HOMOMORPHISM GROUPS OF ELLIPTIC CURVES OVER THE COMPLEX NUMBERS

RACHEL NEWTON

Let $\Lambda = \{\sum_{i=1}^{n} a_i w_i \mid a_i \in \mathbb{Z}\}$ where $w_1, \ldots w_n$ are a basis for $\mathbb{R}^n$ over $\mathbb{R}$. Λ is called a *lattice* in $\mathbb{R}^n$. We identify $\mathbb{C}$ with $\mathbb{R}^2$ as vector spaces over $\mathbb{R}$. An elliptic curve over the complex numbers is a quotient group $\mathbb{C}/\Lambda$ where Λ is a lattice in $\mathbb{C}$. The additive group law on $\mathbb{C}$ induces a group law on $\mathbb{C}/\Lambda$.

Given two elliptic curves over $\mathbb{C}$, E_1 and E_2, we want to study the group of homomorphisms from E_1 to E_2, denoted $\mathrm{Hom}(E_1, E_2)$. We write $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ for the ring of endomorphisms of an elliptic curve E over $\mathbb{C}$.

Since there is a group law on an elliptic curve E over $\mathbb{C}$, for any $n \in \mathbb{Z}_{>0}$, there is an endomorphism $[n] : E \to E$ sending every $P \in E$ to $nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}$. For $n \in \mathbb{Z}_{<0}$, the endomorphism $[n]$ sends $P \in E$ to $nP = \underbrace{-P - P - \cdots - P}_{(-n) \text{ times}}$. The endomorphism $[0]$ sends every $P \in E$ to zero. Thus, $\mathbb{Z} \subset \mathrm{End}(E)$. The endomorphism ring of an elliptic curve over $\mathbb{C}$ is usually just $\mathbb{Z}$ but it can be larger. For example, the elliptic curve $E = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}i)$ has $\mathrm{End}(E) = \mathbb{Z}[i]$.

Definition 0.1. Let E be an elliptic curve over $\mathbb{C}$. If $\mathbb{Z} \subsetneq \mathrm{End}(E)$ then we say that E has *complex multiplication*.

Definition 0.2. Let K be a number field (i.e. a field which is a finite extension of $\mathbb{Q}$). An *order* in K is a subring R of K which is generated as an abelian group by a basis for K over $\mathbb{Q}$.

The ring of integers of a number field K is the maximal order in K.

Example 1. The subring $\mathbb{Z}[\sqrt{-3}]$ is an order in $\mathbb{Q}(\sqrt{-3})$ but it is not maximal. The ring of integers of $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Theorem 0.3. *If an elliptic curve E over $\mathbb{C}$ has complex multiplication then there exists $d \in \mathbb{Z}_{>0}$ such that* $\mathrm{End}(E)$ *is an order in the imaginary quadratic field* $\mathbb{Q}(\sqrt{-d})$.

Proof. See, for example, VI.5.5 in *The Arithmetic of Elliptic Curves* by J. H. Silverman. □

Question 1. What are the possibilities for $\mathrm{Hom}(E_1, E_2)$ for elliptic curves E_1 and E_2 over the complex numbers?

If we have a nonzero homomorphism $\varphi : E_1 \to E_2$ then we can generate new homomorphisms by pre-composing (resp. post-composing) with a non-trivial endomorphism of E_1 (resp. E_2). But can we get the whole of $\mathrm{Hom}(E_1, E_2)$ this way, starting from one nonzero homomorphism?