ARITHMETIC GEOMETRY: RATIONAL POINTS

ALEXEI SKOROBOGATOV

Contents

Introduction

These are lecture notes of a course about rational points on surfaces and higher-dimensional algebraic varieties over number fields, which is an active topic of research in the last thirty years.

Legendre's theorem [8, 4.3.2 Thm. 8 (ii)] says that the Hasse principle holds for smooth plane conics over $\mathbb{Q}$. Iskovskih's counterexample

$$x^2 + y^2 = (t^2 - 2)(3 - t^2)$$

shows that it does not hold for 1-parameter families of conics over $\mathbb{Q}$. In this course we give necessary and sufficient conditions for the existence of points on certain pencils of conics over a number field. This is achieved by a combination of methods from algebra (quaternion algebras, the Brauer group

Date: December 10, 2013.

of a field), number theory (class field theory), algebraic geometry (the Brauer–Grothendieck group of a variety) and analysis.

Let us call a collection of local points on a projective variety, one over each completion of the ground number field, an adelic point. The main idea (due to Manin) is that class field theory gives general conditions on adelic points which are satisfied by all rational points. These so called Brauer–Manin conditions come from elements of the Brauer group of the variety, as defined by Grothendieck. The method of descent, well known in the case of elliptic curves, can be applied to conic bundles (families of conics parameterised by the projective line). In certain cases one can prove that any adelic point satisfying the Brauer–Manin conditions can be approximated by a rational point. One of the first achievements of this theory and the main result of the course is a theorem of Colliot-Thélène–Sansuc–Swinnerton-Dyer on rational points on Châtelet surfaces, a particular type of conic bundles. This method also allows to deduce results on rational points on general conic bundles over $\mathbb{Q}$ with split discriminant from recent spectacular work of Green, Tao and Ziegler in additive combinatorics.

1. Conics, quaternion algebras and the Brauer group

1.1. **Quaternion algebras.** Let k be a field of characteristic not equal to 2.

To elements $a, b \in k^*$ one can attach a non-commutative k-algebra (a ring containing k). The *quaternion algebra* $Q(a,b)$ is defined as the 4-dimensional vector space over k with basis 1, i, j, ij and the multiplication table $i^2 = a$, $j^2 = b$, $ij = -ji$.

Example. If $k = \mathbb{R}$ and $a = b = -1$ we obtain Hamilton's quaternions $\mathbb{H}$. This is a division algebra: the set of units coincides with the set of non-zero elements.

Is the same true for $Q(a,b)$? Define the conjugation and the norm, in the usual way.

Define a pure quaternion as an element q such that $q \notin k$ but $q^2 \in k$. It follows that pure quaternions are exactly the elements of the form $yi+zj+wij$ (just square $x+yi+zj+wij$, then there are some cancellations, and if $x \neq 0$, then $y = z = w = 0$). This gives an intrinsic definition of the conjugation and the norm because any quaternion z is uniquely written as the sum of a pure quaternion and a scalar.

Exercise. If q is a pure quaternion such that q^2 is not a square in k, then $1, q$ span a quadratic field which is a maximal subfield of Q.

Lemma 1.1. *If $c \in k^*$ is a norm from $k(\sqrt{a})^*$, then $Q(a,b) \cong Q(a,bc)$.*

Proof. Write $c = x^2 - ay^2$, then set $J = xj + yij$. Then J is a pure quaternion, so $Ji = -iJ$ and $J^2 = -N(J) = bc$. One checks that $1, i, J, iJ$ is a basis, so we are done. □

When a quaternion algebra is a division algebra? Since $N(q) = q\bar{q}$, if q is a unit, then $N(q) \in k^*$. If $N(q) = 0$, then $q\bar{q} = 0$, so q is a zero divisor. Thus

the units are exactly the elements with non-zero norm. The norm on $Q(a,b)$ is the diagonal quadratic form $\langle 1,-a,-b,ab\rangle$, and this leads us to the following criterion.

Proposition 1.2. *Let $a,b\in k^*$. Then the following statements are equivalent:*
(i) *$Q(a,b)$ is not a division algebra;*
(ii) *$Q(a,b)$ is isomorphic to the matrix algebra $M_2(k)$;*
(iii) *the diagonal quadratic form $\langle 1,-a,-b\rangle$ represents zero;*
(iv) *the diagonal quadratic form $\langle 1,-a,-b,ab\rangle$ represents zero;*
(v) *b is in the image of the norm homomorphism $k(\sqrt{a})^*\to k^*$.*

Proof. The equivalence of all of these is clear when $a\in k^{*2}$. Indeed, to prove the equivalence with (ii) we can assume that $a=1$. The matrix algebra is spanned by

$$1=Id=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad i=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad j=\begin{pmatrix}0&b\\1&0\end{pmatrix},\quad ij=\begin{pmatrix}0&b\\-1&0\end{pmatrix},$$

and so is isomorphic to $Q(1,b)$.

Now assume that a is not a square. Then (i) is equivalent to (iv) since $N(q)=q\bar{q}$. (iv) implies (v) because the ratio of two non-zero norms is a norm. (v) implies (iii) which implies (iv). So (iii), (iv) and (v) are equivalent (i). The previous lemma shows that under the assumption of (v) the algebra $Q(a,b)$ is isomorphic to $Q(a,a^2)=Q(a,1)$, so we use the result of the beginning of the proof. □

If the conditions of this theorem are satisfied one says that $Q(a,b)$ is *split*. If K is an extension of k such that $Q(a,b)\otimes_k K$ is split, then one says that K *splits* $Q(a,b)$.

We see that the quaternion algebra $Q(a,b)$, where $a,b\in k^*$ is a *form* of the 2×2-matrix algebra, which means that $Q(a,b)\otimes_k \bar{k}\cong M_2(\bar{k})$. For example, $\mathbb{H}\otimes_{\mathbb{R}}\mathbb{C}\cong M_2(\mathbb{C})$.

Proposition 1.3. *Any quaternion algebra Q split by $k(\sqrt{a})$ contains this field and can be written as $Q=(a,c)$ for some $c\in k^*$. Conversely, if Q contains $k(\sqrt{a})$, then Q is split by $k(\sqrt{a})$.*

Proof. If the algebra Q is split, take $c=1$. Assume it is not. Then $N(q_0+q_1\sqrt{a})=0$ for some non-zero $q_0,q_1\in Q$. Hence

$$N(q_0)+aN(q_1)+2\sqrt{a}B(q_0,q_1)=0,$$

where B is the bilinear form associated to the quadratic form N. This implies that $N(q_0)+aN(q_1)=0$ and $2B(q_0,q_1)=q_0\bar{q}_1+q_1\bar{q}_0=0$. Set $I=q_0/q_1$. We have $\bar{I}=-I$, hence I is a pure quaternion. Therefore, $I^2=-N(I)=a$. The conjugation by I has order exactly 2 since $I\notin k$ (i.e. I is not in the centre of Q). Hence the -1-eigenspace is non-zero, so we can find $J\in Q$ such that $IJ+JI=0$. One then checks that $1,I,J,IJ$ is a basis, hence $Q=(a,c)$, where $c=J^2$.

The converse follows from the fact that $k(\sqrt{a})\otimes k(\sqrt{a})$ contains zero devisors (the norm form $x^2 - ay^2$ represents zero over $k(\sqrt{a})$). Hence the same is true for $Q \otimes k(\sqrt{a})$. $\square$

Corollary 1.4. *The quadratic fields that split Q are exactly the quadratic subfields of Q.*

1.2. **Conics.** Define *the conic attached to the quaternion algebra* $Q(a,b)$ as the plane algebraic curve $C(a,b) \subset \mathbb{P}^2_k$ (a closed subset of the projective plane) given by the equation

$$ax^2 + by^2 = z^2.$$

It has a k-point if and only if $Q(a,b)$ is split. An intrinsic definition is this: $C(a,b)$ is the conic

$$-ax^2 - by^2 + abz^2 = 0,$$

which is just the expression for the norm of pure quaternions.

Facts about conics. 1. Since the characteristic of k is not 2, every conic can be given by a diagonal quadratic form, and so is attached to some quaternion algebra.

2. The projective line is isomorphic to a conic $xz - y^2 = 0$ via map $(X : Y) \mapsto (X^2 : XY : Y^2)$.

3. If a conic C has a k-point, then $C \cong \mathbb{P}^1_k$. (The projection from a k-point gives rise to a rational parameterisation of C, which is a bijection.)

4. Thus the function field $k(C)$ is a purely transcendental extension of k if and only if C has a k-point.

Exercise. 1. Check that $Q(a, 1-a)$ and $Q(a, -a)$ are split.

2. Check that if $k = \mathbb{F}_q$ is a finite field, then all quaternion algebras are split. (If $char(k)$ is not 2, write $ax^2 = 1 - by^2$ and use a counting argument for x and y to prove the existence of a solution in $\mathbb{F}_q$.)

3. $Q(a,b)$ is split over k if and only if $Q(a,b) \otimes_k k(t)$ is split over $k(t)$. (Take a $k(t)$-point on $C(a,b)$ represented by three polynomials not all divisible by t, and reduce modulo t.)

4. $Q(a,b)$ is split over $k(C(a,b))$. (Consider the generic point of the conic.)

Theorem 1.5 (Tsen)**.** *If k is algebraically closed, then every quaternion algebra over $k(t)$ is split.*

Proof. We only prove that every quaternion algebra over $k(t)$ is split. For this it is enough to show that any conic over $k(t)$ has a point. We can assume that the coefficients of the corresponding quadratic form are polynomials of degree at most m. We look for a solution (X, Y, Z) where X, Y and Z are polynomials in t (not all of them zero) of degree n for some large integer n. The coefficients of these polynomials can be thought of as points of $\mathbb{P}^{3n+2}$. The solutions bijectively correspond to the points of a closed subset of $\mathbb{P}^{3n+2}$ given by $2n+m+1$ homogeneous quadratic equations. Since k is algebraically closed this set is non-empty when $3n + 2 \geq 2n + m + 1$, by a standard result from algebraic geometry. (If an irreducible variety X is not contained in a

hypersurface H, then $\dim(X \cap H) = \dim(X) - 1$. This implies that on intersecting X with r hypersurfaces the dimension drops at most by r, see [10, Ch. 1]). □

Theorem 1.6 (Witt)**.** *Two quaternions algebras are isomorphic if and only if the conics attached to them are isomorphic.*

Proof. Since C_Q is defined intrinsically in terms of Q, it remains to prove that if $C_Q \cong C_{Q'}$ then $Q \cong Q'$. If Q is split, then $C_Q \cong \mathbb{P}^1_k$, hence $C_{Q'} \cong \mathbb{P}^1_k$. Thus Q' is split by the field of functions $k(\mathbb{P}^1_k) \cong k(t)$. Then Q' is split by Exercise 3 above.

Now assume that neither algebra is split. Write $Q = Q(a, b)$ so that $C_Q = C(a, b)$. The conic $C_Q \cong C_{Q'}$ has a $k(\sqrt{a})$-point, hence Q' is split by $k(\sqrt{a})$. By Proposition 1.3 we can write $Q' = Q(a, c)$ for some $c \in k^*$. By Exercise 4 above Q' is split by the function field $k(C_{Q'}) \cong k(C(a, b))$. By Proposition 1.2 this implies that c is contained in the image of the norm map

$$c \in \mathrm{Im}[k(C(a,b))(\sqrt{a})^* \longrightarrow k(C(a,b))^*].$$

Let $\sigma \in \mathrm{Gal}(k(\sqrt{a})/k) \cong \mathbb{Z}/2$ be the generator. Then we can write $c = f\sigma(f)$, where f is a rational function on the conic $C(a, b) \times_k k(\sqrt{a})$. One can replace f with $f\sigma(g)g^{-1}$ for any $g \in k(C(a, b))(\sqrt{a})^*$ without changing c. Our aim is to show that c is a product of a norm from $k(\sqrt{a})^*$ and a power of b. The power of b is odd because Q' is not split over k, so this is enough to prove the theorem.

The group Div of divisors on $C(a, b) \times_k k(\sqrt{a}) \cong \mathbb{P}^1_{k(\sqrt{a})}$ is freely generated by the closed points of $C(a, b) \times_k k(\sqrt{a})$. This is a module of $\mathbb{Z}/2 = \langle\sigma\rangle$ with a σ-stable basis. The divisors of functions are exactly the divisors of degree 0. The divisor $D = \mathrm{div}(f)$ is an element of Div satisfying $(1 + \sigma)D = 0$. Hence there is $G \in Div$ such that $D = (1-\sigma)G$. Let $P = (1 : 0 : \sqrt{a})$. If $n = \deg(G)$ the divisor $G - nP \in Div$ has degree 0, and thus $G - nP = \mathrm{div}(g)$ for some $g \in k(\sqrt{a})(C(a, b))^*$. We have

$$\mathrm{div}(f\sigma(g)g^{-1}) = D + \sigma G - G + n(P - \sigma P) = n(P - \sigma P) = n \ \mathrm{div}\left(\frac{z - \sqrt{a}x}{y}\right).$$

It follows that

$$f\sigma(g)g^{-1} = e\left(\frac{z - \sqrt{a}x}{y}\right)^n,$$

where $e \in k(\sqrt{a})^*$. Thus

$$c = f\sigma(f) = N(e)\left(\frac{z^2 - ax^2}{y^2}\right)^n = N(e)b^n. \qquad \square$$

1.3. **Central simple algebras and the Brauer group.** A k-algebra A is called a *central simple algebra* if and only if A is a form of a matrix algebra, that is, $A \otimes_k \bar{k} \cong M_n(\bar{k})$ for some positive integer n. Equivalently, the centre of A is k (A is "central") and A has no non-trivial two-sided ideals (A is "simple").

Recall that if V and W are vector spaces over k, then $V \otimes_k W$ is the linear span of vectors $v \otimes w$, $v \in V$, $w \in W$, subject to the axioms

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w, \quad v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2,$$

and

$$c(v \otimes w) = (cv) \otimes w = v \otimes (cw) \quad \text{for any} \quad c \in k.$$

This turns $V \otimes_k W$ into a k-vector space. Note that $(V \otimes U) \otimes W$ is canonically isomorphic to $V \otimes (U \otimes W)$.

If (e_i) is a basis of V, and (f_j) is a basis of W, then $(e_i \otimes f_j)$ is a basis of $V \otimes_k W$. Now, if V and W are k-algebras, then $V \otimes_k W$ is a k-algebra with multiplication $(x \otimes y) \cdot (x' \otimes y') = (xx') \otimes (yy')$.

Properties. 1. $M_n(k)$ is a c.s.a.

2. $M_m(k) \otimes_k M_n(k) \cong M_{mn}(k)$. Hence the set of c.s.a. is closed under $\otimes$.

3. $Q(a,b) \otimes_k Q(a,b') \cong Q(a,bb') \otimes_k M_2(k)$. (Proof: The span of $1 \otimes 1$, $i \otimes 1$, $j \otimes j'$, $ij \otimes j'$ is $A_1 = Q(a,bb')$. The span of $1 \otimes 1$, $1 \otimes j'$, $i \otimes i'j'$, $-b(i \otimes i')$ is $A_2 = Q(b', -a^2b') \cong M_2(k)$. The canonical map $A_1 \otimes_k A_2 \to Q(a,b) \otimes_k Q(a,b')$ defined by the product, is surjective. The kernel of a homomorphism is a two-sided ideal, hence it is zero so that this map is an isomorphism.)

4. $Q(a,b) \otimes_k Q(a,b) \cong M_4(k)$. (This follows from parts 2 and 3.)

Two c.s.a. A and B are *equivalent* if there are n and m such that $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$. The relation is transitive by Property 2. The equivalence class of k consists of the matrix algebras of all sizes.

Theorem 1.7. *The tensor product turns the set of equivalence classes of c.s.a. into an abelian group, called the Braeur group* $\mathrm{Br}(k)$.

Proof. The neutral element is the class of k and the inverse element of A is the equivalence class of the *opposite* algebra A°. Indeed, $A \otimes_k A^\circ$ is a c.s.a., and there is a non-zero homomorphism $A \otimes_k A^\circ \to \mathrm{End}_k(A)$ that sends $a \otimes b$ to $x \mapsto axb$. It is injective since a c.s.a. has no two-sided ideals, and hence is an isomorphism by the dimension count. □

We denote by $(a,b) \in \mathrm{Br}(k)$ the class of the quaternion algebra $Q(a,b)$.

We write the group operation in $\mathrm{Br}(k)$ additively. By Property 4 we have $(a,b) \in \mathrm{Br}(k)[2]$ and $(a,b) + (a,b') = (a,bb')$. We also have $(a,-a) = (a,1-a) = 0$ for any $a, b, b' \in k$ for which these symbols are defined.

Examples. $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2$ and $\mathrm{Br}(\mathbb{F}_q) = 0$. (proofs are omitted) The full version of Tsen's theorem states (with a similar proof) that if k is algebraically closed, then $\mathrm{Br}(k(t)) = 0$.

If $k \subset K$ is a field extension, then tensoring with K defines a homomorphism

$$\mathrm{res}_{K/k} : \mathrm{Br}(k) \to \mathrm{Br}(K),$$

call the *restriction* from k to K.

Here are some important facts about c.s.a. We don't prove them because we won't use them.

Wedderburn's theorem *For any c.s.a. A there is a unique division algebra D such that $A \cong D \otimes_k M_n(k) = M_n(D)$.*

Skolem–Noether theorem *Let B be a simple algebra and let A be a c.s.a. Then all non-zero homomorphisms $B \to A$ can be obtained from one another by a conjugation in A.*

This generalises the fact that any automorphism of $M_n(k)$ is inner.

1.4. **Residue.** Let O be a *discrete valuation ring* (DVR). By definition this is a principal ideal domain with a unique maximal ideal $\mathfrak{m} = (\pi)$. The generator π is defined up to multiplication by a unit; any such generator is called a *uniformiser*. We denote by K the fraction field of O and by $\kappa = O/\mathfrak{m}$ the residue field. The valuation $\mathrm{val} : K^* \to \mathbb{Z}$ is a homomorphism defined as follows. For any $x \in K^*$ we have either $x \in O$ or $x^{-1} \in O$. For $x \in O$, we set $\mathrm{val}(x) = n$ if $x \in \mathfrak{m}^n$ but $x \notin \mathfrak{m}^{n+1}$, and then extend to K^* by multiplicativity. Here are two main examples:

(1) $O = \left\{\frac{a}{b} | a, b \in \mathbb{Z},\ (p, b) = 1\right\} \subset \mathbb{Q}$ (the localisation of $\mathbb{Z}$ at p), $\pi = p$, $K = \mathbb{Q}$, $\kappa = \mathbb{F}_p$;

(2) the localisation of $k[t]$ at the prime ideal generated by a monic irreducible polynomial $p(t)$. Here $\pi = p(t)$, $\kappa = k[t]/(p(t))$, $K = k(t)$.

The ring O is called *complete* if $O = \lim O/\mathfrak{m}^n$. We shall work with two main examples of complete DVR:

(1) p-adic case: $O = \mathbb{Z}_p$, $\pi = p$, $K = \mathbb{Q}_p$, $\kappa = \mathbb{F}_p$ (or, more generally, K can be any finite extension of $\mathbb{Q}_p$);

(2) the completion of the localisation of $k[t]$ at the prime ideal generated by a monic irreducible polynomial $p(t)$. Here we have $\pi = p(t)$ and $\kappa = k[t]/(p(t))$. It can be proved that $O \cong \kappa[[p(t)]]$ is the ring of formal power series in $p(t)$ over κ, and hence K is the ring of Laurent poweer series. See [9].

The crucial fact about complete DVRs is that Hensel's lemma holds for them. It says that if a separable polynomial over O has a simple root modulo $\mathfrak{m}$, then it has a root in K.

Lemma 1.8. *Let Q be a non-split quaternion algebra over a complete discrete valuation field K of residual characteristic not equal to 2. There are two mutually excluding possibilities:*

(i) *all quadratic subfields of Q are unramified if and only if $Q = Q(a, b)$, where $a, b \in O^*$;*

(ii) *Q contains a ramified quadratic subfield, say $K(\sqrt{\pi})$. Then $Q = Q(a, \pi)$ for some $a \in O^* \setminus O^{*2}$. Each unramified quadratic subfield of $Q(a, \pi)$ is isomorphic to $K(\sqrt{a})$.*

Proof. Since the characteristic of κ is not 2, a quadratic extension F/K is unramified if and only if $F = K(\sqrt{a})$ for some $a \in O^*$. If all quadratic subfields of Q are unramified, then $a, b \in O^*$. Conversely, suppose that $Q = Q(a, b)$, where $a, b \in O^*$. We need to show that Q does not contain $K(\sqrt{\pi})$. Indeed, otherwise $\sqrt{\pi} \in Q$ is a pure quaternion $yi + zj + wij$ of norm $-\pi = -ay^2 - bz^2 + abw^2$. It follows that there exist $Y, Z, W \in O$ not

all divisible by π such that $\mathrm{val}(aY^2 + bZ^2 - abW^2)$ is odd. Let $\bar{a}, \bar{b} \in \kappa^*$ be the residues of a, b modulo $\mathfrak{m}$. We see that the smooth conic $C(\bar{a}, \bar{b})$ contains a κ-point. By Hensel's lemma the conic $C(a, b)$ contains a K-point, but this contradicts the assumption that $Q(a, b)$ is not split over K.

Now suppose that $K(\sqrt{\pi}) \subset Q$. Then $Q = Q(a, \pi)$ for some $a \in K^*$ by Proposition 1.3. But we also have $Q = Q(-a\pi, \pi)$. Either a or $-a\pi$ has even valuation, so up to a square we can assume that $a \in O^*$. Since Q is not split, $a \notin K^{*2}$. It remains to show that if Q contains a pure quaternion of norm $-b \in O^*$, then $a/b \in K^{*2}$. Indeed, if $-b = -ay^2 - \pi z^2 + a\pi w^2$, then

$$bX^2 - aY^2 = \pi(Z^2 - aW^2)$$

has a solution in O such that not all four coordinates are divisible by π. Since $a \in O^*$ and $a \notin K^{*2}$, we see that $\bar{a} \notin \kappa^{*2}$. Thus the equation $Z^2 - \bar{a}W^2 = 0$ has only the zero solution in κ. It follows that the valuation $\mathrm{val}(Z^2 - aW^2)$ is even, so that the valuation of $bX^2 - aY^2$ is odd, implying that $\bar{a} = \bar{b}$. Then $a/b \in 1 + \mathfrak{m}$, and by Hensel's lemma $a/b \in K^{*2}$. $\square$

Remark. Using the Skolem–Noether theorem one can prove that all unramified subfields of $Q(a, \pi)$ are conjugate.

One defines the residue of (a, b), where $a, b \in K^*$, as an element of κ^*/κ^{*2} as follows. If $Q(a, b)$ is split or falls into case (i), then the residue is 1. In case (ii) the residue is the class of $\bar{a}$. By Lemma 1.8 the residue is well defined.

Remark. It is easy to see that $Res(Q(a, b))$ is the class of the reduction modulo $\mathfrak{m}$ of

$$(-1)^{\mathrm{val}(a)\mathrm{val}(b)} a^{\mathrm{val}(b)} b^{-\mathrm{val}(a)} \in O^* \tag{1.1}$$

in κ^*/κ^{*2}. This formula shows that

$$Res(Q(aa', b)) = Res(Q(a, b)) \cdot Res(Q(a', b)).$$

Now we generalise the definition of residue to any field K with a discrete valuation $\mathrm{val} : K^* \to \mathbb{Z}$, not necessary complete. Let $O \subset K$ be the union of $\{0\}$ and the elements $x \in K$ such that $\mathrm{val}(x) \geq 0$. This is a subring of K such that K is the field of fractions of O. Let O_c be the completion of O, and let K_c be the field of fractions of O_c. We define the residue of $Q(a, b)$, $a, b \in K^*$, as the residue of $Q(a, b) \otimes_K K_c$.

For example, in the arithmetic case we can take $K = \mathbb{Q}$ equipped with the valuation attached to a prime p. Then O is the ring of rational numbers whose denominators are not divisible by p, $\mathfrak{m} = (p)$, $\kappa = \mathbb{F}_p$. The completion of O is $O_c = \mathbb{Z}_p$, so that $K_c = \mathbb{Q}_p$.

In the geometric case take $K = k(t)$, O is the ring of rational functions such that the denominator is not divisible by an irreducible monic polynomial $p(t)$, $\kappa = k[t]/(p(t))$.

Exercise. For any field k of $\mathrm{char}(k) \neq 2$ prove that (x, y) is a non-zero element of $\mathrm{Br}(k(x, y))$.

1.5. **Reciprocity.** For a general discretely valued complete field k we have three cases: split, non-split unramified, non-split ramified. In the first two cases the residue is zero.

Now we consider the case when the residue field is finite. Let K be a p-adic field, that is, a finite extension of $\mathbb{Q}_p$. Let $\mathbb{F}_q = O_k/\mathfrak{m}$ be the residue field. For $a, b \in K^*$ we define the Hilbert symbol $(a,b)_K = 1$ if $Q(a,b)$ is split, and $(a,b)_K = -1$ otherwise.

Proposition 1.9. *When $p \neq 2$, the Hilbert symbol $(a,b)_K = 1$ if and only if $Q(a,b)$ is unramified. In particular, if $K = \mathbb{Q}_p$, then the Hilbert symbol $(a,b)_p$ is the Legendre symbol of the residue of $Q(a,b)$:*

$$(a,b)_p = \left(\frac{Res_p(Q(a,b))}{p}\right).$$

Proof. Using Hensel's lemma it is easy to see that the quadratic form $\langle 1, -a, -\pi\rangle$ represents zero if and only if $\bar{a}$ is a square in $\mathbb{F}_q^*$. For any $a, b \in O^*$ the form $\langle 1, -a, -b\rangle$ represents zero in K, since a smooth conic over $\mathbb{F}_q$ has an $\mathbb{F}_q$-point that can be lifted to a $\mathbb{Q}_p$-point by Hensel's lemma. □

Exercises. 1. Calculate $(a,b)_2$ when $K = \mathbb{Q}_2$. (If a and b are odd, then $(a,b)_2 = -1$ if and only if $a \equiv b \equiv -1 \bmod 4$. The full answer is this: in the basis $2, -1, 5$ the Hilbert symbol equals 1 except for the entries on the skew diagonal when it equals -1. See [8].)

2. For $p \neq 2$ it follows from Proposition 1.9 that $Q(a,p)$, where a is a p-adic unit which is not a square, is the unique non-split quoternion algebra over $\mathbb{Q}_p$, up to isomorphism. Prove that all non-split quoternion algebras over $\mathbb{Q}_2$ are isomorphic, too.

Theorem 1.10 (Product formula)**.** *For $a, b \in \mathbb{Q}^*$ we have $\prod_p (a,b)_p = 1$, where $p = 0$ is included in the product with $(a,b)_0$ defined as $(a,b)_{\mathbb{R}}$.*

Proof. By bimultiplicativity of the Hilber symbol it is enough to prove the product formula for $(-1,-1)$, $(-1,p)$ and (p,q), where $p \neq q$ are prime numbers. In all cases it follows from quadratic reciprocity. □

There is a similar product formula for a general number field: $\prod_v (a,b)_v = 1$ where k_v rages over all completions of k. Note that it is not enough to consider only the *discrete valuations* of k, i.e. functions $\mathrm{val} : k^* \to \mathbb{Z}$ such that $\mathrm{val}(ab) = \mathrm{val}(a) + \mathrm{val}(b)$ and $\mathrm{val}(a+b) \geq \min\{\mathrm{val}(a), \mathrm{val}(b)\}$ (it is convenient to set $\mathrm{val}(0) = \infty$). The discrete valuations are given by the prime ideals of O_k (called the finite places of k) and give rise to non-archimedean completions of k. Ostrowski's theorem classifies all completions of $\mathbb{Q}$. The real completion can be described in terms in a non-discrete valuation, which means that $\mathrm{val}(k^*)$ is any subgroup of $\mathbb{R}^*$ (i.e. $\mathrm{val}(x) = -\log|x|$ for $x \in \mathbb{Q}$). So to get a product formula we need to consider all completions of k, including real and complex completions, sometimes called the infinite places of k.

Now let k be again an arbitrary field.

Exercise The discrete valuations of $k(t)$ that are trivial on k are of the following two kinds: (a) those given by monic irreducible polynomials $p(t)$ (then the residue field is $k_p = k[t]/(p(t))$), and (b) $val(f(t)) = -\deg(f(t))$ (the residue field is k).

Let Res_p denote the residue at $p(t)$.

We shall refer to the elements in the image of $\mathrm{res}_{k(t)/k}$ as *constant* elements. The residue of any constant element is trivial.

The norm $N_{k_p/k} : k_p \to k$ defines a homomorphism

$$N_{k_p/k} : k_p^*/k_p^{*2} \to k^*/k^{*2}.$$

Lemma 1.11. *Let $a, b \in k[t]^*$ be polynomials of degree m and n, respectively. Then the product of $N_{k_p/k}(Res_p(Q(a,b)))$, where $p(t)$ rages over all monic irreducible polynomials in $k[t]$, is*

$$(-1)^{mn} a_m^n b_n^m \in k^*/k^{*2}.$$

Proof. The product is finite (from the definition of residue). By bimultiplicativity of residue it is enough to calculate the product for $(c, b(t))$ and $(a(t), b(t))$, where $c \in k^*$, and $a(t)$ and $b(t)$ are monic irreducible. For the first one we get c^n, which agrees with our formula. For the second one the relevant terms in the product correspond to $p = a$ and $p = b$. Assume $p = a$. Then the residue is the class modulo squares of $a(\theta) \in k_p$, where θ is the image of x in k_p. The norm of an element of k_p is the product of its images under all $[k_p : k]$ embeddings of k_p into $\bar{k}$. In our case these are $a(\theta_i)$, where $\theta_j \in \bar{k}$ are the roots of $b(t) = \prod(t - \theta_j)$. Hence the norm $N_{k_p/k}(a(\theta))$ is the product of $a(\theta_j)$, but this equals the resultant $\mathrm{R}(b(t), a(t))$, which is defined as $\prod_{i,j}(\xi_i - \theta_j)$ where $a(t) = \prod(t - \xi_i)$. Swapping a and b multiplies the resultant by $(-1)^{mn}$. □

The reason why the product is not 1 is that we have forgotten to include the "infinite place" with valuation function is $-\deg(f(t))$. The ring of this discrete valuation is $O = k[t^{-1}]$, $\mathfrak{m} = (t^{-1})$, $\kappa = k$. We refer to this discrete valuation as the point at infinity because it is defined by the order of vanishing of rational functions at the point $\infty \in \mathbb{P}^1$.

Theorem 1.12 (Faddeev's reciprocity law)**.** *For any $a, b \in k(t)^*$ we have $\prod_p N_{k_p/k}(Q(Res_p(a,b))) = 1 \in k^*/k^{*2}$, where we include into this product $p = \infty$ with $k_\infty = k$.*

Proof. It is enough to prove this for polynomials $a(t)$ and $b(t)$, say of degrees m and n, respectively. By Lemma 1.11 it remains to prove that the residue at infinity equals $(-1)^{mn} a_m^n b_n^m$. By multiplicativity it is enough to consider $(c, b(t))$ and $(a(t), b(t))$, where $a(t)$ and $b(t)$ are monic. In the first case we get c^n, as required. In the second case if one of the degrees is even we get 1, as required. If m and n are both odd, then $(a(t), b(t)) = (-a(t)b(t), b(t))$ and this element has residue the class of -1 in k^*/k^{*2}, as required. □

2. Brauer–Grothendieck group and the Brauer–Manin obstruction

2.1. **The Hasse principle and weak approximation.** Let k be a number field. We denote the completions of k by k_v.

Theorem 2.1 (Hasse–Minkowski)**.** *If a smooth projective quadric of dimension at least 1 has a k_v-point for each completion k_v, then it has a k-point.*

If a variety X has k_v-point for each completion k_v but no k-point, then one says that X is a counterexample to the *Hasse principle*. It would be nice to have a tool to prove that $X(k) = \emptyset$ in this case.

The topology of k_v (p-adic or Euclidean) turns the set of k_v-points $X(k_v)$ into a topological space. On each affine piece of X this is the topology induced from $k_v^n = \mathbb{A}^n(k_v)$, so that two k_v-points are close if their coordinates are close. If X is smooth, it follows from the implicit function theorem that every k_v-point of X is contained in a small neighbourhood homeomorphic to a disc (p-adic or Euclidean). This has the important consequence that by a small deformation we can move a local point away from a Zariski closed subset.

Suppose that for every place v of k we have a k_v-point $P_v \in X(k_v)$. The collection (P_v) will be called an adèle of X or an adelic point of X. The space of adèles $\prod_v X(k_v)$ is then equipped with the product topology: two adèles are close if their components for finitely many places v are close. Suppose that $X(k) \neq \emptyset$. One can wonder if we can approximate adèles by k-points, in other words, whether or not for any finite set S of places and any $P_v \in X(k_v)$ for $v \in S$ there exists a k-point $P \in X(k)$ sufficiently close to each P_v in the topology of k_v. If this holds, X is said to satisfy *weak approximation*.

By the independence of valuations this is true for $\mathbb{A}^1$: for any finite set S of places and any $a_v \in k_v$ for $v \in S$ there exists $a \in k$ sufficiently close to each a_v in the topology of k_v. Thus the same is true if X is a *rational* variety, that is, if $k(X)$ is a purely transcendental extension of X. Indeed, in this case X contains an open subset which is also an open subset of some $\mathbb{A}^m$, so after a small deformation the approximation problem reduces to the affine line. Since a smooth projective quadric of dimension at least 1 is rational over k if and only if it has a k-point, this argument applies, so that such quadrics satisfy weak approximation.

We want to have an instrument to control the closure of k-points in the topological space of adelic points on X. This can be done using Azumaya algebras.

2.2. **Azumaya algebras and Brauer group of an algebraic variety.** In this section k is any field and X is an irreducible smooth variety. The structure sheaf of X is the sheaf of rings $\mathcal{O}_X$ such that for any open subset $U \subset X$, $\mathcal{O}_X(U)$ is the ring of regular functions $k[U]$. A sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is a sheaf on X such that for any open subset $U \subset X$, $\mathcal{F}(U)$ is a module over $\mathcal{O}_X(U)$. For an open subset U the restriction $\mathcal{O}_X|_U$ is the structure sheaf $\mathcal{O}_U$.

A sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is locally free if X can be covered by open subsets U such that $\mathcal{F}|_U$ is a free $\mathcal{O}_U$-module.

There is an equivalent definition of a c.s.a. over a field k: it is a k-algebra A such that the canonical homomorphism $A \otimes_k A^\circ \to \mathrm{End}(A)$ is an isomorphism. (As we know, any c.s.a. has this property. Conversely, $Z(A) \otimes_k Z(A^\circ)$ is contained in the centre of the matrix algebra, so $Z(A) = k$. Also, the tensor product of two non-zero 2-sided ideals is a non-zero 2-sided ideal of the matrix algebra, so it is the whole thing. Thus A is a c.s.a.)

This definition is more convenient in case of $\mathcal{O}_X$-algebras. We define an *Azumaya algebra* $\mathcal{A}$ on X as a locally free sheaf of $\mathcal{O}_X$-algebras such that the natural homomorphism

$$\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{A}^\circ \longrightarrow \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{A})$$

is an isomorphism. Here $\mathcal{E}nd_{\mathcal{O}_X}$ is a sheaf of homomorphisms of $\mathcal{O}_X$-modules.

There is an equivalent definition of an Azumaya algebra in terms of local rings of subvarieties. Let $Y \subset X$ be an irreducible subvariety. The local ring O_Y is the subring of $k(X)$ consisting of the rational functions that are regular on some open set $U \subset X$ such that $U \cap Y \neq \emptyset$. In a slightly different language O_Y is the inductive limit of $k[U]$ for such open sets U. If U is affine then O_Y consists of the ratios of functions from $k[U]$ such that the denominator does not identically vanish on $U \cap Y$. The ring O_Y is local, which means that it has a unique maximal ideal $\mathfrak{m}_Y$. It consists of the functions vanishing on Y. We have $\mathcal{O}_Y/\mathfrak{m}_Y = k(Y)$.

For any locally free sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ the inductive limit of $\mathcal{F}(U)$ is an O_Y-module, denoted by $\mathcal{F}_Y$. Define $\mathcal{A}(Y) := \mathcal{A}_Y \otimes_{O_Y} k(Y)$. Here is the second definition of an Azumaya algebra: a locally free sheaf of $\mathcal{O}_X$-algebras $\mathcal{A}$ is an Azumaya algebra if for every irreducible subvariety $Y \subset X$ the $k(Y)$-algebra $\mathcal{A}(Y)$ is a c.s.a. over the field $k(Y)$.

Two Azumaya algebras $\mathcal{A}$ and $\mathcal{B}$ are equivalent if there exist locally free sheaves of $\mathcal{O}_X$-modules $\mathcal{E}$ and $\mathcal{F}$ such that

$$\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{E}) \cong \mathcal{B} \otimes_{\mathcal{O}_X} \mathcal{E}nd_{\mathcal{O}_X}(\mathcal{F}).$$

In the same way as before one checks that this is indeed an equivalence relation. The group of equivalence classes of Azumaya algebras on X is called the Brauer–Grothendieck group $\mathrm{Br}(X)$.

If X is one k-point, then an Azumaya algebra is the same as a c.s.a. over k.

From the definition we obtain that the Brauer group $\mathrm{Br}(X)$ is functorial: if $f : X \to Y$ is a morphism of algebraic varieties, then we have an induced homomorphism of Brauer groups $f^* : \mathrm{Br}(Y) \to \mathrm{Br}(X)$. In particular, if f is an embedding of a k-point P into X, we have the induced map $\mathrm{Br}(X) \to \mathrm{Br}(k)$ also written as $\mathcal{A} \mapsto \mathcal{A}(P)$, called the "evaluation" at P. (This is the c.s.a. from the second definition of the Azumaya algebra.) Similarly, for any field extension $k \subset K$ if there is a K-point on X, then we can evaluate the elements of $\mathrm{Br}(X)$ at K-points of X by considering the map $\mathrm{Br}(X) \to \mathrm{Br}(X_K) \to \mathrm{Br}(K)$. (Here $X_K = X \times_k K$ is the variety obtained

from X by increasing the ground field from k to K.) The evaluation at the generic point $\mathrm{Spec}(k(X))$ of X gives rise to a natural map $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$.

It turns out that the image of this map can be characterised in terms of residues.

Each (irreducible) divisor $D \subset X$, that is, an irreducible subvariety of codimension 1, in some non-empty open neighbourhood of any point $x \in D$ is given by one equation f_D, see [10, Ch. 1]. It follows that the maximal ideal $\mathfrak{m}_D = (f_D)$ is principal, and so $\mathcal{O}_D$ is a DVR. In other words, D defines a discrete valuation $\mathrm{val}_D : k(X)^* \to \mathbb{Z}$ such that $\mathrm{val}_D(f_D) = 1$ and $\mathrm{val}_D(g) = 0$ if D is not contained in the support of the divisor of g. Then

$$O_D = \{0\} \cup \{x \in k(X) | \mathrm{val}_D(x) \geq 0\}, \quad \mathfrak{m}_D = \{0\} \cup \{x \in k(X) | \mathrm{val}_D(x) \geq 1\}.$$

Let Q be a quaternion algebra over $k(X)$. We have the residue $Res_D(Q) \in k(D)^*/k(D)^{*2}$ induced by the discrete valuation val_D. If $Res_D(Q) = 1$, the algebra Q is called *unramified* at D. If Q is unramified at every irreducible divisor of X, it is called unramified on X.

Grothendieck proved the following important results using étale cohomology [7], so we accept them without proof.

Theorem 2.2 (Grothendieck)**.** *Let X be smooth and irreducible. Then*

(i) *the natural map $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$ is injective;*

(ii) *its image consists precisely of the classes of unramified c.s.a. over $k(X)$.*

In the definition of an unramified algebra one could take *all* discrete valuations of $k(X)$ that are trivial on k (which in higher dimension are not necessarily given by the divisors on X). Grothendieck shows that un unramified algebra in the previous sense is also unramified in this stronger sense.

Let us have a closer look at quoternion Azumaya algebras, that is, Azumaya alagebras of rank 4.

Proposition 2.3. *Let X be a variety over a field k, $char(k) \neq 2$. For any quaternion Azumaya algebra $\mathcal{A}$ on X there exists a finite covering of X by open subsets U such that for each U there is an isomorphism of $\mathcal{O}_U$-algebras*

$$\mathcal{A}|_U \cong Q(f_U, g_U) := \mathcal{O}_U \oplus i\mathcal{O}_U \oplus j\mathcal{O}_U \oplus ij\mathcal{O}_U,$$

where $i^2 = f_U$, $j^2 = g_U$, $ij = -ji$, and $f_U, g_U \in k[U]^*$.

Sketch of proof. Any quasi-projective variety is quasi-compact, so any open covering contains a finite sub-covering. It is enough to establish the displayed isomorphism over the local ring $\mathcal{O}_P$, for any closed point P. Indeed, then it extends to some open neighbourhood of P, and in this way we obtain an open covering of X.

Write $R = O_P$, $\mathfrak{m} = \mathfrak{m}_P$, $\kappa = k(P)$, $K = k(X)$, $A = \mathcal{A}$. So we have an R-algebra A, isomorphic to R^4 as an R-module, such that

$$\overline{A} = A \otimes_R \kappa = A/(A \otimes_R \mathfrak{m}) = Q(a, b) = \kappa \oplus i\kappa \oplus j\kappa \oplus ij\kappa$$

is a quaternion algebra over κ for some $a, b \in \kappa^*$. Let $I \in A$ be any element that reduces to i modulo $A \otimes_R \mathfrak{m}$. It can be proved that $I^2 = \alpha I + \beta$ for some $\alpha, \beta \in R$ (this proof goes by defining an analogue of the Cayley–Hamilton characteristic polynomial for any element of A; this is a bit delicate so we omit this proof). Then $\alpha \in \mathfrak{m}$ and β reduces to a modulo $\mathfrak{m}$. We can modify I by $\frac{1}{2}\alpha \in \mathfrak{m}$ and hence assume that $I^2 = f \in R$, where f reduces to a modulo $\mathfrak{m}$, so $f \in R^*$, as required.

Recall that $A_K = A \otimes_R K$ is a quaternion algebra that contains A. Let $A^+ \subset A$ be the set of elements that commute with I, and A^- be the set of elements that anti-commute with I. Since

$$x = \frac{x + a^{-1}IxI}{2} + \frac{x - a^{-1}IxI}{2} \in A^+ \oplus A^-,$$

we have $A = A^+ \oplus A^-$ as R-modules. The reduction modulo $\mathfrak{m}$ gives a surjection from A^+ to $\kappa \oplus i\kappa$, so by Nakayama's lemma $A^+ = R \oplus IR = R[I]$. Next, the reduction modulo $\mathfrak{m}$ gives a surjective map from A^- to the vector subspace of $Q(a, b)$ consisiting of the elements that anti-commute with i, i.e. to $j\kappa \oplus ij\kappa$. Let J be an element of A^- that reduces to j. Since any nonozero element of A_K that anti-commutes with I is a pure quaternion, we have $J^2 \in A \cap K = R$. As $J^2 = g \in R$ is congruent to b modulo $\mathfrak{m}$, we have $g \in R^*$. By Nakayama's lemma $A^- = JR \oplus IJR$, so $A = R \oplus IR \oplus JR \oplus IJR$ and we are done. □

Conversely, suppose that for some open covering of X we are given a compatible system of $\mathcal{O}_U$-algebras $Q(f_U, g_U)$ as above. This means that for each pair of open sets U, V we have isomorphisms of $\mathcal{O}_{U\cap V}$-algebras

$$\varphi_{U,V} : Q(f_U, g_U)|_{U\cap V} \xrightarrow{\sim} Q(f_V, g_V)|_{U\cap V}$$

such that these isomorphisms agree on triple intersections $U \cap V \cap W$, that is, we have $\varphi_{U,W} = \varphi_{V,W}\varphi_{U,V}$. This defines a locally free sheaf of $\mathcal{O}_X$-modules, which is also a sheaf of c.s.a., so it is an Azumaya algebra.

Example. Let X be a projective curve over a field k of characteristic not equal to 2 with the affine equation $y^2 = p(x)q(x)$, where $p(x)$ and $q(x)$ are separable coprime polynomials of degrees m and n over k. Assume that m is even. Let us construct some Azumaya algebras on X from compatible systems of quaternion algebras. We cover X by three open subsets, $X = U_1 \cup U_2 \cup U_3$, where $U_1 \subset \mathbb{A}^1$ is the complement to the closed subset given by $p(x) = 0$, $U_2 \subset \mathbb{A}^1$ is the complement to the closed subset given by $q(x) = 0$, and $U_3 \subset \mathbb{P}^1$ is the complement to the support of the divisor of the rational function $p(x)/x^m$. For any $a \in k^*$ the algebras $Q(a, p(x))$, $Q(a, q(x))$, $Q(a, x^{-m}p(x))$ form a compatible system giving rise to an Azumaya algebra on X.

2.3. **Brauer–Manin obstruction.** For a completion k_v of k and a quaternion algebra Q over k_v we define $\mathrm{inv}_v(Q) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ as follows: $\mathrm{inv}_v(Q) = 0$ if the Hilbert symbol of Q is 1 (i.e. Q is split) and $\mathrm{inv}_v(Q) = \frac{1}{2}$ if the Hilbert symbol of Q is -1 (i.e. Q is non-split). This includes the archimedean and 2-adic completions.

Theorem 2.4. *Let X be a smooth projective irreducible variety over a number field k, and let $\mathcal{A}$ be a quaternion Azumaya algebra on X.*

(1) The evaluation map $\mathcal{A} \mapsto \mathcal{A}(P_v)$ defines a locally constant function $X(k_v) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$;

(2) for almost all places v we have $\mathrm{inv}_v\mathcal{A}(P_v) = 0$ for any $P_v \in X(k_v)$;

(3) for each k-point P we have $\sum_v \mathrm{inv}_v\mathcal{A}(P) = 0$.

Proof. Property (3) immediately follows from the product formula for the Hilbert symbol of $\mathcal{A}(P)$.

To prove (1) choose an open subset U as Proposition 2.3 that contains our k_v-point, so that we can write $\mathcal{A}|_U = Q(f_U, g_U)$. The function f_U (and similarly, g_U) is regular and invertible on U, so it gives a function $U(k_v) \to k_v^*$. Regular functions are continuous in local topology. The value of the Hilbert symbol of $Q(f_U, g_U)$ depends only on the composition of f_U and g_U with the natural map $k_v^* \to k_v^*/k_v^{*2}$. This composition is locally constant, hence we get (1).

Let us prove (2). The variety X is a closed subvariety of a projective space, $X \subset \mathbb{P}^n_k$. Let $(x_0 : \ldots : x_n)$ be homogeneous coordinates in $\mathbb{P}^n_k$. Then $\mathbb{P}^n_k$ is covered by $n+1$ affine spaces $\mathbb{A}^n_i$ given by $x_i \neq 0$. Fix an open covering of X as in Proposition 2.3. We can refine it and assume that each U_j is contained in some affine space $\mathbb{A}^n_i$. We have $U_j = X \setminus Z_j$, where Z_j is a closed subset of X. The intersection of these closed subsets is empty, hence, by the projective version of Hilbert's Nullstellensatz, the sum of the corresponding homogeneous ideals contains a power of the ideal $(x_0, \ldots, x_n)$, i.e. the ideal generated by all monomials of degree m for some $m \geq 1$.

Let O be the ring of integers of k. If S is a finite set of primes of k we denote by O_S the localisation of O at S. We are going to build a model over O_S for some finite set S. There is a finite set of places S such that the equations of X and of each Z_j have coefficients in O_S. We then obtain a closed subscheme $\mathcal{X} \subset \mathbb{P}^n_{O_S}$ and also closed subschemes $\mathcal{Z}_j \subset \mathcal{X}$. Every monomial of degree m is a linear combination of the equations of $\mathcal{Z}_j$ with coefficients in $k[x_0, \ldots, x_n]$. By enlarging S we can assume that the coefficients are in $O_S[x_0, \ldots, x_n]$. Thus the ideal of the intersection of all the $\mathcal{Z}_j$ in $\mathbb{P}^n_{O_S}$ contains $(x_0, \ldots, x_n)^m$, hence this intersection is empty. Therefore, the open subschemes $\mathcal{U}_j = \mathcal{X} \setminus \mathcal{Z}_j$ form an open covering of $\mathcal{X}$.

Let f be a function f_U or g_U associated to some $U = U_j$. By assumption the support of $\mathrm{div}(f)$ does not meet U. Write f as F/G, where F and G are in $k[x_0, \ldots, x_n]$. By enlarging S we can assume that $F, G \in O_S[x_0, \ldots, x_n]$. The closed subscheme of $\mathbb{P}^n_{O_S}$ given by $F = 0$ is the union of a finite number of irreducible components. If an irreducible component $\mathcal{Y}$ is such that $\mathcal{Y} \times_{O_S} k$ is not empty, then $\mathcal{Y}$ is the Zariski closure of $\mathcal{Y} \times_{O_S} k \subset \mathbb{P}^n_k$ in $\mathbb{P}^n_{O_S}$. If an irreducible component $\mathcal{Y}$ is such that $\mathcal{Y} \times_{O_S} k = \emptyset$, then already $\mathcal{Y} \times_{O_S} O_{S'} = \emptyset$ for a finite set S' containing S. Thus, after increasing S if necessary, we can assume that the closed subscheme of $\mathbb{P}^n_{O_S}$ given by $F = 0$ is the Zariski closure of the closed subscheme of $\mathbb{P}^n_k$ given by the same equation. (Think of a polynomial in one variable, then we need to localise at the primes dividing

the leading coefficient.) Thus we can assume without loss of generality that the zeros of F and G do not meet $\mathcal{U}$.

Let O_v be the ring of integers of k_v, where $v \notin S$. Since $O_S \subset O_v$ we can consider the O_v-schemes obtained from $\mathcal{X}$ and $\mathcal{U}_j$ by the same equations and inequalities. Since $\mathcal{X} \subset \mathbb{P}^n_{O_S}$, any k_v-point of X can be written as $P = (a_0 : \ldots : a_n)$, where all $a_i \in O_v$ and $a_r \in O_v^*$ for some r. To fix ideas, suppose that $a_0 \in O_v^*$. Then $P = (a_1/a_0, \ldots, a_n/a_0) \in \mathbb{A}^n_0(O_v)$. More precisely, $P \in \mathcal{U}_j(O_v)$ for some j. Since the zeros of F and G do not meet $\mathcal{U}$ we have $F(P), G(P) \in O_v^*$. It follows that $f_U(P), g_U(P) \in O_v^*$ hence $\mathrm{inv}_v(f_U(P), g_U(P)) = 0$. The proof of (3) is finished. □

Given (P_v) and $\mathcal{A}$, we obtain a collection $\mathcal{A}(P_v)$ of quaternion algebras over k_v for all v. By Theorem 2.4 (2) we have a well defined element $\sum_v \mathrm{inv}_v \mathcal{A}(P_v) \in \{0, \frac{1}{2}\}$. Let $\big(\prod_v X(k_v)\big)^{\mathcal{A}} \subset \prod_v X(k_v)$ be the set of adèles (P_v) for which this sum is zero. It is called the *Brauer–Manin set* of $\mathcal{A}$. By Thereom 2.4 (1) this is a closed subset of the space of adèles. Its complement is also closed, so the Brauer–Manin set of $\mathcal{A}$ is both open and closed. The product formula implies that the image of $X(k)$ in $\prod_v X(k_v)$ is contained in $\big(\prod_v X(k_v)\big)^{\mathcal{A}}$. If follows that if the intersection of one or many of the Brauer–Manin sets is empty, then $X(k) = \emptyset$. The closure of $X(k)$ in the space of adèles is contained in the Brauer–Manin set of $\mathcal{A}$. In particular, no adèle outside of the Brauer–Manin set of $\mathcal{A}$ can be approximated by a k-point on X.

The above definitions and properties can be carried over to arbitrary Azumaya algebras. The intersection of the Brauer–Manin sets attached to all Azumaya algebras on X is called the *Brauer–Manin set of* X.

Conjecture (Colliot-Thélène–Sansuc) *Let X be a smooth and projective surface over a number field with a surjective morphism $X \to \mathbb{P}^1_k$ such that the fibres are conics. Then the Brauer–Manin set of X is the closure of $X(k)$ in the adelic space $\prod_v X(k_v)$.*

The point of this conjecture is that the Brauer–Manin set of a conic bundle can be explicitly determined, and in many cases quaternion Azumaya algebras are enough for this. This is the subject of the next section.

3. Arithmetic of conic bundles

3.1. **Standard smooth proper models.** Consider a conic over the field $k(t)$, where $char(k)$ is not 2. We can diagonalise a quadratic form that defines it,

$$a_0(t)x_0^2 + a_1(t)x_1^2 + a_2(t)x_2^2 = 0, \quad a_0, a_1, a_2 \in k(t), \tag{3.1}$$

and multiply the coefficients by a common multiple so that $a_0(t), a_1(t), a_2(t) \in k[t]$ and $a_0(t)a_1(t)a_2(t)$ is a separable polynomial. Let us treat $(x_0 : x_1 : x_2)$ as homogeneous coordinates in the projective plane and define the surface $X' \subset \mathbb{A}^1 \times \mathbb{P}^2$ by the above equation.

Exercise. X' is smooth. (Can be done over $\bar{k}$ in local coordinates.)

We would like to build a projective surface, with a morphism to $\mathbb{P}^1_k$. First consider the case when the degrees $d_i = \deg(a_i)$ *have the same parity.* The coefficients of the equation

$$T^{d_0}a_0(1/T)X_0^2 + T^{d_1}a_1(1/T)X_1^2 + T^{d_2}a_2(1/T)X_2^2 = 0 \tag{3.2}$$

are polynomials in T. Let $X'' \subset \mathbb{A}^1 \times \mathbb{P}^2$ be the closed subset it defines, where T is a coordinate in $\mathbb{A}^1$, and $(X_0 : X_1 : X_2)$ are homogeneous coordinates in the plane. Note that X'' is smooth since the product of three coefficients is a separable polynomial in T. We think of these two affine lines as affine pieces of $\mathbb{P}^1$, so that the coordinates are related by $T = 1/t$. Let n_i be the integer such that $2n_i = d_i$ or $2n_i = d_i + 1$, where $i = 0, 1, 2$. This substitution tranforms (3.1) in (3.2). Hence the restrictions of X' and X'' to the intersection of two affine pieces of $\mathbb{P}^1$ are isomorphic and we can glue X' and X'' to define a smooth surface X. It comes equipped with the morphism $\pi : X \to \mathbb{P}^1$ that extends the first projections $X' \to \mathbb{A}^1$ and $X'' \to \mathbb{A}^1$. The fibres of π are projective conics.

Now we consider the case when the degrees of coefficients have different parities. Permuting the variables we can assume that either d_0, d_1 are even and d_2 is odd, or d_0, d_1 are odd, and d_2 is even. Consider take the equation

$$T^{d_0}a_0(1/T)X_0^2 + T^{d_1}a_1(1/T)X_1^2 + T^{d_2+1}a_2(1/T)X_2^2 = 0.$$

A similar gluing process as above gives rise to a variety X equipped with a surjective morphism $\pi : X \to \mathbb{P}^1$ whose fibres are plane conics.

This is sometimes called a *standard model*, in these notes a conic bundle is always assumed to be a standard model. (A standard model is not unique.)

The conic $a_0(t)x_0^2 + a_1(t)x_1^2 + a_2(t)x_2^2 = 0$ over the field $k(t)$ is called the *generic fibre* of π.

Proposition 3.1 (Corollary of Tsen's theorem)**.** *Any conic bundle $\pi : X \to \mathbb{P}^1$ over $\bar{k}$ has a section, that is, there is a morphism $\sigma : \mathbb{P}^1_{\bar{k}} \to X \times_k \bar{k}$ such that the composition $\pi\sigma$ is the identity map.*

Proof. By Theorem 1.5 the generic fibre has a $\bar{k}(t)$-point. We need to show that any $\bar{k}(t)$-point on the generic fibre extends to a section. Taking x, y, z to be polynomials in $\bar{k}[t]$ not divisible by a common factor defines a section of $X' \to \mathbb{A}^1_{\bar{k}}$. Similarly for X''. □

Structure of bad fibres. 1. The degenerate fibres are the fibres over the roots of $a_0(t)a_1(t)a_2(t)$ and, when the parities of the degrees of coefficients are not the same, over $t = \infty$.

2. Each degenerate fibre is geometrically a pair of transversal lines meeting at one point.

3. If $p(t)$ is a monic irreducible factor of $a_0(t)$, then the components of the fibre of π at the closed point $p(t) = 0$ are defined over the extension of $k_p = k[t]/(p(t))$ given by the square root of the image of $-a_1(t)a_2(t)$ in $k[t]/(p(t))$. Similarly for the prime factors of a_1 and a_2, and, in the unequal parity case, for the fibre at infinity. We denote this image by α_p.

4. Without loss of generality we can assume that the fibre at ∞ is smooth. Indeed, replacing t by $t-c$ for some $c \in k$ we can assume that the fibre at $t=0$ is smooth. Now let $t=1/T$.

Note that the generic fibre of π is the conic attached to the quaternion algebra

$$Q = Q(-a_0a_1, -a_0a_2) = Q(-a_0a_1, -a_1a_2).$$

Lemma 3.2. *The class of α_p in k_p^*/k_p^{*2} equals the residue $Res_p(Q)$.*

This is clear from (1.1).

Corollary 3.3 (of Faddeev reciprocity law)**.** *We have $\prod_p N_{k_p/k}(\alpha_p) \in k^{*2}$.*

This is an immediate consequence of Theorem 1.12. In the unequal parity case this product includes $p=\infty$ for which we have $k_\infty = k$.

Definition. A standard smooth conic bundle X given by the equation

$$x^2 - ay^2 = b(t)z^2,$$

where $a \in k^* \setminus k^{*2}$ and $b(t)$ is a separable polynomial, is called a (generalised) Châtelet surface.

Exercise. 1. Check that a standard model of a Châtelet surface always has an even number of bad fibres, equal to $\deg(b)$ or $\deg(b)+1$. If $\deg(b)$ is odd, then X has a k-point (check the fibre at infinity).

2. If $b(t)$ is a norm from $k(t, \sqrt{a})$, then the generic fibre has a $k(t)$-point, and so is a rational curve over $k(t)$. Thus $k(X)$ is a purely transcendental extension of k, i.e. X is rational over k. Arithmetic properties of such varieties are of no interest, so we can exclude this case.

3. Check that $\pi : X \to \mathbb{P}^1$ has two disjoint sections $\sigma_\pm$ corresponding to the $\bar{k}(t)$-points of the generic fibre with coordinates $(\pm\sqrt{a} : 1 : 0)$.

We now assume that the quaternion algebra $Q(a, b(t))$ over $k(t)$ is not split. Let $C_\pm = \sigma_\pm(\mathbb{P}^1)$.Then $C = C_+ \cup C_-$ is a k-curve on X. Define $X_0 = X \setminus C$ and $X_0' = X' \cap X_0$.

Lemma 3.4. *Let X be a Châtelet surface. For each factor $p(t)$ of $b(t)$ there is a quaternion Azumaya algebra $\mathcal{A}_p$ on X_0' such that $\mathcal{A}_p|_U = Q(a, p(t))$, where $U \subset X_0'$ is the complement to the zero set of $p(t)$. If $\deg(p(t))$ is even, then $\mathcal{A}_p$ extends to a quaternion Azumaya algebra on X_0.*

Proof. Let us use the converse to Proposition 2.3. The open set $X_0' = X' \cap X_0$ of X' is given by $z \neq 0$, so X_0' is a closed subset of $\mathbb{A}^3$ with equation

$$x^2 - ay^2 = b(t).$$

Let $V \subset X_0'$ be the complement to the zero set of the polynomial $b(t)/p(t)$. Then $b(t) \in k[U \cap V]^*$ is the norm of $x + \sqrt{a}y \in k(\sqrt{a})[U \cap V]^*$. Thus the $\mathcal{O}_U$-algebra $Q(a, p(t))$ and the $\mathcal{O}_V$-algebra $Q(a, b(t)/p(t))$ have isomorphic restrictions to $U \cap V$, so they form a compatible system and hence give rise to a quaternion Azumaya algebra $\mathcal{A}_p$ on X_0'.

The last claim will follow if we set $W \subset X_0$ to be the complement to the zero set of $tb(t)$. Then the $\mathcal{O}_W$-algebra $Q(a, p(t)/t^{2n})$ and $\mathcal{A}_p$ restrict to isomorphic algebras over $W \cap X_0'$, so we are done. $\square$

We note that $Res_C(\mathcal{A}_p) = 1$ since a and $b(t)$ belong to the group of units of the local ring of C. Thus $\mathcal{A}_p$ is unramified on X'.

A standard calculation shows that $Res_\infty(\mathcal{A}_p)$ is the image of the class of a under the map $k^*/k^{*2} \to k(X_\infty)^*/k(X_\infty)^{*2}$. Assume first that X_∞ is smooth. This image is trivial if and only if $a = h^2$ for some $h \in k(X_\infty)^* \setminus k^*$. Then $h \in k[X_\infty]^*$, and since h is not constant it must take both values $\sqrt{a}$ and $-\sqrt{a}$ on $\bar{k}$-points of X. This implies that $\overline{X}$ is a union of two closed subsets, hence is not irreducible, which is a contradiction. Thus a defines a non-trivial class in $k(X_\infty)^*/k(X_\infty)^{*2}$. This is the case when the degree of $b(t)$ is even and the degree of $p(t)$ is odd.

If the degree of $b(t)$ is odd, the same computation shows that the residue at infinity is trivial because on the singular conic $x^2 - ay^2 = 0$ we have $a = h^2$, where $h = x/y$.

Recall that a quaternion algebra over $k(X)$ is called unramified if it has trivial residue at each irreducible divisor of X. We conclude that the *unramified* quaternion algebras of the form $\mathcal{A}_p$ form a finite abelian group $(\mathbb{Z}/2)^r$ if all r irreducible factors of $b(t)$ have even degree, and $(\mathbb{Z}/2)^{r-1}$ otherwise. By Grothendieck's purity theorem unramified $k(X)$-algebras are equivalent to Azumaya algebras, and so define a class in $\mathrm{Br}(X)$, and not just in the bigger group $\mathrm{Br}(k(X))$.

The structure of $\mathrm{Br}(X)$. 1. We know that he $k(t)$-algebra $Q(a, b(t))$ is split over the field of functions of the $k(t)$-conic $C(a, b(t))$, that is, over the field $k(X)$.

2. If a is a square in $k_p = k[t]/(p(t))$, then the $k(t)$-algebra $Q(a, p(t))$ is split. (Proof: Since $k(\sqrt{a}) \subset k_p$, the degree of $p(t)$ is even. All residues of this algebra are trivial, hence, by Faddeev's exact sequence, it comes from $\mathrm{Br}(k)$. Since $p(t)$ is monic, the algebra specialises at infinity to the k-algebra $Q(a, 1)$ which is split.)

3. It is a fact that the algebras $\mathcal{A}_p$, where $p(t)$ is a monic irreducible factor of $b(t)$ such that a is not a square in k_p, generate $\mathrm{Br}(X')$ modulo the image of $\mathrm{Br}(k)$. Let n be the number of such factors. By Fact 1 the product of all these algebras comes from $\mathrm{Br}(k)$.

4. The arguments above show that if the degree of $b(t)$ is even, then $\mathrm{Br}(X)$ is the kernel of the map $\mathrm{Br}(X') \to \mathbb{Z}/2$ that sends $\mathcal{A}_p$ to $\deg(p(t)) \bmod 2$. Therefore, in this case the cokernel of $\mathrm{Br}(k) \to \mathrm{Br}(X)$ is isomorphic to $(\mathbb{Z}/2)^{n-1}$ if all the degrees of $p(t)$ are even, and to $(\mathbb{Z}/2)^{n-2}$ otherwise. If the degree of $b(t)$ is odd, then $\mathrm{Br}(X) = \mathrm{Br}(X')$, and modulo the image of $\mathrm{Br}(k)$ this group is isomorphic to $(\mathbb{Z}/2)^{n-1}$.

These facts will not be used in what follows (though they are not too hard to prove).

3.2. **Conic bundles over number fields: main theorems and examples.** We can now state the first main theorem of this course. It was proved in [2].

Theorem 3.5 (Colliot-Thélène, Sansuc, Swinnerton-Dyer)**.** *Let k be a number field, and let X be a Châtelet surface with* $\deg(b(t)) \le 4$. *Then the closure of $X(k)$ in the space of adèles of X is the Brauer–Manin set of X.*

If $\deg(b(t))$ is 1 or 2, then X is birationally equivalent to a quadric, and then the theorem follows from the Hasse–Minkowski theorem. If $\deg(b(t)) = 3$, the Brauer–Manin set of X is the intersection of the Brauer–Manin sets attached to all $\mathcal{A}_p$. The case when $\deg(b(t)) = 4$ and $b(t)$ has a linear factor can be reduced to this case. If $b(t) = p(t)q(t)$, where $p(t)$ and $q(t)$ are irreducible, then the Brauer–Manin set of X is the Brauer–Manin set of $\mathcal{A}_p$. Finally, if $b(t)$ is irreducible of degree 4, then the Hasse principle and weak approximation hold (the same is true if $b(t)$ is irreducible of degree 3).

The proof of Theorem 3.5 will be sketched in Section 3.5.

Theorem 3.5 has a curious corollary. An integer $n = 2^r m$, where m is odd, can be written as

$$n = a^2 + b^2 + c^4, \quad a, b, c \in \mathbb{Q}$$

if and only if we are not in any of the following cases: $4|r$ and $m \equiv 7 \bmod 8$, or $2||r$ and $m \equiv 3 \bmod 4$. This is an application of the Hasse principle in the case when $b(t) = n - t^4$ is irreducible, which is the case when n is not a square. Local solubility is easy for $p \ne 2$, and is easy but tedious for $p = 2$.

Example (Iskovskikh, Sansuc) Consider the Châtelet surface X_c over $k = \mathbb{Q}$

$$x^2 + 3y^2 = (c - t^2)(t^2 - c + 1) \tag{3.3}$$

where $c \in \mathbb{Z}$, $c \ne 0$, $c \ne 1$. One sees immediately that $X_c(\mathbb{R}) \ne \emptyset$ if and only if $c > 1$. The local solubility of (3.3) in $\mathbb{Q}_p$ for any prime p imposes no restriction on c. This is easily seen for $p \ne 3$ by setting $t = p^{-1}$ and using the fact that a unit is a norm for an unramified extension. For $p = 3$ the solubility of (3.3) is established by a case by case computation.

Consider the quaternion algebra $\mathcal{A} = \mathcal{A}_{c-t^2} = \mathcal{A}_{t^2-c+1}$. As was discussed above, this algebra defines a class in $\mathrm{Br}(X_c)$ and this class generates this group modulo the image of $\mathrm{Br}(\mathbb{Q})$, so to compute the Brauer–Manin obstruction we only need to compute the sum $\sum_v \mathrm{inv}_v(\mathcal{A}(P_v))$, $P_v \in X_c(\mathbb{Q}_v)$.

Statement 1*: If $v \ne 3$, then* $\mathrm{inv}_v(\mathcal{A}(P_v)) = 0$ *for any point $P_v \in X_c(\mathbb{Q}_v)$.* This value is locally constant in the v-adic topology, hence we may assume that P_v is not contained in the fibre at infinity or in any of the singular fibres, that is, $(c-t^2)(t^2-c+1) \ne 0$. We must prove that $c - t^2$ is locally a norm for the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. For $\mathbb{Q}_v = \mathbb{R}$ this easily follows since $c - t^2 > 0$. For a finite $v \ne 3$ we only have to consider the case when p is inert for $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. We have two possibilities: $v(t) < 0$ and $v(t) \ge 0$. In the first case $v(c - t^2)$ is even, hence this is the product of a unit, which is a norm for the unramified extension $\mathbb{Q}_v(\sqrt{-3})$, and an even power of a uniformizer, which is trivially a norm for any quadratic extension. Since $(c - t^2) + (t^2 - c + 1) = 1$, in the

second case either $v(c-t^2)=0$, then $c-t^2$ is a norm, or $v(t^2-c+1)=0$. Then from the equation of X_c it follows that $c-t^2$ is a norm multiplied by a unit, hence is a norm.

Statement 2*: For* $v=3$ *and* $c=3^{2n+1}(3m+2)$ *we have* $\mathrm{inv}_3(\mathcal{A}(P_3))=\frac{1}{2}$ *for any point* $P_3\in X_c(\mathbb{Q}_3)$*, whereas for other values of* c *the local invariant takes both values* 0 *and* $\frac{1}{2}$*.* This purely local computation is omitted here.

Conclusion. When the sum of local invariants is never 0, the Manin obstruction tells us that no $\mathbb{Q}$-point can exist on X_c. This happens for $c=3^{2n+1}(3m+2)$, whereas X_c has adelic points for any $c>1$. Theorem 3.5 implies that in all the other cases for $c\in\mathbb{Z}$, $c>1$, the surface X_c contains a $\mathbb{Q}$-point.

Here is the second main theorem. This and more general results were proved in [1].

Theorem 3.6 (Browning, Matthiesen, AS, based on Green, Tao, Ziegler)**.** *Let* X *be a Châtelet surface over* $\mathbb{Q}$ *such that* $b(t)$ *is totally split over* $\mathbb{Q}$*. Then the closure of* $X(k)$ *in the space of adèles of* X *is the Brauer–Manin set of* X*.*

By a change of variables we can assume that $\deg(b(t))$ is odd. Then the Brauer–Manin set of X is the intersection of the Brauer–Manin sets attached to the classes of $\mathcal{A}_{t-e}$ in $\mathrm{Br}(X)$, where e is a root of $b(t)$.

The proof of Theorem 3.6 is given in Sections 3.3 and 3.4.

This result is interesting because it implies the existence of many (in fact, a Zariski dense set of) solutions in $\mathbb{Q}$ besides the obvious ones for which $b(t)=0$.

3.3. **Descent.** Let us first assume that $k=\mathbb{Q}$ and all the singular fibres of $X\to\mathbb{P}^1_{\mathbb{Q}}$ are above $\mathbb{Q}$-points of $\mathbb{P}^1_{\mathbb{Q}}$. We can choose the point at infinity in $\mathbb{P}^1_{\mathbb{Q}}$ in such a way that the corresponding $\mathbb{Q}$-fibre is singular. Then our Châtelet surface X contains an open subset $X_0'\subset\mathbb{A}^3_{\mathbb{Q}}$ given by the equation

$$x^2-ay^2=b\prod_{i=1}^{n}(t-e_i), \tag{3.4}$$

where n is odd, $a,b\in\mathbb{Q}^*$, and $e_1,\dots,e_n$ are pairwise different elements of $\mathbb{Q}$. Recall that $X_0\subset X$ is given by $x^2-ay^2\neq 0$. By Lemma 3.4 for each $i=1,\dots,n$ we have a quaternion Azumaya algebras $\mathcal{A}_i$ on X_0, which restricts to $Q(a,t-e_i)$ on the open subset $\prod_{i=1}^n(t-e_i)\neq 0$. We checked that these algebras are unramified on X.

Suppose we are given an adèle (M_p) on X, where we include a real point $M_0\in X(\mathbb{R})$, such that

$$\sum_p \mathrm{inv}_p(\mathcal{A}_i(M_p))=0\ \in\ \frac{1}{2}\mathbb{Z}/\mathbb{Z},\quad i=1,\dots,n.$$

By a small deformation that does not change $\mathrm{inv}_p(\mathcal{A}_i(M_p))$ we can assume that M_p lies in $X_0'(\mathbb{Q}_p)$, and, moreover, the t-coordinate of M_p, call it t_p, is

such that $t_p \neq e_i$, $i = 1, \dots, n$. Then

$$\sum_p \mathrm{inv}_p\left((a, t_p - e_i)\right) = 0 \ \in \ \frac{1}{2}\mathbb{Z}/\mathbb{Z}, \quad i = 1, \dots, n.$$

or, in terms of the Hilbert symbol, we have

$$\prod_p (a, t_p - e_i)_p = 1, \quad i = 1, \dots, n.$$

Lemma 3.7. *Let $a \in \mathbb{Q}^*$. Let $\tau_p \in \mathbb{Q}_p^*$ for all primes p, and $\tau_0 \in \mathbb{R}^*$ be such that $(a, \tau_p)_p = 1$ for almost all p and $\prod_p (a, \tau_p)_p = 1$. Then there exists $c \in \mathbb{Q}^*$ such that $(a, \tau_p)_p = (a, c)_p$ for all p.*

Proof. (cf. [8, Ch. III, Thm. 4]) We can assume that $a \in \mathbb{Z}$. Using weak approximation in $\mathbb{Q}$ we find $d \in \mathbb{Q}^*$ such that $d\tau_p \in \mathbb{Q}_p^{*2}$ for all $p|2a$, and $d\tau_0 > 0$. After replacing τ_p by $d\tau_p$ we obtain that $(a, \tau_p)_p = 1$ for each $p|2a$, and $(a, \tau_0)_0 = 1$. Let b be the product of all primes p such that $(a, \tau_p)_p = -1$. (By construction b is odd.) By Dirichlet's theorem on primes in an arithmetic progression we can find a prime $q = b + 8am$ for some large integer m, so that q does not divide $2ab$. We claim that $c = bq$ will work. We need to check that $(a, \tau_p)_p = (a, bq)_p$ for all p, including $p = 0$.

If $\mathbb{Q}_v = \mathbb{R}$, then $1 = (a, \tau_0)_0 = (a, bq)_0$ because $bq > 0$.

If $p = 2$, then $(a, \tau_2)_2 = 1$. But $bq \equiv b^2 \bmod 8$, but this implies that $bq \in \mathbb{Q}_2^{*2}$. Thus $(a, bq)_2 = 1$.

If p is an odd prime factor of a, then $(a, \tau_p)_p = 1$. But $bq \equiv b^2 \bmod p$, and hence $bq \in \mathbb{Q}_p^{*2}$. Thus $(a, bq)_p = 1$.

For the remaining primes p we have $a \in \mathbb{Z}_p^*$. If p is coprime to bq, then $(a, \tau_p)_p = 1$ but we also have $(a, bq)_p = 1$.

If $p|b$, then since $(a, \tau_p)_p = -1$ and a is a unit, $\mathrm{val}_p(\tau_p)$ must be odd and a not a square modulo p. Since $\mathrm{val}_p(bq) = 1$ we then have $(a, bq)_p = -1$.

Finally, we are left with checking that at the last remaining prime q we have $(a, \tau_q)_q = (a, bq)_q$, but by the previous cases this follows from the condition $\prod_p (a, \tau_p)_p = 1$ and the product formula $\prod_p (a, bq)_p = 1$. □

Corollary 3.8. *In the assumptions of Lemma 3.7 there exists $c \in \mathbb{Q}^*$ such that for each prime p we have $c\tau_p = x_p^2 - ay_p^2$, where $x_p, y_p \in \mathbb{Q}_p$.*

Proof. If $a \in \mathbb{Q}_p^{*2}$ there is nothing to prove. Otherwise $\mathbb{Q}_p(\sqrt{a})$ is a quadratic extension of $\mathbb{Q}_p$. The condition $(a, c\tau_p)_p = 1$ means that the quaternion algebra $Q(a, c\tau_p)$ over $\mathbb{Q}_p$ is split, and then $c\tau_p$ is a norm from $\mathbb{Q}_p(\sqrt{a})$ by Proposition 1.2. □

By Corollary 3.8 there exist $c_i \in \mathbb{Q}^*$, $i = 1, \dots, n$, such that

$$c_i(t_p - e_i) = x_{i,p}^2 - ay_{i,p}^2$$

for all i and p (including $p = 0$). Consider the variety $W' \subset \mathbb{A}_{\mathbb{Q}}^{2n+1}$ given by the equations

$$c_i(t - e_i) = x_i^2 - ay_i^2, \quad i = 1, \dots, n. \tag{3.5}$$

We have proved that $t_p \in \mathbb{A}^1_{\mathbb{Q}}(\mathbb{Q}_p)$ is the image of a $\mathbb{Q}_p$-point on W' under the projection $W' \to \mathbb{A}^1_{\mathbb{Q}}$. But then $t_p \in \mathbb{A}^1_{\mathbb{Q}}(\mathbb{Q}_p)$ lifts to a $\mathbb{Q}_p$-point on the variety given by

$$x^2 - ay^2 = b\prod_{i=1}^{n}(t-e_i), \quad c_i(t-e_i) = x_i^2 - ay_i^2, \quad i = 1, \dots, n$$

which is none other but the fibred product $X'_0 \times_{\mathbb{A}^1_{\mathbb{Q}}} W'$. An obvious change of variables shows that this fibred product is birationally equivalent to the product of W' and the conic C with the equation

$$x^2 - ay^2 = b/c_1 \dots c_n.$$

Let us rewrite the equations of W' in a slightly different form. We introduce two independent variables x_0, y_0 and write $v = x_0^2 - ay_0^2$, $u = tv$. Then an easy change of variables shows that $\mathbb{A}^2_{\mathbb{Q}} \times W'$ is birationally equivalent to the closed subvariety $W \subset \mathbb{A}^{2n+2}_{\mathbb{Q}}$ given by

$$v = x_0^2 - ay_0^2, \quad c_i(u - e_i v) = x_i^2 - ay_i^2, \quad i = 0, \dots, n. \tag{3.6}$$

Conclusion of the descent argument: *If the intersection of the Brauer–Manin sets attached to $\mathcal{A}_i$ is non-empty, then $C \times W$ has points everywhere locally. In particular, if W satisfies the Hasse principle and weak approximation, then $X(\mathbb{Q})$ is dense in the intersection of the Brauer–Manin sets attached to $\mathcal{A}_i$, $i = 1, \dots, n$.*

This follows from Legendre's theorem and weak approximation in the affine space. It is an amazing fact that W does satisfy the Hasse principle and weak approximation. This is a consequence of recent spectacular advances in additive combinatorics, see Theorem 3.11 below.

3.4. **Corollary of the Green–Tao–Ziegler theorem.** In a series of papers Green–Tao [4, 5] and Green–Tao–Ziegler [6] proved the generalized Hardy–Littlewood conjecture in the finite complexity case. The following qualitative statement is [4, Cor. 1.9].

Theorem 3.9 (Green, Tao, Ziegler)**.** *Let $L_1(x,y), \dots, L_r(x,y) \in \mathbb{Z}[x,y]$ be pairwise non-proportional linear forms, and let $c_1, \dots, c_r \in \mathbb{Z}$. Assume that for each prime p, there exists $(m,n) \in \mathbb{Z}^2$ such that p does not divide $L_i(m,n) + c_i$ for any $i = 1, \dots, r$. Let $K \subset \mathbb{R}^2$ be an open convex cone containing a point $(m,n) \in \mathbb{Z}^2$ such that $L_i(m,n) > 0$ for $i = 1, \dots, r$. Then there exist infinitely many pairs $(m,n) \in K \cap \mathbb{Z}^2$ such that $L_i(m,n) + c_i$ are all prime.*

A famous particular case is the system of linear forms $x, x+y, \dots, x+(r-1)y$. In this case the result is the existence of arithmetic progressions in primes of arbitrary length r.

We shall use the following easy corollary of Theorem 3.9. For a finite set of rational primes S we write $\mathbb{Z}_S = \mathbb{Z}[S^{-1}]$.

Proposition 3.10. *Suppose that we are given $(\lambda_p, \mu_p) \in \mathbb{Q}_p^2$ for p in a finite set of primes S, and a positive real constant C. Let $e_1, \dots, e_r$ be pairwise different elements of $\mathbb{Z}_S$. Then there exist infinitely many pairs $(\lambda, \mu) \in \mathbb{Z}_S^2$ and pairwise different primes $p_1, \dots, p_r$ not in S such that*

(1) $\lambda > C\mu > 0$;
(2) (λ, μ) *is close to* (λ_p, μ_p) *in the p-adic topology for $p \in S$;*
(3) $\lambda - e_i\mu = p_i u_i$, *where $u_i \in \mathbb{Z}_S^*$, for $i = 1, \dots, r$.*

Proof. (The proof follows [12].) We can multiply λ, μ and all λ_p, μ_p by a product of powers of primes from S, and so assume without loss of generality that $(\lambda_p, \mu_p) \in \mathbb{Z}_p^2$ for $p \in S$.

Using the Chinese remainder theorem, we find $\lambda_0 \in \mathbb{Z}$ such that $\lambda_0 - \lambda_p$ is divisible by a sufficiently high power p^{n_p} for all $p \in S$, and similarly for $\mu_0 \in \mathbb{Z}$. In doing so we can assume that $\lambda_0 > C\mu_0 > 0$ and that $\lambda_0 - e_i\mu_0 \neq 0$ for all i.

Let d be the product of denominators of $e_1, \dots, e_r$. So d is only divisible by primes from S. Let us write $d(\lambda_0 - e_i\mu_0) = M_i c_i$, where M_i is a product of powers of primes from S, and $c_i \in \mathbb{Z}$ is coprime to the primes in S. Let N be a product of primes in S such that $N > |c_i \pm c_j|$ for any i and j. Let $M = \prod_{p \in S} p^{m_p}$ where

$$m_p \geq \max\{n_p, \mathrm{val}_p(N) + \mathrm{val}_p(M_i)\}, \quad i = 1, \dots, r.$$

Then N divides M/M_i for each i. We now look for λ and μ of the form

$$\lambda = \lambda_0 + Mm, \quad \mu = \mu_0 + Mn, \quad (m, n) \in \mathbb{Z}^2. \tag{3.7}$$

Write $L_i(x, y) = M_i^{-1} M d(x - e_i y)$, then

$$\lambda - e_i\mu = d^{-1} M_i (L_i(m, n) + c_i) \tag{3.8}$$

for each $i = 1, \dots, r$. Let us check that the linear functions $L_i(x, y) + c_i$ satisfy the condition of Theorem 3.9. For $p \in S$, the integer $L_i(0, 0) + c_i$ is non-zero modulo p for each i. Now let p be a prime not in S. Since the determinant of the homogeneous part of the affine transformation (3.7) is in $\mathbb{Z}_S^*$ and each $M_i^{-1} d(x - e_i y)$ equals $M_i^{-1} d \in \mathbb{Z}_S^*$ at the point $(1, 0)$, we see that there is $(m, n) \in \mathbb{Z}^2$ such that $\prod_{i=1}^r (L_i(m, n) + c_i)$ is not divisible by p.

We now choose an open convex cone K. Take $(m_0, n_0) \in \mathbb{Z}^2$, $m_0 > Cn_0 > 0$, for which the integers $|L_i(m_0, n_0)|$ are pairwise different and non-zero. Let $\varepsilon_i = \pm 1$ be the sign of $L_i(m_0, n_0)$. After re-ordering the subscripts, we have

$$\varepsilon_1 L_1(m_0, n_0) > \ldots > \varepsilon_r L_r(m_0, n_0) > 0.$$

Define $K \subset \mathbb{R}^2$ by the inequalities

$$x > Cy > 0, \quad \varepsilon_1 L_1(x, y) > \ldots > \varepsilon_r L_r(x, y) > 0.$$

We can apply Theorem 3.9 to the linear functions $\varepsilon_i(L_i(x, y) + c_i)$ and the cone K. Thus there exist infinitely many pairs $(m, n) \in K \cap \mathbb{Z}^2$ such that $\varepsilon_i(L_i(m, n) + c_i) = p_i$, where p_i is a prime not in S, for $i = 1, \dots, r$. The coefficients of each $L_i(x, y)$ are divisible by N, hence

$$\varepsilon_i L_i(m, n) - \varepsilon_{i+1} L_{i+1}(m, n) \geq N > \varepsilon_{i+1} c_{i+1} - \varepsilon_i c_i.$$

Thus $p_i > p_{i+1}$ for each $i = 1, \dots, r-1$, so all the primes p_i are pairwise different. Since $n > 0$ and $m > Cn$ we see that $\mu = \mu_0 + Mn > 0$ and $\lambda = \lambda_0 + Mm > C\mu$.

By (3.8) we see that $\lambda - e_i\mu$ differs from $\varepsilon_i(L_i(x,y) + c_i)$ by an element of $\mathbb{Z}_S^*$, so the proof is now complete. □

Theorem 3.11. *Let $a_i \in \mathbb{Q}^*$, $c_i \in \mathbb{Q}^*$ and $e_i \in \mathbb{Q}$, for $i = 1, \dots, r$, be such that $e_i \neq e_j$ for $i \neq j$. Then the variety $W \subset \mathbb{A}^{2r+2}_{\mathbb{Q}}$ defined by*

$$c_i(u - e_i v) = x_i^2 - a_i y_i^2 \neq 0, \quad i = 1, \dots, r, \tag{3.9}$$

satisfies the Hasse principle and weak approximation.

Proof. (The proof follows [12].) We are given $M_p \in W(\mathbb{Q}_p)$ for each prime p, and $M_0 \in W(\mathbb{R})$. Let S be the set of places of $\mathbb{Q}$ where we need to approximate. We include the real place in S. Note that the set of real points $(u, v, x_1, \dots, x_r, y_1, \dots, y_r) \in W(\mathbb{R})$ for which $(u, v) \in \mathbb{Q}^2$ is dense in $W(\mathbb{R})$, and so it will be enough to prove the claim in the case when the coordinates u and v of M_0 are in $\mathbb{Q}$. By a $\mathbb{Q}$-linear change of variables we can assume without loss of generality that M_0 has coordinates $(u, v) = (1, 0)$. Then we have $c_i > 0$ whenever $a_i < 0$.

We enlarge S so that $c_i \in \mathbb{Z}_S^*$, $e_i \in \mathbb{Z}_S$ and all the primes dividing a_i are in S, for all $i = 1, \dots, r$. For these new primes we take (λ_p, μ_p) defined by some $\mathbb{Q}_p$-point on W. Thus for each $p \in S$ we now have a pair $(\lambda_p, \mu_p) \in \mathbb{Q}_p^2$ such that

$$c_i(\lambda_p - e_i\mu_p) = x_{i,p}^2 - a_i y_{i,p}^2 \neq 0, \quad i = 1, \dots, r,$$

for some $x_{i,p}, y_{i,p} \in \mathbb{Q}_p$. Applying Proposition 3.10 we produce $(\lambda, \mu) \in \mathbb{Z}_S^2$ such that $\lambda > C\mu > 0$, where C is a large positive constant to be specified later. Moreover, for each i the number $c_i(\lambda - e_i\mu) = p_i u_i$, where $u_i \in \mathbb{Z}_S^*$ and p_i is a prime not in S, is a local norm for $\mathbb{Q}(\sqrt{a_i})/\mathbb{Q}$ for any finite place in S. This is also true for the real place because $b_i > 0$ whenever $a_i < 0$, and $\lambda - e_i\mu > 0$ for all i.

Consider the class of the quaternion algebra $Q(a_i, c_i(\lambda - e_i\mu))$ in $\mathrm{Br}(\mathbb{Q})$. By continuity we have $\mathrm{inv}_p(a_i, c_i(\lambda - e_i\mu)) = 0$ for any $p \in S$, and also $\mathrm{inv}_{\mathbb{R}}(a_i, c_i(\lambda - e_i\mu)) = 0$. Next, $c_i(\lambda - e_i\mu)$ is a unit at every prime $p \notin S \cup \{p_i\}$, hence we obtain

$$\mathrm{inv}_p(a_i, c_i(\lambda - e_i\mu)) = 0$$

for any $p \neq p_i$. The global reciprocity law now implies

$$\mathrm{inv}_{p_i}(a_i, c_i(\lambda - e_i\mu)) = \mathrm{inv}_{p_i}(a_i, p_i) = 0,$$

and since the prime factors of a_i are in S, the prime p_i splits completely in $\mathbb{Q}(\sqrt{a_i})$. In particular, $c_i(\lambda - e_i\mu)$ is a local norm at every place of $\mathbb{Q}$. By Legendre's theorem $c_i(\lambda - e_i\mu)$ is a global norm. This proves the Hasse principle for W.

Let us now prove weak approximation. Using weak approximation in $\mathbb{Q}$ we find a positive rational number ρ that is p-adically close to 1 for each prime

$p \in S$, and ρ^2 is close to $\lambda > 0$ in the real topology. We now make the change of variables

$$\lambda = \rho^2 \lambda', \quad \mu = \rho^2 \mu', \quad i = 1, \dots, r.$$

Then (λ', μ') is still close to (λ_p, μ_p) in the p-adic topology for each prime $p \in S$. In the real topology (λ', μ') is close to $(1, \mu/\lambda)$. Since $0 < \mu/\lambda < C^{-1}$, by choosing a large enough C we ensure that (λ', μ') is close to $(1, 0)$. We can conclude by using weak approximation for the variety $x^2 - a_i y^2 = 1$, which is an open subset of $\mathbb{P}^1_{\mathbb{Q}}$. $\square$

This finishes the proof of Theorem 3.6.

3.5. **Geometry of certain intersections of quadrics.** In the remaining part of these notes we sketch the proof of Theorem 3.5. The details can be found in Chapter 7 of [11].

If $\deg b(t) \le 2$, the Châtelet surface is birationally equivalent to a quadric, so the Hasse principle is a consequence of the Hasse–Minkowski theorem. Smooth quadrics with a rational point are rational, so weak approximation holds too.

Let us now assume that $\deg b(t) = 3$ or $\deg b(t) = 4$ and $b(t)$ has a root in $\mathbb{Q}$. The second case reduces to the first one by a change of variable t. We have points $M_v \in X_0'(k_v)$ for each place v of k, where the t-coordinates t_v of M_v are such that $b(t_v) \neq 0$. All algebras $\mathcal{A}_q$, where $q(t)$ is a monic irreducible factor of $b(t)$, are unramified and so give rise to Brauer–Manin conditions. The Brauer–Manin condition given by $\mathcal{A}_q$ is

$$\prod_v (a, q(t_v))_v = 1,$$

where v ranges over all places of k. Let $K = k[t]/(q(t))$ and let θ be the image of t in K. Under the $[K : k]$ distinct embeddings of K into $\bar{k}$ the element θ goes to $[K : k]$ different roots of $q(t) = 0$. We have $q(t) = N_{K/k}(t - \theta)$. Consider the primes of the number field $K = k[t]/(q(t))$ over v. We have $k_v \otimes_k K = \oplus_{w|v} K_w$. Then

$$\begin{aligned}(a, q(t_v))_v = (a, N_{K/k}(t_v - \theta))_v &= \\ (a, \prod_{w|v} N_{K_w/k_v}(t_v - \theta))_v &= \prod_{w|v} (a, N_{K_w/k_v}(t_v - \theta))_v = \prod_{w|v} (a, t_v - \theta)_w.\end{aligned}$$

(The last equality follows from the relation between corestriction and residue, see [9, Prop. XI.2.1 (ii)].) Thus the Brauer–Manin condition can be rewritten as

$$\prod_w (a, t_v - \theta)_w = 1,$$

where w ranges over all places of K. As in Lemma 3.7 one proves that there exists $c(\theta) \in K^*$ such that the quaternion algebra $Q(a, c(\theta)(t_v - \theta))$ over K_w is split for each w. Thus we can write $c(\theta)(t_v - \theta) = x_w^2 - a y_w^2$ for some $x_w, y_w \in K_w$. Define the variety W' by equations $c(\theta)(t - \theta) = x(\theta)^2 - a y(\theta)^2$, one equation for each monic irreducible factor $q(t)$ of $b(t)$. This equation with coefficients in K is equivalent to $[K : k]$ equations with coefficient in k. Over

$\bar{k}$ all these equations together become three equations (3.5) where c_i are the images of $c(\theta)$ under all different embeddings of K into $\bar{k}$. We see, as before, that each t_v lifts to a k_v-point on W' and hence to a k_v-point on the fibred product of W' and X_0' over the affine line. This fibred product is birationally equivalent to the product of W' and a conic. As above, we can work with the variety W defined by equations $c(\theta)(u-\theta v) = x(\theta)^2 - ay(\theta)^2$, one equation for each monic irreducible factor $q(t)$ of $b(t)$, together with $u = x_0^2 - ay_0^2$.

Let us now deal with the case when $\deg b(t) = 4$ and $b(t)$ is either irreducible or a product of two irreducible quadratics. Then the Brauer–Manin condition given by $\mathcal{A}_q$, where $q(t)$ is any monic irreducible factor of $b(t)$, is

$$\prod_v (a, q(t_v))_v = 1.$$

Since $\deg q(t)$ is even, we can rewrite this as

$$\prod_v (a, q(u_v, v_v))_v = 1,$$

where $t_v = u_v/v_v$, and $q(u,v) = v^{\deg q(t)}(u/v)$. The same calculation as above shows that this implies

$$\prod_w (a, u_v - \theta v_v)_w = 1,$$

where w ranges over all places of K. Let W be the variety defined by the equations $c(\theta)(u-\theta v) = x(\theta)^2 - ay(\theta)^2$, one equation for each monic irreducible factor $q(t)$ of $b(t)$. Any collection of local points (M_v) on X_0' that satisfies all Brauer–Manin conditions, lifts to a collection of local points on the fibred product of W and X_0'. This variety is birationally equivalent to the product of W and a conic, so we reach the same conclusion as in the previous case.

To establish Theorem 3.5 it is enough to prove that W satisfies the Hasse principle and weak approximation. In both cases considered above, on eliminating variables u and v we obtain a complete intersection of two quadrics $Y \subset \mathbb{P}^7_k$. It is enough to prove that Y satisfies the Hasse principle and weak approximation. The closed subset of Y given by $u = v = 0$ contains two disjoint $\mathbb{P}^3$'s conjugate over $k(\sqrt{a})$. Let us call them Π_+ and Π_-. The following technical lemma allows us to find a "convenient" pair of disjoint conjugate lines on Y.

Lemma 3.12. *At least one of the two following statements is true:*

(a) There is a projective line $L_+ \subset \Pi_+$ defined over $k(\sqrt{a})$ such that the span of L_+ and its conjugate $L_- \subset \Pi_-$ intersects Y in a skew quadrilateral (a cycle of 4 lines) contained in the smooth locus of Y; or

(b) Y contains $\mathbb{P}^1_k$, in this case Y is k-rational.

Proof. See [11, Lemma 7.2.2]. □

In case (b) the theorem is obvious, so that we assume that we are in case (a), and we fix L_+ and L_- from now on. Let $\Pi = \langle L_+, L_- \rangle$. Fibering Y by

$\mathbb{P}^4$'s passing through Π we see that Y is birationally equivalent to a projective variety Y' equipped with a surjective morphism $f : Y' \to \mathbb{P}^3_k$ whose k-fibres are 2-dimensional intersections of two quadrics in $\mathbb{P}^4_k$ containing a pair of disjoint conjugate lines. At this point we make a few observations, see [11] for proofs.

(1) *The generic fibre of f is smooth.*

(2) *There is a closed subset $V \subset \mathbb{P}^3_k$ of dimension at most 1 such that the restriction of f to $U = \mathbb{P}^3_k \setminus V$ has geometrically integral fibres.*

(3) *Smooth intersections of two quadrics in $\mathbb{P}^4_k$ containing a pair of disjoint conjugate lines satisfy the Hasse principle and weak approximation.*

Facts (1) and (2) are established by direct calculations. Fact (3) is proved as follows. Any smooth intersection of two quadrics in $\mathbb{P}^4_k$ is a del Pezzo surface of degree 4 (a $\overline{k}/k$-form of $\mathbb{P}^2$ with 5 points in general position blown-up; "the general position" here means that no 3 points are on a line, and all 5 points are not on a conic). Therefore, blowing down a pair of disjoint conjugate lines defines a birational morphism to a del Pezzo surface of degree 6 (a $\overline{k}/k$-form of $\mathbb{P}^2$ with 3 non-collinear points blown-up). Any del Pezzo surface of degree 6 is a compactification of a principal homogeneous space of a 2-dimensional torus. The Hasse principle and weak approximation are known to hold for principal homogeneous spaces of tori of dimension at most 2 because all such tori are rational, which is proved by classifying these tori and then directly checking the rationality by an explicit construction is each particular case.

It remains to show how the Hasse principle and weak approximation for the smooth locus of Y follow from (1), (2) and (3).

In the course of the proof one uses the following theorem of Lang and Weil. Let $\mathbf{F}_q$ be a finite field with q elements, and let X be a geometrically integral subvariety of $\mathbb{P}^n_{\mathbf{F}_q}$ of dimension r and degree d. Then there exists a positive constant $C(n, r, d)$ such that the number of $\mathbf{F}_q$-points on X satisfies the following inequality

$$|\#X(\mathbf{F}_q) - q^r| < C(n, r, d)q^{r-\frac{1}{2}}$$

One can apply these estimates to reductions of a geometrically integral variety defined over a number field. They imply that provided q is big enough so that the reduction is also geometrically integral, we can always find an $\mathbf{F}_q$-point in the reduction (even in the reduction of a given dense open subset) of our variety. Since the constant depends only on n, r and d the estimates can be also applied to families of closed subvarieties of $\mathbb{P}^n$ of the same degree and dimension. (Such are flat families; in a flat family of projective varieties the Hilbert polynomial is constant, hence so are the dimension and the degree, see Hartshorne, Ch. III, 9.9, 9.10).

We have to find a smooth k-point on Y' which is close to a given finite collection of smooth local points $Q_v \in Y'(k_v)$, $v \in \Sigma$. In the course of the proof we can enlarge Σ, and move Q_v in a small neighbourhood in the corresponding

local topology. For example, we can assume that Q_v do not belong to some Zariski closed subset.

Choose an auxiliary k-point $P \in U(k)$ such that the fibre $Y_P = f^{-1}(P)$ is smooth. Every geometrically integral smooth k-variety X has k_v-points for all but finitely many places of v. (For almost all primes of k the reduction of X is a well defined geometrically integral smooth variety, thus we can apply the Lang–Weil estimates to X to conclude that for almost all primes the reduction of X has a smooth point over the residue field. To such a point we apply Hensel's lemma to get a local point.) Now we enlarge Σ and our collection of local points $Q_v \in Y'_{smooth}(k_v)$, $v \in \Sigma$, by adding local points for all the places v such that $Y_P(k_v) = \emptyset$. Using weak approximation in $\mathbb{P}^3_k$ we find a k-point R which is close to $f(Q_v)$, $v \in \Sigma$, and such that the line $PR \simeq \mathbb{P}^1_k$ does not meet V, and such that that the generic fibre of the restriction of f to PR is smooth. This is possible since $dim(V) \leq 1$, whereas the space of lines in $\mathbb{P}^3_k$ passing through P is isomorphic to $\mathbb{P}^2_k$. We note that $H = f^{-1}(PR)$ has smooth local points for all places of k. It is enough now to find a k-point in H close to a given finite collection of k_v-points for $v \in \Sigma$. Note that all the fibres of $H \to \mathbb{P}^1_k$ are geometrically integral, and only finitely many fibres are singular. Comparing the Lang–Weil estimates for the fibres and their singular loci we find a finite set of primes with the property that if the reduction of a fibre of $H \to \mathbb{P}^1_k$ at any other prime is geometrically integral, then it has a smooth point over the residue field.

Enlarging Σ again we can find a model $\mathcal{H} \to \mathbb{P}^1_{O_{k,\Sigma}}$ of $H \to \mathbb{P}^1_k$ with all the closed geometric fibres being geometrically integral. (Indeed, the subscheme of $\mathbb{P}^1_{O_{k,\Sigma}}$ corresponding to geometrically reducible or non-reduced fibres does not intersect $\mathbb{P}^1_k$ – the generic fibre of the structure morphism to $Spec(O_{k,\Sigma})$, – hence is contained in a finite number of fibres of $\mathbb{P}^1_{O_{k,\Sigma}} \to Spec(O_{k,\Sigma})$. We only have to include the corresponding primes into Σ.)

Using weak approximation on the base $PR \simeq \mathbb{P}^1_k$ we find a k-point M on this line such that Y_M is smooth and has k_v-points close to the given k_v-points for $v \in \Sigma$. Note that we included into Σ all "small" primes, so that now the reduction of Y_M at any place not in Σ is geometrically integral and has a smooth point over the residue field. Using Hensel's lemma we can lift it to a smooth k_v-point of Y_M, $v \notin \Sigma$. Summing up, we have a k-fibre with points everywhere locally. By (3) it has a k-point which is close to our initial collection of local points on Y'. This finishes the proof of Theorem 3.5. □

References

[1] T.D. Browning, L. Matthiesen and A.N. Skorobogatov. Rational points on pencils of conics and quadrics with many degenerate fibres. (`arXiv:1209.0207`)

[2] J.-L. Colliot-Thélène, J.-J. Sansuc and Sir Peter Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces. I, II. *J. reine angew. Math.* **373** (1987) 37–168.

[3] Ph. Gille and T. Szamuely. *Central simple algebras and Galois cohomology.* Cambridge University Press, 2006.

[4] B. Green and T. Tao. Linear equations in primes. *Ann. Math.* **171** (2010) 1753–1850.

[5] B. Green and T. Tao. The Möbius function is strongly orthogonal to nilsequences. *Ann. Math.* **175** (2012) 541–566.
[6] B. Green, T. Tao and T. Ziegler. An inverse theorem for the Gowers $U^{s+1}[N]$-norm. *Ann. Math.* **176** (2012) 1231–1372.
[7] A. Grothendieck. *Le groupe de Brauer. Dix exposés sur la cohomologie des schémas.* North-Holland, 1968, 46–188.
[8] J.-P. Serre. *A course in arithmetic.* Graduate Texts in Mathematics **7**, Springer-Verlag, 1973.
[9] J.-P. Serre. *Local fields.* Graduate Texts in Mathematics **67**, Springer-Verlag, 1979.
[10] I.R. Shafarevich. *Basic algebraic geometry.* Die Grundlehren der mathematischen Wissenschaften **213**, Springer-Verlag, 1974.
[11] A. Skorobogatov. *Torsors and rational points.* Cambridge University Press, 2001.
[12] Y. Harpaz, A.N. Skorobogatov and O. Wittenberg. The Hardy–Littlewood conjecture and rational points. (`arXiv:1304.3333`)