On cubic surfaces violating the Hasse principle

Jörg Jahnel

University of Siegen

Hannover, August 30, 2018

joint work with
Andreas-Stephan Elsenhans (Würzburg)

The geometry of smooth cubic surfaces

Let $C \subset \mathbf{P}^3$ be a smooth cubic surface over an algebraically closed field.

I.e., $C := V_f$ for $f \in k[x_0, x_1, x_2, x_3]$, $f \not\equiv 0$, a homogeneous cubic form.

This has 20 coefficients, so the Hilbert scheme of all cubic surfaces forms a $\mathbf{P}^{19}$. The smooth ones correspond to a Zariski open subset.

Fact

Smooth cubic surfaces are anticanonically embedded.

Remark

In particular, they are Fano. I.e. Del Pezzo surfaces.

The geometry of smooth cubic surfaces

Let $C \subset \mathbf{P}^3$ be a smooth cubic surface over an algebraically closed field.

I.e., $C := V_f$ for $f \in k[x_0, x_1, x_2, x_3]$, $f \not\equiv 0$, a homogeneous cubic form.

This has 20 coefficients, so the Hilbert scheme of all cubic surfaces forms a $\mathbf{P}^{19}$. The smooth ones correspond to a Zariski open subset.

Fact

Smooth cubic surfaces are anticanonically embedded.

Remark

In particular, they are Fano. I.e. Del Pezzo surfaces.

Proof of the fact: The adjunction formula shows that

$$K_C = K_{\mathbf{P}^3}(3)|_C = \mathscr{O}_{\mathbf{P}^3}(-4+3)|_C = \mathscr{O}_{\mathbf{P}^3}(-1)|_C . \qquad \square$$

The geometry of smooth cubic surfaces II

Classical algebraic geometry gives a lot of information about smooth cubic surfaces. For instance,

- Smooth cubic surfaces are obtained as the blow-ups of $\mathbf{P}^2$ in six points in general position.
- In particular, they are rational.

The geometry of smooth cubic surfaces II

Classical algebraic geometry gives a lot of information about smooth cubic surfaces. For instance,

- Smooth cubic surfaces are obtained as the blow-ups of $\mathbf{P}^2$ in six points in general position.
- In particular, they are rational.

- A smooth cubic surface C contains precisely 27 lines.

  The configuration of the 27 lines is highly symmetric. The group of all permutations respecting the intersection pairing is isomorphic to the Weyl group $W(E_6)$ of order 51 840.

The geometry of smooth cubic surfaces III

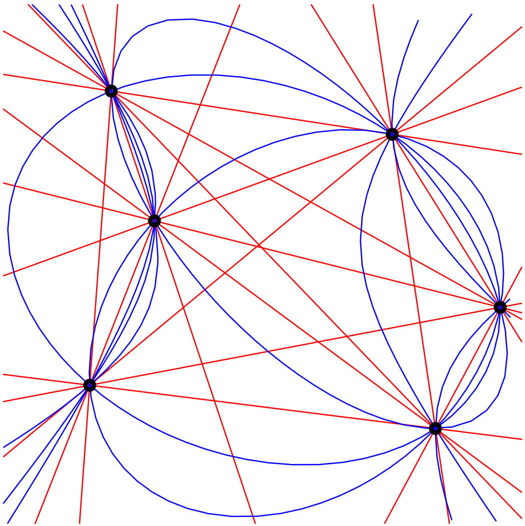

Figure: The 27 lines in the blown-up model

Rationality

Remark

In this talk, we will typically consider cubic surfaces C that are defined over an *algebraically non-closed* field. E.g. over $\mathbb{Q}$.

Then there is no reason to expect that C be rational over $\mathbb{Q}$.

Rationality

Remark

In this talk, we will typically consider cubic surfaces C that are defined over an *algebraically non-closed* field. E.g. over $\mathbb{Q}$.

Then there is no reason to expect that C be rational over $\mathbb{Q}$.

Rationality over $\mathbb{Q}$ implies that $C(\mathbb{Q}) \neq \emptyset$.

Example

The diagonal cubic surface $C := V_f$ for $f := x_0^3 + 7x_1^3 + 2x_2^3 + 14x_3^3$ has no $\mathbb{Q}$-rational point.

In fact, C has no $\mathbb{Q}_7$-rational point.

Rationality

Remark

In this talk, we will typically consider cubic surfaces C that are defined over an *algebraically non-closed* field. E.g. over $\mathbb{Q}$.

Then there is no reason to expect that C be rational over $\mathbb{Q}$.

Rationality over $\mathbb{Q}$ implies that $C(\mathbb{Q}) \neq \emptyset$.

Example

The diagonal cubic surface $C := V_f$ for $f := x_0^3 + 7x_1^3 + 2x_2^3 + 14x_3^3$ has no $\mathbb{Q}$-rational point.

In fact, C has no $\mathbb{Q}_7$-rational point.

Remark

Note that a smooth cubic surface always has real points. Indeed, 27 is an odd integer, so that complex conjugation must fix one of the lines.

It is known that every smooth cubic surface over $\mathbb{R}$ contains at least 3 real lines.

Rationality II

The assumption that $C(\mathbb{Q}) \neq \emptyset$ implies that C is $\mathbb{Q}$-unirational (J. Kollar, 2002), but is by far insufficient for C being rational over $\mathbb{Q}$.

Fact

Assume that a smooth cubic surface C over $\mathbb{Q}$ is rational over $\mathbb{Q}$. Then, on C, there is a Galois invariant set of five or six mutually skew lines.

However, generically, the 27 lines are acted upon by a Galois group isomorphic to $W(E_6)$, which acts transitively on the 27 lines. [The cubic surfaces, for which the Galois group is smaller, form a thin subset of $\mathbf{P}^{19}(\mathbb{Q})$.]

Thus only **very special** smooth cubic surfaces over $\mathbb{Q}$ are rational over $\mathbb{Q}$.

Rationality II

The assumption that $C(\mathbb{Q}) \neq \emptyset$ implies that C is $\mathbb{Q}$-unirational (J. Kollar, 2002), but is by far insufficient for C being rational over $\mathbb{Q}$.

Fact

Assume that a smooth cubic surface C over $\mathbb{Q}$ is rational over $\mathbb{Q}$. Then, on C, there is a Galois invariant set of five or six mutually skew lines.

However, generically, the 27 lines are acted upon by a Galois group isomorphic to $W(E_6)$, which acts transitively on the 27 lines. [The cubic surfaces, for which the Galois group is smaller, form a thin subset of $\mathbf{P}^{19}(\mathbb{Q})$.]

Thus only **very special** smooth cubic surfaces over $\mathbb{Q}$ are rational over $\mathbb{Q}$.

As there is [usually] no rational parametrisation for $C(\mathbb{Q})$, questions on the *arithmetic* of smooth cubic surfaces may well be delicate.

For example, Manin's conjecture making predictions on the growth of

$$\#\{x \in C(\mathbb{Q}) \mid H_{\text{naive}}(x) < B\}$$

is completely open.

Rationality III

Example

Let $C := V_f$, for

$$f := x_0^3 + 7x_1^3 + 2x_2^3 + 14x_3^3 + 3x_0x_1^2 + 5x_0x_2^2 + x_1x_2x_3 \,.$$

Then C is a smooth cubic surface. The Galois group acting on the 27 lines is the full $W(E_6)$. In particular, C is not rational over $\mathbb{Q}$.

Moreover, $C(\mathbb{Q}) \neq \emptyset$. For instance, $(-1:1:1:0) \in C(\mathbb{Q})$.

The first explicit example of a smooth cubic surface with the full $W(E_6)$ acting on the 27 lines is due to T. Ekedahl (1988).

Today, to compute the 27 lines is just a calculation in Gröbner bases.

Eckardt points

The geometry of the 27 lines on a smooth cubic surface is very rigid.

There are 45 tritangent planes. The intersection matrix is the same for all smooth cubic surfaces.

But there are two ways a tritangent plane may look like.

Eckardt points

The geometry of the 27 lines on a smooth cubic surface is very rigid.

There are 45 tritangent planes. The intersection matrix is the same for all smooth cubic surfaces.

But there are two ways a tritangent plane may look like.

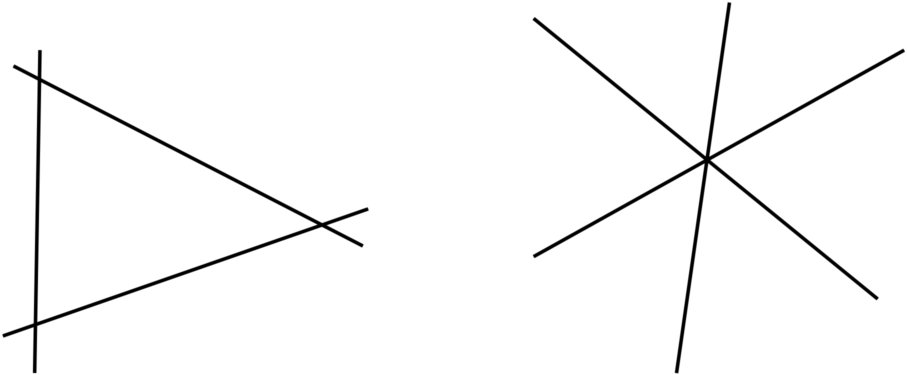

Figure: An ordinary tritangent plane (left) and one with an Eckardt point (right)

Eckardt points II

Facts (well-known in the 19th century)

- *A smooth cubic surface over an algebraically closed field of characteristic* 0 *may have no, 1, 2, 3, 4, 6, 9, 10, or 18 Eckardt points.*
    - *A generic cubic surface has no Eckardt point.*
    - *To have an Eckardt point is a codimension one condition in moduli space.*
    - *To have at least two Eckardt points is a codimension two condition in moduli space.*
- *The existence of an Eckardt point is equivalent to the cubic surface having a non-trivial automorphism.*

The Hasse principle

The Hasse principle (named after H. Hasse)

Let V be a variety, defined over $\mathbb{Q}$. If $V(\mathbb{Q}_p) \neq \emptyset$ and $V(\mathbb{R}) \neq \emptyset$, then $V(\mathbb{Q}) \neq \emptyset$.

The Hasse principle

The Hasse principle (named after H. Hasse)

Let V be a variety, defined over $\mathbb{Q}$. If $V(\mathbb{Q}_p) \neq \emptyset$ and $V(\mathbb{R}) \neq \emptyset$, then $V(\mathbb{Q}) \neq \emptyset$.

It may happen that the Hasse principle is violated. I.e., that $V(\mathbb{Q}_p) \neq \emptyset$ and $V(\mathbb{R}) \neq \emptyset$, but nevertheless $V(\mathbb{Q}) = \emptyset$.

- For varieties of general type, $V(\mathbb{Q}) = \emptyset$ is what one presumes [in view of Lang's conjecture]. Thus, one does not expect the Hasse principle to hold.
- Concerning varieties of intermediate type, genus-1-curves that are counterexamples to the Hasse principle have been constructed by

$$\text{C.-E. Lind (1940): } 2w^2 = x_0^4 - 17x_1^4,$$
$$\text{E. S. Selmer (1951): } 3x_0^3 + 4x_1^3 + 5x_2^3 = 0.$$

- But given a Fano variety (e.g. a smooth cubic surface), one might naively tend to expect the Hasse principle to be true.

The Hasse principle II

Theorem (Hasse-Minkowski, 192?)

Suppose f to be homogeneous of degree two. Then the Hasse principle holds for V_f.

The Hasse principle II

Theorem (Hasse-Minkowski, 192?)

Suppose f to be homogeneous of degree two. Then the Hasse principle holds for V_f.

Theorem (Birch, 1957)

Let $d \geq 3$ be an odd integer. Then there exists a constant $N(d)$ such that $V_f(\mathbb{Q}) \neq \emptyset$ for every homogeneous form of degree d in at least $N(d)$ variables. The Hasse principle holds trivially.

Proof: Circle method. $\square$

Singular cubic surfaces

Let now f be a homogeneous cubic in four variables. Then $C := V_f \subset \mathbf{P}^3$ is a cubic surface.

Theorem (T. A. Skolem, 1955)

Let $C \subset \mathbf{P}^3$ be a singular *cubic surface. Then the Hasse principle holds for C.*

Singular cubic surfaces

Let now f be a homogeneous cubic in four variables. Then $C := V_f \subset \mathbf{P}^3$ is a cubic surface.

Theorem (T. A. Skolem, 1955)

Let $C \subset \mathbf{P}^3$ be a singular *cubic surface. Then the Hasse principle holds for C.*

Idea of proof: 19th century algebraic geometry provides a classification of singular cubic surfaces.

- C geometrically reducible or non-reduced: Contains a $\mathbb{Q}$-rational plane or the intersection of three conjugate planes having a point or line in common.
- Otherwise, but singular locus of dimension 1: Then the singular locus is exactly one line, which must be rational.
- Singular locus of dimension 0: 22 types,
  Triple point, $A_1, A_2, 2A_1, A_3, A_2 + A_1, A_4, \ldots, E_6, \ldots, 3A_1, 3A_2, 4A1$.
  In all types, except for $3A_1$, $3A_2$, and $4A1$, $\mathbb{Q}$-rational points obviously exist.

Singular cubic surfaces II

These three types are handled by Galois descent.

For example $3A_2$: There is the **geometric** normal form

$$x_0^3 = x_1x_2x_3$$

for this type, the singularities are $(0:1:0:0)$, $(0:0:1:0)$, and $(0:0:0:1)$.

Over $\mathbb{Q}$, one may hence write

$$cx_0^3 = l^{\sigma_1} l^{\sigma_2} l^{\sigma_3} \, ,$$

where l is a linear form, defined over a cubic extension L of $\mathbb{Q}$, and $\sigma^i \colon L \to \mathbb{C}$ are the three embeddings. Here, the l^{σ^i} have to be $\mathbb{C}$-linearly independent, implying that $l \colon \mathbb{Q}^4 \to L$ must be surjective.

Thus, the norm equation $N(x) = c$ is to be solved in L.

If $L/\mathbb{Q}$ is Galois then the Hasse norm theorem implies the Hasse principle. If L defines an S_3-extension then existence of points everywhere locally yields a point p over the quadratic intermediate field Q.

Connect p and $\overline{p}$ by a line. The third point of intersection is defined over $\mathbb{Q}$.

Singular cubic surfaces III

The case $3A_1$ works in a similar manner.

The case $4A_1$ leads to a trace equation. There are always $\mathbb{Q}$-rational points.

□

Singular cubic surfaces III

The case $3A_1$ works in a similar manner.

The case $4A_1$ leads to a trace equation. There are always $\mathbb{Q}$-rational points. $\square$

Singular cubic surfaces are not the generic case.

Classical counterexamples

Theorem (Swinnerton-Dyer, 1962)

Let $K/\mathbb{Q}$ be the unique cubic field extension contained in the cyclotomic extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. Put $\theta := \mathrm{Tr}_{\mathbb{Q}(\zeta_7)/K}(\zeta_7 - 1)$ and let C be the cubic surface, given by

$$\begin{aligned} x_3(x_0+x_3)(x_0+2x_3) &= \mathrm{N}_{K/\mathbb{Q}}\big(x_0+\theta x_1+\theta^2 x_2\big) \\ &= x_0^3 - 7x_0^2x_1 + 21x_0^2x_2 + 14x_0x_1^2 - 77x_0x_1x_2 \\ &\qquad + 98x_0x_2^2 - 7x_1^3 + 49x_1^2x_2 - 98x_1x_2^2 + 49x_2^3 \,. \end{aligned}$$

Then C violates the Hasse principle.

Classical counterexamples

Theorem (Swinnerton-Dyer, 1962)

Let $K/\mathbb{Q}$ be the unique cubic field extension contained in the cyclotomic extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. Put $\theta := \mathrm{Tr}_{\mathbb{Q}(\zeta_7)/K}(\zeta_7 - 1)$ and let C be the cubic surface, given by

$$\begin{aligned} x_3(x_0+x_3)(x_0+2x_3) &= \mathrm{N}_{K/\mathbb{Q}}\big(x_0+\theta x_1+\theta^2 x_2\big) \\ &= x_0^3 - 7x_0^2x_1 + 21x_0^2x_2 + 14x_0x_1^2 - 77x_0x_1x_2 \\ &\qquad + 98x_0x_2^2 - 7x_1^3 + 49x_1^2x_2 - 98x_1x_2^2 + 49x_2^3\,. \end{aligned}$$

Then C violates the Hasse principle.

Remark

Swinnerton-Dyer's example was soon generalised by L. J. Mordell. He gave two families of counterexamples, one using norm forms from the cubic subfield of $\mathbb{Q}(\zeta_7)$, the other from the cubic subfield of $\mathbb{Q}(\zeta_{13})$.

The three linear forms on the left hand side are always linearly dependent.

Classical counterexamples II

Theorem (Cassels/Guy, 1966)

Let C be the cubic surface given by

$$5x_0^3 + 12x_1^3 + 9x_2^3 + 10x_3^3 = 0\,.$$

Then C violates the Hasse principle.

Classical counterexamples II

Theorem (Cassels/Guy, 1966)

Let C be the cubic surface given by

$$5x_0^3 + 12x_1^3 + 9x_2^3 + 10x_3^3 = 0\,.$$

Then C violates the Hasse principle.

Remark

This is the historically first example of a diagonal cubic surface violating the Hasse principle.

The arithmetic of diagonal cubic surfaces was systematically investigated by J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc in 1985. More counterexamples to the Hasse principle were found, but also evidence that a general diagonal cubic surface fulfils the Hasse principle (but not weak approximation).

A further generalisation of Mordell's counterexamples

Theorem (J., 2007)

Let $p \equiv 1 \pmod 3$ be any prime, K the cubic subfield of $\mathbb{Q}(\zeta_p)$, and $\theta := \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p - 1)$. For a_1, a_2, d_1, d_2 integers, consider the cubic surface $X \subset \mathbf{P}^3_{\mathbb{Q}}$, given by

$$x_3(a_1x_0 + d_1x_3)(a_2x_0 + d_2x_3) = \mathrm{N}_{K/\mathbb{Q}}\left(x_0 + \theta x_1 + \theta^2 x_2\right).$$

1. *Assume $p \nmid d_1d_2$, that $\gcd(a_1, d_1)$ and $\gcd(a_2, d_2)$ contain only prime factors decomposing in K, and that among the roots z_1, z_2, z_3 of $T(a_1 + d_1T)(a_2 + d_2T) - 1 \in \mathbb{F}_p[T]$, at least one is simple and in $\mathbb{F}_p$. Then, $X(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$.*
2. *Suppose $p \nmid d_1d_2$ and $\gcd(d_1, d_2) = 1$. Then, for every point $(t_0 : t_1 : t_2 : t_3) \in X(\mathbb{Q})$, $s := (t_3/t_0 \mod p)$ admits the property that $\frac{a_1+d_1s}{s}$ is a cube in $\mathbb{F}_p^*$.*
   In particular, if $\frac{a_1+d_1z_i}{z_i} \in \mathbb{F}_p^*$ is a non-cube whenever $z_i \in \mathbb{F}_p$, $i \in \{1, 2, 3\}$, then $X(\mathbb{Q}) = \emptyset$.

The method of the proof

Note that this generalises Mordell's counterexamples further to the cubic subfield of $\mathbb{Q}(\zeta_p)$, for any prime number $p \equiv 1 \pmod 3$.

Existence of adelic points is just an application of Hensel's lemma.

For the second assertion, there is an elementary proof, applying class field theory to the values of the rational function

$$\frac{a_1x_0 + d_1x_3}{x_3}\,.$$

The method of the proof

Note that this generalises Mordell's counterexamples further to the cubic subfield of $\mathbb{Q}(\zeta_p)$, for any prime number $p \equiv 1 \pmod 3$.

Existence of adelic points is just an application of Hensel's lemma.

For the second assertion, there is an elementary proof, applying class field theory to the values of the rational function

$$\frac{a_1x_0 + d_1x_3}{x_3}\,.$$

This function has been very carefully selected.

- $\frac{a_1x_0+d_1x_3}{x_3}$ is not the norm of a function, but "almost".
- $\mathrm{div}(\frac{a_1x_0+d_1x_3}{x_3})$ is the norm of the divisor [a difference of two lines]

$$V(a_1x_0 + d_1x_3, x_0 + \theta x_1 + \theta^2 x_2) - V(x_3, x_0 + \theta x_1 + \theta^2 x_2)\,.$$

The method of the proof II

- Write the equation of C as $l_1 l_2 l_3 = \mathrm{N}_{L/\mathbb{Q}}(l)$ for linear forms l, l_1, l_2, l_3, and $L/\mathbb{Q}$ a cubic Galois extension. (Work over an extension of $\mathbb{Q}$ for C a diagonal surface).
- Ensure that no $\mathbb{Q}$-rational point is contained in the three planes $l_i = 0$. ($l_i = 0$ implies $l^{\sigma_1} = l^{\sigma_2} = l^{\sigma_3} = 0$. I.e., check that the four linear forms are linearly independent.)
- Prove that, for every prime $q \neq p$, independently of the choice of $x \in C(\mathbb{Q}_q)$, the expression $\frac{l_1(x)}{l_2(x)} \in \mathbb{Q}_q^*$ is always a norm from $K_{\mathfrak{q}}$.
  I.e., that for the norm residue symbol, one has
  $$s_q := (\tfrac{l_1(x)}{l_2(x)}, K_{\mathfrak{q}}/\mathbb{Q}_q) = 0 \in \tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\,.$$
- Recall the Hilbert reciprocity law from global class field theory
  $$\sum_q s_q \neq 0 \in \tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\,,$$
  which implies that $\frac{l_1(x)}{l_2(x)} \in \mathbb{Q}_p^*$ must be a norm from $K_{\mathfrak{p}}$.

Manin's interpretation – The Brauer-Manin obstruction

Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. Then the cyclic $K(C)$-algebra

$$\mathscr{A} = (L(C), \sigma, \tfrac{l_1}{l_2}) := L1 \oplus Lu \oplus Lu^2,$$

for u a formal symbol and the relations $u^3 = \frac{l_1}{l_2}$ as well as $ux = \sigma(x)u$ for all $x \in L(C)$, is an Azumaya algebra over $K(C)$.

Manin's interpretation – The Brauer-Manin obstruction

Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. Then the cyclic $K(C)$-algebra

$$\mathscr{A} = (L(C), \sigma, \tfrac{l_1}{l_2}) := L1 \oplus Lu \oplus Lu^2,$$

for u a formal symbol and the relations $u^3 = \frac{l_1}{l_2}$ as well as $ux = \sigma(x)u$ for all $x \in L(C)$, is an Azumaya algebra over $K(C)$.

Observation

The Azumaya algebra $\mathscr{A}$ extends to an Azumaya algebra over the whole scheme C. It defines a class $\alpha \in \mathrm{Br}(C)$

The reason is that $\mathrm{div}(\frac{l_1}{l_2})$ is the norm of the (non-principal) divisor [difference of two lines]

$$V(l_1, l) - V(l_2, l)\,.$$

Thus, $(L(C), \sigma, \frac{l_1}{l_2})$ and $(L(C), \sigma, \frac{l_1}{l_2} \cdot \mathrm{N}_{L(C)/K(C)}(\varphi))$ are isomorphic algebras.

The argument described above is an instance of the Brauer–Manin obstruction. [It is conjectured that, for cubic surfaces, all violations of the Hasse principle are explained by the Brauer–Manin obstruction.]

Eckardt points III

Fact

1. *The Swinnerton-Dyer-Mordell type surfaces are contained in a two-dimensional closed subscheme of the moduli space.*
2. *Diagonal cubic surfaces correspond to a single moduli point.*

Eckardt points III

Fact

1. *The Swinnerton-Dyer-Mordell type surfaces are contained in a two-dimensional closed subscheme of the moduli space.*
2. *Diagonal cubic surfaces correspond to a single moduli point.*

Idea of proof for 1. They have three Eckardt points.

The equations are of the form

$$x_3(a_1x_0 + d_1x_3)(a_2x_0 + d_2x_3) = \mathrm{N}_{K/\mathbb{Q}}(x_0 + \theta x_1 + \theta^2 x_2)\,.$$

The three tritangent planes $V(x_3)$, $V(a_1x_0 + d_1x_3)$, and $V(a_2x_0 + d_2x_3)$ have a line in common. Thus, on each of the three tritangent planes $V(x_0 + \theta^{\sigma_i} x_1 + (\theta^{\sigma_i})^2 x_2)$, the corresponding three lines meet at a single point. □

Eckardt points III

Fact

1. *The Swinnerton-Dyer-Mordell type surfaces are contained in a two-dimensional closed subscheme of the moduli space.*
2. *Diagonal cubic surfaces correspond to a single moduli point.*

Idea of proof for 1. They have three Eckardt points.

The equations are of the form

$$x_3(a_1x_0 + d_1x_3)(a_2x_0 + d_2x_3) = \mathrm{N}_{K/\mathbb{Q}}(x_0 + \theta x_1 + \theta^2 x_2)\,.$$

The three tritangent planes $V(x_3)$, $V(a_1x_0 + d_1x_3)$, and $V(a_2x_0 + d_2x_3)$ have a line in common. Thus, on each of the three tritangent planes $V(x_0 + \theta^{\sigma_i}x_1 + (\theta^{\sigma_i})^2x_2)$, the corresponding three lines meet at a single point. $\square$

Remark

Diagonal cubic surfaces have 18 Eckardt points.

Our family

The family

We consider the cubic surface C over $\mathbb{Q}$, given by the equation

$$x_0x_1x_2 = \mathrm{N}_{K/\mathbb{Q}}(ax_0 + bx_1 + cx_2 + dx_3)\,, \tag{1}$$

for $K/\mathbb{Q}$ a cyclic cubic field extension and $a, b, c, d \in K$.

Our family

The family

We consider the cubic surface C over $\mathbb{Q}$, given by the equation

$$x_0 x_1 x_2 = \mathrm{N}_{K/\mathbb{Q}}(a x_0 + b x_1 + c x_2 + d x_3)\,, \tag{1}$$

for $K/\mathbb{Q}$ a cyclic cubic field extension and $a, b, c, d \in K$.

There is only one change in comparison with the Swinnerton-Dyer-Mordell type surfaces. The three linear forms on the left hand side are now linearly independent.

Inert primes

Proposition (Inert primes)

Let l be a prime that is inert in $K/\mathbb{Q}$. Denote by w the unique prime of K lying above l and assume that

- $a, b, c \in \mathscr{O}_{K_w}$, $d \in \mathscr{O}^*_{K_w}$,
- $(a/d \bmod l), (b/d \bmod l), (c/d \bmod l) \in \mathbb{F}_{l^3}$ *are not contained in* $\mathbb{F}_l$.

Finally, let C denote the surface (1).

For any $(t_0 : t_1 : t_2 : t_3) \in C(\mathbb{Q}_l)$ such that $t_0 t_1 \neq 0$, the quotient $t_1/t_0 \in \mathbb{Q}_l$ is in the image of the norm map $N\colon K_w \to \mathbb{Q}_l$.

Inert primes

Proposition (Inert primes)

Let l be a prime that is inert in $K/\mathbb{Q}$. Denote by w the unique prime of K lying above l and assume that

- $a, b, c \in \mathscr{O}_{K_w}$, $d \in \mathscr{O}_{K_w}^*$,
- $(a/d \bmod l), (b/d \bmod l), (c/d \bmod l) \in \mathbb{F}_{l^3}$ *are not contained in* $\mathbb{F}_l$.

Finally, let C denote the surface (1).

For any $(t_0 : t_1 : t_2 : t_3) \in C(\mathbb{Q}_l)$ such that $t_0 t_1 \neq 0$, the quotient $t_1/t_0 \in \mathbb{Q}_l$ is in the image of the norm map $N \colon K_w \to \mathbb{Q}_l$.

Proof. Normalise such that $t_0, \ldots, t_3 \in \mathbb{Z}_l$ and one of them is a unit.

t_1/t_0 not being a norm means $3 \nmid \nu_l(t_1/t_0)$. Then t_0, t_1, and t_2 have distinct valuations. In particular, at most one of them is a unit.

The assumptions now imply that the right hand side of (1) is a unit, while the left hand side is not. □

Ramification

Lemma

Let $l \neq 3$ be a prime number and consider the nodal cubic curve E over $\mathbb{F}_l$, defined by

$$27x_0x_1x_2 = (x_0 + x_1 + x_2)^3 .$$

Then, for every $\mathbb{F}_l$-rational point $(t_0 : t_1 : t_2)$ on E, at least one of the expressions t_1/t_0, t_2/t_1, and t_0/t_2 is properly defined and non-zero in $\mathbb{F}_l$. Further, these quotients evaluate solely to cubes in $\mathbb{F}_l^*$.

Ramification

Lemma

Let $l \neq 3$ be a prime number and consider the nodal cubic curve E over $\mathbb{F}_l$, defined by

$$27x_0x_1x_2 = (x_0 + x_1 + x_2)^3 .$$

Then, for every $\mathbb{F}_l$-rational point $(t_0 : t_1 : t_2)$ on E, at least one of the expressions t_1/t_0, t_2/t_1, and t_0/t_2 is properly defined and non-zero in $\mathbb{F}_l$. Further, these quotients evaluate solely to cubes in $\mathbb{F}_l^*$.

Remark

$(1 : 1 : 1)$ is the singular point.

Idea of proof. The first assertion simply says that $(1:0:0)$, $(0:1:0)$, $(0:0:1) \notin E$. Further, in $\mathbb{Z}[T_0, T_1, T_2]$, the polynomial expression

$$(T_0^2 + 2T_0T_1 + T_1^2 + 5T_0T_2 - 4T_1T_2 - 5T_2^2)^3 + 729T_0(T_1 - T_2)^3T_2^2$$

splits into two factors, one of which is $27T_0T_1T_2 - (T_0 + T_1 + T_2)^3$.

For $(t_0 : t_1 : t_2) \in E(\mathbb{F}_l)$ with $t_2 \neq 0$, we see that t_0/t_2 is a cube, except possibly for the case when $t_1 = t_2$. But then the equation of the curve shows that $t_0/t_2 = (\frac{t_0+2t_2}{3t_2})^3$. $\square$

Ramification III

Proposition

Let $l \neq 3$ be prime that is ramified in $K/\mathbb{Q}$. Denote by $\mathfrak{p}$ the unique prime of K lying above l and assume that

- $a \in \mathscr{O}_{K_\mathfrak{p}}, (a \bmod \mathfrak{p}) = \frac{\alpha}{3}$,
- $b \in \mathscr{O}_{K_\mathfrak{p}}, (b \bmod \mathfrak{p}) = \frac{1}{3}$,
- $c \in \mathscr{O}_{K_\mathfrak{p}}, (c \bmod \mathfrak{p}) = \frac{1}{3\alpha}$,
- $d \in \mathfrak{p} \backslash \mathfrak{p}^3$.

for some non-cube $\alpha \in \mathbb{F}_l^*$. Finally, let C denote the surface (1).

Let $(t_0 : t_1 : t_2 : t_3) \in C(\mathbb{Q}_l)$ be any point. If, for $0 \leq i < j \leq 2$, one has $t_i t_j \neq 0$ then the quotient $t_j/t_i \in \mathbb{Q}_l$ is not *in the image of the norm map* $\mathrm{N} \colon K_\mathfrak{p} \to \mathbb{Q}_l$.

Ramification III

Proposition

Let $l \neq 3$ be prime that is ramified in $K/\mathbb{Q}$. Denote by $\mathfrak{p}$ the unique prime of K lying above l and assume that

- $a \in \mathscr{O}_{K_\mathfrak{p}}, (a \bmod \mathfrak{p}) = \frac{\alpha}{3}$,
- $b \in \mathscr{O}_{K_\mathfrak{p}}, (b \bmod \mathfrak{p}) = \frac{1}{3}$,
- $c \in \mathscr{O}_{K_\mathfrak{p}}, (c \bmod \mathfrak{p}) = \frac{1}{3\alpha}$,
- $d \in \mathfrak{p} \backslash \mathfrak{p}^3$.

for some non-cube $\alpha \in \mathbb{F}_l^*$. Finally, let C denote the surface (1).

Let $(t_0 : t_1 : t_2 : t_3) \in C(\mathbb{Q}_l)$ be any point. If, for $0 \leq i < j \leq 2$, one has $t_i t_j \neq 0$ then the quotient $t_j/t_i \in \mathbb{Q}_l$ is not *in the image of the norm map* $\mathrm{N} \colon K_\mathfrak{p} \to \mathbb{Q}_l$.

Idea of proof. The reduction of C is non-trivial twist of the nodal cubic curve considered in the lemma. No l-adic point reduces to the cusp $(0:0:0:1)$. $\square$

New counterexamples to the Hasse principle

Theorem (Elsenhans+J.)

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ *and* $z = \zeta_7 + \zeta_7^{-1} - 2$. *Write* $\mathfrak{p} = (z)$ *for the unique prime lying above* (7). *Suppose that* $a, b, c, d \in \mathscr{O}_K$ *satisfy the following conditions.*

1. d *splits as* $(d) = \mathfrak{p}\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$, *where* $\mathrm{N}(\mathfrak{p}_i)$ *are prime numbers* $\neq (7)$. *I.e.,* (d) *contains* $\mathfrak{p}$ *exactly once and, moreover, only split primes.*
2. $a/d = \frac{1}{7}(a_0 + a_1 z + a_2 z^2)$ *for* $a_i \in \mathbb{Z}$ *and* $\gcd(a_1, a_2)$ *is a product of only split primes.*
   - $b/d = \frac{1}{7}(b_0 + b_1 z + b_2 z^2)$ *for* $b_i \in \mathbb{Z}$ *and* $\gcd(b_1, b_2)$ *is a product of only split primes.*
   - $c/d = \frac{1}{7}(c_0 + c_1 z + c_2 z^2)$ *for* $c_i \in \mathbb{Z}$ *and* $\gcd(c_1, c_2)$ *is a product of only split primes.*
3. $a \equiv b \pmod 6$.
4. $a \equiv -1 \pmod{\mathfrak{p}}$, $b \equiv -2 \pmod{\mathfrak{p}}$, *and* $c \equiv -4 \pmod{\mathfrak{p}}$.

Finally, let C *denote the surface (1). Then* $C(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ *but* $C(\mathbb{Q}) = \emptyset$.

New counterexamples to the Hasse principle II

Idea of proof. *Step 1:* Existence of l-adic points for every l.

This is clear for split primes and $l = \infty$, as we have the form $x_0x_1x_2 = l_1l_2l_3$.

For the other primes, use Hensel's lemma. It suffices to show that C_l has a non-singular $\mathbb{F}_l$-rational point. For this, we show that $(C_l)_{\text{sing}}$ is of dimension zero. Thus, $\#(C_l)_{\text{reg}}(\mathbb{F}_l) \geq l^2 - 3l - 3 > 0$ for $l \geq 5$.

The assumption $a \equiv b \pmod 6$ ensures that $(1 : (-1) : 0 : 0) \in C_l(\mathbb{F}_l)$ is a non-singular point for $l = 2, 3$.

Step 2: Non-existence of $\mathbb{Q}$-rational points.

Use the Hilbert reciprocity law form from class field theory. Apply the Propositions above.

l inert $\Longrightarrow a/d = \frac{1}{7}(a_0 + a_1z + a_2z^2)$ for a_0, a_1 not both divisible by l. Hence, $(a/d \bmod l) \in \mathbb{F}_{l^3} \backslash \mathbb{F}_l$. $(b/d \bmod l)$, $(c/d \bmod l)$ are analogous.

The ramified prime: $b \equiv -2 \pmod{\mathfrak{p}}$ means $(b \bmod \mathfrak{p}) = \frac{1}{3}$.
The assumptions on a and c mean $\alpha = \frac{1}{2} \equiv 4 \pmod 7$. This is a non-cube.

An example

Example

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $z := \zeta_7 + \zeta_7^{-1} - 2$, and let C be the cubic surface over $\mathbb{Q}$, given by the equation $x_0 x_1 x_2 = \mathrm{N}_{K/\mathbb{Q}}(ax_0 + bx_1 + cx_2 + dx_3)$, for

$$a := -1, \quad b := 5 + 6z^2, \quad c := 3 + z^2, \quad d := z\,.$$

Then C violates the Hasse principle.

An example

Example

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $z := \zeta_7 + \zeta_7^{-1} - 2$, and let C be the cubic surface over $\mathbb{Q}$, given by the equation $x_0x_1x_2 = \mathrm{N}_{K/\mathbb{Q}}(ax_0 + bx_1 + cx_2 + dx_3)$, for

$$a := -1, \quad b := 5 + 6z^2, \quad c := 3 + z^2, \quad d := z\,.$$

Then C violates the Hasse principle.

Indeed,

1. $d = z$ for $(z) = \mathfrak{p}$, [no further factors].
2. $a/d = \frac{1}{7}(14 + 7z + z^2)$,
   $b/d = \frac{1}{7}(-70 + 7z - 5z^2)$,
   $c/d = \frac{1}{7}(-42 - 14z - 3z^2)$ [calculation using $z^3 + 7z^2 + 14z + 7 = 0$],
   $\gcd(7, 1) = \gcd(7, -5) = \gcd(-14, -3) = 1$.
3. $a \equiv b \pmod{6}$.
4. $a \equiv -1 \pmod{z}$, $b \equiv -2 \pmod{z}$, $c \equiv -4 \pmod{z}$.

An example II

The equation of C is, in explicit form,

$$x_0^3 - 141x_0^2x_1 - 30x_0^2x_2 + 7x_0^2x_3 + 4863x_0x_1^2 + 2233x_0x_1x_2 - 532x_0x_1x_3$$
$$+ 251x_0x_2^2 - 119x_0x_2x_3 + 14x_0x_3^2 - 31499x_1^3 - 26286x_1^2x_2 + 6013x_1^2x_3$$
$$- 6799x_1x_2^2 + 3157x_1x_2x_3 - 364x_1x_3^2 - 559x_2^3 + 392x_2^2x_3 - 91x_2x_3^2 + 7x_3^3 = 0\,.$$

C has bad reduction at 2, 3, 7, 3739, and 7589.

$S_{\mathbb{F}_2}$: binode;

$S_{\mathbb{F}_7}$: cone over a nodal cubic;

other three: conical

An example II

The equation of C is, in explicit form,

$$x_0^3 - 141x_0^2x_1 - 30x_0^2x_2 + 7x_0^2x_3 + 4863x_0x_1^2 + 2233x_0x_1x_2 - 532x_0x_1x_3 + 251x_0x_2^2 - 119x_0x_2x_3 + 14x_0x_3^2 - 31499x_1^3 - 26286x_1^2x_2 + 6013x_1^2x_3 - 6799x_1x_2^2 + 3157x_1x_2x_3 - 364x_1x_3^2 - 559x_2^3 + 392x_2^2x_3 - 91x_2x_3^2 + 7x_3^3 = 0\,.$$

C has bad reduction at 2, 3, 7, 3739, and 7589.

$S_{\mathbb{F}_2}$: binode;

$S_{\mathbb{F}_7}$: cone over a nodal cubic;

other three: conical

A minimisation algorithm yields a reembedding of C as the surface, given by the equation

$$-x_0^3 + 2x_0^2x_1 - x_0^2x_2 - 5x_0^2x_3 + x_0x_1^2 - x_0x_1x_2 + 7x_0x_1x_3 + 2x_0x_2^2 - 15x_0x_2x_3 - 11x_0x_3^2 - x_1^3 - 2x_1^2x_2 + 9x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^3 + x_2^2x_3 + 8x_2x_3^2 - x_3^3 = 0\,.$$

Congruence conditions

Corollary

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $l \equiv \pm 1 \pmod 7$ *be a prime number, and* $\widetilde{a}, \widetilde{b}, \widetilde{c}, \widetilde{d}$ *be four residue classes in* $[\mathscr{O}_K/(l)]^* \cong (\mathbb{F}_l^*)^3$.

Then there exists a cubic surface C *that is a counterexample to the Hasse principle, of the form*

$$x_0 x_1 x_2 = \mathrm{N}_{K/\mathbb{Q}}(a x_0 + b x_1 + c x_2 + d x_3)\,,$$

for $a, b, c, d \in \mathscr{O}_K$ *such that* $(a \bmod (l)) = \widetilde{a}, \ \ldots, \ (d \bmod (l)) = \widetilde{d}$.

Congruence conditions II

Idea of proof. This looks like infinitely many congruences (?).

- d: Choose solution $d' \in \mathscr{O}_K$ of
$$(d' \bmod (l)) = \widetilde{d}, \quad d' \equiv z \pmod{(7)}.$$
Partial factorisation $(d') = \mathfrak{p}\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \cdot (m')$, the $\mathfrak{p}_i$ being factors in K of split primes and $m' > 0$ a product of inert primes.
Choose prime $m \equiv m' \pmod{l}$, $m \equiv \pm 1 \pmod{7}$, and put $d := m \cdot \frac{d'}{m'}$.
- c: [Suppose $d \equiv z \pmod{\mathfrak{p}}$ for the presentation.]
$c \equiv -4 \pmod{\mathfrak{p}}$ is ethen quivalent to $7c/d \equiv 4z^2 \pmod{(7)}$.
Thus choose solution $c' = c'_0 + c'_1 z + c'_2 z^2 \in \mathscr{O}_K$ of
$$(c' \bmod (l)) = 7\widetilde{c}\widetilde{d}^{-1}, \quad c' \equiv 4z^2 \pmod{(7)}$$
and put $c := \frac{c'}{7} \cdot d$.
Assure $\gcd(c'_1, c'_2) = 1$ by choosing c_2 as a large prime number.
- b and a: Analogous to c. $\square$

Zariski density

Theorem (E.+J. 2013)

The cubic surfaces over $\mathbb{Q}$ that are counterexamples to the Hasse principle define a Zariski dense subset of the moduli scheme of smooth cubic surfaces.

Zariski density

Theorem (E.+J. 2013)

The cubic surfaces over $\mathbb{Q}$ that are counterexamples to the Hasse principle define a Zariski dense subset of the moduli scheme of smooth cubic surfaces.

Idea of proof. Over an algebraically closed field, every smooth cubic surface may be brought into Cayley–Salmon form $l_1 l_1 l_3 = l_4 l_5 l_6$. Hence, the morphism

$$\begin{aligned} p\colon \mathbf{A}^{12} &\longrightarrow \mathscr{M} \\ (a_{10}, \ldots, a_{33}) &\mapsto [C_a\colon x_0x_1x_2 = (a_{10}x_0 + \ldots + a_{13}x_3)(a_{20}x_0 + \ldots + a_{23}x_3) \\ &\qquad (a_{30}x_0 + \ldots + a_{33}x_3)] \end{aligned}$$

to the moduli scheme is dominant.

Suppose the counterexamples to the Hasse principle were contained in a proper, Zariski closed subset $H \subset \mathscr{M}$. Then all the counterexamples, we constructed, must be contained in $p^{-1}(H) \subset \mathbf{A}^{12}$, which is a proper, Zariski closed subset. I.e., in a hypersurface $V \subset \mathbf{A}^{12}$ of a certain degree d.

Then $V(\mathbb{F}_l) \leq dl^{11}$ for every prime l. But the counterexamples constructed have at least $(l-1)^{12}$ different reductions modulo a split prime l. $\square$

Zariski density II

The result generalises to the number field case, the proof just becomes more technical.

Corollary

Let K be a number field, $U_{\text{reg}} \subset \mathbf{P}^{19}_K$ the open subset that parametrises smooth cubic surfaces, and $\mathscr{H}\mathscr{C}_K \subset U_{\text{reg}}(K)$ be the set of all cubic surfaces over K that are counterexamples to the Hasse principle.

Then $\mathscr{H}\mathscr{C}_K$ is Zariski dense in $\mathbf{P}^{19}_K$.

Thanks

Thank you!!