Cubic surfaces violating the Hasse principle are Zariski dense in the moduli scheme

Andreas-Stephan Elsenhans* and Jörg Jahnel‡

Abstract

We construct new examples of cubic surfaces, for which the Hasse principle fails. Thereby, we show that, over every number field, the counterexamples to the Hasse principle are Zariski dense in the moduli scheme of non-singular cubic surfaces.

1 Introduction

1.1. —— Cubic surfaces over $\mathbb{Q}$ that violate the Hasse principle are known for more than 50 years. The first example of a cubic surface, for which the Hasse principle provably fails, was contrived by Sir Peter Swinnerton-Dyer [SD], in 1962. The construction had soon been generalized by L. J. Mordell [Mo], who found a whole family of examples. A further generalization was recently given by one of the authors [J].

A completely different kind of counterexample, being a diagonal cubic surface with a very particular coefficient vector, was discovered by J. W. S. Cassels and M. J. T. Guy [CG], in 1966. Later, J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc [CTKS] studied the arithmetic of these surfaces, in general.

Somewhat surprisingly, it seems that, until today, no cubic surface has been found that violates the Hasse principle without being of one of these two types. On the other hand, it is known that the Hasse principle is always valid for singular cubic surfaces [Sk].

*School of Mathematics and Statistics F07, University of Sydney, NSW 2006, Sydney, Australia, `stephan@maths.usyd.edu.au`, Website: `http://www.staff.uni-bayreuth.de/~bt270951`

‡Département Mathematik, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany, `jahnel@mathematik.uni-siegen.de`, Website: `http://www.uni-math.gwdg.de/jahnel`

Key words and phrases. Cubic surface, counterexample to the Hasse principle, moduli scheme

2010 Mathematics Subject Classification. Primary 11G35; Secondary 14G25, 14G05, 14J26, 14J10

1.2. —— The coarse moduli scheme of non-singular cubic surfaces over a base field K is the complement of a hypersurface in the four-dimensional weighted projective space $\mathbf{P}(1,2,3,4,5)_K$ [Cl], [Do, Section 9.4.5]. All diagonal cubic surfaces are geometrically isomorphic to each other. Thus, they correspond to a single point on the moduli scheme.

On the other hand, the Swinnerton-Dyer-Mordell type surfaces are contained in a two-dimensional closed subscheme of $\mathbf{P}(1,2,3,4,5)_{\mathbb{Q}}$. Indeed, they are given by equations of the form

$$T_3(a_1T_0 + d_1T_3)(a_2T_0 + d_2T_3) = \mathrm{N}_{K/\mathbb{Q}}(T_0 + \theta T_1 + \theta^2 T_2)\,, \qquad (1)$$

for $K/\mathbb{Q}$ a cyclic cubic field extension, $\theta \in K$, and $\mathrm{N}_{K/\mathbb{Q}}$ the norm map from K to $\mathbb{Q}$.

Such surfaces have at least three Eckardt points. The reason is that the three tritangent planes $V(T_3)$, $V(a_1T_0+d_1T_3)$, and $V(a_2T_0+d_2T_3)$ have a line in common. Thus, on each of the three tritangent planes $V(T_0+\theta^{(i)}T_1+\theta^{(i)2}T_2)$, the corresponding three lines meet at a single point. Lemma B.1 implies the claim.

1.3. Remarks. —— i) Calculations with concrete coefficients indicate that, generically, there are not more than three Eckardt points on the surfaces (1).

In this case, the automorphism groups of the cubic surfaces are isomorphic to S_3 [Do, Proposition 9.1.27]. Therefore, the surfaces are of type VIII in I. V. Dolgachev's classification [Do, Table 9.6].

ii) On the other hand, a diagonal cubic surface has 18 Eckardt points, which is the maximal number a non-singular cubic surface may have.

1.4. —— Let $\mathscr{HC}_K \subset \mathbf{P}^{19}(K)$ be the set of all cubic surfaces violating the Hasse principle and $\mathrm{C}\colon \mathbf{P}^{19} \dashrightarrow \mathbf{P}(1,\ldots,5)$ the Clebsch invariant map. In view of the considerations above, one is tempted to consider the following problems.

i) Describe the Zariski closure in the moduli space of the locus $\mathrm{HC}_K := \mathrm{C}(\mathscr{HC}_K)$ of the counterexamples to the Hasse principle.

ii) If $\dim \overline{\mathrm{HC}}_K < 4$ then find the geometric properties of cubic surfaces that are implied by the arithmetic property of being a counterexample to the Hasse principle.

In particular, does every cubic surface that does not fulfill the Hasse principle automatically have Eckardt points?

1.5. —— In this article, we will show that actually $\overline{\mathrm{HC}}_K$ is the full moduli space. I.e., that the Hasse counterexamples are Zariski dense in the moduli space of cubic surfaces. In particular, Problem ii) is pointless. Although certainly the case of the base field $\mathbb{Q}$ is of particular interest, we will work over an arbitrary number field K.

2 A family of cubic surfaces

2.1. —— We consider the cubic surface S over a number field K, given by the equation

$$T_0T_1T_2 = \mathrm{N}_{L/K}(aT_0 + bT_1 + cT_2 + dT_3)\,, \qquad (2)$$

for L/K a cyclic cubic field extension and $a, b, c, d \in L$.

2.2. —— Let us assume $d \neq 0$ as, otherwise, this surface is a cone. Further, we require that a/d, b/d, $c/d \notin K$. Then, as $\mathrm{N}_{L/K}$ represents zero only trivially, S has no K-rational point $(t_0 \!:\! t_1 \!:\! t_2 \!:\! t_3) \in S(K)$ with more than one of t_0, t_1, t_2 being equal to 0.

To prove $S(K) = \emptyset$ for particular choices of K, a, b, c, and d, our strategy is as follows. Suppose that there is a point $(t_0 \!:\! t_1 \!:\! t_2 \!:\! t_3) \in S(K)$. Among t_1/t_0, t_2/t_1, and t_0/t_2, consider an expression q that is properly defined and non-zero.

We will show that, for every prime ideal $\mathfrak{l}$ of K with the exception of exactly one, $q \in K_\mathfrak{l}$ is in the image of the norm map $N\colon L_\mathfrak{L} \to K_\mathfrak{l}$, for $\mathfrak{L}$ a prime of L lying above $\mathfrak{l}$. Such a behaviour, however, is incompatible with global class field theory, cf. [Ne, Chapter VI, Corollary 5.7] or [Ta, Theorem 5.1 together with 6.3].

2.3. Remark. —— Equation (2) is similar to the Swinnerton-Dyer-Mordell type. The only difference is that the three linear forms T_0, T_1, T_2 are linearly independent.

2.4. —— There is a conjecture due to J.-L. Colliot-Thélène [CTS, Conjecture C] that actually every cubic surface violating the Hasse principle does so via the Brauer-Manin obstruction, as introduced by Yu. I. Manin in [Ma, Chapter VI]. The new examples are in agreement with Colliot-Thélène's conjecture.

In fact, the choice of a rational function such as T_1/T_0 is not at all arbitrary. The principal divisor $\mathrm{div}(T_1/T_0)$ is the norm of a divisor, which is the difference of two lines. Thus, the cyclic algebra

$$\mathscr{A} := L(S)\{Y\}/(Y^3 - \tfrac{T_1}{T_0})$$

over the function field $K(S)$, where $Yt = \sigma(t)Y$ for $t \in L(S)$ and a fixed generator $\sigma \in \mathrm{Gal}(L/K)$, extends to an Azumaya algebra over S [Ma, Proposition 31.3]. This shows that we work, indeed, with a particular case of the Brauer-Manin obstruction.

2.5. Remarks. —— i) The quotients $\frac{T_1}{T_0}/\frac{T_2}{T_1} = \frac{T_1^3}{T_0T_1T_2}$ and $\frac{T_1}{T_0}/\frac{T_0}{T_2} = \frac{T_0T_1T_2}{T_0^3}$ are norms of rational functions. Thus, the three expressions T_1/T_0, T_2/T_1, T_0/T_2 actually define the same Brauer class.

ii) The non-singular cubic surfaces of the form (2) have a pair of Galois-invariant Steiner trihedra [EJ1, Fact 4.2]. Therefore, their Brauer groups are 3-torsion of order 3 or 9. A general procedure to calculate the Brauer-Manin obstruction to the Hasse principle or weak approximation for such surfaces was described in [EJ2].

The methods developed there are, however, not necessary here in their full strength. In fact, the most complicated case treated in [EJ2] is that of an orbit structure of type $[9, 9, 9]$ on the 27 lines. The surfaces of the form (2) generically have an orbit structure of type $[3, 3, 3, 9, 9]$, which is a technically much simpler case.

2.6. — Although certainly Brauer classes work behind the scenes, we will nevertheless stick to the elementary language of class field theory in the main body of this article. This will turn out to be completely sufficient for our purposes.

3 Unramified primes

3.1. Proposition (Inert primes). — *Let $\mathfrak{l}$ be a prime ideal of K that is inert in L/K. Write $\ell := \#\mathscr{O}_K/\mathfrak{l}$, denote by $\mathfrak{L}$ the unique prime of L lying above $\mathfrak{l}$, and assume that*

- $a, b, c \in \mathscr{O}_{L_\mathfrak{L}}$, $d \in \mathscr{O}^*_{L_\mathfrak{L}}$,
- $(a/d \bmod \mathfrak{L}), (b/d \bmod \mathfrak{L}), (c/d \bmod \mathfrak{L}) \in \mathbb{F}_{\ell^3}$ *are not contained in* $\mathbb{F}_\ell$.

Finally, let S denote the surface (2).

a.i) *If $\ell > 3$ then $S(K_\mathfrak{l}) \neq \emptyset$.*

ii) *If $a \equiv b \pmod{\mathfrak{l}}$ then $S(K_\mathfrak{l}) \neq \emptyset$.*

b) *For any $(t_0 : t_1 : t_2 : t_3) \in S(K_\mathfrak{l})$ such that $t_0 t_1 \neq 0$, the quotient $t_1/t_0 \in K_\mathfrak{l}$ is in the image of the norm map $N\colon L_\mathfrak{L} \to K_\mathfrak{l}$.*

Proof. The assumptions imply that a, b, and c are $\mathfrak{L}$-adic units, too. Let us write $\overline{a} := (a \bmod \mathfrak{L}), \ldots, \overline{d} := (d \bmod \mathfrak{L}) \in \mathbb{F}_{\ell^3}$.

a) The reduction $S_{\mathbb{F}_\ell}$ of S modulo $\mathfrak{l}$ is given by

$$T_0 T_1 T_2 = \mathrm{N}_{\mathbb{F}_{\ell^3}/\mathbb{F}_\ell}(\overline{a}T_0 + \overline{b}T_1 + \overline{c}T_2 + \overline{d}T_3)\,.$$

It is sufficient to show that $S_{\mathbb{F}_\ell}$ admits a non-singular $\mathbb{F}_\ell$-rational point.

i) We claim that the singular locus of $S_{\overline{\mathbb{F}}_\ell}$ is zero-dimensional. To show this, assume the contrary. Then there must exist a singular point x on the plane $E := V(T_0)$. Let us write the equation of $S_{\overline{\mathbb{F}}_\ell}$ in the form $T_0 T_1 T_2 = l_0 l_1 l_2$, for l_0, l_1, l_2 the three conjugates of the linear form $\overline{a}T_0 + \overline{b}T_1 + \overline{c}T_2 + \overline{d}T_3$. Then, by Lemma 3.2, x necessarily satisfies $T_0 = T_1 = 0$ or $T_0 = T_2 = 0$. But this would require $\overline{c}/\overline{d} \in \mathbb{F}_\ell$ or $\overline{b}/\overline{d} \in \mathbb{F}_\ell$ and therefore contradicts our assumptions.

Hence, the singular locus of $S_{\overline{\mathbb{F}}_\ell}$ is finite. It might happen that $S_{\overline{\mathbb{F}}_\ell}$ is a cone over a smooth cubic curve, but then it certainly has a non-singular $\mathbb{F}_\ell$-rational point. Otherwise, it was shown by A. Weil that $\#S_{\overline{\mathbb{F}}_\ell}(\mathbb{F}_\ell) \geq \ell^2 - 2\ell + 1$ [We, page 557], cf. [Ma, Theorem 27.1 and Table 31.1]. Further, it is classically known that not more than four points may be singular [Do, Corollary 9.2.3]. As $\ell^2 - 2\ell - 3 > 0$ for $\ell > 3$, this implies the assertion.

ii) We have $\overline{a} = \overline{b}$, hence $(1:(-1):0:0) \in S_{\mathbb{F}_\ell}(\mathbb{F}_\ell)$. Lemma 3.2 shows that this is a non-singular point.

b) We assume the coordinates of the point to be normalized such that $t_0, \ldots, t_3 \in \mathscr{O}_{K_\mathfrak{l}}$ and at least one of them is a unit. The local extension $L_\mathfrak{L}/K_\mathfrak{l}$ is unramified of degree three. We therefore have to show that $\nu_\mathfrak{l}(t_1/t_0)$ is divisible by three.

Assume the contrary. If $t_2 \neq 0$ then the equation of the surface ensures that $3|\nu_\mathfrak{l}(t_0t_1t_2)$. Thus, the values $\nu_\mathfrak{l}(t_i)$, for $i = 0, 1, 2$, must be mutually non-congruent modulo 3. Otherwise, we know at least $\nu_\mathfrak{l}(t_0) \not\equiv \nu_\mathfrak{l}(t_1) \pmod 3$ and $t_2 = 0$. There are two cases.

First case. There is no unit among t_0, t_1, t_2.
Then t_3 is a unit. Since we assume d to be a unit, too, we clearly have that $at_0 + bt_1 + ct_2 + dt_3 \in \mathscr{O}^*_{L_\mathfrak{L}}$. Hence, $\mathrm{N}_{L_\mathfrak{L}/K_\mathfrak{l}}(at_0 + bt_1 + ct_2 + dt_3) \in \mathscr{O}^*_{K_\mathfrak{l}}$, which, in view of $t_0t_1t_2$ not being a unit, contradicts the equation of the surface.

Second case. There is exactly one unit among t_0, t_1, t_2.
Without restriction, assume that t_0 is the unit. Again, we have that $t_0t_1t_2$ is not a unit. The equation of the surface then requires that $\mathrm{N}_{L_\mathfrak{L}/K_\mathfrak{l}}(at_0 + bt_1 + ct_2 + dt_3)$ must be a non-unit. To ensure this, we need $at_0 + bt_1 + ct_2 + dt_3 \notin \mathscr{O}^*_{L_\mathfrak{L}}$, which means nothing but

$$at_0 + dt_3 \equiv 0 \pmod{\mathfrak{L}}\,.$$

But then $a/d \equiv -t_3/t_0 \pmod{\mathfrak{L}}$, which is impossible since the right hand side modulo $\mathfrak{L}$ is in $\mathbb{F}_\ell$, while the left hand side is not. $\square$

3.2. Lemma. — *Let K be a field, $l_0, l_1, l_2, l'_0, l'_1, l'_2 \in K[T_0, T_1, T_2, T_3]$ linear forms such that $V(l_i) \neq V(l'_j)$ for all $0 \leq i, j \leq 2$, and S be the cubic surface, given by $l_0l_1l_2 = l'_0l'_1l'_2$.*

Then, every singular point on S lying on the plane $V(l_0)$ actually lies on at least two of the planes $V(l_i)$ and two of the planes $V(l'_j)$.

Proof. Let x be a singular point on S lying on the plane $V(l_0)$. Then $x \in V(l'_0l'_1l'_2)$. Without restriction, we may suppose that $x \in V(l'_0)$. Further, the assumption ensures that, after a suitable change of coordinates, we may assume that $l_0 = T_0$ and $l'_0 = T_1$. I.e., that S is given by the equation

$$F(T_0, T_1, T_2, T_3) := T_0l_1l_2 - T_1l'_1l'_2 = 0$$

and we consider a singular point $x = (0 : 0 : t_2 : t_3)$. As $\frac{\partial F}{\partial T_0}(x) = l_1l_2(x)$ and $\frac{\partial F}{\partial T_1}(x) = l'_1l'_2(x)$, the assertion follows. $\square$

3.3. Lemma (Split primes). —— *Let $\mathfrak{l}$ be a prime of K that is split in L/K, $a, b, c, d \in L$ be arbitrary, and S be the cubic surface, given by equation (2).*

a) *Then $S(K_\mathfrak{l}) \neq \emptyset$.*

b) *Every non-zero element of $K_\mathfrak{l}$ is a local norm for the extension L/K of global fields.*

Proof. a) The scheme $S_{K_\mathfrak{l}}$ is defined by the equation

$$T_0T_1T_2 = \prod_{i=1}^{3}[\sigma_i(a)T_0 + \sigma_i(b)T_1 + \sigma_i(c)T_2 + \sigma_i(d)T_3]$$

for $\sigma_i\colon K \hookrightarrow L \otimes_K K_\mathfrak{l} \to K_\mathfrak{l}$ the three homomorphisms. There is a $K_\mathfrak{l}$-rational line or plane, defined by $T_0 = \sigma_1(b)T_1 + \sigma_1(c)T_2 + \sigma_1(d)T_3 = 0$.

b) This is a standard result from class field theory. $\square$

3.4. Remark (The archimedean primes). —— i) Let $\sigma\colon K \hookrightarrow \mathbb{R}$ be a real prime. Then, for a, b, c, $d \in L$ arbitrary, we also have $S_{\mathbb{R},\sigma}(\mathbb{R}) \neq \emptyset$. Further, every non-zero real number is, with respect to σ, a local norm for the extension L/K of global fields.

Indeed, as L/K is a cubic Galois extension, there are three real primes $\sigma_i\colon L \to \mathbb{R}$ extending σ. This immediately implies the second assertion. On the other hand, $S_{\mathbb{R},\sigma}$ is given by the equation $T_0T_1T_2 = \prod_{i=1}^{3}[\sigma_i(a)T_0 + \sigma_i(b)T_1 + \sigma_i(c)T_2 + \sigma_i(d)T_3]$. Thus, the same argument as above yields plenty of real points.

In fact, it is known since the days of L. Schläfli [Sch, pp. 114f.] that a non-singular cubic surface $\mathscr{S}$ over $\mathbb{R}$ always has real points. A nice geometric argument for this is as follows. Start with a $\mathbb{C}$-rational point $x \in \mathscr{S}(\mathbb{C})$ not lying on any of the 27 lines. Unless x is already the extension of a real point, there is a unique line connecting x with its complex conjugate $\overline{x}$. This line meets $\mathscr{S}$ in a third point, which must be real.

ii) For $\sigma\colon K \hookrightarrow \mathbb{C}$ a complex prime and a, b, c, $d \in L$ arbitrary, we clearly have $S_{\mathbb{C},\sigma}(\mathbb{C}) \neq \emptyset$. Further, every non-zero complex number is a local norm with respect to σ.

4 Ramified primes–Reduction to a particular cone

4.1. —— Local class field theory shows that a local field with residue field $\mathbb{F}_\ell$ for $\ell \equiv 2 \pmod 3$ does not allow any ramified, cyclic cubic extensions. Hence, a cyclic cubic extension L/K may ramify only at primes $\mathfrak{l}$ such that either $\#\mathscr{O}_K/\mathfrak{l} \equiv 1 \pmod 3$ or $\#\mathscr{O}_K/\mathfrak{l}$ is a power of 3. We will consider the former case in this article.

4.2. Lemma. —— *Let $p \neq 3$ be a prime number.*

i) *Then the equation*

$$27T_0T_1T_2 = (T_0 + T_1 + T_2)^3$$

defines a cubic curve C over $\mathbb{F}_p$ with a node at $(1{:}1{:}1)$. The two tangent directions at $(1{:}1{:}1)$ are defined over $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$.

ii) *Let $e \geq 1$ be any integer. Then, for every $\mathbb{F}_{p^e}$-rational point $(t_0{:}t_1{:}t_2)$ on C, 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 $\mathbb{F}_{p^e}$. Further, these quotients evaluate solely to cubes in $\mathbb{F}_{p^e}^*$.*

Proof. i) It is a standard calculation to show that C has a singular point at $(1{:}1{:}1)$ and no others. The tangent cone at this point is defined by a binary quadric of discriminant $(-243) = -3 \cdot 9^2$. Thus, it splits if and only if (-3) is a quadratic residue modulo p.

ii) The first assertion simply says that $(1:0:0), (0:1:0), (0:0:1) \notin C$. Further, a calculation in any computer algebra system verifies that, 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 $27T_0T_1T_2 - (T_0 + T_1 + T_2)^3$. Hence, T_0/T_2 is the cube of a rational function on C.

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

Due to symmetry, the same is true for t_1/t_0 and t_2/t_1. This is the assertion. $\square$

4.3. Example. —— Consider the nodal cubic curve, defined by

$$T_0T_1T_2 + (T_0 + T_1 + T_2)^3 = 0$$

over $\mathbb{F}_7$. Besides the node at $(1:1:1)$, there are the six $\mathbb{F}_7$-rational points $(1:(-1):0), (1:0:(-1)), (0:1:(-1)), (1:1:(-1)), (1:(-1):1)$, and $((-1):1:1)$. We see explicitly that, for every $\mathbb{F}_7$-rational point, at least one of the expressions T_1/T_0, T_2/T_1, T_0/T_2 is properly defined and non-zero in $\mathbb{F}_7$ and that all these quotients are cubes in $\mathbb{F}_7^*$.

4.4. Corollary. —— *Let ℓ be a prime power, but not a power of 3, and $\alpha \in \mathbb{F}_\ell^*$ arbitrary.*

i) *Then the equation $T_0T_1T_2 - \frac{1}{27}(\alpha T_0 + T_1 + \frac{1}{\alpha}T_2)^3 = 0$ defines a nodal cubic curve C' over $\mathbb{F}_\ell$.*

ii) *For every $\mathbb{F}_\ell$-rational point $(t_0{:}t_1{:}t_2)$ on C', at least one of the expressions t_1/t_0, t_2/t_1, t_0/t_2 is properly defined and non-zero in $\mathbb{F}_\ell$. Further, these quotients evaluate only to elements in the coset of α modulo the cubic residues.*

Proof. i) The curve C' is isomorphic to C as it is obtained from C by substituting αT_0 for T_0 and $\frac{1}{\alpha}T_2$ for T_2.

This implies, as well, the first assertion of ii). Further, $T_1/\alpha T_0 = \frac{1}{\alpha}T_1/T_0$, $\frac{1}{\alpha}T_2/T_1$, and $\alpha T_0/\frac{1}{\alpha}T_2 = \alpha^2 T_0/T_2$ are cubes as soon as they are properly defined in $\mathbb{F}_\ell^*$. □

4.5. Proposition (Ramified primes). — *Let $\mathfrak{l}$ be a prime ideal of K that is ramified in L/K. Suppose that $\ell := \#\mathscr{O}_K/\mathfrak{l}$ is not a power of* 3*. Denote by $\mathfrak{L}$ the unique prime of L lying above $\mathfrak{l}$ and assume that*

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

for some $\alpha \in \mathbb{F}_\ell^*$. Finally, let S denote the surface (2).

a) *Then one has $S(K_\mathfrak{l}) \neq \emptyset$.*

b) *Let $(t_0 : t_1 : t_2 : t_3) \in S(K_\mathfrak{l})$ be any point. Then not more than one of t_0, t_1, t_2 may vanish.*

c.i) *Suppose that $\alpha \in \mathbb{F}_\ell^*$ is a non-cube. Then the following is true.*

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

ii) *If $\alpha \in \mathbb{F}_\ell^*$ is a cube then, for any $(t_0 : t_1 : t_2 : t_3) \in S(K_\mathfrak{l})$, the quotients $t_j/t_i \in K_\mathfrak{l}$, $0 \leq i < j \leq 2$, are local norms, as soon as they are properly defined.*

Proof. Recall that we automatically have $\ell \equiv 1 \pmod 3$.

a) The reduction of S modulo $\mathfrak{l}$ is given by $T_0T_1T_2 - \frac{1}{27}(\alpha T_0 + T_1 + \frac{1}{\alpha}T_2)^3 = 0$. I.e., it is the cone over the nodal cubic curve C', studied in Corollary 4.4. $S_{\mathbb{F}_\ell}$ has exactly $(\ell-1)\ell$ non-singular $\mathbb{F}_\ell$-rational points.

b) We assume the contrary and consider the case that $t_1 = t_2 = 0$, the others being analogous. The equation of the surface then requires $at_0 + dt_3 = 0$. As our assumptions imply $a \neq 0$ and $d \neq 0$, we certainly have $t_0 \neq 0$ and $t_3 \neq 0$ and may write $d/a = -t_0/t_3$. Here, the right hand side is an element of $K_\mathfrak{l}$. Hence, $3|\nu_\mathfrak{L}(-t_0/t_3)$. On the other hand, since a is a unit, $d/a \in \mathfrak{L}\backslash\mathfrak{L}^3$. Thus, $\nu_\mathfrak{L}(d/a) = 1$ or 2, which is a contradiction.

c) No $K_\mathfrak{l}$-rational point on S may reduce to the cusp $(0:0:0:1) \in S_{\mathbb{F}_\ell}(\mathbb{F}_\ell)$. Indeed, such a point could written in normalized form such that $\nu_\mathfrak{l}(t_0), \nu_\mathfrak{l}(t_1), \nu_\mathfrak{l}(t_2) \geq 1$ and t_3 is a unit. But then $\nu_\mathfrak{l}(t_0t_1t_2) \geq 3$, while

$$\nu_\mathfrak{l}(\mathrm{N}_{L_\mathfrak{L}/K_\mathfrak{l}}(at_0+bt_1+ct_2+dt_3)) = \nu_\mathfrak{L}(at_0+bt_1+ct_2+dt_3) = \nu_\mathfrak{L}(dt_3) = \nu_\mathfrak{L}(d) = 1 \text{ or } 2\,.$$

Consequently, Corollary 4.4.ii) shows that at least one of the quotients t_j/t_i is properly defined and a unit in $\mathscr{O}_{K_\mathfrak{l}}$. Further, its residue modulo $\mathfrak{l}$ is a cube if and only if α is. Hence, $t_j/t_i \in K_{\mathfrak{l}}$ is a local norm when α is a cube and not a local norm, otherwise. Remark 2.5.i) implies that the same is true for each of the three quotients, as soon as it is properly defined in $K_{\mathfrak{l}}^*$. $\square$

5 The main result

5.1. Theorem. — *Let L/K be a cyclic cubic extension that is ramified at at least one prime. Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathscr{O}_K$ the ramified primes and write $\mathfrak{P}_i$ for the unique prime lying above $\mathfrak{p}_i$. Suppose that $q_i := \#\mathscr{O}_K/\mathfrak{p}_i$ is not a power of 3, for any i.*

Choose a non-cube $\alpha_1 \in \mathbb{F}_{q_1}^*$, cubes $\alpha_2 \in \mathbb{F}_{q_2}^*, \ldots, \alpha_r \in \mathbb{F}_{q_r}^*$, and assume that a, b, c, $d \in \mathscr{O}_L$ satisfy the following conditions.

i) *d splits as $(d) = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r \mathfrak{L}_1 \cdot \ldots \cdot \mathfrak{L}_s$, where $\mathrm{N}(\mathfrak{L}_i)$ are prime ideals $\neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. I.e., (d) does not contain any inert prime and contains $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ exactly once.*

ii) *$(a/d \bmod \mathfrak{l}\mathscr{O}_L)$, $(b/d \bmod \mathfrak{l}\mathscr{O}_L)$, $(c/d \bmod \mathfrak{l}\mathscr{O}_L) \in \mathscr{O}_L/\mathfrak{l}\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{l}$ for every inert prime ideal $\mathfrak{l}$ in K.*

iii) *$a \equiv b \pmod{\mathfrak{l}\mathscr{O}_L}$ for every inert prime $\mathfrak{l}$ of K such that $\#\mathscr{O}_K/\mathfrak{l} = 2$ or 3.*

iv) *$(a \bmod \mathfrak{P}_i) = \frac{\alpha_i}{3}$, $(b \bmod \mathfrak{P}_i) = \frac{1}{3}$, and $(c \bmod \mathfrak{P}_i) = \frac{1}{3\alpha_i}$, for $i = 1, \ldots, r$.*

Finally, let S denote the surface (2). Then $S(\mathbb{A}_K) \neq \emptyset$ but $S(K) = \emptyset$.

Proof. *First step.* Preparations.
Let $\mathfrak{l} \subset \mathscr{O}_K$ be any prime ideal.

Case 1. $\mathfrak{l} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r$.
Assumption i) implies that, for $i = 1, \ldots, r$, one has $d \in \mathfrak{P}_i \backslash \mathfrak{P}_i^2 \subset \mathfrak{P}_i \backslash \mathfrak{P}_i^3$. Together with assumption iv), we see that Proposition 4.5 applies.

Case 2. $\mathfrak{l}$ is an inert prime.
Then $\mathfrak{L} := \mathfrak{l}\mathscr{O}_L$ is the unique prime lying above $\mathfrak{l}$. By assumption i), we know that $d \in \mathscr{O}_{K_\mathfrak{L}}^*$. Thus, we are exactly in the situation of Proposition 3.1. Note that we have $S(K_\mathfrak{l}) \neq \emptyset$ for primes $\mathfrak{l}$ with $\#\mathscr{O}_K/\mathfrak{l} = 2, 3$, too, as then $a \equiv b \pmod{\mathfrak{L}}$.

Case 3. $\mathfrak{l}$ is a split prime.
Then Lemma 3.3 applies.

Second step. The existence of an adelic point.
This is equivalent to the existence of a real point on $S_{\mathbb{R},\sigma}$ for every real prime $\sigma\colon K \hookrightarrow \mathbb{R}$, a complex point on $S_{\mathbb{C},\sigma}$ for every complex prime $\sigma\colon K \hookrightarrow \mathbb{C}$, and a $K_\mathfrak{l}$-rational point for every prime ideal $\mathfrak{l} \subset \mathscr{O}_K$. We know from Remark 3.4 that $S_{\mathbb{R},\sigma}$ and $S_{\mathbb{C},\sigma}$ admit real and complex points, respectively. The presence of $K_\mathfrak{l}$-rational points for every $\mathfrak{l}$ is guaranteed by Proposition 4.5.a), Lemma 3.3.a), and Proposition 3.1.a).

Third step. The non-existence of a K-rational point.
Suppose there would be a K-rational point $(t_0 : t_1 : t_2 : t_3) \in S(K)$. Then, by Proposition 4.5.b), among t_0, t_1, t_2, not more than one may vanish. Choose $0 \leq i < j \leq 2$ such that $t_i t_j \neq 0$ and consider the quotient $t_j/t_i \in K$.

This is a local norm at every archimedean prime and at every split prime by Remark 3.4 and Lemma 3.3.b). It is a local norm at every inert prime, too, in view of Lemma 3.1.b). Further, the quotient t_j/t_i is a local norm at the ramified primes $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, as was shown in Proposition 4.5.c). It is, however, not a local norm at the prime $\mathfrak{p}_1$.

The proof is complete, since such a behaviour is in contradiction with global class field theory, [Ne, Chapter VI, Corollary 5.7] or [Ta, Theorem 5.1 together with 6.3]. □

5.2. Remark. —— At a first glance, condition ii) seems to be hard to check as infinitely many primes are involed. Our strategy for its verification is the following.

- Choose elements $z_1, z_2 \in \mathscr{O}_L$ such that $1, z_1, z_2$ are K-linearly independent. Then $\mathscr{O}_L/\langle 1, z_1, z_2 \rangle$ is finite. I.e., for an inert prime $\mathfrak{l}$ of K and $\mathfrak{L}$ the prime lying above $\mathfrak{l}$, one has $\mathscr{O}_{L_\mathfrak{L}} = \langle 1, z_1, z_2 \rangle_{\mathscr{O}_{K_\mathfrak{l}}}$, with only finitely many exceptions $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$.
- For $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$, check condition ii) directly.
- Further, write

$$a/d = \tfrac{1}{N}(a_0 + a_1 z_1 + a_2 z_2), \quad b/d = \tfrac{1}{N}(b_0 + b_1 z_1 + b_2 z_2), \quad c/d = \tfrac{1}{N}(c_0 + c_1 z_1 + c_2 z_2)$$

for $a_i, b_i, c_i \in \mathscr{O}_K$ and $N \in \mathscr{O}_K$ an element that splits only into prime ideals split or ramified in L/K and, possibly, into $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$.
Then check that the ideals $\gcd(a_1, a_2)$, $\gcd(b_1, b_2)$, $\gcd(c_1, c_2) \subset \mathscr{O}_K$ do not contain any inert primes in their factorizations, except possibly $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$.

5.3. Example. —— Let $L := \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $z := \zeta_7 + \zeta_7^{-1} - 2$, and S be the cubic surface over $\mathbb{Q}$, given by equation (2), for

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

Then S violates the Hasse principle.

Proof. L is the unique cubic subfield of the cyclotomic extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. It is ramified only at 7. The primes ($\pm 1 \bmod 7$) are split, the others are inert. The algebraic integer z is chosen such that, for the unique prime of L lying above 7, we have $\mathfrak{P} = (z)$.

We work with the $\mathbb{Q}$-linearly independent elements $1, z, z^2$, which form a $\mathbb{Z}$-basis for $\mathscr{O}_K$. Conditions i) and iii) of Theorem 5.1 are obviously satisfied. For iv), note that, in $\mathbb{F}_7$, one has $\frac{1}{3} = 5$. Further, $\alpha = -\frac{1}{5} = 4$ is a non-cube and $\frac{5}{4} = 3$. Finally, $a/d = \frac{1}{7}(14 + 7z + z^2)$, $b/d = \frac{1}{7}(-70 + 7z - 5z^2)$, and $c/d = \frac{1}{7}(-42 - 14z - 3z^2)$. □

5.4. Example (continued). — The equation of S is, in explicit form,

$$\begin{aligned}&T_0^3-141T_0^2T_1-30T_0^2T_2+7T_0^2T_3+4863T_0T_1^2+2233T_0T_1T_2-532T_0T_1T_3\\&+251T_0T_2^2-119T_0T_2T_3+14T_0T_3^2-31499T_1^3-26286T_1^2T_2+6013T_1^2T_3\\&-6799T_1T_2^2+3157T_1T_2T_3-364T_1T_3^2-559T_2^3+392T_2^2T_3-91T_2T_3^2+7T_3^3=0\,.\end{aligned}$$

S has bad reduction at 2, 3, 7, 3739, and 7589. While, at 7, the reduction is the cone over the nodal cubic curve, described in Corollary 4.4, the reductions at the other bad primes only have one singular point each. $S_{\mathbb{F}_2}$ has a binode. The other three have a conical singularity.

A minimization algorithm yields a reembedding of S as the surface, given by the equation

$$\begin{aligned}&-T_0^3+2T_0^2T_1-T_0^2T_2-5T_0^2T_3+T_0T_1^2-T_0T_1T_2+7T_0T_1T_3+2T_0T_2^2-15T_0T_2T_3\\&-11T_0T_3^2-T_1^3-2T_1^2T_2+9T_1^2T_3+T_1T_2^2+T_1T_3^2+T_2^3+T_2^2T_3+8T_2T_3^2-T_3^3=0\,.\end{aligned}$$

5.5. Corollary. — *Let L/K be a cyclic cubic extension that is ramified at at least one prime, but unramified at all primes dividing* 3. *Choose a split prime $\mathfrak{l}$ of K and let $\widetilde{a},\widetilde{b},\widetilde{c},\widetilde{d}$ be four residue classes in $[\mathscr{O}_L/\mathfrak{l}\mathscr{O}_L]^*\cong(\mathbb{F}_\ell^*)^3$.*

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

$$T_0T_1T_2=\mathrm{N}_{L/K}(aT_0+bT_1+cT_2+dT_3)\,,$$

for $a,b,c,d\in\mathscr{O}_L$ such that $(a \bmod \mathfrak{l}\mathscr{O}_L)=\widetilde{a}$, …, $(d \bmod \mathfrak{l}\mathscr{O}_L)=\widetilde{d}$.

Proof. Denote by $\mathfrak{p}_1,\dots,\mathfrak{p}_r\subset\mathscr{O}_K$ the primes ramified in L/K.

First step. d.

Write $\mathfrak{P}_i$ for the unique prime ideal lying above $\mathfrak{p}_i$, for $i=1,\dots,r$. Further, let $\mathfrak{f}\subseteq\mathscr{O}_K$ be the conductor of the extension L/K of global fields.

According to the Chinese remainder theorem, we may choose an element $d'\in\mathscr{O}_L$ such that $(d' \bmod \mathfrak{l}\mathscr{O}_L)=\widetilde{d}$ and d' is a uniformizer for each $\mathfrak{P}_i$. We find a partial factorization

$$(d')=\mathfrak{P}_1\cdot\ldots\cdot\mathfrak{P}_r\mathfrak{L}_1\cdot\ldots\cdot\mathfrak{L}_s\cdot(m')\,,$$

where $\mathfrak{L}_1,\dots,\mathfrak{L}_s$ are prime factors in L of split primes of K and $m'\in\mathscr{O}_K$ is an element that splits into a product of inert primes. In particular, m' is relatively prime to $\mathfrak{l}$.

By Sublemma 5.7, we may choose some $m\equiv m' \pmod{\mathfrak{l}}$, $m\equiv 1 \pmod{\mathfrak{f}}$, such that (m) is a prime ideal. Indeed, $\mathfrak{l}$ and $\mathfrak{f}$ are relatively prime [Ne, Chapter VI, Corollary 6.6], such that this is in fact a congruence condition modulo $\mathfrak{l}\mathfrak{f}$. According to the decomposition law [Ne, Chapter VI, Theorem 7.3], the congruence $m\equiv 1$ (mod $\mathfrak{f}$) is clearly enough to ensure that (m) splits in L/K.

Thus, put $d := m\cdot\frac{d'}{m'}$. Then $d \in \mathscr{O}_L$ fulfills the congruence condition modulo $\mathfrak{l}\mathscr{O}_L$ and assumption i) of Theorem 5.1.

Second step. c.

By Lemma 5.6, there is a solution $c' \in \mathscr{O}_L$ of the congruence system

$$(c' \bmod \mathfrak{l}\mathscr{O}_L) = (\tfrac{\mathrm{N}(d)}{d} \bmod \mathfrak{l}\mathscr{O}_L)\cdot\widetilde{c}\,,$$
$$(c' \bmod \mathfrak{p}_i\mathscr{O}_L) = \tfrac{1}{3\alpha_i}\cdot(\tfrac{\mathrm{N}(d)}{d} \bmod \mathfrak{p}_i\mathscr{O}_L)\,, \quad i = 1,\ldots,r\,,$$

such that $(c' \bmod \mathfrak{p}\mathscr{O}_L) \notin \mathscr{O}_L/\mathfrak{p}\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{p}$ for any prime $\mathfrak{p}$ of K, different from the ramified ideals $\mathfrak{p}_j$.

Observe here that $\frac{\mathrm{N}(d)}{d}$ is invertible modulo $\mathfrak{l}\mathscr{O}_L$ in view of the first step. Further, $\nu_{\mathfrak{P}_i}(\frac{\mathrm{N}(d)}{d}) = 2$. Thus, actually, $(\frac{\mathrm{N}(d)}{d} \bmod \mathfrak{p}_i\mathscr{O}_L) \in \mathfrak{P}_i^2/\mathfrak{P}_i^3$, which is a module over the residue field.

Finally, put $c := c'\cdot\frac{d}{\mathrm{N}(d)}$. Then $c \in \mathscr{O}_L$ fulfills the congruence condition modulo $\mathfrak{l}\mathscr{O}_L$ and the assumptions on c made in Theorem 5.1.ii) and iv).

Third step. b.

Take a solution $b' \in \mathscr{O}_L$ of the congruence system

$$(b' \bmod \mathfrak{l}\mathscr{O}_L) = (\tfrac{\mathrm{N}(d)}{d} \bmod \mathfrak{l}\mathscr{O}_L)\cdot\widetilde{b}\,,$$
$$(b' \bmod \mathfrak{p}_i\mathscr{O}_L) = \tfrac{1}{3}\cdot(\tfrac{\mathrm{N}(d)}{d} \bmod \mathfrak{p}_i\mathscr{O}_L)\,, \quad i = 1,\ldots,r\,,$$

such that $(b' \bmod \mathfrak{p}\mathscr{O}_L) \notin \mathscr{O}_L/\mathfrak{p}\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of K, different from the $\mathfrak{p}_j$, and put $b := b'\cdot\frac{d}{\mathrm{N}(d)}$. Then $b \in \mathscr{O}_L$ fulfills the congruence condition modulo $\mathfrak{l}\mathscr{O}_L$ and the assumptions on b made in Theorem 5.1.ii) and iv).

Fourth step. a.

For this, take a solution $a' \in \mathscr{O}_L$ of the slightly larger congruence system

$$(a' \bmod \mathfrak{l}\mathscr{O}_L) = (\tfrac{\mathrm{N}(d)}{d} \bmod \mathfrak{l}\mathscr{O}_L)\cdot\widetilde{b}\,,$$
$$(a' \bmod \mathfrak{p}_i\mathscr{O}_L) = \tfrac{\alpha_i}{3}\cdot(\tfrac{\mathrm{N}(d)}{d} \bmod \mathfrak{p}_i\mathscr{O}_L)\,, \quad i = 1,\ldots,r\,,$$
$$a' \equiv b' \pmod{\mathfrak{l}_j}\,,$$

such that $(a' \bmod \mathfrak{p}\mathscr{O}_L) \notin \mathscr{O}_L/\mathfrak{p}\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{p}$ for any unramified prime ideal $\mathfrak{p}$ of K. Here, the $\mathfrak{l}_j \subset \mathscr{O}_K$ run over all inert primes of K such that $\#\mathscr{O}_K/\mathfrak{l}_j = 2$ or 3.

To complete the construction, put $a := a'\cdot\frac{d}{\mathrm{N}(d)}$. Then $a \in \mathscr{O}_L$ fulfills the congruence condition modulo $\mathfrak{l}\mathscr{O}_L$ and the assumptions on a made in Theorem 5.1.ii), iii), and iv). $\square$

5.6. Lemma. — *Let K be a number field, L/K a cyclic cubic extension, $\mathfrak{l}_1,\ldots,\mathfrak{l}_r \subset \mathscr{O}_K$ distinct prime ideals, and $a_1,\ldots,a_r \in \mathscr{O}_K$. Then, for the congruence system*

$$a \equiv a_1 \pmod{\mathfrak{l}_1\mathscr{O}_L}\,,$$
$$\ldots$$
$$a \equiv a_r \pmod{\mathfrak{l}_r\mathscr{O}_L}\,.$$

there is a solution $a \in \mathscr{O}_L$ such that $(a \bmod \mathfrak{l}\mathscr{O}_L) \notin \mathscr{O}_L/\mathfrak{l}\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{l}$ for any prime ideal $\mathfrak{l} \neq \mathfrak{l}_1, \ldots, \mathfrak{l}_r$ of K, unramified in L/K.

Proof. Choose elements $z_1, z_2 \in \mathscr{O}_L$ such that $1, z_1, z_2$ are K-linearly independent. Then $\mathscr{O}_L/\langle 1, z_1, z_2 \rangle$ is finite, such that $\mathscr{O}_L \otimes_{\mathscr{O}_K} \mathscr{O}_{K_\mathfrak{l}} = \langle 1, z_1, z_2 \rangle_{\mathscr{O}_{K_\mathfrak{l}}}$ for all primes $\mathfrak{l}$ of K, with finitely many exceptions $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Unless these are among the $\mathfrak{l}_i$, add congruence conditions

$$a \equiv b_j \pmod{\mathfrak{p}_j \mathscr{O}_L},$$

for $j = 1, \ldots, s$. Choose $b_1, \ldots, b_s \in \mathscr{O}_L$ such that $(b_j \bmod \mathfrak{p}_j\mathscr{O}_L) \notin \mathscr{O}_L/\mathfrak{p}_j\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{p}_j$, whenever $\mathfrak{p}_j$ is unramified in L/K.

Since $\mathscr{O}_L$ is a Dedekind domain, the Chinese remainder theorem applies and we actually have only one congruence condition $a \equiv A \pmod{I}$. Take, at first, any solution $a' \in \mathscr{O}_L$ of it and write it in the form

$$a' = \tfrac{1}{N}(a_0 + a_1 z_1 + a_2 z_2),$$

for $a_0, a_1, a_2 \in \mathscr{O}_K$ and $N \in \mathscr{O}_K$ a product of the exceptional primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. The congruence condition will clearly not be violated as long as we vary a_1 and a_2 in their respective residue classes modulo NI.

By Sublemma 5.7, we may choose a representative $\underline{a}_1$ such that $(\underline{a}_1)$ is a product of some prime divisors of NI and one further prime $\mathfrak{p}'$. In addition, we may choose $\underline{a}_2$ such that $(\underline{a}_2)$ is a product of some some prime divisors of NI and a prime $\mathfrak{p}'' \neq \mathfrak{p}'$. Then $a := \frac{1}{N}(a_0 + \underline{a}_1 z_1 + \underline{a}_2 z_2) \in \mathscr{O}_L$ solves the congruence system modulo the ideals $\mathfrak{l}_i$ and $\mathfrak{p}_j$.

Now let $\mathfrak{l} \subset \mathscr{O}_K$, $\mathfrak{l} \neq \mathfrak{l}_1, \ldots, \mathfrak{l}_r$, be any prime ideal, unramified in L/K. If $\mathfrak{l} = \mathfrak{p}_j$, for some j, then $(a \bmod \mathfrak{l}\mathscr{O}_L) \notin \mathscr{O}_L/\mathfrak{l}\mathscr{O}_L \setminus \mathscr{O}_K/\mathfrak{l}$ is fulfilled by construction. But, otherwise, $\mathfrak{l}$ is not a divisor of of NI. Then $\frac{1}{N} \in \mathscr{O}_{K_\mathfrak{l}}$ and $\underline{a}_1$ and $\underline{a}_2$ cannot be both divisible by $\mathfrak{l}$. This implies the assertion. □

5.7. Sublemma. —— *Let K be a number field, $I \subset \mathscr{O}_K$ an ideal, and $x \in \mathscr{O}_K$. Put $\mathfrak{t} := \operatorname{lcm}_{n \in \mathbb{N}}(\gcd(I^n, (x)))$.*

Then there exist infinitely many pairwise non-associated elements $y_1, y_2, \ldots \in \mathscr{O}_K$ such that $y_i \equiv x \pmod{I}$ and that each (y_i) factors into $\mathfrak{t}$ and a prime ideal.

Proof. Write $(x) = \mathfrak{x}\mathfrak{t}$. Then $\mathfrak{x}$ is an ideal, relatively prime to I. It is known that there exist infinitely many prime ideals $\mathfrak{p}_i \subset \mathscr{O}_K$ with the property below.

There exist some $u_i, v_i \in \mathscr{O}_K$, $u_i \equiv v_i \equiv 1 \pmod{I}$ such that

$$\mathfrak{p}_i \cdot (u_i) = \mathfrak{x} \cdot (v_i).$$

Indeed, the invertible ideals of K modulo the principal ideals generated by elements from the residue class $(1 \bmod I)$ form an abelian group that is canonically isomorphic to the ray class group $Cl_K^I \cong C_K/C_K^I$ of K [Ne, Chapter VI, Proposition 1.9].

Thus, the claim follows from the Cebotarev density theorem applied to the ray class field K^I/K, which has the Galois group $\mathrm{Gal}(K^I/K) \cong Cl_K^I$.

Take one of these prime ideals. Then $\mathfrak{p}_i\mathfrak{t}\cdot(u_i) = \mathfrak{x}\mathfrak{t}\cdot(v_i) = (xv_i)$. As $\mathfrak{p}_i\mathfrak{t} \subset \mathscr{O}_K$, this shows that xv_i is divisible by u_i. Put $y_i := xv_i/u_i$. Then $(y_i) = \mathfrak{p}_i\mathfrak{t}$. Further, $y_i \equiv x \pmod{I}$. □

5.8. Theorem. —— *Let K be any number field, $U_\mathrm{reg} \subset \mathbf{P}^{19}_K$ the open subset parametrizing non-singular cubic surfaces, and $\mathscr{H\!C}_K \subset U_\mathrm{reg}(K)$ be the set of all cubic surfaces over K that are counterexamples to the Hasse principle.*
Then the image of $\mathscr{H\!C}_K$ under Clebsch's invariant map

$$\mathrm{C}\colon U_\mathrm{reg} \longrightarrow \mathbf{P}(1,2,3,4,5)_K$$

is Zariski dense.

Proof. Consider the family $p\colon \mathscr{S} \to \mathbb{A}^{12}_\mathbb{C}$ of cubic surfaces, given by the equation $T_0T_1T_2 = \prod_{i=0}^2 \sum_{j=0}^3 a_{ij}T_j$. Clebsch's fundamental invariants, when applied to this family, define a rational map $\mathrm{Cl}\colon \mathbb{A}^{12}_\mathbb{C} \dashrightarrow \mathbf{P}(1,2,3,4,5)_\mathbb{C}$. We know that Cl is dominant. Indeed, up to isomorphy, every non-singular cubic surface appears as a fiber of the family p [Do, Corollary 9.3.4].

For a cyclic cubic extension L/K, there is the similar family $p^{(L)}\colon \mathscr{S}^{(L)} \to \mathbb{A}^{12}_K$, given by

$$T_0T_1T_2 = \prod_{i=0}^{2} [(a_0 + \sigma_i(z_1)a_1 + \sigma_i(z_2)a_2)T_0 + \cdots + (d_0 + \sigma_i(z_1)d_1 + \sigma_i(z_2)d_2)T_3]\ , \qquad (3)$$

where $(1, z_1, z_2)$ is a K-basis of L and $\sigma_0, \sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$ denote the three elements.

After base extension to $\mathbb{C}$, the family $p^{(L)}$ becomes isomorphic to p. As the property of being dominant may be tested after extension of the base field, we see that the Clebsch invariant map $\mathrm{Cl}^{(L)}\colon \mathbb{A}^{12}_K \dashrightarrow \mathbf{P}(1,2,3,4,5)_K$, associated to the family $p^{(L)}$, is dominant, too.

Now assume that $\mathrm{C}(\mathscr{H\!C}_K) \subset \mathbf{P}(1,2,3,4,5)_K$ were not Zariski dense. Then, even more, the image under $\mathrm{Cl}^{(L)}$ of the counterexamples to the Hasse principle, contained in the family $p^{(L)}$, has to be contained in a proper closed subset $V \subset \mathbf{P}(1,2,3,4,5)_K$. Since $\mathrm{Cl}^{(L)}$ is dominant, this implies that $(\mathrm{Cl}^{(L)})^{-1}(V)$ is a proper closed subset of $\mathbb{A}^{12}_K$.

In other words, there exists a non-zero polynomial $f \in K[A_j, \ldots, D_j]_{j=0,1,2}$ of a certain degree d such that, for every counterexample to the Hasse principle of the form (2) with $a = a_0 + a_1z_1 + a_2z_2, \ \ldots, \ d = d_0 + d_1z_1 + d_2z_2 \in \mathscr{O}_L$, one has

$$f(a_0, a_1, a_2, b_0, b_1, b_2, c_0, c_1, c_2, d_0, d_1, d_2) = 0\,.$$

Without restriction, assume that the coefficients of f are algebraic integers.

We will show that this is in contradiction with our results above. For this, let us choose a particular field L that it is ramified at at least one prime, but unramified at all primes lying above 3. Such a choice is possible due to Lemma 5.10.

Further, take a prime ideal $\mathfrak{l} \subset \mathscr{O}_K$ that does not divide all the coefficients of f, guarantees $\mathscr{O}_L \otimes_{\mathscr{O}_K} \mathscr{O}_{K_\mathfrak{l}} = \langle 1, z_1, z_2 \rangle_{\mathscr{O}_{K_\mathfrak{l}}}$, splits in L, and is large enough to ensure $(\ell - 1)^{12} > d\ell^{11}$ for $\ell := \#\mathscr{O}_K/\mathfrak{l}$. The existence is of such a prime follows from the decomposition law together with the Cebotarev density theorem.

By Corollary 5.5, we know that there are counterexamples to the Hasse principle of the form (2), with $a, b, c, d \in \mathscr{O}_L$ and $(a \bmod \mathfrak{l}\mathscr{O}_L), \dots, (d \bmod \mathfrak{l}\mathscr{O}_L) \in (\mathscr{O}_L/\mathfrak{l}\mathscr{O}_L)^*$ arbitrary. Consequently,

$$f(a_0, a_1, a_2, b_0, b_1, b_2, c_0, c_1, c_2, d_0, d_1, d_2) \equiv 0 \pmod{\mathfrak{l}},$$

whenever $a_0 + a_1 z + a_2 z^2, \dots, d_0 + d_1 z + d_2 z^2 \in \mathscr{O}_L$ are invertible modulo $\mathfrak{l}\mathscr{O}_L$. This shows that $(f \bmod \mathfrak{l})$ vanishes on at least $(\ell-1)^{12}$ vectors in $\mathbb{F}_\ell^{12}$, a contradiction to the lemma below. □

5.9. Lemma. — *Let ℓ be a prime power and $f \in \mathbb{F}_\ell[X_1, \dots, X_n]$ a non-zero polynomial of degree d.*

Then the number $N(\ell)$ of solutions of $f(x_1, \dots, x_n) = 0$ in $\mathbb{F}_\ell^n$ satisfies the inequality $N(\ell) \leq d\ell^{n-1}$.

Proof. For $\mathbb{F}_\ell$ the prime field, this is the lemma in [BS, Chapter 1, Paragraph 5.2]. For the general case, the argument given there works equally well. □

5.10. Lemma. — *Let K be a number field. Then there exists a cyclic cubic extension L/K that is ramified at at least one prime of K, but unramified at all primes above* 3.

Proof. Probably the easiest way to see this is as follows. Let $p \equiv 1 \pmod 3$ be a prime number such that $K/\mathbb{Q}$ is unramified at p. Choose F to be the unique cubic subfield of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Then $KF/\mathbb{Q}$ is ramified at p, which shows that $L := KF \neq K$. This immediately implies $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. By construction. L/K is unramified at all primes above 3. Further, it must be ramified at some of the primes of K lying above p. □

5.11. Remark (Variants)**.** — The family constructed in Theorem 5.1 turned out to be sufficient to prove the main result, but it is certainly not unique in this respect. At least the following modifications are possible.

i) One may allow that (d) contains some of the ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ twice instead of once.

ii) The congruence conditions required modulo the primes $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ could be weakened. In fact, the choice of α_i in Theorem 5.1 actually determines whether the local invariant $(T_j/T_i, L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i})$ is $\frac{1}{3}$, $\frac{2}{3}$, or 0. One has to combine the conditions at the r ramified primes in such a way that the sum is non-zero in $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$.

A Other reduction types

A.1. —— One might ask for counterexamples to the Hasse principle of the form (2), having other reduction types at the ramified primes. We will show that this is impossible, at least for $\mathfrak{p}$ not dividing 3 and as long as we insist on $a, b, c, d \in \mathscr{O}_{L_\mathfrak{P}}$.

A.2. Lemma. —— *Let L be a cyclic cubic extension of the number field K and $\mathfrak{p}$ be a prime of K that is ramified in L/K. Suppose that $q := \#\mathscr{O}_K/\mathfrak{p}$ is not a power of 3 and write $\mathfrak{P}$ for the unique prime of L lying above $\mathfrak{p}$.*
Further, let $a, b, c, d \in L \cap \mathscr{O}_{L_\mathfrak{P}}$ and S be the cubic surface, given by (2). Assume that, for every $(t_0 : t_1 : t_2 : t_3) \in S(K_\mathfrak{p})$, the quotients t_1/t_0, t_2/t_1, t_0/t_2, as soon as they are properly defined in $K_\mathfrak{p}^*$, are local norms.
Then $d \equiv 0 \pmod{\mathfrak{P}}$ and $27abc \equiv 1 \pmod{\mathfrak{P}}$.

Proof. The assumption implies $q \equiv 1 \pmod 3$. Further, the reduction $S_{\mathbb{F}_q}$ of the cubic surface S at a ramified prime is given by

$$T_0T_1T_2 = (\overline{a}T_0 + \overline{b}T_1 + \overline{c}T_2 + \overline{d}T_3)^3 .$$

It suffices to show that there are non-singular $\mathbb{F}_q$-rational points on $S_{\mathbb{F}_q}$ such that the quotients are non-cubes, except in the asserted situation. There are three cases.
First case. $\overline{d} \neq 0$.
Then, after a change of coordinates that does not involve T_0 and T_1, $S_{\mathbb{F}_q}$ is the cubic surface, given by $T_0T_1T_2 = T_3^3$. It is obvious that there are non-singular points such that t_1/t_0 is a non-cube.
Second case. $\overline{d} = 0$, $\overline{a}, \overline{b}, \overline{c} \neq 0$.
After changing coordinates, $S_{\mathbb{F}_q}$ is $T_0T_1T_2 = A(T_0 + T_1 + T_2)^3$ for $A = \overline{abc}$. Assume $A \neq \frac{1}{27}$, as this is the claimed exception.

Then $S_{\mathbb{F}_q}$ is the cone over a non-singular curve C of genus one. The triple cover $T^3 = T_1/T_0$ is unramified and defines another curve $\widetilde{C}$ of genus one. The assumption that t_1/t_0 is always a cube leads to $\#\widetilde{C}(\mathbb{F}_q) = 3 \cdot \#C(\mathbb{F}_q)$, which contradicts Hasse's bound for $q \geq 16$.

Finally, a systematic test shows that, for $q = 4, 7, 13$ and $A \neq 0, \frac{1}{27} \in \mathbb{F}_q$, it does never happen that all the quotients are cubes.
Third case. $\overline{d} = 0$ and at least one of $\overline{a}, \overline{b}, \overline{c}$ is zero.
Without restriction, assume $\overline{c} = 0$. Then the equation of $S_{\mathbb{F}_q}$ simplifies to $T_0T_1T_2 = (\overline{a}T_0 + \overline{b}T_1)^3$. Considering the partial derivative by T_2, we see that, independently of what $\overline{a}$ and $\overline{b}$ are, every point such that $t_0t_1 \neq 0$ is non-singular. We may choose $t_0, t_1 \in \mathbb{F}_q^*$ arbitrarily and find a point just by calculating t_2. □

B A geometric lemma

B.1. Lemma. —— *The cubic surfaces having at least three Eckardt points are contained in a two-dimensional closed subset of the moduli scheme of non-singular cubic surfaces.*

Proof. This follows rather directly from the investigations undertaken by E. Dardanelli and B. van Geemen in [DG]. A cubic surface over an algebraically closed base field may either allow a pentahedral form

$$a_0T_0^3 + \ldots + a_4T_4^3 = 0, \qquad T_0 + \ldots + T_4 = 0$$

or not.

In the first case, in order to have three Eckardt points, three of the five coefficients have to be equal to each other [DG, 2.2]. In particular, the corresponding surfaces are contained in a two-dimensional subset of the moduli scheme.

Otherwise, the surface might be cyclic, ns1 or ns2 [DG, 5.1–5.3]. Cyclic surfaces form a one-dimensional subset, while ns2 surfaces form a two-dimensional subset in the moduli scheme [DG, Theorem 6.6]. Finally, the ns1 surfaces with at least three Eckardt points may be parametrized by a two-dimensional family [DG, Proposition 5.7.(4) and (5)]. □

References

[BS] Borevich, Z. I. and Shafarevich, I. R.: *Number theory*, Academic Press, New York-London 1966

[CG] Cassels, J. W. S. and Guy, M. J. T.: *On the Hasse principle for cubic surfaces,* Mathematika **13** (1966), 111–120

[Cl] Clebsch, A.: *Ueber eine Transformation der homogenen Functionen dritter Ordnung mit vier Veränderlichen,* J. für die reine und angew. Math. **58** (1861), 109–126

[CTKS] Colliot-Thélène, J.-L., Kanevsky, D., and Sansuc, J.-J.: *Arithmétique des surfaces cubiques diagonales,* in: Diophantine approximation and transcendence theory (Bonn 1985), Lecture Notes in Math. 1290, Springer, Berlin 1987, 1–108

[CTS] Colliot-Thélène, J.-L. and Sansuc, J.-J.: *On the Chow groups of certain rational surfaces: A sequel to a paper of S. Bloch,* Duke Math. J. **48** (1981), 421–447

[EJ1] Elsenhans, A.-S. and Jahnel, J.: *Cubic surfaces with a Galois invariant pair of Steiner trihedra,* International Journal of Number Theory **7** (2011), 947–970

[EJ2] Elsenhans, A.-S. and Jahnel, J.: *On the order three Brauer classes for cubic surfaces,* Central European Journal of Mathematics **10** (2012), 903–926

[DG] Dardanelli, E. and van Geemen, B.: *Hessians and the moduli space of cubic surfaces,* in: Algebraic geometry, Contemp. Math. 422, AMS, Providence 2007, 17–36

[Do] Dolgachev, I. V.: *Classical algebraic geometry. A modern view,* Cambridge University Press, Cambridge 2012

[J] Jahnel, J.: *More cubic surfaces violating the Hasse principle,* Journal de Théorie des Nombres de Bordeaux **23** (2011), 471–477

[Ma] Manin, Yu. I.: *Cubic forms, algebra, geometry, arithmetic,* North-Holland Publishing Co. and American Elsevier Publishing Co., Amsterdam-London and New York 1974

[Mo] Mordell, L. J.: *On the conjecture for the rational points on a cubic surface,* J. London Math. Soc. **40** (1965), 149–158

[Ne] Neukirch, J.: *Algebraic number theory,* Grundlehren der Mathematischen Wissenschaften 322, Springer, Berlin 1999

[Sch] Schläfli, L.: *An attempt to determine the twenty-seven lines upon a surface of the third order, and to divide such surfaces into species in reference to the reality of the lines upon the surface,* Quart. J. Math. **2** (1858), 110–120

[Sk] Skolem, Th.: *Einige Bemerkungen über die Auffindung der rationalen Punkte auf gewissen algebraischen Gebilden,* Math. Z. **63** (1955), 295–312

[SD] Swinnerton-Dyer, Sir Peter: *Two special cubic surfaces,* Mathematika **9** (1962), 54–56

[Ta] Tate, J.: *Global class field theory,* in: Algebraic number theory, Edited by J. W. S. Cassels and A. Fröhlich, Academic Press and Thompson Book Co., London and Washington 1967, 162–203

[We] Weil, A.: *Abstract versus classical algebraic geometry,* in: Proc. Int. Cong. of Mathematicians, Amsterdam 1954, vol. III, Erven P. Noordhoff N.V. and North-Holland Publishing Co., Groningen and Amsterdam 1956, 550–558