite side of any $\beta \in \mathcal{U}$, the same must be true of any $\beta' \in \mathcal{V}$; indeed, if $\beta' = \gamma(\beta)$, some γ, then $\mathrm{fin}(\beta') = \gamma(\mathrm{fin}(\beta))$.

Claim: $\mathcal{T}(X) = \mathcal{V}$.

Proof of Claim: Take $\beta \in \mathcal{T}(X)$. Then if β is 1-sided, then it is contained in the finite side of some n-sided vertex for some $n \geq 2$. So without loss of generality β is n-sided with $n \geq 2$. Thus there is a halfline starting at α through β; such a halfline corresponds to a limit point z of Γ. Take any $z_0 \in \mathbb{P}^1_K \backslash \mathcal{L}$, and a sequence γ_m such that $\gamma_m(z_0) \to z$ (which is possible by Lemma 7.7 (ii)). Then $\alpha, \gamma_1(\alpha), \gamma_2(\alpha), \ldots$ are all points on the halfline corresponding to z, and lie in $\mathcal{V}$. So as β lies in a path from $\gamma_k(\alpha)$ to $\gamma_{k+1}(\alpha)$, some k, we have $\beta \in \mathcal{V}$.

Thus $\mathcal{T}/\Gamma$ is finite, as $\mathcal{U}$ is, and every point of $\mathcal{T}(X)$ is equivalent under the action of Γ to one in $\mathcal{U}$. □

Theorem 7.13 (Ihara)**.** *Let* Γ *be a Schottky group. Then* Γ *is free.*

Proof. $\mathcal{T}(X)$ is simply connected, and the projection

$$\mathcal{T}(X) \to \mathcal{T}(X)/\Gamma$$

is clearly surjective. Hence $\mathcal{T}(X)$ is the universal cover for $\mathcal{T}(X)/\Gamma$, with group of covering translations Γ. Thus Γ is isomorphic to the fundamental group of the finite graph $\mathcal{T}(X)/\Gamma$. But the Van Kampen Theorem says that this is free on its generators. □

7.3. The Fundamental Domain of a Schottky Group

We now focus our attention on constructing a space Ω on which Γ acts discontinuously, and a workable notion of Ω/Γ. We do so by cutting discs out of $\mathbb{P}^1_{\mathbb{C}_p}$ and identifying the resulting boundaries in a suitable way.

Recall that $\mathbb{C}_p$ is defined to be the completion of the algebraic closure of K. For ease of notation, we write $\mathbb{P} \coloneqq \mathbb{P}^1_{\mathbb{C}_p}$. We fix some notation:

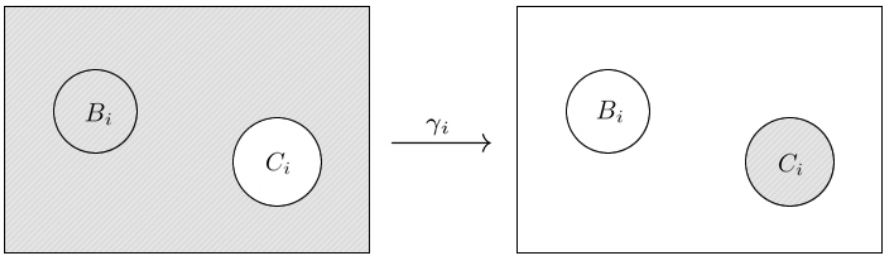
- Let $\overline{B_r(\alpha)} = \{x : |x - \alpha| \leq r\}$, a closed ball, and
- Let $B_r(\alpha) = \{x : |x - \alpha| < r\}$, the corresponding open ball.

Note that $\mathrm{PGL}_2(K)$ takes open (resp. closed) balls to open (resp. closed) balls.

Consider the following construction: Let $\overline{B_1}, ..., \overline{B_g}, \overline{C_1}, ..., \overline{C_g}$ be $2g$ disjoint closed balls in $\mathbb{P}$, with centres in K, and with corresponding open balls $B_1, ...B_g$, $C_1, ..., C_g$. Suppose there exist $\gamma_1, ..., \gamma_g \in \mathrm{PGL}_2(K)$ with

$$\gamma_i(\mathbb{P}\backslash B_i) = \overline{C_i}, \quad \gamma_i(\mathbb{P}\backslash \overline{B_i}) = C_i. \tag{1}$$

Figure 7.1



Let $\Gamma = \langle \gamma_1, ..., \gamma_g \rangle$ be the group generated by the γ_i.

Definition 7.14. Let $F = \mathbb{P}\backslash(\bigcup_{i=1}^{g} B_i \cup \bigcup_{i=1}^{g} C_i)$.

Lemma 7.15. *The group* Γ *is a non-abelian free group on the* γ_i*.*

Proof. We consider, for $\psi \in \Gamma$, the image $\psi(F)$. We can write any such ψ in *reduced form* as

$$\psi = \phi_k \phi_{k-1} \cdots \phi_1,$$

where $\phi_i \in \{\gamma_1, ..., \gamma_g, \gamma_1^{-1}, ..., \gamma_g^{-1}\}$ and there are no γ_i, γ_i^{-1} adjacent to each other.

Claim: We have $\psi(F) \subset \begin{cases} \overline{C_i} & : \phi_k = \gamma_i \\ \overline{B_i} & : \phi_k = \gamma_i^{-1} \end{cases}$

Proof of Claim: We proceed by induction on k. The case $k = 1$ follows from equation (1). Without loss of generality, suppose $\phi_k = \gamma_i$. Then if $\psi' = \phi_{k-1} \cdots \phi_1$, by the induction step we have $\psi'(F) \subset \overline{B_j} \cup \overline{C_j} \subset \mathbb{P}\backslash(\overline{B_i})$ for some $j \neq i$. But $\overline{B_j} \cup \overline{C_j} \subset \mathbb{P}\backslash B_i$; thus

$$\psi(F) = \gamma_i \psi'(F) \subset \gamma_i(\overline{B_j} \cup \overline{C_j}) \subset \gamma_i(\mathbb{P}\backslash B_i) \subset \overline{C_i}.$$

The case $\phi_k = \gamma_i^{-1}$ follows identically since $\gamma_i^{-1}(\mathbb{P}\backslash C_i) = \overline{B_i}$.

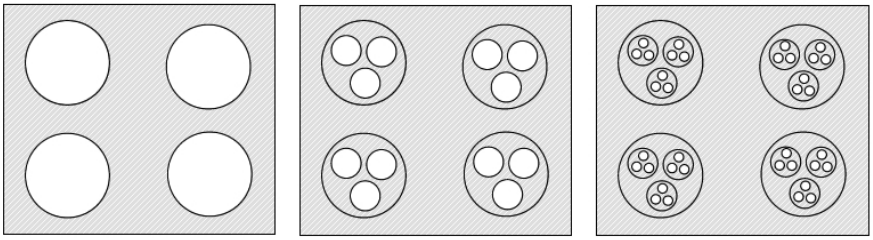
Thus if $\phi_k \cdots \phi_1$ and $\delta_j \cdots \delta_1$ are two reduced forms for $\psi \in \Gamma$, we must have $\phi_k = \delta_j$ as they both map F into the same closed ball. Continuing, we find $\phi_{k-1} = \delta_{j-1}$, etc. until $j = k$ and the forms are the same. The lemma follows. □

Definition 7.16. For $\psi = \phi_k \cdots \phi_1$ in reduced form, we say $\ell(\psi) = k$ is the *length* of ψ. We set $\ell(\mathrm{id}) = 0$ by convention.

Definition 7.17. Define $\Omega_n = \bigcup_{\ell(\psi) \leq n} \psi(F)$, and then set $\Omega = \bigcup_{n \geq 0} \Omega_n$.

Note that for $\psi \in \Gamma$, the intersection $F \cap \psi(F) = \varnothing$ unless $\psi \in \{\mathrm{id}, \gamma_1, ...\gamma_g, \gamma_1^{-1}, ..., \gamma_g^{-1}\}$. This relation means that for ψ and ψ' in Γ, after translates, $\psi(F) \cap \psi'(F) = \varnothing$ unless $\ell(\psi)$ and $\ell(\psi')$ differ by at most 1. We see the following:

Figure 7.2



$F = \Omega_0$ Ω_1 Ω_2

Define, for $\psi = \phi_k \cdots \phi_1 \in \Gamma$,

$$B_\psi = \begin{cases} \psi(\mathbb{P}\backslash\overline{B_i}) & : \phi_1 = \gamma_i \\ \psi(\mathbb{P}\backslash\overline{C_i}) & : \phi_1 = \gamma_i^{-1} \end{cases}.$$

Then the above discussion gives:

Proposition 7.18. *We have*

$$\mathbb{P}\backslash\Omega_{n-1} = \bigcup_{\ell(\psi)=n} B_\psi, \quad n \geq 1.$$

Lemma 7.19. *We have $B_\psi \subset B_{\psi'}$ if and only if $\psi = \psi'\delta$, where $\ell(\psi) = \ell(\psi') + \ell(\delta)$.*

Proof. For the converse direction, we see $B_\psi = \psi'(\delta(\mathbb{P}\backslash\overline{B_i}))$ for some i, and $B_{\psi'} = \psi'(\mathbb{P}\backslash\overline{B_j})$ for some j. But by inspection, as $\psi = \psi'\delta$,

$$\delta(\mathbb{P}\backslash\overline{B_i}) \subset \mathbb{P}\backslash\overline{B_j},$$

hence the result.

For the forwards direction, if $B_\psi \subset B_{\psi'}$, then they both lie in the same B_i or C_i. Write

$$\psi = \phi_k \cdots \phi_1, \quad \psi' = \phi'_j \cdots \phi'_1.$$

Then $\phi_k = \phi'_j$. Continuing in the same way, we obtain the result. □

Theorem 7.20. *The set $\mathcal{L}(\Gamma)$ of limit points of Γ is equal to $\mathbb{P}\backslash\Omega$.*

Proof. First we note that $\mathcal{L} = \mathcal{L}(\Gamma) \subset \mathbb{P}\backslash\Omega$. Indeed, if $\alpha \in \mathcal{L} \cap \Omega$, then we can (after a translation by a suitable element of Γ) assume without loss of generality that $\alpha \in \mathcal{L} \cap F$. Now F contains at least three distinct points of $\mathbb{P}^1_K$, hence by Lemma 7.7 (ii), there exists $x \in F$ with $\mathcal{L} = \mathcal{L}(x)$. Then take an infinite sequence

$$(\phi_n) \subset \Gamma, \quad \phi_n(x) \to \alpha.$$

But we noted above that there are only finitely many elements $\psi \in \Gamma$ with

$$\psi(F) \cap F \neq \phi.$$

It follows that there are only finitely many elements $\psi \in \Gamma$ with

$$\psi(F) \cap \Omega_1 \neq \phi.$$

Thus $\phi_n(x) \notin \Omega_1$ for all but finitely many n, that is, $\alpha \notin F$, which is contradiction. (Here we pass to Ω_1 as F is closed, but there is an open set strictly between F and Ω_1.)

To show the converse, we use Proposition 7.18. Write r_ψ for the radius of B_ψ. We want to show that

$$\lim_{\ell(\psi)\to\infty} r_\psi = 0$$

uniformly. If this holds, then every point of $\mathbb{P}\backslash\Omega$ lies in an infinite sequence of nested open balls of radius tending to 0, i.e. it is a limit point.

Note that if $B_\psi \subsetneq B_{\psi'}$, we can write

$$\psi = \phi_k \cdots \phi_1 \delta, \quad \psi' = \phi_k \cdots \phi_1, \quad \text{with } \ell(\delta) \geq 1.$$

Thus

$$B_\psi = \phi_k \cdots \phi_2(B_{\phi_1\delta}), \quad B_{\psi'} = \phi_k \cdots \phi_2(B_{\phi_1}).$$

It follows that $r_\psi / r_{\psi'} = r_{\phi_1\delta}/r_{\phi_1} < 1$. Let

$$\rho = \max_{\phi,\delta} \frac{r_{\phi\delta}}{r_\phi},$$

where $\phi \in \{\gamma_1, ..., \gamma_g, \gamma_1^{-1}, ..., \gamma_g^{-1}\}$ and $\mathrm{id} \neq \delta \in \Gamma$. Note that at this maximum, $\ell(\delta) = 1$, so $\rho < 1$ (as there are only finitely many δ with $\ell(\delta) = 1$). Induction then gives

$$r_\psi \leq \rho^{\ell(\psi)} R,$$

for some constant R; that is, $r_\psi \to 0$ uniformly as $\ell(\psi) \to \infty$. Thus $\mathbb{P}\backslash\Omega \subset \mathcal{L}$ and we are done. □

Corollary 7.21. *The group $\Gamma = \langle \gamma_1, ..., \gamma_g \rangle$ is a Schottky group.*

Proof. Γ is obviously finitely generated. It is free on the generators, so it has no elements of finite order. It is discontinuous by Theorem 7.20 since the set of limit points is $\mathbb{P}\backslash\Omega$, and $\Omega \neq \mathbb{P}$. □

We state the following important theorem. For a proof, see [1], I.4.3.

Theorem 7.22. *Every Schottky group occurs in this way. That is, if* Γ *is a Schottky group, there exist open balls* $B_1, ..., B_g, C_1, ..., C_g$ *and a set of generators* $\gamma_1, ..., \gamma_g$ *for* Γ *such that*

$$\gamma_i(\mathbb{P}\backslash B_i) = \overline{C_i}, \quad \gamma_i(\mathbb{P}\backslash\overline{B_i}) = C_i.$$

Definition 7.23. Let Γ be a Schottky group, and take B_i, C_i as above. The set

$$F = \mathbb{P}\backslash\left(\bigcup_{i=1}^{g} B_i \cup \bigcup_{i=1}^{g} C_i\right)$$

is called a *good fundamental domain* for Γ.

8. Automorphic Forms

We've constructed, for a Schottky group Γ, a space Ω on which Γ acts discontinuously. We want to look at the quotient space Ω/Γ. To do so, we look at automorphic forms on Ω, returning to p-adic analysis. For points $a, b \in \Omega$, we construct an automorphic form $\theta(a, b; z)$ using Γ, and then prove that any automorphic form with constant factors of automorphy is a finite product of these functions up to a constant factor.

The ultimate goal is, as in part II, to show that the field of $\Gamma-$invariant automorphic forms is a function field of one variable, obtaining the result that Ω/Γ is an algebraic curve. This will be covered in chapter 9.

Before we begin, we prove a simple lemma that will be used constantly throughout this section:

Lemma 8.1. *Let $D = B_r(x) \subset \mathbb{C}_p$ be an open disc, $a, b \in D$. For all $z \in \mathbb{C}_p \backslash D$, we have*

$$\frac{|z-a|}{|z-b|} = 1.$$

Proof. We have $|a-b| < r$ and $|z-a| \geq r$ as by the non-archimedean property, a and b are both centres of D. Hence

$$\frac{|z-a|}{|z-b|} = \frac{|z-a|}{|(z-a)+(a-b)|} = \frac{|z-a|}{|z-a|} = 1. \qquad \square$$

8.1. A Return to p-adic Analysis

Definition 8.2. An *affinoid disc* is a closed disc in $\mathbb{C}_p$ containing ∞, i.e. of form $\mathbb{C}_p \backslash D$, where $D \subset \mathbb{C}_p$ is an open disc. An *affinoid domain* is a finite intersection of affinoid discs.

Remark: The domain F as constructed in chapter 7 is an affinoid domain, as is Ω_n for all n. Recall that we defined$\Omega = \bigcup_{n \geq 0} \Omega_n$.

Definition 8.3. (i) A function on an affinoid domain X is said to be *holomorphic* if it is the uniform limit of rational functions with no pole in X.

(ii) A function on Ω is *holomorphic* if its restriction to Ω_n is holomorphic for each n.

(iii) A function on Ω is *meromorphic* if it is the quotient of two holomorphic functions g/h, with $h \neq 0$.

Definition 8.4. Define the *norm of absolute convergence* $||f||_{\Omega_n} := \sup_{z \in \Omega_n} |f(z)|$.

We quote some important results for holomorphic functions, similar to the complex case:

Proposition 8.5. *Let f be a non-zero holomorphic function on Ω. Then f has a finite number of zeros in F.*

Proposition 8.6. *If f is a holomorphic function that is bounded on Ω, then it is constant.*

Definition 8.7. A meromorphic function f on Ω is said to be an *automorphic form with constant factors of automorphy* if

$$f(z) = \zeta(\phi) f(\phi(z)), \quad \zeta(\phi) \in \mathbb{C}_p^*, \forall \phi \in \Gamma.$$

We're now in a position to associate a class of automorphic functions to a Schottky group Γ. This study is based on the following observation:

Proposition 8.8. *Let $a, b \in \Omega$. Pick $\epsilon > 0$. Then for all but finitely many $\gamma \in \Gamma$,*

$$|\gamma(a) - \gamma(b)| < \epsilon.$$

Proof. In Proposition 7.18, and the proof of Theorem 7.20, we showed that $\mathbb{P}\backslash\Omega_n$ is the disjoint union of a finite number of open balls, whose radius tends to 0 uniformly as $n \to \infty$. So take $N \in \mathbb{N}$ such that, for all $n \geq N$, $\mathbb{P}\backslash\Omega_n$ is a disjoint union of open balls of radius strictly less than ϵ.

In the discussion before Proposition 7.18, we showed that $F \cap \gamma(F) = \phi$ unless $\ell(\gamma) = 1$. A similar argument shows that $\Omega_n \cap \gamma(\Omega_n) = \varnothing$ if $\ell(\gamma) > 2n$. So for $\ell(\gamma) > N$, as $\gamma(\Omega)$ must lie in a single one of these disjoint balls, $\gamma(a)$ and $\gamma(b)$ both lie in the same open ball in $\mathbb{P}\backslash\Omega_n$ of radius less than ϵ. The non-archimedean property means we can take the centre of this ball to be at $\gamma(a)$; hence the result. □

Define, as rational functions,

$$\frac{z-a}{z-\infty} = z - a, \quad \frac{z-\infty}{z-b} = \frac{1}{z-b}, \quad \frac{z-\infty}{z-\infty} = 1.$$

Lemma 8.9. *Let $(a_i), (b_i)$ be sequences in Ω with*

(i) $|a_i - b_i| \longrightarrow 0$ as $i \to \infty$;

(ii) for any n, only finitely many $a_i, b_i \in \Omega_n$.

Then

$$f(z) = \prod_{i=1}^{\infty} \frac{z-a_i}{z-b_i}$$

is a meromorphic function on Ω with zeros only at $\{a_i\}$ and poles only at $\{b_i\}$.

Proof. We must show that f is meromorphic on Ω_n for all n. Fix n, and pick N such that $a_i, b_i \notin \Omega_n$ for all $i \geq N$ (possible by (ii)). Set ϵ to be the *minimum* radius of the open balls that make up $\mathbb{P}\backslash\Omega_n$. Define partial products

$$f_k = \prod_{i=N}^{k} \frac{z-a_i}{z-b_i};$$

f_k is clearly a rational function. Furthermore,

$$|f_{k+1}(z) - f_k(z)| = \left|\frac{z-a_{k+1}}{z-b_{k+1}} - 1\right| |f_k(z)| = \left|\frac{b_{k+1}-a_{k+1}}{z-b_{k+1}}\right| |f_k(z)|.$$

If $z \in \Omega_n$, then z does not lie in the open ball $B_\epsilon(b_{k+1})$, i.e. $|z - b_{k+1}| \geq \epsilon$. So this is less than or equal to $\frac{1}{\epsilon}|b_{k+1} - a_{k+1}| \cdot ||f_k||_{\Omega_n}$.

> *Claim:* $||f_k||_{\Omega_n}$ is bounded as $k \to \infty$.
>
> *Proof of Claim:* It suffices to show that $|(z-a_i)/(z-b_i)| = 1$ for sufficiently large i. Then take M such that $|a_i - b_i| < \epsilon$ for all $i \geq M$, so that a_i and b_i lie in the same open ball. The result follows from Lemma 8.1.

So $||f_{k+1} - f_k||_{\Omega_n} \leq C|b_{k+1} - a_{k+1}|$ for some constant C. Thus

$$f_i = f_N + \sum_{k=N}^{i-1} (f_{k+1} - f_k)$$

is a convergent series, i.e. f_i tends to a holomorphic function g on Ω_n as i tends to ∞. Then

$$f = \prod_{i=1}^{N-1} \frac{z - a_i}{z - b_i} \cdot g$$

is meromorphic on Ω_n, as required. Note convergence is independent of n.

It remains to show that the zeros/poles occur only at a_i or b_i. If there was a pole $c \in \Omega$, then $c \in \Omega_n$ for some n. But $f|_{\Omega_n}$ clearly cannot have a pole at c since the poles occur at $b_1, ..., b_{N-1}$, with N chosen as above. So f has poles only at the $\{b_i\}$; then considering $1/f$, we can show that there are no zeros outside the $\{a_i\}$. □

Theorem 8.10. *Let $a, b \in \Omega$. Then*

$$\theta(a, b; z) := \prod_{\gamma \in \Gamma} \frac{z - \gamma(a)}{z - \gamma(b)}$$

is an automorphic form with constant factors of automorphy.

Proof. Proposition 8.8 shows that θ is meromorphic on Ω, since condition (i) is satisfied by Lemma 8.9, and (ii) by the definition of Γ_n. It remains to show that $\theta(a, b; z) = \zeta(\phi)\theta(a, b; \phi(z))$, for some constant $\zeta(\phi)$. Fix $\phi \in \Gamma$.

Note that

$$\frac{\phi(z) - \gamma(a)}{\phi(z) - \gamma(b)} = c(\gamma) \frac{z - \phi^{-1}(\gamma(a))}{z - \phi^{-1}(\gamma(b))}$$

for some constant $c(\gamma)$, since each side is a rational function with the same zeros and poles (i.e. they differ only by a constant). If $\phi(\infty) \neq \gamma(a), \gamma(b)$, then evaluating at ∞ gives

$$c(\gamma) = \frac{\phi(\infty) - \gamma(a)}{\phi(\infty) - \gamma(b)} \in \mathbb{C}_p^*.$$

Now note that there are at most two elements $\gamma \in \Gamma$ with $\phi(\infty) = \gamma(a)$ or $\gamma(b)$. Indeed, if there were more, then without loss of generality $\gamma(a) = \gamma'(a) = \phi(\infty)$, which implies that $(\gamma')^{-1}\gamma$ fixes a. But only the identity has fixed points in Ω. Write

$$\tilde{\Gamma} = \{\gamma \in \Gamma : \phi(\infty) = \gamma(a) \text{ or } \gamma(b)\}, \quad |\tilde{\Gamma}| \leq 2.$$

So

$$\theta(a, b; \phi(z)) = \prod_{\tilde{\gamma} \in \tilde{\Gamma}} \frac{\phi(z) - \tilde{\gamma}(a)}{\phi(z) - \tilde{\gamma}(b)} \prod_{\gamma \in \Gamma \setminus \tilde{\Gamma}} \frac{\phi(z) - \gamma(a)}{\phi(z) - \gamma(b)}$$

$$= \left(\prod_{\tilde{\gamma} \in \tilde{\Gamma}} c(\tilde{\gamma}) \prod_{\gamma \in \Gamma \setminus \tilde{\Gamma}} \frac{\phi(\infty) - \gamma(a)}{\phi(\infty) - \gamma(b)} \right) \prod_{\gamma \in \Gamma} \frac{z - \phi^{-1}(\gamma(a))}{z - \phi^{-1}(\gamma(b))}$$

$$= \zeta(\phi)^{-1}\theta(a, b; z), \quad \zeta(\phi) \in \mathbb{C}_p^*,$$

where we note that the infinite product gives a well-defined element of $\mathbb{C}_p^*$ since it is the evaluation of the function

$$\theta(a, b; \phi(z)) \prod_{\tilde{\gamma} \in \tilde{\Gamma}} \frac{\phi(z) - \tilde{\gamma}(a)}{\phi(z) - \tilde{\gamma}(b)}$$

at ∞ (and this function is clearly holomorphic and non-zero at ∞). □

Before moving onto a structure theorem for automorphic forms, we give some basic properties of θ.

Proposition 8.11. *(i) For $\phi \in \Gamma$, $\theta(a, \phi(a); z)$ has no zeros or poles.*

(ii) For any $a, b \in \Omega$, we have $\theta(a, \phi(a); z) = \theta(b, \phi(b); z)$.

Proof. (i) It suffices to show that a is not a zero or a pole; then the result follows by the automorphy property. But

$$\theta(a, \phi(a); z) = \frac{z-a}{z-\phi(a)} \cdot \frac{z-\phi^{-1}(a)}{z-\phi^{-1}\phi(a)} \prod_{\gamma \neq \mathrm{id}, \phi^{-1}} \frac{z-\gamma(a)}{z-\gamma(\phi(a))}$$

$$= \frac{z-\phi^{-1}(a)}{z-\phi(a)} \prod_{\gamma \neq \mathrm{id}, \phi^{-1}} \frac{z-\gamma(a)}{z-\gamma(\phi(a))}.$$

Thus there is no zero or pole at a. For (ii),

$$\frac{\theta(a, \phi(a); z)}{\theta(b, \phi(b); z)} = \prod_{\gamma \in \Gamma} \frac{z-\gamma(a)}{z-\gamma(\phi(a))} \frac{z-\gamma(\phi(b))}{z-\gamma(b)}$$

$$= \prod_{\gamma \in \Gamma} \frac{z-\gamma(a)}{z-\gamma(b)} \prod_{\gamma' \in \Gamma} \frac{z-\gamma'(b)}{z-\gamma'(a)} = \frac{\theta(a, b; z)}{\theta(a, b; z)} = 1. \qquad \square$$

Definition 8.12. Define $u_\phi(z) := \theta(a, \phi(a); z)$ for some choice of $a \in \Omega$. We also write $u_i(z) := u_{\gamma_i}(z)$.

Proposition 8.13. *We have $\zeta(\phi) = \zeta(a, b; \phi) = u_\phi(a)/u_\phi(b)$.*

Proof. Rearranging the identity $\zeta(a, b; \phi) = \theta(a, b; z)/\theta(a, b; \phi(z))$ gives the result. $\square$

8.2. A Structure Theorem for Automorphic Forms

We will prove in this section that any automorphic form with constant factors of automorphy is in fact a finite product of $\theta(a, b; z)$ for suitable a, b. First, we enlarge F.

If Γ is a Schottky group with good fundamental domain F and associated generators $\gamma_1, ..., \gamma_g$, then each γ_i has two fixed points. One of these lies in B_i, the other in C_i; call them b_i, c_i. Then as $|\cdot|$ is non-archimedean, we can take these as centres, i.e. for suitable r_i, s_i we have

$$B_i = B_{r_i}(b_i), \quad C_i = B_{s_i}(c_i).$$

Put $w(z) = (z-b_i)/(z-c_i)$; then, for $\phi \in \Gamma$,

$$w(\gamma_i(z)) = q_i w(z),$$

since $w(\gamma_i(z))$ and $w(z)$ have the same zeros and poles. Write $\partial B_i = \overline{B_i} \backslash B_i$, and similarly for ∂C_i. Then γ_i maps ∂B_i to ∂C_i. So if $x \in \partial B_i$, taking valuations,

$$|w(\gamma_i(z))| = \frac{|\gamma_i(x) - b_i|}{|\gamma_i(x) - c_i|} = \frac{|c_i - b_i|}{s_i}$$

$$= |q_i||w(x)| = |q_i| \frac{|x-b_i|}{|x-c_i|} = \frac{|q_i| \cdot r_i}{|c_i - b_i|}.$$

Thus $|q_i| = |b_i - c_i|^2 / r_i s_i > 1$.

Lemma 8.14. *There exists δ, satisfying $1 < \delta < |b_i - c_i|/r_i$, such that the $2g$ annuli*

$$R_i = \{z : \frac{r_i}{\delta} \leq |z - b_i| \leq r_i\delta\}, \quad S_i = \{z : \frac{s_i}{\delta} \leq |z - c_i| \leq s_i\delta\}$$

are disjoint for $i = 1, ..., g$, and $\gamma_i(R_i) = S_i$.

Proof. It's clear that we can take the R_i, S_i disjoint with a small enough δ. Take $1 < \delta < \frac{|b_i - c_i|}{r_i}$, and then x such that $|x - b_i| = r_i\delta$. Now

$$|w(\gamma_i(x))| = \frac{|\gamma_i(x) - b_i|}{|\gamma_i(x) - c_i|} = |q_i|\frac{|x - b_i|}{|x - c_i|},$$

so $(|c_i - b_i|)/(|\gamma_i(x) - c_i|) = r_i\delta|q_i|/(|b_i - c_i|)$, i.e. $|\gamma_i(x) - c_i| = s_i/\delta$. The result follows as the circles are mapped to the right place inside the annulus. □

This construction leads to the concept of the order of a holomorphic function at B_i. Let f be holomorphic on Ω, with no zero on R_i. We can write f as a convergent Laurent series

$$f(z) = \sum_{n \in \mathbb{Z}} a_n(z - b_i)^n.$$

As there are no zeros in R_i, by Remark 3.3, there exists an n such that on R_i,

$$|f(z)| = |a_n||z - b_i|^n.$$

Write $n = \text{ord}_{B_i} f$. We also, for convenience, use the notation $B_{i+g} = C_i$ in the next two results to simplify cases.

Lemma 8.15. *Let $\tilde{F} = F \cup \bigcup_{i=1}^{g} R_i \cup \bigcup_{i=1}^{g} S_i$, and let f be holomorphic on $\tilde{F}$ with no zeros in $\bigcup_{i=1}^{g} R_i \cup \bigcup_{i=1}^{g} S_i$. Then (the number of zeros of f) $= -\sum_{i=1}^{2g} \text{ord}_{B_i} f$.*

Proof. Note any rational function on $\mathbb{P}$ can be written as a finite product $\prod \frac{z - a_i}{z - b_i}$, where the number of zeros and poles are the same, as $z - a = (z - a)/(z - \infty)$ and $1/(z - b) = (z - \infty)/(z - b)$. We prove the result for $f = (z - a)/(z - b)$. Note $b \notin \tilde{F}$, so without loss of generality $b \in B_1$, and $a \in \mathbb{P}$. There are three cases:

(i) $a \in B_1$. Then $\text{ord}_{B_i} = 0$ for all i, since a, b are in the same open ball (Lemma 8.1).

(ii) $a \in B_j, j \neq 1$. Then $\text{ord}_{B_1} f = -1$, and $\text{ord}_{B_j} f = 1$, with $\text{ord}_{B_i} f = 0, i \neq 1, j$ (using a simple variant of Lemma 8.1).

(iii) $a \in F$. Then $\text{ord}_{B_1} f = -1$, and $\text{ord}_{B_j} f = 0$ for $j > 1$.

Thus the result is true for functions of this form. Now note that $\text{ord}_{B_i} fg = \text{ord}_{B_i} f + \text{ord}_{B_i} g$, from which the result follows for rational functions.

The general case follows: if f is holomorphic, write $f = gh$, where g is holomorphic with no zeros and h rational (which is possible since there are a finite number of zeros in $\tilde{F}$). It suffices to prove that $\text{ord}_{B_i} g = 0$ for all i. But g is bounded below (as $\tilde{F}$ is compact) by ϵ, say. As g is holomorphic, it is a uniform limit of rational functions with no pole in $\tilde{F}$, so take some $\tilde{g}$ rational with $||g - \tilde{g}||_{\tilde{F}} < \epsilon$. Then

$$|\tilde{g}(z)| = |(\tilde{g}(z) - g(z)) + g(z)| = |g(z)|.$$

But $\tilde{g}(z)$ has no zeros, so the result follows from our work above. □

Corollary 8.16. *Let f be holomorphic on $\tilde{F}$, with $ord_{B_i} f = 0$ for all i. Then $|f|$ is constant.*

Proof. As above, since by assumption f has no zeros in $\tilde{F}$, we can approximate f by a rational function $\tilde{f}$, with $|f(z)| = |\tilde{f}|$. Write

$$\tilde{f}(z) = \frac{(z-a_1)\cdots(z-a_k)}{(z-b_1)\cdots(z-b_k)},$$

with k minimal. Then if, without loss of generality, $a_1, b_1 \in B_1$, then

$$|\tilde{f}(z)| = C\left|\frac{(z-a_2)\cdots(z-a_k)}{(z-b_2)\cdots(z-b_k)}\right|$$

with C some constant by Lemma 8.1. Thus we could have taken $k-1$. Thus no a_i, b_i lie in the same ball. But then if $k \geq 1$, say $b_1 \in B_1$; then $\mathrm{ord}_{B_1}\tilde{f} \leq -1$, contradiction. So $k = 0$ and f is constant. □

Proposition 8.17. *Let f be an automorphic form on Ω with constant factors of automorphy. Then f has no zeros in $\tilde{F}$ if and only if f has no poles in $\tilde{F}$.*

Proof. It suffices to show that if f has no poles in $\tilde{F}$, then f has no zeros in $\tilde{F}$. Given this, the converse follows by considering $1/f$. We split into two cases.

(i) There are no zeros on $\bigcup_{i=1}^{g} R_i \cup \bigcup_{i=1}^{g} S_i$. Then:

Claim: $\mathrm{ord}_{C_i} f(z) = -\mathrm{ord}_{B_i} f(\gamma_i(z))$.

Proof of Claim: If $|f|$ is constant on S_i, then $|f \cdot \gamma_i|$ is constant on B_i. Also, if

$$g(z) = \frac{z-b_i}{z-c_i},$$

then $\mathrm{ord}_{C_i} g = -1$, $\mathrm{ord}_{B_i} g \cdot \gamma_i = 1$. The general case follows: we can approximate any such automorphic form by $|f| = |g|^k|h|$, $\mathrm{ord}_{B_i} h = 0$, by similar methods to above.

Thus $\mathrm{ord}_{B_i} f + \mathrm{ord}_{C_i} f = 0$, so there are no zeros in $\tilde{F}$ by Lemma 8.15.

(ii) There are a finite number of zeros in $\bigcup_{i=1}^{g} R_i \cup \bigcup_{i=1}^{g} S_i$, say $a_1, ..., a_k$. Then pick

$$b \in F \backslash (\bigcup_{i=1}^{g} R_i \cup \bigcup_{i=1}^{g} S_i).$$

Now

$$\tilde{f} = f \cdot \theta(b, a_1; z) \cdots \theta(b, a_k; z)$$

is holomorphic on $\tilde{F}$, hence on Ω (automorphic), with no zeros in $\bigcup_{i=1}^{g} R_i \cup \bigcup_{i=1}^{g} S_i$. So by (i), $\tilde{f}$ has no zeros in $\tilde{F}$. But it has a zero at b, contradiction. So case (ii) can't happen. □

We're finally in a position to prove the structure theorem for automorphic forms.

Theorem 8.18 (Structure theorem for automorphic forms)**.** *Let f be an automorphic form on Ω with constant factors of automorphy. Then we can write*

$$f = C\theta(a_1, b_1; z) \cdots \theta(a_k, b_k; z), \quad a_i, b_i \in \Omega, \ \ C \in \mathbb{C}_p \text{ constant.}$$

Proof. We have finite sets $\{a_1, ..., a_m\}$ of zeros and $\{b_1, ..., b_n\}$ of poles of f in F. Then without loss of generality $m \leq n$, and we can write

$$f = \tilde{f} \cdot \theta(a_1, b_1; z) \cdots \theta(a_m, b_m; z),$$

$\tilde{f}$ with no zeros in F (hence Ω). But then by Proposition 8.17, $\tilde{f}$ also has no poles in F.

Recall $u_i(z) = u_{\gamma_i}(z)$. Proposition 8.11 (i) shows that u_i has no zeros or poles in Ω. In the proof, we showed that

$$u_i(z) = \frac{z - \gamma_i^{-1}(a)}{z - \gamma_i(a)} \prod_{\phi \neq \mathrm{id}, \gamma_i^{-1}} \frac{z - \phi(a)}{z - \phi(\gamma_i(a))}.$$

Now $\phi(a), \phi\gamma_i(a)$ lie in the same B_i, so $|\frac{z-\phi(a)}{z-\phi(\gamma_i(a))}| = 1$ for all $\phi \in \Gamma \backslash \{\mathrm{id}, \gamma_i^{-1}\}$ by Lemma 8.1. It follows that

$$\mathrm{ord}_{B_j} u_i = \begin{cases} 1 & : i = j \\ 0 & : i \neq j \end{cases}, \quad \mathrm{ord}_{C_j} u_i = \begin{cases} -1 & : i = j \\ 0 & : i \neq j \end{cases}.$$

Set $n_j = \mathrm{ord}_{B_i} \tilde{f}$. Then if $g = u_1^{n_1} \cdots u_g^{n_g}$, then $\mathrm{ord}_{B_i} \tilde{f}/g = 0$ for all i, so Corollary 8.16 implies that $|\tilde{f}/g|$ is constant on F, thus is constant (and hence bounded) on Ω, i.e. $\tilde{f}/g$ is constant on Ω.

Thus

$$f = C u_1^{n_1} \cdots u_g^{n_g} \theta(a_1, b_1; z) \cdots \theta(a_m, b_m; z)$$

as required. □

9. The Curve Ω/Γ

To complete our work, we will use the theory developed so far to prove that Ω/Γ is a smooth irreducible algebraic curve. Our approach will be similar to Chapter 3, in that we consider the field of Γ-invariant functions, $\mathbb{C}_p(\Omega/\Gamma)$, proving that it has transcendence degree 1 over $\mathbb{C}_p$. Analogously to before, Ω/Γ is the set of places of $\mathbb{C}_p(\Omega/\Gamma)$, and hence Ω/Γ is isomorphic to a smooth irreducible algebraic curve. We also state another version of Riemann-Roch that says that this curve has genus g, hence showing that this does indeed generalise Tate's work.

In this chapter, we will require some results from analytic geometry; there is not space here to develop the theory in all but the briefest detail, but there are large parallels with *algebraic* geometry. Indeed, an *analytic set* is locally the zero set of a finite number of holomorphic functions on $\mathbb{C}_p^n$. A point P of an analytic set V is *regular* if V is locally an analytic manifold at P, in which case we define the *dimension at* P to be the dimension of this manifold. We say the *dimension of* V is the maximum of the dimensions of the regular points. An *analytic function* on V is a map $\psi : V \subset \mathbb{C}_p^n \to \mathbb{C}_p$ that is a product of holomorphic functions on each component, and an *analytic map* $\phi : V \to V'$ is a map that respects analytic functions on V.

The only result we really require from this is that for an analytic map $\phi : V \to V'$, with $\dim(V) > \dim(V')$, the non-empty fibres are not discrete (as they have dimension ≥ 1).

9.1. The Field of Γ-invariant Meromorphic Functions

The major step in what follows is proving the existence of *one* non-constant Γ-invariant meromorphic function h. Once we've done this, we show that $\mathbb{C}_p(\Omega/\Gamma)/\mathbb{C}_p(h)$ is an algebraic extension using linear algebra.

Let $\Gamma = \langle \gamma_1, ..., \gamma_g \rangle$ be a Schottky group. Recall that $u_i(z) = u_{\gamma_i}(z)$ (Definition 8.12). Define, for $r > g$,

$$\phi_r : \Omega^r \longrightarrow \Omega^g,$$

$$(z_1, ..., z_r) \mapsto (u_1(z_1) \cdots u_1(z_r), ..., u_g(z_1) \cdots u_g(z_r)).$$

This is an analytic map, and since $r > g$, the fibres are non-discrete. Thus, for $(z_1, ..., z_r) \in \Omega^r$, there is some $(w_1, ..., w_r) \in \Omega^r$ with

(i) $w_1 \notin \bigcup_{j=1}^{r} \Gamma(z_j)$, and

(ii) $\phi_r(z_1, ..., z_r) = \phi_r(w_1, ..., w_r)$.

Note by (i) that the w_i are not just a re-arrangement of the z_i. Condition (ii) says that

$$u_1(z_1) \cdots u_1(z_r) = u_1(w_1) \cdots u_1(w_r), \quad \dots,$$

$$u_g(z_1) \cdots u_g(z_r) = u_g(w_1) \cdots u_g(w_r).$$

Now consider

$$f(z) = \theta(z_1, \infty; z) \cdots \theta(z_r, \infty; z),$$

$$g(z) = \theta(w_1, \infty; z) \cdots \theta(w_r, \infty; z).$$

By Proposition 8.13,

$$f(z) = \prod_{j=1}^{r} \frac{u_i(z_j)}{u_i(\infty)} f(\gamma_i(z)),$$

$$g(z) = \prod_{j=1}^{r} \frac{u_i(w_j)}{u_i(\infty)} g(\gamma_i(z)).$$

Thus f, g are automorphic forms with the *same* constant of automorphy. In particular, $h := f/g$ is invariant under the action of Γ. But h is non-constant; indeed, because of condition (i) above, it has a pole at w_1.

Theorem 9.1. *The field $\mathbb{C}_p(\Omega/\Gamma)$ is a function field of one variable over $\mathbb{C}_p$.*

Proof. It suffices to prove that $\mathbb{C}_p(\Omega/\Gamma)/\mathbb{C}_p(h)$ is an algebraic extension, as then

$$\mathrm{trdeg}_{\mathbb{C}_p} \mathbb{C}_p(\Omega/\Gamma) = 1.$$

The structure theorem for automorphic forms implies that h has the same number of zeros as poles in Ω/Γ; call this n. Then we claim that any $n+1$ functions

$$f_1, ..., f_{n+1} \in \mathbb{C}_p(\Omega/\Gamma)$$

are linearly dependent over $\mathbb{C}_p(h)$. For each i, write m_i for the number of poles of f_i in Ω/Γ, and put

$$m = \sum_{i=1}^{n+1} m_i.$$

Let

$$\alpha_k = c_{km} h^m + \cdots + c_{k1} h + c_{k0}, \quad 1 \leq k \leq n+1,$$

a collection of $n+1$ polynomials in h, with the c_{ij} indeterminates. Then consider

$$g = \alpha_1 f_1 + \cdots + \alpha_{n+1} f_{n+1}.$$

Now g has poles only at poles of h or f_i; thus there at *most* $mn + m = m(n+1)$ poles of g. Now choose $(m+1)(n+1) - 1$ distinct points $z_1, ..., z_{(m+1)(n+1)-1} \in \Omega/\Gamma$; then we have $(m+1)(n+1) - 1$ linear equations

$$g(z_i) = 0$$

in $(m+1)(n+1)$ unknowns $c_{ij}, 1 \leq i \leq n+1, 0 \leq j \leq m$. Thus there is a solution. But for such a solution, g has at most $m(n+1)$ poles, but at least $(m+1)(n+1) - 1$ zeros; and as $n \geq 1$ (by construction of h), the number of zeros is greater than the number of poles. But this can only happen - by the structure theorem - if $g \equiv 0$, that is, if we have exhibited a linear dependence between the f_i over $\mathbb{C}_p(h)$, as required. □

Hence we obtain a smooth irreducible algebraic curve, V, with $\mathbb{C}_p(\Omega/\Gamma) = \mathbb{C}(V)$ the function field of V.

Before completing the proof that Ω/Γ is an algebraic curve, we note some analogues to the genus 1 case. We can, for $f \in \mathbb{C}_p(\Omega/\Gamma)$, define a Γ-invariant divisor $\{m_\alpha : \alpha \in \Omega/\Gamma\}$, where m_α represents the order of zero or pole at α. The structure theorem says that only finitely many of the m_α are non-zero in Ω/Γ, and that the degree of such a principal divisor (in the obvious sense) is 0. We can say any collection of integers $\{m_\alpha : \alpha \in \Omega/\Gamma\}$, with this finiteness condition, is a divisor, and for any divisor $\underline{d}$ define the vector space

$$L(\underline{d}) = \{f \in \mathbb{C}_p(\Omega/\Gamma) : \mathrm{div}(f) \geq -\underline{d}\}$$

as before. Then we state the following:

Lemma 9.2. *If $\underline{d}$ is a divisor on Ω/Γ, and deg($\underline{d}$) $> 2g-2$, then*

$$\dim_{\mathbb{C}_p} L(\underline{d}) = \deg(\underline{d}) - g + 1.$$

Hence the genus of $\mathbb{C}_p(\Omega/\Gamma)$ is g, using Riemann-Roch. Now recall we defined $A(\mathbb{C}_p(\Omega/\Gamma))$ to be the set of places of $\mathbb{C}_p(\Omega/\Gamma)$, leading to:

Lemma 9.3. *There is an isomorphism*

$$\Omega/\Gamma \longrightarrow A(\mathbb{C}_p(\Omega/\Gamma)) \longrightarrow V(\mathbb{C}_p),$$

$$\alpha \longmapsto \mathrm{ord}_\alpha \longmapsto P_\alpha,$$

where ord_α *is centred at* P_α*.*

Proof. This is almost completely analogous to the genus 1 case. For surjectivity, we need to consider - for a point $Q \in V$ - a non-constant function $f \in L(nQ)$, some $n \in \mathbb{N}$, rather than just $L(2Q)$. Rather than using Schnirelmann's theorem, we use the structure theorem for automorphic forms to show existence of a pole of f in Ω/Γ. □

We collect our results in the following final theorem:

Theorem 9.4. *Let Γ be a Schottky group generated freely by g elements. Let*

$$\Omega = \mathbb{P}^1_{\mathbb{C}_p} \backslash \mathcal{L},$$

with $\mathcal{L}$ the set of limit points of Γ. Then Ω/Γ is a smooth irreducible algebraic curve of genus g.

Remarks: (i) The genus 1 case is an immediate corollary of this work.

(ii) We call curves of this form *Mumford curves*. Mumford's work was considerably more extensive than the account presented here; he went on to prove that an algebraic curve is a Mumford curve if and only if it has split degenerate reduction, using rigid analysis. For details of this, including the proof that Ω/Γ has genus g, see [1], Chapter III onwards.

References

Note on references:

The major sources used in parts I and II were: [7] (chapters 2 and 5), [3] (chapters 1.2 and 3), and [4] (chapter 4). For part III, the approach I have taken is largely that of [1], chapters I and II, though I have filled in details left to the reader and gone into much greater detail in many proofs - and in some cases given my own proofs where the authors omitted them (e.g. Lemma 6.9, Proposition 7.11, Lemma 7.19, and the first half of Theorem 7.20).

[1] Lothar Gerritzen & Marius van der Put, *Schottky Groups and Mumford Curves*. Springer-Verlag, Lecture Notes in Mathematics 817, 1980.

[2] Robin Hartshorne, *Algebraic Geometry*. Springer, Graduate Texts in Mathematics 52, 1977.

[3] Alain Robert, *Elliptic Curves*. Springer-Verlag, Lecture Notes in Mathematics 326, 1973.

[4] Peter Roquette, *Analytic Theory of Elliptic Functions over Local Fields*. Vandenhoeck & Ruprecht, Hamburger Mathematische Einzelschriften, 1970.

[5] Carl L. Siegel, *Topics in Complex Function Theory (vol II)*. Wiley & Sons, 1971.

[6] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, Graduate Texts in Mathematics 106, 1986.

[7] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, Graduate Texts in Mathematics 151, 1994.

[8] John Tate, *Rational Points on Elliptic Curves over Complete Fields*. Unpublished Paper.