# Elliptic curves and the Hesse pencil

Ane Anema

RUG

28 November 2013

# Outline

# Galois representations on 3-torsion

- Let $k$ be a perfect field of $\mathrm{char}\,(k) \neq 2, 3$.
- Denote the absolute Galois group of $k$ by $G_k$.
- Given an elliptic curve $E$ defined over $k$, the action of $G_k$ on the coordinates of the points of $E$ induces

$$\rho : G_k \to \mathrm{Aut}\,(E\,[3]),$$

that is, $E\,[3]$ is a $G_k$-module.

# The Hesse pencil of a cubic curve

- Consider $E = Z(F)$ with $F \in k[X, Y, Z]_{\text{hom}}$ and $\deg F = 3$.
- Define the *Hessian* of $F$ as

$$\operatorname{Hess}(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}.$$

- The *Hesse pencil* of $E$ is defined as

$$\mathcal{E} = Z(tF + \operatorname{Hess}(F))$$

  over $k(t)$.
- Denote the member of $\mathcal{E}$ at $t_0 \in \mathbb{P}^1(k)$ by $E_{t_0}$, i.e.

$$E_{t_0} = \begin{cases} Z(F) & \text{if } t_0 = \infty, \\ Z(t_0 F + \operatorname{Hess}(F)) & \text{otherwise.} \end{cases}$$

**Theorem**

*If $E$ and $E'$ are elliptic curves given by some Weierstrass equation defined over $k$, then the following two statements are equivalent:*

1. $E' \cong_k E_{t_0}$ *for some* $t_0 \in \mathbb{P}^1(k)$,
2. *there exists a* $G_k$*-module isomorphism* $E[3] \to E'[3]$ *respecting the Weil-pairings.*

- Related to earlier results by:
  - K. Rubin and A. Silverberg (1993),
  - T.A. Fisher (2012),
  - M. Kuwata (2012).

# Outline

# Flex points

- A point $P$ on $E$ is called a *flex point* if there is a line $L$ which intersects $E$ at $P$ with multiplicity $\geq 3$.

**Proposition**

*If $P \in E$ and $\operatorname{char}(k) \neq 2$, then*

$$P \text{ flex point} \iff P \in Z(\operatorname{Hess}(F)).$$

**Corollary**

*If $P \in E$ is a flex point, then $P \in \mathcal{E}$ and is again a flex point.*

- Use

$$\operatorname{Hess}(tF + \operatorname{Hess}(F)) = \alpha F + \beta \operatorname{Hess}(F)$$

for some $\alpha, \beta \in k[t]$.

# 3-torsion points

- Let $E = Z(F)$ with $F \in k[X, Y, Z]_{\text{hom}}$ and $\deg F = 3$ be an elliptic curve with unit element $O$.

**Proposition**

*Let $S, T \in E$. If $S$ is a flex point, then*

$$T \text{ flex point} \iff S - T \in E[3].$$

- From now on assume that $O$ is a flex point, then
  - $O$ is a flex point on $\mathcal{E}$,
  - choose $O$ as the unit element of $\mathcal{E}$,
  - a flex point on $E$ is a 3-torsion point on $E$,
  - so $E[3] \subset \mathcal{E}[3]$,
  - in fact $E[3] = \mathcal{E}[3]$ since $\operatorname{char}(k) \neq 3$,
  - as groups as well.
- Also $E[3] = E_{t_0}[3]$ for all $t_0 \in \mathbb{P}^1(k)$ for which $E_{t_0}$ is non-singular.

# The Weil-pairing

- Let $e_3$ and $e_3^{t_0}$ be the Weil-pairings on the 3-torsion of $\mathcal{E}$ and $E_{t_0}$.

## Proposition

*If $O$ is a flex point, then $e_3 = e_3^{t_0}$ on $E[3]$.*

- Let $S, T \in \mathcal{E}[3]$ such that $\mathcal{E}[3] = \langle S, T \rangle$.
- Denote the tangent line to $\mathcal{E}$ at $P$ by $L_P$.
- Via $D_S = (S) - (O)$ and $D_T = 2(T) - 2(-T)$ obtain

$$e_3(S, T) = \left( \frac{L_S(T) L_O(-T) L_T(O) L_{-T}(S)}{L_O(T) L_S(-T) L_{-T}(O) L_T(S)} \right)^2 .$$

- Let $s \in \overline{k}(t)$ be a local coordinate at $t_0$.
- The line $L_O$ modulo $s$ is the tangent line to $E_{t_0}$ at $O$.
- Construct $e_3^{t_0}(S, T)$ as above.

# Outline

- Let $E$ and $E'$ be elliptic curves given by a Weierstrass equation defined over $k$.

### Proposition

*If $\phi : E[3] \to E'[3]$ is an isomorphism which respects the Weil-pairings, then there exists a linear change of coordinates $\Phi : E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(\overline{k})$ such that $\Phi|_{E[3]} = \phi$.*

# Hesse pencil in Weierstrass form

## Lemma

*Let* $E = Z\left(x^3 + axz^2 + bz^3 - y^2z\right)$ *be an elliptic curve. The linear change of coordinates*

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix} \quad \textit{with} \quad A = \begin{pmatrix} t & 0 & 3at^2 - 27bt - 9a^2 \\ 0 & 1 & 0 \\ -3 & 0 & t^3 + 9at - 27b \end{pmatrix}$$

*transforms* $\mathcal{E}$ *into* $\mathcal{E}^W = Z\left(\xi^3 + a_t\xi\zeta^2 + b_t\zeta^3 - \eta^2\zeta\right)$ *with*

$$a_t = at^4 + \ldots \qquad \textit{and} \qquad b_t = bt^6 + \ldots .$$

*Moreover* $\Delta\left(\mathcal{E}^W\right) = \Delta(E)\left(\det A\right)^3$ *with*

$$\det A = t^4 + 18at^2 - 108bt - 27a^2.$$

# Proof of the proposition

- Let $j_0$ and $j_0'$ be the $j$-invariants of $E$ and $E'$.
- Assume that $j_0' \neq j_0, 0, 1728$.
- For which $t_i \in \mathbb{P}^1\left(\overline{k}\right)$ is $j\left(E_{t_i}\right) = j_0'$?
  - Precisely for the zeros of the polynomial

$$G = -1728\left(4a_t\right)^3 - j_0'\Delta\left(\mathcal{E}^W\right) = \left(j_0 - j_0'\right)\Delta\left(E\right)\ t^{12} + \ldots$$

  - It has discriminant

$$-3^{147}{j_0'}^8\left(j_0' - 1728\right)^6\Delta\left(E\right)^{44}.$$

  - Thus $G$ has precisely 12 zeros.
- Define

$$\phi_{i,\sigma} = \sigma \circ \Psi_i \circ A_i|_{E_{t_i}[3]} : E\left[3\right] \to E'\left[3\right]$$

for every $i = 1, \ldots, 12$ and $\sigma \in \mathrm{Aut}\left(E'\right)$, where
  - $A_i : E_{t_i} \to E_{t_i}^W$ is induced by $A : \mathcal{E} \to \mathcal{E}^W$,
  - $\Psi_i : E_{t_i}^W \to E'$ an isomorphism.

# Linear change of coordinates and 3-torsion (intermezzo)

**Lemma**

*If* $E[3] = \langle S, T \rangle$ *and* $E'[3] = \langle S', T' \rangle$, *then* $\exists!\, A \in \mathrm{PGL}_3\left(\overline{k}\right)$ *such that*

$$O \mapsto O', \quad S \mapsto S', \quad T \mapsto T', \quad S + T \mapsto S' + T'.$$

- No three of $O, S, T, S + T$ are collinear:
  - Suppose that $O$, $S$ and $T$ are contained in some line $L$, then

$$\operatorname{div}\left(\frac{L}{L_O}\right) = (O) + (S) + (T) - 3\,(O),$$

so $S + T = O$ in $E$, which is impossible.

- No three of $O', S', T', S' + T'$ are collinear.
- Hence such a $A$ exists.

# Proof of the proposition (continued)

- Suppose that $\phi_{i,\sigma} = \phi_{j,\tau}$, then
  - previous lemma implies $\sigma \circ \Psi_i \circ A_i = \tau \circ \Psi_j \circ A_j$
  - members of $\mathcal{E}$ only have 3-torsion points in common, so $i = j$,
  - $A_i$ and $\Psi_i$ are isomorphisms, therefore $\sigma = \tau$.
- The $\phi_{i,\sigma}$ respect the Weil-pairings,
- There are $12 \cdot \#\mathrm{Aut}\left(E'\right) = 24$ distinct $\phi_{i,\sigma}$'s.

**Lemma**

*Of the 48 isomorphisms $E\left[3\right] \to E'\left[3\right]$, 24 respect the Weil-pairings.*

- Hence $\phi = \phi_{i,\sigma}$ for some $i = 1, \ldots, 12$ and $\sigma \in \mathrm{Aut}\left(E'\right)$.

# Outline

# Proof of the theorem ($\Longrightarrow$)

- Assume that there exists an isomorphism $\Phi : E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(k)$ defined over $k$, then

$$\Phi|_{E_{t_0}[3]} : E_{t_0}[3] \to E'[3].$$

  is a $G_k$-module isomorphism and respects the Weil-pairings.
- $E[3] = E_{t_0}[3]$ as groups with identical Weil-pairings.
- Hence $\phi = \Phi|_{E_{t_0}[3]}$ is the map we want.

# Proof of the theorem ($\Longleftarrow$)

- Suppose that there exists a $G_k$-module isomorphism $\phi : E[3] \to E'[3]$ respecting the Weil-pairings.
- There exists a linear isomorphism $\Phi : E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(\overline{k})$ with $\Phi|_{E[3]} = \phi$,
- Now

$$\sigma(\Phi)(\sigma(S)) = \sigma \circ \Phi(S) = \sigma \circ \phi(S) = \phi \circ \sigma(S) = \Phi(\sigma(S))$$

for all $S \in E[3]$ and $\sigma \in G_k$, so $\sigma(\Phi) = \Phi$ for all $\sigma \in G_k$.

**Lemma**

*Since $k$ is a perfect field,* $\mathrm{PGL}_3(\overline{k})^{G_k} = \mathrm{PGL}_3(k)$.

- Hence $\Phi \in \mathrm{PGL}_3(k)$, that is $\Phi : E_{t_0} \to E'$ is defined over $k$.