BRAUER-MANIN OBSTRUCTION FOR MARKOFF SURFACES

J.-L. COLLIOT-THÉLÈNE, DASHENG WEI, AND FEI XU

Abstract. Ghosh and Sarnak have studied integral points on surfaces defined by an equation $x^2 + y^2 + z^2 - xyz = m$ over the integers. For these affine surfaces, we systematically study the Brauer group and the Brauer-Manin obstruction to the integral Hasse principle. We prove that strong approximation for integral points on any such surface, away from any finite set of places, fails, and that, for $m \neq 0, 4$, the Brauer group does not control strong approximation.

1. Introduction

Fix $m \in \mathbb{Z}$. Let $\mathcal{U}_m \subset \mathbb{A}^3_{\mathbb{Z}}$ be the affine scheme over $\mathbb{Z}$ defined by the equation

$$x^2 + y^2 + z^2 - xyz = m.$$

The surface $U_m = \mathcal{U}_m \times_{\mathbb{Z}} \mathbb{Q}$ over $\mathbb{Q}$ is called a Markoff surface.

In [12], A. Ghosh and P. Sarnak study the set $\mathcal{U}_m(\mathbb{Z})$ of integral solutions of such equations. A key tool is the action of the automorphism group Γ generated by the following three types of elements

(a) the Vieta involution: $(x, y, z) \mapsto (yz - x, y, z)$.

(b) the sign change: $(x, y, z) \mapsto (-x, -y, z)$.

(c) the permutations of x, y, z.

Here are some of the main results from [12].

The integer $m - 4$ plays an important rôle. Once and for all we set $d := m - 4$. We assume $m \neq 0$ and $d \neq 0$. These are the conditions for the $\mathbb{Q}$-surface U_m to be smooth.

We denote $\mathcal{U}_m(A_{\mathbb{Z}}) = \prod_p \mathcal{U}_m(\mathbb{Z}_p)$, where p runs through all primes and ∞, and $\mathbb{Z}_\infty = \mathbb{R}$. We let

$$\mathcal{U}_m(A_{\mathbb{Z}})_{\bullet} = \prod_{p<\infty} \mathcal{U}_m(\mathbb{Z}_p) \times \pi_0(U_m(\mathbb{R}))$$

where $\pi_0(U_m(\mathbb{R}))$ is the set of connected components of $U_m(\mathbb{R})$. This is called the (reduced) Brauer-Manin set of $\mathcal{U}_m$.

(0) $\mathcal{U}_m(A_{\mathbb{Z}}) = \emptyset$ if and only if $m \equiv 3 \bmod 4$ or $m \equiv \pm 3 \bmod 9$. Other values of m are called "admissible".

(1) For m admissible and "generic" ([12, p. 3], see Proposition 6.1 below), following Markoff, Hurwitz, Mordell, they develop a reduction theory : there exists a bounded fundamental domain in $\mathbb{R}^3$ for integral solutions. In particular the set $\mathcal{U}_m(\mathbb{Z})/\Gamma$ is finite.

Date: 13 September 2018; revised, December 7th, 2018.

2010 *Mathematics Subject Classification.* 11G35 (11D25, 14F22).

Key words and phrases. Brauer group, Brauer-Manin obstruction, strong approximation, Markoff surface.

(2) Suppose that $m \neq 2$ and that m is not a square. Then $\mathcal{U}_m(\mathbb{Z})$ is Zariski dense in $\mathcal{U}_m$ if and only if $\mathcal{U}_m(\mathbb{Z})$ is not empty [12, (1.5)]. Zariski density still holds if m is a square and contains an odd prime factor congruent to 1 modulo 4 [12, final comment in §5.2.1].

(3) Strong approximation need not hold, i.e. $\mathcal{U}_m(\mathbb{Z})$ need not be dense in $\mathcal{U}_m(A_{\mathbb{Z}})_\bullet$ (see [12, p. 21]). This uses the quadratic reciprocity law.

(4) There are infinitely many m's such that $\mathcal{U}_m$ does not satisfy the integral Hasse principle. The examples in [12] are all of the shape $d = r.v^2$, with $r = \pm 2$, $r = 12$, $r = 20$, and specific properties for the primes dividing v. The arguments use quadratic reciprocity. They are in the same spirit as earlier examples [6, 7] accounted for by the integral Brauer-Manin obstruction. From a historical point of view, it is interesting to note that examples very close to those of [12] are already given in Mordell's 1953 paper [17, §3].

(5) For "generic values" of m, reduction theory leads to examples where $\mathcal{U}_m(A_{\mathbb{Z}}) \neq \emptyset$ but $\mathcal{U}_m(\mathbb{Z}) = \emptyset$. On the basis of intensive numerical experiment, Ghosh and Sarnak suggest that there are many such examples that cannot be explained by a reciprocity argument, i.e. for which, in our language, $\mathcal{U}_m(A_{\mathbb{Z}})_\bullet^{\mathrm{Br}} \neq \emptyset$. More precisely they predict a count for the set of m's with local solutions and no global solution which is much higher than what their families of counterexamples produce.

The cubic surface $t(x^2 + y^2 + z^2) - xyz = mt^3$ over $\mathbb{Q}$ is smooth as soon as $m \neq 0, 4$. The surface $U = \mathcal{U} \otimes_{\mathbb{Z}} \mathbb{Q}$ is the complement in X of the hyperplane section H defined by plane section $t = 0$. Its geometric fundamental group is trivial (Prop. 4.1). Thus U, or rather the pair (X, H), is in a strong sense a log K3 surface [13, Definition 2.4].

The search for integral points on $\mathcal{U}$ bears some analogy with the search for rational points on smooth, projective $K3$-surfaces W. For this latter situation, Skorobogatov has put forward the conjecture : The closure of the set $W(\mathbb{Q})$ in the adelic set $W(A_{\mathbb{Q}})_\bullet$ is just the Brauer-Manin set $W(A_{\mathbb{Q}})_\bullet^{\mathrm{Br}}$. One may wonder whether there is a similar result for integral points on log K3 surfaces U. Here some restriction must be made. It may indeed happen that the set $\mathcal{U}(\mathbb{Z})$ is not empty but not Zariski dense in U (Harpaz [13, Theorem 1.4]; Jahnel and Schindler [11, Theorem 2.6]).

Here are some questions raised by the paper of Ghosh and Sarnak.

(A) A first problem is to check that all counterexamples in [12] are of Brauer-Manin type, and to search for as many families of counterexamples as possible.

This problem is best handled by solving problems (B) and (C) :

(B) For arbitrary m, can one determine $\mathrm{Br}(U_m)/\mathrm{Br}(\mathbb{Q})$? Is this quotient finite ?

(C) For arbitrary m, can one determine $\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}}$?

(D) When (how often) is the closure of $\mathcal{U}_m(\mathbb{Z})$ equal to the Brauer-Manin set $\mathcal{U}_m(A_{\mathbb{Z}})_\bullet^{\mathrm{Br}}$, which is the subset of $\mathcal{U}_m(A_{\mathbb{Z}})_\bullet$ orthogonal to $\mathrm{Br}(U_m)$ under the Brauer-Manin pairing

$$\mathcal{U}_m(A_{\mathbb{Z}})_\bullet \times \mathrm{Br}(U_m) \to \mathbb{Q}/\mathbb{Z}.$$

Here are the main results of this paper.

(a) We solve Problem (A), i.e. we check that the counterexamples to the integral Hasse principle based on the quadratic reciprocity law in [12] are of Brauer-Manin type, and we produce more families of counterexamples of the same kind.

(b) We solve Problem (B) for all values of m. This in principle solves Problem (C).

(c) Over an arbitrary ground field, we give generators for the algebraic part of the Brauer group of U, and we systematically study the "transcendental part" of the Brauer group of U.

(d) We get a satisfactory answer to Problem (D). More precisely, we prove (see Theorem 6.2):

Theorem 1.1. *Let $m \in \mathbb{Z}$ be any integer. Suppose $\mathcal{U}_m(A_{\mathbb{Z}}) \neq \emptyset$. For any finite set S of primes the image of the natural map $\mathcal{U}_m(\mathbb{Z}) \to \prod_{p \notin S} \mathcal{U}_m(\mathbb{Z}_p)$ is not dense.*

The proof of this theorem does not involve the Brauer group, it only uses reduction theory. It should be compared with the statement at the bottom of page 2 of [12], with reference to [3], that if $d = m - 4 > 0$ is a square, then $\mathcal{U}_m$ "satisfies a form of strong approximation". See Remark 6.4 below.

As a corollary, one gets (see Corollary 6.6)

Corollary 1.2. *Suppose $m \neq 0, 4$ and $\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}}_{\bullet} \neq \emptyset$. Then $\mathcal{U}_m(\mathbb{Z})$ is not dense in $\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}}_{\bullet}$.*

Since there are infinitely many $m \neq 0, 4$ such that $\mathcal{U}_m(\mathbb{Z})$ is Zariski dense in $\mathcal{U}_m$ by [12, §5.2], we obtain infinitely many log K3 surfaces where integral points are Zariski dense but are not dense in the integral Brauer-Manin sets (see Corollary 6.7).

Such a behaviour had not been yet observed, even in the context of rational points. If one allows discussion of density in the real locus, one may only compare this with the examples of smooth projective surfaces $X/\mathbb{Q}$ with the property that the closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ does not coincide with a union of connected components of the real locus $X(\mathbb{R})$ [5, §5].

This work was started in Beijing in November 2017. In a recent preprint, D. Loughran and V. Mitankin [15] have made an independent study.

With the restrictions m, d, md not squares, [15] independently solves problem (B). [15] also solves Problem (A) and produces some more types of counterexamples. and a lower count for the m's giving rise to such counterexamples. Our stock of counterexamples enables us to produce a slightly better lower count than [15, Theorem 1.4].

With the same restriction that m, d, md are not squares, towards Problem (C), Loughran and Mitankin establish the beautiful result that the only possible examples with $\mathcal{U}_m(A_{\mathbb{Z}}) \neq \emptyset$ and $\mathcal{U}_m(A_{\mathbb{Z}})^{Br} = \emptyset$ satisfy that the class of $d = m - 4$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ lies in the subgroup spanned by $\pm 1, 2, 3, 5$. This finiteness result, which is in the spirit of the finiteness of exceptional spinor classes in the study of the representation of an integer by a ternary quadratic form (see [6, Remark 7.11]), explains why the examples in [12] based on the quadratic reciprocity law were of a rather special type. It is used in [15] to show that there are indeed far less values of m with Brauer-Manin counterexamples than the number of values of m predicted by [12] for counterexamples to the integral Hasse principle.

Notation Let k be a field and $\overline{k}$ a separable closure of k. We let $g = g_k = \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group. A k-variety is a separated k-scheme of finite type. If X is a k-variety, we write $\overline{X} = X \times_k \overline{k}$. We let $k[X] = H^0(X, O_X)$ and $\overline{k}[X] = H^0(\overline{X}, O_{\overline{X}})$. If X is an integral k-variety, we let $k(X)$ denote the function field of X. If X is a geometrically integral k-variety, we let $\overline{k}(X)$ denote the function field of $\overline{X}$. We let $\mathrm{Pic}(W) = H^1_{Zar}(W, \mathbb{G}_m) = H^1_{\text{ét}}(W, \mathbb{G}_m)$ denote the Picard group of a scheme W. We let $\mathrm{Br}(W) = H^2_{\text{ét}}(W, \mathbb{G}_m)$ denote the Brauer group of a scheme W. If W is a smooth integral k-variety, the natural map $\mathrm{Br}(W) \to \mathrm{Br}(k(W))$ is injective, and for torsion prime to the characteristic, it identifies $\mathrm{Br}(W)$ with the group of elements of $\mathrm{Br}(k(W))$ whose residues at all codimension 1 points of W vanish. We let

$$\mathrm{Br}_1(X) = \mathrm{Ker}[\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})]$$

denote the algebraic Brauer group of a k-variety X and we let $\mathrm{Br}_0(X) \subset \mathrm{Br}_1(X)$ denote the image of $\mathrm{Br}(k) \to \mathrm{Br}(X)$. The image of $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})$ is sometimes referred to as the "transcendental Brauer group" of X.

Given a field F of characteristic zero containing a primitive n-th root of unity $\zeta = \zeta_n$, we have $H^2(F, \mu_n^{\otimes 2}) = H^2(F, \mu_n) \otimes \mu_n$. The choice of ζ_n then defines an isomorphism $\mathrm{Br}(F)[n] = H^2(F, \mu_n) \cong H^2(F, \mu_n^{\otimes 2})$. Given two elements $f, g \in F^\times$, they have classes (f) and (g) in $F^\times/F^{\times n} = H^1(F, \mu_n)$. One denotes $(f, g)_\zeta \in \mathrm{Br}(F)[n] = H^2(F, \mu_n)$ the class corresponding to the cup-product $(f) \cup (g) \in H^2(F, \mu_n^{\otimes 2})$. Suppose F/E is a finite Galois extension with Galois group G. Given $\sigma \in G$ and $f, g \in F^\times$, we have $\sigma((f, g)_{\zeta_n}) = (\sigma(f), \sigma(g))_{\sigma(\zeta_n)} \in \mathrm{Br}(F)$. In particular, if $\zeta_n \in E$, then $\sigma((f, g)_{\zeta_n}) = (\sigma(f), \sigma(g))_{\zeta_n}$.

Let R be a discrete valuation ring with field of fractions F and residue field κ. Let v denote the valuation $F^\times \to \mathbb{Z}$. Let $n > 1$ be an integer invertible in R. Assume F contains a primitive n-th root of unity ζ. For $f, g, \in F^*$, we have the residue map

$$\partial_R : H^2(F, \mu_n) \to H^1(\kappa, \mathbb{Z}/n) \cong H^1(\kappa, \mu_n) = \kappa^\times/\kappa^{\times n},$$

where $H^1(\kappa, \mathbb{Z}/n) \cong H^1(\kappa, \mu_n)$ is defined by the choice of ζ. This map sends the class of $(f, g)_\zeta \in \mathrm{Br}(F)[n] = H^2(F, \mu_n)$ to

$$(-1)^{v(f)v(g)} \ \mathrm{class}(g^{v(f)}/f^{v(g)}) \in \kappa^\times/\kappa^{\times n}.$$

Structure of the paper

Let k be a field of characteristic zero. Let $m \in k$. Assume $m(m-4) \neq 0$. Let $X = X_m \subset \mathbb{P}^3_k$ be the smooth cubic surface defined by the projective equation

$$t(x^2 + y^2 + z^2) - xyz = mt^3.$$

Let $U = U_m \subset X_m$ be the smooth affine cubic surface defined by the affine equation

$$x^2 + y^2 + z^2 - xyz = m.$$

In §2, we study the Galois modules $\mathrm{Pic}(\overline{X}), \mathrm{Pic}(\overline{U}), \mathrm{Br}(\overline{U})$. We show $\mathrm{Br}(\overline{U}) \simeq \mathbb{Q}/\mathbb{Z}(-1)$. In §3, we compute $\mathrm{Br}(X) = \mathrm{Br}_1(X)$ and the algebraic part $\mathrm{Br}_1(U)$ of $\mathrm{Br}(U)$. In §4, we compute the transcendental part of $\mathrm{Br}(U)$, namely the quotient $\mathrm{Br}(U)/\mathrm{Br}_1(U)$. We then turn to the case $k = \mathbb{Q}$ and m is an integer. In §5, we show how to compute the integral Brauer-Manin obstruction for the affine scheme $\mathcal{U}_m$ over $\mathbb{Z}$ defined by $x^2 + y^2 + z^2 - xyz = m$. We then show that the counterexamples to the integral Hasse principle for $\mathcal{U}_m$ in [12] may all be explained by a combination of integral Brauer-Manin obstruction and reduction theory. We increase the stock of such counterexamples, thus leading to an improvement on a counting result in [15]. In

§6, we prove that strong approximation never holds for Markoff type surfaces. Section §7 is an appendix giving the structure of the real locus $U_m(\mathbb{R})$ depending on the value of $m \in \mathbb{R}$.

2. Computation of Brauer groups I, general setting

Proposition 2.1. *Let X be a smooth, projective, geometrically rational surface over a field k of characteristic zero. Suppose that U is an open subset of X such that $X \setminus U$ is the union of three distinct k-lines, by which we mean a smooth projective curve isomorphic to $\mathbf{P}^1_k$. Suppose three lines intersect each other transversely with three distinct intersection points. Let L be one of the three lines and $V \subset L$ be the complement of the 2 intersection points of L with the other two lines. Then the residue map*

$$\partial_L : \ \mathrm{Br}(\bar{k}(X)) \to H^1(\bar{k}(L), \mathbb{Q}/\mathbb{Z})$$

induces a g-isomorphism

$$\mathrm{Br}(\overline{U}) \xrightarrow{\cong} H^1(\overline{V}, \mathbb{Q}/\mathbb{Z}) \simeq H^1(\overline{\mathbb{G}}_m, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}(-1).$$

Proof. Since X is smooth, the homology of the Bloch-Ogus complex

$$H^2(\bar{k}(X), \mathbb{Q}/\mathbb{Z}(1)) \to \oplus_{x\in\overline{X}^{(1)}} H^1(\bar{k}(x), \mathbb{Q}/\mathbb{Z}) \to \oplus_{x\in\overline{X}^{(2)}} H^0(\bar{k}(x), \mathbb{Q}/\mathbb{Z}(-1))$$

at the second term is $H^1_{Zar}(\overline{X}, \mathcal{H}^2_{\overline{X}}(\mathbb{Q}/\mathbb{Z}(1)))$ by [2, (6.1) Theorem]. The spectral sequence

$$E_2^{p,q} = H^p_{Zar}(\overline{X}, \mathcal{H}^q_{\overline{X}}(\mathbb{Q}/\mathbb{Z}(1))) \Rightarrow H^{p+q}_{\text{ét}}(\overline{X}, \mathbb{Q}/\mathbb{Z}(1))$$

in [2, (6.3) Corollary] implies that $H^1_{Zar}(\overline{X}, \mathcal{H}^2_X(\mathbb{Q}/\mathbb{Z}(1)))$ is a subgroup of $H^3_{\text{ét}}(\overline{X}, \mathbb{Q}/\mathbb{Z}(1))$. Since

$$H^1_{\text{ét}}(\overline{X}, \mu_n) = \mathrm{Pic}(\overline{X})[n] = 0$$

for all $n > 0$ by the Kummer sequence, one has

$$H^3_{\text{ét}}(\overline{X}, \mathbb{Q}/\mathbb{Z}(1)) = \varinjlim_n H^3_{\text{ét}}(\overline{X}, \mu_n) = 0$$

by Poincaré duality. Therefore the above Bloch-Ogus complex is exact.

Since X is a smooth, projective, geometrically rational surface, $\mathrm{Br}(\overline{X}) = 0$ and the following diagram of exact sequences

$$\begin{array}{ccccccc} & & \mathrm{Br}(\overline{X}) = 0 & \longrightarrow & H^2(\bar{k}(X), \mathbb{Q}/\mathbb{Z}(1)) & \longrightarrow & \oplus_{x\in\overline{X}^{(1)}} H^1(\bar{k}(x), \mathbb{Q}/\mathbb{Z}) \\ & & & & \simeq\downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Br}(\overline{U}) & \longrightarrow & H^2(\bar{k}(U), \mathbb{Q}/\mathbb{Z}(1)) & \longrightarrow & \oplus_{x\in\overline{U}^{(1)}} H^1(\bar{k}(x), \mathbb{Q}/\mathbb{Z}) \end{array}$$

commutes by [4, (3.9)]. Let $\{L_1, L_2, L_3\}$ be the set of three lines in $X \setminus U$ and let $\{P_1, P_2, P_3\}$ be the set of three intersection points of L_1, L_2 and L_3 such that $P_i \notin L_i$ for $1 \leq i \leq 3$. Set

$$V_i = L_i \setminus \{P_j\}_{j\neq i} \simeq_k \mathbb{G}_m$$

for $1 \leq i \leq 3$. Combining the above diagram with the above Bloch-Ogus exact sequence yields the following exact sequence, where the maps are given by the residues

$$0 \to \mathrm{Br}(\overline{U}) \to \oplus_{i=1}^{3} H^1_{\text{ét}}(\overline{V}_i, \mathbb{Q}/\mathbb{Z}) \to \oplus_{i=1}^{3} H^0(\bar{k}(P_i), \mathbb{Q}/\mathbb{Z}(-1)).$$

For $1 \leq i \leq 3$, the residue map induces the following short exact sequence

$$0 \to H^1_{\text{ét}}(\overline{V}_i, \mathbb{Q}/\mathbb{Z}) \to \oplus_{j\neq i} H^0_{\text{ét}}(\bar{k}(P_j), \mathbb{Q}/\mathbb{Z}(-1)) \xrightarrow{\sum_{j\neq i}} \mathbb{Q}/\mathbb{Z} \to 0$$

(this uses $V_i \simeq \mathbb{G}_m$). One thus has g-isomorphisms

$$\mathrm{Br}(\overline{U}) \simeq H^1_{\text{ét}}(\overline{V}_i, \mathbb{Q}/\mathbb{Z}) \simeq H^1(\overline{\mathbb{G}}_m, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}(-1)$$

for $1 \leq i \leq 3$. □

For cubic surfaces over an algebraically closed field k, one has the following result.

Proposition 2.2. *Let $X \subset \mathbf{P}^3_k$ is a smooth, projective, cubic surface over a field k of characteristic zero. Suppose a plane $\mathbf{P}^2_k \subset \mathbf{P}^3_k$ cuts out on $\bar{X}$ three lines L_1, L_2, L_3 over $\bar{k}$. Let $U \subset X$ be the complement of this plane. Then the natural map $\bar{k}^\times \to \bar{k}[U]^\times$ is an isomorphism of Galois modules and the natural map*

$$0 \to \oplus_{i=1}^{3} \mathbb{Z}L_i \to \mathrm{Pic}(\bar{X}) \to \mathrm{Pic}(\bar{U}) \to 0$$

is an exact sequence of Galois lattices.

Proof. We may assume $k = \bar{k}$. Let

$$aL_1 + bL_2 + cL_3 = 0 \in \mathrm{Pic}(X)$$

with $a, b, c \in \mathbb{Z}$. By the assumption that $(L_i.L_i) = -1$ and $(L_i.L_j) = 1$ for $i \neq j$, one has

$$-a + b + c = 0, \quad a - b + c = 0, \quad a + b - c = 0.$$

This implies that $a = b = c = 0$.

To complete the proof, one only needs to show that $\mathrm{Pic}(U)$ is torsionfree.

Let $e_1, e_2, \cdots, e_6$ and l be given by [10, Chapter V, Proposition 4.8].

Suppose that one of L_1, L_2 and L_3 is in $\{e_1, \cdots, e_6\}$. Say that $L_1 = e_1$. Then L_2 and L_3 are exactly in one of the following sets

$$\{l - e_1 - e_i : \ 2 \leq i \leq 6\} \quad \text{and} \quad \{2l - \sum_{k\neq i} e_k : \ 2 \leq i \leq 6\}$$

by inspecting the intersection property of L_1, L_2, L_3. Without loss of generality, one can assume that $L_2 = l - e_1 - e_2$. Then

$$L_3 = 2l - \sum_{k\neq 2} e_k.$$

By [10, Chapter V, Proposition 4.8], one concludes that $\mathrm{Pic}(X)/(\oplus_{i=1}^{3}\mathbb{Z}L_i)$ is free.

Otherwise, all L_1, L_2 and L_3 are in $\{l - e_i - e_j : \ 1 \leq i < j \leq 6\}$. Say

$$L_1 = l - e_1 - e_2, \quad L_2 = l - e_3 - e_4 \ \text{ and } \ L = l - e_5 - e_6.$$

Then $\mathrm{Pic}(X)/(\oplus_{i=1}^{3}\mathbb{Z}L_i)$ is free by [10, Chapter V, Proposition 4.8].

Alternative completion of the proof The first argument shows that L_1, L_2, L_3 are linearly independent. It also shows that $k^\times = k[U]^\times$. Since the determinant of the system of equations is ± 4, and $\mathrm{Pic}(X)$ is torsionfree, the only torsion that could exist in $\mathrm{Pic}(U)$ is 2-primary. Let us show there is no 2-torsion in $\mathrm{Pic}(U)$. If there was, there would exist a principal divisor on X of the shape $2D + L_1$, or $2D + L_1 + L_2$, or $2D + L_1 + L_2 + L_3$. Intersecting with a hyperplane already rules out $2D + L_1$ and $2D + L_1 + L_2 + L_3$. By the well known configuration of the 27 lines on a cubic surface, there exists a line L on X which meets L_1 in one point and does not meet L_2 or L_3. Intersection with L rules out the three possibilities. □

The following corollary applies to number fields and more generally to function fields of varieties over a number field.

Corollary 2.3. *Let k be a field of characteristic zero such that in any finite field extension there are only finitely many roots of unity. Let $X \subset \mathbf{P}^3_k$ is a smooth, projective, cubic surface over k. Suppose a plane cuts out on X three nonconcurrent lines. Let $U \subset X$ be the complement of the plane section. Then the quotient $\mathrm{Br}(U)/\mathrm{Br}_0(U)$ is finite.*

Proof. Let $g = \mathrm{Gal}(\overline{k}/k)$ where $\overline{k}$ is an algebraic closure of k. Since $\overline{k}^* = \overline{k}[U]^*$, we have an exact sequence

$$\mathrm{Br}(k) \to \mathrm{Ker}[\mathrm{Br}(U) \to \mathrm{Br}(\overline{U})^g] \to H^1(g, \mathrm{Pic}(\overline{U}))$$

by [6, Lemma 2.1]. Since $\mathrm{Pic}(\overline{U})$ is free of finite rank by Proposition 2.2, $H^1(g, \mathrm{Pic}(\overline{U}))$ is finite.

Let $K \subset \overline{k}$ be a field over which one of the three lines, call it L, is defined. Let $g_K = \mathrm{Gal}(\overline{k}/K)$. The isomorphism

$$\mathrm{Br}(\overline{U}) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}(-1)$$

attached to the line L is g_K-equivariant. We thus have

$$\mathrm{Br}(\overline{U})^g \subset \mathrm{Br}(\overline{U})^{g_K} \simeq \mathbb{Q}/\mathbb{Z}(-1)^{g_K}$$

Since there are finitely many roots of unity in K, the group $\mathbb{Q}/\mathbb{Z}(-1)^{g_K}$ is finite (use Lemma 2.4). Thus $\mathrm{Br}(\overline{U})^g$ is finite. The result now follows from the above exact sequence. □

Lemma 2.4. *Let k be a field of characteristic 0. Let $g = \mathrm{Gal}(\overline{k}/k)$. Let $\mu_\infty(\overline{k}) = \mathbb{Q}/\mathbb{Z}(1)$ be the subgroup of roots of unity in $\overline{k}^\times$. Then $\mathbb{Q}/\mathbb{Z}(-1)^g$ is (noncanonically) isomorphic to $\mu_\infty(k)$, the group of roots of unity in k.*

Proof. We only need to show: $\mathbb{Z}/n \subset \mathbb{Q}/\mathbb{Z}(-1)^g$ holds if and only if $\mu_n \subset k$.

If $\mu_n \subset k$, obviously $\mathbb{Z}/n \subset \mathbb{Q}/\mathbb{Z}(-1)^g$. On the other hand, let $a \in \mathbb{Q}/\mathbb{Z}(-1)$ be of order n. For any $\sigma \in g$, then $\sigma(a) = \chi(\sigma)^{-1}a$, here χ is the cyclotomic character. Therefore, if a is a fixed point, then $(\chi(\sigma) - 1)a = 0$ for any $\sigma \in g$, i.e., $\chi(\sigma) - 1 \equiv 0 \bmod n$, it implies $\mu_n \subset k$. □

3. Computation of Brauer groups II, algebraic parts

For Markoff surfaces, one can further compute the algebraic part of Brauer groups explicitly by using the equations.

Lemma 3.1. *Let k be a field of characteristic zero and $\overline{k}$ an algebraic closure of k. Let $m \in k$ and $d = m-4$. Let $X \subset \mathbb{P}^3_k$ be defined by the equation*

$$t(x^2+y^2+z^2) - xyz = mt^3.$$

Then X is smooth over k if and only if $md \neq 0$. If $md \neq 0$, fix a square root $\sqrt{m} \in \overline{k}$ and a square root $\sqrt{d} \in \overline{k}$. Then the 27 lines on $\overline{X}$ are defined over $k(\sqrt{m}, \sqrt{d})$ by the following equations

$$L_1: \ x = t = 0; \qquad L_2: \ y = t = 0; \qquad L_3: \ z = t = 0$$

and

$$\begin{cases} l_1(\epsilon,\delta): \ x = 2\epsilon t, \ y - \epsilon z = \delta\sqrt{d}t \\ l_2(\epsilon,\delta): \ y = 2\epsilon t, \ z - \epsilon x = \delta\sqrt{d}t \\ l_3(\epsilon,\delta): \ z = 2\epsilon t, \ x - \epsilon y = \delta\sqrt{d}t \\ l_4(\epsilon,\delta): \ x = \epsilon\sqrt{m}t, \ y = \frac{1}{2}(\epsilon\sqrt{m} + \delta\sqrt{d})z \\ l_5(\epsilon,\delta): \ y = \epsilon\sqrt{m}t, \ z = \frac{1}{2}(\epsilon\sqrt{m} + \delta\sqrt{d})x \\ l_6(\epsilon,\delta): \ z = \epsilon\sqrt{m}t, \ x = \frac{1}{2}(\epsilon\sqrt{m} + \delta\sqrt{d})y \end{cases}$$

with $\epsilon = \pm 1$ and $\delta = \pm 1$. Moreover, the intersection number

$$(l_i(\epsilon,\delta).l_j(\epsilon,\delta)) = 0$$

for any fixed pair (ϵ, δ), whenever $1 \leq i \neq j \leq 6$.

Proof. For $m = 4$, the singular points are

$$(x:y:z:t) = (2\varepsilon : 2\eta : 2\varepsilon\eta : 1)$$

with $\varepsilon = \pm 1, \eta = \pm 1$. For $m = 0$, there is only one singular point, namely $(0:0:0:1)$. Assume $m \neq 0, 4$. Any line L on X which is not in the plane $t = 0$ meets this plane in one point, and that point must be on one of the lines L_1, L_2, L_3. Say it is L_1. The plane containing L and L_1 is one of the planes through L_1 which intersects X in three lines. Writing down the planes through each L_i with this property (there are 5 such planes for each L_i) produces all lines on X, which are indeed 27 in number. □

Proposition 3.2. *Let k be a field of characteristic zero and $m \in k \setminus \{0,4\}$. Set $d = m-4$. Let $X \subset \mathbb{P}^3_k$ be defined by the equation*

$$t(x^2+y^2+z^2) - xyz = mt^3. \tag{3.1}$$

If $[k(\sqrt{m}, \sqrt{d}) : k] = 4$, then

$$\mathrm{Br}(X)/\mathrm{Br}_0(X) = \mathrm{Br}_1(X)/\mathrm{Br}_0(X) \cong \mathbb{Z}/2$$

with a generator

$$\{((\frac{x}{t})^2 - 4, d) = ((\frac{y}{t})^2 - 4, d) = ((\frac{z}{t})^2 - 4, d)\}$$

over $t \neq 0$.

If $d \notin k^{\times 2}$ and $m \in k^{\times 2}$, then

$$\mathrm{Br}(X)/\mathrm{Br}_0(X) = \mathrm{Br}_1(X)/\mathrm{Br}_0(X) \cong (\mathbb{Z}/2)^2$$

with two generators

$$\{((\frac{x}{t})^2-4,d),\ ((\sqrt{m}-\frac{x}{t})(\frac{x}{t}+2),d)\}$$

over $t\neq 0$.

If $d\in k^{\times 2}$ *or* $d\cdot m\in k^{\times 2}$*, then* $\mathrm{Br}(k)=\mathrm{Br}_1(X)=\mathrm{Br}(X)$

Proof. Since X is geometrically rational, one has $\mathrm{Br}(X)=\mathrm{Br}_1(X)$. One clearly has $X(k)\neq\emptyset$. By the Hochschild-Serre spectral sequence (see [6, Lemma 2.1]), one has an isomorphism

$$\mathrm{Br}_1(X)/\mathrm{Br}_0(X)\simeq H^1(k,\mathrm{Pic}(\overline{X})). \tag{3.2}$$

By [10, Chapter V, Proposition 4.10] and Lemma 3.1, there is $l\in\mathrm{Pic}(\overline{X})$ satisfying the following intersection property

$$(l.l)=1 \quad \text{and} \quad (l.l_i(1,1))=0$$

for $1\leq i\leq 6$ such that $\{l_i(1,1):\ 1\leq i\leq 6\}\cup\{l\}$ forms a basis of $\mathrm{Pic}(\overline{X})$ where $l_i(1,1)$ are the lines in Lemma 3.1 with $1\leq i\leq 6$. Indeed, the six lines $l_i(1,1), i=1,\dots,6$ are skew to one another, hence may be simultaneously blown down, the surface obtained is $\mathbb{P}^2$. The class l is the inverse image of the class of lines in $\mathrm{Pic}(\mathbb{P}^2)$. Since

$$(L_j.l_i(1,1))=\begin{cases}1 & i-j\equiv 0 \text{ or } 3 \bmod 6\\ 0 & \text{otherwise}\end{cases}$$

where L_j are the lines in Lemma 3.1 with $1\leq j\leq 3$ and $1\leq i\leq 6$, one concludes that

$$L_j=l-l_j(1,1)-l_{j+3}(1,1) \tag{3.3}$$

in $\mathrm{Pic}(\overline{X})$ for $1\leq j\leq 3$ by [10, Chapter V, Proposition 4.8 (e)]. For simplicity, we sometimes write l_i for $l_i(1,1)$ with $1\leq i\leq 6$.

(1) Suppose $d\notin k^{\times 2}$ and $md\notin k^{\times 2}$.
There is $\sigma\in\mathrm{Gal}(k(\sqrt{d},\sqrt{m})/k)$ such that

$$\sigma(\sqrt{d})=-\sqrt{d} \quad \text{and} \quad \sigma(\sqrt{m})=\sqrt{m}.$$

Since the intersection numbers

$$(\sigma l_j(1,1).l_i(1,1))=(l_j(1,-1).l_i(1,1))=\begin{cases}0 & i=j+3\\ 1 & i\neq j+3\end{cases} \tag{3.4}$$

and

$$(\sigma l_{3+j}(1,1).l_i(1,1))=(l_{3+j}(1,-1).l_i(1,1))=\begin{cases}0 & i=j\\ 1 & i\neq j\end{cases} \tag{3.5}$$

for $1\leq j\leq 3$, one obtains

$$\sigma l_j(1,1)=2l-\sum_{i\neq j+3}l_i(1,1) \quad \text{and} \quad \sigma l_{3+j}(1,1)=2l-\sum_{i\neq j}l_i(1,1) \tag{3.6}$$

in $\mathrm{Pic}(\overline{X})$ by [10, Chapter V, Theorem 4.9] for $1 \leq j \leq 3$. This implies that

$$\sigma l = 5l - 2\sum_{i=1}^{6} l_i(1,1) \tag{3.7}$$

by (3.3). Then

$$\ker(1+\sigma) = \langle (l-l_1-l_2-l_3), (l_1-l_4), (l_2-l_5), (l_3-l_6) \rangle \tag{3.8}$$

and

$$(1-\sigma)\mathrm{Pic}(\overline{X}) = \langle 2(l-l_1-l_2-l_3), (l_1-l_4+l_3-l_6), (l_2-l_5-l_3+l_6), (l_2-l_5+l_3-l_6) \rangle \tag{3.9}$$

by (3.6), (3.7).

Given a finite cyclic group $G = <\sigma>$ and a G-module M, recall that we have isomorphisms $H^1(G,M) \cong \hat{H}^{-1}(G,M)$, where the later group is the quotient of ${}^{N_\sigma}(M)$, the set of elements of M of norm 0, by its subgroup $(1-\sigma)M$.

(1a) Suppose $d \notin k^{\times 2}$ and $m \in k^{\times 2}$. Then

$$H^1(k, \mathrm{Pic}(\overline{X})) = H^1(<\sigma>, \mathrm{Pic}(\overline{X})) \simeq \hat{H}^{-1}(<\sigma>, \mathrm{Pic}(\overline{X})) \cong (\mathbb{Z}/2)^2$$

by [18, (1.6.6) and (1.6.12) Proposition] and (3.8) and (3.9).

(2) Suppose $m \notin k^{\times 2}$ and $md \notin k^{\times 2}$.
There is $\tau \in \mathrm{Gal}(k(\sqrt{d}, \sqrt{m})/k)$ such that

$$\tau(\sqrt{m}) = -\sqrt{m} \quad \text{and} \quad \tau(\sqrt{d}) = \sqrt{d}.$$

Since the intersection numbers

$$(\tau l_{j+3}(1,1).l_i(1,1)) = (l_{j+3}(-1,1).l_i(1,1)) = \begin{cases} 0 & 1 \leq i \leq 3 \text{ and } i = j+3 \\ 1 & 4 \leq i \leq 6 \text{ and } i \neq j+3 \end{cases} \tag{3.10}$$

for $1 \leq j \leq 3$, one obtains

$$\tau l_{j+3}(1,1) = l - \sum_{4 \leq i \neq j+3 \leq 6} l_i(1,1) \tag{3.11}$$

in $\mathrm{Pic}(\overline{X})$ by [10, Chapter V, Theorem 4.9] for $1 \leq j \leq 3$. This implies that

$$\tau l = 2l - \sum_{i=4}^{6} l_i(1,1) \tag{3.12}$$

by (3.3). Then

$$\ker(1+\tau) = \langle l-l_4-l_5-l_6 \rangle \quad \text{and} \quad \ker(1-\tau) = \langle l_1, l_2, l_3, (l-l_4), (l-l_5), (l-l_6) \rangle \tag{3.13}$$

and

$$(1-\tau)\mathrm{Pic}(\overline{X}) = \langle l-l_4-l_5-l_6 \rangle \tag{3.14}$$

by (3.11), (3.12).

(2a) If $m \notin k^{\times 2}$ and $d \in k^{\times 2}$, then

$$H^1(k, \mathrm{Pic}(\overline{X})) = H^1(<\tau>, \mathrm{Pic}(\overline{X})) \simeq \hat{H}^{-1}(<\tau>, \mathrm{Pic}(\overline{X})) = 0$$

by [18, (1.6.6) and (1.6.12) Proposition] and (3.13) and (3.14).

If $d \in k^{\times 2}$ and $m \in k^{\times 2}$, then we also have $H^1(k, \mathrm{Pic}(\overline{X})) = 0$. Indeed, in that case all 27 lines are defined over k and the action of the Galois group on $\mathrm{Pic}(\overline{X})$ is the trivial action.

(3) Suppose that none of d, m, dm is a square, that it $[k(\sqrt{m}, \sqrt{d}) : k] = 4$.
Then

$$H^1(k, \mathrm{Pic}(\overline{X})) = H^1(G, \mathrm{Pic}(\overline{X}))$$

by [18, (1.6.6) Proposition], where $G = \mathrm{Gal}(k(\sqrt{m}, \sqrt{d})/k)$. Let $\sigma, \tau \in G$ as above. Then one has the following exact sequence

$$0 \to H^1(\langle\sigma\rangle, \mathrm{Pic}(\overline{X})^{\langle\tau\rangle}) \to H^1(G, \mathrm{Pic}(\overline{X})) \to H^1(\langle\tau\rangle, \mathrm{Pic}(\overline{X})) = 0$$

by [18, (1.6.6) and (1.6.12) Proposition] and (3.13) and (3.14). Since

$$\ker(1+\sigma) \cap \mathrm{Pic}(\overline{X})^{\langle\tau\rangle} = \langle (l - l_4 - l_2 - l_3), (l - l_5 - l_1 - l_3), (l - l_6 - l_1 - l_2) \rangle$$

by (3.8), (3.13) and

$$(1-\sigma)\mathrm{Pic}(\overline{X})^{\langle\tau\rangle} = [(1-\sigma)\mathrm{Pic}(\overline{X})] \cap \mathrm{Pic}(\overline{X})^{\langle\tau\rangle}$$
$$= \langle (2l - l_1 - 2l_2 - l_3 - l_4 - l_6), (l_2 - l_3 - l_5 + l_6), (2l - 2l_1 - l_2 - l_3 - l_5 - l_6) \rangle$$

by (3.6), (3.7), (3.9), (3.13) and (3.14), one concludes that

$$H^1(k, \mathrm{Pic}(\overline{X})) = [\ker(1+\sigma) \cap \mathrm{Pic}(\overline{X})^{\langle\tau\rangle}]/[(1-\sigma)\mathrm{Pic}(\overline{X})^{\langle\tau\rangle}] \cong \mathbb{Z}/2.$$

(4) Suppose $m, d \notin k^{\times 2}$ and $md \in k^{\times 2}$, i.e. $k(\sqrt{m}) = k(\sqrt{d}) \neq k$.
Let ρ be the generator of $\mathrm{Gal}(k(\sqrt{m})/k)$. Since the intersection numbers

$$(\rho l_{j+3}(1,1).l_i(1,1)) = (l_{j+3}(-1,-1).l_i(1,1)) = \begin{cases} 1 & 1 \leq i \neq j \leq 3 \\ 0 & \text{otherwise} \end{cases}$$

for $1 \leq j \leq 3$, one obtains that

$$\rho l_{j+3}(1,1) = l - \sum_{1 \leq i \neq j \leq 3} l_i(1,1) \tag{3.15}$$

for $1 \leq j \leq 3$. Then

$$\rho l = 4l - \sum_{i=1}^{3} (l_i(1,1)) - \sum_{i=1}^{6} l_i(1,1) \tag{3.16}$$

by (3.6) and (3.15). Since

$$\ker(1+\rho) = (1-\rho)\mathrm{Pic}(\overline{X}) = \langle (l - l_2 - l_3 - l_4), (l - l_1 - l_3 - l_5), (l - l_1 - l_2 - l_6) \rangle$$

by (3.6), (3.15) and (3.16), one concludes that

$$H^1(k, \mathrm{Pic}(\overline{X})) = H^1(<\rho>, \mathrm{Pic}(\overline{X})) \cong \hat{H}^{-1}(<\rho>, \mathrm{Pic}(\overline{X})) = 0.$$

Now we produce concrete generators in $\mathrm{Br}_1(X)$ for $\mathrm{Br}_1(X)/\mathrm{Br}(k) \cong H^1(k, \mathrm{Pic}(\overline{X}))$. If $d \in k^{\times 2}$ or $md \in k^{\times 2}$, we have just seen that $\mathrm{Br}_1(X)/\mathrm{Br}(k) = 0$. Let us consider the other cases.

Let U be the open subset of X defined by $t \neq 0$. Then equation (3.1) is equivalent to

$$(2z - xy)^2 - 4d = (x^2 - 4)(y^2 - 4) \tag{3.17}$$

for U. Since

$$\{x \pm 2 = 0\} \cap \{((x \mp 2)(y^2 - 4) = 0\}$$

is a closed subset of codimension ≥ 2 on U, one obtains that $(x \pm 2, d) \in \mathrm{Br}_1(U)$. This implies that

$$B = (x^2 - 4, d) = (y^2 - 4, d) = (z^2 - 4, d) \in \mathrm{Br}_1(U).$$

The residues of B at the lines L_1, L_2 and L_3 which form the complement of U in X (cf. Lemma 3.1) are easily seen to be trivial. One thus has $B \in \mathrm{Br}_1(X)$.

If $m \in k^{\times 2}$, equation (3.1) is equivalent to

$$(2y - \sqrt{m}z)^2 - dz^2 = 4(x - \sqrt{m})(yz - x - \sqrt{m})$$

for U. Then $(\sqrt{m} - x, d) \in \mathrm{Br}_1(U)$ by the same argument as above. This implies that

$$M = ((x+2)(\sqrt{m} - x), d) \in \mathrm{Br}_1(U).$$

Then $M \in \mathrm{Br}_1(X)$ by computing the residues of M at L_1, L_2 and L_3 as above.

To show that these elements B and M are not constant, one uses the conic fibration

$$\pi : \ U \to \mathbb{A}^1; \ (x, y, z) \mapsto x.$$

The generic fibre $U_\eta \xrightarrow{\pi_\eta} \eta$ induces

$$\pi_\eta^* : \mathrm{Br}(\eta) \to \mathrm{Br}(U_\eta) \quad \text{with} \quad \ker(\pi_\eta^*) = (x^2 - 4, m - x^2)$$

by [9, Theorem 5.4.1].

If $[k(\sqrt{m}, \sqrt{d}) : k] = 4$, then the residue of $(x^2 - 4, d)$ at $(x^2 - m)$ is different from that of $(x^2 - 4, m - x^2)$. This implies that $\pi_\eta^*(x^2 - 4, d)$ is not constant by the Faddeev exact sequence (see [9, Corollary 6.4.6]). Since $\pi_\eta^*(x^2 - 4, d)$ is the pull-back of B by the projection map $X_\eta \to X$, one concludes that B is not constant, hence B generates $\mathrm{Br}_1(X)/\mathrm{Br}(k) = \mathbb{Z}/2$.

If $d \notin k^{\times 2}$ and $m \in k^{\times 2}$, then we have the residues

$$\partial_P(x^2 - 4, d) = \begin{cases} d \in k^\times/k^{\times 2} & \text{if } P \in \{(x \pm 2)\} \\ 1 \in k^\times/k^{\times 2} & \text{otherwise} \end{cases}$$

and

$$\partial_P((\sqrt{m} - x)(x + 2), d) = \begin{cases} d \in k^\times/k^{\times 2} & \text{if } P \in \{(x + 2), (x - \sqrt{m})\} \\ 1 \in k^\times/k^{\times 2} & \text{otherwise} \end{cases}$$

and

$$\partial_P(x^2 - 4, m - x^2) = \begin{cases} d \in k^\times/k^{\times 2} & \text{if } P \in \{(x \pm 2), (x \pm \sqrt{m})\} \\ 1 \in k^\times/k^{\times 2} & \text{otherwise} \end{cases}$$

for all closed points P of $\mathbb{P}^1$. Then

$$\pi_\eta^*(x^2-4,d), \quad \pi_\eta^*((\sqrt{m}-x)(x+2),d) \quad \text{and} \quad \pi_\eta^*((x^2-4,d)\cdot((\sqrt{m}-x)(x+2),d))$$

are not constant by the Faddeev exact sequence. Therefore B and M have independent classes in over $\mathrm{Br}_1(X)/\mathrm{Br}(k) \cong (\mathbb{Z}/2)^2$, hence generate that group. □

Remark 3.3. If $d \in k^{\times 2}$ or $d \cdot m \in k^{\times 2}$, then $\overline{X}$ contains a pair of globally rational skew lines. As for any smooth projective cubic surface with this property, this implies that X is k-birational to projective space $\mathbb{P}^2_k$. This general fact goes back to L. Euler in the case of the diagonal cubic surface $x^3+y^3+z^3+t^3=0$ and a generalisation is due to B. Segre. Segre's result was completed by Swinnerton-Dyer's paper [20]. Therefore $\mathrm{Br}(X) = \mathrm{Br}(k)$. We keep this part of the computation in Proposition 3.2 because some intermediate results will later be used.

Theorem 3.4. *Let k be a field of characteristic zero and let $m \in k \setminus \{0,4\}$ and $d = m-4$. Let U be the affine variety over k defined by the equation*

$$x^2+y^2+z^2-xyz=m. \tag{3.18}$$

If $[k(\sqrt{m},\sqrt{d}):k]=4$ then

$$\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \cong (\mathbb{Z}/2)^3$$

with the generators $\{(x-2,d),\ (y-2,d),\ (z-2,d)\}$.

If $d \notin k^{\times 2}$ and $dm \in k^{\times 2}$ then

$$\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \cong (\mathbb{Z}/2)^2$$

with the generators $\{(x-2,d),\ (y-2,d)\}$.

If $d \notin k^{\times 2}$ and $m \in k^{\times 2}$, then

$$\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \cong (\mathbb{Z}/2)^4$$

with the generators $\{(x-2,d),\ (y-2,d),\ (z-2,d),\ (x-\sqrt{m},d)\}$.

Otherwise, i.e. if $d \in k^{\times 2}$, then $\mathrm{Br}_1(U) = \mathrm{Br}_0(U)$.

Proof. We keep notation as in Lemma 3.1. Let $l \in \mathrm{Pic}(\overline{X})$ as in the proof of Proposition 3.2. Then $\mathrm{Pic}(\overline{U})$ is given by the following quotient group

$$((\oplus_{i=1}^6 \mathbb{Z}l_i(1,1)) \oplus \mathbb{Z}l)/(l - l_j(1,1) - l_{j+3}(1,1) : 1 \le j \le 3) \cong \oplus_{i=1}^4 \mathbb{Z}\overline{l_i(1,1)}$$

by Proposition 2.2 and formula (3.3). By Proposition 2.2 we have $\overline{k}^\times = \overline{k}[U]^\times$. The Hochschild-Serre spectral sequence (see [6, Lemma 2.1]) then gives an injective homomorphism

$$\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \hookrightarrow H^1(k, \mathrm{Pic}(\overline{U})). \tag{3.19}$$

In fact, it is an isomorphism since the smooth compactification X of U has rational points, hence also U (any smooth cubic surface over an infinite field k is k-unirational as soon as it has a k-rational point).

• Case $[k(\sqrt{m},\sqrt{d}):k]=4$. Let $G=\mathrm{Gal}(k(\sqrt{m},\sqrt{d})/k)$. Let σ and τ be the generators of $\mathrm{Gal}(k(\sqrt{m},\sqrt{d})/k)$ satisfying

$$\sigma(\sqrt{d})=-\sqrt{d},\quad \sigma(\sqrt{m})=\sqrt{m};\qquad \tau(\sqrt{d})=\sqrt{d},\quad \tau(\sqrt{m})=-\sqrt{m}.$$

Then in $\mathrm{Pic}(\overline{U})$ we have the following equalities

$$\sigma(\overline{l_i(1,1)})=-\overline{l_i(1,1)} \tag{3.20}$$

for $1\leq i\leq 4$ by (3.6), $\tau(\overline{l_i(1,1)})=\overline{l_i(1,1)}$ for $1\leq i\leq 3$ and

$$\tau(\overline{l_4(1,1)})=-\overline{l_1(1,1)}+\overline{l_2(1,1)}+\overline{l_3(1,1)}-\overline{l_4(1,1)} \tag{3.21}$$

by (3.11). Since $\mathrm{Pic}(\bar{U})$ is free and $\mathrm{Gal}(\bar{k}/k(\sqrt{m},\sqrt{d}))$ acts on $\mathrm{Pic}(\overline{U})$ trivially, one obtains that

$$H^1(G,\mathrm{Pic}(\overline{U}))\cong H^1(k,\mathrm{Pic}(\overline{U}))$$

by [18, (1.6.6) Proposition]. Let H be the subgroup of G generated by σ. Then

$$\mathrm{Pic}(\overline{U})^H=0$$

by the equation (3.20). Therefore

$$H^1(G,\mathrm{Pic}(\overline{U}))\cong H^1(H,\mathrm{Pic}(\overline{U}))^{G/H}$$

by [18, (1.6.6) Proposition]. Since

$$H^1(H,\mathrm{Pic}(\overline{U}))\cong \hat{H}^{-1}(<\sigma,>\mathrm{Pic}(\overline{U}))\cong \oplus_{i=1}^4(\mathbb{Z}/2)\overline{l_i(1,1)}$$

by [18, (1.6.12) Proposition] and the equation (3.20), one concludes

$$H^1(k,\mathrm{Pic}(\overline{U}))\cong H^1(H,\mathrm{Pic}(\overline{U}))^{G/H}\cong \oplus_{i=1}^3(\mathbb{Z}/2)\overline{l_i(1,1)}$$

by (3.21).

• Case $k(\sqrt{m})=k(\sqrt{d})\neq k$. Let ρ be the generator of $\mathrm{Gal}(k(\sqrt{m})/k)$. Since (3.6) is still available, one has $\rho(\overline{l_i(1,1)})=-\overline{l_i(1,1)}$ for $1\leq i\leq 3$. By (3.15), one obtains

$$\rho(\overline{l_4(1,1)})=\overline{l_1(1,1)}-\overline{l_2(1,1)}-\overline{l_3(1,1)}+\overline{l_4(1,1)}.$$

Therefore

$$H^1(k,\mathrm{Pic}(\overline{U}))=H^1(\rho,\mathrm{Pic}(\overline{U}))\cong \hat{H}^{-1}(\rho,\mathrm{Pic}(\overline{U}))\cong \oplus_{i=1}^2(\mathbb{Z}/2)\overline{l_i(1,1)}.$$

• Case $k(\sqrt{d})\neq k(\sqrt{m})=k$. Let σ be the generator of $\mathrm{Gal}(k(\sqrt{d})/k)$. Since the intersection formulae (3.4) and (3.5) are still available, one has $\sigma(\overline{l_i(1,1)})=-\overline{l_i(1,1)}$ for $1\leq i\leq 4$. Then

$$H^1(k,\mathrm{Pic}(\overline{U}))=H^1(<\sigma>,Pic(\overline{U}))\cong \hat{H}^{-1}(<\sigma>,Pic(\overline{U}))\cong \oplus_{i=1}^4(\mathbb{Z}/2)\overline{l_i(1,1)}.$$

• The remaining case is $d\in k^{\times 2}$. If also $m\in k^{\times 2}$, then the Galois action on the lattice $\mathrm{Pic}(\overline{U})$ is trivial, hence $H^1(k,\mathrm{Pic}(\overline{U}))=0$. Suppose $m\notin k^{\times 2}$. Let τ be the generator of $\mathrm{Gal}(k(\sqrt{m})/k)$. Since

$$\ker(1+\tau)=\langle\overline{l_1(1,1)}-\overline{l_2(1,1)}-\overline{l_3(1,1)}+2\overline{l_4(1,1)}\rangle$$

and

$$(1-\tau)(\overline{l_4(1,1)})=\overline{l_1(1,1)}-\overline{l_2(1,1)}-\overline{l_3(1,1)}+2\overline{l_4(1,1)}$$

by (3.21), one concludes that $H^1(k, \mathrm{Pic}(\overline{U})) = 0$.

Let us now produce concrete elements in $\mathrm{Br}_1(U)$. Since

$$(2z - xy)^2 - 4d = (x^2 - 4)(y^2 - 4) \tag{3.22}$$

is another way to write the given equation (3.18), one concludes that the quaternion class $(x \pm 2, d)$ is in $\mathrm{Br}_1(U)$ by the same argument as that in Proposition 3.2. Similar formulas give the same result for $(y \pm 2, d)$ and $(z \pm 2, d)$.

The plane $t = 0$ cuts out the three lines (L_1, L_2, L_3), each with multiplicity 1. The plane $x \pm 2t = 0$ cuts out L_1 and two lines each defined over $k(\sqrt{d})$. From this we compute the residues:

$$\partial_{L_i}((x \pm 2t)/t, d) = \begin{cases} 1 \in k^\times/(k^\times)^2 & i = 1 \\ d \in k^\times/(k^\times)^2 & i = 2 \text{ and } 3. \end{cases}$$

Similarly, one has

$$\partial_{L_i}((y \pm 2t)/t, d) = \begin{cases} 1 \in k^\times/(k^\times)^2 & i = 2 \\ d \in k^\times/(k^\times)^2 & i = 1 \text{ and } 3 \end{cases}$$

and

$$\partial_{L_i}((z \pm 2t)/t, d) = \begin{cases} 1 \in k^\times/(k^\times)^2 & i = 3 \\ d \in k^\times/(k^\times)^2 & i = 1 \text{ and } 2. \end{cases}$$

This computation of residues will enable us to establish independence modulo 2 of various classes in $\mathrm{Br}_1(U)/\mathrm{Br}_0(U)$.

Since

$$(x - y - z + 2)^2 - d = (x + 2)(y - 2)(z - 2) \tag{3.23}$$

by (3.18), one has

$$((x - 2)(y - 2)(z - 2), d) = (x^2 - 4, d). \tag{3.24}$$

When $[K : k] = 4$, the quaternion $(x^2 - 4, d)$ is not constant by Proposition 3.2. Therefore $\{(x - 2, d),\ (y - 2, d),\ (z - 2, d)\}$ is a set of generators of $\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \cong (\mathbb{Z}/2)^3$.

When $k(\sqrt{d}) = k(\sqrt{m}) \neq k$, then $\{(x-2, d),\ (y-2, d)\}$ is a set of generators of $\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \cong (\mathbb{Z}/2)^2$.

When $m \in k^{\times 2}$ and $d \notin k^{\times 2}$, the equation (3.18) can be written as

$$(2y - \sqrt{m}z)^2 - dz^2 = 4(x - \sqrt{m})(yz - x - \sqrt{m}).$$

Then $(x - \sqrt{m}, d) \in \mathrm{Br}_1(U)$ by the same argument as that in Proposition 3.2. Since $(x - \sqrt{m}, d)$ has the same residues as $(x - 2, d)$ at L_i for $1 \le i \le 3$, the class $(x - \sqrt{m}, d)$ in $\mathrm{Br}_1(U)/\mathrm{Br}_0(U)$ is different from $(x - 2, d)$, $(y - 2, d)$ and $(z - 2, d)$ by Proposition 3.2. Since

$$((x - \sqrt{m})(y - 2)(z - 2), d) = ((x - \sqrt{m})(x + 2), d)$$

is not a constant element by (3.23) and Proposition 3.2, one concludes that

$$\{(x - 2, d),\ (y - 2, d),\ (z - 2, d),\ (x - \sqrt{m}, d)\}$$

is a set of generators of $\mathrm{Br}_1(U)/\mathrm{Br}_0(U) \cong (\mathbb{Z}/2)^4$. ☐

Remark 3.5. Note that the set $\{(x+2,d),\ (y+2,d),\ (z+2,d)\}$ is not a set of generators of $\mathrm{Br}_1(U)/\mathrm{Br}_0(U)$ in Theorem 3.4 because (3.18) can be written as

$$(x+y+z+2)^2 - d = (x+2)(y+2)(z+2). \tag{3.25}$$

4. Computation of Brauer groups III, transcendental parts

Let k be a field of characteristic zero, and $m \in k \setminus \{0,4\}$. Let $d = m-4 \neq 0$. Let $X \subset \mathbb{P}^3_k$ be the smooth cubic surface defined by the equation

$$t(x^2+y^2+z^2) - xyz = mt^3.$$

Let U be the affine open sub-variety of X given by $t \neq 0$, i.e. by the affine equation

$$x^2+y^2+z^2-xyz = m.$$

By Proposition 2.1, we have $\mathrm{Br}(\overline{U}) \simeq \mathbb{Q}/\mathbb{Z}$. In this section, we determine the transcendental Brauer group $\mathrm{Br}(U)/\mathrm{Br}_1(U) \subset \mathrm{Br}(\overline{U})$ of U.

By [10, Chapter V, Proposition 4.10], one can contract $\overline{X}$ to $\mathbb{P}^2_{\bar{k}}$ over $\bar{k}$ by sending the 6 lines $\{l_i(1,-1)\}_{i=1}^6$ to the 6 points. The 3 lines $\{L_i\}_{i=1}^3$ correspond to three lines in $\mathbb{P}^2_{\bar{k}}$ by this contraction and each of these three corresponding lines passes through one pair among the 6 points by [10, Chapter V, Theorem 4.9]. Then this contraction induces an isomorphism

$$V := \overline{U} \setminus \{l_i(1,-1)\}_{i=1}^6 \simeq \mathbb{G}_m \times_{\bar{k}} \mathbb{G}_m$$

over $\bar{k}$.

Though this will not be used in the paper, it is worth noticing the following consequence.

Proposition 4.1. *The (Grothendieck) geometric fundamental group $\pi_1(\overline{U})$ is trivial.*

Proof. Recall $\mathrm{char}(k) = 0$. Since V is open in $\overline{U}$, the group $\pi_1(\overline{U})$ is a quotient of $\pi_1(V)$. The group $\pi_1(\mathbb{G}_m \times_{\bar{k}} \mathbb{G}_m) = \hat{\mathbb{Z}}^2$ is abelian. From the above isomorphism we conclude that $\pi_1(\overline{U})$ is abelian. It is thus isomorphic to the profinite completion of the system of groups $H^1(\overline{U}, \mathbb{Z}/n)$. By Proposition 2.2, $\overline{k}^* \simeq \overline{k}[U]^*$ and $\mathrm{Pic}(\overline{U})$ is torsionfree. The Kummer sequence then gives $H^1(\overline{U}, \mathbb{Z}/n) \simeq \mathrm{Pic}(\overline{U})[n] = 0$. ☐

As we shall see just below, the restriction map

$$\mathrm{Br}(\overline{U}) \to \mathrm{Br}(V)$$

is an isomorphism.

At least over some field extension of k one may thus compute the transcendental elements in $\mathrm{Br}(\overline{U})$ by pull-back of $\mathrm{Br}(\mathbb{G}_m \times_{\bar{k}} \mathbb{G}_m) \simeq \mathbb{Q}/\mathbb{Z}$.

Theorem 4.2. *Let n be a positive integer and $\zeta \in \bar{k}$ be a primitive n-th root of unity. Keep notation as in Lemma 3.1 and Theorem 3.4. Then the unique cyclic group of order n in* $\mathrm{Br}(\overline{U})$

is generated by the cyclic algebra $R_n = (\frac{f}{g}, \frac{u}{v})_\zeta$ *of dimension* n^2*, where*

$$\begin{cases} f = \frac{1}{2}(\sqrt{m} - \sqrt{d} - 2)xz + \sqrt{d}x + (2 - \sqrt{m})y + \sqrt{d}z - \sqrt{m} \cdot \sqrt{d} \\ g = \frac{1}{2}(\sqrt{m} + \sqrt{d} - 2)yz - \sqrt{d}y + (2 - \sqrt{m})x - \sqrt{d}z + \sqrt{m} \cdot \sqrt{d} \\ u = \frac{1}{2}(\sqrt{m} - \sqrt{d} - 2)xy + \sqrt{d}y + (2 - \sqrt{m})z + \sqrt{d}x - \sqrt{m} \cdot \sqrt{d} \\ v = \frac{1}{2}(\sqrt{m} + \sqrt{d} - 2)xz - \sqrt{d}z + (2 - \sqrt{m})y - \sqrt{d}x + \sqrt{m} \cdot \sqrt{d} \end{cases}.$$

Proof. By Bezout's theorem (see [10, Chapter I, Theorem 7.7]), one has

$$\begin{cases} div(f) = L_1 + L_3 + l_1(1,-1) + l_3(1,1) + l_4(1,-1) + l_6(1,1) \\ div(g) = L_2 + L_3 + l_2(1,-1) + l_3(1,1) + l_5(1,-1) + l_6(1,1) \\ div(u) = L_1 + L_2 + l_1(1,1) + l_2(1,-1) + l_4(1,1) + l_5(1,-1) \\ div(v) = L_1 + L_3 + l_1(1,1) + l_3(1,-1) + l_4(1,1) + l_6(1,-1) \end{cases}$$

where L_i with $1 \le i \le 3$ and $l_j(\epsilon, \delta)$ with $1 \le j \le 6$, $\epsilon = \pm 1$ and $\delta = \pm 1$ are given by Lemma 3.1. For instance, one checks that each of the lines involved in $div(f)$ is contained in the projective quadric defined by $f = 0$. Since the degree of f is 2 and that of the cubic surface is 3, Bezout's theorem implies that the multiplicity of each line in $div(f)$ is 1.

This implies that

$$\begin{cases} div(\frac{f}{g}) = L_1 - L_2 + l_1(1,-1) - l_2(1,-1) + l_4(1,-1) - l_5(1,-1) \\ div(\frac{u}{v}) = L_2 - L_3 + l_2(1,-1) - l_3(1,-1) + l_5(1,-1) - l_6(1,-1). \end{cases} \tag{4.1}$$

Let us first prove that the restriction map

$$\mathrm{Br}(\overline{U}) \to \mathrm{Br}(V)$$

is an isomorphism. Indeed, the lines $\{l_i(1,-1)\}$ are skew to one another, and each of them intersects the plane $t = 0$ in just one point, call it P_i. Let $m_i := \{l_i(1,-1)\} \setminus \{P_i\} \cong \mathbb{A}^1_{\bar{k}}$. We thus have an exact sequence

$$0 \to \mathrm{Br}(\overline{U}) \to \mathrm{Br}(V) \to \oplus_{i=1}^6 H^1_{\text{ét}}(m_i, \mathbb{Q}/\mathbb{Z}).$$

But $H^1_{\text{ét}}(m_i, \mathbb{Q}/\mathbb{Z}) = H^1_{\text{ét}}(\mathbb{A}^1_{\bar{k}}(\mathbb{Q}/\mathbb{Z}) = 0$.

We thus have $R_n \in \mathrm{Br}(\overline{U})$.

The line L_1 does not appear in the divisor of u/v. In the divisor of f/g it appears with valuation 1. The residue of R_n at the generic point of L_1 is thus given by the class in $k(L_1)^\times/k(L_1)^{\times n}$ of the rational function induced by u/v on L_1.The divisor of that function is a linear combination of points which in particular contains $L_3 \cap L_1$ with multiplicity -1. Thus the order of the residue is n, and R_n itself is of order n, hence generates $\mathrm{Br}(\overline{U})[n]$. □

Over any field K containing $k(\sqrt{d}, \sqrt{m})$, the 27 lines are defined over K, we may consider the complement V/K of the 6 lines $l_i(1,-1)$. The same localisation argument together with the triviality of étale cohomology with constant coefficients of an affine line yields an exact sequence

$$0 \to \mathrm{Br}(U_K) \to \mathrm{Br}(V) \to \oplus_{i=1}^6 H^1(K, \mathbb{Q}/\mathbb{Z}).$$

We are interested in the computation of the transcendental Brauer group over the ground field. For this, an explicit computation of residues at the generic points of the lines $l_i(1,-1)$ seems necessary. Since f, g, u, v and each of the curves $D = l_i(1,-1)$ are defined over $K = k(\sqrt{d}, \sqrt{m})$, we can compute the residues $\partial_D(R_n)$ over any field E containing K and μ_n in

$$H^1(E(D), \mathbb{Z}/n) \simeq E(D)^\times / E(D)^{\times n}.$$

These residues, as explained above, actually take their values in $E^\times/E^{\times n}$.

Proposition 4.3. *With notation as above :*

For $D = l_2(1,-1)$, $\partial_D(R_n) = \frac{\sqrt{m}+\sqrt{d}-2}{\sqrt{m}-\sqrt{d}-2} = -\frac{1}{2}(\sqrt{d}+\sqrt{m}) \in E^\times/E^{\times n}$

For $D = l_5(1,-1)$, $\partial_D(R_n) = \frac{\sqrt{m}-\sqrt{d}}{2} \cdot \frac{\sqrt{m}+\sqrt{d}-2}{\sqrt{m}-\sqrt{d}-2} = -1 \in E^\times/E^{\times n}$.

$$\partial_D(R_n) = \begin{cases} -1 \in E^\times/E^{\times n} & D \in \{l_1(1,-1),\ l_3(1,-1)\} \\ \frac{\sqrt{d}-\sqrt{m}}{2} \in E^\times/E^{\times n} & D \in \{l_4(1,-1),\ l_6(1,-1)\} \end{cases}$$

Proof. In the course of our computations, we shall make tacit use of the equality

$$(\frac{\sqrt{d}-\sqrt{m}}{2}).(\frac{\sqrt{d}+\sqrt{m}}{2}) = -1 \tag{4.2}$$

.

Let us compute $\partial_D(R_n)$ for $D = l_2(1,-1)$. Since

$$g = [\frac{1}{2}(\sqrt{m}+\sqrt{d}-2)y - \sqrt{d}](z-x+\sqrt{d}) + (y-2)[\frac{1}{2}(\sqrt{m}+\sqrt{d}-2)x - \frac{1}{2}\sqrt{d}(\sqrt{m}+\sqrt{d})]$$

and

$$u = (2-\sqrt{m})(z-x+\sqrt{d}) + (y-2)[\frac{1}{2}(\sqrt{m}-\sqrt{d}-2)x + \sqrt{d}],$$

one has

$$\frac{g}{u} = \frac{[\frac{1}{2}(\sqrt{m}+\sqrt{d}-2)y - \sqrt{d}](\frac{z-x+\sqrt{d}}{y-2}) + [\frac{1}{2}(\sqrt{m}+\sqrt{d}-2)x - \frac{1}{2}\sqrt{d}(\sqrt{m}+\sqrt{d})]}{(2-\sqrt{m})(\frac{z-x+\sqrt{d}}{y-2}) + [\frac{1}{2}(\sqrt{m}-\sqrt{d}-2)x + \sqrt{d}]}.$$

Since

$$\frac{z-x+\sqrt{d}}{y-2} = \frac{xz-y-2}{z-x-\sqrt{d}}$$

by (3.18), one obtains that

$$\partial_D(R_n) = -\frac{v}{u}\cdot\frac{g}{f} = -\frac{v}{f}\cdot\frac{(\sqrt{m}-2)\cdot\frac{x(x-\sqrt{d})-4}{-2\sqrt{d}} + \frac{1}{2}(\sqrt{m}+\sqrt{d}-2)x - \frac{1}{2}\sqrt{d}(\sqrt{m}+\sqrt{d})}{(2-\sqrt{m})\cdot\frac{x(x-\sqrt{d})-4}{-2\sqrt{d}} + \frac{1}{2}(\sqrt{m}-\sqrt{d}-2)x + \sqrt{d}}$$

$$= \frac{v}{f}\cdot\frac{(\sqrt{m}-2)[x(x-\sqrt{d})-4] - (\sqrt{m}+\sqrt{d}-2)\sqrt{d}x + d(\sqrt{m}+\sqrt{d})}{(\sqrt{m}-2)[x(x-\sqrt{d})-4] + (\sqrt{m}-\sqrt{d}-2)\sqrt{d}x + 2d}.$$

Since

$$f|_D = \frac{1}{2}(\sqrt{m}-\sqrt{d}-2)x^2 + \sqrt{d}[3-\frac{1}{2}(\sqrt{m}-\sqrt{d})]x + 2(2-\sqrt{m}) - d - \sqrt{m}\cdot\sqrt{d}$$

and

$$v|_D = \frac{1}{2}(\sqrt{m}+\sqrt{d}-2)x^2 - \sqrt{d}[1+\frac{1}{2}(\sqrt{m}+\sqrt{d})]x + d + 2(2-\sqrt{m}) + \sqrt{m}\cdot\sqrt{d},$$

one concludes that

$$\partial_D(R_n) = \frac{\sqrt{m}+\sqrt{d}-2}{\sqrt{m}-\sqrt{d}-2} = -\frac{1}{2}(\sqrt{d}+\sqrt{m}) \in E(D)^\times/E(D)^{\times n}.$$

For $D = l_5(1,-1)$, one has

$$g = [\frac{1}{2}(\sqrt{m}+\sqrt{d}-2)y - \sqrt{d}]\cdot[z - \frac{1}{2}(\sqrt{m}-\sqrt{d})x] + (y-\sqrt{m})[\frac{1}{2}(2+\sqrt{d}-\sqrt{m})x - \sqrt{d}]$$

and

$$u = (2-\sqrt{m})[z - \frac{1}{2}(\sqrt{m}-\sqrt{d})x] + (y-\sqrt{m})[\frac{1}{2}(\sqrt{m}-\sqrt{d}-2)x + \sqrt{d}].$$

Since

$$\frac{z-\frac{1}{2}(\sqrt{m}-\sqrt{d})x}{y-\sqrt{m}} = \frac{xz-y-\sqrt{m}}{z-\frac{1}{2}(\sqrt{m}+\sqrt{d})x}$$

by (3.18), one obtains that

$$\begin{aligned}\partial_D(R_n) &= -\frac{v}{f}\cdot\frac{\frac{1}{2}(\sqrt{m}+\sqrt{d})(\sqrt{m}-2)\cdot\frac{(\sqrt{m}-\sqrt{d})x^2-4\sqrt{m}}{-2\sqrt{d}x} + \frac{1}{2}(2+\sqrt{d}-\sqrt{m})x - \sqrt{d}}{(2-\sqrt{m})\cdot\frac{(\sqrt{m}-\sqrt{d})x^2-4\sqrt{m}}{-2\sqrt{d}x} + \frac{1}{2}(\sqrt{m}-\sqrt{d}-2)x + \sqrt{d}}\\
&= \frac{v}{f}\cdot\frac{(\sqrt{m}-\sqrt{d})(\sqrt{m}-2)x^2 - 2dx + 2\sqrt{m}(\sqrt{m}+\sqrt{d})(\sqrt{m}-2)}{(2\sqrt{m}-4)x^2 - 2dx + 4\sqrt{m}(\sqrt{m}-2)}\\
&= \frac{v}{f}\cdot\frac{(\sqrt{m}-\sqrt{d})x^2 - 2(\sqrt{m}+2)x + 2\sqrt{m}(\sqrt{m}+\sqrt{d})}{2x^2 - 2(\sqrt{m}+2)x + 4\sqrt{m}}.\end{aligned}$$

Since

$$f|_D = \frac{\sqrt{m}-\sqrt{d}-2}{\sqrt{m}+\sqrt{d}}\cdot x^2 + \frac{\sqrt{d}}{2}(\sqrt{m}-\sqrt{d}+2)x + \sqrt{m}(2-\sqrt{m}-\sqrt{d})$$

and

$$v|_D = \frac{\sqrt{m}+\sqrt{d}-2}{\sqrt{m}+\sqrt{d}}x^2 - \sqrt{d}[1+\frac{1}{2}(\sqrt{m}-\sqrt{d})]x + \sqrt{m}(\sqrt{d}-\sqrt{m}+2),$$

one concludes that

$$\partial_D(R_n) = \frac{\sqrt{m}-\sqrt{d}}{2}\cdot\frac{\sqrt{m}+\sqrt{d}-2}{\sqrt{m}-\sqrt{d}-2} = -1 \in E(D)^\times/E(D)^{\times n}.$$

The other residues are

$$\partial_D(R_n) = \begin{cases} -1 \in E(D)^\times/E(D)^{\times n} & D\in\{l_1(1,-1),\ l_3(1,-1)\}\\ \frac{\sqrt{d}-\sqrt{m}}{2} \in E(D)^\times/E(D)^{\times n} & D\in\{l_4(1,-1),\ l_6(1,-1)\}\end{cases}$$

by (4.1) and straightforward computations. □

Lemma 4.4. *Let $K = k(\sqrt{m}, \sqrt{d}) \subset \bar{k}$. Then*

$$\mathrm{Br}(U_K)/\mathrm{Br}_1(U_K) \supset (\mathbb{Z}/n) \quad \text{if and only if} \quad \mu_n \subset K \text{ and } -1, \frac{\sqrt{d}-\sqrt{m}}{2} \in K^{\times n}.$$

In this case, $R_n \in \mathrm{Br}(V)$ as defined in Theorem 4.2 belongs to $\mathrm{Br}(U_K) \subset \mathrm{Br}(V)$, is of order n, and generates th n-torsion subgroup of $\mathrm{Br}(U_K)/\mathrm{Br}_1(U_K) \subset \mathrm{Br}(\bar{U})$.

Proof. Note that under the hypothesis $-1 \in K^{\times n}$, formula (4.2) shows that the condition $\frac{\sqrt{d}-\sqrt{m}}{2} \in K^{\times n}$ is independent of the choice of the square roots of d and m in $\bar{k}$.

If $\mu_n \subset K$ and $-1, (\sqrt{d}-\sqrt{m})/2 \in K^{\times n}$, then $R_n \in \mathrm{Br}(U_K)$ by Proposition 4.3 and it has image of order n in $\mathrm{Br}(\overline{U}) \simeq \mathbb{Q}/\mathbb{Z}$ by Theorem 4.2.

Let us prove the converse statement.

Assume $(\mathbb{Z}/n) \subset \mathrm{Br}(U_K)/\mathrm{Br}_1(U_K)$. The isomorphism $\mathrm{Br}(\overline{U}) \cong (\mathbb{Q}/\mathbb{Z})(-1)$ given by Proposition 2.1 is Galois equivariant. From Lemma 2.4, we then get $\mu_n \subset K$.

Since the lines $l_i(1,-1)$ in Lemma 3.1 are defined over $K \subset \bar{k}$ for $1 \le i \le 6$, the open subset

$$V = U_K \setminus \{l_i(1,-1)\}_{i=1}^6$$

is defined over K and satisfies $\mathrm{Pic}(V_{\bar{k}}) = 0$ since $V_{\bar{k}} \cong \mathbb{G}_{m,\bar{k}}^2$. One has the following commutative diagram of exact sequences

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathrm{Br}(K) = \mathrm{Br}_1(U_K) & \longrightarrow & \mathrm{Br}_1(V) & \xrightarrow{\partial_K} & \oplus_{i=1}^6 H^1(K, (\mathbb{Q}/\mathbb{Z}) l_i(1,-1)) \\
& \downarrow & & \downarrow & & \downarrow = \\
0 \longrightarrow & \mathrm{Br}(U_K) & \longrightarrow & \mathrm{Br}(V) & \xrightarrow{\partial_K} & \oplus_{i=1}^6 H^1(K, \mathbb{Q}/\mathbb{Z}) l_i(1,-1)
\end{array} \tag{4.3}$$

by [4, Theorem 3.4.1, Remark 3.3.2], [19, Lemma 6.1] and Theorem 3.4. From Prop. 2.2 we know that $\bar{k} = \bar{k}[U]^\times$ and that $\mathrm{Pic}(\overline{U})$ is a lattice. From the exact sequence of lattices with trivial Galois action

$$1 \to \bar{k}[V]^\times/\bar{k}^\times \xrightarrow{div} \oplus_{i=1}^6 \mathbb{Z} l_i(1,-1) \xrightarrow{\psi} \mathrm{Pic}(\overline{U}) \to 1,$$

Galois cohomology gives the long exact sequence

$$0 = H^1(K, \mathrm{Pic}(\overline{U})) \to H^2(K, \bar{k}[V]^\times/\bar{k}^\times) \xrightarrow{div} \oplus_{i=1}^6 H^2(K, \mathbb{Z} l_i(1,-1)) \to H^2(K, \mathrm{Pic}(\overline{U})).$$

That $H^1(K, \mathrm{Pic}(\overline{U})) = 0$ follows from the fact that $\mathrm{Pic}(\overline{U})$ is a lattice with trivial $\mathrm{Gal}(\bar{k}/K)$ action. Since the following diagram

$$\begin{array}{ccc}
H^2(K, \bar{k}[V]^\times) & \xrightarrow{\simeq} & \mathrm{Br}_1(V) \\
{\scriptstyle div}\downarrow & & \downarrow{\scriptstyle \partial_K} \\
\oplus_{i=1}^6 H^2(K, \mathbb{Z} l_i(1,-1)) & \xleftarrow{\simeq} & \oplus_{i=1}^6 H^1(K, (\mathbb{Q}/\mathbb{Z}) l_i(1,-1))
\end{array}$$

commutes up to sign by [4, Remark 3.3.2] and [6, Lemma 2.1], one has the following short exact sequence

$$0 \to \mathrm{Br}(K) \to \mathrm{Br}_1(V) \xrightarrow{\partial_K} \oplus_{i=1}^6 H^1(K, (\mathbb{Q}/\mathbb{Z}) l_i(1,-1)) \xrightarrow{\phi} \oplus_{i=1}^4 H^1(K, (\mathbb{Q}/\mathbb{Z})\overline{l_i(1,-1)}) \tag{4.4}$$

which extends the first line of (4.3), here ϕ is induced by ψ, and

$$\phi(\chi_1, \cdots, \chi_6) = (\chi_1 + \chi_5 + \chi_6, \chi_2 - \chi_5, \chi_3 - \chi_6, \chi_4 + \chi_5 + \chi_6).$$

By Proposition 4.3, one has

$$\partial_K(R_n) = (-1, -\frac{1}{2}(\sqrt{d} + \sqrt{m}), -1, \frac{\sqrt{d} - \sqrt{m}}{2}, -1, \frac{\sqrt{d} - \sqrt{m}}{2}) \in \oplus_{i=1}^{6} K^\times / K^{\times n}.$$

Since

$$\overline{l_5(1,-1)} = \overline{l_1(1,-1)} + \overline{l_4(1,-1)} - \overline{l_2(1,-1)} \text{ and } \overline{l_6(1,-1)} = \overline{l_1(1,-1)} + \overline{l_4(1,-1)} - \overline{l_3(1,-1)}$$

in $\mathrm{Pic}(\overline{U})$ by a similar argument as in the proof of Theorem 3.4, one concludes that

$$\phi(\partial_K(R_n)) = (\frac{\sqrt{d} - \sqrt{m}}{2}, \frac{\sqrt{d} + \sqrt{m}}{2}, \frac{\sqrt{d} + \sqrt{m}}{2}, -(\frac{\sqrt{d} - \sqrt{m}}{2})^2) \in \oplus_{i=1}^{4} K^\times / K^{\times n}$$

By Theorem 4.2, $R_n \in \mathrm{Br}(V)$ is of order n, since it is of order n by going over to $\bar{k}$. By hypothesis, we have $\mathbb{Z}/n \subset [\mathrm{Br}(U_K)/\mathrm{Br}_1(U_K)][n] \subset \mathrm{Br}(\overline{U})[n] \simeq \mathbb{Z}/n$. The restriction map $\mathrm{Br}(\overline{U})[n] \to \mathrm{Br}(V_{\bar{k}})[n]$ is an isomorphism, and the last group is spanned by the class of R_n, which comes from $R_n \in \mathrm{Br}(V)$. Thus there exist $\mathcal{B} \in \mathrm{Br}(U_K)$ such that R_n and $\mathcal{B}$ have the same image in $\mathrm{Br}(\overline{U})$. Since $R_n, \mathcal{B}$ are both contained in $\mathrm{Br}(V)$, one concludes $R_n - \mathcal{B} \in \mathrm{Br}_1(V)$. Then

$$\phi(\partial_K(R_n - \mathcal{B})) = \phi(\partial_K(R_n))$$

$$= (\frac{\sqrt{d} - \sqrt{m}}{2}, \frac{\sqrt{d} + \sqrt{m}}{2}, \frac{\sqrt{d} + \sqrt{m}}{2}, -(\frac{\sqrt{d} - \sqrt{m}}{2})^2) \in \oplus_{i=1}^{4} K^\times / K^{\times n}$$

is trivial, this implies -1 and $(\sqrt{d} - \sqrt{m})/2 \in K^{\times n}$. □

Lemma 4.5. *Let $K = k(\sqrt{m}, \sqrt{d})$. Suppose that $R_n = (f, g)_{\zeta_n}$ belongs to $\mathrm{Br}(U_K)$. Suppose $\mu_n \subset k$. Then the image of $\mathcal{B} := Cor_{K/k}(R_n) \in \mathrm{Br}(U)$ in $\mathrm{Br}(U)/\mathrm{Br}_1(U) \subset (\mathbb{Z}/n)$ is a cyclic group of order $n_1 = n/gcd(n, [K:k])$.*

Proof. In $\mathrm{Br}(\overline{U})$, one has

$$Res_{k/\bar{k}}(\mathcal{B}) = Res_{k/\bar{k}} \circ Cor_{K/k}(R_n) = \sum_{\sigma} R_n^{\sigma},$$

where σ runs through the embeddings of K into $\bar{k}$. Since $\mu_n \subset k$, one has $R_n^{\sigma} = R_n$ by Proposition 2.1. Therefore $Res_{k/\bar{k}}(\mathcal{B}) = [K:k] \cdot R_n$ in $\mathrm{Br}(\overline{U})$, the proof follows. □

Lemma 4.6. *Let $K = k(\sqrt{m}, \sqrt{d})$. Suppose $\mu_n \subset k$. Let $n_1 = n/gcd(n, [K:k])$.*

1) If -1 and $(\sqrt{d} - \sqrt{m})/2 \in K^{\times n}$, then the element $\mathcal{B} := Cor_{K/k}(R_n)$ belongs to $\mathrm{Br}(U)$ and generates the cyclic subgroup of order n_1 of $\mathrm{Br}(U)/\mathrm{Br}_1(U)$.

2) Suppose n is odd. Then $\mathrm{Br}(U)/\mathrm{Br}_1(U) \supset (\mathbb{Z}/n)$ if and only if $(\sqrt{d} - \sqrt{m})/2 \in K^{\times n}$. In that case, the element $\mathcal{B} := Cor_{K/k}(R_n)$ belongs to $\mathrm{Br}(U)[n]$ and generates the cyclic subgroup of order n of $\mathrm{Br}(U)/\mathrm{Br}_1(U)$.

Proof. 1) Suppose -1 and $(\sqrt{d}-\sqrt{m})/2 \in K^{\times n}$, then $R_n \in \mathrm{Br}(U_K)$ by the computation of residues in Proposition 4.3. By Lemma 4.5, the image of $\mathcal{B} \in \mathrm{Br}(U)$ in $\mathrm{Br}(U)/\mathrm{Br}_1(U)$ is cyclic of order n_1.

2) Suppose n is odd. Then $n = n_1$ and $-1 \in K^{\times n}$. The sufficiency follows from 1). The converse follows from

$$\mathbb{Z}/n \subset \mathrm{Br}(U)/\mathrm{Br}_1(U) \subset \mathrm{Br}(U_K)/\mathrm{Br}_1(U_K) \subset \mathrm{Br}(\overline{U}).$$

and Lemma 4.4. □

Lemma 4.7. *Let $F = k(\sqrt{d})$ and $G = \mathrm{Gal}(F/k)$. Then the natural map $\mathrm{Br}(U) \to \mathrm{Br}(U_F)^G$ is surjective.*

Proof. We may assume that F/k is of degree 2. We know that $F^\times = H^0(U_F, \mathbb{G}_m)$ by Proposition 2.2. This implies

$$H^3(G, H^0(U_F, \mathbb{G}_m)) = H^3(G, F^\times) = H^1(G, F^\times) = 0$$

by periodicity of the cohomology of cyclic groups and by Hilbert's theorem 90. The spectral sequence

$$E_2^{p,q} = H^p(G, H^q(U_F, \mathbb{G}_m)) \Rightarrow H^{p+q}(U, \mathbb{G}_m).$$

then gives an exact sequence

$$\mathrm{Br}(U) \to \mathrm{Br}(U_F)^G \to H^2(G, \mathrm{Pic}(U_F)),$$

which by periodicity of the cohomology of cyclic groups for Tate cohomology groups reads

$$\mathrm{Br}(U) \to \mathrm{Br}(U_F)^G \to \hat{H}^0(G, \mathrm{Pic}(U_F)).$$

a) Suppose $F \neq k(\sqrt{m})$. Since $\bar{k}[U]^\times = \bar{k}^\times$, the natural map $\mathrm{Pic}(U_F) \hookrightarrow \mathrm{Pic}(\overline{U})^{g_F}$ is injective (in fact, it is an isomorphism since $U(F) \neq \emptyset$). This implies that $\mathrm{Pic}(U_F)^G \hookrightarrow \mathrm{Pic}(\overline{U})^g$ is injective. Since

$$\mathrm{Pic}(\overline{U})^g = \mathrm{Pic}(U_K)^{\mathrm{Gal}(K/k)} = 0$$

with $K = F(\sqrt{m})$ by (3.20) in the proof of Theorem 3.4, one has $\mathrm{Pic}(U_F)^G = 0$, hence $\hat{H}^0(G, \mathrm{Pic}(U_F)) = 0$.

b) Suppose $F = k(\sqrt{m})$. Let ρ be the generator of G. By the computation in Theorem 3.4 for the case $k(\sqrt{d}) = k(\sqrt{m}) \neq k$, $\mathrm{Pic}(U_F)^G$ is generated by

$$2\overline{l_4(1,1)} + \overline{l_1(1,1)} - \overline{l_2(1,1)} - \overline{l_3(1,1)} = (1+\rho)\overline{l_4(1,1)},$$

hence $\hat{H}^0(G, \mathrm{Pic}(U_F)) = 0$. □

Let $K = k(\sqrt{d}, \sqrt{m})$. Define

$$I = \{n \in \mathbb{N} : \mu_n \subset k \text{ and } -1, \frac{\sqrt{d}-\sqrt{m}}{2} \in K^{\times n}\}. \tag{4.5}$$

If p, q are coprime integers, then $\mu_{pq} \subset k$ if and only if $\mu_p \subset k$ and $\mu_q \subset k$. Similarly, for p and q coprime integers, and $\rho \in K^*$, one has $\rho \in K^{\times pq}$ if and only if $\rho \in K^{\times p}$ and $\rho \in K^{\times q}$. Going over to primary components, one concludes that if p, q are integers in I, then the least common multiple $[p, q]$ of p and q is in I. Therefore I is a directed set with respect to divisibility. The following theorem is the main result of this section.

Theorem 4.8. *Let $K = k(\sqrt{d}, \sqrt{m})$. Let*

$$I = \{n \in \mathbb{N} : \mu_n \subset k \textit{ and } -1, \frac{\sqrt{d}-\sqrt{m}}{2} \in K^{\times n}\}.$$

Then

$$\mathrm{Br}(U)/\mathrm{Br}_1(U) \cong \varinjlim_{n \in I} \mathbb{Z}/n.$$

In particular, if I is finite, for instance if k is a number field, then

$$\mathrm{Br}(U)/\mathrm{Br}_1(U) \cong \mathbb{Z}/N$$

where N is the biggest integer in I.

Proof. One has $\mathrm{Br}(U)/\mathrm{Br}_1(U) \subset \mathbb{Q}/\mathbb{Z}(-1)^g$ by Proposition 2.1. Hence $\mathrm{Br}(U)/\mathrm{Br}_1(U)$ is a subgroup of the abelian group $\mathbb{Q}/\mathbb{Z}$. We thus only need to show:

$$\mathbb{Z}/n \subset \mathrm{Br}(U)/\mathrm{Br}_1(U) \quad \text{if and only if} \quad n \in I \tag{4.6}$$

and we only need to show this for n a power of a prime number.

Suppose $\mathrm{Br}(U)/\mathrm{Br}_1(U) \supset \mathbb{Z}/n$. Then $\mu_n \subset k$ by Proposition 2.1 and Lemma 2.4. We have

$$\mathrm{Br}(U)/\mathrm{Br}_1(U) \subset \mathrm{Br}(U_K)/\mathrm{Br}_1(U_K) \subset \mathrm{Br}(\overline{U}).$$

Thus $\mathbb{Z}/n \subset \mathrm{Br}(U)/\mathrm{Br}_1(U)$ implies $\mathbb{Z}/n \subset \mathrm{Br}(U_K)/\mathrm{Br}_1(U_K)$. Then $n \in I$ follows from Lemma 4.4. This establishes one direction of the equivalence (4.6).

Suppose $n \in I$ is an odd integer. Lemma 4.6 gives the reverse direction in (4.6) in a very precise form, namely the image of the element $Cor_{K/k}(R_n) \in \mathrm{Br}(U)[n]$ generates the cyclic subgroup of order n of $\mathrm{Br}(U)/\mathrm{Br}_1(U)$.

We are thus reduced to prove :

$$n = 2^s \text{ and } n \in I \Longrightarrow \mathrm{Br}(U)/\mathrm{Br}_1(U) \supset \mathbb{Z}/n. \tag{4.7}$$

This will be proved in a less explicit manner : we shall prove that there exists an explicit element of order n in $\mathrm{Br}(U)/\mathrm{Br}_1(U)$ which is the image of some nonexplicit element of $\mathrm{Br}(U)$.

Since $-1 \in K^{\times n}$, one concludes that $\mu_{2n} \subset K$. Fix a primitive $2n$-th root of unity $\zeta_{2n} \in K$. Computations as in Proposition 4.3 give :

$$\partial_D(\frac{f}{g}, -\frac{u}{v})_{\zeta_{2n}} = \begin{cases} \frac{\sqrt{d}+\sqrt{m}}{2} \in K(D)^\times/K(D)^{\times 2n} & D = l_2(1,-1) \\ -1 \in K(D)^\times/K(D)^{\times 2n} & D = l_3(1,-1) \\ \frac{\sqrt{m}-\sqrt{d}}{2} \in K(D)^\times/K(D)^{\times 2n} & D = l_4(1,-1) \\ \frac{\sqrt{d}-\sqrt{m}}{2} \in K(D)^\times/K(D)^{\times 2n} & D = l_6(1,-1) \\ 1 \in K(D)^\times/K(D)^{\times 2n} & D \in \{l_1(1,-1), l_5(1,-1)\} \end{cases} \tag{4.8}$$

Let $F = k(\sqrt{d})$. If K/F is of degree 2, let τ be the generator of $\mathrm{Gal}(K/F)$. If F/k is of degree 2, let σ denote the generator of $\mathrm{Gal}(F/k)$.

i) The case $K = k$ follows from Lemma 4.4.

ii) Suppose $[K : k] = 4$. Let

$$\mathcal{B} = Cor_{K/F}(\frac{f}{g}, -\frac{u}{v})_{\zeta_{2n}} + Cor_{K/F}(\frac{u_1}{v_1}, \frac{\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} \in \mathrm{Br}(F(X))$$

where $u_1 = y - 2$ and $v_1 = x + \frac{1}{2}(\sqrt{d}-\sqrt{m})y - z + \sqrt{m}$. Since

$$div(u_1) = L_2 + l_2(1,-1) + l_2(1,1) \quad \text{and} \quad div(v_1) = l_6(1,-1) + \tau(l_4(1,-1)) + l_2(1,1)$$

by Bezout's theorem, one obtains that

$$\partial_D(\frac{u_1}{v_1}, \frac{\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} = \frac{\sqrt{d}-\sqrt{m}}{2} \in K(D)^\times/K(D)^{\times 2n} \tag{4.9}$$

for $D \in \{l_2(1,-1), \tau(l_4(1,-1)), l_6(1,-1)\}$. Since $(\sqrt{d}-\sqrt{m})/2 \in K^{\times n}$, we have

$$-1 = N_{K/F}((\sqrt{d}-\sqrt{m})/2) \in F^{\times n} \quad \text{and} \quad \mu_{2n} \subset F.$$

When D is defined over F, the corestriction map

$$H^1(K(D), \mathbb{Z}/2n) = K(D)^\times/K(D)^{\times 2n} \xrightarrow{Cor_{K/F}} H^1(F(D), \mathbb{Z}/2n) = F(D)^\times/F(D)^{\times 2n}$$

is given by norm. Since the residue maps commute with corestriction, the residues of $\mathcal{B}$ at $D \in \{l_i(1,-1)\}_{i=1}^3$ are trivial by (4.8) and (4.9).

For $i = 4,5,6$, $D \in \{l_i(1,-1)\}$ is not defined over F, one can identify $K(D)$ with $F(\mathcal{D})$ where $\mathcal{D}$ is the integral divisor on X_F image of the divisor D on X_L via the projection map $X_L \to X_F$. We shall say that $\mathcal{D}$ is below D. Then τ induces an isomorphism from $K(\tau D)$ to $F(\mathcal{D})$.

For $\mathcal{D}$ below $l_4(1,-1)$, one has

$$\partial_{\mathcal{D}}(\mathcal{B}) = \frac{\sqrt{m}-\sqrt{d}}{2} \cdot (\frac{\sqrt{d}+\sqrt{m}}{2})^{-1} = (\frac{\sqrt{m}-\sqrt{d}}{2})^2 \in F(\mathcal{D})^\times/F(\mathcal{D})^{\times 2n}$$

by (4.8), (4.9) and the above identification. For $\mathcal{D}$ below $l_6(1,-1)$, one has

$$\partial_{\mathcal{D}}(\mathcal{B}) = 1 \in F(\mathcal{D})^\times/F(\mathcal{D})^{\times 2n}$$

by (4.8), (4.9) and the above identification. Since

$$\frac{\sqrt{d}-\sqrt{m}}{2} \in K^{\times n} \subset K(D)^{\times n} = F(\mathcal{D})^{\times n},$$

one also has $\partial_{\mathcal{D}}(\mathcal{B})$ is trivial in $H^1(F(\mathcal{D}), \mathbb{Z}/2n)$. Therefore $\mathcal{B} \in \mathrm{Br}(U_F)$. Note that $\mu_{2n} \subset F$, then $\mathcal{B}$ is of order n in $\mathrm{Br}(\overline{U})$ by Lemma 4.5 (replacing k by F).

Since we have $\mu_n \subset k$, Proposition 2.1 shows that the Galois group $\mathrm{Gal}(\overline{k}/k)$ acts trivially on the unique subgroup of order n in $\mathrm{Br}(\overline{U})$. This implies that $\mathcal{B} - \mathcal{B}^\sigma \in \mathrm{Br}_1(U_F)$, and $\mathrm{Br}_1(U_F) = \mathrm{Br}(F)$ by Theorem 3.4. Let $A = \mathcal{B} - \mathcal{B}^\sigma \in \mathrm{Br}(F)$.

Case a). Suppose $\mu_{2n} \subset k$. By evaluating $\mathcal{B}$ and $\mathcal{B}^\sigma$ at the special point $(-2,0,\sqrt{d})$ in $U(F)$, one obtains that

$$\begin{aligned} A =& Cor_{K/F}(\frac{-2\sqrt{d}(\sqrt{m}-\sqrt{d})}{-m+\sqrt{md}+2\sqrt{m}}, \frac{-\sqrt{m}}{\sqrt{d}-2})_{\zeta_{2n}} - Cor_{K/F}(\frac{-2\sqrt{d}}{\sqrt{d}-\sqrt{m}+2}, \frac{2}{\sqrt{m}-\sqrt{d}})_{\zeta_{2n}} \\ &+ Cor_{K/F}(\frac{2}{\sqrt{d}-\sqrt{m}+2}, \frac{\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} - Cor_{K/F}(\frac{2}{\sqrt{d}-\sqrt{m}+2}, \frac{-\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} \end{aligned}$$

in $\mathrm{Br}(F)$. Since $(\alpha,\beta)_{\zeta_{2n}} = (\alpha^{-1},\beta^{-1})_{\zeta_{2n}}$ in $\mathrm{Br}(K)$ for $\alpha,\beta \in K^\times$, one has

$$\begin{aligned} &(\frac{-2\sqrt{d}(\sqrt{m}-\sqrt{d})}{-m+\sqrt{md}+2\sqrt{m}}, \frac{-\sqrt{m}}{\sqrt{d}-2})_{\zeta_{2n}} = (-\frac{\sqrt{m}(\sqrt{m}+\sqrt{d}-2)}{4\sqrt{d}}, -\frac{\sqrt{d}-2}{\sqrt{m}})_{\zeta_{2n}} \\ &= (-\frac{\sqrt{m}(\sqrt{m}+\sqrt{d}-2)}{4\sqrt{d}} \cdot (1+\frac{\sqrt{d}-2}{\sqrt{m}})^{-1}, -\frac{\sqrt{d}-2}{\sqrt{m}})_{\zeta_{2n}} = (-\frac{m}{4\sqrt{d}}, -\frac{\sqrt{d}-2}{\sqrt{m}})_{\zeta_{2n}} \end{aligned}$$

by $((1-\alpha)^{-1},\alpha)_{\zeta_{2n}} = 0$ in $\mathrm{Br}(K)$ for any $\alpha \neq 0,1$ in K. Similarly, one has

$$\begin{aligned} &(\frac{-2\sqrt{d}}{\sqrt{d}-\sqrt{m}+2}, \frac{2}{\sqrt{m}-\sqrt{d}})_{\zeta_{2n}} = (\frac{\sqrt{d}-\sqrt{m}+2}{-2\sqrt{d}}, \frac{\sqrt{m}-\sqrt{d}}{2})_{\zeta_{2n}} \\ &= (\frac{\sqrt{d}-\sqrt{m}+2}{-2\sqrt{d}} \cdot (1-\frac{\sqrt{m}-\sqrt{d}}{2})^{-1}, \frac{\sqrt{m}-\sqrt{d}}{2})_{\zeta_{2n}} = (\frac{-1}{\sqrt{d}}, \frac{\sqrt{m}-\sqrt{d}}{2})_{\zeta_{2n}}. \end{aligned}$$

Therefore

$$\begin{aligned} A =& Cor_{K/F}(-\frac{m}{4\sqrt{d}}, -\frac{\sqrt{d}-2}{\sqrt{m}})_{\zeta_{2n}} - Cor_{K/F}(\frac{-1}{\sqrt{d}}, \frac{\sqrt{m}-\sqrt{d}}{2})_{\zeta_{2n}} \\ &+ Cor_{K/F}(\frac{2}{\sqrt{d}-\sqrt{m}+2}, (\frac{\sqrt{d}-\sqrt{m}}{2})^2)_{\zeta_{2n}} \\ =&(-\frac{m}{4\sqrt{d}}, \frac{m-4\sqrt{d}}{-m})_{\zeta_{2n}} + (-\frac{1}{\sqrt{d}}, -1)_{\zeta_{2n}}. \end{aligned}$$

Since $(\alpha,-\alpha)_{\zeta_{2n}} = 0$ in $\mathrm{Br}(F)$ for any $\alpha \in F^\times$, one has

$$\begin{aligned} &(-\frac{m}{4\sqrt{d}}, \frac{m-4\sqrt{d}}{-m})_{\zeta_{2n}} = (-\frac{m}{4\sqrt{d}}, \frac{m}{4\sqrt{d}} \cdot \frac{m-4\sqrt{d}}{-m})_{\zeta_{2n}} = (-\frac{m}{4\sqrt{d}}, 1-\frac{m}{4\sqrt{d}})_{\zeta_{2n}} \\ &= (-1, 1-\frac{m}{4\sqrt{d}})_{\zeta_{2n}} = (-1, \frac{(\sqrt{d}-2)^2}{-4\sqrt{d}})_{\zeta_{2n}} = (-1, \frac{1}{-4\sqrt{d}})_{\zeta_{2n}} = (-1, -\frac{1}{\sqrt{d}})_{\zeta_{2n}}. \end{aligned}$$

One concludes that $A = 0$.

Case b). Suppose $\mu_{2n} \not\subset k$. Since $\mu_{2n} \subset F$ and $[F:k]=2$, one has $F = k(\zeta_{2n})$. Note that $\mu_n \subset k$, one gets $\zeta_{2n}^\sigma = \zeta_{2n}^{1+n}$. Considering the action of Galois group on the cyclic algebra $(a,b)_{\zeta_{2n}}$ for $a,b \in K(U)^\times$, one has

$$(a,b)_{\zeta_{2n}}^\sigma = (a^\sigma, b^\sigma)_{\zeta_{2n}^\sigma}.$$

Since the character given by b^σ and ζ_{2n}^σ is the $(n+1)$-th power of the character given by b^σ and ζ_{2n}, one concludes

$$(a^\sigma, b^\sigma)_{\zeta_{2n}^\sigma} = (n+1)(a^\sigma, b^\sigma)_{\zeta_{2n}}$$

in $\mathrm{Br}(K(U))$.

By evaluating $\mathcal{B}$ and $\mathcal{B}^\sigma$ at the special point $(-2, 0, \sqrt{d})$ in $U(F)$, one concludes that

$$\begin{aligned} A =& Cor_{K/F}(\frac{-2\sqrt{d}(\sqrt{m}-\sqrt{d})}{-m+\sqrt{md}+2\sqrt{m}}, \frac{-\sqrt{m}}{\sqrt{d}-2})_{\zeta_{2n}} - (1+n)Cor_{K/F}(\frac{-2\sqrt{d}}{\sqrt{d}-\sqrt{m}+2}, \frac{2}{\sqrt{m}-\sqrt{d}})_{\zeta_{2n}} \\ &+ Cor_{K/F}(\frac{2}{\sqrt{d}-\sqrt{m}+2}, \frac{\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} - (1+n)Cor_{K/F}(\frac{2}{\sqrt{d}-\sqrt{m}+2}, \frac{-\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} \end{aligned}$$

in $\mathrm{Br}(F)$. Since

$$\frac{2}{\sqrt{m}-\sqrt{d}}, \quad \frac{-\sqrt{d}-\sqrt{m}}{2} \in K^{\times n},$$

one obtains that

$$n(\frac{-2\sqrt{d}}{\sqrt{d}-\sqrt{m}+2}, \frac{2}{\sqrt{m}-\sqrt{d}})_{\zeta_{2n}} = n(\frac{2}{\sqrt{d}-\sqrt{m}+2}, \frac{-\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}} = 0$$

in $\mathrm{Br}(K)$. Therefore the computation in Case a) is still available and $A = 0$.

We have thus proves $\mathcal{B} \in \mathrm{Br}(U_F)^G$. By Lemma 4.7, this implies that $\mathcal{B}$ is in the image of $\mathrm{Br}(U) \to \mathrm{Br}(U_F)$.

iii) Suppose $m \in k^{\times 2}$ and $d \notin k^{\times 2}$. Then $F = K$. Let $\mathcal{B} = R_n$ in Theorem 4.2. Then $\mathcal{B} \in \mathrm{Br}(U_K) = \mathrm{Br}(X_F)$ by Lemma 4.4. There is

$$A \in \mathrm{Br}_1(U_F) = \mathrm{Br}(F) \quad \text{such that} \quad R_n^\sigma = R_n + A$$

by Proposition 2.1 and Theorem 3.4. By evaluating R_n and R_n^σ at the special point $(-\sqrt{m}, 0, 0)$, one concludes that $A = 0$. Therefore $R_n \in \mathrm{Br}(U_F)^G$ and the result again follows from Lemma 4.7.

iv) Suppose $d \in k^{\times 2}$ and $m \notin k^{\times 2}$. Let

$$\mathcal{B} = Cor_{K/k}(\frac{f}{g}, -\frac{u}{v})_{\zeta_{2n}} + Cor_{K/k}(\frac{u_1}{v_1}, \frac{\sqrt{d}-\sqrt{m}}{2})_{\zeta_{2n}}$$

where

$$u_1 = y - 2 \quad \text{and} \quad v_1 = x + \frac{1}{2}(\sqrt{d}-\sqrt{m})y - z + \sqrt{m}.$$

The result follows from the same computation as in Case ii).

v) Suppose $md \in k^{\times 2}$ and $d \notin k^{\times 2}$. Recall that $n > 1$ is a power of 2, one has $\frac{\sqrt{d}-\sqrt{m}}{2} = (r + s\sqrt{d})^2$ by the definition of I, where $r, s \in k^\times$. Therefore we have $r^2 + ds^2 = 0$. This implies $\sqrt{-d} \in k$. Therefore $F = k(\sqrt{d}) = k(\sqrt{-1}) \neq k$, hence $\sqrt{-1} \notin k$, so $n = 2$ by the definition of I.

Let $\mathcal{B} = R_2$ in Theorem 4.2. Then $\mathcal{B} \in \mathrm{Br}(U_F)$ by Lemma 4.4. There is

$$A \in \mathrm{Br}_1(U_F) = \mathrm{Br}(F) \quad \text{such that} \quad R_2^\rho = R_2 + A$$

by Proposition 2.1 and Theorem 3.4, where ρ is the generator of $\mathrm{Gal}(F/k)$. By evaluating R_2 and R_2^σ at the special point $(-2, 0, \sqrt{d})$ and a similar computation as in case ii), one concludes

$$\begin{aligned}
A =& -(\frac{-2\sqrt{d}(\sqrt{m}-\sqrt{d})}{-m+\sqrt{md}+2\sqrt{m}}, \frac{\sqrt{m}}{\sqrt{d}-2})_{-1} + (\frac{-2\sqrt{d}}{\sqrt{d}+\sqrt{m}+2}, \frac{2}{\sqrt{m}+\sqrt{d}})_{-1} \\
=& -(\frac{-2\sqrt{d}(\sqrt{m}-\sqrt{d})}{-m+\sqrt{md}+2\sqrt{m}}, \frac{-\sqrt{m}}{\sqrt{d}-2})_{-1} + 0 = -(-\frac{m}{4\sqrt{d}}, -\frac{\sqrt{d}-2}{\sqrt{m}})_{-1} \\
=& -(-\frac{m}{4\sqrt{d}}, \frac{(\sqrt{d}-2)^2}{m})_{\zeta_4} = -(-\frac{m}{4\sqrt{d}}, \frac{m-4\sqrt{d}}{m})_{\zeta_4} = (-\frac{4\sqrt{d}}{m}, 1-\frac{4\sqrt{d}}{m})_{\zeta_4} \\
=&(-1, 1-\frac{4\sqrt{d}}{m})_{\zeta_4} = (-1, \frac{(\sqrt{d}-2)^2}{m})_{\zeta_4}
\end{aligned}$$

in $\mathrm{Br}(F)$, where ζ_4 is a primitive 4-th root of unity. Note that $\sqrt{-1}, \sqrt{m} \in F$, hence we have $A = 0$. Therefore $R_2 \in \mathrm{Br}(U_F)^G$ and the result follows from Lemma 4.7. □

Corollary 4.9. *Suppose that k is a field with an ordering. Then $\mathrm{Br}(U)/\mathrm{Br}_1(U) \subset \mathbb{Z}/2$. If d is positive in that ordering, then $\mathrm{Br}_1(U) = \mathrm{Br}(U)$.*

Proof. Let $n \in I$. By (the easy part of the proof of) Theorem 4.8, we have $\mu_n \subset k$ and $-1 \in K^{\times 2}$. If k can be ordered, this implies $n \in \{1, 2\}$. If d is positive with respect to an ordering, then d and $m = d + 4$ are both positive in the real closure R of k with respect to this ordering. There is an embedding $K \subset R$. Thus -1 is not a square in K. This implies $I = \{1\}$. □

Corollary 4.10. *Let k be a field of characteristic zero. If $-1 \notin k^{\times 2}$ and $-d \notin k^{\times 2}$, then the quotient $\mathrm{Br}(U)/\mathrm{Br}_1(U)$ has no 2-primary part. If moreover k admits an ordering then $\mathrm{Br}_1(U) = \mathrm{Br}(U)$.*

Proof. The hypothesis is equivalent to $\sqrt{-1} \notin k(\sqrt{d})$. Suppose $2 \in I$. By (the easy part of the proof of) Theorem 4.8, we then have

$$\sqrt{-1} \in K^\times \quad \text{and} \quad \frac{\sqrt{d}-\sqrt{m}}{2} \in K^{\times 2}$$

with $K = k(\sqrt{m}, \sqrt{d})$. Since $\sqrt{-1} \notin k(\sqrt{d})$, one has $k(\sqrt{d}) \neq K$ and $\sqrt{m} \notin k(\sqrt{d})$. Therefore

$$-1 = N_{K/k(\sqrt{d})}(\frac{\sqrt{d}-\sqrt{m}}{2}) \in k(\sqrt{d})^{\times 2}$$

which contradicts $-d \notin k^{\times 2}$. □

Remark 4.11. In the case $k = \mathbb{Q}$, we find that $\mathrm{Br}_1(U) = \mathrm{Br}(U)$ as soon as $-d \notin \mathbb{Q}^{\times 2}$.

Remark 4.12. Suppose $-1 \notin k^{\times 2}$. There exist $\gamma, \delta \in k^{\times}$ be such that $\gamma^2+\delta^2=1$ and $\gamma \neq \pm\delta$. Set $u=4\gamma\delta$ and $v=2(\delta^2-\gamma^2)$. Then $u^2+v^2=4$. Let $d=-u^2$ and $m=4-u^2=v^2$. Fix $i:=\sqrt{-1}\in \bar{k}$. Then $K=k(\sqrt{d},\sqrt{m})=k(i)$ is of degree 2 over k, contains $\sqrt{-1}$ and we have:

$$(\sqrt{d}-\sqrt{m})/2=(ui-v)/2=\gamma^2-\delta^2+2\gamma\delta i=(\gamma+\delta i)^2\in K^{\times 2}.$$

For $U=U_m$, the hard part of the proof of Theorem 4.8 then gives $\mathbb{Z}/2\subset \mathrm{Br}(U)/\mathrm{Br}_1(U)$. If $k=\mathbb{Q}$, it then gives $\mathrm{Br}(U)/\mathrm{Br}_1(U)=\mathbb{Z}/2$.

Remark 4.13. Suppose $m\in k^{\times 2}$ and $d\notin k^{\times 2}$, so that $K=k(\sqrt{d})\neq k$. Suppose $n\in I$ is a power of 2. If $n=2$, assume $\mu_4\subset k$. Then we can write down an explicit element in $\mathrm{Br}(U)$ whose image generates the cyclic subgroup of order n of $\mathrm{Br}(U)/\mathrm{Br}_1(U)$.

Indeed, by assumption we have $\mu_n\subset k$ and $-1,\alpha\in K^{\times n}$ where $\alpha=(\sqrt{d}-\sqrt{m})/2$. Let

$$\chi_1\in H^1(\mathrm{Gal}(k(\mu_{4n})/k),\mathbb{Q}/\mathbb{Z}) \quad \text{and} \quad \chi_2\in H^1(\mathrm{Gal}(k(\sqrt{d},\sqrt[2n]{\alpha})/k),\mathbb{Q}/\mathbb{Z})$$

such that the restrictions of χ_1 and χ_2 to

$$\mathrm{Gal}(K(\mu_{4n})/K) \quad \text{and} \quad \mathrm{Gal}(k(\sqrt{d},\sqrt[2n]{\alpha})/k(\sqrt{d}))$$

are the respective generators of these groups. Then the element

$$\mathcal{B}=Cor_{K/k}(\frac{f}{g},\frac{u}{v})_{\zeta_{2n}}+((x-2)(y-\sqrt{m})(z-2),\chi_1)+((x-\sqrt{m})(y-2)(z-\sqrt{m}),\chi_2)$$

is in $\mathrm{Br}(U)[2n]$, where ζ_{2n} is a primitive $2n$-th root of unity. Under the assumption $\mu_4\subset k$ if $n=2$, the image of $\mathcal{B}$ is of order n in $\mathrm{Br}(\overline{U})$.

5. Failure of the integral Hasse principle

In this section, we explain that all examples which do not satisfy the Hasse principle in [12] can be explained by integral Brauer-Manin obstruction or by the combination of Brauer-Manin obstruction with the reduction theory.

Given a scheme $\mathcal{U}$ over $\mathbb{Z}$, and $U:=\mathcal{U}\times_{\mathbb{Z}}\mathbb{Q}$, we let $\mathcal{U}(A_{\mathbb{Z}})=\prod_p \mathcal{U}(\mathbb{Z}_p)$, where p runs through all primes and ∞, and $\mathbb{Z}_\infty=\mathbb{R}$. We let

$$\mathcal{U}(A_{\mathbb{Z}})_\bullet=\prod_{p<\infty}\mathcal{U}(\mathbb{Z}_p)\times\pi_0(U(\mathbb{R}))$$

where $\pi_0(U(\mathbb{R}))$ is the set of connected components of $U(\mathbb{R})$. We have the Brauer-Manin pairing

$$\mathcal{U}(A_{\mathbb{Z}})_\bullet\times\mathrm{Br}(U)\to\mathbb{Q}/\mathbb{Z}.$$

The (modified) Brauer-Manin set is the left kernel of this pairing. Note that the Legendre symbol takes values in ± 1 but the Hilbert symbols used below take values 0 or $1/2$ in $\mathbb{Q}/\mathbb{Z}$.

5.1. **Integral Brauer-Manin obstructions.** Let $d \neq 0, -4$ be an integer. Let $\mathcal{U}$ be the scheme over $\mathbb{Z}$ defined by the following equation

$$x^2 + y^2 + z^2 - xyz = d + 4 \tag{5.1}$$

and $U = \mathcal{U} \times_{\mathbb{Z}} \mathbb{Q}$.

Lemma 5.1. *If p is an odd prime with $(p, d) = 1$, then each element in the following set*

$$\{(x \pm 2, d),\ (y \pm 2, d),\ (z \pm 2, d)\} \subset \mathrm{Br}(U)$$

vanishes over $\mathcal{U}(\mathbb{Z}_p)$ and $(x^2 - 4, d) = (y^2 - 4, d) = (z^2 - 4, d)$ vanishes over $U(\mathbb{Q}_p)$. If $d > 0$, these elements vanish over $U(\mathbb{R})$.

Proof. One only needs to consider the case that $(\frac{d}{p}) = -1$. Since (5.1) is equivalent to the following equation

$$(2z - xy)^2 - 4d = (x^2 - 4)(y^2 - 4) \tag{5.2}$$

over $\mathbb{Z}$, one concludes that

$$ord_p(x_p^2 - 4) = ord_p(y_p^2 - 4) = 0$$

for all $M_p = (x_p, y_p, z_p) \in \mathcal{U}(\mathbb{Z}_p)$. By symmetry, one can further obtain

$$ord_p(x_p^2 - 4) = ord_p(y_p^2 - 4) = 0 = ord_p(z_p^2 - 4) = 0$$

for all $M_p = (x_p, y_p, z_p) \in \mathcal{U}(\mathbb{Z}_p)$. This implies that $(x \pm 2, d), (y \pm 2, d), (z \pm 2, d)$ vanish over $\mathcal{U}(\mathbb{Z}_p)$.

If $(x_p, y_p, z_p) \in U(\mathbb{Q}_p) \setminus \mathcal{U}(\mathbb{Z}_p)$, one of $x_p, y_p, z_p \in \mathbb{Q}_p \setminus \mathbb{Z}_p$. Without loss of generality, we assume that $x_p \in \mathbb{Q}_p \setminus \mathbb{Z}_p$. Then $ord_p(x_p^2 - 4)$ is even and $(x_p^2 - 4, d)_p = 0$. The result follows. □

Lemma 5.2. *If $m < 0$, then $|x| > 2, |y| > 2, |z| > 2$ for any $(x, y, z) \in \mathcal{U}_m(\mathbb{R})$.*

Proof. Let $(x, y, z) \in \mathcal{U}_m(\mathbb{R})$. Suppose $|x| \leq 2$. Then

$$m = (y - xz/2)^2 + (1 - x^2/4)z^2 + x^2 \geq 0$$

which contradicts $m < 0$. So $|x| > 2$. Similarly $|y| > 2, |z| > 2$. □

Remark 5.3. Let $f : U_m \to \mathbb{A}^2$ be the morphism defined by projecting (x, y, z) to (x, y). Therefore the image of $U_m(\mathbb{R})$ by f is the subset

$$W := \{(x, y) \in \mathbb{R}^2 : (x^2 - 4)(y^2 - 4) + 4(m - 4) \geq 0\} \subset \mathbb{R}^2.$$

The connected components of $U_m(\mathbb{R})$ are just the preimage of connected components of W by f. The four lines $x = \pm 2$ and $y = \pm 2$ divide the plane $\mathbb{R}^2$ into nine parts. Considering the signature of $(x^2 - 4)(y^2 - 4)$ on the nine parts, we have

$$\#\pi_0(U_m(\mathbb{R})) = \#\pi_0(W) = \begin{cases} 1 & \text{if } m \geq 4 \\ 5 & \text{if } 0 \leq m < 4 \\ 4 & \text{if } m < 0. \end{cases}$$

All connected components of $U_m(\mathbb{R})$ are unbounded except the connected component defined by $|x|, |y| < 2$ when $0 \leq m < 4$, and the bounded connected component becomes a single point

$(0,0,0)$ when $m = 0$. If $m < 4$, Γ permutes the four unbounded components transitively. Full details are given in section 7.

We consider the scheme $\mathcal{U}_m$ over $\mathbb{Z}$ defined by the equation

$$x^2 + y^2 + z^2 - xyz = m \quad \text{ with } m \neq 0, 4. \tag{5.3}$$

Let $U_m = \mathcal{U}_m \times_{\mathbb{Z}} \mathbb{Q}$. Then $\mathrm{Br}_1(U_m)/\mathrm{Br}_0(U_m)$ is generated by

$$\{\mathcal{B}_1 = (x-2, d), \mathcal{B}_2 = (y-2, d), \mathcal{B}_3 = (z-2, d)\}$$

by Theorem 3.4.

Let $B = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$. One can define the evaluation of B over $\mathcal{U}_m(\mathbb{Z}_p)$ by

$$B(M_p) = (\mathcal{B}_1(M_p), \mathcal{B}_2(M_p), \mathcal{B}_3(M_p)) \in (\mathbb{Q}/\mathbb{Z})^3$$

for $M_p \in \mathcal{U}_m(\mathbb{Z}_p)$ and

$$B(\mathcal{U}_m(\mathbb{Z}_p)) = \{B(M_p) : \ M_p \in \mathcal{U}_m(\mathbb{Z}_p)\} \subset (\mathbb{Q}/\mathbb{Z})^3$$

for $p \leq \infty$. By the symmetry of the coordinates of (5.3), the symmetric group S_3 acts on $B(\mathcal{U}_m(\mathbb{Z}_p))$ by coordinate permutation.

Lemma 5.4. *If* $m \equiv 1 \bmod 8$*, then*

$$B(\mathcal{U}_m(\mathbb{Z}_2)) = \{(1/2, 1/2, 0), (1/2, 0, 1/2), (0, 1/2, 1/2)\}.$$

Proof. Since $m \equiv 1 \bmod 8$, one obtains that $d \equiv 5 \bmod 8$ and there is one and only one coordinate of any point in $\mathcal{U}_m(\mathbb{Z}_2)$ belonging to $\mathbb{Z}_2^\times$ by (5.3). The remaining two coordinates belong to $4\mathbb{Z}_2$ by (5.3). The result follows from the straightforward computation of the Hilbert symbols and the symmetry of the coordinates. □

The following lemma corrects [15, Proposition 5.4].

Lemma 5.5. *If* $\mathrm{ord}_p(d)$ *is odd for* $p = 3$ *and* 5*, then*

$$B(\mathcal{U}_m(\mathbb{Z}_p)) = \begin{cases} \{(1/2,0,0),(0,1/2,0),(0,0,1/2)\} & \text{for } p = 3 \text{ and } \mathrm{ord}_3(d) = 1 \\ (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^3 & \text{for } p = 3 \text{ and } \mathrm{ord}_3(d) \geq 3 \\ (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^3 \setminus (0,0,0) & \text{for } p = 5 \text{ and } \mathrm{ord}_5(d) = 1 \\ (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^3 & \text{for } p = 5 \text{ and } \mathrm{ord}_5(d) \geq 3. \end{cases}$$

Proof. Case i) $p = 3$ and $ord_3(d) = 1$. Since (5.3) is equivalent to

$$(x^2-4)(y^2-4) = (2z - xy)^2 - 4d \tag{5.4}$$

and its coordinate permutation, any point in $\mathcal{U}(\mathbb{Z}_3)$ must have two coordinates in $3\mathbb{Z}_3$ and the remaining coordinate in $\mathbb{Z}_3^\times$ by (5.4). Without loss of generality, we assume $x, y \in 3\mathbb{Z}_3$ and $z \in \mathbb{Z}_3^\times$. Therefore

$$(x-2, d)_3 = (y-2, d)_3 = 0 \text{ and } (x+2, d)_3 = 1/2.$$

By (3.24), one has $(z-2, d)_3 = 1/2$, hence $B((x, y, z)) = (0, 0, 1/2)$. The result follows from the permutation of coordinates.

Case ii) $p = 3$ and $ord_3(d) \geq 3$. Let $d = 3^{2n+1}d_0$ with $d_0 \in \mathbb{Z}_3^\times$ and $n \geq 1$.

By Hensel's lemma, there is $\xi \in \mathbb{Z}_3^\times$ such that
$$4\xi + 3^{2n+1}\xi^2 = d_0.$$
This implies that $(3^{2n+1}\xi, d)_3 = (3\xi, d)_3 = (3d_0, d)_3 = (3d_0, 3d_0)_3 = (-1, 3d_0)_3 = 1/2$. Then
$$M_3 = (0, 0, 2 + 3^{2n+1}\xi) \in \mathcal{U}_m(\mathbb{Z}_3) \quad \text{and} \quad B(M_3) = (0, 0, 1/2).$$
For any $a \in \mathbb{Z}_3^\times$, there is $\xi \in \mathbb{Z}_3^\times$ such that
$$\xi^2 - (4a + 3a^2)\xi = 3^{2n-1}d_0$$
by Hensel's lemma. This implies that
$$\xi \in a(\mathbb{Z}_3^\times)^2 \quad \text{and} \quad (3\xi, d)_3 = (3a, d)_3 = (-ad_0, 3d_0)_3.$$
Take
$$M_3 = (2 + 3\xi, 2 + 3a, 2 + 3a) \in \mathcal{U}_m(\mathbb{Z}_p).$$
Then
$$B(M_3) = \begin{cases} (0, 0, 0) & \text{if } ad_0 \in 2 + 3\mathbb{Z}_3 \\ (1/2, 1/2, 1/2) & \text{if } ad_0 \in 1 + 3\mathbb{Z}_3 \end{cases}.$$
Since there is $\xi \in \mathbb{Z}_3^\times$ such that
$$\xi^2 + d_0(4 - 3d_0)\xi = 3^{2n-1}d_0$$
by Hensel's lemma, one obtains that
$$-\xi \in d_0(\mathbb{Z}_3^\times)^2 \quad \text{and} \quad (3\xi, d)_3 = (-3d_0, 3d_0)_3 = 0.$$
Then
$$M_3 = (-2 + 3d_0, -2 + 3d_0, 2 + 3\xi) \in \mathcal{U}_m(\mathbb{Z}_3) \quad \text{and} \quad B(M_3) = (1/2, 1/2, 0).$$
The result follows from the permutation of coordinates.

Case iii) $p = 5$ and $\mathrm{ord}_5(d) = 1$. One can use the lifting of smooth points of $\mathcal{U}_m(\mathbb{Z}/5)$ as in [15, Proposition 5.4] to show that B can take all possible values over $\mathcal{U}_m(\mathbb{Z}_5)$ except $(0, 0, 0)$. We prove $(0, 0, 0) \notin B(\mathcal{U}_m(\mathbb{Z}_5))$.

By (5.4), there is at most one coordinate of a point in $\mathcal{U}_m(\mathbb{Z}_5)$ which is congruent to 3 mod 5. If that is the case, the sum of the two remaining coordinates is congruent to 0 mod 5 as one sees by reducing (5.3) over $\mathbb{Z}/5$. By inspecting cases, one sees that Therefore B cannot take the value $(0, 0, 0)$ over such points.

By (5.4), there is at most one coordinate of a point in $\mathcal{U}_m(\mathbb{Z}_5)$ which is congruent to 2 mod 5. If that is the case, both remaining coordinates are congruent to 1 or 4 mod 5 simultaneously as one sees by reducing (5.3) over $\mathbb{Z}/5$. One only needs to show that B cannot take the value $(0, 0, 0)$ when both remaining coordinates are congruent 1 mod 5. Without loss of generality, we assume that $(x_5, y_5, z_5) \in \mathcal{U}_m(\mathbb{Z}_5)$ satisfies $x_5 \equiv y_5 \equiv 1 \bmod 5$ and $z_5 \equiv 2 \bmod 5$. Since $(x_5 - 2, d)_5 = (y_5 - 2, d)_5 = 0$, one obtains that $(z_5 + 2, d)_5 = 0$ by (3.23). By Proposition 3.2, one hass
$$(x_5^2 - 4, d)_5 = (y_5^2 - 4, d)_5 = (z_5^2 - 4, d)_5 = 1/2.$$
This implies that $(z_5 - 2, d)_5 = 1/2$.

This only remaining possibility which one needs to consider is that all coordinates of the points in $\mathcal{U}_m(\mathbb{Z}_5)$ are congruent 1 mod 5. This is impossible as one sees by reducing (5.3) over $\mathbb{Z}/5$.

Case iv) $p = 5$ and $ord_5(d) \geq 3$. One only needs to show $(0,0,0) \in B(\mathcal{U}_m(\mathbb{Z}_5))$. Let $d = 5^{2n+1}d_0$ with $(d_0, 5) = 1$ and $n \geq 1$. There is $\xi \in \mathbb{Z}_5^\times$ such that

$$\xi^2 + d_0(4 - 5d_0)\xi = 5^{2n-1}d_0$$

by Hensel's lemma. This implies that $\xi \equiv -d_0 \bmod 5$ and $(5\xi, d)_5 = (-5d_0, 5d_0)_5 = 0$. Then

$$M_5 = (2 + 5\xi, -2 + 5d_0, -2 + 5d_0) \in \mathcal{U}_m(\mathbb{Z}_5) \quad \text{and} \quad B(M_5) = (0,0,0)$$

as required. ☐

The following Proposition extends [12, Prop.8.1(i), Prop. 8.2], which only involve elements in $\mathrm{Br}(X)$.

Proposition 5.6. *Let $\mathcal{U}$ be the scheme over $\mathbb{Z}$ given by*

$$x^2 + y^2 + z^2 - xyz = 4 + rv^2 \tag{5.5}$$

where $r \in \mathbb{Z}$ is one of $2, -2, -3, 12, -12$ and all prime factors of v are congruent to

$$\begin{cases} \pm 1 \bmod 8 & \text{when } r = 2 \\ \pm 1 \bmod 12 \quad \text{and} \quad v^2 \equiv 25 \bmod 32 & \text{when } r = 12 \\ 1 \quad \text{or} \quad 3 \bmod 8 & \text{when } r = -2 \\ 1 \bmod 3 & \text{when } r = -3 \\ 1 \bmod 3 & \text{when } r = -12 \end{cases}$$

and $v \neq \pm 1$ when $r = -2, -3$, and

$$B = (x^2 - 4, r) = (y^2 - 4, r) = (z^2 - 4, r) \in \mathrm{Br}_1(U)$$

with $U = \mathcal{U} \times_{\mathbb{Z}} \mathbb{Q}$. Then

$$\mathcal{U}(A_{\mathbb{Z}})^B = \emptyset.$$

Proof. When $r = \pm 2$, for any $M_2 = (x_2, y_2, z_2) \in \mathcal{U}(\mathbb{Z}_2)$, one of x_2, y_2, z_2 is a unit of $\mathbb{Z}_2$ by (5.5). For example, x_2 is a unit, then

$$x_2^2 - 4 \equiv 5 \bmod 8 \quad \text{and} \quad (x_2^2 - 4, \pm 2)_2 = 1/2.$$

Under the assumption $v \neq \pm 1$ when $r = -2$, by Lemma 5.2, $(x_\infty^2 - 4, \pm 2)_\infty = 0$. For $M_p \in \mathcal{U}(\mathbb{Z}_p)$, one has

$$B(M_p) = \begin{cases} 1/2 & \text{if } p = 2, \\ 0 & \text{otherwise} \end{cases}$$

by Lemma 5.1 and the given condition for v. It implies

$$\sum_{p \leq \infty} B(M_p) = 1/2 \neq 0,$$

hence

$$\mathcal{U}(A_{\mathbb{Z}})^B = \emptyset.$$

Suppose $r = -3, \pm 12$. For any local solution $M_3 = (x_3, y_3, z_3) \in \mathcal{U}(\mathbb{Z}_3)$, there is at least one coordinate of M_3 belonging to $3\mathbb{Z}_3$. Otherwise, suppose x_3 and y_3 are in $\mathbb{Z}_3^\times$. Then $(x_3^2-4)(y_3^2-4) \in 9\mathbb{Z}_3$. A contradiction is derived by (5.5). Since $(\alpha^2-4, r)_3 = 1/2$ for $\alpha \in 3\mathbb{Z}_3$, one concludes that $B(M_3) = 1/2$.

When $r = 12$, then $B = (x^2-4, 3) = (y^2-4, 3) = (z^2-4, 3)$. Since $(\frac{3}{p}) = (-1)^{\frac{1}{2}(p-1)}(\frac{p}{3}) = 1$ for any $p \equiv \pm 1 \bmod 12$ by the quadratic reciprocity law, one only needs to consider $p = 2$ by Lemma 5.1. Similarly, since $(\frac{-3}{p}) = (\frac{p}{3}) = 1$ for $p \equiv 1 \bmod 3$, one also reduces to the case $p = 2$ by Lemma 5.2 for $r = -3, -12$.

We claim that for any local solution $M_2 = (x_2, y_2, z_2) \in \mathcal{U}(\mathbb{Z}_2)$, there is at least one coordinate of M_2 in $\mathbb{Z}_2^\times$ when for $r = -3, \pm 12$. This is clear for $r = -3$ since v is odd. Suppose $r = \pm 12$, otherwise, we can write $x_2 = 2\xi, y_2 = 2\eta$ and $z_2 = 2\delta$ with $\xi, \eta, \delta \in \mathbb{Z}_2$ and obtain the following equation

$$(\xi^2-1)(\eta^2-1) = (\delta - \xi\eta)^2 - rv^2/4 \tag{5.6}$$

by (5.5). Since $\pm 3 \notin \mathbb{Z}_2^{\times 2}$, one concludes that ξ and η are in $2\mathbb{Z}_2$ by (5.6). Similarly, $\delta \in 2\mathbb{Z}_2$.

Suppose $r = -12$. The left hand side of (5.6) is $\equiv 1 \bmod 4$, but the right hand side is $\equiv 3 \bmod 4$, it is impossible. So there is at least one coordinate of M_2 in $\mathbb{Z}_2^\times$.

Suppose $r = 12$. Write $\xi = 2\xi_1, \eta = 2\eta_1$ and $\delta = 2\delta_1$ with $\xi_1, \eta_1, \delta_1 \in \mathbb{Z}_2$. One obtains that

$$(4\xi_1^2-1)(4\eta_1^2-1) = 4(\delta_1 - 2\xi_1\eta_1)^2 - 3v^2. \tag{5.7}$$

If all ξ_1, η_1 and δ_1 are in $2\mathbb{Z}_2$, then $-3 \in \mathbb{Z}_2^{\times 2}$ by (5.7), it is impossible.

If two of $\{\xi_1, \eta_1, \delta_1\}$ are in $2\mathbb{Z}_2$ and the remaining one is in $\mathbb{Z}_2^\times$, we can write

$$\xi_1 = 2a, \quad \eta_1 = 2b \quad \text{with} \quad a, b \in \mathbb{Z}_2$$

and $\delta_1 \in \mathbb{Z}_2^\times$ by symmetry. Then

$$4 - 3v^2 \equiv (16a^2-1)(16b^2-1) \equiv \begin{cases} 1 \bmod 32 & \text{when } a \in 2\mathbb{Z}_2,\ b \in 2\mathbb{Z}_2 \\ -15 \bmod 32 & \text{when } ab \in 2\mathbb{Z}_2 \\ 15^2 \bmod 32 & \text{when } ab \in \mathbb{Z}_2^\times \end{cases}$$

by (5.7). This implies that

$$v^2 \equiv \begin{cases} 1 \bmod 32 & \text{when } a \in 2\mathbb{Z}_2,\ b \in 2\mathbb{Z}_2 \\ 17 \bmod 32 & \text{when } ab \in 2\mathbb{Z}_2 \\ 1 \bmod 32 & \text{when } ab \in \mathbb{Z}_2^\times \end{cases}$$

which contradicts the assumption on v.

If two of $\{\xi_1, \eta_1, \delta_1\}$ are in $\mathbb{Z}_2^\times$ and the remaining one is in $2\mathbb{Z}_2$, we can assume $\delta_1 \in 2\mathbb{Z}_2$ and $\xi_1, \eta_1 \in \mathbb{Z}_2^\times$ by symmetry. This implies that $-3 \in (\mathbb{Z}_2^\times)^2$ by (5.7), it is impossible.

If all ξ_1, η_1 and δ_1 are in $\mathbb{Z}_2^\times$, then $3 \cdot 3 \equiv 4 - 3v^2 \bmod 32$ by (5.7). Therefore $v^2 \equiv 9 \bmod 32$ which contradicts the assumption on v.

Therefore the above claim follows, i.e., there is at least one coordinate of M_2 in $\mathbb{Z}_2^\times$. Since $(\alpha_2^2-4,\pm 3)_2=(-3,\pm 3)_2=0$ for $\alpha_2\in\mathbb{Z}_2^\times$, one concludes that B vanishes over $\mathcal{U}(\mathbb{Z}_2)$. For $M_p\in\mathcal{U}(\mathbb{Z}_p)$, one has

$$B(M_p)=\begin{cases}1/2 & \text{if } p=2,\\ 0 & \text{otherwise.}\end{cases}$$

It implies

$$\sum_{p\leq\infty} B(M_p)=1/2\neq 0,$$

hence $\mathcal{U}(A_{\mathbb{Z}})^B=\emptyset$. □

Remark 5.7. The element $B=(x^2-4,r)\in \mathrm{Br}(U)$ actually belongs to $\mathrm{Br}(X)$. Let S be the finite set of primes which divide $2d=2rv^2$. For a prime $p\notin S$, the element B vanishes not only on $\mathcal{U}(\mathbb{Z}_p)$ but also on $\mathcal{U}(\mathbb{Q}_p)$ (Lemma 5.1). From $m>4$ and $m<0$ we get that B vanishes on $U(\mathbb{R})$ (Lemma 5.1 and Lemma 5.2). The above proof then shows that

$$[\prod_{p\in S}\mathcal{U}(\mathbb{Z}_p)\times\prod_{p\notin S}U(\mathbb{Q}_p)]^B$$

is empty. In particular, assuming there are $\mathbb{Q}_p$-points everywhere locally, we get that $U(\mathbb{Q})$ does not meet the open subset of $\prod_{p\in S}\mathcal{U}(\mathbb{Z}_p)$ which is orthogonal to the element B. This represents a lack of weak approximation – which is a stronger result than the same statement for $\mathcal{U}(\mathbb{Z})$.

Remark 5.8. There is an error in the proof of [12, Proposition 8.1 (i)]. A contradiction is derived from the fact that $q\equiv\pm 5 \bmod 8$ and $\{\pm 2\}$ is a quadratic residue modulo q. However, when $q\equiv 3 \bmod 8$, -2 is a quadratic residue modulo q and this is not a contradiction. The corresponding result should be modified. Moreover, the additional requirement that $v\in\{0,\pm 3,\pm 4\} \bmod 9$ can be replaced by the local condition in [12, Proposition 6.1].

Proposition 8.3 in [12] can be improved as follows.

Proposition 5.9. *Let $\mathcal{U}$ be the scheme over $\mathbb{Z}$ given by*

$$x^2+y^2+z^2-xyz=4+20v^2$$

where all prime factors of v are congruent to $\pm 1 \bmod 5$. Then $\mathcal{U}(A_{\mathbb{Z}})^{\mathrm{Br}_1}=\emptyset$ where $U=\mathcal{U}\times_{\mathbb{Z}}\mathbb{Q}$. The smallest $v=11$ with $m=2424$.

Proof. We only consider the following subset A of $\mathrm{Br}_1(U)$

$$\{(x\pm 2,5),(y\pm 2,5),(z\pm 2,5)\}.$$

Then each element $\beta\in A$ vanishes over $\mathcal{U}(\mathbb{Z}_p)$ for $p\neq 2,5$ by Lemma 5.1 and the property $(\frac{5}{p})=(\frac{p}{5})=1$ for $p\equiv\pm 1 \bmod 5$.

Let $M_5=(x_5,y_5,z_5)\in\mathcal{U}(\mathbb{Z}_5)$. By permutation of the coordinates and reduction of the equation

$$(x^2-4)(y^2-4)=(2z-xy)^2-80v^2$$

modulo 25, one sees that there is is at most one coordinate of M_5 which is congruent ± 2 mod 5. by the equation

$$(x^2-4)(y^2-4) = (2z-xy)^2 - 80v^2.$$

We consider

$$V = (x_5^2-4,5)_5 = (y_5^2-4,5)_5 = (z_5^2-4,5)_5.$$

We have two possibilities.

a) At least one of the coordinates is ± 1 mod 5, then $V = 1/2$. Therefore half of the elements in A vanish at M_5 and the other half do not vanish.

b) Two coordinates of M_5 are in $5\mathbb{Z}_5$ and the remaining one is ± 2 mod 5. In this case, $V = 0$. Without loss of generality, we assume $x_5, y_5 \in 5\mathbb{Z}_5$. Then $z_5^2 \equiv 4 + 20$ mod 25 by the given equation. This implies that $z_5 \equiv \pm 7$ mod 25. Therefore

$$(x_5 \pm 2, 5)_5 = (y_5 \pm 2, 5)_5 = 1/2 \quad \text{and} \quad (z_5 \pm 2, 5)_5 = 0.$$

Thus for any point $M_5 \in U(\mathbb{Z}_5)$ at most 3 of the elements in A vanish at M_5.

Let $M_2 = (x_2, y_2, z_2) \in \mathcal{U}(\mathbb{Z}_2)$. Recall that $(2,5)_2 = 1/2$ and $(u,5)_2 = 0$ for any $u \in \mathbb{Z}_2^\times$.

c) If one coordinate, say x_2, belongs to $\mathbb{Z}_2^\times$ then each of $x_2 \pm 2$ is in $\mathbb{Z}_2^\times$ hence $(x_2 \pm 2, 5)_2 = 0$. From the given equation we immediately see that if M_2 has one coordinate in $\mathbb{Z}_2^\times$, then it has at least 2. This then implies that at least 4 elements in A vanish at M_2.

d) If no coordinate of M_2 is in $\mathbb{Z}_2^\times$, then one can write

$$x_2 = 2\xi,\ y_2 = 2\eta,\ z_2 = 2\delta \quad \text{with} \quad \xi, \eta, \delta \in \mathbb{Z}_2$$

and the equation gives

$$(\xi^2-1)(\eta^2-1) = (\delta - \xi\eta)^2 - 5v^2.$$

Since $5 \notin \mathbb{Z}_2^{\times 2}$, one concludes that ξ and η are in $2\mathbb{Z}_2$. Similarly, $\delta \in 2\mathbb{Z}_2$. For each element in the set

$$\{(x \pm 2, 5), (y \pm 2, 5), (z \pm 2, 5)\}$$

the value it takes on M_2 is of the shape $(2.u, 5)_2$ with $u \in \mathbb{Z}_2^\times$. we see that all elements in A take the value $1/2$ at M_2.

It is then an easy matter to see that in whichever combination of one of a), b) with one of c), d), there exists an element $\beta \in B$ such that $\beta(M_5) + \beta(M_2) \neq 0$, hence for any adèle $\{M_p\} \in \mathcal{U}(A_{\mathbb{Z}})$, there exists an element $\beta \in A$ with the property

$$\sum_p \beta(M_p) \neq 0 \in \mathbb{Q}/\mathbb{Z}.$$

$\square$

5.2. **Combination of Brauer-Manin obstruction with the reduction theory.**

Lemma 5.10. *Suppose $m \neq 0, 4$ and $d = m - 4$. Let p be an odd prime such that $ord_p(d)$ is even and positive. Then there is a point $(x_p, y_p, z_p) \in \mathcal{U}_m(\mathbb{Z}_p)$ such that*

$$(x_p - 2, d)_p = (y_p - 2, d)_p = (z_p - 2, d)_p = 0.$$

Proof. There is a smooth point $(a, a, 2)$ (i.e. $a \neq \pm 2$) of the affine variety defined by

$$x^2 + y^2 + z^2 - xyz = 4$$

over the finite field $\mathbb{F}_p$. By Hensel's Lemma, there exists a point $(x_p, y_p, z_p) \equiv (a, a, 2) \mod p$ in $\mathcal{U}_m(\mathbb{Z}_p)$. Therefore

$$(x_p + 2, d)_p = (x_p - 2, d)_p = (y_p - 2, d)_p = 0.$$

By (3.24), one has $(z_p - 2, d)_p = 0$. □

The following proposition points out that [12, Proposition 8.1 ii)] cannot be explained only by Brauer-Manin obstruction.

Proposition 5.11. *Let $\mathcal{U}$ be the scheme over $\mathbb{Z}$ given by*

$$x^2 + y^2 + z^2 - xyz = 4 + 2l^2w^2 \tag{5.8}$$

where w is an odd integer and l is a prime with $l \equiv \pm 3 \mod 8$.

If $lw \equiv \pm 4 \mod 9$, then $\mathcal{U}(A_{\mathbb{Z}})^{\mathrm{Br}} \neq \emptyset$.

Proof. The condition $lw \equiv \pm 4 \mod 9$ implies that $\prod_{p \leq \infty} \mathcal{U}(\mathbb{Z}_p) \neq \emptyset$ by [12, Proposition 6.1]. Since lw is odd, the integer $4 + 2l^2w^2$ is not a square. Therefore $\mathrm{Br}(U)/\mathrm{Br}_0(U)$ is generated by

$$\{(x - 2, 2), (y - 2, 2), (z - 2, 2)\} \tag{5.9}$$

by Corollary 4.9 and Theorem 3.4.

All three elements in (5.9) vanish over $\mathcal{U}(\mathbb{Z}_p)$ and for $p \nmid 2lw$ by Lemma 5.1. By Lemma 5.10, there is a $\mathbb{Z}_p$-point M_p at which all three elements in (5.9) vanish for any $p \mid w$ and $p \neq l$. Therefore, one only needs to construct local points $M_p = (x_p, y_p, z_p)$ for $p = 2, l$.

For $p = 2$, we take $x_2 = y_2 = 1$. There is $z_2 \in \mathbb{Z}_2^\times$ satisfying

$$z^2 - z = 2 + 2l^2w^2 \tag{5.10}$$

by Hensel's Lemma. Then $(x_2 - 2, 2)_2 = (y_2 - 2, 2)_2 = 0$ and

$$(z_2 - 2, 2)_2 = (-1 - r, 2)_2 = \frac{1}{2}$$

where r is the other root of (5.10) with $\mathrm{ord}_2(r) = \mathrm{ord}_2(2 + 2l^2w^2) = 2$.

Over the finite field $\mathbb{F}_l$, we can choose $(a, b, c) \in \mathbb{F}_l \times \mathbb{F}_l^\times \times \mathbb{F}_l^\times$ satisfying $a^2 - 4bc = 2w^2$. Obviously $a - b - c \neq 0$, otherwise we have $(b - c)^2 = 2w^2$, it is impossible since $(\frac{2}{l}) = -1$. Therefore $(b, c, a - b - c)$ is a solution of the equation

$$(x' + y' + z')^2 - 4x'y' = 2w^2 \mod l$$

with $x'y'z' \neq 0$, hence there is a solution $(\alpha_l, \beta_l, \gamma_l)$ of the equation

$$(x' + y' + z')^2 - x'y'(4 + l \cdot z') = 2w^2$$

over $\mathbb{Z}_l$ with $\gamma_l \in \mathbb{Z}_l^\times$ by Hensel's lemma. Then

$$(x_l, y_l, z_l) = (-2+\alpha_l l, -2+\beta_l l, 2+\gamma_l l) \in \mathcal{U}_m(\mathbb{Z}_l)$$

with

$$(x_l-2,2)_l = (y_l-2,2)_l = 0 \text{ and } (z_l-2,2)_l = 1/2.$$

One concludes that

$$(x_p, y_p, z_p)_{p\le\infty} \in \mathcal{U}(A_{\mathbb{Z}})^{\mathrm{Br}}$$

as desired.

□

If $w = 1$ in Proposition 5.11 and l is a sufficiently large prime, one can still prove the equation (5.8) has no integral solutions by combining Brauer-Manin obstruction with the reduction theory as given in [12, Proposition 8.1 ii)]. In fact, we produce more counterexamples.

Proposition 5.12. *The equation*

$$x^2 + y^2 + z^2 - xyz = 4 + rl^2$$

has no integral solution in each of the following cases:

i) $r = 2$ and $l \ge 13$ is a prime with $l \equiv \pm 4 \bmod 9$;

ii) $r = 12$ and $l \ge 37$ is a prime, $l^2 \equiv 25 \bmod 32$ and $1+3l^2$ is not a sum of two squares (e.g. $l = 37, 43, \ldots$);

iii) $r = -2$ and $l \ge 13$ is a prime;

iv) $r = -3$ and $l \ge 17$ is a prime;

v) $r = -12$ and $l \ge 37$ is a prime.

Proof. Let us first check that in each of the above case, $m = 4 + rl^2$ is "generic" as defined in [12], i.e. there is no integral solution with one of the coordinates of absolute value 0, 1 or 2. This is automatic for $m < 0$, hence in cases (iii), (iv), (v). In case i), see the proof of [12, Proposition 8.1]. In case ii), $u^2 + 3v^2 = 4(m-1) = 4(3+12l^2)$ is not solvable over $\mathbb{Z}$ because

$$(-3, 4(3+12l^2))_3 = (-3, 1+4l^2)_3 = (-3,5)_3 = 1/2.$$

By our assumption, $u^2 + v^2 = 4 + 12l^2$ is not solvable over $\mathbb{Z}$. Since $12l^2$ is not a square, $4+12l^2$ is generic.

Let us now suppose that one of the given equations has an integral solution.

For the cases i) and ii), by the reduction theory ([12, Theorem 1.1]), there is an integral solution (x_0, y_0, z_0) satisfying

$$3 \le |x_0| \le |y_0| \le |z_0| \text{ and } |x_0| \le (4+rl^2)^{\frac{1}{3}}.$$

Suppose $r = 2$ and $l \ge 13$, or $r = 12$ and $l \ge 37$. We have $|x_0| + 2 < l$. This implies that $x_0^2 - 4$ has no l-factor. Therefore the Hilbert symbol $(x_0^2-4, r)_l = 0$.

By the purely local computation in proposition 5.6, if $r = 2$, we have $(x_0^2-4, r)_2 = 1/2$. Then we have

$$(x_0^2-4, r)_p = \begin{cases} 0 & \text{if } p \ne 2 \\ 1/2 & \text{if } p = 2; \end{cases}$$

Similarly, by the purely local computation in proposition 5.6, if $r = 12$, we have

$$(x_0^2 - 4, r)_2 = 0 \text{ and } (x_0^2 - 4, r)_3 = 1/2.$$

Therefore

$$(x_0^2 - 4, r)_p = \begin{cases} 0 & \text{if } p \neq 3 \\ 1/2 & \text{if } p = 3. \end{cases}$$

This contradicts the Hilbert reciprocity law.

For the cases iii), iv) and v), by the reduction theory ([12, Theorem 1.1]), there is an integral solution (x_0, y_0, z_0) satisfying

$$3 \leq x_0 \leq y_0 \leq z_0 \leq \frac{1}{2} x_0 y_0.$$

We claim $x_0 < l - 2$. Otherwise, we have

$$\begin{aligned} -rl^2 - 4 =& x_0 y_0 z_0 - x_0^2 - y_0^2 - z_0^2 \geq x_0 y_0 z_0 - x_0^2 - y_0^2 - \frac{1}{2} x_0 y_0 z_0 \\ =& \frac{1}{2} x_0 y_0 z_0 - x_0^2 - y_0^2 \geq \frac{1}{2}(l-2) y_0^2 - 2y_0^2 \\ =& \frac{1}{2}(l-6) y_0^2 \geq \frac{1}{2}(l-6)(l-2)^2. \end{aligned}$$

If $r = -2$ and $l \geq 13$, or $r = -3$ and $l \geq 17$, or $r = -12$ and $l \geq 37$, it is impossible. This implies that $x_0^2 - 4$ has no l-factor and the Hilbert symbol $(x_0^2 - 4, 2)_l = 0$.

By the purely local computation in proposition 5.6, if $r = -2$, we have $(x_0^2 - 4, r)_2 = 1/2$. Then

$$(x_0^2 - 4, r)_p = \begin{cases} 0 & \text{if } p \neq 2 \\ 1/2 & \text{if } p = 2. \end{cases}$$

This contradicts the Hilbert reciprocity law.

By the purely local computation in proposition 5.6, if $r = -3, -12$, one has

$$(x_0^2 - 4, r)_2 = 0 \text{ and } (x_0^2 - 4, r)_3 = 1/2.$$

So

$$(x_0^2 - 4, r)_p = \begin{cases} 0 & \text{if } p \neq 3 \\ 1/2 & \text{if } p = 3. \end{cases}$$

This contradicts the Hilbert reciprocity law. □

The following Lemma is an extension of the previous proposition, one needs this extension in order to get the lower bound in Theorem 5.14.

Lemma 5.13. *Let $r = 2, -2, -3, -12$. Let $a > 0$ be an integer and l be a prime. Let $m = 4 + ra^2l^2$. Suppose $a > 0$ is prime to r and that the Hilbert symbol $(p, r)_p = 0$ for any prime divisor p of a. If $r = 2$, we suppose $al \equiv \pm 4 \bmod 9$.*

Then there exists a positive constant $\theta_r > 0$ only depending on r, such that if $a < \theta_r l^{1/2}$ and l is large enough (depending on θ_r), then the equation

$$x^2 + y^2 + z^2 - xyz = 4 + ra^2l^2$$

has no integral solution.

Proof. Assume there is an integral solution.

i) Suppose $r = 2$. It is clear that $4 + ra^2l^2$ is "generic" by the last part of the proof of [12, Proposition 8.1]. By the reduction theory ([12, Theorem 1.1]), there is an integral solution (x_0, y_0, z_0) satisfying

$$3 \le |x_0| \le |y_0| \le |z_0| \text{ and } |x_0| \le (4 + 2a^2l^2)^{\frac{1}{3}}.$$

If $\theta_2 < 1/\sqrt{2}$, then

$$|x_0| \le (4 + 2a^2l^2)^{\frac{1}{3}} < (4 + 2\theta_2^2 l^3)^{1/3} < l - 2,$$

the last inequality holds for l large enough. This implies that $x_0^2 - 4$ has no l-factor. Therefore the Hilbert symbol $(x_0^2 - 4, 2)_l = 0$. By a similar purely local computations as in Proposition 5.12, the equation

$$x^2 + y^2 + z^2 - xyz = 4 + ra^2l^2$$

has no integral solution by Brauer-Manin obstruction.

ii) Suppose $r = -2, -3, -12$. By the reduction theory ([12, Theorem 1.1]), there is an integral solution (x_0, y_0, z_0) satisfying

$$3 \le x_0 \le y_0 \le z_0 \le x_0y_0/2.$$

We have

$$\begin{aligned} -ra^2l^2 - 4 =& x_0y_0z_0 - x_0^2 - y_0^2 - z_0^2 \ge x_0y_0z_0/2 - x_0^2 - y_0^2 \\ \ge& x_0y_0^2/2 - y_0^2 - x_0^2 \ge x_0 \cdot x_0^2/2 - x_0^2 - x_0^2 = x_0^3/2 - 2x_0^2. \end{aligned}$$

If we choose $0 < \theta_r < 1/\sqrt{-2r}$, then $x_0 < l - 2$ for l large enough. Therefore the Hilbert symbol $(x_0^2 - 4, r)_l = 0$. By a similar purely local computations as in Proposition 5.12, the equation

$$x^2 + y^2 + z^2 - xyz = 4 + ra^2l^2$$

has no integral solution by Brauer-Manin obstruction. □

Recall that $\mathcal{U}_m$ is the affine scheme over $\mathbb{Z}$ defined by the equation

$$x^2 + y^2 + z^2 - xyz = m.$$

The following result improves improves upon the lower bound $\sqrt{N}(\log N)^{-1}$ in [15, Theorem 1.4].

Theorem 5.14. *We have*

$$\#\{m \in \mathbb{Z} : 0 < m < N,\ \mathcal{U}_m(A_\mathbb{Z})^{\mathrm{Br}} \ne \emptyset \ \ \textit{but} \ \ \mathcal{U}_m(\mathbb{Z}) = \emptyset\} \gg \sqrt{N}(\log N)^{-1/2};$$
$$\#\{m \in \mathbb{Z} : -N < m < 0,\ \mathcal{U}_m(A_\mathbb{Z})^{\mathrm{Br}} \ne \emptyset \ \ \textit{but} \ \ \mathcal{U}_m(\mathbb{Z}) = \emptyset\} \gg \sqrt{N}(\log N)^{-1/2}$$

as $N \to +\infty$.

Proof. a) Consider $0 < m < N$. Let l be a prime with $l \equiv 19 \mod 72$. Suppose $m = 4 + 2a^2l^2$ such that a is an odd positive integer satisfying

$$(*): \quad a \equiv \pm 4 \mod 9 \ \text{ and all prime divisors of } a \text{ are congruent to } \pm 1 \mod 8 \ .$$

By the case $r = 2$ of Lemma 5.13, we fix $\theta_2 \leq 1/\sqrt{2}$, if $a < \theta_2 l^{1/2}$ and l is large enough, then the equation

$$x^2 + y^2 + z^2 - xyz = 4 + 2a^2l^2$$

has no integral solution. We have $\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}} \neq \emptyset$ for the above m by Proposition 5.11.

Let

$$N_B = \#\{m \in \mathbb{Z} : 0 < m < N,\ \mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}} \neq \emptyset \ \text{ but } \ \mathcal{U}_m(\mathbb{Z}) = \emptyset\}.$$

By Lemma 5.13, one obtains

$$\begin{aligned} N_B &\gg \sum_{l<\sqrt{N},\ l\equiv 19 \mod 72} \#\{a : a < \theta_2\sqrt{l}, a < \sqrt{N}/l, a \text{ satisfies } (*)\} \\ &\gg \sum_{\theta_2^{-2/3}N^{1/3}<l<N^{1/2},\ l\equiv 19 \mod 72} \#\{a : a < \sqrt{N}/l, a \text{ satisfies } (*)\} \\ &\gg \sum_{\theta_2^{-2/3}N^{1/3}<l<N^{5/12},\ l\equiv 19 \mod 72} \#\{a : a < \sqrt{N}/l, a \text{ satisfies } (*)\} \end{aligned}$$

as $N \to +\infty$. By a well known lemma (e.g., [15, §5.6]), one has

$$\#\{a < N : a \text{ satisfies } (*)\} \sim cN(\log N)^{-1/2} \qquad \text{as } N \to +\infty$$

where $c > 0$ is a constant. So

$$\begin{aligned} N_B &\gg \sum_{\theta_2^{-2/3}N^{1/3}<l<N^{5/12},\ l\equiv 19 \mod 72} \sqrt{N}(\log\sqrt{N} - \log l)^{-1/2} l^{-1} \\ &\geq \sqrt{N}(\log N)^{-1/2} \sum_{\theta_2^{-2/3}N^{1/3}<l<N^{5/12},\ l\equiv 19 \mod 72} l^{-1} \\ &\gg \sqrt{N}(\log N)^{-1/2}(\log\log(N^{5/12}) - \log\log(N^{1/3}) - \log(1 - \frac{2\log(\theta_2)}{\log N}) + O((\log N)^{-1})) \\ &= \sqrt{N}(\log N)^{-1/2}(\log(5/4) + O((\log N)^{-1})) \gg \sqrt{N}(\log N)^{-1/2} \end{aligned}$$

as $N \to +\infty$ by [1, p.156, Ex. 6].

b) Suppose $-N < m < 0$. We apply Lemma 5.13 to the case $r = -2$. Since

$$\sqrt{-1} \notin \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-2}),$$

one has $\mathrm{Br}(U_m) = \mathrm{Br}_1(U_m)$ by Corollary 4.10. The result follows from the similar argument. □

6. Strong approximation always fails

Let $\mathcal{U}_m$ be the scheme over $\mathbb{Z}$ defined by the equation

$$x^2 + y^2 + z^2 - xyz = m. \tag{6.1}$$

The following proposition complements [12, Theorem 1.1 (i)] (see also the discussion below [12, Lemma 2.1]), which goes back Markoff, Hurwitz, Mordell. Theorem 1.1(i) of [12] contains the further information that if $m \in \mathbb{Z}$ is "generic", i.e. there no point on $U_m(\mathbb{Z})$ with $x = 0, 1, 2$, then Γ acts transitively on the solutions and it describes an explicit fundamental set for the set of integral solutions.

Proposition 6.1. *If $m > 0$, then any integral point in $\mathcal{U}_m(\mathbb{Z})$ is Γ-equivalent to an integral point $(x_0, y_0, z_0) \in \mathcal{U}_m(\mathbb{Z})$ such that*

$$3 \le x_0 \le y_0 \le -z_0 \quad \text{or} \quad x_0 = 0, 1, 2. \tag{6.2}$$

Proof. For a given integral point, if its Γ-orbit contains an integral point with the coordinate $x = 0, 1, 2$, then the proof is completed. Therefore, we may assume there is no integral point in the Γ-orbit with $x = 0, 1, 2$. By changing sign of two coordinates and permutation of the coordinates, one only needs to consider the generic case, i.e. Γ-orbits of integral points such that for any point (x, y, z) in the orbit we have

$$\min\{|x|, |y|, |z|\} \ge 3.$$

By changing sign of two coordinates simultaneously, we only need to consider the following two cases: two coordinates of (x, y, z) are positive and the remaining one is negative; or all coordinates of (x, y, z) are positive.

Suppose that there is an integral point $(x, y, z) \in \mathcal{U}_m(\mathbb{Z})$ such that two coordinates of (x, y, z) are positive and the remaining one is negative. Then the result follows from changing sign of two coordinates so that all of them are negative, permutation of the coordinates so as to get $|x| \le |y| \le |z|$ and then change of sign of x and y.

Now we consider an integral point $(x, y, z) \in \mathcal{U}_m(\mathbb{Z})$ such that $3 \le x \le y \le z$.

If $z \le \frac{1}{2}xy$, then one obtains

$$z = \frac{1}{2}(xy - \sqrt{x^2y^2 - 4(x^2 + y^2 - m)})$$

by solving (5.3) for z. This implies that

$$\sqrt{x^2y^2 - 4(x^2 + y^2 - m)} = xy - 2z \le xy - 2y.$$

Therefore one has

$$(x-2)y^2 \le x^2 - m$$

by squaring. Since $x \ge 3$ and $m > 0$, one concludes $y^2 < x^2$. A contradiction is derived.

For any integral point $(x, y, z) \in \mathcal{U}_m(\mathbb{Z})$ with $3 \le x \le y \le z$, we thus have $z > \frac{1}{2}xy$. Applying the Vieta involution, one obtains a new integral point $(x, y, xy - z)$ which satisfies $xy - z < z$. If $xy - z \le 2$, since we are in the generic case we must have $xy - z \le -3$, so we have a situation with two coordinates positive and one negative, and we conclude as above. Suppose $xy - z \ge 3$.

We obtain a new integral point (x_1, y_1, z_1) in the Γ-orbit of (x, y, z) with positive coordinates and $x_1 + y_1 + z_1 < x + y + z$. This process must stop, that is we reach a situation with two coordinates positive and one negative. □

The main result of this section is the following theorem.

Theorem 6.2. *Let m be any integer. Suppose $\mathcal{U}_m(A_{\mathbb{Z}}) \neq \emptyset$. For any finite set S of primes, the image of the natural map $\mathcal{U}_m(\mathbb{Z}) \to \prod_{p\notin S} \mathcal{U}_m(\mathbb{Z}_p)$ is not dense.*

Proof. For any sets of primes $S_1 \supset S_2$, if $\mathcal{U}_m(\mathbb{Z})$ is not dense in $\prod_{p\notin S_1} \mathcal{U}_m(\mathbb{Z}_p)$, then $\mathcal{U}_m(\mathbb{Z})$ is not dense in $\prod_{p\notin S_2} \mathcal{U}_m(\mathbb{Z}_p)$. One can thus enlarge S if necessary.

i) Suppose $m \neq 0$. We may assume S contains 2 and ∞. Let $S' = \{p \text{ prime} : p \mid m\}$ and $R = \prod_{p\in S\setminus S'} p$. Let a be a positive integer prime to m such that

$$a^2R^2 - 2aR - m \geq 0 \text{ and } aR > \sqrt{|m| + 9}. \tag{6.3}$$

Let $d' = a^2R^2 - m$ and $e'_p = ord_p(d')$.

Denote

$$\mathcal{V}_{\epsilon,1,d'} := \prod_{p|d'} \{(x_p, y_p, z_p) \in \mathcal{U}_m(\mathbb{Z}_p) : (x_p, y_p, z_p) \equiv (\epsilon aR, 0, 0) \bmod p^{e'_p}\},$$

$$\mathcal{V}_{\epsilon,2,d'} := \prod_{p|d'} \{(x_p, y_p, z_p) \in \mathcal{U}_m(\mathbb{Z}_p) : (x_p, y_p, z_p) \equiv (0, \epsilon aR, 0) \bmod p^{e'_p}\},$$

$$\mathcal{V}_{\epsilon,3,d'} := \prod_{p|d'} \{(x_p, y_p, z_p) \in \mathcal{U}_m(\mathbb{Z}_p) : (x_p, y_p, z_p) \equiv (0, 0, \epsilon aR) \bmod p^{e'_p}\},$$

where $\epsilon = \pm 1$. Let

$$\mathcal{V}_{\epsilon,d'} = \bigcup_{i=1}^{3} \bigcup_{\epsilon=\pm 1} \mathcal{V}_{\epsilon,i,d'}.$$

It is clear that $\mathcal{V}_{\epsilon,d'}$ is Γ-invariant, where Γ is the group defined in §1. It is clear that d' has no prime factor in $S \cup S'$. Obviously, It is clear that $\mathcal{V}_{\epsilon,d'}$ is Γ-invariant, where Γ is the group defined in §1. Since d' has no prime factor in $S \cup S'$, we can take the local point $(x'_p, 0, 0)$ of $\mathcal{U}_m(\mathbb{Z}_p)$ with $x'_p \equiv aR \bmod p^{e'_p}$ for any $p \mid d'$ by Hensel's lemma. Obviously, $\prod_{p|d'} (x'_p, 0, 0) \in \mathcal{V}_{1,1,d'}$. Therefore $\mathcal{V}_{\epsilon,d'}$ is a non-empty open subset of $\prod_{p|d'} \mathcal{U}_m(\mathbb{Z}_p)$.

a) Suppose $m > 0$. Assume that $\mathcal{U}_m(\mathbb{Z})$ is dense in $\prod_{p\notin S} \mathcal{U}_m(\mathbb{Z}_p)$. Then $\mathcal{U}_m(\mathbb{Z}) \cap \mathcal{V}_{\epsilon,d'} \neq \emptyset$. By Proposition 6.1, there is an integral point $(x_0, y_0, z_0) \in \mathcal{U}_m(\mathbb{Z}) \cap \mathcal{V}_{\epsilon,d'}$ such that

$$3 \leq x_0 \leq y_0 \leq -z_0 \quad \text{ or } \quad x_0 = 0, 1, 2. \tag{6.4}$$

Since $(x_0, y_0, z_0) \in \mathcal{V}_{\epsilon,d'}$, we have

$$(x_0, y_0, z_0) \equiv (\pm aR, 0, 0), (0, \pm aR, 0) \text{ or } (0, 0, \pm aR) \mod d'.$$

If $x_0 > 0$, then

$$x_0 \geq min\{d', d' - aR, aR\} = aR > \sqrt{m + 9} > 3 \tag{6.5}$$

by (6.3). Hence $3 \leq x_0 \leq (m-27)^{1/3}$ by (6.1) and (6.4). Since $\sqrt{m+9} > (m-27)^{1/3}$, a contradiction is derived by (6.5). Therefore

$$x_0 = 0, y_0^2 + z_0^2 = m \text{ and } (y_0, z_0) \equiv (\pm aR, 0) \text{ or } (0, \pm aR) \bmod d',$$

which is impossible by (6.3). Therefore $\mathcal{U}_m(\mathbb{Z})$ is not dense in $\prod_{p|d'} \mathcal{U}_m(\mathbb{Z}_p)$, hence is not dense in $\prod_{p \notin S} \mathcal{U}_m(\mathbb{Z}_p)$.

b) Suppose $m < 0$. Assume that $\mathcal{U}_m(\mathbb{Z})$ is dense in $\prod_{p \notin S} \mathcal{U}_m(\mathbb{Z}_p)$. Then $\mathcal{U}_m(\mathbb{Z}) \cap \mathcal{V}_{\epsilon,d'} \neq \emptyset$. By [12, Theorem 1.1 (ii)], there is an integral point $(x_0, y_0, z_0) \in \mathcal{U}_m(\mathbb{Z}) \cap \mathcal{V}_{\epsilon,d'}$ such that

$$3 \leq x_0 \leq y_0 \leq z_0 \leq x_0 y_0 / 2.$$

By [12, Lemma 2.2], one has $3 \leq x_0 \leq \sqrt{|m|+9}$. Since $(x_0, y_0, z_0) \in \mathcal{V}_{\epsilon,d'}$, we have

$$(x_0, y_0, z_0) \equiv (\pm aR, 0, 0), (0, \pm aR, 0) \text{ or } (0, 0, \pm aR) \quad \bmod d',$$

Since $x_0 > 0$, then

$$x_0 \geq min\{d', d' - aR, aR\} = aR > \sqrt{m+9}$$

by (6.3), which is contradiction to $x_0 \leq \sqrt{|m|+9}$. Therefore $\mathcal{U}_m(\mathbb{Z})$ is not dense in $\prod_{p|d'} \mathcal{U}_m(\mathbb{Z}_p)$, hence is not dense in $\prod_{p \notin S} \mathcal{U}_m(\mathbb{Z}_p)$.

ii) Suppose $m = 0$.

We can choose a prime $l \notin S$ and $l \equiv 1 \bmod 4$. Then we may take $\delta \in \mathbb{Z}_l^\times$ such that $\delta^2 = -1$. Therefore $(\delta l, l, 0) \in \mathcal{U}_0(\mathbb{Z}_l)$. If $\mathcal{U}_0(\mathbb{Z})$ is dense in $\prod_{p \notin S} \mathcal{U}_0(\mathbb{Z}_p)$, then there is an integral point $(x_0, y_0, z_0) \equiv (\delta l, l, 0) \bmod l^2$. Therefore $(x_0, y_0, z_0) \neq (0, 0, 0)$ and x_0, y_0, z_0 are divided by l. Since $\mathcal{U}_0(\mathbb{Z})$ just have two orbits $(0, 0, 0)$ and $(3, 3, 3)$ (see [12, §3.1]), (x_0, y_0, z_0) is contained in the orbit $(3, 3, 3)$. One has $l \mid 3$ since x_0, y_0, z_0 are divisible by l, it is impossible. Therefore $\mathcal{U}_0(\mathbb{Z})$ is not dense in $\prod_{p \notin S} \mathcal{U}_0(\mathbb{Z}_p)$. The proof follows. □

Remark 6.3. We can ask for a lighter version of strong approximation: could it be that the map $\mathcal{U}_m(\mathbb{Z}) \to \mathcal{U}_m(\mathbb{Z}/l)$ is surjective for almost all primes l?

If m is not a square, we have a negative answer under the well-known conjecture that the polynomial $x^2 - m$ can represent infinite many primes. In fact, assume m is not a square and the above conjecture. Then there exist infinitely many primes l for which there is a point in $\mathcal{U}_m(\mathbb{Z}/l)$ of the shape $(\overline{x}, 0, 0)$ with $\overline{x} \neq 0$ which is not in the image of $\mathcal{U}_m(\mathbb{Z}) \to \mathcal{U}_m(\mathbb{Z}/l)$.

Proof. Take $l = a^2 - m$, l is a prime, a is a positive integer prime to m such that

$$a^2 - 2a - m \geq 0 \text{ and } a > \sqrt{|m|+9}. \tag{6.6}$$

We have infinitely many such (l, a) by the above conjecture.

Denote

$$\mathcal{V}_l := \{(\pm\overline{a}, 0, 0), (0, \pm\overline{a}, 0), (0, 0, \pm\overline{a})\},$$

here $\overline{a}$ is the image of a in $\mathbb{Z}/l$. It is clear that $\mathcal{V}_l \subset \mathcal{U}_m(\mathbb{Z}/l)$ is Γ-invariant.

We will assume $m > 0$ ($m < 0$ can be proved similarly). Assume that the map $\mathcal{U}_m(\mathbb{Z}) \to \mathcal{U}_m(\mathbb{Z}/l)$ is surjective. Then there is an integral point $\vec{x} \in \mathcal{U}_m(\mathbb{Z}) \cap \mathcal{V}_l$. By Proposition 6.1 ([12, Theorem 1.1 (ii) and Lemma 2.2] for $m < 0$), there is an integral point $(x_0, y_0, z_0) \in \mathcal{U}_m(\mathbb{Z}) \cap \mathcal{V}_l$ such that

$$3 \leq x_0 \leq y_0 \leq -z_0, \text{ or } x_0 = 0, 1, 2.$$

Since $(x_0, y_0, z_0) \in \mathcal{V}_l$, we have

$$(x_0, y_0, z_0) \equiv (\pm a, 0, 0), (0, \pm a, 0) \text{ or } (0, 0, \pm a) \mod l,$$

hence if $x_0 > 0$, then

$$x_0 \geq min\{l, l-a, a\} = a > \sqrt{m+9} \tag{6.7}$$

by (6.6). Since $\sqrt{m+9} > 3$, one has $x_0 \neq 1, 2$. If $3 \leq x_0 \leq y_0 \leq -z_0$, hence $3 \leq x_0 \leq (m-27)^{1/3}$ by (6.1). But $(x_0, y_0, z_0) \in \mathcal{V}_l$, one has $x_0 > \sqrt{m+9} > (m-27)^{1/3}$ by (6.7), which is a contradiction to $x_0 \leq (m-27)^{1/3}$. Therefore

$$x_0 = 0, y_0^2 + z_0^2 = m \text{ and } (y_0, z_0) \equiv (\pm a, 0) \text{ or } (0, \pm a) \text{ mod } l.$$

Then

$$(y_0, z_0) \equiv (\pm a, 0) \text{ or } (0, \pm a) \text{ mod } l$$

implies $|y_0|$ or $|z_0| \geq min\{l-a, a\} = a$, hence $a^2 \leq m$, it is impossible by (6.6). Therefore $\mathcal{U}_m(\mathbb{Z}) \to \mathcal{U}_m(\mathbb{Z}/l)$ is not surjective. □

Remark 6.4. When comparing the above results with [3], one should note that the failures of strong approximation described here correspond to points $(x_p, y_p, z_p) \in U_m(\mathbb{Z}_p)$ whose reduction modulo p has two coordinates equal to 0, hence which geometrically lift to points whose Γ-orbit is finite.

Lemma 6.5. *Let k be a number field. Let U be a smooth geometrically connected variety over k such that $\mathrm{Br}(U)/\mathrm{Br}_0(U)$ is finite. Let v run through the places of k. Suppose $\mathcal{U}$ is an integral model of U over $\mathfrak{o}_k$ with $\mathcal{U}(A_{\mathfrak{o}_k})^{\mathrm{Br}} \neq \emptyset$, here $\mathcal{U}(A_{\mathfrak{o}_k}) = \prod_{v|\infty} U(k_v) \times \prod_{v<\infty} \mathcal{U}(\mathfrak{o}_v)$. Let $pr_f : \mathcal{U}(A_{\mathfrak{o}_S}) \to \prod_{v<\infty} \mathcal{U}(\mathfrak{o}_v)$ be the natural projection.*

If $\mathcal{U}(\mathfrak{o}_k)$ is dense in $pr_f(\mathcal{U}(A_{\mathfrak{o}_k})^{\mathrm{Br}})$, then there exists a finite set S of places containing ∞_k such that the natural map $\mathcal{U}(\mathfrak{o}_k) \to \prod_{v \notin S} \mathcal{U}_m(\mathfrak{o}_v)$ has dense image.

Proof. Suppose $\mathcal{B}_1, \cdots, \mathcal{B}_n$ generate $\mathrm{Br}(U)/\mathrm{Br}_0(U)$. Then, there exists a finite set S of places containing ∞_k such that $\mathcal{B}_1, \cdots, \mathcal{B}_n$ vanish on $\mathcal{U}(\mathfrak{o}_v)$ for any $v \notin S$. Since $\mathcal{U}(A_{\mathfrak{o}_k})^{\mathrm{Br}} \neq \emptyset$, the natural projection $\mathcal{U}(A_{\mathfrak{o}_k})^{\mathrm{Br}} \to \prod_{v \notin S} \mathcal{U}(\mathfrak{o}_v)$ is surjective. So, if $\mathcal{U}(\mathfrak{o}_k)$ is dense in $pr_f(\mathcal{U}(A_{\mathfrak{o}_k})^{\mathrm{Br}})$, then $\mathcal{U}(\mathfrak{o}_k)$ is dense in $\prod_{v \notin S} \mathcal{U}(\mathfrak{o}_v)$. □

The above lemma is the exact analogue of the well known statement: if X is projective over a number field k and $\mathrm{Br}(X)/\mathrm{Br}(k)$ is finite, and $X(k)$ is dense in $X(A_k)^{\mathrm{Br}}$ nonempty, then weak weak approximation holds for X.

Corollary 6.6. *Suppose $m \neq 0, 4$ and $\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}} \neq \emptyset$. Then $\mathcal{U}_m(\mathbb{Z})$ is not dense in $pr_f(\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}})$, where $pr_f : \mathcal{U}_m(A_{\mathbb{Z}}) \to \prod_{p<\infty} \mathcal{U}_m(\mathbb{Z}_p)$ is the natural projection.*

Proof. By Theorem 3.4 and 4.8, $\mathrm{Br}(U_m)/\mathrm{Br}_0(U_m)$ is finite. The proof follows from Theorem 6.2 and Lemma 6.5. □

Corollary 6.7. *Let $pr_f : \mathcal{U}_m(A_{\mathbb{Z}}) \to \prod_{p<\infty} \mathcal{U}_m(\mathbb{Z}_p)$ be the natural projection. Assume that $\mathcal{U}_m(\mathbb{Z}) \neq \emptyset$.*

If $m > 4$ is not a square, or m is a square with a prime factor congruent 1 mod 4, *or $m < 0$, then $\mathcal{U}_m(\mathbb{Z})$ is Zariski dense but is not dense in $pr_f(\mathcal{U}_m(A_{\mathbb{Z}})^{\mathrm{Br}})$.*

Proof. By [12, §5.2], $\mathcal{U}_m(\mathbb{Z})$ is Zariski dense. The result follows from Corollary 6.6. □

Let X be a smooth, projective and geometrically connected variety over a number field k such that $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ is finite and the Brauer-Manin set of X is not empty. It is well-known that $X(k)$ is Zariski dense in X if $X(k)$ is dense in its Brauer-Manin set. Indeed this then follows from weak weak approximation. Let $S \supset \infty_k$ be a finite subset of Ω_k, $\mathfrak{o}_S$ the ring of S-integers of k. Let U be a smooth geometrically connected variety U over k, $\mathcal{U}$ an integral model over $\mathfrak{o}_S$. We denote

$$\mathcal{U}(A_{\mathfrak{o}_S}) = \prod_{v\in S} U(k_v) \times \prod_{v\notin S} \mathcal{U}(\mathfrak{o}_v)$$

where k_v and $\mathfrak{o}_v$ are the completion of k and $\mathfrak{o}_S$ with respect to $v \in \Omega_k$ respectively. One has the following integral analogy.

Proposition 6.8. *Let U be a smooth geometrically connected variety over a number field k such that $\mathrm{Br}(U)/\mathrm{Br}_0(U)$ is finite. Suppose $\mathcal{U}$ is an integral model of U over $\mathfrak{o}_S$ with $\mathcal{U}(A_{\mathfrak{o}_S})^{\mathrm{Br}} \neq \emptyset$. If $\mathcal{U}(\mathfrak{o}_S)$ is dense in $pr_S(\mathcal{U}(A_{\mathfrak{o}_S})^{\mathrm{Br}})$ where $pr_S : \mathcal{U}(A_{\mathfrak{o}_S}) \to \prod_{v\notin S} \mathcal{U}(\mathfrak{o}_v)$ is the natural projection, then $\mathcal{U}(\mathfrak{o}_S)$ is Zariski dense in $\mathcal{U}$.*

Proof. Let $\mathcal{N}$ be a non-empty Zariski open subset of $\mathcal{U}$ and fix a finite set $B \subset \mathrm{Br}(U)$ generating $\mathrm{Br}(U)/\mathrm{Br}_0(U)$. There is a sufficiently large finite subset $S' \supset S$ of Ω_k such that $\mathcal{N}(\mathfrak{o}_v) \neq \emptyset$, $\mathcal{N}$ is smooth over $\mathfrak{o}_v$ and each element in B vanishes over $\mathcal{U}(\mathfrak{o}_v)$ for all $v \notin S'$.

Take $v_0 \notin S'$. Then the open subset $\mathcal{N}(\mathfrak{o}_{v_0}) \times \prod_{v\notin(S\cup\{v_0\})} \mathcal{U}(\mathfrak{o}_v)$ has non-empty intersection with $pr_S(\mathcal{U}(A_{\mathfrak{o}_S})^{\mathrm{Br}})$ by the assumption. This implies that

$$\mathcal{U}(\mathfrak{o}_{v_0}) \supset \mathcal{U}(\mathfrak{o}_S) \cap \mathcal{N}(\mathfrak{o}_{v_0}) \neq \emptyset.$$

Therefore $\mathcal{N} \cap \mathcal{U}(\mathfrak{o}_S) \neq \emptyset$ as desired. □

As we have seen in this section, the converse of Proposition 6.8 does not hold.

7. Appendix: the real locus

We here provide details for Remark 5.3. The following lemma should be well-known. We provide the proof for convenience of the reader.

Lemma 7.1. *Let X be a topological space. Suppose that $\{X_i\}_{i=1}^n$ is a family of connected subsets of X with $X = \bigcup_{i=1}^n X_i$ such that for any two elements X_i and X_j in $\{X_i\}_{i=1}^n$, there are $X_{k_1}, \cdots, X_{k_s}$ in $\{X_i\}_{i=1}^n$ satisfying*

$$\overline{X}_i \cap \overline{X}_{k_1} \neq \emptyset,\ \overline{X}_{k_1} \cap \overline{X}_{k_2} \neq \emptyset, \cdots, \overline{X}_{k_{s-1}} \cap \overline{X}_{k_s} \neq \emptyset,\ \overline{X}_{k_s} \cap \overline{X}_j \neq \emptyset$$

where $\overline{X}_i, \overline{X}_{k_1}, \cdots, \overline{X}_{k_s}, \overline{X}_j$ are the topological closures of $X_i, X_{k_1}, \cdots, X_{k_s}, X_j$ in X respectively. Then X is connected.

Proof. Suppose that X is not connected. Then X contains a non-empty, open and closed subset $D \neq X$. This implies that there is $1 \le i_0 \le n$ such that $X_{i_0} \not\subset D$. By the connectedness of X_i, one has

$$D \cap \overline{X_i} = \emptyset \quad \text{or} \quad \overline{X_i} \subset D \tag{7.1}$$

for $1 \leq i \leq n$. Since D is not empty, there is $1 \leq j_0 \leq n$ such that $\overline{X}_{j_0} \subset D$ by (7.1). By the assumption, there are $X_{k_1}, \cdots, X_{k_s}$ in $\{X_i\}_{i=1}^n$ satisfying

$$\overline{X}_{j_0} \cap \overline{X}_{k_1} \neq \emptyset,\ \overline{X}_{k_1} \cap \overline{X}_{k_2} \neq \emptyset, \cdots, \overline{X}_{k_{s-1}} \cap \overline{X}_{k_s} \neq \emptyset,\ \overline{X}_{k_s} \cap \overline{X}_{i_0} \neq \emptyset.$$

Applying (7.1), one concludes that $\overline{X}_{i_0} \subset D$. A contradiction is derived. ☐

Recall that U_m is the affine scheme over $\mathbb{R}$ defined by the equation

$$x^2 + y^2 + z^2 - xyz = m. \tag{7.2}$$

Proposition 7.2. *For $m \in \mathbb{R}$, the number of connected components of $U_m(\mathbb{R})$ is given by*

$$\#\pi_0(U_m(\mathbb{R})) = \begin{cases} 1 & \text{for } m \geq 4 \\ 5 & \text{for } 0 \leq m < 4 \\ 4 & \text{for } m < 0. \end{cases}$$

More precisely,

When $m < 0$, the connected components of $U_m(\mathbb{R})$ are

$$\begin{cases} \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ y \geq 2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ y \geq 2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ y \leq -2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ y \leq -2\}. \end{cases}$$

They are unbounded and transitively permuted by Γ.

When $0 \leq m < 4$, the connected components of $U_m(\mathbb{R})$ are

$$\begin{cases} \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ y \geq 2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ y \geq 2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ y \leq -2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ y \leq -2\} \\ \{(x,y,z) \in U_m(\mathbb{R}) : -2 \leq x \leq 2,\ -2 \leq y \leq 2\}. \end{cases}$$

The first four components are unbounded and Γ permutes them transitively. The last component is bounded and reduced to the point $(0,0,0)$ if $m = 0$.

Proof. Since (7.2) is equivalent to

$$(2z - xy)^2 = (x^2 - 4)(y^2 - 4) + 4(m - 4),$$

one concludes that the following closed subsets of $U_m(\mathbb{R})$

$$\begin{cases} D_1 = \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ y \geq 2\} \\ D_2 = \{(x,y,z) \in U_m(\mathbb{R}) : -2 \leq x \leq 2,\ y \geq 2\} \\ D_3 = \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ y \geq 2\} \\ D_4 = \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ -2 \leq y \leq 2\} \\ D_5 = \{(x,y,z) \in U_m(\mathbb{R}) : x \leq -2,\ y \leq -2\} \\ D_6 = \{(x,y,z) \in U_m(\mathbb{R}) : -2 \leq x \leq 2,\ y \leq -2\} \\ D_7 = \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ y \leq -2\} \\ D_8 = \{(x,y,z) \in U_m(\mathbb{R}) : x \geq 2,\ -2 \leq y \leq 2\} \\ D_9 = \{(x,y,z) \in U_m(\mathbb{R}) : -2 \leq x \leq 2,\ -2 \leq y \leq 2\} \end{cases}$$

are connected with $U_m(\mathbb{R}) = \bigcup_{i=1}^{9} D_i$.

When $m \geq 4$, then $D_9 \cap D_i \neq \emptyset$ for $1 \leq i \leq 8$. Therefore $U_m(\mathbb{R})$ is connected by Lemma 7.1.

When $m < 4$, then $D_2 = D_4 = D_6 = D_8 = \emptyset$. Moreover $D_9 = \emptyset$ if and only if $m < 0$. In this case, one obtains that D_1, D_3, D_5, D_7 are the connected components of $U_m(\mathbb{R})$, which are unbounded. Using $(x,y,z) \mapsto (-x,-y,z)$ and $(x,y,z) \mapsto (-x,y,-z)$ one sees that Γ transitively permutes these 4 components. For $0 \leq m < 4$, one has $D_9 \cap D_i = \emptyset$ for $i = 1,3,5,7$. Therefore D_9 is a bounded connected component of $U_m(\mathbb{R})$. □

References

[1] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

[2] S. Bloch and A. Ogus, Gersten's conjecture and the homology of schemes, Ann. Sc. E.N.S. **7** (1974) 181–202.

[3] J. Bourgain, A. Gamburd, P. Sarnak, Markoff triples and strong approximation. C. R. Math. Acad. Sci. Paris **354** (2016), no. 2, 131–135.

[4] J.-L. Colliot-Thélène, Birational invariants, purity and the Gersten conjecture, in *K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras*, AMS Summer Research Institute, Santa Barbara 1992, ed. W. Jacob and A. Rosenberg, Proceedings of Symposia in Pure Mathematics **58**, Part I (1995) 1–64.

[5] J.-L. Colliot-Thélène, A.N. Skorobogatov and Sir Peter Swinnerton-Dyer, Double fibres and double covers: paucity of rational points, Acta Arithmetica LXXIX.2 (1997) 113–135.

[6] J.-L. Colliot-Thélène and F. Xu, Brauer-Manin obstruction for integral points of homogeneous spaces and representation of integral quadratic forms, Compositio Mathematica **145** (2009), 309–363.

[7] J.-L. Colliot-Thélène et O. Wittenberg, Groupe de Brauer et points entiers de deux familles de surfaces cubiques affines, American Journal of Mathematics **134** (2012), no. 5, 1303–1327.

[8] A. Grothendieck, Le groupe de Brauer III; in *Dix exposés sur la cohomologie des schémas*, Masson, North-Holland, 1968.

[9] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101**, Cambridge University Press, 2006.

[10] R. Harshorne:, *Algebraic Geometry*, GTM **52**, Springer.

[11] J. Jahnel and D. Schindler, On integral points of degree four del Pezzo surfaces, Israel J. Math. **222** (2017), 21-62.

[12] A. Ghosh and P. Sarnak, Integral points on Markoff type cubic surfaces, arXiv: 1706.06712v2

[13] Y. Harpaz, Geometry and arithmetic of certain log $K3$ surfaces, Journal de l'Institut Fourier (Grenoble), Tome **67** (2017) 2167–2200.

[14] K. Kato, A Hasse principle for two dimensional global fields, J. für die reine und angew. Math. **366** (1986) 142–181.
[15] D. Loughran and V. Mitankin, Integral Hasse principle and strong approximation for Markoff surfaces, arXiv: 1807.10223v2
[16] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980.
[17] L. J. Mordell, On the integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$, Journal of the London Math. Soc. **28** (1953) 500–510.
[18] J. Neukirch, A.Schmidt and K.Wingberg, *Cohomology of Number Fields*, Grundlehren der Math. **323**, Springer, 2000.
[19] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, J. für die reine und angew. Math. **327** (1981), 12–80.
[20] H.P.F. Swinnerton-Dyer, The birationality of cubic surfaces over a given field. Michigan Math. J. **17** (1970) 289–295.

Université Paris Sud, Mathématiques, Bâtiment 307, 91405 Orsay Cedex, France
E-mail address: jlct@math.u-psud.fr

Academy of Mathematics and System Science, Chinese Academy of Sciences, Beijing 100190, China
E-mail address: dshwei@amss.ac.cn

School of Mathematical Science, Capital Normal University, Beijing 100048, China
E-mail address: xufei@math.ac.cn