18.783 Elliptic Curves
Lecture 12

Andrew Sutherland

March 9, 2022

The endomorphism ring of an elliptic curve E

Recall that the endomorphism ring $\mathrm{End}(E)$ is the ring of morphisms $E \to E$ in which addition is defined pointwise and we multiply via composition.

- $\mathrm{End}(E)$ has no zero divisors;
- $\deg\colon \mathrm{End}(E) \to \mathbb{Z}_{\geq 0}$ defined by $\alpha \mapsto \deg \alpha$ is multiplicative (with $\deg 0 := 0$);
- $\deg n = n^2$ for all $n \in \mathbb{Z} \subseteq \mathrm{End}(E)$;
- $\hat{\alpha} \in \mathrm{End}(E)$ with $\alpha\hat{\alpha} = \hat{\alpha}\alpha = \deg \alpha = \deg \hat{\alpha}$, and $\hat{\hat{\alpha}} = \alpha$;
- $\hat{n} = n$ for all $n \in \mathbb{Z} \subseteq \mathrm{End}(E)$;
- $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}$ and $\widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}$ for all $\alpha, \beta \in \mathrm{End}(E)$;
- $\mathrm{tr}\,\alpha := \alpha + \hat{\alpha}$ satisfies $\mathrm{tr}\,\alpha = \mathrm{tr}\,\hat{\alpha}$ and $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}\,\alpha + \mathrm{tr}\,\beta$;
- $\mathrm{tr}\,\alpha = \deg \alpha + 1 - \deg(\alpha - 1) \in \mathbb{Z}$ for all $\alpha \in \mathrm{End}(E)$;
- α and $\hat{\alpha}$ are the roots of the characteristic equation $x^2 - (\mathrm{tr}\,\alpha)x + \deg \alpha \in \mathbb{Z}[x]$.

Tensor products of algebras

Definition

For a commutative ring R an (associative unital) R-algebra A is a ring equipped with a homomorphism $R \to A$ whose image lies in the center. Every ring is a $\mathbb{Z}$-algebra.

Definition

The tensor product of two R-algebras A and B is the R-algebra $A \otimes_R B$ generated by the formal symbols $\alpha \otimes \beta$ with $\alpha \in A$, $\beta \in B$, subject to the relations

$$(\alpha_1 + \alpha_2) \otimes \beta = \alpha_1 \otimes \beta + \alpha_2 \otimes \beta, \quad \alpha \otimes (\beta_1 + \beta_2) = \alpha \otimes \beta_1 + \alpha \otimes \beta_2$$

$$r\alpha \otimes \beta = \alpha \otimes r\beta = r(\alpha \otimes \beta), \quad (\alpha_1 \otimes \beta_1)(\alpha_2 \otimes \beta_2) = \alpha_1\alpha_2 \otimes \beta_1\beta_2$$

It comes with an R-linear map $\varphi\colon A \times B \to A \otimes_R B$ defined by $(\alpha, \beta) \mapsto \alpha \otimes \beta$ with the universal property that every R-bilinear map of R-algebras $\psi\colon A \times B \to C$ factors uniquely through $A \otimes_R B$: there is a unique $\psi'\colon A \otimes_R B \to C$ such that $\psi = \psi' \circ \varphi$.

Base change

Definition

If $R \to S$ is a homomorphism of commutative rings, then S as an R-algebra.
If A is an R-algebra, the S-algebra $S \to A \otimes_R S$ is the base change of A to S.
(the map $S \to A \otimes_R S$ is defined by $s \mapsto 1 \otimes s$).

Lemma

If R is an integral domain with fraction field S then every element of $A \otimes_R S$ can be written as a pure tensor $\alpha \otimes s$.

Example

The ring of integers $\mathcal{O}_K$ of a number field $K/\mathbb{Q}$ is a $\mathbb{Z}$-algebra of rank $n := [K : \mathbb{Q}]$.
The base change $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra of dimension n isomorphic to K.

The endomorphism algebra of an elliptic curve

Definition

The endomorphism algebra of an elliptic curve E is the $\mathbb{Q}$-algebra

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Its elements can all be written in the form $r\alpha$ with $r \in \mathbb{Q}$ and $\alpha \in \mathrm{End}(E)$.
We extend the map $\alpha \to \hat{\alpha}$ to $\mathrm{End}^0(E)$ by defining $\widehat{r\alpha} = r\hat{\alpha}$. We then have $\hat{\hat{\alpha}} = \alpha$, $\widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}$ and $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta}$ for $\alpha, \beta \in \mathrm{End}^0(E)$, and $\hat{r} = r$ for $r \in \mathbb{Q}$.

Definition

An anti-homomorphism $\varphi\colon R \to S$ of rings is a homomorphism of additive groups with $\varphi(1_R) = 1_S$ and $\varphi(\alpha\beta) = \varphi(\beta)\varphi(\alpha)$ for all $\alpha, \beta \in R$. An involution (or anti-involution) is an anti-homomorphism $\varphi\colon R \to R$ that is its own inverse: $\varphi \circ \varphi$ is the identity map.

The involution $\alpha \mapsto \hat{\alpha}$ of $\mathrm{End}(E)$ is called the Rosati involution.

Norm and trace

Definition

For $\alpha \in \mathrm{End}^0(E)$, we define the (reduced) norm $\mathrm{N}\alpha := \alpha\hat{\alpha}$ and trace $\mathrm{T}\alpha := \alpha + \hat{\alpha}$.
We have $\mathrm{N}\hat{\alpha} = \mathrm{N}\alpha$, $\mathrm{T}\hat{\alpha} = \mathrm{T}\alpha$, $\mathrm{N}(\alpha\beta) = \mathrm{N}\alpha\mathrm{N}\beta$, $\mathrm{T}(\alpha+\beta) = \mathrm{T}\alpha + \mathrm{T}\beta$, $\mathrm{T}(r\alpha) = r\mathrm{T}\alpha$,
and we note that $\mathrm{T}\alpha = \alpha + \hat{\alpha} = 1 + \alpha\hat{\alpha} - (1-\alpha)(1-\hat{\alpha}) = 1 + \mathrm{N}\alpha - \mathrm{N}(1-\alpha) \in \mathbb{Q}$.

Lemma

For all $\alpha \in \mathrm{End}^0(E)$ we have $\mathrm{N}\alpha \in \mathbb{Q}_{\geq 0}$ with $\mathrm{N}\alpha = 0$ if and only if $\alpha = 0$.

Proof: *If $\alpha = r\phi$ then $\mathrm{N}\alpha = \alpha\hat{\alpha} = r\phi r\hat{\phi} = r^2 \deg\phi \geq 0$ with equality only if $r\phi = 0$.*

Corollary

Every nonzero $\alpha \in \mathrm{End}^0(E)$ has a multiplicative inverse α^{-1}.

Proof: *If $\beta = \hat{\alpha}/\mathrm{N}\alpha$, then $\alpha\beta = \mathrm{N}\alpha/\mathrm{N}\alpha = 1$ and $\beta\alpha = \mathrm{N}\hat{\alpha}/N\alpha = 1$, so $\beta = \alpha^{-1}$.*

Lemma

An element $\alpha \in \mathrm{End}^0(E)$ is fixed by the Rosati involution if and only if $\alpha \in \mathbb{Q}$.

Proof: *If $\hat{\alpha} = \alpha$ then $\mathrm{T}\alpha = \alpha + \hat{\alpha} = 2\alpha$ and $\alpha = \mathrm{T}\alpha/2 \in \mathbb{Q}$.*

Lemma

Let $\alpha \in \mathrm{End}^0(E)$. Then α and $\hat{\alpha}$ are roots of the polynomial

$$x^2 - (\mathrm{T}\alpha)x + \mathrm{N}\alpha \in \mathbb{Q}[x]$$

Proof: $0 = (\alpha - \alpha)(\hat{\alpha} - \hat{\alpha}) = \alpha^2 - \alpha(\alpha + \hat{\alpha}) + \alpha\hat{\alpha}) = \alpha^2 - (\mathrm{T}\alpha)\alpha + \mathrm{N}\alpha$.

Corollary

For any nonzero $\alpha \in \mathrm{End}^0(E)$, if $\mathrm{T}\alpha = 0$ then $\alpha^2 = -\mathrm{N}\alpha < 0$ and $\alpha \notin \mathbb{Q}$.

Quaternion algebras

Definition

A quaternion algebra H over a field k is a k-algebra with a basis $\{1, \alpha, \beta, \alpha\beta\}$ satisfying $\alpha^2, \beta^2 \in k^\times$ and $\alpha\beta = -\beta\alpha$. We distinguish quaternion algebras as non-split or split depending on whether they are division rings or not.

Example

Non-split: the $\mathbb{R}$-algebra with basis $\{1, i, j, ij\}$ satisfying $i^2 = j^2 = -1$ and $ij = -ji$.

Split: the ring of 2×2 matrices over k with $\alpha^2 = \beta^2 = 1$, where

$$\alpha := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \beta := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \alpha\beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \beta\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Endomorphism algebra classification theorem

Theorem

Let E/k be an elliptic curve. Then $\mathrm{End}^0(E)$ is isomorphic to one of the following:

- *the field of rational numbers $\mathbb{Q}$;*
- *an imaginary quadratic field $\mathbb{Q}(\alpha)$ with $\alpha^2 < 0$;*
- *a quaternion algebra $\mathbb{Q}(\alpha, \beta)$ with $\alpha^2, \beta^2 < 0$.*

Proof: To the blackboard!

Definition

An elliptic curve with $\mathrm{End}^0(E) \neq \mathbb{Q}$ is said to have complex multiplication.

Orders in $\mathbb{Q}$-algebras

Definition

Let K be a $\mathbb{Q}$-algebra of finite dimension r as a $\mathbb{Q}$-vector space.
A subring $\mathcal{O}$ of K is an order in K if is a free $\mathbb{Z}$-module of rank r.
Equivalently, $\mathcal{O}$ is a finitely generated as a $\mathbb{Z}$-module with $K = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Example

$\mathbb{Z}$ is an order in $\mathbb{Q}$, but $2\mathbb{Z}$ and $\{a/2^n : a, n \in \mathbb{Z}\} \subseteq \mathbb{Q}$ are not orders in $\mathbb{Q}$.

Corollary

The endomorphism ring $\mathrm{End}(E)$ *is an order in* $\mathrm{End}^0(E)$*.*

Proof: To the blackboard!

Orders in number fields

Definition

An algebraic number $\alpha \in \mathbb{C}$ is any root of a polynomial with coefficients in $\mathbb{Z}$.
An algebraic integer $\alpha \in \mathbb{C}$ is any root of a monic polynomial with coefficients in $\mathbb{Z}$.
The algebraic integers form a ring $\overline{\mathbb{Z}}$.

Definition

A number field K is a finite extension of $\mathbb{Q}$. Its ring of integers $\mathcal{O}_K$ is the ring $K \cap \overline{\mathbb{Z}}$, which is a free $\mathbb{Z}$-module of rank $\dim_{\mathbb{Q}} K$, hence an order in K. Moreover, it is the unique maximal order in K.

Theorem

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. The orders in K are precisely the subrings $\mathbb{Z} + f\mathcal{O}_K$ with $f \in \mathbb{Z}_{>0}$.

Proof: See notes.