Complex Multiplication

We wish to study about the endomorphism ring of an elliptic curve E over complex numbers. ~~Where the~~ We have known that the endomorphism of E always include multiplication ~~as~~ by any integer. When the endomorphism ring of E is strictly larger than $\mathbb{Z}$ (the endomorphism ring of $E \simeq$ some structure R where $\mathbb{Z} \subset R$), then we say that E has complex multiplication.

We will now give an example about complex multiplication:

Consider the following curve over $\mathbb{C}$:

$$E: y^2 = 4x^3 - 4x$$

In chapter 9, we have known that every elliptic curve over $\mathbb{C}$ corresponds to a torus $\mathbb{C}/\Lambda$, and the above curve corresponds to the torus $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} + i\mathbb{Z}$, as seen in chapter 9.4. The exact isomorphism from E to $\mathbb{C}/\Lambda$ given by

$$\Phi: E \longrightarrow \mathbb{C}/\Lambda$$
$$z \longrightarrow (\wp(z), \wp'(z)) \quad (z \neq 0)$$
$$0 \longrightarrow \infty$$

where $\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ is the Weierstrass function

Now, we can easily see that in the case of E,:

$$\wp(iz) = \frac{1}{(iz)^2} + \sum_{\omega \neq 0} \left(\frac{1}{(iz-\omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{(iz)^2} + \sum_{\omega \neq 0} \left(\frac{1}{(iz-i\omega)^2} - \frac{1}{\omega^2} \right) = -\wp(z)$$

$$\wp'(iz) = i \cdot \wp'(z)$$

Thus, we have the following relation:

$$\begin{array}{ccc} z & \longrightarrow & iz \\ \downarrow \Phi & & \downarrow \Phi \\ (\wp(z), \wp'(z)) & \longrightarrow & (-\wp(z), i\wp(z)) \end{array}$$

From the image above, we can define the following endomorphism:

$[i]: E \to E$

$(x;y) \to (-x; iy)$

It is an endomorphism because if X, Y, Z are points $\in E$ such that $X, Y \in \mathbb{C}/\Lambda$ such that $\Phi(x) = X$, $\Phi(y) = Y$ and $X + Y = Z$, then there are $x, y \in \mathbb{C}/\Lambda$ such that ... $\Phi(\overset{x+y}{z}) = \overset{Z}{\cancel{X+Y}}$, and $\Phi(ix) = [i]X$, $\Phi(iy) = [i]Y$, therefore $[i]Z = \Phi(i(x+y)) = \Phi(ix) + \Phi(iy) = [i]X + [i]Y$, and the multiplication is expressed by rational functions.

Similarly, for integers $a, b \in \mathbb{Z}$, we can define the following endomorphism:

$[a+bi]: E \to E$

$(x;y) \to [a](x;y) + [b](-x; iy)$

Let $End(E)$ denote the ring of endomorphisms of E, and $\mathbb{Z}[i] \overset{(i)}{=} \{a + bi \mid a, b \in \mathbb{Z}\}$

For each $\beta \in \mathbb{Z}[i]$, multiplying points by β is an endomorphism of E, as shown above. Therefore we have:

$$\mathbb{Z}[i] \subseteq End(E)$$

Later, we will prove that, $End(E) \simeq \mathbb{Z}[i]$.

We have given an example about complex multiplication. Now, we will consider an abitrary elliptic curve E over $\mathbb{C}$. and study its endomorphism ring $End(E)$. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the lattice corresponding to E.

First, we will prove ~~that~~ the following theorem:

<u>Theorem 1</u>: $End(E) \simeq \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}$

<u>Proof</u>: Similar to the example above, for the map $z \to \beta z$, we consider the two values $\wp(\beta z)$ and $\wp'(\beta z)$. Since $\beta\Lambda \subseteq \Lambda$, both $\wp(\beta z)$ and $\wp'(\beta z)$ are doubly periodic functions with respect to Λ. Now using the 5th statement of theorem 9.3 in the book (the proof of this part is quite long and uses results from theorem 9.1, so I won't write it here), there are rational functions R, S such that $\wp(\beta z) =$

Thus, for each β such that $\beta\Lambda \subseteq \Lambda$ gives us an endomorphism.

Next, we will prove that, [illegible]

Let α be an endomorphism of E, then α is given by rational functions: Λ

$$[\alpha](x,y) = (R(x), y\,S(x)) \quad \text{(Chapter 2.9)}$$

Now, we consider the map

$$\tilde{\alpha} : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$$
$$z \longrightarrow \Phi^{-1}([\alpha](\Phi(z)))$$

We see that $\tilde{\alpha}$ is a homomorphism from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\Lambda$. If we restrict to a sufficiently small neighbourhood of U of $z=0$, we obtain an analytic map from U to $\mathbb{C}$ such that:

$$\tilde{\alpha}(z_1+z_2) \equiv \tilde{\alpha}(z_1)+\tilde{\alpha}(z_2) \pmod{\Lambda} \quad \forall z_1, z_2 \in U$$

By subtracting an appropriate element of Λ, we can assume $\tilde{\alpha}(0)=0$. By continuity $\tilde{\alpha}(z) \to 0$ when $z \to 0$, thus we can assume that:

$$\tilde{\alpha}(z_1+z_2) = \tilde{\alpha}(z_1)+\tilde{\alpha}(z_2) \quad \forall z_1, z_2 \in U$$

Thus, we have: $\forall z \in U$, $\tilde{\alpha}'(z) = \lim_{h\to 0} \dfrac{\tilde{\alpha}(z+h)-\tilde{\alpha}(z)}{h} = \lim_{h\to 0} \dfrac{\tilde{\alpha}(h)-\tilde{\alpha}(0)}{h} = \tilde{\alpha}'(0)$

Let $\beta = \tilde{\alpha}'(0)$, since $\tilde{\alpha}'(z) = \beta \ \forall z \in U$, we have $\tilde{\alpha}(z) = \beta z \ \forall z \in U$

Consider $z \in \mathbb{C}$, there is $n \in \mathbb{N}^*$ st $\frac{z}{n} \in U$, therefore:

$$\tilde{\alpha}(z) \equiv n\tilde{\alpha}\left(\frac{z}{n}\right) \equiv n.\frac{\beta z}{n} \equiv \beta z \pmod{\Lambda}$$

So the endomorphism $\tilde{\alpha}$ is given by multiplication by β. Since $\tilde{\alpha}(\Lambda) \subseteq \Lambda$, we must have $\beta\Lambda \subset \Lambda$, thus theorem 1 is proven.

We proved that $\mathrm{End}(E) \simeq R_\Lambda = \{\beta \in \mathbb{C} \mid \beta\Lambda \subset \Lambda\}$, where Λ is the lattice corresponding to E. Now we would like to give a nice form of the set R_Λ. To do that, we will prove the following statements:

1) $\forall \beta \in R_\Lambda$, β is an algebraic integer.
2) $R_\Lambda = \mathbb{Z}$, or there exist an integer $d > 0$ such that $R_\Lambda \subset \mathbb{Q}(\sqrt{-d})$

Proof: We have $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for $\omega_1, \omega_2 \in \mathbb{C}$, Let $\beta \in R_\Lambda$ then we have $\beta\omega_1 = j\omega_1 + k\omega_2$, $\beta\omega_2 = m\omega_1 + n\omega_2$ for some $j, k, m, n \in \mathbb{Z}$. It means that $\beta \begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} = \begin{bmatrix} j & k \\ m & n\end{bmatrix}\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}$, or β is a root of the polynomial $(\beta-j)(\beta-n)-mk$, this is a monic polynomial with integer coefficients. This proves 1). It also means that there is an interger such that $\beta \in \mathbb{Q}(\sqrt{-d})$.

To prove 2), note that if $\beta \in \mathbb{R}$, $(\beta - j)\omega_1 = k\omega_2$, but since ω_1 and ω_2 are linearly independent over $\mathbb{R}$, β must be $j \in \mathbb{Z}$.

Suppose $\beta \notin \mathbb{Z}$, then there is an integer $d > 0$ such that $\beta \in \mathbb{Q}(\sqrt{-d})$. Let $\beta' \notin \mathbb{Z}$ be another element of R_Λ, then, there is an integer $d' > 0$ such that $\beta' \in \mathbb{Q}(\sqrt{-d'})$. It is easy to see that R_Λ is a ring, thus, $\beta + \beta' \in \mathbb{Q}(\sqrt{-d''})$ for some integer $d'' > 0$.

Lemma 1: $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$

Proof: WLOG, d, d', d'' are square free, and we have $a\sqrt{d} + b\sqrt{d'} = c + e\sqrt{d''}$ for some $a, b, c, e \in \mathbb{Q}$ and $a, b, e \neq 0$.

Then we have $(a\sqrt{d} + b\sqrt{d'})^2 - 2c(a\sqrt{d} + b\sqrt{d'}) + c^2 - e^2 d'' = 0$.

By expanding, we get $\sqrt{d'}(2ab\sqrt{d} - 2cb) = c^2 - e^2 d'' - a^2 d - b^2 d' + 2ca\sqrt{d}$

This means $\sqrt{d'} \in \mathbb{Q}(\sqrt{d})$ and $\sqrt{d} \in \mathbb{Q}(\sqrt{d'})$ similarly. We can easily have $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ ~~and since ... we must have ...~~

Back to proving 2), since $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{-d'})$, we see that $\forall \beta \in R_\Lambda$, $\beta \in \mathbb{Q}(\sqrt{-d})$ and thus we proved 2).

~~Now~~,

Now, time for some definitions. For a quadratic field $K = \mathbb{Q}(\sqrt{-d})$, define

$$O_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & \text{if } d \equiv 3 \pmod 4 \\ \mathbb{Z}[\sqrt{-d}] & \text{if } d \equiv 1, 2 \pmod 4 \end{cases}$$

We will prove the following lemma

Lemma 2: O_K is the ring of algebraic integers that belongs to $K = \mathbb{Q}(\sqrt{-d})$

Proof: It is easy to see that if $\beta \in O_K$, then β is an algebraic integer

Now, suppose $\beta = \frac{x + y\sqrt{-d}}{z}$ $(GCD(x,y,z) = 1)$ is an algebraic integer, then we have $\beta^2 - \frac{2x}{z}\beta + \frac{x^2 + y^2 d}{z^2} = 0$. If $\beta \notin \mathbb{Z}$ then the minimal of β has degree 2, this means $2x \,\vdots\, z$ and $x^2 + y^2 d \,\vdots\, z^2$. $\boxed{\text{If } z \text{ is odd}}$ then $z \mid x$ and $GCD(y, z) = 1$, we must have $z^2 \mid d$, thus $z = 1 \Rightarrow \boxed{\beta \in \mathbb{Z}}$.

$\boxed{\text{If } z \text{ is even}}$, $z = 2z' \Rightarrow x \,\vdots\, z'$ and $x^2 + y^2 d \,\vdots\, 4z'^2$, we easily have $z' = 1$ and $x^2 + dy^2 \,\vdots\, 4$. If $d \equiv 1, 2 \pmod 4$ then $2 \mid x$ and $2 \mid y$, contradiction since $GCD(x, y, z) = 1$ and $2 \mid z$. Thus, if z is even, then $d \equiv 3 \pmod 4$ and we can write β in the form of $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$.

Now, we will prove the following theorem, to give a nice form of $End(E)$:

<u>Theorem 2</u>: $\begin{cases} End(E) \simeq \mathbb{Z} \\ End(E) \simeq \mathbb{Z}[f\sqrt{-d}] & \text{for } d \equiv 1,2 \pmod 4 \text{ and } f \in \mathbb{Z} \\ End(E) \simeq \mathbb{Z}[f\frac{1+\sqrt{-d}}{2}] & \text{for } d \equiv 3 \pmod 4 \text{ and } f \in \mathbb{Z} \end{cases}$

<u>Proof</u>: If $R\Lambda \neq \mathbb{Z}$, then $R\Lambda \subset Q(\sqrt{-d})$ for some d. WLOG, $d \equiv 1, 2 \pmod 4$.
Since each element of $R\Lambda$ is an algebraic integer, we have $R\Lambda \subseteq O_K$ where $K = Q(\sqrt{-d})$. Let $e + f\sqrt{-d} \in R\Lambda$ with $|f|$ minimal, then we can easily prove that if $e' + f'\sqrt{-d} \in R\Lambda$, then $f \mid f'$. In the other hand, $\mathbb{Z} \subset R\Lambda$ and $e + f\sqrt{-d} \in R\Lambda \Rightarrow m + n(e + f\sqrt{-d}) \in R\Lambda \ \forall m, n \in \mathbb{Z}$, this means $R\Lambda = \mathbb{Z}[f\sqrt{-d}]$.
Thus $End(E) \simeq R\Lambda = \mathbb{Z}[f\sqrt{-d}]$ for some f if $d \equiv 1, 2 \pmod 4$ and $R\Lambda \neq \mathbb{Z}$, and theorem 2 is proven.

As we can see, in theorem 2, $End(E) \simeq \mathbb{Z}$, or $End(E) \simeq \mathbb{Z}[u]$ for some algebraic integer u. In the latter case, $End(E)$ is strictly larger than $\mathbb{Z}$ and E has complex multiplication, defined in the first part of theorem;

In the example, we had $\mathbb{Z}[i] \subseteq End(E)$ where $E: y^2 = 4x^3 - 4x$.
Now by theorem 2, we have $\mathbb{Z}[i] \supseteq End(E)$, thus $\mathbb{Z}[i] \simeq End(E)$