Binary forms with given invariant order

Jan-Hendrik Evertse
Universiteit Leiden

Leuca2016

Celebrating Michel Waldschmidt's 70th birthday

Marina di San Gregorio, Patú, June 16, 2016

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

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

Properties:

(i) $D(F) \in \mathbb{Z}[a_0, \ldots, a_n]$;

(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 $G = \varepsilon F_U$.

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

Thus, the solutions of the "discriminant equation"

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

can be divided into $GL(2, A)$-equivalence classes.

Finiteness results 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 $n \geq 2$ and $\delta \in O_S \setminus \{0\}$. Then there are only finitely many $GL(2, O_S)$-equivalence classes of binary forms $F \in O_S[X, Y]$ with

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

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

E. and Győry (1991) gave an effective proof (based on Baker type lower bounds for logarithmic forms and on geometry of numbers).

The number of equivalence classes

The splitting field of a binary form $F \in K[X, Y]$ over a field K is the smallest extension of K over which F factors into linear forms.

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

$$C^{\mathrm{eff}}(n, K, \#S, \epsilon) \cdot (\#O_S/\delta O_S)^{(1/n(n-1))+\epsilon} \quad \text{for all } \epsilon > 0,$$

where C^{eff} is effectively computable in terms of $n, K, \#S, \epsilon$.

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 $GL(2, O_S)$-eq. classes of binary forms $F \in O_S[X, Y]$ with

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

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

The result is almost optimal in terms of δ:

For every K, S and $n \geq 2$ there are L and $\delta \in O_S \setminus \{0\}$ with $\#O_S/\delta O_S$ arbitrarily large, such that (1) is satisfied by $\gg (\#O_S/\delta O_S)^{1/n(n-1)}$ $GL(2, O_S)$-eq. classes of binary forms $F \in O_S[X, Y]$.

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 $GL(2, O_S)$-eq. classes of binary forms $F \in O_S[X, Y]$ with

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

is at most $C^{\text{eff}}(n, K, \#S, \epsilon) \cdot (\#O_S/\delta O_S)^{(1/n(n-1))+\epsilon}$ 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?*

For this, we need a very good upper bound for the number of L for which (1) is solvable.

The invariant order of a binary form

Let A be a non-zero commutative ring. An *A-order of rank n* is a commutative ring O whose additive structure is a free A-module of rank n, i.e., O has a basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ such that every element of O can be written uniquely as $x_0 + x_1\omega_1 + \cdots + x_{n-1}\omega_{n-1}$ with $x_i \in A$ and such that $\omega_i\omega_j$ is an A-linear combination of $1, \omega_1, \ldots, \omega_{n-1}$ for all i, j.

One can attach to every binary form $F \in A[X, Y]$ of degree n an A-order of rank n, its *invariant A-order A_F*.

This was introduced and studied by Nakagawa (1989) and Simon (2001) (over $\mathbb{Z}$) and Wood (2011) (in general).

We will consider "equations"

$$A_F \cong O \quad \text{(as } A\text{-algebras)}$$

to be solved in binary forms $F \in A[X, Y]$, where O is a given A-order.

Definition of the invariant order A_F

Let for the moment A be an integral domain with quotient field K, and $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X,Y]$ a binary form that is irreducible over K.

Let θ be a zero of $F(X,1)$. Define $A_F \subset K(\theta)$ to 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 $1 \le i, j \le n-1$,

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

Thus A_F is an A-order, the *invariant A-order* of F.

Now for arbitrary non-zero commutative rings A and binary forms $F = \sum_{i=0}^{n} a_iX^{n-i}Y^i \in A[X,Y]$ we define A_F to be the free A-module with basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ with multiplication table (*).

This is an A-order (commutative and associative).

Properties of the invariant order

(i) Let A be any non-zero commutative ring and $F, G \in A[X, Y]$ two $GL(2, A)$-eq. binary forms. Then $A_F \cong A_G$ (as A-algebras).

(ii) Let A be an integral domain and $F \in A[X, Y]$ a binary form. Then A_F determines $D(F)$ up to a factor from A^*, i.e., there is $\delta \in A$ depending only on A_F such that $D(F) \in \delta A^*$
(in fact, if $1, \omega_1, \ldots, \omega_{n-1}$ is the basis of A_F from the definition, then $D(F) = D_{A_F/A}(1, \omega_1, \ldots, \omega_{n-1})$).

(iii) 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;
$D(F) \neq 0 \iff A_F$ reduced (without nilpotents).

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 binary cubic forms $F \in A[X, Y]$ with $A_F \cong O$.

Delone and Faddeev (1940) proved this for $A = \mathbb{Z}$, O an integral domain; Gan, Gross and Savin (2002) and Deligne extended this.

The proof uses only elementary algebra.

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 $F \in O_S[X, Y]$.

Let O be a reduced O_S-order of rank ≥ 4.
Then every binary form $F \in O_S[X, Y]$ with $O_{S,F} \cong O$ satisfies $D(F) \in \delta O_S^*$ for some non-zero δ depending only on O.

By the result of Birch and Merriman, the binary forms $F \in O_S[X, Y]$ with $O_{S,F} \cong O$ lie in only finitely many $GL(2, O_S)$-equivalence classes.

The condition $O_{S,F} \cong O$ is much more restrictive than $D(F) \in \delta O_S^*$.
So we expect a much better upper bound for the number of eq. classes of binary forms F with $O_{S,F} \cong O$.

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 $h_2(O_S)$ the number of ideal classes of O_S of order dividing 2.

Theorem 1 (Bérczes, E. and Győry, 2004; E. and Győry, 2016)

Let O be a reduced O_S-order of rank $n \geq 4$. Then the number of $GL(2, O_S)$-eq. classes of binary forms $F \in O_S[X, Y]$ with

$$O_{S,F} \cong O \tag{2}$$

has a uniform upper bound $c(n, O_S)$ depending only on O_S and n.

For $c(n, O_S)$ we may take

$$2^{5n^2 \# S} \text{ if } n \text{ is odd}, \quad 2^{5n^2 \# S} \cdot h_2(O_S) \text{ if } n \text{ is even.}$$

BEG proved this with O an integral domain and with a larger upper bound; EG proved the general result.

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 $h_2(O_S)$ the number of ideal classes of O_S of order dividing 2.

Theorem 1 (Bérczes, E. and Győry, 2004; E. and Győry, 2016)

Let O be a reduced O_S-order of rank $n \geq 4$. Then the number of $GL(2, O_S)$-eq. classes of binary forms $F \in O_S[X, Y]$ with

$$O_{S,F} \cong O \tag{2}$$

has a uniform upper bound $c(n, O_S)$ depending only on O_S and n.

For $c(n, O_S)$ we may take

$$2^{5n^2 \# S} \text{ if } n \text{ is odd}, \quad 2^{5n^2 \# S} \cdot h_2(O_S) \text{ if } n \text{ is even}.$$

The factor $h_2(O_S)$ is necessary.

For every K, S and every even $n \geq 4$ there are O_S-orders O of rank n such that (2) is satisfied by $\gg_n h_2(O_S)$ $GL(2, O_S)$-eq. cl. of binary forms $F \in O_S[X, Y]$.

Generalizations to other integral domains

Various finiteness results for Diophantine equations to be solved in S-integers of number fields have been extended to equations with solutions taken from integral domains of characteristic 0 that are finitely generated as a $\mathbb{Z}$-algebra, i.e., domains $A = \mathbb{Z}[z_1, \dots, z_t]$ with possibly some of the z_i transcendental.

Question

Given such a domain A, a non-zero $\delta \in A$, and a reduced A-order O of rank n, do the binary forms $F \in A[X, Y]$ of degree n with

$$D(F) \in \delta A^*, \quad \text{resp.} \quad A_F \cong O$$

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

Generalizations to other integral domains

Various finiteness results for Diophantine equations to be solved in S-integers of number fields have been extended to equations with solutions taken from integral domains of characteristic 0 that are finitely generated as a $\mathbb{Z}$-algebra, i.e., domains $A = \mathbb{Z}[z_1, \ldots, z_t]$ with possibly some of the z_i transcendental.

Question

Given such a domain A, a non-zero $\delta \in A$, and a reduced A-order O of rank n, do the binary forms $F \in A[X, Y]$ of degree n with

$$D(F) \in \delta A^*, \quad \text{resp.} \quad A_F \cong O$$

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

NO IN GENERAL 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 b such that A/bA is infinite (e.g., $A = \mathbb{Z}[z]$ with z transcendental and $b = z$).

Take such b and choose a binary form $F^* \in A[X, Y]$ of degree n with $D(F^*) \neq 0$.

Then the binary forms $F_m(X, Y) := F^*(bX, mX + Y)$ $(m \in A)$ have degree n and discriminant

$$D(F_m) = b^{n(n-1)} D(F^*) =: \delta$$

and do not lie in finitely many $GL(2, A)$-equivalence classes.

Theorem 2 (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 reduced 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 2 is:

Theorem (Beukers and Schlickewei, 1996)

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

$$x + y = 1$$

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

A brief outline of the proof of Theorem 2

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 over K and put $\Delta_{pq} := \alpha_p\beta_q - \alpha_q\beta_p$. Then

$$(*) \qquad \frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}} + \frac{\Delta_{jk}\Delta_{il}}{\Delta_{ik}\Delta_{jl}} = 1, \ (i, j, k, l \text{ distinct}).$$

- Show that $\lambda_{ijkl}(F) := \Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl}$ belongs to a multiplicative group $\Gamma(O)$ depending only on O of rank $\leq c_1(A)n^4$.
- Apply the theorem of BS to (*) and deduce an upper bound $\exp(c_2(A)n^4)$ for the number of possible values for $\lambda_{ijkl}(F)$, $\forall\, i, j, k, l$.
- Deduce from this an upper bound $\exp(c(A)n^5)$ for the number of $GL(2, A)$-eq. classes of binary forms $F \in A[X, Y]$ with $A_F \cong O$ (requires some work).

Thanks for your attention.