COMPLEX MULTIPLICATION: LECTURE 5

1. Complex tori

Let us take stock of where we are. As Yihang has shown, knowledge of how primes decompose in finite extensions of $\mathbb{Q}$ really help us when trying to solve concrete number theoretic problems. In turn, we can detect how primes decompose by finding explicit generators of the Hilbert class field. In general then, the problem we consider is that of producing explicit generators for the abelian extensions of a number field. In this course we restrict attention to quadratic imaginary extensions of $\mathbb{Q}$.

The starting point for complex multiplication is the following theorem due to Kronecker and Weber.

Theorem 1.1. *(Kronecker-Weber) Let $F/\mathbb{Q}$ be a finite abelian extension of $\mathbb{Q}$, then $\exists n$ such that*

$$F \subset \mathbb{Q}(\zeta_n)$$

where ζ_n is a primitive root of unity.

This theorem says that in order to produce abelian extension of $\mathbb{Q}$ you only need to use roots of unity. The roots of unity are the images of torsion the points on the group $\mathbb{C}/2\pi i\mathbb{Z}$ under the holomorphic map exp. Thus one can interpret this theorem as saying the abelian extensions of $\mathbb{Q}$ are generated by the images of special points under the image of a holomorphic map.

Thus one way to approach the problem of generalising this theorem would be to consider suitable analogues of the Riemann surface $\mathbb{C}/2\pi i\mathbb{Z}$ and to look at the images of certain special under certain holomorphic maps on this Riemann surface. This can be achieved through theory of elliptic/modular curves and elliptic/ modular functions.

1.1. Riemann surfaces.

In this section we will introduce complex tori, which over $\mathbb{C}$ are the same thing as elliptic curves. We will prove the set of the isomorphism classes of complex tori are naturally in bijection with some other Riemann surface known as the modular curve. Of course since we are really interested in arithmetic, we need some sort of algebraic incarnation of these objects, more precisely we will prove that any complex tori is naturally in bijection with set of solutions on an equation of the form

$$y^2 = ax^3 + bx + c$$

This result, known as the uniformisation theorem is extremely important as it forms a bridge between the worlds of complex analysis and algebra.

Let us first review the definition of Riemann surfaces, these are objects which first arose in trying to find better domains of definitions of holomorphic functions.

To motivate the definition, let us first consider the log function on the complex plane. There are many ways to define this function, see Ahlfors. but morally one should think of it as the inverse of the exponential function. However the exponential is neither surjective nor injective. If we wanted to define an inverse, the non-surjectivity is not a big problem; one could just restrict to the image of exp which is $\mathbb{C}^\times$. Similiarly one could try and get around the non-injectivity in defining log by picking a particular pre-image. Since $e^x = e^y$ if and only if $y - x$ is a multiple of $2\pi i$, any two preimages will differ by a multiple of $2\pi i$. Now exp is locally biholomorphic (bijective holomorphic with holomorphic inverse) hence if we pick a particular value for $\log(1)$, this will determine the value in any small neighbourhood about 1.

Now suppose we walk around the circle of radius 1 and try and define log on the circle. We see that the continuity forces the value at the end of the path to differ from the value at the beginning by $2\pi i$. Thus we cannot extend log to a holomorphic function on the whole $\mathbb{C}$, however it is easy to see that we can define it on $\mathbb{C} - [0, \infty)$. This is still somewhat unsatisfactory.

This problem can be resolved by noticing that exp is a bijection from $[2\pi i n, 2\pi i(n+1))$ to $\mathbb{C} - [0, \infty)$ for all $n \in \mathbb{Z}$. Then taking $\mathbb{Z}$ copies of $\mathbb{C} - [0, \infty)$ and gluing them together along the line $[0, \infty)$ we obtain a space which locally is isomorphic to $\mathbb{C}$ and for which is a natural domain of definition for log. In our case the space obtained looks like an infinite helix and furnishes our first example of a Riemann surface.

Now we come to the general definition of Riemann surfaces. Let X be a Hausdorff topological space. The definition below gives a sense to concept of X being locally the same as $\mathbb{C}$.

Definition 1.2. A chart on X is a pair (U, ϕ) where U is an open subset of X and

$$\phi : U \to V$$

is a homeomorphism from U to an open ball $V \subset \mathbb{C}$.

Given two charts $(U_\alpha, \phi_\alpha), (U_\beta, \phi_\beta)$ the transition function $\varphi_{\alpha\beta}$ is defined to be the map

$$\phi_\beta \circ \phi_\alpha^{-1}|_{\phi_\alpha(U_\alpha \cap U_\beta)} : \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$$

An atlas on X is a collection of charts $(U_\alpha, \phi_\alpha)_{\alpha \in A}$ such that $\bigcup_{\alpha \in A} U_\alpha = X$ and the transition functions $\varphi_{\alpha,\beta}$ are holomorphic.

Definition 1.3. A Riemann surface is a Hausdorff topological space X together with an atlas (U_α, ϕ_α).

Exercise: Show that the sphere S defined by the equation $x^2 + y^2 + z^2 = 1$ is a Riemann surface by using the charts given by the open covering $U_1 = S - (0, 0, 1)$ and $U_2 = S - (0, 0, -1)$ and the ϕ_i the homoemorphisms onto the (x, y)-plane given by projection from $(0, 0, 1)$ and $(0, 0, -1)$ respectively. We will denote this Riemann surface by $\mathbb{P}^1(\mathbb{C})$ and it is compact.

You should think of a Riemann surface as some topological space which is locally isomorphic to an open ball in $\mathbb{C}$, the notion of an atlas formalises this idea. There is notion of equivalence between atlases on X, two equivalent atlases define equivalent Riemann surface structures on X. This notion will not concern us as most of the time we will be working with very explicit atlases.

Since holomorphicity of map is a completely local property, the complex structure on a Riemann surface allows us to define the notion of a holomoprhic map between Riemann surfaces.

Definition 1.4. Let X and Y be Riemann surfaces with atlases $(U_\alpha, \phi_\alpha), (W_\beta, \psi_\beta)$, a map $f : X \to Y$ is holomorphic if the composite map

$$\psi_\beta \circ f \circ \phi_\alpha^{-1}|_{\phi_\alpha(U_\alpha \cap \phi^{-1}(W_\beta))} : \phi_\alpha(U_\alpha \cap \phi^{-1}(W_\beta)) \to \psi_\beta(W_\beta)$$

is a holomorphic map

A holomorphic map $f : X \to \mathbb{P}^1(\mathbb{C})$ is a called a meromorphic map.

Remark 1.5. When $X = \mathbb{C}$ this definition coincides with the standard definition meromorphic function. Indeed the condition that the singularities of f are at worst poles, is precisely the condition required so that f extends to a holomorphic map $f : \mathbb{C} \to \mathbb{P}^1(\mathbb{C})$.

The next result is an analogue of Liouville's theorem in the context of Riemann surfaces.

Proposition 1.6. *Let $f : X \to \mathbb{C}$ be a holomorphic map where X is a compact Riemann surface. Then f is constant.*

Proof. By the open mapping theorem $f(X)$ is open, but $f(X)$ is also compact hence closed. Since $\mathbb{C}$ is connected $f(X) = \mathbb{C}$, contradicting $f(X)$ compact. □

1.2. **Complex tori.** In the following we give a way of constructing a large class of Riemann surfaces.

Definition 1.7. A lattice Λ in $\mathbb{C}$ is a free $\mathbb{Z}$-submodule of $\mathbb{C}$ of rank 2. As such any lattice consists of complex numbers of the form $n\omega_1 + m\omega_2$ for some ω_1, ω_2 two $\mathbf{R}$-linearly independent elements of $\mathbb{C}$. We write $\Lambda = \langle \omega_1, \omega_2 \rangle$.

Example 1.8. Let τ be any element of the upper half plane $\mathfrak{h}$ in $\mathbb{C}$, i.e.

$$\mathfrak{h} = \{z \in \mathbb{C} : \Im z > 0\}$$

Then define the lattice Λ_τ to be the free $\mathbb{Z}$ submodule of $\mathbb{C}$ generated by $\langle 1, \tau \rangle$.

Definition 1.9. Let Λ be a lattice in $\mathbb{C}$, we define E_Λ to be the quotient space $\mathbb{C} \backslash \Lambda$. We will call any such space a complex torus.

(Technically speaking it is a complex torus of dimension one, but since we do not consider higher dimensional complex manifolds we will us this term for ease of notation)

One sees without too much difficulty, that topologically E_Λ is a torus (i.e. doughnut) and that it is compact as a topological space. The addition on $\mathbb{C}$ also carries over to $\mathbb{C}/\Lambda$ so that it is endowed with an abelian group structure with identity element 0, the image of the origin.

Proposition 1.10. *E_Λ has the natural structure of a Riemann surface.*

Proof. Since the action of Λ on $\mathbb{C}$ is free, by definition of the quotient topology any sufficiently small open set in $\mathbb{C}/\Lambda$ is isomorphic to an open set in $\mathbb{C}$. This allows us to define charts covering $\mathbb{C}/\Lambda$ and the transition maps are just the identity on subset of $\mathbb{C}$ so we have an atlas. □

Given a lattice Λ in $\mathbb{C}$ and $\alpha \in \mathbb{C}^\times$, the set $\{\alpha z : z \in \Lambda\}$ is also a lattice which we denote by $\alpha\Lambda$. Now suppose we have two lattices Λ_1 and Λ_2, and suppose $\exists \alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 \subset \Lambda_2$, then the multiplication by α defines a map $\mathbb{C} \to \mathbb{C}$ which induces a map

$$[\alpha] : E_{\Lambda_1} \to E_{\Lambda_2}$$

and it is clear that such a map is holomorphic and preserves the group structure of the tori.

Amazingly these are the only maps between complex tori.

Proposition 1.11. *Let $f : E_{\Lambda_1} \to E_{\Lambda_2}$ be a holomorphic map of complex tori which maps 0 to 0. Then f is the map $[\alpha]$ for some $\alpha \in \mathbb{C}^\times$ for which $\alpha\Lambda_1 \subset \Lambda_2$.*

Proof. Since $\mathbb{C}$ is simply connected, the map $\mathbb{C} \to E_{\Lambda_1} \to E_{\Lambda_2}$ lifts to a continuous map F

$$\begin{tikzcd}
\mathbb{C} \arrow[r, dashed, "F"] \arrow[d] & \mathbb{C} \arrow[d] \\
E_{\Lambda_1} \arrow[r, "f"] & E_{\Lambda}
\end{tikzcd}$$

where the vertical maps are just the natural projections and we can assume F maps 0 to 0.. Since the projections $\pi_i : \mathbb{C} \to E_{\Lambda_i}$ are local isomorphisms, the map F is holomorphic.

Let $\omega \in \Lambda_1$, then $G(z) = F(z+\omega) - F(z)$ takes values in Λ_2 which is discrete, hence $G(z)$ is constant. Thus $F'(z+\omega) = F'(z)$ and since this is true for all $\omega \in \Lambda_1$, by considering F' on a fundamental parallelogram we conclude that F' is bounded. It follows from Liouville's theorem that F is constant, i.e. $F(z) = \alpha z + \beta$. As f maps 0 to 0, we must have $\beta \in \Lambda_2$, and we conclude that f is the map $[\alpha]$. □

We call any holomorphic map between complex tori which maps 0 to 0 a homomorphism of complex tori (it is an isomorphism if it is also surjective). It follows from the above Proposition that any homomorphism of complex tori also preserves the group structure (since it is of the form $z \mapsto \alpha z$). A natural question to ask then is what are the isomorphism classes of complex tori?

Definition 1.12. Let Λ_1, Λ_2 be two lattices in $\mathbb{C}$. We say Λ_1 and Λ_2 are homothetic if there exists $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$.

The following is a direct consequence of Proposition 1.10

Corollary 1.13. *Two complex tori $E_{\Lambda_1}, E_{\Lambda_2}$ are isomorphic if and only Λ_1 and Λ_2 are homothetic.*

Thus if we want to classify complex tori up to isomorphism, all we need to is classify lattices in $\mathbb{C}$ up to homothety!

Let $\Lambda = \langle \omega_1, \omega_2 \rangle$ be a lattice in $\mathbb{C}$, wlog. we may assume $\omega_1/\omega_2 \in \mathfrak{h}$. Then Λ is homothetic to the lattice $\omega_2^{-1}\Lambda = \langle 1, \omega_1/\omega_2 \rangle$, so that every lattice is homothetic to a lattice of the form Λ_τ as in Example 2.8. Thus we need to consider when two lattice $\Lambda_{\tau_1}, \Lambda_{\tau_2}$ are homothetic. Let Γ be the group $SL_2(\mathbb{Z})$, then Γ acts on $\mathfrak{h}$ in the following way.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \quad \gamma\tau = \frac{a\tau + b}{c\tau + d}$$

Exercise: Let γ be as above, then prove

$$\Im\gamma(z) = \frac{\det(\gamma)}{|cz+d|^2}\Im z$$

Proposition 1.14. *Two lattices Λ_{τ_1} and Λ_{τ_2} are homothetic if and only if $\tau_2 = \gamma\tau_1$ for some $\gamma \in \Gamma$*

Proof. Let γ be as above, then $\Lambda_{\gamma\tau}$ is homothetic to the lattice $\langle a\tau+b, c\tau+d\rangle$, but since $ad-bc=1$, this lattice is just Λ_τ.

Conversely, let us suppose Λ_{τ_1} and Λ_{τ_2} are homothetic, so that $\exists\alpha\in\mathbb{C}^\times$ such that $\langle\alpha,\alpha\tau_2\rangle=\langle 1,\tau_1\rangle$. Thus $\alpha=c\tau_1+d$ for some $c,d\in\mathbb{Z}$ and $\alpha\tau_2=a\tau_1+b$ for some $a,b\in\mathbb{Z}$. Similarly there are $w,x,y,z\in\mathbb{Z}$ such that

$$\tau_1=w(a\tau_1+b)+x(c\tau_1+d)$$

$$1=y(a\tau_1+b)+z(c\tau_1+d)$$

Since τ_1 and 1 are $\mathbb{Z}$ linearly independent, this condition is equivalent to

$$\begin{pmatrix} w & x\\ y & z\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$$

Therefore $\det(\gamma)\in\{\pm1\}$, but one checks that

$$\Im\tau_2=\Im\frac{a\tau_1+b}{c\tau_1+d}=\frac{\det(\gamma)}{|c\tau_1+d|^2}\Im\tau_1$$

Then since $\Im\tau_1,\Im\tau_2>0$ we have $\det(\gamma)>0$ and hence $\gamma\in SL_2(\mathbb{Z})$. □

Thus we may identify the set of isomorphism classes of complex tori with $\Gamma\backslash\mathfrak{h}$. This in turn can be identified with a nice set of representatives as in the following proposition. Let us define the following elements of Γ:

$$\mu=\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix},\zeta=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$$

Proposition 1.15. *i)Any element in $z\in\mathfrak{h}$ can be mapped to the set*

$$D:=\{z\in\mathbb{C}:\ |z|\geq1\}\cap\{z\in\mathbb{C}:-1/2\leq\mathfrak{Re}(z)\leq1/2\}$$

ii) If z and z' are elements of D with the same image in $\mathfrak{h}$, then $z=\pm\mu z'$ or $z=\pm\zeta z'$ and z,z' both lie on the boundary of D.

Proof. By the above exercise we have $\Im\gamma z\to0$ as $c,d\to\infty$. Thus there exists $\lambda\in\Gamma$ for which $\Im\lambda z$ is maximal. Suppose $|\lambda z|<1$, then applying μ we have $\Im\mu\lambda z=1/|\lambda z|>1$, contradicting $\Im\lambda z$ maximal.

Now assume z is such that $\Im z$ is maximal. We see that

$$\zeta z=z+1$$

Thus applying a multiple of ζ, say ζ^n, we can arrange $0\leq|\Re z|\leq1/2$. By the above we must also have $|\zeta^n z|\geq1$ so we are done.

ii) Suppose $z,z'\in D$ and $\exists\gamma\in\Gamma$ such that $\gamma z=z'$. Assume $\Im z'\geq\Im z$, so that $|cz+d|\leq1$. But we also have $\Im z\geq\frac{\sqrt{3}}{2}$, hence $1\geq\Im(cz+d)\geq\frac{\sqrt{3}}{2}c$. It follows that $c=0$ or 1.

For the case $c=0$, we must have $a=1$ since $\det\gamma=1$. Then $\gamma=\zeta^n$, so that $z'=z+n$. Since $z,z'\in D$ we have $n=\pm1$.

Suppose now $c=1$. Since $|\Re(cz+d)|\leq|cz+d|\leq1$, we have $d=0,\pm1$. We consdier these cases separately

A) $d=0$. Since $|z|=|cz+d|\leq1$ we have $|z|$ lies on the boundary of D. In this case $\gamma=\begin{pmatrix} a & -1\\ 1 & 0\end{pmatrix}=\zeta^a\mu$, thus $a=0,\pm1$. If $a=0$, we are done, otherwise since $|\mu z|=1$ we have $z=\omega$ or ω^2, and in each of these two cases $\gamma z=z$. □

Thus any complex torus if isomorphic to E_{Λ_τ} for some $\tau \in D$, and the τ is unique up to identifications on the boundaries, which in turn is identified with the quotient set $\Gamma\backslash\mathfrak{h}$. However there is a little more we can say.

Exercise: Let $\omega = \frac{1+\sqrt{-3}}{2}$ For $z \in D$ let $\Gamma(z)$ denote the stabilizer of D. Show that

$$\Gamma_z = \begin{cases} \pm I & z \neq i, \omega, \omega^2 \\ \pm I, \pm\mu & z = i \\ \pm I, \pm\mu\lambda^{-1}, \pm\lambda\mu & z = \omega \\ \pm I, \pm\mu\lambda, \pm\lambda^{-1}\mu & z = \omega^2 \end{cases}$$

Theorem 1.16. *The set* $\Gamma\backslash\mathfrak{h}$ *has a natural structure of a Riemann surface.*

Proof. i) Since the action of $\Gamma/\pm I$ is no longer free, there is some subtlety when it comes to defining charts around the points i and ω. This is done in the last chapter of Serre's "A Course in Arithmetic."

ii) Exercise. □

Remark 1.17. The quotient $\Gamma\backslash\mathfrak{h}$ is an example of a moduli space. These are spaces whose points correspond to some isomorphism class of objects (eg. complex tori). It turns out that if one wants to some study a certain type of object, it can prove to be very fruitful to actually study the moduli space of such objects.

Definition 1.18. The modular curve of level 1 is the Riemann surface

$$Y(1) := \Gamma\backslash\mathfrak{h}$$

The two types of Riemann surfaces that we have constructed will play the role of $\mathbb{C}/2\pi i\mathbb{Z}$ as in the Kronecker Weber theorem. The reason there are two types of Riemann surfaces appearing is because the Hilbert class field for imaginary quadratic fields can be non-trivial. Given a quadratic imaginary field K, the elliptic curves with CM by K will determine points on $Y(1)$ whose images under a meromorphic map will generate the Hilbert class field of K. The torsion points of elliptic curves with CM by K will then generate the rest of the abelian extension in analogy with the case for $\mathbb{Q}$.

Our task now now will be to study the meromorphic functions on these Riemann surfaces analogous to the exponential function.

References