Computing structure constants for rings of finite rank from minimal free resolutions

Lazar Radičević (Laboratoire de mathématiques de Besançon)
Joint work with Tom Fisher (University of Cambridge)

May 18, 2023

Introduction

- A ring of rank n is a commutative, associative ring with an identity that is free of rank n as a $\mathbb{Z}$-module.
- Basic examples of rings of rank n are orders in degree n number fields.
- For applications in arithmetic statistics it is important to have parametrizations of these rings.

Parametrizations of rings of rank $n \leq 5$

- For $n \leq 5$ there are explicit parametrizations of rank n rings, due to Levi-Delone-Faddeev and Bhargava.

Parametrizations of rings of rank $n \leq 5$

- For $n \leq 5$ there are explicit parametrizations of rank n rings, due to Levi-Delone-Faddeev and Bhargava.
- $n = 2$ is easy: every quadratic ring is of the form $\mathbb{Z}[\frac{D+\sqrt{D}}{2}]$, for a unique integer $D \equiv 0, 1 \bmod 4$

Parametrizations of rings of rank $n \leq 5$

- For $n \leq 5$ there are explicit parametrizations of rank n rings, due to Levi-Delone-Faddeev and Bhargava.
- $n = 2$ is easy: every quadratic ring is of the form $\mathbb{Z}[\frac{D+\sqrt{D}}{2}]$, for a unique integer $D \equiv 0, 1 \bmod 4$
- Cubic rings are parametrized by integral binary cubic forms.

- Let R be a cubic ring with a $\mathbb{Z}$-basis $1, \omega, \theta$.
- We have $\omega\theta = A \cdot 1 + B \cdot \omega + C \cdot \theta$ for some $A, B, C \in \mathbb{Z}$.

- Let R be a cubic ring with a $\mathbb{Z}$-basis $1, \omega, \theta$.
- We have $\omega\theta = A \cdot 1 + B \cdot \omega + C \cdot \theta$ for some $A, B, C \in \mathbb{Z}$.
- By subtracting appropriate multiples of 1 from ω and θ, we may assume $\omega\theta = I \in \mathbb{Z}$. We say $1, \omega, \theta$ is a normal basis of R.

- Let R be a cubic ring with a $\mathbb{Z}$-basis $1, \omega, \theta$.
- We have $\omega\theta = A \cdot 1 + B \cdot \omega + C \cdot \theta$ for some $A, B, C \in \mathbb{Z}$.
- By subtracting appropriate multiples of 1 from ω and θ, we may assume $\omega\theta = l \in \mathbb{Z}$. We say $1, \omega, \theta$ is a normal basis of R.
- The multiplication table for this basis can be written

$$\begin{aligned} \omega^2 &= k - b\omega + a\theta \\ \omega\theta &= l \\ \theta^2 &= m - d\omega + c\theta \end{aligned}$$

for some integers a, b, c, d, k, l, m

- Let R be a cubic ring with a $\mathbb{Z}$-basis $1, \omega, \theta$.
- We have $\omega\theta = A \cdot 1 + B \cdot \omega + C \cdot \theta$ for some $A, B, C \in \mathbb{Z}$.
- By subtracting appropriate multiples of 1 from ω and θ, we may assume $\omega\theta = l \in \mathbb{Z}$. We say $1, \omega, \theta$ is a normal basis of R.
- The multiplication table for this basis can be written

$$\omega^2 = k - b\omega + a\theta$$
$$\omega\theta = l$$
$$\theta^2 = m - d\omega + c\theta$$

  for some integers a, b, c, d, k, l, m
- Associative law: $\omega^2\theta = \omega \cdot \omega\theta$ and $\omega\theta^2 = \omega\theta \cdot \theta$ imply that $k = -ac, l = -ad, m = -bd$.

- Let R be a cubic ring with a $\mathbb{Z}$-basis $1, \omega, \theta$.
- We have $\omega\theta = A \cdot 1 + B \cdot \omega + C \cdot \theta$ for some $A, B, C \in \mathbb{Z}$.
- By subtracting appropriate multiples of 1 from ω and θ, we may assume $\omega\theta = l \in \mathbb{Z}$. We say $1, \omega, \theta$ is a normal basis of R.
- The multiplication table for this basis can be written

$$\omega^2 = k - b\omega + a\theta$$
$$\omega\theta = l$$
$$\theta^2 = m - d\omega + c\theta$$

  for some integers a, b, c, d, k, l, m
- Associative law: $\omega^2\theta = \omega \cdot \omega\theta$ and $\omega\theta^2 = \omega\theta \cdot \theta$ imply that $k = -ac, l = -ad, m = -bd$.
- Any 4 integers a, b, c, d determine a commutative associative cubic rang via the above multiplication table!

Cubic rings

- Levi-Delone-Faddeev: To a binary cubic form $f = ax^3 + bx^2y + cxy^2 + dy^3$ we associate the cubic ring R with a normal basis $1, \omega, \theta$ and multiplication

$$\omega^2 = -ac - b\omega + a\theta$$
$$\omega\theta = -ad$$
$$\theta^2 = -bd - d\omega + c\theta$$

Cubic rings

- Levi-Delone-Faddeev: To a binary cubic form $f = ax^3 + bx^2y + cxy^2 + dy^3$ we associate the cubic ring R with a normal basis $1, \omega, \theta$ and multiplication

$$\omega^2 = -ac - b\omega + a\theta$$
$$\omega\theta = -ad$$
$$\theta^2 = -bd - d\omega + c\theta$$

- We have a bijection:

$$\{\text{Binary cubic forms } f(x,y) \in \mathbb{Z}[x,y]\} \leftrightarrow \{\text{Based cubic rings } (R,\omega,\theta)$$

- Suppose that $\mathrm{Disc}(f) \neq 0$, $f = ax^3 + bx^2y + cxy^2 + dy^3$. Then $X = \{(x : y) \in \mathbb{P}^1(\bar{\mathbb{Q}}) | f(x, y) = 0\}$ consists of 3 different points which are permuted by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

- Suppose that $\mathrm{Disc}(f) \neq 0$, $f = ax^3 + bx^2y + cxy^2 + dy^3$. Then $X = \{(x : y) \in \mathbb{P}^1(\bar{\mathbb{Q}}) | f(x, y) = 0\}$ consists of 3 different points which are permuted by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- The ring $\Gamma(X)$ of global functions on X is a cubic algebra over $\mathbb{Q}$.

- Suppose that $\mathrm{Disc}(f) \neq 0$, $f = ax^3 + bx^2y + cxy^2 + dy^3$. Then $X = \{(x : y) \in \mathbb{P}^1(\bar{\mathbb{Q}}) | f(x, y) = 0\}$ consists of 3 different points which are permuted by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- The ring $\Gamma(X)$ of global functions on X is a cubic algebra over $\mathbb{Q}$.
- The cubic ring R associated to f is an order in the algebra $\Gamma(X)$.
- Explicitly, if f is irreducible and $f(\alpha, 1) = 0$ for $\alpha \in \bar{\mathbb{Q}}$: $R \cong \mathbb{Z}[a \cdot \alpha, d/\alpha] \subset \mathbb{Q}(\alpha)$, with $\omega \mapsto a \cdot \alpha$ and $\theta \mapsto d/\alpha$

Quartic and quintic rings

- Bhargava: parametrizations of quartic and quintic rings.
- $n = 4$: To a pair of quadratic forms $f, g \in \mathbb{Z}[x_1, x_2, x_3]$ one attaches a quartic ring R together with a normal $\mathbb{Z}$-basis $1, \alpha_1, \alpha_2, \alpha_3$.

Quartic and quintic rings

- Bhargava: parametrizations of quartic and quintic rings.
- $n = 4$: To a pair of quadratic forms $f, g \in \mathbb{Z}[x_1, x_2, x_3]$ one attaches a quartic ring R together with a normal $\mathbb{Z}$-basis $1, \alpha_1, \alpha_2, \alpha_3$.
- The multiplication table for R w.r.t. this basis is given by explicit polynomials in terms of the coefficients of f and g.

Quartic and quintic rings

- Bhargava: parametrizations of quartic and quintic rings.
- $n = 4$: To a pair of quadratic forms $f, g \in \mathbb{Z}[x_1, x_2, x_3]$ one attaches a quartic ring R together with a normal $\mathbb{Z}$-basis $1, \alpha_1, \alpha_2, \alpha_3$.
- The multiplication table for R w.r.t. this basis is given by explicit polynomials in terms of the coefficients of f and g.
- Every quartic ring arises from a pair (f, g) like this, and two rings are isomorphic if and only if their corresponding pairs of quadrics are are $\mathbb{Z}$-equivalent.

- A pair (f, g) of quadrics corresponds to a pair of conics $V(f)$ and $V(g)$ in $\mathbb{P}^2$,
- For generic (f, g), their intersection $X = V(f) \cap V(g)$ is a set of 4 points in $\mathbb{P}^2$ in general position (no 3 are on a line).

- A pair (f, g) of quadrics corresponds to a pair of conics $V(f)$ and $V(g)$ in $\mathbb{P}^2$,
- For generic (f, g), their intersection $X = V(f) \cap V(g)$ is a set of 4 points in $\mathbb{P}^2$ in general position (no 3 are on a line).
- The ring $\Gamma(X)$ of global functions on these 4 points is a quartic algebra over $\mathbb{Q}$, and the ring R associated to (f, g) is an order in $\Gamma(X)$.

- A pair (f, g) of quadrics corresponds to a pair of conics $V(f)$ and $V(g)$ in $\mathbb{P}^2$,
- For generic (f, g), their intersection $X = V(f) \cap V(g)$ is a set of 4 points in $\mathbb{P}^2$ in general position (no 3 are on a line).
- The ring $\Gamma(X)$ of global functions on these 4 points is a quartic algebra over $\mathbb{Q}$, and the ring R associated to (f, g) is an order in $\Gamma(X)$.
- $n = 5$: To an alternating 5×5-matrix A with entries linear forms in $\mathbb{Z}[x_1, \ldots, x_4]$ one attaches a quintic ring R with a basis $1, \alpha_1, \ldots, \alpha_4$.

- A pair (f, g) of quadrics corresponds to a pair of conics $V(f)$ and $V(g)$ in $\mathbb{P}^2$,
- For generic (f, g), their intersection $X = V(f) \cap V(g)$ is a set of 4 points in $\mathbb{P}^2$ in general position (no 3 are on a line).
- The ring $\Gamma(X)$ of global functions on these 4 points is a quartic algebra over $\mathbb{Q}$, and the ring R associated to (f, g) is an order in $\Gamma(X)$.
- $n = 5$: To an alternating 5×5-matrix A with entries linear forms in $\mathbb{Z}[x_1, \ldots, x_4]$ one attaches a quintic ring R with a basis $1, \alpha_1, \ldots, \alpha_4$.
- A generic A determines a set X of 5 points in general position in $\mathbb{P}^3$. The ring R is an order in the ring of global functions of X.

Generalizing to $n \geq 5$

- From now on we assume that R is non-degenerate — the trace pairing on $R \otimes \mathbb{Q}$ is non-degenerate.

Generalizing to $n \geq 5$

- From now on we assume that R is non-degenerate — the trace pairing on $R \otimes \mathbb{Q}$ is non-degenerate.
- To a non-degenerate rank n ring R we associate a set X of n points in $\mathbb{P}^{n-2}$ in general position.

Generalizing to $n \geq 5$

- From now on we assume that R is non-degenerate — the trace pairing on $R \otimes \mathbb{Q}$ is non-degenerate.
- To a non-degenerate rank n ring R we associate a set X of n points in $\mathbb{P}^{n-2}$ in general position.
- Choose a basis $1, \alpha_1, \ldots, \alpha_{n-1}$ of R and let $1, \alpha_1^*, \ldots, \alpha_{n-1}^*$ be the dual basis of $R \otimes \mathbb{Q}$ w.r.t the trace pairing.

Generalizing to $n \geq 5$

- From now on we assume that R is non-degenerate — the trace pairing on $R \otimes \mathbb{Q}$ is non-degenerate.
- To a non-degenerate rank n ring R we associate a set X of n points in $\mathbb{P}^{n-2}$ in general position.
- Choose a basis $1, \alpha_1, \ldots, \alpha_{n-1}$ of R and let $1, \alpha_1^*, \ldots, \alpha_{n-1}^*$ be the dual basis of $R \otimes \mathbb{Q}$ w.r.t the trace pairing.
- Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of $R \otimes \mathbb{Q}$ into $\bar{\mathbb{Q}}$. Then the n points in $\mathbb{P}^{n-2}$ are given by

$$X := \{(\sigma_i(\alpha_1^*) : \sigma_i(\alpha_2^*) : \ldots : \sigma_i(\alpha_{n-1}^*)) : 1 \leq i \leq n\}.$$

- The action of Galois permutes the points of X.

Generalizing to $n \geq 5$

- From now on we assume that R is non-degenerate — the trace pairing on $R \otimes \mathbb{Q}$ is non-degenerate.
- To a non-degenerate rank n ring R we associate a set X of n points in $\mathbb{P}^{n-2}$ in general position.
- Choose a basis $1, \alpha_1, \ldots, \alpha_{n-1}$ of R and let $1, \alpha_1^*, \ldots, \alpha_{n-1}^*$ be the dual basis of $R \otimes \mathbb{Q}$ w.r.t the trace pairing.
- Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of $R \otimes \mathbb{Q}$ into $\bar{\mathbb{Q}}$. Then the n points in $\mathbb{P}^{n-2}$ are given by

$$X := \{(\sigma_i(\alpha_1^*) : \sigma_i(\alpha_2^*) : \ldots : \sigma_i(\alpha_{n-1}^*)) : 1 \leq i \leq n\}.$$

- The action of Galois permutes the points of X.
- We construct a multiplication table for R from the minimal graded free resolution of the set X.

- Let $R := \mathbb{Q}[x_1, \ldots, x_{n-1}]$. A resolution of X is a chain complex of graded free R-modules

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

- Here $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$. Maps ϕ_1 and ϕ_{n-2} are row and column vectors of quadratic forms. The other ϕ_i are matrices of linear forms.

- Let $R := \mathbb{Q}[x_1, \ldots, x_{n-1}]$. A resolution of X is a chain complex of graded free R-modules

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

- Here $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$. Maps ϕ_1 and ϕ_{n-2} are row and column vectors of quadratic forms. The other ϕ_i are matrices of linear forms.
- $\phi_1 := (f_1, \ldots, f_m)$ is a vector of quadratic forms that generate the ideal $I(X)$ that defines X.

- Let $R := \mathbb{Q}[x_1, \ldots, x_{n-1}]$. A resolution of X is a chain complex of graded free R-modules

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

- Here $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$. Maps ϕ_1 and ϕ_{n-2} are row and column vectors of quadratic forms. The other ϕ_i are matrices of linear forms.
- $\phi_1 := (f_1, \ldots, f_m)$ is a vector of quadratic forms that generate the ideal $I(X)$ that defines X.
- $\phi_2 = (l_j^i)$ is a matrix of linear forms. Columns of ϕ_2 correspond to relations between the generators f_i:

$$\begin{gathered} l_1^1 \cdot f_1 + \ldots + l_m^1 \cdot f_m = 0 \\ \vdots \\ l_1^k \cdot f_1 + \ldots + l_m^k \cdot f_m = 0 \end{gathered}$$

- Let $R := \mathbb{Q}[x_1, \ldots, x_{n-1}]$. A resolution of X is a chain complex of graded free R-modules

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

- Here $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$. Maps ϕ_1 and ϕ_{n-2} are row and column vectors of quadratic forms. The other ϕ_i are matrices of linear forms.
- $\phi_1 := (f_1, \ldots, f_m)$ is a vector of quadratic forms that generate the ideal $I(X)$ that defines X.
- $\phi_2 = (l_j^i)$ is a matrix of linear forms. Columns of ϕ_2 correspond to relations between the generators f_i:

$$\begin{gathered} l_1^1 \cdot f_1 + \ldots + l_m^1 \cdot f_m = 0 \\ \vdots \\ l_1^k \cdot f_1 + \ldots + l_m^k \cdot f_m = 0 \end{gathered}$$

- ϕ_3 encodes all linear relations that these relations satisfy, and so on.

Examples of resolutions

- Let $X \subset \mathbb{P}^1$ is a set of 3 distinct points. Then X is defined by the vanishing of a binary cubic form $f(x_1, x_2)$, and the resolution is just

$$R(-3) \xrightarrow{f} R$$

- $n = 4$, $X \subset \mathbb{P}^2$ a set of 4 points defined by the vanishing of f and g. We easily observe the relation $(-g) \cdot f + f \cdot g = 0$, and any relation $l_1 \cdot f + l_2 \cdot g = 0$ is a multiple of this one. The resolution of X is

$$R(-4) \xrightarrow{\begin{pmatrix} -g \\ f \end{pmatrix}} R(-2)^2 \xrightarrow{\begin{pmatrix} f & g \end{pmatrix}} R$$

- For $n = 5$, $X \subset \mathbb{P}^3$ a set of 5 points, the resolution is

$$R(-5) \xrightarrow{\phi^T} R(-3)^5 \xrightarrow{A} R(-2)^5 \xrightarrow{\phi} R$$

where A is an alternating 5×5 matrix of linear forms in $x_1, \ldots, x_4$. Entries of ϕ are the five 4×4-Pfafians of A.

- Let $X \subset \mathbb{P}^{n-2}$ be a set of n points in general position, defined over $\mathbb{Q}$, and let $F_\bullet$ the minimal free resolution of its homogeneous ideal.

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

- For $1 \leq a_1, \ldots, a_{n-2} \leq n-1$, define

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

  These are quadratic forms in $x_1, \ldots, x_{n-1}$.

- Let $X \subset \mathbb{P}^{n-2}$ be a set of n points in general position, defined over $\mathbb{Q}$, and let $F_\bullet$ the minimal free resolution of its homogeneous ideal.

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

- For $1 \leq a_1, \ldots, a_{n-2} \leq n-1$, define

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

  These are quadratic forms in $x_1, \ldots, x_{n-1}$.
- Consider the $(n-2)$-cycle $\sigma = (12 \ldots n-2) \in S_{n-2}$. Set:

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

- Finally, we set $\Omega_k = (-1)^k [[1, 2, \ldots, \hat{k}, \ldots, n-1]]$.

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

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

where $c_{ij}^0 \in \mathbb{Q}$ uniquely determined by the associative law in terms of $\frac{\partial^2 \Omega_k}{\partial x_i \partial x_j}$.

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

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

where $c_{ij}^0 \in \mathbb{Q}$ uniquely determined by the associative law in terms of $\frac{\partial^2 \Omega_k}{\partial x_i \partial x_j}$.

- Suppose that the resolution $F_\bullet$ of X is scaled so that the matrices ϕ_i have integer coefficients. Then $\frac{\partial^2 \Omega_k}{\partial x_i \partial x_j}$ are integers by construction, and so we have a multiplication table for an order $\mathcal{O}$ in A.

- The multiplication table for the order B recovers the Levi-Delone-Faddeev and Bhargava parametrizations for non-degenerate rings when we specialize to $n \leq 5$.

- The multiplication table for the order B recovers the Levi-Delone-Faddeev and Bhargava parametrizations for non-degenerate rings when we specialize to $n \leq 5$.
- For example: Let $f(x_1, x_2)$ be a binary cubic and consider the free resolution

$$R(-3) \xrightarrow{\cdot f} R$$

The multiplication table constructed in our theorem (after normalizing the basis α_1, α_2) is the same as the one of Delone-Faddev correspondence.

- The multiplication table for the order B recovers the Levi-Delone-Faddeev and Bhargava parametrizations for non-degenerate rings when we specialize to $n \leq 5$.
- For example: Let $f(x_1, x_2)$ be a binary cubic and consider the free resolution

$$R(-3) \xrightarrow{\cdot f} R$$

  The multiplication table constructed in our theorem (after normalizing the basis α_1, α_2) is the same as the one of Delone-Faddev correspondence.
- In his 2022 PhD thesis, Seok Hyeong Lee gives a different construction of a ring of rank n attached to a free resolution of n points, by computing the hypercohomology of the resolution the Cech coverings. This method was also used in the work of Melanie Wood on ring parametrizations.

Some applications

- Let $C \subset \mathbb{P}^{n-1}$ be a smooth genus one curve of degree n defined over $\mathbb{Q}$, $n \geq 3$.

Some applications

- Let $C \subset \mathbb{P}^{n-1}$ be a smooth genus one curve of degree n defined over $\mathbb{Q}$, $n \geq 3$.
- The minimal free resolution of C has the same shape as the resolution of a set of n points, with one extra variable.
- When $n = 3$, $C \subset \mathbb{P}^2$ is cut out by a cubic form $F(x_1, x_2, x_3)$,
- When $n = 4$, $C \subset \mathbb{P}^3$ is the intersection of two quadrics $P(x_1, x_2, x_3, x_4), Q(x_1, x_2, x_3, x_4)$

Some applications

- Let $C \subset \mathbb{P}^{n-1}$ be a smooth genus one curve of degree n defined over $\mathbb{Q}$, $n \geq 3$.
- The minimal free resolution of C has the same shape as the resolution of a set of n points, with one extra variable.
- When $n = 3$, $C \subset \mathbb{P}^2$ is cut out by a cubic form $F(x_1, x_2, x_3)$,
- When $n = 4$, $C \subset \mathbb{P}^3$ is the intersection of two quadrics $P(x_1, x_2, x_3, x_4), Q(x_1, x_2, x_3, x_4)$
- When C has points over every completion of $\mathbb{Q}$, it represents an element of $Ш(E/\mathbb{Q})[n]$. If it has no $\mathbb{Q}$-points, it is a non-trivial element.

- For any hyperplane H, the intersection of $C \cap H$ is a set of n points in $\mathbb{P}^{n-2}$ in general position, and C has a point defined over the corresponding degree n algebra A.

- For any hyperplane H, the intersection of $C \cap H$ is a set of n points in $\mathbb{P}^{n-2}$ in general position, and C has a point defined over the corresponding degree n algebra A.
- Theorem in my thesis: there is a constant $c(n) \in \mathbb{R}$ such that any such $C \subset \mathbb{P}^{n-1}$ that is everywhere locally soluble has a point over a degree n number field of discriminant at most $c(n)H_E^{2n-2}$, where H_E is the naive height of $E = \mathrm{Jac}(C)$

- For any hyperplane H, the intersection of $C \cap H$ is a set of n points in $\mathbb{P}^{n-2}$ in general position, and C has a point defined over the corresponding degree n algebra A.
- Theorem in my thesis: there is a constant $c(n) \in \mathbb{R}$ such that any such $C \subset \mathbb{P}^{n-1}$ that is everywhere locally soluble has a point over a degree n number field of discriminant at most $c(n)H_E^{2n-2}$, where H_E is the naive height of $E = \mathrm{Jac}(C)$
- Now fix $n = 3$ and suppose $C \subset \mathbb{P}^2$ is defined by a ternary cubic $F(x_1, x_2, x_3) \in \mathbb{Z}[x_1, x_2, x_3]$. Let $g \in \mathbb{Z}[x_1, x_2, x_3]$ be a quadratic form, which defines a plane conic $Q \subset \mathbb{P}^2$.
- By Bezout's theorem, $|C \cap Q| = 6$. The embedding $\mathbb{P}^2 \to \mathbb{P}^5$

$$(x : y : z) \mapsto (x^2 : y^2 : z^2 : xy : yz : zx)$$

maps Q to a hyperplane H in $\mathbb{P}^5$, C to a genus one curve D of degree 6, and hence $C \cap Q$ to $D \cap H$.

- For any hyperplane H, the intersection of $C \cap H$ is a set of n points in $\mathbb{P}^{n-2}$ in general position, and C has a point defined over the corresponding degree n algebra A.
- Theorem in my thesis: there is a constant $c(n) \in \mathbb{R}$ such that any such $C \subset \mathbb{P}^{n-1}$ that is everywhere locally soluble has a point over a degree n number field of discriminant at most $c(n)H_E^{2n-2}$, where H_E is the naive height of $E = \mathrm{Jac}(C)$
- Now fix $n = 3$ and suppose $C \subset \mathbb{P}^2$ is defined by a ternary cubic $F(x_1, x_2, x_3) \in \mathbb{Z}[x_1, x_2, x_3]$. Let $g \in \mathbb{Z}[x_1, x_2, x_3]$ be a quadratic form, which defines a plane conic $Q \subset \mathbb{P}^2$.
- By Bezout's theorem, $|C \cap Q| = 6$. The embedding $\mathbb{P}^2 \to \mathbb{P}^5$

$$(x : y : z) \mapsto (x^2 : y^2 : z^2 : xy : yz : zx)$$

maps Q to a hyperplane H in $\mathbb{P}^5$, C to a genus one curve D of degree 6, and hence $C \cap Q$ to $D \cap H$.

- Upshot: To a pair (f, g) of a cubic and a quadric in $\mathbb{Z}[x_1, x_2, x_3]$ we attach a sextic ring.

Thanks for listening!

- Where does the basis $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ come from?

- Where does the basis $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ come from?
- $n = 3$ and $f(x_1, x_2)$ a binary cubic form. The free resolution of graded modules

$$0 \to R(-3) \xrightarrow{f} R \to R/fR(-3) \to 0$$

corresponds to a free resolution of sheaves on $\mathbb{P}^1$

$$0 \to \mathcal{O}_{\mathbb{P}^1}(-3) \xrightarrow{f} \mathcal{O}_{\mathbb{P}^1} \to \mathcal{O}_X \to 0$$

where $\mathcal{O}_{\mathbb{P}^1}$ and $\mathcal{O}_X$ is the sheaf of regular functions on $\mathbb{P}^1$ and X. We take the long exact sequence of cohomology:

$$0 \to H^0(\mathcal{O}_{\mathbb{P}^1}) \to H^0(\mathcal{O}_X) \to H^1(\mathcal{O}_{\mathbb{P}^1}(-3)) \to 0$$

- $H^0(\mathcal{O}_X)$ is a cubic algebra over $\mathbb{Q}$. The map $H^0(\mathcal{O}_{\mathbb{P}^1}) \to H^0(\mathcal{O}_X)$ corresponds to the constant function $1 \in H^0(\mathcal{O}_X)$. We can identify $H^1(\mathcal{O}_{\mathbb{P}^1}(-3))$ with $A/(\mathbb{Q} \cdot 1)$.
- Having chosen coordinates x_1, x_2 on $\mathbb{P}^1$, we can also identify $H^1(\mathcal{O}_{\mathbb{P}^1}(-3))$ with the space of degree -3 polynomials in $\frac{1}{x_1 x_2}\mathbb{Q}[\frac{1}{x_1}, \frac{1}{x_2}]$.

- $H^0(\mathcal{O}_X)$ is a cubic algebra over $\mathbb{Q}$. The map $H^0(\mathcal{O}_{\mathbb{P}^1}) \to H^0(\mathcal{O}_X)$ corresponds to the constant function $1 \in H^0(\mathcal{O}_X)$. We can identify $H^1(\mathcal{O}_{\mathbb{P}^1}(-3))$ with $A/(\mathbb{Q} \cdot 1)$.
- Having chosen coordinates x_1, x_2 on $\mathbb{P}^1$, we can also identify $H^1(\mathcal{O}_{\mathbb{P}^1}(-3))$ with the space of degree -3 polynomials in $\frac{1}{x_1 x_2}\mathbb{Q}[\frac{1}{x_1}, \frac{1}{x_2}]$.
- The Delone-Faddeev basis ω, θ of $A/(\mathbb{Q} \cdot 1)$ then corresponds to the basis $\frac{1}{x_1^2 x_2}, \frac{1}{x_1 x_2^2}$ of $H^1(\mathcal{O}_{\mathbb{P}^1}(-3))$.