Sist: Viste, ved hjelp av Tate-modulen, at $\mathrm{Hom}(E_1, E_2)$, og spesielt $\mathrm{End}(E)$, er på formen $\mathbb{Z}^n$ for $n \geq 4$.

I dag: Hva er den multiplikative strukturen til ringen $\mathrm{End}(E)$?

Vi vet en hel del om ringen $\mathrm{End}(E)$.

- $\mathrm{End}(E) \cong \mathbb{Z}^n$, $n \leq 4$ som gruppe
- For $0 \neq \phi, \psi \in \mathrm{End}(E)$, har vi $\phi\psi \neq 0$
- Vi har operasjonen $\phi \mapsto \hat{\phi}$, som tilfredsstiller:
  - Linearitet: $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$
  - Anti-multiplikativitet: $\widehat{\phi\psi} = \hat{\psi}\hat{\phi}$
  - Den er en *involusjon*: $\hat{\hat{\phi}} = \phi$
  - For alle ϕ er $\phi\hat{\phi} = \hat{\phi}\phi = n$, hvor $n = \deg \phi \geq 0$ er et heltall.

Kandidatringer

Hva kan $\mathrm{End}(E)$ nå potensielt være?

Trivielt eksempel: $\mathrm{End}(E) = \mathbb{Z}$, $\phi \mapsto \hat{\phi}$ er identiteten.

Ordener. La $\mathcal{K}$ være en endelig-dimensjonal (muligens ikkekommutativ) $\mathbb{Q}$-algebra. En *orden* $\mathcal{R}$ i $\mathcal{K}$ er en underring som er endelig generert som gruppe, og slik at $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Eksempel: $\mathbb{Z}$ er en orden i $\mathbb{Q}$.

Kvadratiske kropper: En *kvadratisk kropp* er en utvidelse av $\mathbb{Q}$ på formen $\mathbb{Q}(\sqrt{d})$, hvor d er et heltall. For alle heltall $k > 0$ er ringen

$$\mathcal{R} = \{x + yk\sqrt{d} \mid x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{d})$$

en orden i $\mathbb{Q}(\sqrt{d})$.

Definer involusjonen $X \mapsto \hat{X}$, $X \in \mathcal{R}$, ved $x + y\sqrt{d} \mapsto x - y\sqrt{d}$. Da er $X\hat{X} = x^2 - dy^2$, så hvis $d < 0$, tilfredsstiller $\mathcal{R}$ alt vi vet om $\mathrm{End}(E)$, og er en kandidat.

Kvaternioniske algebraer: En *kvaternionisk algebra* (over $\mathbb{Q}$) er en algebra $\mathcal{K}$ med basis $1, \alpha, \beta, \gamma$ som tilfredsstiller $\alpha^2, \beta^2 \in \mathbb{Q}$, og videre

$$\alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta,$$

dette er nok til å bestemme strukturen til algebraen. Vi setter $\alpha^2 = a$ og $\beta^2 = b$, og skriver $\mathcal{K}(a, b)$ for denne algebraen.

For alle $a, b < 0$ har vi at $\mathcal{K}(a, b) \otimes_{\mathbb{Q}} \mathbb{R}$ er isomorf med den "vanlige" kvaternionringen, altså ringen

$$K = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

$$\text{med relasjoner } i^2 = j^2 = k^2 = ijk = -1$$

Hvis $a = b = -1$ setter vi $\alpha = i, \beta = j, \gamma = k$. Generelt kan vi reskalere α, β for å få en isomorfi.

Hvis $a, b \in \mathbb{Z}$, så får vi ordenen

$$\mathcal{R}(a,b) = \{x + y\alpha + z\beta + w\alpha\beta \mid x, y, z, w \in \mathbb{Z}\} \subset \mathcal{K}(a,b).$$

Definerer, for alle $X = x + y\alpha + z\beta + w\alpha\beta \in \mathcal{K}(a,b)$, at $\hat{X} = x - y\alpha - z\beta - w\alpha\beta$. Hvis $X \in \mathcal{R}(a,b)$, så blir da

$$X\hat{X} = -\hat{X}X = x^2 - ay^2 - bz^2 + abw^2 \in \mathbb{Z}_{\geq 0}.$$

så $\mathcal{R}(a,b)$ er en kandidat for $\mathrm{End}(E)$.

Teorem. *Ringen* $\mathrm{End}(E)$ *er en av følgende tre typer ringer:*

(1) $\mathbb{Z}$

(2) En orden i $\mathbb{Q}(\sqrt{d})$ *hvor* $d < 0$

(3) En orden i en kvaternioniske algebra $\mathcal{K}(a,b)$

Merknad. Som gruppe har vi altså $\mathrm{End}(E) = \mathbb{Z}, \mathbb{Z}^2$ eller $\mathbb{Z}^4$.

Merknad. Hvis $\mathrm{End}(E)$ er kommutativ (som vi skal se gjelder dette alltid når $\mathrm{char}\, K = 0$), så er $\mathrm{End}(E)$ enten (1) eller (2), og vice versa, hvis $\mathrm{End}(E)$ er ikke-kommutativ så er $\mathrm{End}(E)$ tilfelle (3).

Bevis. La $\mathcal{K} = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Per definisjon er $\mathrm{End}(E)$ en orden i $\mathcal{K}$, så det holder å finne ut hva slags ring $\mathcal{K}$ er. Vi vet at $1 \leq \dim_{\mathbb{Q}} \mathcal{K} \leq 4$, og vi utvider involusjonen $\phi \mapsto \hat{\phi}$ på $\mathrm{End}(E)$ lineært til en involusjon $X \mapsto \hat{X}$ på $\mathcal{K}$.

Hvis $\mathcal{K} = \mathbb{Q}$, så må $\mathbb{Z} \subset \mathrm{End}(E) \subset \mathbb{Q}$. Hvis $\mathbb{Z} \neq \mathrm{End}(E)$, så finnes en $\frac{a}{b} \in \mathrm{End}(E) \setminus \mathbb{Z}$, men da inneholder $\mathrm{End}(E)$ også $\frac{a^n}{b^n}$ for alle n, som er umulig siden $\mathrm{End}(E)$ er endeliggenerert som gruppe.[1]

Så anta at $\mathbb{Q} \subsetneq \mathcal{K}$. For $X \in \mathcal{K}$, definer *normen* $N(X) = X\hat{X}$, hvor $N(X) \in \mathbb{Q}_{\geq 0}$ med $N(X) = 0$ hvis og bare hvis $X = 0$. Definer *trasen* $T(X) = X + \hat{X}$.

Hvis $x \in \mathbb{Q} \subset \mathcal{K}$, har vi $\hat{x} = x$, så

$$N(x) = x^2 \quad T(x) = 2x.$$

Følgende triks viser at vi alltid har $T(X) \in \mathbb{Q}$:

$$N(X+1) = (X+1)(\widehat{X+1}) = X\hat{X} + X + \hat{X} + 1 = N(X) + T(X) + 1,$$

så

$$T(X) = N(X+1) - N(X) - 1 \in \mathbb{Q}$$

La $\alpha \in \mathcal{K} \setminus \mathbb{Q}$. Bytter vi α med $\alpha - \frac{1}{2}T(\alpha)$, så får vi at

$$T(\alpha) = T(\alpha) - T\left(\frac{1}{2}T(\alpha)\right) = 0.$$

Dermed har vi $\hat{\alpha} = -\alpha$, og slik at

$$\alpha^2 = -\alpha\hat{\alpha} = -N(\alpha) \in \mathbb{Q}_{<0}$$

[1] Dette avsnittet viser egentlig at $\mathbb{Z}$ er den eneste ordenen i $\mathbb{Q}$.

Så $\alpha^2 = a \in \mathbb{Q}$, med $a < 0$. Hvis $\dim_{\mathbb{Q}} \mathcal{K} = 2$ er vi nå ferdige, og har vist at $\mathcal{K} = \mathbb{Q}(\sqrt{a})$.

Hvis $\dim_{\mathbb{Q}} \mathcal{K} > 2$, så finnes en $\beta \in \mathcal{K} \setminus \mathbb{Q}(\alpha)$. Bytter vi nå ut β med $\beta - \frac{1}{2}T(\beta) - \frac{T(\alpha\beta)}{2\alpha^2}\alpha$, så får vi etter litt regning at

$$T(\beta) = T(\alpha\beta) = 0.$$

På samme måte som med α har vi at

$$T(\beta) = 0 \Rightarrow \beta = -\hat{\beta} \Rightarrow \beta^2 = -\beta\hat{\beta} = -N(\beta) \in \mathbb{Q}_{<0}$$

Nå har vi vist at $\alpha^2, \beta^2 \in \mathbb{Q}_{<0}$, og

$$\beta\alpha = (-\beta)(-\alpha) = \hat{\beta}\hat{\alpha} = \widehat{\alpha\beta} = -\alpha\beta,$$

hvor siste ligning bruker $T(\alpha\beta) = 0$. Altså har vi vist at ligningene for en kvaternionisk algebra er tilfredssstilt.

Hvis vi kan vise at $\alpha\beta$ er lineært uavhengig av $1, \alpha, \beta$, så utgjør $1, \alpha, \beta, \alpha\beta$ en basis for $\mathcal{K}$, siden $\dim_{\mathbb{Q}} \mathcal{K} \leq 4$, og dermed er da $\mathcal{K}$ en kvaternionisk algebra.

For å se dette, la x, y, z, w være slik at

$$X = x + y\alpha + z\beta + w\alpha\beta = 0.$$

Da er $T(X) = 2x = 0$, så $x = 0$. Videre er $\alpha X \beta = (y\alpha^2)\beta + (z\beta^2)\alpha + w\alpha^2\beta^2 = 0$. Vi vet at $1, \alpha, \beta \in \mathcal{K}$ er lineært uavhengige siden $\beta \notin \mathbb{Q}(\alpha$. Dermed er

$$y\alpha^2 = z\beta^2 = w\alpha^2\beta^2 = 0,$$

og altså er $y = z = w = 0$. □

Automorfier

La $\phi\colon E \to E$ være en *automorfi* av elliptiske kurver (så vi krever at $\phi(O) = O$). Da er spesielt ϕ et inverterbart element i $\mathrm{End}(E)$. Men vi har faktisk mye bedre kontroll over automorfier enn over hele $\mathrm{End}(E)$.

Husk at vi tidligere har vist at for to kurver på Weierstrass-form

$$E_1\colon y^2 = x^3 + A_1x + B_1 \qquad E_2\colon y^2 = x^3 + A_2x + B_2,$$

så kan enhver isomorfi skrives som $\phi_u\colon E_1 \to E_2$, for en $u \in \overline{K}^*$, hvor

$$\phi_u(x, y) = (u^2x, u^3y).$$

Morfien ϕ_u er bare veldefinert hvis den faktisk sender punkter i E_1 til E_2, som er det samme som å si at $(x, y) \mapsto (u^2x, u^3y)$ transformerer ligning 2 til ligning 1:

$$\begin{aligned}(u^3y)^2 &= (u^2x)^3 + A_2(u^2x) + B_2\\ u^6y^2 &= u^6x^3 + u^2A_2x + B_2\\ y^2 &= x^3 + u^{-4}A_2x + u^{-6}B_2,\end{aligned}$$

altså hvis $A_1 = u^{-4}A_2$ og $B_1 = u^{-6}B_2$.

La nå E være gitt ved $y^2 = x^3 + Ax + B$. Hvis $u \in \overline{K}^*$ er slik at $u^4A = A$ og $u^6B = B$, så er $\phi_u\colon E \to E$ som over en isomorfi, og det er lett å se at $\phi_{u_1u_2} = \phi_{u_1}\phi_{u_2}$.

Dermed har vi en gruppeisomorfi

$$\mathrm{Aut}(E) = \{u \in \overline{K}^* \mid A = u^4 A, B = u^6 B\}.$$

Tre tilfeller:

Hvis $A, B \neq 0$, så er $u^4 = u^6 = 1$, altså er $u^2 = 1$, så $\mathrm{Aut}(E) \cong \mathbb{Z}/2$.

Hvis $A = 0$, $B \neq 0$, får vi at $u^6 = 1$, så $\mathrm{Aut}(E) \cong \mathbb{Z}/6$ (dette tilsvarer $j(E) = 0$).

Hvis $A \neq 0$, $B = 0$, får vi at $u^4 \cong 1$, så $\mathrm{Aut}(E) \cong \mathbb{Z}/4$ (dette tilsvarer $j(E) = 1728$).