VII. Complex multiplication (II)

Let $\mathbb{C}/\Lambda_1$, $\mathbb{C}/\Lambda_2$ be two complex tori. A map $\varphi: \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, $\bar{z} \longmapsto \varphi(\bar{z})$ is call a morphism of complex tori if $\varphi(\bar{z}_1+\bar{z}_2) = \varphi(\bar{z}_1)+\varphi(\bar{z}_2)$.

Prop (Sil. I. Ch. VI). Every morphism $\mathbb{C}/\Lambda_1 \xrightarrow{\varphi} \mathbb{C}/\Lambda_2$ is of the form $\varphi(z+\Lambda_1) = \alpha z + \Lambda_2$ where $\alpha\Lambda_1 \subseteq \Lambda_2$.

Due to the uniformisation theorem presented in VI, we can and will assume that a complex elliptic curve is a complex torus $\mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\oplus\mathbb{Z}\tau$, $\mathrm{Im}(\tau)>0$ and $\boxed{\mathrm{End}(E) = \{\alpha\in\mathbb{C} \mid \alpha\Lambda\subseteq\Lambda\}}$ E[n]: 

In this case, $\alpha.1 = \alpha = n+m\tau$, $\alpha\tau = n\tau + m\tau^2 \in \Lambda \Rightarrow n\tau+m\tau^2 = r\tau+s$
$\Rightarrow m\tau^2+(n-r)\tau-s=0$. $\Rightarrow m=0 \Rightarrow \alpha=n$ or $m\neq 0 \Rightarrow \tau$ is quadratic imaginary and hence α.

Hence, it may happen $\mathrm{End}(E)\neq\mathbb{Z}$. Notice that $\mathbb{Z}\subseteq\mathrm{End}(E)$. $\ni [n]\ \forall n$.

Def: If $\mathrm{End}(E)\neq\mathbb{Z} \Rightarrow$ we say that E has CM (complex multiplication).

Def: K number field. An order R in K is a subring of K, finitely generated as $\mathbb{Z}$-module s.t. $R\otimes\mathbb{Q}=K$.

Obs: The maximal order in K is $\mathcal{O}_K$ (exercise). Actually, if K is quadratic and $\mathcal{O}_K = \mathbb{Z}\oplus\mathbb{Z}\omega_K$, then every order is of the form $R = \mathbb{Z}\oplus\mathbb{Z}c\omega_K$ for some c, called the conductor of the order.
$\Downarrow$ requires proof!!

Notice: $\forall\alpha\in\mathrm{End}(E)$ $\alpha = n+m\tau$ where τ is quadratic imaginary
$\Rightarrow \mathrm{End}(E)=R$ is an order in a quadratic imaginary field, namely: $K=\mathbb{Q}(\tau)$ (exercise)

In that case, we also say that E has CM by R.

Prop (Sil. II, ch. 2)

Let $E/\mathbb{C}$ be a complex elliptic curve with CM by R. Then, $\exists!\ [\ ]: R \xrightarrow{\sim} \mathrm{End}(E)$ s.t. $\forall \omega \in \Omega_E$, $[\alpha]^* \omega = \alpha \omega$, where
$$[\alpha]^*: \Omega_E \to \Omega_E, \quad \underset{f\cdot dz}{\overset{\shortparallel}{\eta}} \mapsto (f \circ [\alpha])\, d([\alpha] z)$$

$(E, [\ ])$ is called a normalised pair.

Cor: Let $(E_i, [\ ]_{E_i})$ be normalised CM pairs. Then $\phi: E_1 \to E_2$ is an isogeny $\iff$ $\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi$.

We have, then:

$$\mathcal{Ell}(R) = \{\text{elliptic curves } E/\mathbb{C},\ \mathrm{End}(E) \cong R\}/\cong_{\mathbb{C}} \ \cong \ \{\text{lattices } \Lambda \subseteq \mathbb{C} \mid \underset{R}{\overset{\shortparallel}{\mathrm{End}(\Lambda)}}\}/\text{homothety}.$$

Given K, quadratic imaginary, $\mathfrak{a} \subseteq R_K$ ideal $\Rightarrow \mathfrak{a} \subseteq K$ is a lattice ($\mathbb{Z}$-module of rk 2 $\not\subseteq \mathbb{R}$), $E_{\mathfrak{a}} := \mathbb{C}/\mathfrak{a}$ is s.t. $E_{\mathfrak{a}}$ has CM by $R_K = \mathcal{O}_K$.

$$\mathrm{End}(E_{\mathfrak{a}}) = \{\alpha \in \mathbb{C} \mid \alpha \mathfrak{a} \subseteq \mathfrak{a}\} = \{\alpha \in K \mid \alpha \mathfrak{a} \subseteq \mathfrak{a}\} = R_K$$

$\alpha \in K$; $\Uparrow$ $\mathfrak{a}$ free $\Rightarrow$ has a basis, det. trick.

$\Rightarrow$
$$\mathrm{Cl}(R_K) = \{\text{frac ideals of } K\}/\text{ppals} \cong \{\text{ideals of } R_K\}/\sim \ \to \mathcal{Ell}(R_K), \quad \bar{\mathfrak{a}} \mapsto [E_{\mathfrak{a}}]$$

More generally, Λ lattice, $E_\Lambda \in \mathcal{Ell}(R_K)$, $0 \neq \mathfrak{a} \subseteq K$ frac. ideal $\Rightarrow$ define $\mathfrak{a}\Lambda := \{\alpha_1 \lambda_1 + \dots + \alpha_r \lambda_r \mid \alpha_i \in \mathfrak{a},\ \lambda_i \in \Lambda\}$.

e.g. $\Lambda = \mathbb{Z}[i]$, $\mathrm{End}(E_\Lambda) = \mathbb{Z}[i]$.

$i\Lambda = \Lambda$; g_3 modular, weight 6

$g_3(\Lambda) = g_3(i\Lambda) = i^6 \cdot g_3(\Lambda) = -g_3(\Lambda) = 0 \Rightarrow E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x$,

$j = 1728 \Rightarrow E_\Lambda \cong E/\mathbb{Q}$, for instance $y^2 = x^3 + x$.

However, $g_2(\Lambda) = g_2(\mathbb{Z}[i]) \underset{\text{Hurwitz}}{=} 64\left(\int_0^1 \frac{dt}{\sqrt{1-t^4}}\right)^4 \notin \mathbb{Q}$.

• If E has CM by $K \Rightarrow$ we will use torsion points of E to generate abelian extensions of K.

Def: $\mathfrak{a} \leq R_K$ ideal, $E[\mathfrak{a}] = \{P \in E \mid [\alpha]P = 0 \ \forall \alpha \in \mathfrak{a}\}$. $\quad \bar{\mathfrak{a}}\Lambda/\Lambda \cong \mathcal{O}_K/\mathfrak{a}$.

Prop: a) $E[\mathfrak{a}] = \mathrm{Ker}[\underset{z+\Lambda \mapsto z+\bar{\mathfrak{a}}\Lambda}{E \longrightarrow \bar{\mathfrak{a}} * E}]$ isogeny.

b) $\boxed{E[\mathfrak{a}] \text{ free } R_K/\mathfrak{a}\text{-lattice of rk } 1.}$

$\deg[E \to \bar{\mathfrak{a}} * E] = N^K_{\mathbb{Q}}\mathfrak{a}$.

Cor: If $E \in \mathcal{ELL}(R_K)$, $\forall \mathfrak{a} \leq R_K$,

---

• Rationality of the j-invariant

Prop (Sil. II, 2.1).

a) Let $E/\mathbb{C}$ be an elliptic curve, $\sigma : \mathbb{C} \to \mathbb{C}$ field automorphism $\Rightarrow$

$\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)^\sigma$

b) If $\mathrm{End}(E) \cong R_K \Rightarrow j(E) \in \overline{\mathbb{Q}}$

c) $\mathcal{ELL}(R_K) \cong \{$elliptic curves $E/\overline{\mathbb{Q}}$ s.t. $\mathrm{End}(E) \cong R_K\}/\overline{\mathbb{Q}}$-isomorphism.

Proof: a) $\phi : E \to E$ endomorphism $\Leftrightarrow$ $\underset{\sigma\circ\phi\circ\sigma^{-1}}{\phi^\sigma} : E^\sigma \to E^\sigma$ endomorphism.

b) E^σ is obtained acting σ on the Weierstrass $\Rightarrow j(E^\sigma) = j(E)^\sigma$.

Further, $\mathrm{End}(E^\sigma) \overset{a)}{\cong} R_K^\sigma \underset{\sigma(\alpha)\bar{\sigma}^{-1} = \alpha}{=} R_K \Rightarrow E^\sigma$ is in one of the finitely many $\mathbb{C}$-iso classes of elliptic curves with CM by $R_K \Rightarrow j(E)^\sigma$ takes finitely many values as $\sigma \in \mathrm{Aut}(\mathbb{C}) \Rightarrow [\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite #

Prop (Sil II. Ch. 2, 1.2) Notations as before:

a) Let $\Lambda \subseteq \mathbb{C}$ be a lattice, $E_\Lambda = \mathbb{C}/\Lambda \in \mathcal{E}\ell\ell(R_K)$ and $\mathfrak{a}, \mathfrak{b}$ frac. ideals. Then:

i) $\mathfrak{a}\Lambda$ is a lattice

ii) $E_{\mathfrak{a}\Lambda} \in \mathcal{E}\ell\ell(R_K)$

iii) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \Leftrightarrow \bar{\mathfrak{a}} = \bar{\mathfrak{b}}$.

Hence $Cl(R_K)$ acts on $\mathcal{E}\ell\ell(R_K)$ via $\bar{\mathfrak{a}} * E_\Lambda := E_{\mathfrak{a}^{-1}\Lambda}$.

b) This action is simply transitive. In particular:

$|\mathcal{E}\ell\ell(R_K)| = |Cl(R_K)|$.

Proof a) i): Since $End(E_\Lambda) = R_K \Rightarrow R_K\Lambda = \Lambda$. Take $d \in \mathbb{Z}^* \setminus \{0\}$, s.t. $d\mathfrak{a} \subseteq R_K$ and $dR_K \subseteq \mathfrak{a}$ $\Rightarrow \mathfrak{a} \subseteq \frac{1}{d}\Lambda \Rightarrow \mathfrak{a}\Lambda$ discrete subgroup of $\mathbb{C}$

$\Rightarrow d\Lambda \subseteq \mathfrak{a}\Lambda \Rightarrow \mathfrak{a}\Lambda \otimes \mathbb{R} = \mathbb{C} \Rightarrow \mathfrak{a}\Lambda$ lattice.

ii) $\alpha \in \mathbb{C}\setminus\{0\}$, $\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda \Leftrightarrow \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}^{-1}\mathfrak{a}\Lambda \Leftrightarrow \alpha\Lambda \subseteq \Lambda \Rightarrow End(E_{\mathfrak{a}\Lambda}) = End(E_\Lambda) = R_K$.

iii) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \Leftrightarrow \exists c \in \mathbb{C}\setminus\{0\} \mid \mathfrak{a}\Lambda = c\mathfrak{b}\Lambda \Leftrightarrow \Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda$

$\Leftrightarrow \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda \Leftrightarrow c\mathfrak{a}^{-1}\mathfrak{b}, c^{-1}\mathfrak{a}\mathfrak{b}^{-1}$ take Λ to $\Lambda \Rightarrow$ they belong

$\underset{R_K\Lambda = \Lambda}{\Leftrightarrow}$ to $R_K \Leftrightarrow \mathfrak{a} = c\mathfrak{b}$.

b) $\bar{\mathfrak{a}} * (\bar{\mathfrak{b}} * E_\Lambda) = \bar{\mathfrak{a}} * E_{\mathfrak{b}^{-1}\Lambda} = E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda} = E_{(\mathfrak{a}\mathfrak{b})^{-1}\Lambda} = (\overline{\mathfrak{a}\mathfrak{b}}) * E_\Lambda \Rightarrow$ this is an action.

Given $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{E}\ell\ell(R_K) \Rightarrow \mathfrak{a}_i = \frac{1}{\lambda_i}\Lambda_i$, $\lambda_i \in \Lambda_i \setminus \{0\} \Rightarrow \mathfrak{a} := \mathfrak{a}_2^{-1}\mathfrak{a}_1$ is s.t. $\bar{\mathfrak{a}} * E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} =$

$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \Lambda_2 \Rightarrow$

$= E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}$. Also $\bar{\mathfrak{a}} * E_\Lambda = \bar{\mathfrak{b}} * E_\Lambda \Rightarrow \bar{\mathfrak{a}} = \bar{\mathfrak{b}}$ (from ii) a).

c) See textbook #

Thm (Sil. II, 2.3) Let $E/\mathbb{C}$ have CM by R_K, $L = K(j(E), E_{tors})$ be the field generated by $j(E)$ and the x-coordinate of all torsion points.
$\Rightarrow L|K(j(E))$ is abelian (but $L|K$ not necessarily so).

Proof: $H := K(j(E))$, $L_m = H(E[m])$. Enough to see $L_m|H$ abelian $\forall m$.

There is $\rho: Gal(\bar{K}|H) \to Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$

$\sigma \longmapsto \rho(\sigma): T \to T^{\sigma}$

$Ker(\rho) = Gal(\bar{K}|L_m) \Rightarrow Gal(L_m|H) \hookrightarrow \underbrace{GL_2(\mathbb{Z}/m\mathbb{Z})}$ non-commutative!!

However, E/H and $\forall \alpha \in End(E)$, $\boxed{\sigma/H \text{ (Sil II 2.2b)}}$ $\Rightarrow$ elements in $Gal(L_m/H)$ commute with R_K acting on $E[m]$ $\Rightarrow \rho: Gal(\bar{K}|H) \to Aut_{R_K/mR_K}(E[m])$

but this has rank 1 over $R_K/mR_K \Rightarrow Gal(L_m|H) \leq (R_K/mR_K)^*$ #

Thm (Sil. II. 4.1) Let $K|\mathbb{Q}$ be quadratic imaginary, R_K its ring of integers and $E/\mathbb{C}$ elliptic curve with $End(E) \cong R_K \Rightarrow K(j(E)) = H_K$.

Proof: Fix E, CM by R_K, $\boxed{F: Gal(\bar{K}|K) \to Cl(R_K) \ (\text{abelian}), \quad \sigma \longmapsto F(\sigma) \mid E^{\sigma} = F(\sigma) * E}$

doesn't depend on E. It factors $F: Gal(K^{ab}|K) \to Cl(R_K)$,

K^{ab} = max abelian extension of K.

Fact: $\exists$ finite set of rational primes $S \subseteq \mathbb{Z}$ s.t. if $p \notin S$, p splits in K as $pR_K = \mathfrak{p}\mathfrak{p}' \Rightarrow F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}} \in Cl(R_K)$.

Now, if $L|K$ is the finite extension corresponding to $F: Gal(\bar{K}|K) \to Cl(R_K) \Rightarrow Gal(\bar{K}|L) = \{\sigma \in Gal(\bar{K}|K) \mid F(\sigma)*E = E\}$
$= \{\sigma \in Gal(\bar{K}|K) \mid \underbrace{E^{\sigma} = E}_{\Leftrightarrow\, j(E)^{\sigma} = j(E)}\} = Gal(\bar{K}|K(j(E)))$.

$\Rightarrow L = K(j(E))$. Since $F(Gal(L|K)) \hookrightarrow Cl(R_K) \Rightarrow L|K$ is abelian

$\Rightarrow L = K(j(E))|K$ abelian.

If $\mathfrak{c}_{L|K}$ = conductor of $L|K$, consider $I(\mathfrak{c}_{L|K}) \xrightarrow{(\cdot, L|K)} Gal(L|K) \xrightarrow{F} Cl(R_K)$

$\Rightarrow F \circ (\cdot, L|K) =$ proj. of $I(\mathfrak{c}_{L|K})$ onto $Cl(R_K)$.

Since $F: Gal(L|K) \hookrightarrow Cl(R_K) \Rightarrow \forall (\alpha) \in I(\mathfrak{c}_{L|K})$, $((\alpha), L|K) = 1$

$\Rightarrow \mathfrak{c}_{L|K} = (1) \Rightarrow L|K$ unramified abelian. $\Rightarrow L \subseteq H_K$.

Now, $I(\mathfrak{c}_{L|K}) \to Cl(R_K) \to 1 \Rightarrow F$ surjective $\Rightarrow$ isomorphism $\Rightarrow$

$[L:K] = |Cl(R_K)| = [H_K : K] \Rightarrow L = H_K$. #

Notice, $[\mathbb{Q}(j(E)):\mathbb{Q}] \leq h_K$

$[K(j(E)):K] = h_K \Rightarrow [\mathbb{Q}(j(E)):\mathbb{Q}] = [K(j(E)):K] = h_K$

$[K:\mathbb{Q}] = 2$

$\Rightarrow$ $\boxed{\text{Irr}(j(E), \cancel{K}) = \text{Irr}(j(E), \mathbb{Q}) \text{ and has degree } h_K}$.