Hessians, automorphisms of p-groups, and torsion points of elliptic curves

Mima Stanojkovski, joint with C. Voll

Max-Planck-Institut für
Mathematik
in den Naturwissenschaften

Women in Algebra and Symbolic Computations

11th December 2019

MAX-PLANCK-GESELLSCHAFT

MOTIVATION

How did we end up with such a cocktail?

- Understanding the symmetries of an (algebraic) object, helps understanding the object itself; also holds for groups

- Understanding the symmetries of an (algebraic) object, helps understanding the object itself; also holds for groups
- Finite groups are understood (externally) via their composition factors and (internally) via their Sylows; reduction to p-groups

- Understanding the symmetries of an (algebraic) object, helps understanding the object itself; also holds for groups
- Finite groups are understood (externally) via their composition factors and (internally) via their Sylows; reduction to p-groups
- In the study of p-groups it is often beneficial to look at groups in natural families, i.e. $\mathbf{G}(\mathbb{F}_p)$ or $\mathbf{G}(\mathbb{F}_{p^r})$; interplay between geometry of $\mathbf{G}$ and properties of $\mathbf{G}(\mathbb{F}_p)$

- Understanding the symmetries of an (algebraic) object, helps understanding the object itself; also holds for groups
- Finite groups are understood (externally) via their composition factors and (internally) via their Sylows; reduction to p-groups
- In the study of p-groups it is often beneficial to look at groups in natural families, i.e. $\mathbf{G}(\mathbb{F}_p)$ or $\mathbf{G}(\mathbb{F}_{p^r})$; interplay between geometry of $\mathbf{G}$ and properties of $\mathbf{G}(\mathbb{F}_p)$

This is one of those stories, where $\mathbf{G}$ is defined starting from

"Hessian matrices encoding elliptic curves"

- Understanding the symmetries of an (algebraic) object, helps understanding the object itself; also holds for groups
- Finite groups are understood (externally) via their composition factors and (internally) via their Sylows; reduction to p-groups
- In the study of p-groups it is often beneficial to look at groups in natural families, i.e. $\mathbf{G}(\mathbb{F}_p)$ or $\mathbf{G}(\mathbb{F}_{p^r})$; interplay between geometry of $\mathbf{G}$ and properties of $\mathbf{G}(\mathbb{F}_p)$

This is one of those stories, where $\mathbf{G}$ is defined starting from

"Hessian matrices encoding elliptic curves"

What about the torsion points?

GROUPS AND ALGEBRAS FROM MATRICES

A general construction for class at most 2

Ingredients:

- K field
- $\phi : K^d \times K^e \to K^f$ given by $B \in \mathrm{Mat}_{d\times e}(K[x_1, \ldots, x_f])$ via

$$(u, w) \mapsto \phi(u, w) = uBw^{\mathrm{t}}$$

- $V = K^d \times K^e \times K^f$

Ingredients:

- K field
- $\phi : K^d \times K^e \to K^f$ given by $B \in \mathrm{Mat}_{d\times e}(K[x_1, \ldots, x_f])$ via

$$(u, w) \mapsto \phi(u, w) = uBw^{\mathrm{t}}$$

- $V = K^d \times K^e \times K^f$

Cook-ups:

- a group $G = G_B(K) = (V, \star)$ by

$$(u, w, t) \star (u', w', t') = (u + u', w + w', t + t' + \phi(u, w'))$$

- a K-Lie algebra $L = L_B(K) = (V, [\,,\,])$ by

$$[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w) \in K^f$$

Abelian groups

Assume $B = 0$. Then $G \cong K^{d+e+f}$ with the natural operation.

Abelian groups

Assume $B = 0$. Then $G \cong K^{d+e+f}$ with the natural operation.

The Heisenberg group

Assume $d = e = f = 1$ and $B = (x)$. Then

$$G \cong \begin{pmatrix} 1 & K & K \\ 0 & 1 & K \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{Heis}(K).$$

Abelian groups

Assume $B = 0$. Then $G \cong K^{d+e+f}$ with the natural operation.

The Heisenberg group

Assume $d = e = f = 1$ and $B = (x)$. Then

$$G \cong \begin{pmatrix} 1 & K & K \\ 0 & 1 & K \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{Heis}(K).$$

For $d = e$ and $f = 1 \rightsquigarrow$ Higher-dimensional Heisenberg group.

For $K = \mathbb{F}_p$ and p odd, extraspecial groups of exponent p.

Exercise: determine L.

Identities in the group

- $\mathrm{id} = (0, 0, 0)$
- $(u, w, t)^{-1} = (-u, -w, -t + \phi(u, w))$
- $[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w) \in K^f$

Identities in the group

- $\mathrm{id} = (0, 0, 0)$
- $(u, w, t)^{-1} = (-u, -w, -t + \phi(u, w))$
- $[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w) \in K^f$

For $K = \mathbb{F}_{p^r}$ and $p \neq 2$, then G is a p-group and $\exp(G) = p$.

Identities in the group

- $\mathrm{id} = (0, 0, 0)$
- $(u, w, t)^{-1} = (-u, -w, -t + \phi(u, w))$
- $[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w) \in K^f$

For $K = \mathbb{F}_{p^r}$ and $p \neq 2$, then G is a p-group and $\exp(G) = p$.

Groups and algebras

Recall: $V = K^d \times K^e \times K^f$

- K^f is central in G resp. in L
- G resp. L is nilpotent of class at most 2
- "in some cases L can be recovered from G and viceversa"

AUTOMORPHISMS OF GROUPS

A recipe for symmetric matrices

AUTOMORPHISMS OF ~~GROUPS~~ LIE ALGEBRAS

A recipe for symmetric matrices

Let $d = e = f = 3$ and

$$B_{1,1} = \begin{pmatrix} z & -x & y \\ -x & z & 0 \\ y & 0 & -x \end{pmatrix}.$$

Let $d = e = f = 3$ and

$$B_{1,1} = \begin{pmatrix} z & -x & y \\ -x & z & 0 \\ y & 0 & -x \end{pmatrix}.$$

and get, for each odd prime p, the group $G_{1,1}(p) = G_{B_{1,1}}(\mathbb{F}_p)$ and the algebra $L_{1,1}(p) = L_{B_{1,1}}(\mathbb{F}_p)$.

Then $|G_{1,1}(p)| = |L_{1,1}(p)| = p^9$ and $\exp(G_{1,1}(p)) = p$.

Let $d = e = f = 3$ and

$$B_{1,1} = \begin{pmatrix} z & -x & y \\ -x & z & 0 \\ y & 0 & -x \end{pmatrix}.$$

and get, for each odd prime p, the group $G_{1,1}(p) = G_{B_{1,1}}(\mathbb{F}_p)$ and the algebra $L_{1,1}(p) = L_{B_{1,1}}(\mathbb{F}_p)$.

Then $|G_{1,1}(p)| = |L_{1,1}(p)| = p^9$ and $\exp(G_{1,1}(p)) = p$.

Note: $\det(B) = -z^2x - y^2z + x^3$ and so $\det(B) = 0$ describes the elliptic curve

$$E: \quad y^2 = x^3 - x.$$

Let V_p be the number of points $(x, y) \in E(\mathbb{F}_p)$ such that

$$x^4 + 6x^2 - 3 = 0.$$

Theorem (du Sautoy, Vaughan-Lee, 2012)

$$|\operatorname{Aut}(G_{1,1}(p))| = \begin{cases} 4p^{18}|\operatorname{GL}_2(\mathbb{F}_p)| & \text{if } p \equiv 1 \bmod 12,\ V_p = 0, \\ 36p^{18}|\operatorname{GL}_2(\mathbb{F}_p)| & \text{if } p \equiv 1 \bmod 12,\ V_p \neq 0, \\ 6p^{18}|\operatorname{GL}_2(\mathbb{F}_p)| & \text{if } p \equiv -1 \bmod 12, \\ 4p^{18}|\operatorname{GL}_2(\mathbb{F}_p)| & \text{if } p \equiv 5 \bmod 12, \\ 2p^{18}|\operatorname{GL}_2(\mathbb{F}_p)| & \text{if } p \equiv 7 \bmod 12. \end{cases}$$

Connection to Higman's famous PORC conjecture: potential evidence against it?

Question

What is the actual role of the elliptic curve E in the structure of $\mathrm{Aut}(G_{1,1}(\mathbb{F}_p))$?

Question

What is the actual role of the elliptic curve E in the structure of $\mathrm{Aut}(G_{1,1}(\mathbb{F}_p))$?

Theorem (S., Voll '19+)

$$|\mathrm{Aut}(G_{1,1}(p))| = \gcd\{p-1, 4\} \cdot |E[3](\mathbb{F}_p)| \cdot |\mathrm{GL}_2(\mathbb{F}_p)| \cdot p^{18}$$

Question

What is the actual role of the elliptic curve E in the structure of $\mathrm{Aut}(G_{1,1}(\mathbb{F}_p))$?

Theorem (S., Voll '19+)

$$|\mathrm{Aut}(G_{1,1}(p))| = \gcd\{p-1,4\} \cdot |E[3](\mathbb{F}_p)| \cdot |\mathrm{GL}_2(\mathbb{F}_p)| \cdot p^{18}$$

Remarks

- $\gcd\{p-1,4\} = |\mu_4(\mathbb{F}_p)| = |\mathrm{Aut}(E)(\mathbb{F}_p)|$
- $E[3]$ denotes the 3-torsion of E and corresponds to the translations of E that are realizable in $\mathrm{PGL}_3(\mathbb{F}_p)$

We show that

$$|\operatorname{Aut}(G_{1,1}(p))| \overset{\text{Lazard}}{=} |\operatorname{Aut}(L_{1,1}(p))| = |\operatorname{Im}\bar{c}| \cdot |\operatorname{GL}_2(\mathbb{F}_p)| \cdot |\mathbb{F}_p|^{18}$$

where

$$\begin{array}{ccc} \operatorname{Aut}(L_{1,1}(p)) & & \\ \Big| & & \\ \operatorname{Aut}_f(L_{1,1}(p)) & \xrightarrow{\bar{c}} & E(\mathbb{F}_p) \rtimes \operatorname{Aut}(E)(\mathbb{F}_p) \end{array}$$

We show that

$$|\operatorname{Aut}(G_{1,1}(p))| \overset{\text{Lazard}}{=} |\operatorname{Aut}(L_{1,1}(p))| = \underline{|\operatorname{Im}\bar{c}|} \cdot \underline{|\operatorname{GL}_2(\mathbb{F}_p)|} \cdot \underline{|\mathbb{F}_p|^{18}}$$

where

$$\begin{array}{ccc} \operatorname{Aut}(L_{1,1}(p)) & & \\ \Big| & & \\ \operatorname{Aut}_f(L_{1,1}(p)) & \xrightarrow{\bar{c}} & E(\mathbb{F}_p) \rtimes \operatorname{Aut}(E)(\mathbb{F}_p) \end{array}$$

General remarks

- in general $K^{(d+e)f}$
- if $d = e = f$ and B symmetric, then $\operatorname{GL}_2(K)$
- if $d = e = f = 3$, B symmetric, and $\det B = 0$ defines an elliptic curve, then $\operatorname{Im}\bar{c}_B$

SYMMETRIC DETERMINANTAL REPRESENTATIONS OF CURVES

and where to find them

Question

Is any elliptic curve realizable as $\det B = 0$ for $d = e = f = 3$ and B symmetric?

Question

Is any elliptic curve realizable as $\det B = 0$ for $d = e = f = 3$ and B symmetric?

Theorem (Hesse, 1844)

Let $F \in \mathbb{C}[x, y, z]$ homogeneous be such that $F = 0$ defines an elliptic curve E. Then there are, up to equivalence, exactly three symmetric linear determinantal representations of E corresponding to the three solutions $(\alpha, \beta) \in \mathbb{C}^2$ of $\alpha F = \mathrm{Hes}(\beta F + \mathrm{Hes}(F))$.

Question

Is any elliptic curve realizable as $\det B = 0$ for $d = e = f = 3$ and B symmetric?

Theorem (Hesse, 1844)

Let $F \in \mathbb{C}[x, y, z]$ homogeneous be such that $F = 0$ defines an elliptic curve E. Then there are, up to equivalence, exactly three symmetric linear determinantal representations of E corresponding to the three solutions $(\alpha, \beta) \in \mathbb{C}^2$ of $\alpha F = \mathrm{Hes}(\beta F + \mathrm{Hes}(F))$.

Answer

Yes, in $\mathbb{C}$. Moreover, each such representation is equivalent to a Hessian one. $(B \sim B' \Leftrightarrow \exists U \in \mathrm{GL}_3(\mathbb{C}) \text{ s.t. } B' = UBU^{\mathrm{t}})$

Theorem (S., Voll 2019+)

Let $0 \neq \varepsilon \in \mathbb{Z}$ *and assume* $p \nmid 2\varepsilon$. *Define* $E_\varepsilon : y^2 = x^3 - \varepsilon^{-2}x$. *Then there exist inequivalent matrices* $B_{1,\varepsilon}, B_{2,\varepsilon}, B_{3,\varepsilon}$ *such that the following hold:*

- $\det B_{i,\varepsilon} = 0$ *defines* E_ε;
- $|\operatorname{Aut}(G_{i,\varepsilon})| = \gcd\{p-1, \lceil 4/i \rceil\} |\operatorname{GL}_2(\mathbb{F}_p)| \cdot p^{18} \cdot |E_\varepsilon[3](\mathbb{F}_p)|$
- $G_{i,\varepsilon} \ncong G_{j,\varepsilon'}$ *in "almost all cases"*

Theorem (S., Voll 2019+)

Let $0 \neq \varepsilon \in \mathbb{Z}$ *and assume* $p \nmid 2\varepsilon$. *Define* $E_\varepsilon : y^2 = x^3 - \varepsilon^{-2}x$. *Then there exist inequivalent matrices* $B_{1,\varepsilon}, B_{2,\varepsilon}, B_{3,\varepsilon}$ *such that the following hold:*

- $\det B_{i,\varepsilon} = 0$ *defines* E_ε*;*
- $|\operatorname{Aut}(G_{i,\varepsilon})| = \gcd\{p-1, \lceil 4/i \rceil\} |\operatorname{GL}_2(\mathbb{F}_p)| \cdot p^{18} \cdot |E_\varepsilon[3](\mathbb{F}_p)|$
- $G_{i,\varepsilon} \ncong G_{j,\varepsilon'}$ *in "almost all cases"*

Remarks

- All E_ε's are isomorphic over $\mathbb{F}_p^{\mathrm{alg}}$, but almost all groups are not!
- Can be generalized for general fields of characteristic not dividing 2ε.

Example

- If $p \equiv 1 \bmod 4$, then $G_{2,1}(p) \cong G_{3,1}(p) \ncong G_{1,1}(p)$ and $2|\operatorname{Aut}(G_{2,1}(p))| = 2|\operatorname{Aut}(G_{3,1}(p))| = |\operatorname{Aut}(G_{1,1}(p))|$.
- If $p \equiv 3 \bmod 4$, then $G_{2,1}(p) \ncong G_{3,1}(p) \ncong G_{1,1}(p)$ and $|\operatorname{Aut}(G_{2,1}(p))| = |\operatorname{Aut}(G_{3,1}(p))| = |\operatorname{Aut}(G_{1,1}(p))|$.

Example

- If $p \equiv 1 \bmod 4$, then $G_{2,1}(p) \cong G_{3,1}(p) \ncong G_{1,1}(p)$ and $2|\operatorname{Aut}(G_{2,1}(p))| = 2|\operatorname{Aut}(G_{3,1}(p))| = |\operatorname{Aut}(G_{1,1}(p))|$.
- If $p \equiv 3 \bmod 4$, then $G_{2,1}(p) \ncong G_{3,1}(p) \ncong G_{1,1}(p)$ and $|\operatorname{Aut}(G_{2,1}(p))| = |\operatorname{Aut}(G_{3,1}(p))| = |\operatorname{Aut}(G_{1,1}(p))|$.

Further research

- Compute $\operatorname{Im}\bar{c}$ for general elliptic curves.
- Symmetric case for other smooth hypersurfaces.
- Non-smooth case?
- Non-symmetric case?
- Other input?


thank you