Capitulation Discriminants of Genus One Curves

Lazar Radicevic

January 19, 2022

An example of a smooth curve C of genus one, defined over $\mathbb{Q}$, that has a point over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points:

$$C := \{(x : y : z) \in \mathbb{P}^2 : 3x^3 + 4y^3 + 5z^3 = 0\}$$

An example of a smooth curve C of genus one, defined over $\mathbb{Q}$, that has a point over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points:

$$C := \{(x : y : z) \in \mathbb{P}^2 : 3x^3 + 4y^3 + 5z^3 = 0\}$$

C admits points over a cubic extension of $\mathbb{Q}$. For example, by setting $z = 0$, we see that C has a point defined over $\mathbb{Q}(\sqrt[3]{-3/4}) = \mathbb{Q}(\sqrt[3]{-6})$. More generally, whenever we intersect C with a hyperplane H, we get a set of 3 points defined over a cubic algebra.

An example of a smooth curve C of genus one, defined over $\mathbb{Q}$, that has a point over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points:

$$C := \{(x : y : z) \in \mathbb{P}^2 : 3x^3 + 4y^3 + 5z^3 = 0\}$$

C admits points over a cubic extension of $\mathbb{Q}$. For example, by setting $z = 0$, we see that C has a point defined over $\mathbb{Q}(\sqrt[3]{-3/4}) = \mathbb{Q}(\sqrt[3]{-6})$.
More generally, whenever we intersect C with a hyperplane H, we get a set of 3 points defined over a cubic algebra.
The curve C represents a non-trivial element of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ of its Jacobian elliptic curve E. We say this element *capitulates* over the field $\mathbb{Q}(\sqrt[3]{-6})$.

- The Selmer example is an element of 3-torsion of $\text{Ш}(E/\mathbb{Q})$. We can also look at n-torsion elements.

- The Selmer example is an element of 3-torsion of $\text{Ш}(E/\mathbb{Q})$. We can also look at n-torsion elements.
- Elements of n-torsion of $\text{Ш}(E/\mathbb{Q})$ are represented by degree n curves $C \subset \mathbb{P}^{n-1}$, of genus one, that have points everywhere locally.

- The Selmer example is an element of 3-torsion of $\text{Ш}(E/\mathbb{Q})$. We can also look at n-torsion elements.
- Elements of n-torsion of $\text{Ш}(E/\mathbb{Q})$ are represented by degree n curves $C \subset \mathbb{P}^{n-1}$, of genus one, that have points everywhere locally.
- Intersection of C and a random hyperplane $C \cap H$ consists of n points defined over a degree n extension of $\mathbb{Q}$.
- Question: What is the smallest degree n field L over which C has a rational point?

- The Selmer example is an element of 3-torsion of $\text{Ш}(E/\mathbb{Q})$. We can also look at n-torsion elements.
- Elements of n-torsion of $\text{Ш}(E/\mathbb{Q})$ are represented by degree n curves $C \subset \mathbb{P}^{n-1}$, of genus one, that have points everywhere locally.
- Intersection of C and a random hyperplane $C \cap H$ consists of n points defined over a degree n extension of $\mathbb{Q}$.
- Question: What is the smallest degree n field L over which C has a rational point?
- Main result: the discriminant of L is bounded by a power of the height of the Jacobian elliptic curve of C.

Background

- An elliptic curve $E/\mathbb{Q}$ is a smooth curve of genus one with a marked rational point 0_E. There is a natural way to make E into a group variety, with the point 0_E being the identity.
- The curve E admits a Weierstrass model - it can be defined as a plane curve by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Twists

- $X/\mathbb{Q}$ a variety. A twist of X is a variety Y, defined over $\mathbb{Q}$, that is isomorphic to X over $\bar{\mathbb{Q}}$. Two twists $Y_1/\mathbb{Q}$ and $Y_2/\mathbb{Q}$ are isomorphic if Y_1 and Y_2 are isomorphic over $\mathbb{Q}$.
- Example: The plane conic $Y : \{x^2 + y^2 + z^2 = 0\}$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{C}$, but not over $\mathbb{Q}$ - the set $Y(\mathbb{R})$ is empty.

Twists

- $X/\mathbb{Q}$ a variety. A twist of X is a variety Y, defined over $\mathbb{Q}$, that is isomorphic to X over $\bar{\mathbb{Q}}$. Two twists $Y_1/\mathbb{Q}$ and $Y_2/\mathbb{Q}$ are isomorphic if Y_1 and Y_2 are isomorphic over $\mathbb{Q}$.
- Example: The plane conic $Y : \{x^2 + y^2 + z^2 = 0\}$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{C}$, but not over $\mathbb{Q}$ - the set $Y(\mathbb{R})$ is empty.
- Let $C/\mathbb{Q}$ be a general curve of genus one. It is possible that C does not have rational points. If so, so then it can't be defined by a Weierstrass equation.
- The Jacobian variety of C is an elliptic curve $E/\mathbb{Q}$, that is a twist of C. C has a rational point precisely when it is isomorphic to E, i.e. when this twist is trivial.

- Let $n \geq 3$. An n-diagram is a closed embedding $[C \to \mathbb{P}^{n-1}]$, where the curve C is a genus one curve, of degree n, that spans $\mathbb{P}^{n-1}$.
- For $n = 2$: A 2-diagram is a double cover $[C \to \mathbb{P}^1]$.

- Let $n \geq 3$. An n-diagram is a closed embedding $[C \to \mathbb{P}^{n-1}]$, where the curve C is a genus one curve, of degree n, that spans $\mathbb{P}^{n-1}$.
- For $n = 2$: A 2-diagram is a double cover $[C \to \mathbb{P}^1]$.
- Let $C/\mathbb{Q}$ be a genus one curve that is everywhere locally soluble. Then for some n, there exists an n-diagram $[C \to \mathbb{P}^{n-1}]$.

- Let $n \geq 3$. An n-diagram is a closed embedding $[C \to \mathbb{P}^{n-1}]$, where the curve C is a genus one curve, of degree n, that spans $\mathbb{P}^{n-1}$.
- For $n = 2$: A 2-diagram is a double cover $[C \to \mathbb{P}^1]$.
- Let $C/\mathbb{Q}$ be a genus one curve that is everywhere locally soluble. Then for some n, there exists an n-diagram $[C \to \mathbb{P}^{n-1}]$.
- Two n-diagrams $[C_1 \to \mathbb{P}^{n-1}]$ and $[C_2 \to \mathbb{P}^{n-1}]$ are equivalent if there is an automorphism of $\mathbb{P}^{n-1}$ taking C_1 to C_2.

- Let $n \geq 3$. An n-diagram is a closed embedding $[C \to \mathbb{P}^{n-1}]$, where the curve C is a genus one curve, of degree n, that spans $\mathbb{P}^{n-1}$.
- For $n = 2$: A 2-diagram is a double cover $[C \to \mathbb{P}^1]$.
- Let $C/\mathbb{Q}$ be a genus one curve that is everywhere locally soluble. Then for some n, there exists an n-diagram $[C \to \mathbb{P}^{n-1}]$.
- Two n-diagrams $[C_1 \to \mathbb{P}^{n-1}]$ and $[C_2 \to \mathbb{P}^{n-1}]$ are equivalent if there is an automorphism of $\mathbb{P}^{n-1}$ taking C_1 to C_2.
- The set of everywhere locally soluble n-diagrams that are twists of a fixed elliptic curve E is parametrized by the n-Selmer group of E.

Main result

- Fix a global minimal Weierstrass equation for E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Let c_4 and c_6 be the associated invariants of the equation. The naive height of E is $H_E = \max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6})$.

Main result

- Fix a global minimal Weierstrass equation for E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Let c_4 and c_6 be the associated invariants of the equation. The naive height of E is $H_E = \max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6})$.
- If $E : y^2 = x^3 + Ax + B$, then $H_E^{12} = O(\max(|A|^3, B^2))$.

Main result

- Fix a global minimal Weierstrass equation for E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Let c_4 and c_6 be the associated invariants of the equation. The naive height of E is $H_E = \max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6})$.
- If $E : y^2 = x^3 + Ax + B$, then $H_E^{12} = O(\max(|A|^3, B^2))$.

Theorem

Let $n \geq 3$ be an odd integer, and let C be a twist of E that represents an element of $\text{Ш}(E/\mathbb{Q})[n]$. Suppose that the index of C is equal to n. There exists a constant $c(n)$, depending only on n, and a degree n number field K of discriminant at most $c(n)H_E^{2n-2}$, such that C admits a K-rational point.

Equations for n-diagrams

Let $[C \to \mathbb{P}^{n-1}]$ be an n-diagram. For small n, we can describe the equations that define it:

Equations for n-diagrams

Let $[C \to \mathbb{P}^{n-1}]$ be an n-diagram. For small n, we can describe the equations that define it:

- $n = 2$: The double cover $C \to \mathbb{P}^1$ can be realized by a model of the form $y^2 = f(x, z)$, where $f(x, z)$ is a binary quartic.
- $n = 3$: $C \subset \mathbb{P}^2$ is a plane cubic, and so defined by a ternary cubic form $F(x, y, z)$.
- $n = 4$: $C \subset \mathbb{P}^3$ is a space curve of degree 4. C is always an intersection of two quadrics P and Q in variables x, y, z, t.

Equations for n-diagrams

Let $[C \to \mathbb{P}^{n-1}]$ be an n-diagram. For small n, we can describe the equations that define it:

- $n = 2$: The double cover $C \to \mathbb{P}^1$ can be realized by a model of the form $y^2 = f(x, z)$, where $f(x, z)$ is a binary quartic.
- $n = 3$: $C \subset \mathbb{P}^2$ is a plane cubic, and so defined by a ternary cubic form $F(x, y, z)$.
- $n = 4$: $C \subset \mathbb{P}^3$ is a space curve of degree 4. C is always an intersection of two quadrics P and Q in variables x, y, z, t.

Conversely, a generic equation in the above list defines a smooth genus one curve. The space X_n of genus one models of degree n is the affine space of binary quartics, ternary cubics and pairs of quaternary quadrics.

- A genus one model of a given n-diagram $[C \to \mathbb{P}^{n-1}]$ is far from unique. There are two reasons for this: we are free to make projective changes of coordinates on the ambient space $\mathbb{P}^{n-1}$, and the equations that define the curve C are not unique.
- For example, if F is a ternary cubic and $g \in \mathrm{GL}_n(\mathbb{Q})$, $F(x, y, z)$ and $F((x, y, z) \cdot g)$ represent the same diagram, as well as $\lambda \cdot F$ for any $\lambda \in \mathbb{Q}$.

- A genus one model of a given n-diagram $[C \to \mathbb{P}^{n-1}]$ is far from unique. There are two reasons for this: we are free to make projective changes of coordinates on the ambient space $\mathbb{P}^{n-1}$, and the equations that define the curve C are not unique.
- For example, if F is a ternary cubic and $g \in \mathrm{GL}_n(\mathbb{Q})$, $F(x, y, z)$ and $F((x, y, z) \cdot g)$ represent the same diagram, as well as $\lambda \cdot F$ for any $\lambda \in \mathbb{Q}$.
- This is encoded in the action of a group $\mathcal{G}_n$ on the space X_n of genus one models of degree n. Every n-diagram $[C \to \mathbb{P}^{n-1}]$ gives rise to a well-defined equivalence class in $\mathcal{G}_n(\mathbb{Q})\backslash X_n(\mathbb{Q})$.

- We can use invariant theory to study the set $\mathcal{G}_n(\mathbb{Q})\backslash X_n(\mathbb{Q})$. Let $\mathbb{Z}[X_n]$ be the ring of polynomials in the coefficients of genus one models.

- We can use invariant theory to study the set $\mathcal{G}_n(\mathbb{Q})\backslash X_n(\mathbb{Q})$. Let $\mathbb{Z}[X_n]$ be the ring of polynomials in the coefficients of genus one models.
- There exist polynomials c_4 and c_6 in $\mathbb{Z}[X_n]$, which are invariants of weight 4 and 6 for the action of $\mathcal{G}_n$, with the property that if $F \in X_n(\mathbb{Q})$ is a genus one model that defines a smooth genus one curve $C \subset \mathbb{P}^{n-1}$, then

$$y^2 = x^3 - 27c_4(F) + 54c_6(F)$$

defines the Jacobian of C. There is also the discriminant invariant $\Delta \in \mathbb{Z}[X_n]$, with $1728\Delta(F) = c_4(F)^3 - c_6(F)^2$.

- We can use invariant theory to study the set $\mathcal{G}_n(\mathbb{Q})\backslash X_n(\mathbb{Q})$. Let $\mathbb{Z}[X_n]$ be the ring of polynomials in the coefficients of genus one models.
- There exist polynomials c_4 and c_6 in $\mathbb{Z}[X_n]$, which are invariants of weight 4 and 6 for the action of $\mathcal{G}_n$, with the property that if $F \in X_n(\mathbb{Q})$ is a genus one model that defines a smooth genus one curve $C \subset \mathbb{P}^{n-1}$, then

$$y^2 = x^3 - 27c_4(F) + 54c_6(F)$$

  defines the Jacobian of C. There is also the discriminant invariant $\Delta \in \mathbb{Z}[X_n]$, with $1728\Delta(F) = c_4(F)^3 - c_6(F)^2$.
- Example: $n = 2$, $f = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in X_2(\mathbb{Q})$ has invariants $c_4 = 2^4 I$ and $c_6 = 2^5 J$ where

$$\begin{aligned} I &= 12ae - 3bd + c^2 \\ J &= 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3. \end{aligned}$$

Integral models

- We say a genus one model F of an n-diagram $[C \to \mathbb{P}^{n-1}]$ is minimal if F has integer coefficients, so $F \in X_n(\mathbb{Z})$, and the discriminant $\Delta(F)$ is equal to the discriminant of the minimal Weierstrass equation for the Jacobian of C.
- Minimization theorem: An n-diagram $[C \subset \mathbb{P}^{n-1}]$ where C is everywhere locally soluble admits a minimal model.

Integral models

- We say a genus one model F of an n-diagram $[C \to \mathbb{P}^{n-1}]$ is minimal if F has integer coefficients, so $F \in X_n(\mathbb{Z})$, and the discriminant $\Delta(F)$ is equal to the discriminant of the minimal Weierstrass equation for the Jacobian of C.
- Minimization theorem: An n-diagram $[C \subset \mathbb{P}^{n-1}]$ where C is everywhere locally soluble admits a minimal model.
- A minimal model of $[C \to \mathbb{P}^{n-1}]$ has small integer coefficients.
- Goes back to the work of Birch and Swinnterton-Dyer in the 60s.
- Useful when searching for rational points on elliptic curves.
- Also used in the work of Bhargava and Shankar on average ranks of n-Selmer groups of elliptic curves.

Generalizing to $n \geq 5$

- For $n \geq 5$: $C \to \mathbb{P}^{n-1}$ is a closed embedding, and the homogeneous ideal $I(C)$ that defines C is generated by $n(n-3)/2$ quadrics, and is not a complete intersection.
- $n = 5$: $[C \subset \mathbb{P}^4]$ a 5-diagram. $I(C)$ generated by 5 quadrics in 5 variables.

Generalizing to $n \geq 5$

- For $n \geq 5$: $C \to \mathbb{P}^{n-1}$ is a closed embedding, and the homogeneous ideal $I(C)$ that defines C is generated by $n(n-3)/2$ quadrics, and is not a complete intersection.
- $n = 5$: $[C \subset \mathbb{P}^4]$ a 5-diagram. $I(C)$ generated by 5 quadrics in 5 variables.
- The quadrics that cut out a genus one curve are very special - if we take five random quadrics in $\mathbb{Q}[x_1, \ldots, x_5]$, they usually won't even define a curve.

Generalizing to $n \geq 5$

- For $n \geq 5$: $C \to \mathbb{P}^{n-1}$ is a closed embedding, and the homogeneous ideal $I(C)$ that defines C is generated by $n(n-3)/2$ quadrics, and is not a complete intersection.
- $n = 5$: $[C \subset \mathbb{P}^4]$ a 5-diagram. $I(C)$ generated by 5 quadrics in 5 variables.
- The quadrics that cut out a genus one curve are very special - if we take five random quadrics in $\mathbb{Q}[x_1, \ldots, x_5]$, they usually won't even define a curve.

- Let $R = \mathbb{Q}[x_1, \ldots, x_n]$ be the graded homogeneous coordinate ring of $\mathbb{P}^{n-1}$.
- Minimal graded free resolution of I is a chain complex of graded free R-modules

$$0 \to F_m \xrightarrow{\phi_m} F_{m-1} \xrightarrow{\phi_{m-2}} \ldots \to F_1 \xrightarrow{\phi_1} F_0 = R \to 0$$

that is exact, except at the rightmost step, where $\mathrm{im}(\phi_1) = I(C)$.
- $n = 3$: $C \subset \mathbb{P}^2$ is a plane cubic, so the ideal $I(C)$ is principal, generated by $F \in R$. The resolution is

$$0 \to R \xrightarrow{\cdot F} R \to 0$$

- $n = 4$: $C \subset \mathbb{P}^4$. The ideal $I(C)$ is generated by a pair of quadratic forms f and g. The resolution of $I(C)$:

$$F_\bullet : 0 \to R \xrightarrow{\begin{pmatrix} g \\ -f \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} f & g \end{pmatrix}} R \to 0.$$

- The map $R^2 \to R$ says: $I(C) = R \cdot f \oplus R \cdot g$.
- The map $R \to R^2$: $g \cdot f + (-f) \cdot g = 0$, and any R-linear relation $p \cdot f + q \cdot g = 0$ is a multiple of this one.

- $n = 5$, $C \subset \mathbb{P}^4$. The minimal graded free resolution of $I(C)$ is of the form:

$$0 \to R \xrightarrow{\phi^T} R^5 \xrightarrow{A} R^5 \xrightarrow{\phi} R \to 0$$

- $n = 5$, $C \subset \mathbb{P}^4$. The minimal graded free resolution of $I(C)$ is of the form:

$$0 \to R \xrightarrow{\phi^T} R^5 \xrightarrow{A} R^5 \xrightarrow{\phi} R \to 0$$

- A is a skew-symmetric 5×5-matrix, with entries linear forms in $x_1, x_2, \ldots, x_5$. ϕ is the row vector of (signed) 4×4 Pfaffians of A.
- Pfaffian of a skew-symmetric matrix is square root of its determinant.

- $n = 5$, $C \subset \mathbb{P}^4$. The minimal graded free resolution of $I(C)$ is of the form:

$$0 \to R \xrightarrow{\phi^T} R^5 \xrightarrow{A} R^5 \xrightarrow{\phi} R \to 0$$

- A is a skew-symmetric 5×5-matrix, with entries linear forms in $x_1, x_2, \ldots, x_5$. ϕ is the row vector of (signed) 4×4 Pfaffians of A.
- Pfaffian of a skew-symmetric matrix is square root of its determinant.
- In fact, for a generic matrix A as above, the variety in $\mathbb{P}^4$ defined by the Pfaffians of A is a genus one curve of degree 5.
- X_5 is the affine space of skew-symmetric matrices A of linear forms in $x_1, \ldots, x_5$.

- $n = 5$, $C \subset \mathbb{P}^4$. The minimal graded free resolution of $I(C)$ is of the form:

$$0 \to R \xrightarrow{\phi^T} R^5 \xrightarrow{A} R^5 \xrightarrow{\phi} R \to 0$$

- A is a skew-symmetric 5×5-matrix, with entries linear forms in $x_1, x_2, \dots, x_5$. ϕ is the row vector of (signed) 4×4 Pfaffians of A.
- Pfaffian of a skew-symmetric matrix is square root of its determinant.
- In fact, for a generic matrix A as above, the variety in $\mathbb{P}^4$ defined by the Pfaffians of A is a genus one curve of degree 5.
- X_5 is the affine space of skew-symmetric matrices A of linear forms in $x_1, \dots, x_5$.
- Fisher: as before, there are invariants $c_4, c_6 \in \mathbb{Z}[X_5]$ that can be used to write down the Jacobian of C, and the minimization theorem holds.

- For $n > 5$, do not have a simple description of the resolution $F_\bullet$ of $I(C)$. We do have a structure theorem: $F_\bullet$ is a chain complex of form

$$R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} \ldots\ldots \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R$$

where $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$

- For $n > 5$, do not have a simple description of the resolution $F_\bullet$ of $I(C)$. We do have a structure theorem: $F_\bullet$ is a chain complex of form

$$R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} \ldots\ldots \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R$$

  where $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$
- The ideal $I(C)$ is Gorenstein, so $F_\bullet$ is self-dual.
- The space of genus one models of degree n is defined as the space of chain complexes as above that are self-dual.

- For $n > 5$, do not have a simple description of the resolution $F_\bullet$ of $I(C)$. We do have a structure theorem: $F_\bullet$ is a chain complex of form

$$R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} \ldots\ldots \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R$$

  where $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$
- The ideal $I(C)$ is Gorenstein, so $F_\bullet$ is self-dual.
- The space of genus one models of degree n is defined as the space of chain complexes as above that are self-dual.
- Group $\mathcal{G}_n = \mathrm{GL}_{b_{n-2}} \times \ldots \times \mathrm{GL}_{b_0} \times \mathrm{GL}_n$ on the space X_n. The group $\mathrm{GL}_{b_{n-2}} \times \ldots \times \mathrm{GL}_{b_0}$ acts on the free modules in the resolution, and GL_n acts by linear substitutions in $x_1, \ldots, x_n$.
- Non-degenerate orbits in $\mathcal{G}_n \backslash X_n$ parametrise isomorphism classes of n-diagrams $[C \to \mathbb{P}^{n-1}]$.

- Fisher defines invariants c_4 and c_6 for these models. The basic building blocks are square bracket symbols built out of partial differentials:

$$[a_1, a_2, \dots, a_{n-2}] = \frac{\partial \phi_1}{\partial x_{a_1}} \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}},$$

These are quadratic forms in $x_1, \dots, x_n$.

- Fisher defines invariants c_4 and c_6 for these models. The basic building blocks are square bracket symbols built out of partial differentials:

$$[a_1, a_2, \ldots, a_{n-2}] = \frac{\partial \phi_1}{\partial x_{a_1}} \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}},$$

These are quadratic forms in $x_1, \ldots, x_n$.

- Let $\sigma = (1, 2, \ldots, n-2) \in S_{n-2}$. We then define

$$[[a_1, a_2, \ldots, a_{n-2}]] = \sum_{k=1}^{n-2} [a_{\sigma^{2k}(1)}, a_{\sigma^{2k}(2)}, \ldots, a_{\sigma^{2k}(n-2)}].$$

The symbols $[[\ldots]]$ assemble to an alternating matrix Ω of quadratic forms, which transforms in a natural way for the action of $\mathcal{G}_n$ on X_n.

- [[. . .]] turn out to be invariant under the action of the first factor $\mathrm{GL}_{b_{n-2}} \times \ldots \times \mathrm{GL}_{b_0}$ of $\mathcal{G}_n$.
- Let V be the space of linear forms $x_1, \ldots, x_n$ - view it as the standard representation of $\mathrm{GL}_n = \mathrm{GL}(V)$. The matrix Ω is an element of $\det V \otimes \Lambda^2 V \otimes S^2 V$.
- From Ω we construct two further invariants, $c_4 \in (\det V)^{\otimes 4}$ and $c_6 \in (\det V)^{\otimes 6}$.
- Method of proof: GL_n is generated by diagonal matices, upper triangular matrices, and a copy of S_n (permutation matrices).

- [[...]] turn out to be invariant under the action of the first factor $\mathrm{GL}_{b_{n-2}} \times \ldots \times \mathrm{GL}_{b_0}$ of $\mathcal{G}_n$.
- Let V be the space of linear forms $x_1, \ldots, x_n$ - view it as the standard representation of $\mathrm{GL}_n = \mathrm{GL}(V)$. The matrix Ω is an element of $\det V \otimes \Lambda^2 V \otimes S^2 V$.
- From Ω we construct two further invariants, $c_4 \in (\det V)^{\otimes 4}$ and $c_6 \in (\det V)^{\otimes 6}$.
- Method of proof: GL_n is generated by diagonal matices, upper triangular matrices, and a copy of S_n (permutation matrices). Checking the transformation law for first two is straightforward. Permutation matrices are done by a lot of combinatorial fiddling with symbols [...]

- [[...]] turn out to be invariant under the action of the first factor $\mathrm{GL}_{b_{n-2}} \times \ldots \times \mathrm{GL}_{b_0}$ of $\mathcal{G}_n$.
- Let V be the space of linear forms $x_1, \ldots, x_n$ - view it as the standard representation of $\mathrm{GL}_n = \mathrm{GL}(V)$. The matrix Ω is an element of $\det V \otimes \Lambda^2 V \otimes S^2 V$.
- From Ω we construct two further invariants, $c_4 \in (\det V)^{\otimes 4}$ and $c_6 \in (\det V)^{\otimes 6}$.
- Method of proof: GL_n is generated by diagonal matices, upper triangular matrices, and a copy of S_n (permutation matrices). Checking the transformation law for first two is straightforward. Permutation matrices are done by a lot of combinatorial fiddling with symbols [...]
- Main results: For n odd, the formula for the Jacobian, and the minimization theorem hold.

Rank n rings and sets of n points

- A set X of n points in $\mathbb{P}^{n-2}$ is in general position if no $n-1$ of them lie on a hyperplane.
- If X is defined over $\mathbb{Q}$, the ring of global functions on X is an n-dimensional etale $\mathbb{Q}$-algebra.

Rank n rings and sets of n points

- A set X of n points in $\mathbb{P}^{n-2}$ is in general position if no $n-1$ of them lie on a hyperplane.
- If X is defined over $\mathbb{Q}$, the ring of global functions on X is an n-dimensional etale $\mathbb{Q}$-algebra.
- $n = 3$: $X \subset \mathbb{P}^1$: 3 roots of a binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbb{Q}[x, y]$.
- $n = 4$: $X \subset \mathbb{P}^2$: intersection of a pair of quadratic forms $f(x, y, z), g(x, y, z) \in \mathbb{Q}[x, y, z]$.
- $n = 5$: $X \subset \mathbb{P}^3$: Pfaffians of a 5×5-matrix $A(x_1, x_2, x_3, x_4) \in \mathbb{Q}[x_1, x_2, x_3, x_4]$.

Rank n rings and sets of n points

- Resolution models of sets of n points are the same as for genus one curves, but with one less variable:

$$R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} \ldots\ldots \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R$$

where $R = \mathbb{Q}[x_1, \ldots, x_{n-1}]$, satisfying the same duality condition.

Rank n rings and sets of n points

- Resolution models of sets of n points are the same as for genus one curves, but with one less variable:

$$R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} \ldots\ldots \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R$$

where $R = \mathbb{Q}[x_1, \ldots, x_{n-1}]$, satisfying the same duality condition.

- In the same way as before, we define the symbols $[[\ldots]]$. Instead of a matrix, we get $n-1$ quadrics $\Omega_1, \ldots, \Omega_{n-1}$, that represent an element of $V^* \otimes S^2 V$, V the vector space of linear forms on $\mathbb{P}^{n-2}$.

Our main result is

Theorem (Fisher - R.)

The ring A of global functions on X has a basis $1, \alpha_1, \ldots, \alpha_{n-1}$, such that for all $1 \leq i, j \leq n-1$ we have

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{n-1} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k.$$

for some $c_{ij}^0 \in k$.

Our main result is

Theorem (Fisher - R.)

The ring A of global functions on X has a basis $1, \alpha_1, \dots, \alpha_{n-1}$, such that for all $1 \leq i, j \leq n-1$ we have

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{n-1} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k.$$

for some $c_{ij}^0 \in k$.

- Key point - if the resolution model $F_\bullet$ is integral, then the structure constants are integers, and define an order in the algebra A.

Our main result is

Theorem (Fisher - R.)

The ring A of global functions on X has a basis $1, \alpha_1, \ldots, \alpha_{n-1}$, such that for all $1 \leq i, j \leq n-1$ we have

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{n-1} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k.$$

for some $c_{ij}^0 \in k$.

- Key point - if the resolution model $F_\bullet$ is integral, then the structure constants are integers, and define an order in the algebra A.
- When $n = 3, 4, 5$, this specializes to the Delone-Faddeev correspondence and higher composition laws of Bhargava. These are more general: they account for all rings of rank $n \leq 5$.

- The proof: First step is to show that we can reduce to the case when $k = \bar{k}$ is algebraically closed.

- The proof: First step is to show that we can reduce to the case when $k = \bar{k}$ is algebraically closed.
- Every set X of n points in general position is projectively equivalent to $(1:0:\ldots:0),(0:1:0:\ldots:0),\ldots,(1:0:\ldots:0),(1:1:\ldots:1)$

- The proof: First step is to show that we can reduce to the case when $k = \bar{k}$ is algebraically closed.
- Every set X of n points in general position is projectively equivalent to $(1 : 0 : \ldots : 0), (0 : 1 : 0 : \ldots : 0), \ldots, (1 : 0 : \ldots : 0), (1 : 1 : \ldots : 1)$
- Since we know how the symbols $[[\ldots]]$ behave under changes of coordinates, suffices to compute them for this set.
- We do this by explicitly computing the minimal free resolution of this set.

$n = 3$

- $C \subset \mathbb{P}^2$ a 3-diagram, C everywhere locally soluble.

$n = 3$

- $C \subset \mathbb{P}^2$ a 3-diagram, C everywhere locally soluble.
- Let $F(x, y, z) \in \mathbb{Q}[x, y, z]$ be a cubic that defines C. Consider a hyperplane $H : ux + vy + wz = 0$. The intersection $H \cap C$ consists of the roots of the binary cubic

$$F(wx, wy, -u \cdot -v \cdot y) = 0$$

$n = 3$

- $C \subset \mathbb{P}^2$ a 3-diagram, C everywhere locally soluble.
- Let $F(x, y, z) \in \mathbb{Q}[x, y, z]$ be a cubic that defines C. Consider a hyperplane $H : ux + vy + wz = 0$. The intersection $H \cap C$ consists of the roots of the binary cubic

$$F(wx, wy, -u \cdot -v \cdot y) = 0$$

- The discriminant of this cubic factors as $w^6 \cdot D(u, v, w)$, where $D(u, v, w)$ is a homogeneous polynomial of degree 6 in u, v, w. $D(u, v, w)$ defines the the *dual* curve to C: It vanishes exactly when the hyperplane H is tangent to C at some point.

$n = 3$

- $C \subset \mathbb{P}^2$ a 3-diagram, C everywhere locally soluble.
- Let $F(x, y, z) \in \mathbb{Q}[x, y, z]$ be a cubic that defines C. Consider a hyperplane $H : ux + vy + wz = 0$. The intersection $H \cap C$ consists of the roots of the binary cubic

$$F(wx, wy, -u \cdot -v \cdot y) = 0$$

- The discriminant of this cubic factors as $w^6 \cdot D(u, v, w)$, where $D(u, v, w)$ is a homogeneous polynomial of degree 6 in u, v, w. $D(u, v, w)$ defines the the *dual* curve to C: It vanishes exactly when the hyperplane H is tangent to C at some point.
- A consequence of Delone-Faddeev: when F has integer coefficents, and $u, v, w \in \mathbb{Z}$, then $D(u, v, w)$ is the discriminant of an order in a cubic field, and so an upper bound for the discriminant of the field.

- By the minimization theorem: there exists $F \in \mathbb{Z}[x, y, z]$, with $c_k(F) = c_k(E)$. Want to show that there exist $u, v, w \in \mathbb{Z}$ so that $D(u, v, w)$ is small.

- By the minimization theorem: there exists $F \in \mathbb{Z}[x, y, z]$, with $c_k(F) = c_k(E)$. Want to show that there exist $u, v, w \in \mathbb{Z}$ so that $D(u, v, w)$ is small.
- F is $\mathrm{SL}_3(\mathbb{R})$-equivalent to a cubic G of the form

$$G := a(x^3 + y^3 + z^3) - 3bxyz$$

  the Hesse normal form of F.
- It follows that D is $\mathrm{SL}_3(\mathbb{R})$-equivalent to the dual curve D_G of G

$$\begin{aligned} &-27a^4(u^6 + v^6 + w^6) + 162a^2b^2(u^4vw + uv^4w + uvw^4) \\ &+ (54a^4 - 108ab^3)(u^3v^3 + v^3w^3 + w^3u^3) + (-324a^3b + 81b^4)u^2v^2w^2 \end{aligned}$$

- By the minimization theorem: there exists $F \in \mathbb{Z}[x, y, z]$, with $c_k(F) = c_k(E)$. Want to show that there exist $u, v, w \in \mathbb{Z}$ so that $D(u, v, w)$ is small.
- F is $\mathrm{SL}_3(\mathbb{R})$-equivalent to a cubic G of the form

$$G := a(x^3 + y^3 + z^3) - 3bxyz$$

  the Hesse normal form of F.
- It follows that D is $\mathrm{SL}_3(\mathbb{R})$-equivalent to the dual curve D_G of G

$$-27a^4(u^6 + v^6 + w^6) + 162a^2b^2(u^4vw + uv^4w + uvw^4) \\ + (54a^4 - 108ab^3)(u^3v^3 + v^3w^3 + w^3u^3) + (-324a^3b + 81b^4)u^2v^2w^2$$

- Under this equivalence, the lattice $\mathbb{Z}^3$ of integral hyperplanes in $\mathbb{R}^3$ maps to some lattice $\Lambda \in \mathbb{R}^3$ of covolume 1.

- By the minimization theorem: there exists $F \in \mathbb{Z}[x, y, z]$, with $c_k(F) = c_k(E)$. Want to show that there exist $u, v, w \in \mathbb{Z}$ so that $D(u, v, w)$ is small.
- F is $\mathrm{SL}_3(\mathbb{R})$-equivalent to a cubic G of the form

$$G := a(x^3 + y^3 + z^3) - 3bxyz$$

  the Hesse normal form of F.
- It follows that D is $\mathrm{SL}_3(\mathbb{R})$-equivalent to the dual curve D_G of G

$$\begin{aligned} &-27a^4(u^6 + v^6 + w^6) + 162a^2b^2(u^4vw + uv^4w + uvw^4) \\ &+ (54a^4 - 108ab^3)(u^3v^3 + v^3w^3 + w^3u^3) + (-324a^3b + 81b^4)u^2v^2w^2 \end{aligned}$$

- Under this equivalence, the lattice $\mathbb{Z}^3$ of integral hyperplanes in $\mathbb{R}^3$ maps to some lattice $\Lambda \in \mathbb{R}^3$ of covolume 1.
- By Minkowski's theorem, Λ contains a small vector (u, v, w). Final step is to bound the coefficients of D_G by a power of the naive height H_E. Then $D_G(u, v, w)$ is the required bound on the discriminant.

Thanks for listening!