# Automorphic Functions and Number Theory

-

Re-TEXed by Seewoo Lee*

Goro Shimura

Last updated: February 4, 2024

## 1 Introduction

Our starting point is the following theorem which was stated by Kronercker and proved by Weber:

**Theorem 1.1.** Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta)$ with an $m$-th root of unity $\zeta = e^{2\pi i/m}$ for some positive integer $m$.

As is imeediately observed, $\zeta$ is the special value of the exponential function $e^{2\pi iz}$ at $z = 1/m$. One can natually ask the follwoing question:

**Find analytic functions which play a role analogous to $e^{2\pi iz}$ for a given algebraic number field.**

Such a question was raised by Kronecker and later taken up by Hilbert as the 12th of his famous mathematical problems. For an imaginary quadratic field $K$, this was settled by the workds of Kronecker himself, Weber, Takagi, and Hasse. It turns out that the maximal abelian extension of $K$ is generated over $K$ by th especial values of certain elliptic functions and elliptic modular functions. A primary purpose of these lectures is to indicate briefly how this result can be generalized for the number fields of higher degree, making thereby an introduction to the theory of automorphic functions and abelian varieties. I will also include some results concerning the zeta function of an algebraic curve in the sense of Hasse and Weil, since this subject is closely connected with the above question. Further, it should be point out that the automorphic functions

*seewoo5@berkeley.edu.

are meaningful as a means of generating not only abelian but also non-abelian algebraic extensions of a number field. Some ideas in this direction will be explained in the last part of the lectures.

## 2 Automorphic functions on the upper half plane, especially modular functions

Let $\mathcal{H}$ denote the complex upper half plane:

$$\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}.$$

We let every element $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, with $\det(\alpha) > 0$, act on $\mathcal{H}$ by

$$\alpha(z) = \frac{az + b}{cz + d} \tag{2.1}$$

It is well known that the gorup of analytic automorphisms of $\mathcal{H}$ is isomorphic to $\mathrm{SL}_2(\mathbb{R})/\{\pm 1_2\}$. Let $\Gamma$ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. Then the quotient $\mathcal{H}/\Gamma$ has a structure of Riemann surface such that the natural projection $\mathcal{H} \to \mathcal{H}/\Gamma$ is holomorphic. If $\mathcal{H}/\Gamma$ is compact, one can simply define an *automorphic function on $\mathcal{H}$ weith respect to* $\Gamma$ to be a meromorphic function on $\mathcal{H}$ invariant under the elements of $\Gamma$. Such a function may be regarded as a meromorphic function on the Riemann surface $\mathcal{H}/\Gamma$ in an obvious way, and vice versa. We shall later discuss special values of automorphic functions with respect to $\Gamma$ for an *arithmetically defined* $\Gamma$ with compact $\mathcal{H}/\Gamma$. But we first consider the most classical group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Since $\mathcal{H}/\Gamma$ is not compact in this case, one has to impose a certain condition on automorphic functions. It is well known that every point of $\mathcal{H}$ can be transformed by an element of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ into the region

$$F = \{z \in \mathcal{H} : |z| \geq 1, |\Re(z)| \leq 1/2\}.$$

Now two distinct inner points of $F$ can be transformed to each other by an elemtn of $\Gamma$. Now $\mathcal{H}/\Gamma$ can be compactified by adjoining a point at infinity. By taking $e^{2\pi i z}$ as a local parameter around this point, we see that $\mathcal{H}/\Gamma$ becomes a compact Riemann surface of genus 0. Thus we define an automorphic function with respect to $\Gamma$ to be a meromorphic function on this Riemann surface, considered as a function on $\mathcal{H}$. In other words, let $f$ be a $\Gamma$-invariant meromorphic function on $\mathcal{H}$. For $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we have $\gamma(z) = z + 1$. Since $f(\gamma(z)) = f(z)$, we can express $f(z)$ in the form $f(z) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi i n z}$ with $c_n \in \mathbb{C}$. Now an automorphic function with respect to $\Gamma$ is an $f$ such that $c_n = 0$ for all $n < n_0$ for some $n_0$,

i.e. meromorphic in the local parameter $q = e^{2\pi iz}$ at $q = 0$. Such a function is usually called a *modular function of level one*. Since $\mathcal{H}/\Gamma$ is of genus 0, all modular functions of level one form a rational function field over $\mathbb{C}$. As a generator of this field, one can choose a function $j$ such that

$$j(\sqrt{-1}) = 1, j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, j(\infty) = \infty. \tag{2.2}$$

Obviously the function $j$ can be characterized by (2.2) and the property of being a generator of the field of all modular functions of level one.

Now let $K$ be an imaginary quadratic field, and $\mathfrak{a}$ a fractional ideal in $K$. Take a basis $\{\omega_1, \omega_2\}$ of $\mathfrak{a}$ over $\mathbb{Z}$. Since $K$ is imaginary, $\omega_1/\omega_2$ is not real. Therefore one may assume that $\omega_1/\omega_2 \in \mathcal{H}$, by exchanging $\omega_1$ and $\omega_2$ if necessary. In this setting, we have

**Theorem 2.1.** The maximal unramified abelian extension of $K$ can be generated by $j(\omega_1/\omega_2)$ over $K$.

This is the first main theorem of the classical theory of complex multiplication. To construct ramified abelian extensions of $K$, one needs modualr functions of higher level (see below) or elliptic functions with periods $\omega_1, \omega_2$. Even Theorem 2.1 can be fully understood with the knowledge of elliptic functions of elliptic curves, though such are not explicitly involved in the statement. Therefore, our next task is to recall some elementary facts on this subject. But before that, it will be worth discussing a few elementary facts about the fractional linear transformations and discontinuous groups.

Every

## References