How to find endomorphism ring of an isogenous elliptic curve

[+2] [1] samething

[2024-12-20 16:15:43]

[elliptic-curves noncommutative-rings isogenies]

[https://mathoverflow.net/questions/484539/how-to-find-endomorphism-ring-of-an-isogenous-elliptic-curve]

I have a supersingular elliptic curve E with a known endomorphism ring $\mathrm{End}(E)$. I'd like to find an isogeny $\varphi : E \to E'$, and by Deuring correspondence I know the corresponding ideal I_φ in quaternion algebra. How could I find the endomorphism ring of E' in this case?

What do you mean by "finding" the endomorphism ring? Is it enough to determine the isomorphism type (e.g. as a set of elements in the quaternion algebra containing $\mathrm{End}(E)$), or do you need some an explicit description of the endomorphisms generating $\mathrm{End}(E')$ (e.g. rational functions in the coordinates of E')? And likewise, what data do we have about each of $\mathrm{End}(E)$, φ, and I_φ? - **Jonathan Love**

For a preliminary answer: working in the quaternion algebra B, if $\mathrm{End}(E)$ is the *right-order* of I_φ (the set of all $\alpha \in B$ such that if $f \in I_\varphi$ then $f \cdot \alpha \in I_\varphi$) then $\mathrm{End}(E')$ will be isomorphic to the *left-order* of I_φ (the set of all $\alpha \in B$ such that if $f \in I_\varphi$ then $\alpha \cdot f \in I_\varphi$). These are not equal because B is not commutative. So if you're given I_φ as a subset of B then it's quite straightforward to compute a ring isomorphic to $\mathrm{End}(E')$. - **Jonathan Love**

Your formulation is unclear to me. What is given to you as input? I_φ? E'? It makes a big difference. Could you please clarify? - **Aurel**

I have an elliptic curve E and I know it's endomorphism ring. For example: $E : y^2 = x^3 + x$ over $\mathbb{F}_p,\ p \equiv 3 \bmod 4$. It is known that the endomorphism ring is isomorphic to the following order $\mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$. Then I choose some ideal I_φ which is equal to an isogeny $\varphi : E \to E'$ (according to Deuring correspondence) and find it. I'd like to understand how, in this case, I could find the endomorphism ring of E' using the information above. - **samething**

So the known parameters are: $E(\mathbb{F}_p), E', \mathrm{End}(E) \cong \mathcal{O}_0, \varphi : E \to E', I_\varphi$. I'd like to find $\mathrm{End}(E')$. - **samething**

Then the answer is in Jonathan Love's second comment: $\mathrm{End}(E')$ is the left order of I_φ. - **Aurel**

[+3] [2024-12-21 04:16:59] Jonathan Love [✔ACCEPTED]

Moving this from a comment to an answer since it seems that this might be what you're looking for. I'm also using this opportunity to switch right vs left - it is just a convention (do you define the multiplication $a \cdot b$ in the quaternion algebra to correspond to the composition $a \circ b$ or $b \circ a$ in the endomorphism ring) but in my comment I used the less natural choice. In what follows $a \cdot b$ corresponds to $a \circ b$.

Let B be the unique quaternion algebra ramified at p and ∞. The endomorphism ring $\mathrm{End}(E)$ is isomorphic to some maximal order $\mathcal{O} \subseteq B$. To any isogeny $\varphi : E \to E'$ we can associate a *left* $\mathcal{O}$-ideal $I_\varphi \subseteq \mathcal{O}$ as the image of $\mathrm{Hom}(E', E)$ in $\mathcal{O}$ under the pullback map $\psi \mapsto \psi \circ \varphi$. Note that this is indeed a left $\mathcal{O}$-ideal because if $\alpha \in \mathrm{End}(E)$ and $\psi \circ \varphi \in I_\varphi$ then $(\alpha \circ \psi) \circ \varphi \in I_\varphi$.

Given this setup, $\mathrm{End}(E')$ is isomorphic to the *right* order $\mathcal{O}'$ of I_φ. In fact, we have an explicit isomorphism $\mathrm{End}(E') \to \mathcal{O}'$ given by

$$\beta \mapsto \frac{1}{\deg \varphi}(\phi^\vee \circ \beta \circ \phi).$$

To see that $\mathcal{O}'$ is indeed a right order, if $\beta \in \mathrm{End}(E')$ and $\psi \circ \phi \in I_\varphi$ then

$$(\psi \circ \phi) \cdot \left(\frac{1}{\deg \varphi}(\phi^\vee \circ \beta \circ \phi) \right) = \frac{1}{\deg \phi}(\psi \circ \varphi \circ \varphi^\vee \circ \beta \circ \varphi) = (\psi \circ \beta) \circ \varphi \in I_\varphi$$

showing that I_φ is closed under multiplication by elements of $\mathcal{O}'$ on the right.

To summarize: if you are given a maximal order $\mathcal{O} \simeq \mathrm{End}(E)$, and a left $\mathcal{O}$-ideal I_φ corresponding to $\varphi : E \to E'$, then you can recover $\mathrm{End}(E')$ up to isomorphism by computing the right order of I_φ, that is, the set of all elements $b \in B$ such that $I_\varphi b \subseteq I_\varphi$.

One possible reference is John Voight's *Quaternion Algebras* Section 42.2.