Binary forms of given discriminant and given invariant order

Jan-Hendrik Evertse
Universiteit Leiden

Current Trends in Diophantine Geometry and Transcendence

Taipei, May 23, 2016

Slides will be posted on http://pub.math.leidenuniv.nl/∼evertsejh/lectures.shtml

Discriminants of binary forms

The discriminant of a binary form

$$F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$$

is given by $D(F) = \prod_{1\leq i<j\leq n}(\alpha_i\beta_j - \alpha_j\beta_i)^2$.

For $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we define $F_U(X,Y) := F(aX+bY, cX+dY)$.

Properties:

(i) *$D(F)$ is a homogeneous polynomial in $\mathbb{Z}[a_0,\ldots,a_n]$ of degree $2n-2$;*

(ii) *$D(\lambda F_U) = \lambda^{2n-2}(\det U)^{n(n-1)}D(F)$ for every scalar λ and 2×2-matrix U.*

$GL(2, A)$-equivalence of binary forms

Definition

Let A be a non-zero commutative ring. Two binary forms $F, G \in A[X, Y]$ are called $GL(2, A)$-equivalent if there are $\varepsilon \in A^*$ and $U \in GL(2, A)$ such that $G = \varepsilon F_U$.

Fact:

Let $F, G \in A[X, Y]$ be two $GL(2, A)$-equivalent binary forms. Then $D(G) = \eta D(F)$ for some $\eta \in A^*$.

For integral domains A of characteristic 0 and non-zero $\delta \in A$, we consider the "discriminant equation"

$$D(F) \in \delta A^* := \{\delta\eta : \eta \in A^*\} \text{ in binary forms } F \in A[X, Y].$$

The solutions of this equation can be divided into $GL(2, A)$-equivalence classes.

A finiteness result over the S-integers

Let K be an algebraic number field and S a finite set of places of K, containing all infinite places. Denote by O_S the ring of S-integers of K.

Theorem (Birch and Merriman, 1972)

Let $n \geq 2$. Then there are only finitely many $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in O_S^*$.

The proof of Birch and Merriman is *ineffective*, in that it does not give a method to determine the equivalence classes.

E. and Győry (1991) proved in an effective way that for every $\delta \in O_S \setminus \{0\}$, the binary forms $F \in O_S[X, Y]$ with

$$D(F) \in \delta O_S^*$$

lie in only finitely many $GL(2, O_S)$-eq. classes. This was recently sharpened.

An effective result

For $\alpha \in \overline{\mathbb{Q}}$, denote by $h(\alpha)$ the absolute logarithmic Weil height of α. For a binary form $F \in \overline{\mathbb{Q}}[X, Y]$, define $h(F) := \max h(\text{coeff of } F)$.

Denote by $|\mathcal{A}|$ the cardinality of a set $\mathcal{A}$.

Let K be a number field of degree d and S a finite set of places of K, containing all infinite places.

Theorem 1 (E., Győry, 2016(?))

Let $n \geq 4$ and $\delta \in O_S \setminus \{0\}$. Then every binary form $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ is $GL(2, O_S)$-equivalent to a binary form F^* for which

$$h(F^*) \leq C_1^{\mathrm{eff}}(K, S, n) \cdot |O_S/\delta O_S|^{5n-3},$$

where $C_1^{\mathrm{eff}}(K, S, n)$ is an effectively computable number, depending only on K, S and n.

For binary forms of degree 2 or 3 one can deduce by elementary means a similar result with $h(F^*) \leq C_2^{\mathrm{eff}}(K, S) + \frac{1}{d} \cdot \log |O_S/\delta O_S|$.

An outline of the proof (I)

Let $F \in O_S[X,Y]$ be a binary form of degree $n \geq 4$ with $D(F) \in \delta O_S^*$.
Denote by L its splitting field over K, i.e., the smallest extension over K over which F can be factorized into linear forms.
Write $F(X,Y) = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ with $\alpha_i, \beta_i \in L$.

- Apply effective finiteness results for S-unit equations to the identities

$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1, \text{ where } \Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \ (1 \leq p < q \leq n).$$

  This leads to an effective upper bound in terms of K, S, n, δ for the heights of $cr_{ijkl}(F) := \Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl}$ $(1 \leq i < j < k < l \leq n)$.
  Notice that $cr_{ijkl}(F)$ is the cross ratio of the four zeros $P_i := (\beta_i : \alpha_i), P_j, P_k, P_l \in \mathbb{P}^1(L)$ of F.

An outline of the proof (II)

- We have an effective upper bound in terms of K, S, n, δ for the heights of the cross ratios $cr_{ijkl}(F)$, for all binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ and all $i, j, k, l \in \{1, \dots, n\}$.

An outline of the proof (II)

- We have an effective upper bound in terms of K, S, n, δ for the heights of the cross ratios $cr_{ijkl}(F)$, for all binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ and all $i, j, k, l \in \{1, \dots, n\}$.
- Projective geometry and Galois invariance imply that if $F, G \in O_S[X, Y]$ are two binary forms of degree $n \geq 4$ such that $cr_{ijkl}(F) = cr_{ijkl}(G)$ for all i, j, k, l then there is a unique projective transformation defined over K mapping the zeros of F to those of G. This means that F, G are $GL(2, K)$-equivalent, i.e., $G = \lambda F_U$ for some $\lambda \in K^*$ and $U \in GL(2, K)$.

An outline of the proof (II)

- We have an effective upper bound in terms of K, S, n, δ for the heights of the cross ratios $cr_{ijkl}(F)$, for all binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ and all $i, j, k, l \in \{1, \ldots, n\}$.
- Projective geometry and Galois invariance imply that if $F, G \in O_S[X, Y]$ are two binary forms of degree $n \geq 4$ such that $cr_{ijkl}(F) = cr_{ijkl}(G)$ for all i, j, k, l then there is a unique projective transformation defined over K mapping the zeros of F to those of G. This means that F, G are $GL(2, K)$-equivalent, i.e., $G = \lambda F_U$ for some $\lambda \in K^*$ and $U \in GL(2, K)$.
- Thus, the binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ lie in finitely many $GL(2, K)$-eq. classes, and each of them contains a binary form with height below an effective bound in terms of K, S, n, δ.

An outline of the proof (II)

- We have an effective upper bound in terms of K, S, n, δ for the heights of the cross ratios $cr_{ijkl}(F)$, for all binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ and all $i, j, k, l \in \{1, \dots, n\}$.
- Projective geometry and Galois invariance imply that if $F, G \in O_S[X, Y]$ are two binary forms of degree $n \geq 4$ such that $cr_{ijkl}(F) = cr_{ijkl}(G)$ for all i, j, k, l then there is a unique projective transformation defined over K mapping the zeros of F to those of G. This means that F, G are $GL(2, K)$-equivalent, i.e., $G = \lambda F_U$ for some $\lambda \in K^*$ and $U \in GL(2, K)$.
- Thus, the binary forms $F \in O_S[X, Y]$ of degree n with $D(F) \in \delta O_S^*$ lie in finitely many $GL(2, K)$-eq. classes, and each of them contains a binary form with height below an effective bound in terms of K, S, n, δ.
- Using adèlic geometry of numbers one shows that each of these $GL(2, K)$-eq. classes is the union of finitely many $GL(2, O_S)$-eq. classes, and that each of them contains a binary form with height below an effective bound in terms of K, S, n, δ. □

A function field analogue

Let $A := \mathbb{C}[t]$, $K := \mathbb{C}(t)$ with t a variable.
For a binary form $F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X, Y]$, put $h(F) := \max_i \deg a_i$.

Theorem (Zhuang, PhD-thesis, Leiden, 2015)

Let $\delta \in A \setminus \{0\}$ and $F \in A[X, Y]$ a binary form of degree $n \geq 4$ with $D(F) = \delta$. Then F is $GL(2, A)$-equivalent to a binary form F^* with

$$h(F^*) \leq n^2 + 5n - 6 + (20 + n^{-1}) \deg \delta.$$

A function field analogue

Let $A := \mathbb{C}[t]$, $K := \mathbb{C}(t)$ with t a variable.
For a binary form $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X,Y]$, put $h(F) := \max_i \deg a_i$.

Theorem (Zhuang, PhD-thesis, Leiden, 2015)

Let $\delta \in A \setminus \{0\}$ and $F \in A[X,Y]$ a binary form of degree $n \geq 4$ with $D(F) = \delta$. Then F is $GL(2,A)$-equivalent to a binary form F^* with

$$h(F^*) \leq n^2 + 5n - 6 + (20 + n^{-1}) \deg \delta.$$

Idea.

Write $F(X,Y) = \prod_{i=1}^n (\alpha_i X - \beta_i Y)$ with α_i, β_i in the splitting field L of F over K. Apply Mason's abc-theorem for function fields to the identities

$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1, \quad \text{where } \Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \ (1 \leq p < q \leq n).$$

$\square$

A conjecture over number fields

Zhuang's theorem can be translated into a *conjecture* over the ring of S-integers in a number field K by replacing $\deg \delta$ by $\frac{1}{[K:\mathbb{Q}]} \cdot \log |O_S/\delta O_S|$.

A conjecture over number fields

Zhuang's theorem can be translated into a *conjecture* over the ring of S-integers in a number field K by replacing $\deg \delta$ by $\frac{1}{[K:\mathbb{Q}]} \cdot \log |O_S/\delta O_S|$.

Conjecture

Let K be a number field of degree d and S a finite set of places of K, containing all infinite places. Further, let $n \geq 4$, $\delta \in O_S \setminus \{0\}$ and let $F \in O_S[X,Y]$ be a binary form of degree n with $D(F) \in \delta O_S^*$.
Then F is $GL(2, O_S)$-equivalent to a binary form F^* with

$$h(F^*) \leq C_3(n, K, S) + \frac{C_4}{d} \cdot \log |O_S/\delta O_S| \quad (C_4 \text{ absolute constant}).$$

Proof, assuming abc over number fields.

Follow Zhuang's proof, and apply the abc-conjecture over number fields instead of Mason's abc-theorem to the identities

$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1. \qquad \square$$

The number of equivalence classes

Let as before K be a number field and S a finite set of places of K, containing all infinite places.

We now consider upper bounds for the *number* of $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ with

$$D(F) \in \delta O_S^*, \quad \deg F = n.$$

We focus on the dependence on δ of such bounds.

The number of equivalence classes

Theorem (Bérczes, E., Győry, 2004)

Let K be a number field, S a finite set of places of K containing all infinite places, L a finite normal extension of K, $n \geq 3$ and $\delta \in O_S \setminus \{0\}$.

Then the number of $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ such that

(1) $\qquad D(F) \in \delta O_S^*, \quad \deg F = n, \quad$ *F has splitting field L over K*

is at most $C^{\mathrm{eff}}(n, K, |S|, \epsilon) \cdot |O_S/\delta O_S|^{(1/n(n-1))+\epsilon}$ for all $\epsilon > 0$.

Idea of proof.

Write $F(X, Y) = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ with $\alpha_i, \beta_i \in L$.
Put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p$ and apply estimates for the number of solutions of S-unit equations to

$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1. \qquad \square$$

The number of equivalence classes

Theorem (Bérczes, E., Győry, 2004)

Let K be a number field, S a finite set of places of K containing all infinite places, L a finite normal extension of K, $n \geq 3$ and $\delta \in O_S \setminus \{0\}$.

Then the number of $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ such that

(1) $\quad D(F) \in \delta O_S^*, \quad \deg F = n, \quad$ *F has splitting field L over K*

is at most $C^{\mathrm{eff}}(n, K, |S|, \epsilon) \cdot |O_S/\delta O_S|^{(1/n(n-1))+\epsilon}$ for all $\epsilon > 0$.

The exponent $\frac{1}{n(n-1)}$ is best possible.

For instance, fix a binary form $F_0 \in O_S[X, Y]$ of degree n with $D(F_0) \neq 0$ and some non-zero $a \in O_S$.

Then the binary forms $F_b(X, Y) := F_0(aX, bX + Y)$ ($b \in O_S$) all have discriminant $a^{n(n-1)} D(F_0) =: \delta$, have the same splitting field, and lie in

$$\gg_{F_0} |O_S/aO_S| \gg_{F_0} |O_S/\delta O_S|^{1/n(n-1)} \; GL(2, O_S)\text{-eq. classes.}$$

The number of equivalence classes

Theorem (Bérczes, E., Győry, 2004)

Let K be a number field, S a finite set of places of K containing all infinite places, L a finite normal extension of K, $n \geq 3$ and $\delta \in O_S \setminus \{0\}$.

Then the number of $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ such that

$$(1) \qquad D(F) \in \delta O_S^*, \quad \deg F = n, \quad F \text{ has splitting field } L \text{ over } K$$

is at most $C^{\mathrm{eff}}(n, K, |S|, \epsilon) \cdot |O_S/\delta O_S|^{(1/n(n-1))+\epsilon}$ for all $\epsilon > 0$.

Open problem: Can we get a similar upper bound without fixing the splitting field L of the binary forms under consideration?

The number of equivalence classes

Theorem (Bérczes, E., Győry, 2004)

Let K be a number field, S a finite set of places of K containing all infinite places, L a finite normal extension of K, $n \geq 3$ and $\delta \in O_S \setminus \{0\}$.

Then the number of $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ such that

$$(1) \qquad D(F) \in \delta O_S^*, \quad \deg F = n, \quad F \text{ has splitting field } L \text{ over } K$$

is at most $C^{\mathrm{eff}}(n, K, |S|, \epsilon) \cdot |O_S/\delta O_S|^{(1/n(n-1))+\epsilon}$ for all $\epsilon > 0$.

Open problem: Can we get a similar upper bound without fixing the splitting field L of the binary forms under consideration?

If there is a binary form $F \in O_S[X, Y]$ with (1), then $g := [L : K]$ divides $n!$ and $\delta^g \in \mathfrak{d}_{L/K} O_S$, where $\mathfrak{d}_{L/K}$ is the relative discriminant of L/K.

What is the number of such L? Maybe $\ll_{K,S,n,\epsilon} |O_S/\delta O_S|^\epsilon$ for all $\epsilon > 0$?

The invariant order of a binary form

Let A be any commutative ring $\neq \{0\}$. An *A-order of rank n* is a commutative ring whose additive structure is a free A-module of rank n.

Following Nakagawa (1989) and Simon (2001), we attach to every binary form $F \in A[X,Y]$ of degree n an A-order A_F of rank n, called the *invariant A-order of F*, which has the following properties:

(i) If $F, G \in A[X,Y]$ are two $GL(2,A)$-equivalent binary forms, then $A_F \cong A_G$ (as A-algebras);

(ii) A_F determines $D(F)$ up to a factor from A^*. That is, if $F, G \in A[X,Y]$ are binary forms with $A_F \cong A_G$, then $D(G) = \eta D(F)$ for some $\eta \in A^*$.

The invariant order of a binary form

Let A be any commutative ring $\neq \{0\}$. An *A-order of rank n* is a commutative ring whose additive structure is a free A-module of rank n.

Following Nakagawa (1989) and Simon (2001), we attach to every binary form $F \in A[X, Y]$ of degree n an A-order A_F of rank n, called the *invariant A-order of F*, which has the following properties:

(i) If $F, G \in A[X, Y]$ are two $GL(2, A)$-equivalent binary forms, then $A_F \cong A_G$ (as A-algebras);

(ii) A_F determines $D(F)$ up to a factor from A^*. That is, if $F, G \in A[X, Y]$ are binary forms with $A_F \cong A_G$, then $D(G) = \eta D(F)$ for some $\eta \in A^*$.

We will consider "equations"

$$A_F \cong O \quad \text{in binary forms } F \in A[X, Y] \qquad (O \text{ given } A\text{-order}).$$

Fix a solution $F_0 \in A[X, Y]$ and put $\delta := D(F_0)$. Then every other solution F satisfies $D(F) \in \delta A^*$.

Definition of the invariant order

Let for the moment A be an integral domain with quotient field K of characteristic 0.

Let $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X,Y]$ be a binary form that is irreducible over K.

Define $L = K(\theta)$ where $F(\theta,1) = 0$, let A_F be the free A-module with basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ where

$$\omega_i := a_0\theta^i + a_1\theta^{i-1} + \cdots + a_{i-1}\theta \quad (i = 1, \ldots, n-1),$$

and let $\omega_n := -a_n$. Then for $1 \le i, j \le n-1$,

$$(*) \qquad \omega_i\omega_j = -\sum_{\max(i+j-n,1)\le k\le i} a_{i+j-k}\omega_k + \sum_{j<k\le\min(i+j,n)} a_{i+j-k}\omega_k.$$

We call A_F the *invariant A-order* of F.

We can use (*) to extend this to arbitrary commutative rings A and arbitrary binary forms F.

Extension to arbitrary rings and binary forms

Definition:

Let A be an arbitrary non-zero commutative ring and
$F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X, Y]$ any binary form.

The *invariant A-order* A_F of F is the free A-module with basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ with prescribed multiplication rules

$$\omega_i\omega_j = -\sum_{\max(i+j-n,1)\leq k\leq i} a_{i+j-k}\omega_k + \sum_{j<k\leq\min(i+j,n)} a_{i+j-k}\omega_k \quad \forall i, j.$$

A_F is indeed a commutative ring (commutative and associative).

Extension to arbitrary rings and binary forms

Definition:

Let A be an arbitrary non-zero commutative ring and $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X,Y]$ any binary form.

The *invariant A-order* A_F of F is the free A-module with basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ with prescribed multiplication rules

$$\omega_i\omega_j = -\sum_{\max(i+j-n,1)\le k\le i} a_{i+j-k}\omega_k + \sum_{j<k\le\min(i+j,n)} a_{i+j-k}\omega_k \quad \forall i,j.$$

Properties:

(i) Let $F, G \in A[X,Y]$ be binary forms. Then

F, G $GL(2,A)$-equivalent $\Longrightarrow A_F \cong A_G$;
$A_F \cong A_G \Longrightarrow D(G) = \eta D(F)$ for some $\eta \in A^*$.

(ii) Let A be an integral domain with quotient field K of characteristic 0 and $F \in A[X,Y]$ a binary form. Then

F irreducible over $K \iff A_F$ integral domain;
$D(F) \neq 0 \iff A_F$ nilpotent-free.

Binary cubic forms vs orders of rank 3

Theorem (Delone and Faddeev; Gan, Gross and Savin; Deligne)

Let A be an arbitrary non-zero commutative ring. Then for every A-order O of rank 3 there is precisely one $GL(2, A)$-equivalence class of cubic forms $F \in A[X, Y]$ with $A_F \cong O$.

Binary cubic forms vs orders of rank 3

Theorem (Delone and Faddeev; Gan, Gross and Savin; Deligne)

Let A be an arbitrary non-zero commutative ring. Then for every A-order O of rank 3 there is precisely one $GL(2, A)$-equivalence class of cubic forms $F \in A[X, Y]$ with $A_F \cong O$.

This was proved by Delone and Faddeev (1940) for $A = \mathbb{Z}$ and $\mathbb{Z}$-orders O that are integral domains, thus with binary forms F that are irreducible over $\mathbb{Q}$.

Then this was extended to arbitrary $\mathbb{Z}$-orders O of rank 3 by Gan, Gross and Savin (2002).

The extension to arbitrary rings A is straightforward (follows also from general unpublished work of Deligne).

The proof uses only elementary algebra.

Binary cubic forms vs orders of rank 3

Theorem (Delone and Faddeev; Gan, Gross and Savin; Deligne)

Let A be an arbitrary non-zero commutative ring. Then for every A-order O of rank 3 there is precisely one $GL(2, A)$-equivalence class of cubic forms $F \in A[X, Y]$ with $A_F \cong O$.

This was proved by Delone and Faddeev (1940) for $A = \mathbb{Z}$ and $\mathbb{Z}$-orders O that are integral domains, thus with binary forms F that are irreducible over $\mathbb{Q}$.

Then this was extended to arbitrary $\mathbb{Z}$-orders O of rank 3 by Gan, Gross and Savin (2002).

The extension to arbitrary rings A is straightforward (follows also from general unpublished work of Deligne).

The proof uses only elementary algebra.

Simon (2001) constructed number fields of degree $n = 4$ and of any prime degree ≥ 5 whose rings of integers are not the invariant $\mathbb{Z}$-order of a binary form.

Quantitative results for orders of rank ≥ 4

Let K be a number field and S a finite set of places of K, containing the infinite places. Denote by $O_{S,F}$ the invariant O_S-order of a binary form $F \in O_S[X, Y]$.

Theorem 2 (Bérczes, E. and Győry, 2004; E. and Győry, 2016(?))

Let O be a nilpotent-free O_S-order of rank $n \geq 4$. Then the binary forms $F \in O_S[X, Y]$ with

$$O_{S,F} \cong O$$

lie in at most

$$\begin{array}{ll} 2^{5n^2|S|} & GL(2, O_S)\text{-equivalence classes if } n \text{ is odd,} \\ h_2(S) \cdot 2^{5n^2|S|} & GL(2, O_S)\text{-equivalence classes if } n \text{ is even,} \end{array}$$

where $h_2(S)$ denotes the number of ideal classes of O_S of order ≤ 2.

This upper bound has no dependence on O other than its rank.

Quantitative results for orders of rank ≥ 4

Let K be a number field and S a finite set of places of K, containing the infinite places. Denote by $O_{S,F}$ the invariant O_S-order of a binary form $F \in O_S[X,Y]$.

Theorem 2 (Bérczes, E. and Győry, 2004; E. and Győry, 2016(?))

Let O be a nilpotent-free O_S-order of rank $n \geq 4$. Then the binary forms $F \in O_S[X,Y]$ with

$$O_{S,F} \cong O$$

lie in at most

$2^{5n^2\lvert S\rvert}$	*$GL(2, O_S)$-equivalence classes if n is odd,*
$h_2(S) \cdot 2^{5n^2\lvert S\rvert}$	*$GL(2, O_S)$-equivalence classes if n is even,*

where $h_2(S)$ denotes the number of ideal classes of O_S of order ≤ 2.

Bérczes, E. and Győry proved this result for O_S-orders O that are integral domains, and with a slightly larger upper bound for the number of equivalence classes. The general result is due to E. and Győry.

Quantitative results for orders of rank ≥ 4

Let K be a number field and S a finite set of places of K, containing the infinite places. Denote by $O_{S,F}$ the invariant O_S-order of a binary form $F \in O_S[X, Y]$.

Theorem 2 (Bérczes, E. and Győry, 2004; E. and Győry, 2016(?))

Let O be a nilpotent-free O_S-order of rank $n \geq 4$. Then the binary forms $F \in O_S[X, Y]$ with

$$O_{S,F} \cong O$$

lie in at most

$2^{5n^2\lvert S\rvert}$	*$GL(2, O_S)$-equivalence classes if n is odd,*
$h_2(S) \cdot 2^{5n^2\lvert S\rvert}$	*$GL(2, O_S)$-equivalence classes if n is even,*

where $h_2(S)$ denotes the number of ideal classes of O_S of order ≤ 2.

For every even $n \geq 4$ there are O_S-orders O of rank n such that the number of $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ with $O_{S,F} \cong O$ is at least $h_2(S)/n!$.

Generalizations to other integral domains

Many Diophantine results valid over rings of S-integers of number fields have been generalized to integral domains of characteristic 0 that are finitely generated as a $\mathbb{Z}$-algebra.

Does it hold that for every such domain A, and every $\delta \in A \setminus \{0\}$, resp. nilpotent-free A-order O of rank n, the solutions of

$$D(F) \in \delta A^*, \quad A_F \cong O \quad \text{in binary forms } F \in A[X, Y] \text{ of degree } n$$

lie in only finitely many $GL(2, A)$-equivalence classes?

Generalizations to other integral domains

Many Diophantine results valid over rings of S-integers of number fields have been generalized to integral domains of characteristic 0 that are finitely generated as a $\mathbb{Z}$-algebra.

Does it hold that for every such domain A, and every $\delta \in A \setminus \{0\}$, resp. nilpotent-free A-order O of rank n, the solutions of

$$D(F) \in \delta A^*, \quad A_F \cong O \ \text{ in binary forms } F \in A[X, Y] \text{ of degree } n$$

lie in only finitely many $GL(2, A)$-equivalence classes?

NO for $D(F) \in \delta A^*$; **YES** for $A_F \cong O$ (if A is integrally closed).

$D(F) \in \delta A^*$

Assume that A has non-zero elements a such that A/aA is infinite (e.g., $A = \mathbb{Z}[t]$, $a = t$).

Fix such a and choose a binary form $F_0 \in A[X, Y]$ with $D(F_0) \neq 0$.

Then the binary forms $F_b(X, Y) := F(aX, bX + Y)$ $(b \in A)$ satisfy

$$D(F_b) = \delta := a^{n(n-1)} D(F_0)$$

and lie in infinitely many $GL(2, A)$-equivalence classes.

$A_F \cong O$

Theorem 3 (E.)

Let A be an integral domain of characteristic 0. Assume that A is finitely generated as a $\mathbb{Z}$-algebra and that A is integrally closed.

Further, let O be a nilpotent-free A-order of rank $n \geq 4$.

Then the binary forms $F \in A[X, Y]$ with $A_F \cong O$ lie in at most

$$\exp\left(c(A)n^5\right)$$

$GL(2, A)$-equivalence classes, where $c(A)$ depends on A only.

The main tool

The main tool in the proof of Theorem 3 is:

Theorem (Beukers and Schlickewei, 1996)

Let $\mathbb{F}$ be a field of characteristic 0, and let Γ be a subgroup of $\mathbb{F}^*$ of finite rank r. Then the equation

$$x + y = 1$$

has at most $2^{16(r+1)}$ solutions in $x, y \in \Gamma$.

An outline of the proof of Theorem 3

Let K be the quotient field of A. Take a binary form $F \in A[X, Y]$ with $A_F \cong O$. Write $F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ over the splitting field of F and put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \quad (1 \leq p, q \leq n)$.

An outline of the proof of Theorem 3

Let K be the quotient field of A. Take a binary form $F \in A[X, Y]$ with $A_F \cong O$. Write $F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ over the splitting field of F and put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \ \ (1 \le p, q \le n)$.

- Prove that $cr_{ijkl}(F) := \Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl} \in \Gamma_{ijkl}(O)$, where $\Gamma_{ijkl}(O)$ is a multiplicative group of rank $\le c_1(A)n^4$, depending only on O.

An outline of the proof of Theorem 3

Let K be the quotient field of A. Take a binary form $F \in A[X, Y]$ with $A_F \cong O$. Write $F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ over the splitting field of F and put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \quad (1 \le p, q \le n)$.

- Prove that $cr_{ijkl}(F) := \Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl} \in \Gamma_{ijkl}(O)$, where $\Gamma_{ijkl}(O)$ is a multiplicative group of rank $\le c_1(A)n^4$, depending only on O.
- Applying the theorem of Beukers and Schlickewei to the identities
$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1$$
conclude that for each cross ratio $cr_{ijkl}(F)$ there are at most $\exp\left(c_2(A)n^4\right)$ possible values.

An outline of the proof of Theorem 3

Let K be the quotient field of A. Take a binary form $F \in A[X, Y]$ with $A_F \cong O$. Write $F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ over the splitting field of F and put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \ \ (1 \leq p, q \leq n)$.

- Prove that $cr_{ijkl}(F) := \Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl} \in \Gamma_{ijkl}(O)$, where $\Gamma_{ijkl}(O)$ is a multiplicative group of rank $\leq c_1(A)n^4$, depending only on O.
- Applying the theorem of Beukers and Schlickewei to the identities
$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1$$
conclude that for each cross ratio $cr_{ijkl}(F)$ there are at most $\exp\left(c_2(A)n^4\right)$ possible values.
- The cross ratios $cr_{123l}(F)$ $(l = 4, \ldots, n)$ fix the $GL(2, K)$-equivalence class of F.
Deduce that the binary forms $F \in A[X, Y]$ with $A_F \cong O$ lie in at most $\exp\left(c_2(A)n^5\right)$ $GL(2, K)$-equivalence classes.

An outline of the proof of Theorem 3

Let K be the quotient field of A. Take a binary form $F \in A[X, Y]$ with $A_F \cong O$. Write $F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ over the splitting field of F and put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p \ \ (1 \le p, q \le n)$.

- Prove that $cr_{ijkl}(F) := \Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl} \in \Gamma_{ijkl}(O)$, where $\Gamma_{ijkl}(O)$ is a multiplicative group of rank $\le c_1(A)n^4$, depending only on O.
- Applying the theorem of Beukers and Schlickewei to the identities
$$\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1$$
conclude that for each cross ratio $cr_{ijkl}(F)$ there are at most $\exp\left(c_2(A)n^4\right)$ possible values.
- The cross ratios $cr_{123l}(F)$ $(l = 4, \ldots, n)$ fix the $GL(2, K)$-equivalence class of F.
Deduce that the binary forms $F \in A[X, Y]$ with $A_F \cong O$ lie in at most $\exp\left(c_2(A)n^5\right)$ $GL(2, K)$-equivalence classes.
- Prove that each of these $GL(2, K)$-equivalence classes is the union of at most $c_3(A)$ $GL(2, A)$-equivalence classes. $\square$

Thank you for your attention!