Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points

J.-L. Colliot-Thélène, A. N. Skorobogatov and Sir Peter Swinnerton-Dyer

Introduction

Let k be a number field, X a smooth, proper, connected surface over k equipped with a map $\pi : X \to \mathbf{P}^1_k$ whose generic fibre over the function field $K = k(\mathbf{P}^1)$ is a curve of genus one X_K, and whose special fibres are all reduced. Let E_K be the Jacobian of X_K. Assume that the class of X_K in the Weil-Châtelet group $H^1(K, E_K)$ is of order two but is not divisible by 2. Suppose that all 2-division points of E_K are defined over K, and that the only possible bad reduction of E_K at closed points of $\mathbf{P}^1_k$ is multiplicative with two components. Let

$$\mathrm{Br}_{\mathrm{vert}}(X) = \mathrm{Br}(X) \cap \pi^*(\mathrm{Br}(k(\mathbf{P}^1)) \subset \mathrm{Br}(X) \subset \mathrm{Br}(k(X))$$

be the *vertical* subgroup of the Brauer group. Under a condition slightly stronger than the hypothesis that the 2-primary torsion of $\mathrm{Br}(X)$ lies entirely in $\mathrm{Br}_{\mathrm{vert}}(X)$, and at the expense of assuming two difficult conjectures, we prove that the Brauer-Manin obstruction attached to $\mathrm{Br}_{\mathrm{vert}}(X)$ is the only obstruction to the Hasse principle for the existence of rational points on X. As a matter of fact, when there is no such obstruction, we prove that k-rational points are Zariski-dense on X.

The two conjectures are : finiteness of the Tate-Shafarevich groups of elliptic curves, and Schinzel's hypothesis (H), which is a well-known and wild generalization of the conjecture on twin primes and of Bouniakowsky's conjecture.

In a series of earlier papers (see the survey [CT97]), the Hasse principle has been studied for varieties equipped with a (linear) pencil of algebraic varieties. Under Schinzel's hypothesis, general results were obtained for the total space of a pencil of Severi-Brauer varieties (e.g. surfaces which admit a conic bundle structure over the projective line) ([CT/SwD94]), and more generally for the total space of a pencil of varieties, when these varieties satisfy the Hasse principle and there is no multiple fibre in the pencil ([CT/Sk/SwD97b]).

Building upon Schinzel's hypothesis, and also on the conjectural finiteness of the Tate-Shafarevich group of elliptic curves, Swinnerton-Dyer in [SwD95] gave sufficient conditions for the existence of a rational point on some surfaces which are defined over the rationals and are equipped with a pencil of curves of genus one.

A number of the computations in [SwD95] are rather mysterious, and some of them seem to rely on a series of lucky coincidences. Because [SwD95] represents the first, albeit conjectural, approach to the study of rational points on elliptic surfaces without a section, it is important to understand the scope of the method. The present paper represents the result of our joint efforts in this direction.

Although one is still a long way from the ideal results, we have succeeded in this enterprise in various ways :

(i) Condition (D) of [SwD95] is generalized. It is interpreted in terms of an algebraico-geometric version of a Selmer group attached to the Jacobian of X_K.

(ii) This condition is also interpreted in terms of the Brauer group of X.

(iii) On the number-theoretic side, we compute the 2-Selmer group as the kernel of a certain *symmetric* bilinear form. This replaces the case-by-case discussion in section 3 of [SwD95].

As a consequence, our main result holds over an arbitrary number field, and it holds for a much bigger class of elliptic surfaces.

In order to state our main theorem precisely, we need some preparation.

Let k be a field, $\mathrm{char}(k) \neq 2$. We start with a family of elliptic curves $E/\mathbf{P}^1_k$, over the projective line $\mathbf{P}^1_k$, given by the equation

$$Y^2 = (X - c_1(t))(X - c_2(t))(X - c_3(t))$$

in affine space $\mathbf{A}^2_k \times \mathbf{A}^1_k$ (with coordinates $(X, Y; t)$), where the $c_i(t) \in k[t]$ are polynomials. For $\{i, j, k\}$ a cyclic permutation of $\{1, 2, 3\}$, we write $p_i(t) = c_j(t) - c_k(t)$ and

$$R(t) = p_1(t)p_2(t)p_3(t) = (c_2(t) - c_3(t))(c_3(t) - c_1(t))(c_1(t) - c_2(t)).$$

We assume that $R(t)$ is square free and not constant. We shall assume that the $p_i(t)$ have the same even degree. These conditions ensure that the above elliptic curve E_K has good reduction at the point at infinity of the projective line and that the bad fibres have multiplicative reduction of type I_2 (i.e. with two components). Conversely, using Tate's algorithm [Ta72], one may check that any elliptic curve over K whose 2-torsion is rational over $K = k(\mathbf{P}^1)$ and which has bad reduction only of type I_2 may be given by an equation as above with the same conditions on $R(t)$ and on the degrees of the polynomials p_i.

We let $T \subset \mathbf{A}^1_k$ be the set of closed points defined by $R(t) = 0$. This is the set of bad reduction points for $E/\mathbf{P}^1_k$. We let $U \subset \mathbf{A}^1_k$ be the open set defined by $R(t) \neq 0$ and $k[U]^* = H^0(U, O_U^*)$ be the group of rational functions invertible on U. Thus E_U/U is an abelian scheme over U. The group of sections $E(U)$ of E_U over U coincides with the group $E(k(\mathbf{P}^1_k)) = E(k(t))$ of $k(t)$-rational points of the generic fibre.

Given an integer $n > 0$ and an abelian group A, we let ${}_nA = \{x \in A,\ nx = 0\}$. The exact sequence of U-group schemes

$$0 \to {}_2E_U \to E_U \xrightarrow{x \mapsto 2x} E_U \to 0$$

gives rise to the Kummer map $\partial : E(U) \to H^1(U, {}_2E_U)$ in étale cohomology, which defines an embedding $E(U)/2 \hookrightarrow H^1(U, {}_2E_U)$ (sometimes also denoted ∂).

The generic fibre of $E/\mathbf{P}^1_k$ is an elliptic curve over the field $k(\mathbf{P}^1)$ all 2-torsion points of which are defined over $k(\mathbf{P}^1)$. Thus the finite U-group scheme ${}_2E_U$ is isomorphic to the constant group scheme $(\mathbf{Z}/2)^2$ over U. The group $H^1(U, {}_2E_U)$ may therefore be identified with the group of triples $m = (m_1, m_2, m_3) \in (k[U]^*/k[U]^{*2})^3$ such that the product $m_1m_2m_3 = 1 \in k[U]^*/k[U]^{*2}$. Given an element $m \in H^1(U, {}_2E_U)$, we may represent it by a triple of square-free polynomials $(m_1(t), m_2(t), m_3(t))$ whose product is a square and divides $R(t)^2$. In the product $\mathbf{P}^3_k \times \mathbf{A}^1_k$, with coordinates $(X_0, X_1, X_2, X_3; t)$, the system of equations

$$m_i(t)X_i^2 - m_j(t)X_j^2 = (c_j(t) - c_i(t))X_0^2 \qquad i, j \in \{1, 2, 3\}$$

then defines a surface equipped with a pencil of curves of genus one, pencil whose fibres are smooth over the open set U of $\mathbf{P}^1_k$ (informally speaking, the above system is a one-parameter family of 2-descents). One knows that any such fibration may be extended to an essentially unique relatively minimal model $\pi : X \to \mathbf{P}^1_k$ with $X = X(m)$ smooth over k, projective and geometrically connected (for surfaces over a field of characteristic zero, this is a very classical fact, which has been extended to more general situations, see [Sha66] and [BLR90] p. 21 for further references). The singular fibres $X_M = \pi^{-1}(M)$ of π lie over T and possibly the point at infinity of $\mathbf{P}^1_k$.

We shall need to impose some conditions on the fibration $X(m)/\mathbf{P}^1_k$, i.e. on m. Let $\mathfrak{S} \subset H^1(U, {}_2E_U)$ be the subgroup consisting of triples $m = (m_1, m_2, m_3) \in (k[U]^*/k[U]^{*2})^3$, with product equal to 1, such that for each i and each irreducible $p(t)$ dividing p_i, the p-valuation of m_i is even. Once m is represented by a triple $m = (m_1, m_2, m_3)$ of square-free polynomials with product a square dividing $R(t)^2$, the condition that the class of m lies in $\mathfrak{S}$ reads : for each i the polynomials m_i and p_i are coprime. We also introduce the subgroup $\mathfrak{S}_0 \subset \mathfrak{S}$ consisting of classes $m = (m_1, m_2, m_3) \in \mathfrak{S}$ such that moreover the valuation at infinity of each $m_i(t)$ is even. Once $m = (m_1, m_2, m_3) \in (k[U]^*/k[U]^{*2})^3$ is represented by a triple $m = (m_1, m_2, m_3)$ of square-free polynomials with product a square dividing $R(t)^2$, it lies in $\mathfrak{S}_0$ if and only if for each i, the polynomials m_i and p_i are coprime, and moreover the degree of any m_i is even. An easy valuation computation shows that $\partial(E(U)) \subset H^1(U, {}_2E_U)$ lies in $\mathfrak{S}_0$.

The condition that $m \in H^1(U, {}_2E_U)$ belongs to $\mathfrak{S}$ implies (and is essentially equivalent to) the following geometric properties of the relatively minimal model $X/\mathbf{P}^1_k$. The set of points $M \in \mathbf{A}^1_k$ whose fibre X_M is singular coincides with the set $T \subset \mathbf{A}^1_k$ of points of bad reduction for the restriction of $E/\mathbf{P}^1_k$ over $\mathbf{A}^1_k$. For any such $M \in T$, with residue field k_M, the fibre X_M is reduced (as a divisor on X) and there exists a constant or quadratic extension K_M of k_M such that $X_M \times_{k_M} K_M$ is the union of two smooth conics defined over K_M and meeting transversally ; over a separable closure of K_M, the intersection of these two conics consists of two points. If moreover m lies in $\mathfrak{S}_0$, then the fibre of $X(m)/\mathbf{P}^1_k$ over the point at infinity of $\mathbf{P}^1_k$ is smooth.

Given $m \in \mathfrak{S}$ and $M \in T$ as above, let $\delta_M(m) \in k_M^*/k_M^{*2}$ be the class of the quadratic extension K_M/k_M. We have thus defined a map

$$\delta : \mathfrak{S} \to \bigoplus_{M \in T} k_M^*/k_M^{*2}$$

where T denotes the set of points of bad reduction for $E/\mathbf{P}^1_k$. One checks that the map δ is a homomorphism and that its kernel is finite and contains $\partial(E(U))$ (lemma 2.2.1 below).

Before stating the main Theorem, let us say a few words on the Brauer group and the Brauer-Manin obstruction. For a more detailed discussion of the Brauer-Manin obstruction, see [CT/SwD94, section 3] and [CT97]. The Brauer group $\mathrm{Br}(X)$ is the étale cohomology group $H^2_{\text{ét}}(X, \mathbf{G}_m)$. Given $\pi : X \to \mathbf{P}^1_k$ as above, the vertical subgroup $\mathrm{Br}_{\mathrm{vert}}(X)$ of the Brauer group of X with respect to π has been defined in the beginning. In the situation above ($m \in \mathfrak{S}_0$), all geometric fibres of π are reduced. This implies that the quotient $\mathrm{Br}_{\mathrm{vert}}(X)/\mathrm{Br}(k)$ is finite (see [Sk96, Cor. 4.5]).

Let now k be a number field. Let Ω be the set of places of k. For $v \in \Omega$, let k_v be the completion of k at v. For any proper k-variety X, let $X(\mathbb{A}_k) = \prod_{v \in \Omega} X(k_v)$ be the space of adèles of X, equipped with its natural topology, which is none but the product topology. For any element $A \in \mathrm{Br}(X)$, the map which sends the adèle $\{P_v\}$ to $\sum_{v \in \Omega} \mathrm{inv}_v(A(P_v)) \in \mathbf{Q}/\mathbf{Z}$ is a continuous function $\theta_A : X(\mathbb{A}_k) \to \mathbf{Q}/\mathbf{Z}$ with finite image. Given $B \subset \mathrm{Br}(X)$, we let $X(\mathbb{A}_k)^B \subset X(\mathbb{A}_k)$ denote the closed subset which is the intersection of the kernels $\theta_A^{-1}(0)$ for $A \in B$. The diagonal inclusion $X(k) \subset X(\mathbb{A}_k)^B$ of the set of k-rational points of X in the set of adèles of X shows that $X(\mathbb{A}_k)^B \neq \emptyset$ is a necessary condition for the existence of a k-rational point on X. For $\pi : X \to \mathbf{P}^1_k$ as above, the finiteness of $\mathrm{Br}_{\mathrm{vert}}(X)/\mathrm{Br}(k)$ implies that $X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)}$ is open in $X(\mathbb{A}_k)$.

We are now in a position to state our main result.

Theorem *Let k be a number field. Let $E/\mathbf{P}^1_k$ be an elliptic surface as above. Let $m \in H^1(U, {}_2E)$ and let $X = X(m)$ be the associated surface, equipped with the relatively minimal k-morphism $\pi : X \to \mathbf{P}^1_k$. Assume :*

(1) The class m belongs to $\mathfrak{S}_0$.

(2) The class m does not belong to $\partial({}_2E(U))$, the image of the 2-torsion subgroup ${}_2E(U)$ of $E(U)$ under the Kummer map.

(3) The kernel of the composite map

$$\mathfrak{S}_0 \xrightarrow{\delta} \bigoplus_{M \in T} k_M^*/k_M^{*2} \to \bigoplus_{M \in T} k_M^*/ < k_M^{*2}, \delta_M(m) >$$

is generated by m and by $\partial({}_2E(U))$. (This will later be referred to as condition (D)*.)*

(4) The Tate-Shafarevich group of each elliptic curve occurring as a fibre of $E/\mathbf{P}^1_k$ is finite.

(5) Schinzel's hypothesis (H) *holds.*

Let $\mathcal{R} \subset \mathbf{P}^1(k)$ be the set of k-points $x \in \mathbf{P}^1(k)$ such that the fibre $X_x = \pi^{-1}(x)$ is smooth and has infinitely many k-points. Let $\mathcal{R}_E \subset \mathbf{P}^1(k)$ be the set of k-points $x \in \mathbf{P}^1(k)$ such that the fibre E_x of $E/\mathbf{P}^1_k$ is an elliptic curve over k of rank ($= \dim_{\mathbf{Q}}(E(k) \otimes \mathbf{Q})$) at least equal to one. We have $\mathcal{R} \subset \mathcal{R}_E$. Then :

(a) The closure of $\mathcal{R}$ in $\mathbf{P}^1(\mathbb{A}_k)$ coincides with $\pi(X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)})$.

(b) Assume $X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)} \neq \emptyset$, i.e. assume that there is no vertical Brauer-Manin obstruction to the existence of a rational point (this is certainly the case if $X(k) \neq \emptyset$). Then for any non-empty finite set $S \subset \Omega$, the closure of $\mathcal{R}$ in $\prod_{v \in S} \mathbf{P}^1(k_v)$ contains a non-empty open set. The same therefore holds for $\mathcal{R}_E$. In particular $\mathcal{R}$ and $\mathcal{R}_E$ are Zariski-dense in $\mathbf{P}^1_k$, the set $X(k)$ is Zariski-dense in X and the set $E(k)$ is Zariski-dense in the surface E.

(c) Assume $X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)} \neq \emptyset$. Then there exists a finite set $S_0 \subset \Omega$ such that for any finite set $S \subset \Omega$ with $S \cap S_0 = \emptyset$, the closure of $\mathcal{R}$ under the diagonal embedding $\mathbf{P}^1(k) \to \prod_{v \in S} \mathbf{P}^1(k_v)$ coincides with $\prod_{v \in S} \pi(X(k_v))$.

Let us comment on the various hypotheses in the Theorem.

As mentioned above, hypothesis (1) ensures in particular that all fibres of $\pi : X \to \mathbf{P}^1_k$ are reduced. Some condition of that kind is required, if we hope to conclude that infinitely many k-fibres of π have rational points (see Cor. 2.2, Cor. 2.4, Prop. 4.1, Prop. 4.2 of [CT/Sk/SwD97a]). Hypothesis (4) (finiteness of Tate-Shafarevich groups) is precisely condition (A) of [SwD95], and Hypothesis (5) (Schinzel's hypothesis) is essentially condition (B) of [SwD95]. If (2) is not satisfied, then the surface $X/\mathbf{P}^1_k$ is k-birational to $E/\mathbf{P}^1_k$ over $\mathbf{P}^1_k$ and under the assumption (3), the rank of $E(k(t))$ is zero. In this case $X(k)$ is not empty, but we do not know whether $X(k)$ is Zariski-dense in X. Hypothesis (3) (condition (D)) is a generalization of condition (D) in [SwD95] (p. 290), which is of a kind which had not appeared in previous papers on the Hasse principle. The algebraic significance of this condition in [SwD95] was unclear. In section 4, we show that (D) is closely connected with the hypothesis that the 2-primary part of the Brauer group of X lies in the vertical subgroup $\mathrm{Br}_{\mathrm{vert}}(X)$. This fits in well with the obvious remark that the necessary condition $X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)} \neq \emptyset$ for the existence of a rational point is a priori weaker than the condition $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$. For the pencils of algebraic varieties under consideration in [CT/SwD94], the whole Brauer group is vertical, but it is not the case any more here.

The last two assumptions in the Theorem are of a very different kind to the first three; and one way of looking at the Theorem is to regard it as providing strong support for the following conjecture :

Conjecture *Let k be a number field and let E, m, X be as in the Theorem. Assume that hypotheses (1), (2) and (3) of the Theorem hold. Then so do the conclusions of the Theorem. In particular, if there exists a k-rational point on X, then rational points are Zariski dense on X.*

The most surprising feature of this conjecture is that the assumptions are all effectively computable, and that condition (3) (= condition (D)), as well as the additional condition

$\mathrm{Br}_{\mathrm{vert}}(X)/\mathrm{Br}(k) = 0$, tend to be satisfied by general members of the families of surfaces to which this conjecture applies, thereby predicting a Hasse principle in many cases. In particular, there are large families of $K3$ surfaces to which this conjecture applies – for example the 13-parameter family of surfaces given by an equation of the form

$$q_0(x_0, ..., x_3)q_1(x_0, ..., x_3) = q_2(x_0, ..., x_3)q_3(x_0, ..., x_3),$$

where the q_i are homogeneous diagonal quadratic forms in $x_0, ..., x_3$. Such examples lead us to ask whether there are more general families of $K3$ surfaces for which there is an effectively computable sufficient condition for the Hasse principle to hold. Until we embarked on the current research, we would not have supposed that this was a sensible question to ask.

We hope that, for the pencils of curves of genus 1 with which we are concerned in this paper (and perhaps for more general ones also), further progress will enable us to forget about hypothesis (3) (i.e. condition (D)) and establish that the closure of $\mathcal{R}$ in $\mathbf{P}^1(\mathbb{A}_k)$ coincides with $\pi(X(\mathbb{A}_k)^{\mathrm{Br}(X)})$. Still granting (4) and (5), this would in particular imply that $X(k) \neq \emptyset$ as soon as $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$, i.e. the (total) Brauer-Manin obstruction to the Hasse principle would be the only obstruction to the existence of a rational point. But this would not be an unmixed gain, for it would replace a condition which is too strong but which is effectively computable by one which, although natural as well as necessary and sufficient, is at most semi-computable.

Here is the idea of the proof, which is given in section 2 after some preliminary work in the first section. Start with an adèle $\{P_v\} \in X(\mathbb{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)}$. Let S_1 be a finite set of places of k. Using Schinzel's Hypothesis (H), find $x \in U(k) \subset \mathbf{A}^1(k)$, close to each $\pi(P_v)$ for $v \in S_1$ and such that

(a) the curve $X_x = \pi^{-1}(x)$ (the fibre at x) has points in all the completions of k;

(b) the 2-Selmer group of the elliptic curve E_x has order exactly 8 (generators being $m(x)$ and $\partial({}_2E_x)$), so that the 2-torsion subgroup of the Tate-Shafarevich group of E_x has order at most 2.

Assume that the Tate-Shafarevich group $Ш(E_x)$ of E_x is finite. The Cassels-Tate pairing, which is alternating (Cassels, see [Milne86], Remark 6.12, p. 100), is then non-degenerate (Cassels [Cass62]; [Milne86] thm. 6.13, p. 101), hence the order of the 2-primary subgroup of $Ш(E_x)$ is a square. Thus the 2-torsion of the Tate-Shafarevich group of E_x is trivial, whence $X_x(k) \neq \emptyset$.

The proof of (a) follows a general pattern (see [CT/SwD94] and [CT/Sk/SwD97b]). It 'only' uses assumption (5) (Schinzel's hypothesis) and the fact that m lies in $\mathfrak{S}_0$ (assumption (1)), which guarantees that the reducible fibres of $X/\mathbf{P}^1_k$ are not too bad. However, to get (a) together with (b), one also needs to use assumptions (2) and (3) in the theorem.

Section 1 contains results on the computation of the 2-Selmer group of an elliptic curve over a number field k, when its 2-torsion is entirely defined over k. These results are crucial for the proof in section 2, but they seem to be of independent interest. They provide a general explanation for the computations made in section 3 of [SwD95], including the symmetry statement in Lemma 3 of that paper. This Lemma is now replaced by our proposition 1.2.3, which enables one to compute the 2-Selmer group as the kernel of a certain *symmetric* bilinear form. Some class field theory is used to cover the case of arbitrary number fields (in [SwD95], attention was restricted to the rational field $\mathbf{Q}$).

Section 2 contains the proof of the Theorem. The next sections are independent. Section 3 discusses the geometrical types of surfaces to which the Theorem applies. It also gives a readily computable version of condition (D). In Section 4, which uses more sophisticated tools than in the previous sections, such as the the geometry of Néron minimal models, we provide a general context for some of the previous computations. In particular the groups $\mathfrak{S}$ and $\mathfrak{S}_0$ turn out to be geometric versions of the 2-Selmer group. We define a generalized condition (D) and relate it with the Grothendieck Brauer group. The special case of interest in this paper is described in subsection 4.7.

1. Arithmetical prerequisites

1.1. A statement from global class field theory, and some linear algebra

Let k be a number field, Ω the set of its places and $L \subset \Omega$ a finite subset. Consider the vector space $\oplus_{v\in L} k_v^*/k_v^{*2}$ over the finite field $\mathbf{F}_2$. We equip this space with the bilinear form $(\ ,\ ) = \oplus_{v\in L}(\ ,\ )_v$, where $(\ ,\ )_v$ is the bilinear pairing (the local symbol)

$$H^1(k_v, \mathbf{Z}/2) \times H^1(k_v, \mathbf{Z}/2) \to H^2(k_v, \mathbf{Z}/2) \hookrightarrow \mathbf{Z}/2$$

(where the right arrow is an isomorphism provided v is not a complex place). It is a standard fact of local class field theory that the pairing $(\ ,\ )_v$, and hence the pairing $(\ ,\ )$, is non-degenerate. This pairing is skew-symmetric : for any $a, b \in k_v^*$, we have $(a, b)_v + (b, a)_v = 0$. Let O_L be the ring of L-integers of k, and let A_L be the image of O_L^*/O_L^{*2} in $\oplus_{v\in L} k_v^*/k_v^{*2}$.

Proposition 1.1.1 *Let L be a finite set of places containing all the archimedean places, and all the places over 2. Then the dimension of the $\mathbf{F}_2$-vector space O_L^*/O_L^{*2} is equal to half the dimension of the $\mathbf{F}_2$-vector space $\oplus_{v\in L} k_v^*/k_v^{*2}$. If moreover L contains a set of generators of the ideal class group of k, then the natural map $O_L^*/O_L^{*2} \to \oplus_{v\in L} k_v^*/k_v^{*2}$ is injective and its image A_L is a maximal isotropic subspace of $\oplus_{v\in L} k_v^*/k_v^{*2}$.*

Proof Let us compare $\mathbf{F}_2$-dimensions. By Dirichlet's theorem, $\dim(O_L^*/O_L^{*2}) = \#L$. On the other hand $\dim(\oplus_{v\in L} k_v^*/k_v^{*2}) = 2\#L$ (note that $\#(k_v^*/k_v^{*2}) = 4/|2|_v$ and use the product formula). This proves the first assertion. The fact that A_L is isotropic follows from the global reciprocity law. Assume $\mathrm{Pic}(O_L) = 0$. Lemma 9.2 of [ANT67], VII, together with our assumptions, implies that the map $O_L^*/O_L^{*2} \to \oplus_{v\in L} k_v^*/k_v^{*2}$ is injective (see [ANT67], Exercise 2.16). By dimension count, we conclude that A_L is maximal isotropic. $\square$

Remarks

a) One could also prove the proposition by using Poitou-Tate duality : in [Milne86], combine theorem 4.10 p. 70, proposition 2.9 p. 209, the duality statement on top of p. 70, and finally the injection of the Brauer group of a number field into the direct sum of the Brauer groups of its completions.

b) One may prove a similar statement with 2 replaced by an arbitrary prime p, provided k contains the p-th roots of unity.

Let S_0 denote a fixed family of places of k satisfying all the conditions of the proposition. Clearly, for any finite set of places L containing S_0, the statement of the proposition holds.

For any place v of k, we let $V_v = H^1(k_v, (\mathbf{Z}/2)^2) = (k_v^*/k_v^{*2})^2$. We equip this $\mathbf{F}_2$-vector space with the bilinear form :

$$e_v((a, b), (c, d)) = (a, d)_v - (c, b)_v \in \mathbf{Z}/2$$

(this is also equal to $(a, d)_v + (b, c)_v$.) This bilinear form is clearly alternating : $e_v((a, b), (a, b)) = 0$, and it is non-degenerate since e_v is non-degenerate.

For any finite set L of places containing S_0, we let $V_L = \oplus_{v\in L} V_v$. This space comes equipped with the symplectic structure $e_L = \oplus_{v\in L} e_v$ given by the orthogonal sum of the structures on the individual V_v.

Because L contains S_0, we have $\mathrm{Pic}(O_L)=0$. Hence the diagonal map

$$H^1(O_L,(\mathbf{Z}/2)^2)\to\bigoplus_{v\in L}H^1(k_v,(\mathbf{Z}/2)^2)$$

may be read

$$(O_L^*/O_L^{*2})^2\to\bigoplus_{v\in L}(k_v^*/k_v^{*2})^2$$

and it is injective by the previous proposition. By the global reciprocity law, the image U_L of this map is isotropic with respect to the symplectic pairing $e=\oplus_{v\in L}e_v$ defined above. By dimension count (using proposition 1.1.1), we then see that it is maximal isotropic.

Note that for any L, the natural map $H^1(O_L,(\mathbf{Z}/2)^2)\to H^1(k,(\mathbf{Z}/2)^2)$ is injective. For L containing S_0, we shall identify $(O_L^*/O_L^{*2})^2=H^1(O_L,(\mathbf{Z}/2)^2)$ with the corresponding subgroup of $(k^*/k^{*2})^2=H^1(k,(\mathbf{Z}/2)^2)$, and also with U_L. The elements of U_L may thus be identified with the elements of $(k^*/k^{*2})^2=H^1(k,(\mathbf{Z}/2)^2)$ whose image in $(k_v^*/k_v^{*2})^2=H^1(k_v,(\mathbf{Z}/2)^2)$ belongs to $(O_v^*/O_v^{*2})^2=H^1(O_v,(\mathbf{Z}/2)^2)$ for each $v\notin L$.

Proposition 1.1.2 *Let S_0 be as above, and let L be a finite family of places containing S_0. There exist subspaces $K_v\subset V_v$, $v\in L$, such that :*
(a) for each place $v\in L$, K_v is a maximal isotropic subspace of V_v ;
(b) $V_L=U_L\oplus K_L$, where $K_L:=\oplus_{v\in L}K_v$.
For $v\notin S_0$, one may choose $K_v=(O_v^*/O_v^{*2})^2\subset V_v$.

Proof The space $U_L\subset V_L$ is maximal isotropic. Thus except for the last sentence, the statement follows from the general lemma :

Lemma 1.1.3 *Let k be a field and V_i, $i=1,\cdots,n$, be vector spaces each equipped with a non-degenerate alternating bilinear form. Let $V=\oplus_iV_i$ be equipped with the direct sum of these alternating forms. Let $U\subset V$ be a maximal isotropic subspace. Then there exist maximal isotropic subspaces $K_i\subset V_i$ such that $U\oplus(\oplus_iK_i)=V$.*

Proof Let $2d$ be the dimension of V. We have $d=\dim(U)$. For $j=0,1,\ldots,d$ we shall construct isotropic subspaces $K^j=\oplus_iK_i^j$ with $K_i^j\subset V_i$ such that $\dim(K^j)=j$ and $U\cap K^j=0$. We shall set $U^j:=U\cap(K^j)^\perp$.

From $U\cap K^j=0$ and $U=U^\perp$ we deduce $V=U+(K^j)^\perp$, hence

$$2d=\dim(U)+\dim((K^j)^\perp)-\dim(U\cap(K^j)^\perp)=d+(2d-j)-\dim(U^j).$$

Thus $\dim(U^j)=d-j$.

For $j=0$, one simply takes $K^0=0$. Here is how to pass from $j<d$ to $j+1$. The composite map

$$U^j\to(K^j)^\perp\to(K^j)^\perp/K^j,$$

where the first arrow is the inclusion $U^j:=U\cap(K^j)^\perp\to(K^j)^\perp$, is injective, since $U\cap K^j=0$. The dimension of U^j is $d-j$, that of $(K^j)^\perp/K^j$ is $2d-2j$, as one easily checks. The space $(K^j)^\perp/K^j$ is equipped with an induced non-degenerate alternating form, and via the above embedding U^j is an isotropic hence (dimension count) maximal isotropic subspace. One may find a class in $(K^j)^\perp/K^j$ which does not vanish on U^j. We may choose it as the image of $v\in(K_i^j)^\perp\subset V_i$ for a suitable i. One then defines $K^{j+1}=K^j+k<v>$. This is isotropic in V. We clearly have $\dim(K^{j+1})=j+1$. We have $U\cap K^{j+1}\subset U\cap(K^{j+1})^\perp=U^j\cap(K^{j+1})^\perp$ hence $U\cap K^{j+1}=U^j\cap K^{j+1}$. However U^j and K^j are orthogonal and v does not vanish on U^j. Thus $U\cap K^{j+1}=0$. For $j=d$, the equation $\dim(K^d)=d$ ensures that K^d is maximal isotropic. The way in which it is built guarantees that it is a sum $K^d = \oplus_i K_i^d$ of isotropic, hence maximal isotropic, subspaces $K_i^d \subset V_i$. □

We apply the lemma to $L = S_0$ and the maximal isotropic subspace $U_{S_0} \subset V_{S_0}$, thus producing maximal isotropic subspaces $K_v \subset V_v$ for each $v \in S_0$, with the property $V_{S_0} = U_{S_0} \oplus K_{S_0}$, where $K_{S_0} := \oplus_{v \in S_0} K_v$. This proves the proposition for $L = S_0$.

For arbitrary L, take the just found K_v's for $v \in S_0$, and let $K_v = (O_v^*/O_v^{*2})^2$ for $v \in L, v \notin S_0$. Each $K_v \subset V_v$ is maximal isotropic. By dimension count, it is enough to show $U_L \cap K_L = 0$. But any element of $U_L = (O_L^*/O_L^{*2})^2$ which belongs to $U_L \cap K_L$ actually belongs to $U_{S_0} = (O_{S_0}^*/O_{S_0}^{*2})^2$ (both groups being viewed as subgroups of $(k^*/k^{*2})^2$), since $K_v = (O_v^*/O_v^{*2})^2$ for $v \notin S_0$. Thus $U_L \cap K_L \subset U_{S_0} \cap K_{S_0} = 0$. □

In the sequel, when applying proposition 1.1.2, we shall always choose $K_v = (O_v^*/O_v^{*2})^2 \subset V_v$ for $v \notin S_0$.

1.2. The 2-Selmer group of an elliptic curve (with rational 2-torsion) as the kernel of a symmetric bilinear form

Let E be an elliptic curve over a number field k, let ${}_2E$ be the k-subgroup of points of order 2. Assume all 2-division points are defined over k. Fix an isomorphism ${}_2E \simeq (\mathbf{Z}/2)^2$ of k-group schemes. The curve E may be given by an equation $Y^2 = (X - c_1)(X - c_2)(X - c_3)$, $c_i \in k$. We shall fix the isomorphism above in such a way that the point $(X, Y) = (c_1, 0)$, resp. $(X, Y) = (c_2, 0)$, corresponds to $(1, 0) \in (\mathbf{Z}/2)^2$, resp. $(0, 1) \in (\mathbf{Z}/2)^2$. There is a corresponding isomorphism $H^1(k, {}_2E) \simeq (k^*/k^{*2})^2$.

Consider the following diagram, deduced from the Kummer sequence :

$$\begin{array}{ccccccccc}
0 & \to & E(k)/2 & \to & H^1(k, {}_2E) & \to & {}_2H^1(k, E) & \to & 0 \\
 & & \downarrow & & r_v \downarrow & & \rho_v \downarrow & & \\
0 & \to & E(k_v)/2 & \xrightarrow{\partial_v} & H^1(k_v, {}_2E) & \xrightarrow{i_v} & {}_2H^1(k_v, E) & \to & 0
\end{array}$$

where the vertical arrows (e.g. r_v and ρ_v) are the restrictions to k_v. If $P \in E(k_v)$ has coordinates (X, Y) and is not a point of order 2, then the Kummer map $\partial_v : E(k_v) \to H^1(k_v, {}_2E)$ sends P to $\partial_v(P) = (X - c_1, X - c_2)$.

For any place v of k, we let $V_v = H^1(k_v, {}_2E) = H^1(k_v, (\mathbf{Z}/2)^2) = (k_v^*/k_v^{*2})^2$. The Weil pairing and cup-product define a non-degenerate alternating pairing $V_v \times V_v \to \mathbf{Z}/2$, i.e. a symplectic space structure e_v on V_v which coincides with the pairing described in subsection 1.1. For any finite set L of places containing S_0, we let $V_L = \oplus_{v \in L} V_v$. This space comes equipped with the symplectic structure $e_L = \oplus_{v \in L} e_v$ given by the orthogonal sum of the structures on the individual V_v.

For each place $v \in \Omega$, let $W_v = W_v(E) = \partial_v(E(k_v)/2) \subset V_v$. According to Tate (see [Milne86], p. 56), $W_v(E)$ is a maximal isotropic subspace of the symplectic space V_v. If $v \notin S$ is a place of good reduction for E, then $W_v = H^1(O_v, {}_2E) \subset V_v$, in other words $W_v = (O_v^*/O_v^{*2})^2 \subset (k_v^*/k_v^{*2})^2$. For any finite set L of places containing S_0, let $W_L = W_L(E) = \oplus_{v \in L} W_v(E)$. This is clearly a maximal isotropic subspace of V_L.

Recall that the 2-torsion subgroup of the Tate-Shafarevich group of E is given by :

$${}_2\text{Ш}(E) := \{x \in {}_2H^1(k, E) \mid \rho_v(x) = 0 \text{ for all places } v\}.$$

As for the 2-Selmer group $\mathcal{S}(E,2)$, it is defined by

$$\mathcal{S}(E,2) := \{x \in H^1(k, {}_2E) \mid i_v r_v(x) = 0 \text{ for all places } v\}.$$

There is the well-known exact sequence

$$0 \to E(k)/2 \to \mathcal{S}(E,2) \to {}_2\text{Ш}(E) \to 0.$$

Proposition 1.2.1 *Let S_0 be as in subsection 1.1, and let L be a finite family of places containing S_0 and the places of bad reduction for the elliptic curve E. Let V_L and $U_L \subset V_L$ be as in subsection 1.1, and $W_L = W_L(E) \subset V_L$ as above. The 2-Selmer group $\mathcal{S}(E,2)$ is isomorphic to each of the following groups :*

(1) The intersection $U_L \cap W_L \subset V_L$.

(2) The left kernel of the pairing $e_L : U_L \times W_L \to \mathbf{Z}/2$ induced by the symplectic pairing $e_L : V_L \times V_L \to \mathbf{Z}/2$.

(3) The right kernel of the pairing $e_L : U_L \times W_L \to \mathbf{Z}/2$ induced by the symplectic pairing $e_L : V_L \times V_L \to \mathbf{Z}/2$.

Proof We have to compare two subgroups of $H^1(k, {}_2E)$. Since

$$\operatorname{im}(\partial_v) = W_v(E) = H^1(O_v, {}_2E) \subset V_v$$

for $v \notin L$, the class $\alpha \in H^1(k, {}_2E)$ belongs to U_L if and only if for each $v \notin L$, the restriction $\alpha_v \in H^1(k_v, {}_2E)$ belongs to the image of ∂_v. The condition $\alpha_v \in W_v$ for $v \in S$ exactly says that α_v belongs to the image of ∂_v. This proves (1). As for (2) and (3), they follow from (1) and from the fact that U_L and W_L are maximal isotropic subspaces, hence each equal to its own orthogonal. $\square$

Given any finite set of places L containing S_0, but not necessarily containing the primes of bad reduction for E, let us define several important objects, whose definition depends on the K_v's and the W_v's.

We define $t_L : V_L \to U_L$ to be the projector along K_L.

We set $U'_L = U'_L(E) = U_L \cap (W_L(E) + K_L) \subset V_L$.

We set $W'_L = W'_L(E) = W_L(E)/(W_L(E) \cap K_L) = \bigoplus_{v \in L}(W_v(E)/W_v(E) \cap K_v)$.

Note that for $S_0 \subset L \subset L_1$, the natural inclusion $U_L \subset U_{L_1}$ induces the equality $U'_L = U'_{L_1} \cap U_L$.

Lemma 1.2.2 *Let $x, y \in V_L$. Then $e_L(x,y) = e_L(t_L(x), y) + e_L(x, t_L(y))$.*

Proof The homomorphism t_L (resp. $1 - t_L$) is a projector to the isotropic subspace U_L (resp. K_L). Hence $e_L(t_L(x), t_L(y)) = e_L(x - t_L(x), y - t_L(y)) = 0$, which implies the lemma. $\square$

Proposition 1.2.3 *Assume that L contains S_0.*

(1) The projection map $t_L : V_L \to U_L$, when restricted to $W_L \subset V_L$, induces an isomorphism

$$\tau_L : W'_L \xrightarrow{\simeq} U'_L.$$

(2) The map τ_L^{-1} associates to $u = \sum_{v \in L}(\alpha_v + \beta_v) \in U'_L$ (with $\alpha_v \in W_v$ and $\beta_v \in K_v$) the class of $\sum_{v \in L} \alpha_v \in W_L/(W_L \cap K_L) = W'_L$.

(3) The pairing $e_L : U_L \times W_L \to \mathbf{Z}/2$ induces a pairing $e'_L : U'_L \times W'_L \to \mathbf{Z}/2$.

Assume that L also contains all the places of bad reduction for the elliptic curve E.

(4) The left and right kernel of the pairing e'_L are both isomorphic to $\mathcal{S}(E,2)$.

(5) The pairing $U'_L \times U'_L \to \mathbf{Z}/2$ given by $(x,y) \to e'_L(x, \tau_L^{-1}(y))$ is symmetric and its kernel is isomorphic to $\mathcal{S}(E,2)$.

(6) The pairing $W'_L \times W'_L \to \mathbf{Z}/2$ given by $(x,y) \to e'_L(\tau_L(x), y)$ is symmetric and its kernel is isomorphic to $\mathcal{S}(E,2)$.

Proof Statements (1) and (2) follow from the definitions. We have

$$U'_L = U_L \cap (W_L + K_L) = U_L \cap (W_L^{\perp} + K_L^{\perp}) = U_L \cap (W_L \cap K_L)^{\perp}.$$

Here the first equality follows from the definitions, and the second one follows from $W_L = W_L^{\perp}$ and $K_L = K_L^{\perp}$. This implies (3).

The subgroup $\mathcal{S}(E,2) \subset U_L$ is equal to $U_L \cap W_L$, hence is contained in $U'_L = U_L \cap (W_L + K_L)$. From (3) and proposition 1.2.1 (2) we conclude that the left kernel of e'_L is isomorphic to $\mathcal{S}(E,2)$. By dimension count, this also holds for the right kernel, hence (4).

Given $x, y \in U'_L$, there exist $\alpha, \beta \in W_L$ such that $t_L(\alpha) = x$ and $t_L(\beta) = y$. We have $e_L(\alpha,\beta) = 0$. From the lemma we conclude $e_L(x,\beta) + e_L(\alpha, y) = 0$, hence $e_L(x,\beta) - e_L(y,\alpha) = 0$, hence finally $e'_L(x, \tau_L^{-1}(y)) - e'_L(y, \tau_L^{-1}(x)) = 0$. This proves the symmetry in (5). The proof of the symmetry in (6) is also a straightforward application of the lemma and of the fact that W_L is isotropic. That the kernel of either symmetric pairing is isomorphic to $\mathcal{S}(E,2)$ then follows from (4). □

Describing $U'_L(E) \subset U_L$

From the definition $U'_L(E) = U_L \cap (W_L(E) + K_L)$ we have that U'_L as a subspace of $U_L = (O_L^*/O_L^{*2})^2$ is given by local conditions, namely, for each $v \in L$ the image of the corresponding global element $\xi \in (O_L^*/O_L^{*2})^2$ in $(k_v^*/k_v^{*2})^2$ must belong to $W_v + K_v$, where

$$W_v = W_v(E) = \partial_v(E(k_v)/2) \subset H^1(k_v, {}_2E) = (k_v^*/k_v^{*2})^2.$$

For some places $v \in L$ this condition on $\xi \in (O_L^*/O_L^{*2})^2$ can be made explicit. For $v \notin S_0$, letting κ_v be the residue field at v we have a residue map :

$$\delta_v : H^1(k_v, (\mathbf{Z}/2)^2) \to H^0(\kappa_v, (\mathbf{Z}/2)^2)$$

simply given by valuation modulo 2 on each summand :

$$\delta_v : (k_v^*/k_v^{*2})^2 \to (\mathbf{Z}/2)^2.$$

If v is not in S_0 and v is a place of good reduction of E, then $K_v = (O_v^*/O_v^{*2})^2 = H^1(O_v, {}_2E) = W_v(E)$; hence the condition at such a v simply says that the image of ξ under the composite map $H^1(O_S, (\mathbf{Z}/2)^2) \to H^1(k_v, (\mathbf{Z}/2)^2) \to H^0(\kappa_v, (\mathbf{Z}/2)^2)$ is zero.

In general, as long as v does not belong to S_0, since $K_v = H^1(O_v, (\mathbf{Z}/2)^2)$ the condition that ξ belongs to $W_v + K_v$ is equivalent to the condition that $\delta_v(\xi) \in H^0(\kappa_v, (\mathbf{Z}/2)^2)$ belongs to $\delta_v(W_v) \subset H^0(\kappa_v, (\mathbf{Z}/2)^2)$.

In this paper, we shall be interested in the following concrete case of bad reduction. We consider an elliptic curve given by an affine equation $y^2 = (x - c_1)(x - c_2)(x - c_3)$. We are concerned with a (finite) place $v \notin S_0$ such that all c_i are in O_v and that $(c_1 - c_2)(c_2 - c_3)(c_3 - c_1)$ has valuation one. If $c_1 - c_2$ is the uniformizing parameter at v (hence the other two are units), then $\delta_v(W_v) = \{(0,0),(1,1)\} \subset (\mathbf{Z}/2)^2$. If $c_2 - c_3$ is the uniformizing parameter, then $\delta_v(W_v) = \{(0,0),(0,1))\} \subset (\mathbf{Z}/2)^2$. If $c_3 - c_1$ is the uniformizing parameter, then $\delta_v(W_v) = \{(0,0),(1,0))\} \subset (\mathbf{Z}/2)^2$.

In the particular case under consideration, one can also phrase this by saying that the valuations of an element of $U'_L(E)$ must belong to the subgroup of $(\mathbf{Z}/2)^2$ consisting of the image of ${}_2E(k)$ under the composite map

$${}_2E(k) \to E(k_v)/2 \to H^1(k_v, {}_2E) \to H^0(\kappa_v, (\mathbf{Z}/2)^2) = (\mathbf{Z}/2)^2.$$

2. Proof of the Theorem

2.1 Fibres with points everywhere locally

Let k be a number field. We are given a smooth projective surface E/k equipped with a fibration $p : E \to \mathbf{P}^1_k$, the generic fibre of which is given by the affine equation

$$Y^2 = (X - c_1(t))(X - c_2(t))(X - c_3(t)).$$

We assume that the product $R(t) = (c_1(t) - c_2(t))(c_2(t) - c_3(t))(c_3(t) - c_1(t))$ is squarefree and non-constant, and that the various polynomials $p_i(t) = c_j(t) - c_k(t)$ all have the same even degree.

We are given a triple $(m_1(t), m_2(t), m_3(t))$ of non-zero squarefree elements of $k[t]$, whose product is a square and divides $R(t)^2$. We shall represent each $m_i(t)$ as the product of a constant ρ_i and polynomials of the type $R_M(t)$, where $R_M(t)$ runs through the monic irreducible polynomials dividing $R(t)$.

By assumptions (1) and (2) of the Theorem, we have :

The class m of $(m_1(t), m_2(t), m_3(t))$ lies in $\mathfrak{S}_0 \subset H^1(U, {}_2E)$ and it does not belong to $\partial({}_2E(U)) \subset H^1(U, {}_2E)$.

The surface given in affine coordinates by the system of equations

$$x - c_i(t) = m_i(t)y_i^2, \quad i = 1, 2, 3$$

in affine space with coordinates x, t, y_1, y_2, y_3, together with its projection on the t-axis, may be extended to a unique smooth proper k-variety X, equipped with a relatively minimal fibration $\pi : X \to \mathbf{P}^1_k$ (see [Sha66]). The singular fibres of this fibration are over the closed points $M \in \mathbf{A}^1_k$ which correspond to the irreducible factors of $R(t)$. We let T be the set of such points. Over the quadratic (or trivial) extension $K_M = k_M(\sqrt{\delta_M(m)})$ of k_M, the fibre X_M at $M \in T$ breaks up into a union of two smooth conics. Over an algebraic closure of k_M, this fibre consists of two smooth conics intersecting transversally in two points.

We let $\mathrm{Br}_{\mathrm{vert}}(X) \subset \mathrm{Br}(X)$ be the vertical Brauer group with respect to the map π, as defined in the introduction. Since the geometric fibres are reduced, the quotient $\mathrm{Br}_{\mathrm{vert}}(X)/\mathrm{Br}(k)$ is finite ([Sk96], Cor. 4.5). We start with an adèle $\{P_v\} \in X(\mathbb{A}_k) = \prod_{v\in\Omega} X(k_v)$. We assume that for all $A \in \mathrm{Br}_{\mathrm{vert}}(X)$, we have

$$\sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) = 0 \in \mathbf{Q}/\mathbf{Z},$$

in other words we assume that $\{P_v\}$ is in the kernel of all reciprocity maps $\theta_A : X(\mathbb{A}_k) \to \mathbf{Q}/\mathbf{Z}$ associated to elements $A \in \mathrm{Br}_{\mathrm{vert}}(X)$ (see [CT97]).

Let S_1 be a finite set of places of k containing all the archimedean places; for $v \in S_1$, let $U_v \subset \mathbf{P}^1(k_v)$ be an open neighbourhood of $\pi(P_v)$. Under the five assumptions of the Theorem, we want to show that we may find a k-point $x \in \mathbf{P}^1(k)$, lying in U_v for $v \in S_1$, and such that moreover the fibre $X_x = \pi^{-1}(x)$ is smooth and has infinitely many rational points. This will prove statement (a) in the Theorem. Statements (b) and (c) will then follow easily.

A standard procedure, which uses the finiteness of $\mathrm{Br}_{\mathrm{vert}}(X)/\mathrm{Br}(k)$, and is described in full detail in [CT/Sk/SwD97b] (proof of Theorem 1.1) allows us to choose the rational point at infinity and the parameter t on $\mathbf{A}^1_k = \mathrm{Spec}(k[t]) = \mathbf{P}^1_k \setminus \infty$ so that :

(a) For each place $v \in \Omega$, the point P_v lies on a smooth fibre of π and does not lie on the fibre at infinity (i.e. $\pi(P_v)$ lies in $U(k_v)$, for $U \subset \mathbf{A}^1_k$ as in the introduction).

(b) For each place $v \in S_1$, the projection $X(k_v) \to \mathbf{P}^1(k_v)$ admits an analytic section $\sigma_v : U_v \to X(k_v)$ over U_v.

(c) For each real place v, the neighbourhood U_v coincides with the open set $t_v > 0$, and for v complex, U_v contains the point at infinity.

The mentioned procedure involves a projective transformation of the projective line $\mathbf{P}^1_k$ sending a k-point $m \in \mathbf{P}^1(k)$ to the point at infinity. Because the polynomials $p_i(t) = c_j(t) - c_k(t)$ all have the same even degree, after suitable and obvious birational transformations we find that the restriction to $\mathbf{A}^1_k$ of $E/\mathbf{P}^1_k$ in the new system of coordinates still reads as it did, namely

$$Y^2 = (X - c_1(t))(X - c_2(t))(X - c_3(t)),$$

with the same degree and coprimality conditions on the $p_i = c_j - c_k$. One easily checks that the new $\mathfrak{S}$ and the new $\mathfrak{S}_0$ are the obvious transforms of the old ones, that the new m lies in the new $\mathfrak{S}_0$ and that condition (2) in the main Theorem (Introduction) is preserved (the other ones are obviously preserved). From now on, we assume that conditions (a),(b),(c) above are fulfilled.

Given (the new) m and its associated model $X = X(m)/\mathbf{P}^1_k$, we shall define a finite set S_0 of 'bad' places of k. As in proposition 1.1.1, we want it to contain all the archimedean places and all the places above 2, and we want the class group of O_{S_0} to be trivial. We also want it to contain the set S_1 given above. Given $v \notin S_0$, we want all polynomials $c_i(t)$ and $m_i(t)$ to be O_v-integral, we want the constants ρ_i to be O_v-units, and we want $R(t)$ to define a closed subscheme of $\mathrm{Spec}(O_{S_0}[t])$ which is finite and étale over O_{S_0}, the ring of S_0-integers of k. Given any monic irreducible factor $R_M(t)$ of $R(t)$, we have the closed subscheme $\tilde{M} = \mathrm{Spec}(O_{S_0}[t]/R_M(t))$ of $\mathbf{A}^1_{O_{S_0}}$, which is finite and étale over $\mathrm{Spec}(O_{S_0})$. For each $M \in T$, we want the (trivial or) quadratic extension K_M/k_M (see above) to be unramified over the ring of S_0-integers of k_M. For much later use, we want S_0 to contain all the places above a prime of $\mathbf{Q}$ less than or equal to the product of the degree $[k : \mathbf{Q}]$ and the degree of the polynomial $R(t)$. We also want S_0 to be big enough so that the fibration $\pi : X \to \mathbf{P}^1_k$ extends to a fibration $\mathcal{X}/\mathbf{P}^1_{O_{S_0}}$ with the following property. The scheme $\mathrm{Spec}(O_{S_0}[t]/R(t)) = \cup_{M \in T} \tilde{M}$ is the set of points of $\mathbf{P}^1_{O_{S_0}}$ whose fibre is singular. Over any geometric point of this subscheme, the fibre consists of two smooth conics intersecting transversally in two points. (That this can be achieved may be seen directly on projective equations, as in the introduction.)

Given a finite set of primes S containing S_0, we shall be interested in the affine line $\mathbf{A}^1_{O_S}$ over O_S and in its open set $\mathcal{U}_S = \mathrm{Spec}(O_S[t][1/R])$. The group of units of $O_S[t][1/R]$ is the direct product of O_S^* and the free group generated by the polynomials P_M for $M \in T$, as one easily checks. Also, one easily checks that the Picard group of $O_S[t][1/R]$ vanishes (this uses the vanishing of the Picard group of O_S).

A point $x \in \mathbf{P}^1(k) = \mathbf{P}^1(O_{S_0})$ (resp. $x \in \mathbf{P}^1(k_v) = \mathbf{P}^1(O_v)$ for $v \notin S_0$) defines a section $\tilde{x} : \mathrm{Spec}(O_{S_0}) \to \mathbf{P}^1_{O_{S_0}}$ (resp. a local section $\tilde{x} : \mathrm{Spec}(O_v) \to \mathbf{P}^1_{O_v}$). We shall call such a point *transversal* if the corresponding section (resp. local section) $\tilde{x}$ defined over $\mathrm{Spec}(O_{S_0})$ (resp. $\mathrm{Spec}(O_v)$) transversally intersects with the finite étale O_{S_0}-scheme (resp O_v-scheme) which is the union of all the (restrictions over O_{S_0} of the) $\tilde{M}$'s ($M \in T$) and the section at infinity of $\mathbf{P}^1_{O_{S_0}}$ (resp. which is the pull-back to O_v of this étale scheme). In less geometric terms, this simply means that for each $M \in T$, the element $R_M(x) \in k^*$ (resp. $R_M(x) \in k_v^*$) is either a unit or a uniformizing parameter at each $v \notin S_0$ (resp. at v), and that if $v(x) < 0$, then $v(x) = -1$.

Lemma 2.1.1 *Let S_0 be as above. Let $v \notin S_0$ and $x \in \mathbf{A}^1(k_v)$ be a transversal point.*
(a) If $\tilde{x}$ does not intersect any of the $\tilde{M}$'s, then $X_x(k_v) \neq \emptyset$;
(b) if $\tilde{x}$ intersects $\tilde{M}$ at some place w of k_M (w unramified over v, of degree one over v), then $X_x(k_v) \neq \emptyset$ if and only if w splits in K_M.

Proof Let $\mathcal{X}_x/O_v$ be the O_v-scheme which is the inverse image of $\mathcal{X}/\mathbf{P}^1_O$ under $\tilde{x}$.

(a) The reduction mod v of the fibre $\mathcal{X}_x/O_S$ is a smooth curve of genus one over a finite field, hence has a rational point by F. K. Schmidt's theorem (or Lang's theorem). Such a point can be lifted to a point over O_v, hence over k_v, by Hensel's lemma.

(b) Since $\mathcal{X}_x/O_S$ is proper we have $X_x(k_v) = \mathcal{X}_x(O_v)$. Thus a point of $X_x(k_v)$ gives a local section over $\mathrm{Spec}(O_v)$ which intersects just one component of the closed fibre; the closed fibre is therefore split. Thus the unramified extension K_M/k_M splits over w. Conversely, if this is so, the two conics which constitute the closed fibre of $\mathcal{X}_x/O_S$ at v are individually defined over $\mathbf{F}_w = \mathbf{F}_v$. Any conic contains at least 3 points, thus we can always find a smooth rational point in such a fibre. Again, this point can be lifted to a point over k_v by Hensel's lemma. □

Given $M \in T$, we may write $R_M(t) = N_{k_M/k}(t - a_M)$ with $a_M \in k_M$. Let us define

$$\alpha_M(t) = \mathrm{Cores}_{k_M/k}((K_M/k_M, t - a_M)) \in \mathrm{Br}(k(\mathbf{P}^1_k)).$$

One may check that the inverse image of such a classe on X is unramified on the complement in X of the fibre at infinity of $X/\mathbf{P}^1_k$, but this will be used only in remark 2.5.4 (v).

Lemma 2.1.2 *Let $\pi : X \to \mathbf{P}^1_k$ and S_0 be as above, and let $\{P_v\} \in \prod_{v\in\Omega} X(k_v)$ be an adelic point of X such that $\sum_{v\in\Omega} \mathrm{inv}_v(\mathcal{A}(P_v)) = 0$ for all $\mathcal{A} \in \mathrm{Br}_{\mathrm{vert}}(X)$. There exists a finite set of places S of k, containing S_0, and there exist points $Q_v \in X_U(k_v)$ for $v \in S$, with $Q_v = P_v$ for $v \in S_0$ (hence for $v \in S_1$), such that*

$$\sum_{v\in S} \mathrm{inv}_v(\alpha_M(\pi(Q_v))) = 0$$

for all $M \in T$.

Proof This is just a special case of Harari's 'formal lemma' ([Ha94], Cor. 2.6.1; [CT/SwD94], Theorem 3.2.1). □

From now on and until the end of section 2, the set S of places will be fixed and taken as in lemma 2.1.2 above. So will be $x_v = \pi(Q_v)$ (with smooth fibres E_{x_v} and X_{x_v}) for $v \in S$.

Proposition 2.1.3 *Let $\pi : X \to \mathbf{P}^1_k$, the set of places S and the $Q_v \in X(k_v)$, $v \in S$ be as in the conclusion of the previous lemma. For each point $M \in T \cup \infty$, let L_M be a finite set of places of k such that $L_M \cap S = \emptyset$, $L_M \cap L_N = \emptyset$ for $M \neq N$. Let $x \in U(k) \subset \mathbf{P}^1(k) = \mathbf{P}^1(O_S)$.*

Assume :

(1) For each place $v \in L_M$, there is an associated place w of k_M (of degree one over k) which splits in the quadratic extension $K_M = k_M(\sqrt{\delta_M(m)})/k_M$ (i.e. $\delta_M(m)$ is a square in k_{Mw});

(2) each place $v \in L_\infty$ splits in each quadratic extension $k(\sqrt{N_{k_M/k}(\delta_M(m))})/k$ (i.e. $N_{k_M/k}(\delta_M(m))$ is a square in k_v for each $v \in L_\infty$);

(3) x is transversal over O_S;

(4) for any $M \in T$, the (transversal) intersection of x and $\tilde{M}$, when viewed on $\tilde{M}$, consists of the places $w \in L_M$ and just one place w_M of k_M, of degree one over a place v_M of k;

(5) the transversal intersection of x and the section at infinity of $\mathbf{P}^1_{O_S}$ consists exactly of the places $v \in L_\infty$ (hence for any such v, we have $v(x) = -1$);

(6) x is very close to $x_v = \pi(Q_v) \in U(k_v)$ for $v \in S$ and lies in U_v for $v \in S_1$.

Let $L = S \cup (\cup_{M\in T} L_M)$ and $L(x) = L \cup (\cup_{M\in T}\{v_M\})$.

Then one has :

(i) $X_x(k_v) \neq \emptyset$ for all places v of k;

(ii) the 'evaluation map' $\mathrm{ev}_x : (O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2})^2 \to (O^*_{L(x)\cup L_\infty}/O^{*2}_{L(x)\cup L_\infty})^2$ is an isomorphism;

(iii) the images of the points of order 2 on E_x under the Kummer map ∂ and the class of $m(x)$ in $(k^*/k^{*2})^2$ lie in the subgroup $U_{L(x)} = (O^*_{L(x)}/O^{*2}_{L(x)})^2$ and are independent.

Proof (i) We proceed as in [CT/SwD94] and [CT/Sk/SwD97b]. We have

$$\sum_{v\in S} \mathrm{inv}_v(\alpha_M(\pi(Q_v))) = 0$$

for all $M \in T$. For $x \in k$ close enough to each x_v for $v \in S$ (condition (6)), we therefore have

$$\sum_{v\in S} \mathrm{inv}_v(\alpha_M(x)) = 0;$$

hence

$$\sum_{v\notin S} \mathrm{inv}_v(\alpha_M(x)) = 0$$

by the global reciprocity law. Now $\mathrm{inv}_v(\alpha_M(x)) = \mathrm{inv}_v(\mathrm{Cores}_{k_M/k}((K_M/k_M, x-a_M)))$ vanishes if $R_M(x) = N_{k_M/k}(x-a_M)$ is a unit at $v \notin S$. Thus for $v \notin S$ we have $\mathrm{inv}_v(\alpha_M(x)) = 0$ except perhaps if $v \in L_\infty \cup L_M \cup \{v_M\}$. For $v \in L_M$, condition (1) guarantees that v splits in the unramified extension K_M/k_M, hence

$$\mathrm{inv}_v(\alpha_M(x)) = \mathrm{inv}_v(\mathrm{Cores}_{k_M/k}((K_M/k_M, x-a_M))) = 0.$$

For $v \in L_\infty$, using (5) and the projection formula, we have

$$\mathrm{inv}_v(\alpha_M(x)) = \mathrm{inv}_v(\mathrm{Cores}_{k_M/k}((K_M/k_M, x-a_M))) = \mathrm{inv}_v(N_{k_M/k}(\delta_M(m)), 1/\pi_v)$$

where π_v denotes a uniformizer for k_v, and this last quantity is zero since $N_{k_M/k}(\delta_M(m))$ is a square in k_v (hypothesis (2)). We now conclude

$$\mathrm{inv}_{v_M}(\alpha_M(x)) = \mathrm{inv}_{v_M}(\mathrm{Cores}_{k_M/k}((K_M/k_M, x-a_M))) = 0.$$

In view of the transversality condition at v_M ((3) and (4)), this last vanishing implies that K_M/k_M splits at v_M.

Now for any place $v \notin S$, either x does not intersect any of the $\tilde{M}$, whence $X_x(k_v) \neq \emptyset$ by lemma 2.1.1 (a), or x meets one $\tilde{M}$ transversally at v (viewed as a place of k or of k_M) and this place of k_M splits in K_M, whence $X_x(k_v) \neq \emptyset$ by lemma 2.1.1 (b). If x is close enough to x_v for $v \in S$ (condition (6) – already used above), we have $X_x(k_v) \neq \emptyset$ by the implicit function theorem. This completes the proof of (i).

(ii) Evaluating 'functions' from $O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2}$ at x gives the identity map on $O^*_{L\cup L_\infty}/O^{*2}_{L\cup L_\infty}$. The group $O_{L\cup L_\infty}[\mathcal{U}]^*$ is generated by $O^*_{L\cup L_\infty}$ and the polynomials $R_M(t)$ for $M \in T$.

Consider the diagram

(2.1.1)

$$\begin{array}{ccccccccc}
0 & \to & (O^*_{L\cup L_\infty}/O^{*2}_{L\cup L_\infty})^2 & \to & (O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2})^2 & \to & \oplus_{M\in T}(\mathbf{Z}/2)^2 & \to & 0 \\
 & & \downarrow = & & \downarrow \mathrm{ev}_x & & \downarrow = & & \\
0 & \to & (O^*_{L\cup L_\infty}/O^{*2}_{L\cup L_\infty})^2 & \to & (O^*_{L(x)\cup L_\infty}/O^{*2}_{L(x)\cup L_\infty})^2 & \to & \oplus_{M\in T}(\mathbf{Z}/2)^2 & \to & 0
\end{array}$$

where the top right hand side arrow is induced by the valuation maps $k(\mathbf{P}^1)^* \to \mathbf{Z}$ at the points $M \in T$, and where the bottom right hand side arrow is induced by the valuation maps $k^* \to \mathbf{Z}$ at the places v_M of k. Using property (4), we find that this diagram is commutative. Hence the middle vertical map is an isomorphism, as claimed in (ii).

(iii) Let us first consider the Kummer map $\partial : E(U) \to (k[U]^*/(k[U]^{*2})^2$. The point $(X, Y) = (c_1, 0)$ is mapped to the class $e_1 = ((c_1-c_2)(c_1-c_3), c_1-c_2))$ and the point $(X, Y) = (c_2, 0)$ to the class $e_2 = (c_2-c_1, (c_2-c_1)(c_2-c_3))$. As for the point $(X, Y) = (c_3, 0)$, it is sent to (c_3-c_1, c_3-c_2), which is the product of the two previous classes. By assumption, $R(t) = (c_2-c_3)(c_3-c_1)(c_1-c_2)$ is a non-constant squarefree polynomial and the various $c_i - c_j$ all have the same even degree, which is therefore positive. Comparing the irreducible factors of the coordinates of e_1 and e_2 shows that these classes are independent in $(k[U]^*/(k[U]^{*2})^2$ (here and later, independence refers to independence in the $\mathbf{F}_2$-vector spaces under consideration). As for $m = (m_1, m_2)$, it lies in $\mathfrak{S}_0$ and by assumption does not belong to the subgroup of $(k[U]^*/(k[U]^{*2})^2$ spanned by the two previous classes. The classes m, e_1, e_2 all lie in $(O_{S_0}[\mathcal{U}]^*/O_S[\mathcal{U}]^{*2})^2$. By (ii), evaluating these classes at x gives rise to independent classes in $(O^*_{L(x)\cup L_\infty}/O^{*2}_{L(x)\cup L_\infty})^2$. To complete the proof of (iii), it only remains to observe that since any $c_i - c_j$ has even degree and since m belongs to $\mathfrak{S}_0$, the degrees (modulo 2) of the coordinates of m, e_1, e_2 are all even, hence for any $v \in L_\infty$, condition (5) implies that the v-adic valuation of the coordinates of $\mathrm{ev}_x(m), \mathrm{ev}_x(e_1), \mathrm{ev}_x(e_2)$ is even. □

2.2 The group $\mathfrak{S}$ and the map δ

We want to give a precise description of the group $\mathfrak{S}$ defined in the introduction. In this subsection, k is any field of characteristic not 2. We have the split exact sequence

$$0 \to (k^*/k^{*2})^2 \to (k[U]^*/k[U]^{*2})^2 \to \oplus_{M\in T}(\mathbf{Z}/2)^2 \to 0$$

where the right hand side map is given by taking valuation at points in T, one splitting being given by the polynomials R_M.

Recall that the product $R(t) = (c_2 - c_3)(c_3 - c_1)(c_1 - c_2)$ is squarefree and differs from $\prod_{M\in T} R_M$ by a constant. Hence each R_M divides a well-defined $c_i - c_j$. For any $M \in T$, let us define $(\beta_M, \gamma_M) \in (\mathbf{Z}/2)^2$ in the following explicit fashion. If R_M divides $c_1 - c_2$, let $(\beta_M, \gamma_M) = (1, 1)$. If R_M divides $c_2 - c_3$, let $(\beta_M, \gamma_M) = (0, 1)$. If R_M divides $c_3 - c_1$, let $(\beta_M, \gamma_M) = (1, 0)$. Note that since none of the $c_i - c_j$ is constant, any non-zero element of $(\mathbf{Z}/2)^2$ is equal to (β_M, γ_M) for some M.

Comparing this definition with the definition of $\mathfrak{S}$ in the introduction, we find that the group $\mathfrak{S} \subset (k[U]^*/k[U]^{*2})^2$ is the inverse image of the subgroup

$$\oplus_{M\in T}(\mathbf{Z}/2)(\beta_M, \gamma_M) \subset \oplus_{M\in T}(\mathbf{Z}/2 \times \mathbf{Z}/2)$$

under the right hand side map in the above diagram. In other words, the group $\mathfrak{S} \subset (k[U]^*/k[U]^{*2})^2$ is isomorphic to the direct sum of $(k^*/k^{*2})^2$ and the free $\mathbf{Z}/2$-module with generators $(R_M^{\beta_M}, R_M^{\gamma_M})$ for M running through T. Since the polynomials R_M all belong to $O_{S_0}[\mathcal{U}]^*$, in the description we have just given, we may replace k everywhere by any ring between O_{S_0} and k.

We shall later need to consider the map $\eta : (k[U]^*/k[U]^{*2})^2 \to (\mathbf{Z}/2)^2$ given by the valuation at infinity (degree map). Indeed, the subgroup $\mathfrak{S}_0 \subset \mathfrak{S}$ is precisely the kernel of the composite map $\mathfrak{S} \subset (k[U]^*/k[U]^{*2})^2 \xrightarrow{\eta} (\mathbf{Z}/2)^2$, which we shall also denote η. This map sends the element $(R_M^{\beta_M}, R_M^{\gamma_M})$ to $(\beta_M.\deg(R_M), \gamma_M.\deg(R_M)) \in (\mathbf{Z}/2)^2$.

We now discuss the map δ. Let $b(t) = (b_1(t), b_2(t)) \in \mathfrak{S} \subset (k[U]^*/k[U]^{*2})^2$. Let $M \in T$. Let $i \in \{1,2,3\}$ be the unique value such that R_M divides $c_j - c_k$, where $\{i,j,k\} = \{1,2,3\}$. Let Q_j be a point of order exactly 2 of $E(U) = E(k(t))$ other than the point with coordinate $(X,Y) = (c_i, 0)$. Consider the image $\varepsilon_j = (\varepsilon_{j,1}, \varepsilon_{j,2}) \in H^1(U, (\mathbf{Z}/2)^2)$ of Q_j under the Kummer map $\partial : E(U)/2 \to H^1(U, (\mathbf{Z}/2)^2)$. We can then form the cup-product

$$< b, \varepsilon_j >= (b_1, \varepsilon_{j,2}) - (\varepsilon_{j,1}, b_2) \in H^2(U, \mathbf{Z}/2) \xrightarrow{\simeq} {}_2\mathrm{Br}(U).$$

Lemma 2.2.1 *Let $\delta_M : \mathfrak{S} \to k_M^*/k_M^{*2}$ be the set-theoretic map defined in the introduction.*
(i) For any $b \in \mathfrak{S}$ as above, $\delta_M(b)$ coincides with the image of $< b, \varepsilon_j > \in {}_2\mathrm{Br}(U)$ under the residue map ${}_2\mathrm{Br}(U) \to H^1(k_M, \mathbf{Z}/2) = k_M^*/k_M^{*2}$. In particular, δ_M is a homomorphism.
(ii) The image $\partial(E(U))$ of $E(U)$ under the Kummer map lies in the kernel of δ_M.
(iii) For $(c,d) \in (k^*/k^{*2})^2 \subset \mathfrak{S}$, we have $\delta_M(c,d) = c^{\gamma_M}.d^{\beta_M} \in k_M^*/k_M^{*2}$.
(iv) The kernel of the diagonal map $\delta : \mathfrak{S} \to \oplus_{M\in T} k_M^*/k_M^{*2}$ is a finite group.
(v) The kernel of the composite map

$$\mathfrak{S} \xrightarrow{\delta} \bigoplus_{M\in T} k_M^*/k_M^{*2} \to \bigoplus_{M\in T} k_M^*/ < k_M^{*2}, \delta_M(m) >$$

is a finite group.

Proof (i) This is checked by a straightforward but tedious computation. Let us assume that the polynomial R_M divides $p_1 = c_2 - c_3$. We may assume that b_1, b_2 are in $k[t]$ and are square-free and that b_3 is $b_1.b_2$ divided by its square factors. Since $b \in \mathfrak{S}$, we know that b_1 is prime to p_1, hence in particular $b_1(M) \neq 0 \in k(M)$. The image of the 2-torsion point Q_2 $(X = c_2, Y = 0)$ under the Kummer map is $\varepsilon_2 = (\varepsilon_{2,1}, \varepsilon_{2,2}) = (c_2 - c_1, (c_2 - c_1)(c_2 - c_3)) \in (k[U]^*/k[U]^{*2})^2$. Hence

$$< b, \varepsilon_2 >= (b_1, (c_2 - c_1)(c_2 - c_3)) - (c_2 - c_1, b_2) \in H^2(U, \mathbf{Z}/2) = {}_2\mathrm{Br}(U).$$

Now

$$(b_1, (c_2-c_1)(c_2-c_3))-(c_2-c_1, b_2) = (b_1, (c_2-c_1)(c_2-c_3))+(b_2, c_2-c_1) = (b_1, c_2-c_3)+(b_3, c_2-c_1).$$

Since the R_M valuation of b_1 and of $c_2 - c_1$ is 0, and that of $c_2 - c_3$ is one, we find that the residue of $< b, \varepsilon_2 >$ at M is

$$b_1(M).(c_2(M) - c_1(M))^{v_M(b_3)} \in k_M^*/k_M^{*2}, \tag{2.2.1}$$

where v_M denotes the valuation at M. We leave it to the reader to write down the equations of the surface $X(b)$ above a neighbourhood of M and check that this class coincides with $\delta_M(m)$ as defined in the introduction : one has to distinguish two cases, depending on whether the R_M-valuation of each b_i is even (hence zero), or not.

(ii) This is proved by a case-by-case discussion involving valuation arguments and formula (2.2.1), in the case where R_M divides p_1, and is checked similarly in the other cases.

(iii) The statement follows from formula (2.2.1) in the case where R_M divides p_1, and is checked similarly in the other cases.

(iv) Since $\mathfrak{S}$ is spanned by the finitely many elements $(R_M^{\beta_M}, R_M^{\gamma_M})$ and by $(k^*/k^{*2})^2$, it is enough to check that the kernel of the induced map $\delta : (k^*/k^{*2})^2 \to \oplus_{M\in T} k_M^*/k_M^{*2}$ is finite. There exists a point $M_1 \in T$ with $(\beta_{M_1}, \gamma_{M_1}) = (1,0)$ and a point $M_2 \in T$ with $(\beta_{M_2}, \gamma_{M_2}) = (0,1)$. It is enough to show that the kernel of the induced map $k^*/k^{*2} \oplus k^*/k^{*2} \to k_{M_1}^*/k_{M_1}^{*2} \oplus k_{M_2}^*/k_{M_2}^{*2}$ is finite. By (ii), this map simply reads $(c,d) \mapsto (c,d)$, and we are reduced to the simple algebraic fact : if K/k is a finite separable extension of a field k of characteristic not 2, the kernel of the map $k^*/k^{*2} \to K^*/K^{*2}$ is finite (reduce to the case where K/k is Galois with group

G, and use the restriction inflation sequence, which shows that the kernel is the finite group $H^1(G, \mathbf{Z}/2) = \mathrm{Hom}(G, \mathbf{Z}/2)$).

(v) This immediately follows from (iv). □

Remark To any $b = (b_1, b_2) \in (k(t)^*/k(t)^{*2})^2$ one may associate the element

$$\xi = (X - c_1(t), b_2(t)) + (X - c_2(t), b_1(t))$$

in the (2-torsion subgroup of the) Brauer group of the generic fibre of the regular minimal model $E/\mathbf{P}^1_k$. The assumption $b \in \mathfrak{S}$ guarantees that all residues of ξ at generic points of components of closed fibres over $\mathbf{A}^1_k$ are constant. Given $M \in T$, the fibre E_M has two components, the neutral component C_M and the 'second' one C'_M. The residue $\delta_{C'_M} \in H^1(k(C'_M), \mathbf{Z}/2)$ at the second component comes from $H^1(k_M, \mathbf{Z}/2)$, and one checks that it comes from $\delta_M(b) \in k^*_M/k^{*2}_M = H^1(k_M, \mathbf{Z}/2)$ as defined in the introduction. Suppose R_M divides p_i. Then any 2-torsion point $Q_j, j \neq i$, defines a section of $E/\mathbf{P}^1_k$ which hits the second component (whereas 0 and the point $(X, Y) = (c_i, 0)$ hit the neutral component). The class $< b, \varepsilon_j >$ is none other than the inverse image under the section Q_j of the class ξ, and the residue of this inverse image at M is just the inverse image under Q_j of the (constant) residue $\delta_M(b)$, hence equal to $\delta_M(b)$.

2.3 Independence on x : the space

Given $x \in k$ as in proposition 2.1.3, let us consider the curve E_x. It has good reduction at all places outside $L(x)$ (it has indeed good reduction at places in L_∞). In subsection 1.1 we defined $U_{L(x)} = (O^*_{L(x)}/O^{*2}_{L(x)})^2$ and in subsection 1.2 we considered the subspace $U'_{L(x)} \subset U_{L(x)}$ attached to the curve E_x. By proposition 1.2.3, this is the space with which one computes the Selmer group. It is defined by local conditions, namely, it consists of elements in $(O^*_{L(x)}/O^{*2}_{L(x)})^2$ whose image under the map

$$(O^*_{L(x)}/O^{*2}_{L(x)})^2 \to (k^*_v/k^{*2}_v)^2$$

belongs to $W_v(E_x) + K_v$, this for all $v \in L(x)$. In particular, statement (iii) in proposition 2.1.3 may be completed as follows : for x as in that proposition, the images of the points of order 2 on E_x under the Kummer map ∂ and the class of $m(x)$ in $(k^*/k^{*2})^2$ lie in the subgroup $U'_{L(x)}$ and are independent.

The spaces K_v do not depend on x. By the approximation condition (6) in proposition 2.1.3, for $v \in S$ the elliptic curve E_x is very close to E_{x_v} in the v-adic topology; hence, with the notation of the first section, the subspaces $W_v(x) = W_v(E_x)$ and $W_v(x_v) = W_v(E_{x_v})$ of V_v are identical. Hence the conditions defining $U'_{L(x)}$ at the places of S do not depend on x.

Let us revert to the considerations at the end of subsection 1.2. They imply the following : given $R_M(t)$ a monic irreducible divisor of $R(t)$, and $(\beta_M, \gamma_M) \neq 0 \in (\mathbf{Z}/2)^2$ as in the beginning of subsection 2.2, for any $x \in U(k_v)$ which intersects $\tilde{M}$ *transversally* above the place v of k, the subspace $W_v(x) + K_v \subset V_v$ consists of the elements of $(k^*_v/k^{*2}_v)^2$ whose image under the valuation map lies in $\{(0,0), (\beta_M, \gamma_M)\} \subset (\mathbf{Z}/2)^2$. Thus for a prime $v \in L(x) \setminus S$, the condition that an element of $(O^*_{L(x)}/O^{*2}_{L(x)})^2$ lies in $W_v(x) + K_v$ only depends on which $L_M \cup v_M$ the place v belongs to, it does not depend on x. Note that for $v \in L(x) \setminus S$, the quotient $(W_v + K_v)/K_v \simeq W_v/W_v \cap K_v$ is isomorphic to $\mathbf{Z}/2$.

Lemma 2.3.1 *Let L and x be as in proposition 2.1.3.*

a) The inverse image $N_0 = U'_S$ in $(O_S{}^*/O_S{}^{*2})^2 \subset V_L$ of $U'_{L(x)} \subset V_{L(x)}$ (under the diagonal map $(O^*_S/O^{*2}_S)^2 \to (O^*_{L(x)}/O^{*2}_{L(x)})^2$) depends neither on L nor on x.

b) The inverse image U'_L of $U'_{L(x)} \subset V_{L(x)}$ in $U_L = (O_L{}^*/O_L{}^{*2})^2 \subset V_L$ (under the diagonal map $(O_L^*/O_L^{*2})^2 \to (O_{L(x)}^*/O_{L(x)}^{*2})^2$) only depends on $L = S \cup (\cup_{M \in T} L_M)$, it does not depend on x.

Proof For the subgroup $(O_S{}^*/O_S{}^{*2})^2 \subset (O_{L(x)}{}^*/O_{L(x)}{}^{*2})^2$, the condition at a place $v \notin S$ is automatically satisfied, since $K_v = (O_v^*/O_v^{*2})^2$ for such a v, and we have seen that the conditions at the places in S are independent of L and x.

For the subgroup $(O_L{}^*/O_L{}^{*2})^2 \subset (O_{L(x)}{}^*/O_{L(x)}{}^{*2})^2$, the condition at a place v_M $(M \in T)$ is automatically satisfied, since $K_v = (O_v^*/O_v^{*2})^2$ for any $v \notin S$, and we have seen that the conditions at other places are independent of x. $\square$

The proof to follow will involve the construction of a 'subdiagram' of the diagram appearing in the proof of 2.1.3. Basically, we want to look at the inverse image of $U'_{L(x)} \subset U_{L(x) \cup L_\infty}$ under ev_x. Before doing this, we shall fix L_∞.

Consider the finite subgroup $\mathfrak{S}_S$ of $\mathfrak{S}$ spanned by U_S and the elements $(R_M(t)^{\beta_M}, R_M(t)^{\gamma_M})$ for M running through T. This subgroup contains m. For each $M \in T$, we have the finite subgroup $\delta_M(\mathfrak{S}_S) \subset k_M^*/k_M^{*2}$, which defines a multiquadratic extension F_M/k_M. Let F/k be the composite of the extensions F_M/k. It is a consequence of Tchebotarev's theorem that there exist infinitely many principal ideals (π_v) in the ring of integers O of k such that the (chosen) generator π_v is a square (as a matter of fact, as close as one wishes to 1) in each completion k_w for $w \in S$, and such that moreover the place v splits in each quadratic extension $k(\sqrt{N_{k_M/k}(\delta_M(m))})/k$, $M \in T$. Choose $v_\infty \notin S$ a place which satisfies these properties (required in proposition 2.1.3), and which moreover is unramified in the extension F/k. Let $\mu = \pi_{v_\infty} \in O$ be a generator of the corresponding principal ideal. For each $w \in S$, μ is a square in k_w. For the rest of section 2, we fix the set $L_\infty = \{v_\infty\}$, and we let $x_\infty = x_{v_\infty} = 1/\mu \in k_{v_\infty}$.

Remark In the special case where all the R_M's are of even degree, or more generally under an assumption slightly stronger than (D) (see remark 2.5.4 (iv)), one may take $L_\infty = \emptyset$ and $\mu = 1$ in the proof to follow.

Lemma 2.3.2 *Let X and S be as above. For each $M \in T$, there exists a uniquely defined $(a_M, b_M) \in U_S = (O_S{}^*/O_S{}^{*2})^2$ such that for any $L_\infty = \{v_\infty\}$ and μ as above, any L and x as in proposition 2.1.3,*

$$(a_M(\mu^{\deg(R_M)} R_M(x))^{\beta_M}, b_M(\mu^{\deg(R_M)} R_M(x))^{\gamma_M}) \in U_{L(x) \cup L_\infty}$$

is in the subspace of $U'_{L(x)} \subset U_{L(x) \cup L_\infty}$ defined by the additional conditions that the local projection at $v \in S$ is in K_v for all $v \in S$.

Proof Let us write $\zeta = (a_M(\mu^{\deg(R_M)} R_M(x))^{\beta_M}, b_M(\mu^{\deg(R_M)} R_M(x))^{\gamma_M}) \in U_{L(x) \cup L_\infty}$. For any $(a_M, b_M) \in U_S$, and x as in proposition 2.1.3, for any valuation $v \notin L(x)$, the coordinates of ζ have even valuation : this is clear for $v \notin L_\infty$, and for $v \in L_\infty$, it follows from the transversality conditions (3) and (5), together with the definition of μ. Thus $\zeta \in U_{L(x)}$. For any $(a_M, b_M) \in U_S$, the local condition $\zeta \in W_v(E_x) + K_v$ is satisfied at places $v \in L_{M_1} \cup \{v_{M_1}\}$ for $M_1 \neq M$, since at such places the coordinates have even valuation and $K_v = (O_v^*/O_v^{*2})^2$ for any $v \notin S$. For any $(a_M, b_M) \in U_S$, the local condition is also satisfied at places in $L_M \cup \{v_M\}$ (see comment before lemma 2.3.1). Since x is v-adically very close to x_v for $v \in S$ (condition (6) in proposition 2.1.3), the class of $R_M(x)$ in k_v^*/k_v^{*2} for such v does not depend on x. Since μ is a square in each k_v for $v \in S$, this implies that the projection of $((\mu^{\deg(R_M)} R_M(x))^{\beta_M}, (\mu^{\deg(R_M)} R_M(x))^{\gamma_M})$ to V_S is independent of x, L and L_∞. Since

$U_S \oplus K_S = V_S$, by modifying $((\mu^{\deg(R_M)}R_M(x))^{\beta_M}, (\mu^{\deg(R_M)}R_M(x))^{\gamma_M})$ by a well-defined $(a_M, b_M) \in U_S$, we can achieve that the projection of

$$\zeta = (a_M(\mu^{\deg(R_M)}R_M(x))^{\beta_M}, b_M(\mu^{\deg(R_M)}R_M(x))^{\gamma_M})$$

to V_v belong to K_v for all $v \in S$. □

Let $A_M = (a_M(\mu^{\deg(R_M)}R_M(t))^{\beta_M}, b_M(\mu^{\deg(R_M)}R_M(t))^{\gamma_M}) \in (O_{S\cup L_\infty}[\mathcal{U}]^*/O_{S\cup L_\infty}[\mathcal{U}]^{*2})^2$. As we have seen above, these are elements of $\mathfrak{S} \subset (k[U]^*/k[U]^{*2})^2$.

Notation 2.3.3 *Let $A \subset (O_{S\cup L_\infty}[\mathcal{U}]^*/O_{S\cup L_\infty}[\mathcal{U}]^{*2})^2 \subset (k[U]^*/k[U]^{*2})^2$ be the subspace spanned by the A_M for $M \in T$. Let $N = A \oplus U'_L \subset (O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2})^2$ be the subspace generated by A and $U'_L = U'_{L(x)} \cap ({O_L}^*/{O_L}^{*2})^2$.*

The definition of N depends on the choice of the family of subspaces K_v (fixed once and for all) as well as on the points $Q_v \in X(k_v), v \in S$ (which determine the spaces $W_v(x) = W_v(Q_v)$ for $v \in S$), as well as on L and L_∞. But once these choices have been made, lemma 2.3.1 shows that N does not depend on the particular point x chosen as in proposition 2.1.3.

If we fix L_∞ and μ as above, but still let the L_M's and v_M's vary, there is a subspace of $(k[U]^*/k[U]^{*2})^2$ which is contained in any N, namely the subspace $N_0 \oplus A \subset (O_{S\cup L_\infty}[\mathcal{U}]^*/O_{S\cup L_\infty}[\mathcal{U}]^{*2})^2$, where $N_0 = U'_S$ is as above, and may be defined as $N_0 = N \cap (O_S^*/O_S^{*2})^2 \subset (O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2})^2$. Both N_0 and A are independent of L, and they clearly do not intersect.

As we observed in the proof of part (ii) of proposition 2.1.3, the evaluation map $\mathrm{ev}_x : (O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2})^2 \to (O^*_{L(x)\cup L_\infty}/O^{*2}_{L(x)\cup L_\infty})^2$ is an isomorphism as soon as properties (3) and (4) hold.

Proposition 2.3.4 *Let L, L_∞ and x be as in proposition 2.1.3, and let N be as above.*
(a) The evaluation map ev_x from $(O_{L\cup L_\infty}[\mathcal{U}]^*/O_{L\cup L_\infty}[\mathcal{U}]^{*2})^2$ to $(O^*_{L(x)\cup L_\infty}/O^{*2}_{L(x)\cup L_\infty})^2$ induces an isomorphism between N and $U'_{L(x)}$.
(b) Denote by φ_x the composition of this isomorphism with the isomorphism $\tau^{-1}_{L(x)} : U'_{L(x)} \xrightarrow{\simeq} W'_{L(x)} = \oplus_{v\in L(x)}(W_v/W_v \cap K_v)$. There is a direct sum decomposition :

$$N = N_0 \oplus A \oplus \varphi_x^{-1}(\oplus_{v\in L\setminus S}(W_v/W_v \cap K_v)).$$

Proof That the isomorphism ev_x sends N into $U'_{L(x)}$ follows from lemma 2.3.2. The image of $U'_{L(x)}$ under the bottom horizontal map

$$({O_{L(x)}}^*/{O_{L(x)}}^{*2})^2 \to \oplus_{M\in T}(\mathbf{Z}/2)^2$$

in diagram (2.1.1) (map induced by the valuations v_M of k) has dimension equal to the order of T. Indeed, for each M, the image of the corresponding projection $U'_{L(x)} \to (\mathbf{Z}/2)^2$ falls into $\{(0,0), (\beta_M, \gamma_M)\}$. On the other hand, the image of

$$A_M(x) = (a_M(\mu^{\deg(R_M)}R_M(x))^{\beta_M}, b_M(\mu^{\deg(R_M)}R_M(x))^{\gamma_M})$$

has projection (β_M, γ_M) at M and $(0,0)$ at the points of $T \setminus M$. Inspection of diagram (2.1.1) completes the proof of (a).

As for (b), note that $\varphi_x(N_0) = \varphi_x(U'_S) = \tau^{-1}_{L(x)}(U'_S) = \oplus_{v\in S}(W_v/W_v \cap K_v) \subset W'_{L(x)}$, and that, by the choice of μ and A_M (see lemma 2.3.2), the image of $A_M \in N$ under φ_x has zero component at all places in S, as well as at places in $L_{M_1} \cup v_{M_1}$ for $M_1 \neq M$, whereas it has component $1 \in \mathbf{Z}/2 = W_v/W_v \cap K_v$ for $v \in L_M \cup v_M$. $\square$

2.4 Independence on x : the pairing

In the previous subsection, given any L , L_∞ and any x as in proposition 2.1.3, and N as in definition 2.3.3, we have obtained an isomorphism

$$\mathrm{ev}_x : N \xrightarrow{\simeq} U'_{L(x)}.$$

According to proposition 1.2.3, there is an isomorphism $\tau_{L(x)} : W'_{L(x)} \xrightarrow{\simeq} U'_{L(x)}$ and the $e_{L(x)}$-pairing on $V_{L(x)}$ induces a pairing $e'_{L(x)} : U'_{L(x)} \times W'_{L(x)} \to \mathbf{Z}/2$ and then a symmetric pairing $U'_{L(x)} \times U'_{L(x)} \to \mathbf{Z}/2$ defined by $(x, y) \mapsto e'_{L(x)}(x, \tau^{-1}_{L(x)}(y))$.

Notation 2.4.1 *Let $e_N : N \times N \to \mathbf{Z}/2$ be the symmetric pairing given by the composite map*

$$N \times N \xrightarrow{(\mathrm{ev}_x,\mathrm{ev}_x)} U'_{L(x)} \times U'_{L(x)} \xrightarrow{(id,\tau^{-1}_{L(x)})} U'_{L(x)} \times W'_{L(x)} \xrightarrow{e'_{L(x)}} \mathbf{Z}/2$$

Note that the space N depends on L and L_∞ and that the pairing e_N should be denoted $e_{N,L,L_\infty,x}$, since it depends on all these data. The proof of the following important proposition will occupy the rest of this subsection.

Proposition 2.4.2 *Let L, $L_\infty = \{v_\infty\}$ and x be as above, and let N be as above. Then provided x is close enough to $x_\infty = 1/\mu$ at v_∞, the restriction to the subspace $N_0 \oplus A \subset (O_S[\mathcal{U}]^*/O_S[\mathcal{U}]^{*2})^2$ of the pairing e_N on $N \subset (k[U]^*/k[U]^{*2})^2$ depends neither on L nor on x.*

Proof As we have seen in subsection 2.2, the space $N_0 \oplus A$ depends neither on x nor on L. Under the evaluation map ev_x, the space $N_0 = U'_S \subset (O^*_S/O^{*2}_S)^2$ is mapped identically to itself.

Let $W'_S \to W'_{L(x)}$ be the map induced by the map $W_S \to W_{L(x)}$ sending the family $\{\alpha_v\}_{v\in S}$ to $\{\alpha^1_v\}_{v\in L(x)}$ with $\alpha^1_v = \alpha_v$ for $v \in S$ and $\alpha^1_v = 0$ for $v \in L(x) \setminus S$. Then the diagram

$$\begin{array}{ccc} U'_{L(x)} & \xrightarrow{\tau^{-1}_{L(x)}} & W'_{L(x)} \\ \uparrow & & \uparrow \\ U'_S & \xrightarrow{\tau^{-1}_S} & W'_S \end{array}$$

commutes, where the left vertical map is the natural inclusion of subgroups of $(k^*/k^{*2})^2$.

One now easily checks that the following diagram is commutative

$$\begin{array}{ccccccccccc} N & \times & N & \xrightarrow{(\mathrm{ev}_x,\mathrm{ev}_x)} & U'_{L(x)} & \times & U'_{L(x)} & \xrightarrow{(id,\tau^{-1}_{L(x)})} & U'_{L(x)} & \times & W'_{L(x)} & \xrightarrow{e'_{L(x)}} & \mathbf{Z}/2 \\ \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ N_0 & \times & N_0 & \xrightarrow{(\mathrm{ev}_x,\mathrm{ev}_x)} & U'_S & \times & U'_S & \xrightarrow{(id,\tau^{-1}_S)} & U'_S & \times & W'_S & \xrightarrow{e'_S} & \mathbf{Z}/2 \end{array}$$

From this diagram it follows that the restriction of the pairing $e_N : N \times N \to \mathbf{Z}/2$ to $N_0 \times N_0$ depends neither on x nor on L.

We now discuss the induced pairing on $A \times N_0$. Given $A_M \in A$ and $\rho \in N_0 \subset (O_S^*/O_S^{*2})^2$, we have

$$e_N(A_M, \rho) = e'_{L(x)}(A_M(x), \tau_{L(x)}^{-1}(\rho)).$$

From $\rho \in N_0 = U'_S$ we conclude as above (commutativity of the last but one diagram) that $\tau_{L(x)}^{-1}(\rho) \in W'_{L(x)} = \oplus_{v \in L(x)} W_v/(W_v \cap K_v)$ is of the shape $\sum_{v \in S} \beta_v$ (all the factors in $L(x) \setminus S$ are zero). The β_v's clearly do not depend on x. Now $e_N(A_M, \rho) = \sum_{v \in S} e'_v(A_M(x), \beta_v)$ only depends on the image of x in $\oplus_{v \in S} k_v$, hence by condition (6) of proposition 2.1.3 is independent of x and L. (Note also that since μ is a square in each k_v for $v \in S$, the pairing essentially does not depend on $L_\infty = \{v_\infty\}$.) Thus the restriction of e_N to $A \times N_0$ does not depend on x or L. By symmetry of the pairing e_N, we conclude that the restriction of e_N to $N_0 \times A$ also does not depend on x or L.

It remains to study the pairing e_N on $A \times A$. In other terms, we want to discuss $e_N(A_P, A_Q)$ for P and Q in T. Recall that

$$A_M(t) = (a_M(\mu^{\deg(R_M)} R_M(t))^{\beta_M}, b_M(\mu^{\deg(R_M)} R_M(t))^{\gamma_M})$$

with a_M and b_M in O_S^*/O_S^{*2}. We have $e_N(A_P, A_Q) = e'_{L(x)}(A_P(x), \tau_{L(x)}^{-1}(A_Q(x)))$. Let us write

$$A_Q(x) = \sum_{v \in L(x)} (\alpha_v + \beta_v) \ \in \ \bigoplus_{v \in L(x)} V_v$$

with $\alpha_v \in W_v$ and $\beta_v \in K_v$. For $v \notin S \cup L_Q \cup v_Q$, we may and will choose $\alpha_v = 0$. We have

$$\tau_{L(x)}^{-1}(A_Q(x)) = \sum_{v \in L(x)} \alpha_v \ \in \ \bigoplus_{v \in L(x)} W_v/(W_v \cap K_v),$$

with $\alpha_v = 0$ for $v \notin S \cup L_Q \cup v_Q$, hence :

$$e_N(A_P, A_Q) = \sum_{v \in L(x)} e_v(A_P(x), \alpha_v) = \sum_{v \in S} e_v(A_P(x), \alpha_v) + \sum_{v \in L_Q \cup v_Q} e_v(A_P(x), \alpha_v).$$

In view of property (6) of proposition 2.1.3, the sum $\sum_{v \in S} e_v(A_P(x), \alpha_v)$ depends neither on L nor on x (and it essentially does not depend on $L_\infty = \{v_\infty\}$, since μ is a square in each k_v for $v \in S$). Let us study $\sum_{v \in L_Q \cup v_Q} e_v(A_P(x), \alpha_v)$.

Assume first $P \neq Q$. Since $L_Q \cup \{v_Q\}$ does not meet $L_P \cup \{v_P\} \cup L_\infty$, and μ is a unit away from L_∞, the coordinates of $A_P(x)$ are units at each $v \in L_Q \cup v_Q$, hence $e_v(A_P(x), \beta_v) = 0$ at each such v (recall $\beta_v \in K_v$ and $K_v = (O_v^*/O_v^{*2})^2$ for $v \notin S$) hence $e_v(A_P(x), \alpha_v) = e_v(A_P(x), \alpha_v + \beta_v) = e_v(A_P(x), A_Q(x))$ at each such v. We thus find

$$\sum_{v \in L_Q \cup v_Q} e_v(A_P(x), \alpha_v) = \sum_{v \in L_Q \cup v_Q} e_v(A_P(x), A_Q(x)).$$

All components of $A_P(x)$ and $A_Q(x)$ have even valuation at any v_∞, hence for any such place we have $e_v(A_P(x), A_Q(x)) = 0$. The sum above is thus equal to

$$\sum_{v \in L_Q \cup v_Q \cup L_\infty} e_v(A_P(x), A_Q(x)).$$

We claim that this sum does not depend on L or x, provided that x satisfies the proximity condition (6) in proposition 2.1.3 and also satisfies a suitable proximity condition at v_∞. Given the definition of the A_M's, and the computation of the pairing e_v, this reduces to the following, which will be applied to $S \cup L_\infty$ rather than S. Suppose we have two irreducible polynomials $f(t)$ and $g(t)$ in $O_S[t]$ such that the product $f(t)g(t)$ defines a closed subscheme of $\mathbf{A}^1_{O_S}$ which is finite and étale over O_S, and suppose that $x \in \mathbf{P}^1(O_S)$ is transversal to this closed subscheme. Let $k_g = k[t]/g(t) = k(a_g)$, with $g(t) = uN_{k_g/k}(t - a_g)$, $u \in O_S^*$. Note that $f(a_g)$ is a unit at all places of k_g not above a place of S. Then

$$\sum_{v \notin S,\ v(g(x))>0} \mathrm{inv}_v(f(x), g(x)) = \sum_{v \notin S,\ v(g(x))>0} \mathrm{inv}_v(f(x), N_{k_g/k}(x - a_g))$$

since $f(x)$ is a unit at the places v where $v(g(x)) > 0$. This last sum is equal to

$$\sum_{v \notin S,\ v(g(x))>0} \mathrm{inv}_v(\mathrm{Cores}_{k_g/k}(f(x), x - a_g))$$

by the projection formula, and in turn this sum may be written

$$\sum_{v \notin S,\ v(g(x))>0} \mathrm{inv}_v(\mathrm{Cores}_{k_g/k}(f(a_g), x - a_g))$$

since $f(a_g)$ is a unit away from S. This also coincides with

$$\sum_{v \notin S} \mathrm{inv}_v(\mathrm{Cores}_{k_g/k}(f(a_g), x - a_g)) = -\sum_{v \in S} \mathrm{inv}_v(\mathrm{Cores}_{k_g/k}(f(a_g), x - a_g))$$

where the last equality follows from the reciprocity law in global class field theory. Now for x close enough to given values in k_v for $v \in S$, this last term is constant. (For similar computations, see [SwD94], Lemma 2, [SwD95] and [CT/SwD94], Lemmas 7.2.1 and 7.2.4.)

Let us now assume $P = Q$. To fix ideas, let us assume that $R_P(t)$ divides $p_3(t) = c_1(t) - c_2(t)$. Then $(\beta_P, \gamma_P) = (1, 1)$, hence $A_P(t) = (a_P R_P(t), b_P R_P(t))$. The point of order 2 on $E_x(k_v)$ given by $X = c_1(x)$ has image $((c_1(x) - c_2(x))(c_1(x) - c_3(x)), c_1(x) - c_2(x)) \in (k_v^*/k_v^{*2})^2$ under the Kummer map. For any $v \in L_P \cup v_P$, it follows that one may write $A_P(x) \in V_v$ as the sum of $\alpha_v = ((c_1(x) - c_2(x))(c_1(x) - c_3(x)), c_1(x) - c_2(x)) \in W_v$ and an element in K_v. Thus

$$\sum_{v \in L_P \cup v_P} e_v(A_P(x), \alpha_v) = \sum_{v \in L_P \cup v_P} e_v(A_P(x), ((c_1(x) - c_2(x))(c_1(x) - c_3(x)), c_1(x) - c_2(x))).$$

Let $B(t) = (C(t), D(t))$ be the quotient of $((c_1(t) - c_2(t))(c_1(t) - c_3(t)), c_1(t) - c_2(t))$ by $A_P(t)$; the polynomials $C(t)$ and $D(t)$ are now coprime with $R_P(t)$, with coefficients in $O_{S \cup L_\infty}$, and leading coefficients in $O^*_{S \cup L_\infty}$. We have

$$e_v(A_P(x), A_P(x)) = 0$$

for any place v (using the skew-symmetry of e_v). Thus

$$\sum_{v \in L_P \cup v_P} e_v(A_P(x), \alpha_v) = \sum_{v \in L_P \cup v_P} e_v(A_P(x), B(x)).$$

Now the same argument as for the case $P \neq Q$ enables us to conclude that provided x satisfies the proximity condition (6) in proposition 2.1.3 and also satisfies a suitable proximity condition at v_∞, this sum is independent both of x and L, hence so is also $e_N(A_P, A_P)$. □

2.5 Completion of the proof of the Theorem

In this subsection, we shall complete the proof of the Theorem, as stated in the introduction.

Proposition 2.5.1 *Let $m = (m_1(t), m_2(t), m_3(t)) \in \mathfrak{S}_0$ be as in the beginning of this section, and let $X/\mathbf{P}^1_k$ be the associated pencil of curves of genus one. Assume that $m \in H^1(k(t), (\mathbf{Z}/2)^2)$ is not the image of a point of order 2 under the Kummer map. Assume :*

(D) *The kernel of the composite map*

$$\mathfrak{S}_0 \to \bigoplus_{M\in T} k_M^*/k_M^{*2} \to \bigoplus_{M\in T} k_M^*/ < k_M^{*2}, \delta_M(m) >$$

is generated by m and the image of the 2-torsion subgroup ${}_2E(U)$ of $E(U)$ under the Kummer map.

Let $L_\infty = \{v_\infty\}$ be as above. Then there exist finite sets L_M of places of k, for $M \in T$, satisfying properties (1) and (2) of proposition 2.1.3 and points $x_v \in O_v$ for $v \in \cup_{M\in T} L_M$ such that for any $x \in U(k)$ satisfying properties (3) to (6) of that same proposition, close enough to $x_\infty = 1/\mu$ at v_∞ and close enough to each x_v for $v \in \cup_{M\in T} L_M$, the 2-Selmer group $\mathcal{S}(E_x, 2)$ has order 8 and is generated by $m(x)$ and the images of the 2-torsion points of $E_x(k)$.

Proof First of all $m(x)$ and the image of the 2-torsion points of $E_x(k)$ under the Kummer map are in the 2-Selmer group of E_x. This is clear for the 2-torsion points. As for $m(x)$, this is the content of (i) in proposition 2.1.3 : X_x has points everywhere locally. By proposition 2.1.3 (iii), these three classes define independent elements in the $\mathbf{F}_2$-vector space $U'_{L(x)}$, which contains the 2-Selmer group (proposition 1.2.3).

Under the isomorphism $\mathrm{ev}_x : N \xrightarrow{\simeq} U'_{L(x)}$ these classes correspond to elements in the group $N_0 \oplus A$. Indeed, from the definition of the (β_M, γ_M) one checks that there exists a suitable product of the $A_M(x)$ such that the quotient of $m(x)$ by this product, which a priori lies in $U'_{L(x)} \subset (O^*_{L(x)}/O^{*2}_{L(x)})^2$, actually lies in $(O^*_S/O^{*2}_S)^2$ hence lies in U'_S. The inverse image of $m(x)$ under ev_x thus lies in $N_0 \oplus A$. The argument is similar for the points of order 2. Let $B_0 \subset N_0 \oplus A \subset (O_{S\cup L_\infty}[\mathcal{U}]^*/O_{S\cup L_\infty}[\mathcal{U}]^{*2})^2$ be the subgroup they generate, which is clearly independent of L. Since the corresponding elements in $U'_{L(x)}$ are in the 2-Selmer group, the group B_0 is in the kernel of the pairing e_N on $N \times N$ (see proposition 1.2.3). Let $B \subset N_0 \oplus A$ be the kernel of the restriction of e_N to $N_0 \oplus A \subset N$; this kernel is independent of x and L (proposition 2.4.2). Let $B_1 \subset B$ (independent of x and L) be such that $B = B_0 \oplus B_1$. Let $B_2 \subset N_0 \oplus A$ be a supplementary space for $B \subset N_0 \oplus A$. Finally, let $B_3 = \varphi_x^{-1}(\oplus_{v\in L\setminus S}(W_v/W_v \cap K_v))$ be as in proposition 2.3.4. This is a supplementary space for $N_0 \oplus A \subset N$. We thus have $N = B_0 \oplus B_1 \oplus B_2 \oplus B_3$.

Lemma 2.5.2 *Let S_1 be a finite set of places containing S. Assume that $b(t) = (b_1(t), b_2(t)) \in (O_{S_1}[\mathcal{U}]^*/O_{S_1}[\mathcal{U}]^{*2})^2$ lies in $\mathfrak{S}$ but is not in the kernel of the map*

$$\mathfrak{S} \to \bigoplus_{M\in T} k_M^*/k_M^{*2} \to \bigoplus_{M\in T} k_M^*/ < k_M^{*2}, \delta_M(m) > .$$

Then there exist infinitely many places $v \notin S_1$ such that

(a) there exists a point $M \in T$ and a place v^M of k_M which is of degree one over k and which splits in K_M ;

(b) for any point $x_v \in \mathbf{A}^1(O_v)$ which meets $\tilde{M} \subset \mathbf{A}^1_{O_S}$ at the place v^M and is transversal to it there, there exists an element $\sigma_v \in W_v(x_v)$ such that $e_v(\mathrm{ev}_{x_v}(b), \sigma_v) \neq 0$.

Proof By assumption, there exists $M \in T$ such that $K_M(\sqrt{\delta_M(b)})/K_M$ is a non-trivial extension. A suitable version of Tchebotarev's theorem (see [Ha94], Prop. 2.2.1) ensures that there exist infinitely many places v of k such that v extends to a place w of K_M of degree one over v, the place w itself being inert in the extension $K_M(\sqrt{\delta_M(b)})/K_M$. Let v be any such place. Let v^M be the trace of the corresponding w on k_M. Because of the degree one condition, this place splits in K_M, as required in (a).

Let $\mathcal{U} = \mathcal{U}_{S_1} = \mathrm{Spec}(O_{S_1}[t][1/R])$. The residue map $H^2(U, \mathbf{Z}/2) \to H^1(k_M, \mathbf{Z}/2)$ induces a residue map $H^2(\mathcal{U}, \mathbf{Z}/2) \to H^1(\tilde{M}, \mathbf{Z}/2) \subset H^1(k_M, \mathbf{Z}/2)$.

Given a point $x_v \in U(k_v)$ which comes from a point $x_v \in \mathbf{A}^1(O_v)$ and which meets $\tilde{M}$ and is transversal to it in v^M, there is a commutative diagram :

$$\begin{array}{ccc} H^2(k_v, \mathbf{Z}/2) & \xrightarrow{\mathrm{inv}_v} & H^1(\mathbf{F}_v, \mathbf{Z}/2) \\ \uparrow x_v^* & & \uparrow \\ H^2(\mathcal{U}, \mathbf{Z}/2) & \xrightarrow{\mathrm{Res}_{\tilde{M}}} & H^1(\tilde{M}, \mathbf{Z}/2) \end{array}$$

Here the horizontal maps are residue maps (the top one giving the invariant of local class field theory, which is an isomorphism), the left vertical map is restriction to $x_v \in U(k_v) \subset k_v$, the right vertical arrow is restriction to the closed point $\mathrm{Spec}(\mathbf{F}_v)$ of $\tilde{M}$ defined by v^M.

Let $i \in \{1,2,3\}$ be such that $R_M(t)$ divides $p_i(t)$. Let Q_j and ε_j be as in lemma 2.2.1. Note that the classes b and ε_j actually belong to $H^1(\mathcal{U}, (\mathbf{Z}/2)^2)$. Let us now compute the image of $< b, \varepsilon_j > \in H^2(\mathcal{U}, \mathbf{Z}/2)$ under the two routes in the above commutative diagram. Applying lemma 2.2.1 and using the fact that the place v^M of k_M is inert in $k_M(\sqrt{\delta_M(b)})$, we find that the image is non-zero. Since $< b, \varepsilon_j >$ goes to $e_v(\mathrm{ev}_{x_v}(b), \varepsilon_j(x_v))$ under the left vertical map in the diagram, we see :

$$e_v(\mathrm{ev}_{x_v}(b), \varepsilon_j(x_v)) \neq 0.$$

In other words, for each x_v satisfying the above transversality condition we have found an element $\sigma_v = \varepsilon_j(x_v) \in W_v(x_v) \subset V_v$ (as a matter of fact the image of an element of order 2 in $E_{x_v}(k_v)$) such that

$$e_v(\mathrm{ev}_{x_v}(b), \sigma_v) \neq 0. \qquad \square$$

We now resume the proof of proposition 2.5.1. The finite set $B_1 \setminus \{1\}$ lies in $\mathfrak{S}$ and does not meet B_0. Condition (D) ensures that the hypothesis of lemma 2.5.2 (with S_1 any set of places containing S) is satisfied by the elements of $B_1 \setminus \{1\}$ which lie in $\mathfrak{S}_0$.

Any element $\xi \in B_1$ which does not lie in $\mathfrak{S}_0$ is the product of an element of U'_S and a certain product of elements

$$A_M = (a_M(\mu^{\deg(R_M)} R_M(t))^{\beta_M}, b_M(\mu^{\deg(R_M)} R_M(t))^{\gamma_M}) \in (O_{S\cup L_\infty}[\mathcal{U}]^*/O_{S\cup L_\infty}[\mathcal{U}]^{*2})^2,$$

with the property that $\eta(\xi) = (\eta_1(\xi), \eta_2(\xi)) \neq 0 \in (\mathbf{Z}/2)^2$. In the group $\mathfrak{S}$, we may rewrite this product as $\xi = (\mu^{\eta_1(\xi)}, \mu^{\eta_2(\xi)}).\xi_1$, where ξ_1 belongs to the finite subgroup of $\mathfrak{S}_S \subset \mathfrak{S}$ spanned by U_S and the elements $(R_M(t)^{\beta_M}, R_M(t)^{\gamma_M})$. Let us consider the set $\mathcal{M}$ of elements $\xi \in \mathfrak{S}_S$ in this finite subgroup with the property that $\eta(\xi) \neq 0$. For any point $M \in T$, we have

$$\delta_M(\xi) = \delta_M((\mu^{\eta_1(\xi)}, \mu^{\eta_2(\xi)})).\delta_M(\xi_1) = \mu^{\gamma_M.\eta_1(\xi)+\beta_M.\eta_2(\xi)}.\delta_M(\xi_1).$$

For any element $\xi \in \mathcal{M}$, there exist at least one closed point $M \in T$ and a pair (β_M, γ_M) such that $\gamma_M.\eta_1(\xi) + \beta_M.\eta_2(\xi) = 1 \in \mathbf{Z}/2$. Now by the very choice of $L_\infty = \{v_\infty\}$ before lemma 2.3.2, for such a point M the element $\delta_M(\xi) = \mu.\delta_M(\xi_1) \in k_M^*/k_M^{*2}$ differs both from 1 and from $\delta_M(m)$.

The hypothesis of lemma 2.5.2 is therefore satisfied by *all* elements in $B_1 \setminus \{1\}$. Applying lemma 2.5.2 to each element of $B_1 \setminus \{1\}$ in turn, we produce a finite set of distinct places of k, away from S, indexed by $B_1 \setminus \{1\}$, such that conditions (a) and (b) of the lemma hold for each $b \in B_1 \setminus \{1\}$ and its associated place. For each such place v, fix $x_v \in O_v$ as in part (b) of the lemma (such points exist), together with some associated $\sigma_v \in W_v(x_v)$. Let $1_v \in \oplus_{v \in S_1} \mathbf{Z}/2$ be the element with all coordinates zero except the one at v. The bilinear pairing

$$B_1 \times (\oplus_{v \in S_1} \mathbf{Z}/2) \to \mathbf{Z}/2$$

sending $(b, 1_v)$ to $e_v(\mathrm{ev}_{x_v}(b), \sigma_v)$ is non-degenerate on the left hand side. By linear algebra, we may find a subset $S_2 \subset S_1$ of order equal to the rank of B_1, such that the induced pairing

$$B_1 \times (\oplus_{v \in S_2} \mathbf{Z}/2) \to \mathbf{Z}/2$$

is non-degenerate on both sides.

We now take L to be $S \cup S_2$, together with the decomposition $L \setminus S = (\cup_{M \in T} L_M)$ coming from the above proof. Note that the order of $L \setminus S$ is precisely equal to the rank of B_1. For any $x \in O_S$ close enough to each x_v for $v \in L$, the corresponding pairing

$$B_1 \times (\oplus_{v \in S_2} \mathbf{Z}/2) \to \mathbf{Z}/2$$

with x in place of x_v is still non-degenerate. Since $B_3 = \varphi_x^{-1}(\oplus_{v \in L \setminus S}(W_v / W_v \cap K_v))$, we find that the pairing $B_1 \times B_3 \to \mathbf{Z}/2$ induced by e_N is non-degenerate.

If we now apply lemma 2.5.3 below to $V = B_1 \oplus B_2$, $V' = B_3$, $V_0 = B_1$ and Ψ the restriction of e_N to $B_1 \oplus B_2 \oplus B_3$, we find that this restriction is non-degenerate. Recall that B_0 was orthogonal to all of N. We thus find that the left kernel of the pairing e_N, which by proposition 1.2.3 is the 2-Selmer group, is precisely B_0, is of rank 3, and is spanned by the points of order 2 and $m(x)$. $\square$

The following lemma replaces the matrix game of [SwD95].

Lemma 2.5.3 *Let Ψ be a symmetric bilinear form on a vector space $V \oplus V'$ over a field F. Let $V_0 \subset V$ be the kernel of the restriction of Ψ to a bilinear form on V. Suppose that the pairing between V_0 and V' given by Ψ is non-degenerate (that is, defines an isomorphism between V' and the dual V_0^* of V_0). Then Ψ is non-degenerate.*

Proof Let $V_1 \subset V$ be the left kernel of the pairing between V and V' given by Ψ, then $V = V_0 \oplus V_1$. We have $V \oplus V' = V_1 \perp (V_0 \oplus V')$ where $\perp$ denotes the orthogonal direct sum. The restriction of Ψ to a bilinear form on V_1 is non-degenerate. The same is true for the restriction of Ψ to a bilinear form on $V_0 \oplus V'$, because Ψ identifies V' and V_0^*, and the restriction of Ψ to V_0 is zero. Hence our lemma is proved. $\square$

The final step

Having chosen $L = \cup_{M \in T} L_M$ as in proposition 2.5.1, for each $M \in T$ and each $v \in L_M$, we choose a point $x_v \in \mathbf{A}^1(O_v)$ such that x_v meets $\tilde{M}$ in v and is transversal there. For a finite place $v \in S$, x_v was defined in proposition 2.1.3. For $v = v_\infty$, we have defined $x_v = 1/\mu$ (see proposition 2.4.2).

We now apply Schinzel's hypothesis (H), in its (H_1) version (due to Serre, see [CT/SwD94], p. 71), to the family of irreducible polynomials R_M and to the family of points $x_v \in k_v$, for $v \in S_{\mathrm{finite}} \cup L \cup \{v_\infty\}$ (recall that all 'small' primes had been included in $S_0 \subset S$ at the beginning of subsection 2.1). This produces an $x \in k$ which satisfies all assumptions of proposition 2.1.3, in particular such that $x \in U_v$ for $v \in S_1$. According to proposition 2.5.1, for any such x the 2-Selmer group $\mathcal{S}(E_x, 2)$ has order 8 and is generated by $m(x)$ and the 2-torsion points of $E_x(k)$. Thus the 2-torsion of the Tate-Shafarevich group of E_x has order at most 2. Assuming that the

Tate-Shafarevich group is finite, we know (Cassels [Cass62]; [Milne86], thm. 6.13, p. 101) that the order of its 2-torsion must be a square. Hence ${}_2\text{Ш}(k, E_x) = 0$, and the element $m(x)$ of the 2-Selmer group must come from $E_x(k)/2$, hence its image in $H^1(k, E_x)$ is trivial : the principal homogeneous space X_x has a k-point. Note that the 2-Selmer group $\mathcal{S}(E_x, 2)$ is of order 8 and coincides with the image of $E_x(k)/2$ under the Kummer map. Thus each E_x is an elliptic curve over k of rank exactly one. Since the principal homogeneous space X_x under E_x has a k-point, it is trivial, i.e. X_x is k-isomorphic to E_x, and $X_x(k)$ is infinite.

This completes the proof of statement (a) in the main Theorem. Since $E_x(k)$ is infinite if $X_x(k)$ is infinite, the proof also shows that under assumptions (1) to (4) and $X(\mathbb{A}_k)^{\mathrm{Br_{vert}}(X)} \neq \emptyset$, the set of k-points x with $E_x(k)$ of rank one is Zariski-dense in $\mathbf{P}^1_k$, hence $E(k)$ is Zariski-dense in the surface E. Since the group $\mathrm{Br_{vert}}(X)/\mathrm{Br}(k)$ is finite, the results on X stated in (b) and (c) of the Theorem are direct consequences of (a) (see [CT/Sk/SwD97b], proof of Theorem 1.1). ∎

Remarks 2.5.4

(i) Under the hypotheses of the theorem, the quotient $E(U)/(2E(U) + {}_2E(U))$ is either zero or is isomorphic to $\mathbf{Z}/2$, the generator having the same image as m in the quotient of $\mathfrak{S}_0$ by the image of ${}_2E(U)$. The rank of $E(k(t))$ is zero in the first case. In the second case, the rank of $E(k(t))$ is one, and $X = X(m)$ and E are birational over $\mathbf{P}^1_k$. In the second case, the main Theorem is therefore essentially obvious. In the first case however, although the generic fibre of $E/\mathbf{P}^1_k$ has rank zero, under the assumptions of the theorem and $X(\mathbb{A}_k)^{\mathrm{Br_{vert}}(X)} \neq \emptyset$ (e.g. $X(k) \neq \emptyset$) we find that the set of k-points x such that the specialized curve E_x has rank at least one is Zariski-dense in $\mathbf{P}^1_k$.

(ii) Under the hypotheses of the theorem, when $X(k) \neq \emptyset$, we conclude that the rational points on both surfaces E and X are Zariski dense. This is worth pointing out, since some of our examples (see section 3) include $K3$-surfaces, for which little was known in such respect.

(iii) Suppose we start with $E/\mathbf{P}^1_k$ as in the Introduction. There is an associated map $\delta : \mathfrak{S}_0 \to \oplus_{M\in T} k^*_M/k^{*2}_M$. We know (lemma 2.2.1) that the kernel $\mathrm{Ker}(\delta)$ is a finite abelian group of exponent 2. This group is of order at least 4, since it contains the image of ${}_2E(U)$ under the Kummer map. One may wonder whether one may find $m \in \mathfrak{S}_0$ such that the hypotheses of the main theorem are fulfilled. A necessary condition is that the order of $\mathrm{Ker}(\delta)$ be exactly 8. Indeed, if the order is 4, then Hypothesis (1) in the main Theorem cannot be fulfilled, and if the order is at least 16, then (2) cannot be fulfilled.

(iv) Instead of hypothesis (D), let us make the stronger assumption :

(D_0) *The kernel of the composite map*

$$\mathfrak{S} \to \bigoplus_{M\in T} k^*_M/k^{*2}_M \to \bigoplus_{M\in T} k^*_M/ < k^{*2}_M, \delta_M(m) >$$

is generated by m and by the image of the 2-torsion points of $E(U)$ under the Kummer map.

Then, as the reader will check, we can take $L_\infty = \emptyset$ in the above proof. We have the exact sequence

$$0 \to \mathfrak{S}_0 \to \mathfrak{S} \xrightarrow{\eta} (\mathbf{Z}/2)^2$$

with η as in the beginning of subsection 2.2. Thus when all R_M's are of even degree, the two conditions (D) and (D_0) agree, and there is no need for L_∞.

(v) Under (D_0), the x's produced in the proof are integral away from the set S. One can actually go further. We shall here ignore the difficulties produced by the real places, assume that k is totally imaginary and ignore approximation at the complex places. Then there is no need to make the projective transformation mentioned at the beginning of subsection 2.1. As pointed out after lemma 2.1.1, the image of each $\alpha_M(t)$ under the map $\mathrm{Br}(k(t)) \to \mathrm{Br}(k(X))$ lies in the subgroup $\mathrm{Br}(X_{\mathrm{aff}})$, where X_{aff} denotes the inverse image of $\mathbf{A}^1_k$ under $X \to \mathbf{P}^1_k$. We can produce a finite set S_0 as in lemma 2.1.2, with the additional condition that the α_M lie in the Brauer group of an integral model of Y over O_{S_0}. Assume that there is no Brauer-Manin obstruction to the existence of an integral point (in an obvious sense) on Y. Then we have the same conclusion as in lemma 2.1.2, with the additional property that each x_v lies in O_v for $v \notin S_0$. Under (D_0), we ultimately produce an element $x \in k$ integral away from S_0 and such that $X_x(k) \neq \emptyset$.

(vi) It is quite likely that the theorem goes through if we replace (D) by the assumption :

(D_1) *The kernel of the composite map*

$$\mathfrak{S}_0 \xrightarrow{\delta} \bigoplus_{M \in T} k_M^*/k_M^{*2} \to \bigoplus_{M \in T} k_M^*/ < k_M^{*2}, \delta_M(m) >$$

is generated by m *and by the image of* $E(U)$ *under the Kummer map, and* m *does not belong to the image of the whole group* $E(U)$ *under the Kummer map.*

3. Surfaces to which the theorem applies

3.1 Equations

The surfaces to which the theorem applies can be given by more symmetrical looking systems of equations. Let k be a field, $\mathrm{char}(k) \neq 2$. Given $a_i(t)$ and $b_i(t)$ in $k[t]$, consider the surface $W \subset \mathbf{P}^3_k \times_k \mathbf{A}^1_k$ defined by the system of equations

$$\sum_{i=0}^{3} a_i(t) x_i^2 = 0, \quad \sum_{i=0}^{3} b_i(t) x_i^2 = 0.$$

Here $\mathbf{A}^1_k = \mathrm{Spec}(k[t])$, the a_i and b_i belong to $k[t]$, and (x_0, x_1, x_2, x_3) are homogeneous coordinates for $\mathbf{P}^3_k$.

We shall make the following 'generic' assumptions :

(i) deg a_i − deg b_i does not depend on i, deg a_i − deg a_j is even for all i, j, and for $i \neq j$ the difference $\Delta_{ij}(t) = a_i(t)b_j(t) - a_j(t)b_i(t)$ has degree equal to the degree of $a_i b_j$ (equal to the degree of $a_j b_i$ by the previous assumptions).

(ii) The product $R(t) = \prod_{i<j} \Delta_{ij}(t)$ is separable.

There then exists a model $\pi : X \to \mathbf{P}^1_k$ of $W/\mathbf{A}^1_k$ such that X/k is smooth and proper, the fibre at infinity is smooth (this is guaranteed by condition (i)), the singular fibres of π correspond to the zeros of $\prod_{i<j} \Delta_{ij}(t)$, and each geometric singular fibre is the union of two smooth conics in $\mathbf{P}^3$ which are not coplanar and which meet in two points.

The number of geometric singular fibres is given by

$$\sum_{i<j} \deg(\Delta_{ij}) = (3/2) \sum_i (\deg(a_i) + \deg(b_i)),$$

which is always divisible by 6.

Note that we have identically

$$\Delta_{01}(t)\Delta_{23}(t) + \Delta_{02}(t)\Delta_{31}(t) + \Delta_{03}(t)\Delta_{12}(t) = 0.$$

The system of equations above is equivalent (over $R(t) \neq 0$) to the system

$$\begin{aligned}\Delta_{01}(t)x_0^2 + \Delta_{21}(t)x_2^2 + \Delta_{31}(t)x_3^2 = 0\\ \Delta_{02}(t)x_0^2 + \Delta_{12}(t)x_1^2 + \Delta_{32}(t)x_3^2 = 0\\ \Delta_{03}(t)x_0^2 + \Delta_{13}(t)x_1^2 + \Delta_{23}(t)x_2^2 = 0,\end{aligned}$$

where any one of the three equations may be deduced from the other two. The jacobian of this curve may be written in the standard form

$$Y^2 = (X - c_1(t))(X - c_2(t))(X - c_3(t)),$$

with

$$c_1 - c_2 = \Delta_{12}\Delta_{30},\ c_2 - c_3 = \Delta_{23}\Delta_{10},\ c_3 - c_1 = \Delta_{31}\Delta_{20}.$$

The relatively minimal fibration $X/\mathbf{P}^1_k$ associated to the surface we started with, in terms of the introduction of this paper, corresponds to the element $m(t) = (m_1(t), m_2(t), m_3(t))$ with

$$m_1 = -\Delta_{12}\Delta_{13},\ m_2 = -\Delta_{21}\Delta_{23},\ m_3 = -\Delta_{31}\Delta_{32}\ .$$

The hypotheses on the polynomials a_i and b_i ensure that all the hypotheses of the introduction are satisfied; in particular m lies in $\mathfrak{S}_0$.

Conversely, provided the coordinates are general enough, one may go from the equations given in the introduction to a system of two simultaneously diagonal quadratic equations as the one we started with here. The details will be left to the reader.

Deciding whether condition (3) (= condition (D)) in the Theorem holds reduces to the following explicit computation. Let T be the set of monic irreducible divisors of $R(t)$. For each monic irreducible factor $R_M(t)$ of $R(t)$, with residue field $k_M = k[t]/R_M(t)$, one computes $\delta_M(m) \in k_M^*/k_M^{*2}$ according to the recipe given in the introduction. If e.g. R_M divides Δ_{01}, then $\delta_M(m)$ is given by the class of $-\Delta_{21}\Delta_{31}$ modulo R_M, as is clear from the system of equations above. As for $\mathfrak{S}_0 \subset (k(t)^*/k(t)^{*2})^3$, it consists of classes $(a\prod_{M\in T} R_M^{r_M}, b\prod_{M\in T} R_M^{s_M}, c\prod_{M\in T} R_M^{t_M})$ with $a, b, c \in k^*/k^{*2}$ such that $abc = 1$, and with r_M, s_M, t_M each equal to 0 or 1, satisfying the conditions : $r_M + s_M + t_M$ is even; if R_M divides $c_2 - c_3 = \Delta_{23}\Delta_{10}$, then $r_M = 0$, if R_M divides $c_3 - c_1 = \Delta_{31}\Delta_{20}$, then $s_M = 0$, if R_M divides $c_1 - c_2 = \Delta_{12}\Delta_{30}$, then $t_M = 0$; finally, each of $\sum_{M\in T} r_M \deg(R_M), \sum_{M\in T} s_M \deg(R_M), \sum_{M\in T} t_M \deg(R_M)$ is even. One computes the map δ on $\mathfrak{S}_0$ as we did above for $\delta(m)$, or by using the recipe given in the proof of lemma 2.2.1. The composite map

$$\mathfrak{S}_0 \xrightarrow{\delta} \bigoplus_{M\in T} k_M^*/k_M^{*2} \to \bigoplus_{M\in T} k_M^*/ < k_M^{*2}, \delta_M(m) >$$

is now completely explicit. One knows that its kernel is finite (lemma 2.2.1). Condition (D) holds if and only if this kernel is of rank 3, generated by the classes of m and of the elements

$$((c_1 - c_2)(c_1 - c_3), (c_1 - c_2), (c_1 - c_3)) = (\Delta_{12}\Delta_{30}\Delta_{13}\Delta_{20}, \Delta_{12}\Delta_{30}, \Delta_{13}\Delta_{20})$$

and

$$(c_2 - c_1, (c_2 - c_1)(c_2 - c_3), (c_2 - c_3)) = (-\Delta_{12}\Delta_{30}, -\Delta_{12}\Delta_{30}\Delta_{23}\Delta_{10}, \Delta_{23}\Delta_{10}).$$

3.2 The Egloffstein case

In [SwD95], one starts with a smooth complete intersection of two quadrics $W \subset \mathbf{P}^4_k$ given by a system of equations

$$\sum_{i=0}^{4} a_i x_i^2 = 0, \quad \sum_{i=0}^{4} b_i x_i^2 = 0,$$

where all a_i, b_i belong to k, and $a_i b_j - a_j b_i \neq 0$ for $i \neq j$. This is a Del Pezzo surface of degree 4. One may transform this surface into a pencil of curves of genus one by considering the pencil $x_4 = t x_0$. The new system now reads

$$\sum_{i=1}^{3} a_i x_i^2 + (a_0 + t^2 a_4) x_0^2 = 0,$$

$$\sum_{i=1}^{3} b_i x_i^2 + (b_0 + t^2 b_4) x_0^2 = 0$$

in $\mathbf{A}^1_k \times \mathbf{P}^3_k$, which one may extend to a pencil of curves of genus one $\pi : X \to \mathbf{P}^1_k$ over the projective line. One readily checks that the number of singular geometric fibres is 6.

Proposition 3.2.1 *Let $\pi : X \to \mathbf{P}^1_k$ be as above.*

(1) If none of the $-d_{i0}d_{i4}$ is a square in k, then the vertical Brauer group of X (with respect to π) is reduced to the image of $\mathrm{Br}(k)$.

(2) If moreover the three classes $-d_{12}d_{13}, -d_{21}d_{23}, \prod_{i\neq 4} d_{4i}$ are independent in k^*/k^{*2}, then condition (D) *holds for π.*

(3) Assume that k is a number field. Assume that the various indepence hypotheses above are fulfilled. Assume Schinzel's hypothesis, and assume that the Tate-Shafarevich group of elliptic curves over k is finite. Then the Hasse principle holds for the intersection of two quadrics

$$\sum_{i=0}^{4} a_i x_i^2 = 0, \quad \sum_{i=0}^{4} b_i x_i^2 = 0.$$

Proof In the above notation we have $\Delta_{ij}(t) = d_{ij}$ if i and j are in $\{1,2,3\}$, and by assumption $\Delta_{i0}(t) = d_{i4}t^2 + d_{i0}$ is irreducible for $i \in \{1,2,3\}$. The closed points $M \in \mathbf{P}^1_K$ such that X_M is singular are given by $\Delta_{i0}(t) = 0$ for $i \in \{1,2,3\}$. Let us call these points M_1, M_2, M_3. Their residue fields are $k_i = k(\sqrt{\beta_i})$ where β_i is the class of $-d_{i4}d_{i0}$ in k^*/k^{*2}. The class $m = (m_1, m_2) \in (k(t)^*/k(t)^{*2})^2$ is given by the constants $(\alpha_1, \alpha_2) \in (k^*/k^{*2})^2$, where $\alpha_i = -d_{ij}d_{ir}$ if $\{i,j,r\} = \{1,2,3\}$.

Let $A \in \mathrm{Br}_{\mathrm{vert}}(X) \subset \mathrm{Br}(k(X))$. Write $A = \pi^*(a)$ with $a \in \mathrm{Br}(k(t))$. The class a can have non-trivial residues only at the points M_i ($i \in \{1,2,3\}$). Moreover, at the point M_i, its residue is either trivial or equal to the image of α_i. The quaternion algebra $(\alpha_i, \Delta_{i0}(t))$ has residue $\alpha_i \in k_i^*/k_i^{*2} = H^1(k_i, \mathbf{Z}/2)$ at M_i and has residue zero at all other closed points of $\mathbf{P}^1_k$. By the Faddeev exact sequence, the element a belongs to the subgroup of $\mathrm{Br}(k(t))$ spanned by $\mathrm{Br}(k)$ and the quaternion algebras $(\alpha_i, \Delta_{i0}(t))$. But a glance at the equations defining X shows that each of these quaternion algebras becomes trivial over $k(X)$. This proves (1).

Since each $\Delta_{i0}(t)$ is irreducible and of even degree, the group $\mathfrak{S} \subset ((k(t)^*/k(t)^{*2}))^2$ coincides with the group $\mathfrak{S}_0$. One easily checks that $\mathfrak{S}_0$ coincides with the subgroup spanned by $(k^*/k^{*2})^2$, the image $\partial({}_2E(k(t)))$ of the points of order 2 under the Kummer map and the class $(\Delta_{30}(t), \Delta_{30}(t))$.

Using the explicit description of the map

$$\delta : \mathfrak{S}_0 \to \oplus_{i=1}^{3} k_i^*/k_i^{*2}$$

given by lemma 2.2.1, one obtains the following results. For $(c_1, c_2) \in (k^*/k^{*2})^2$, letting $c_3 = c_1c_2 \in k^*/k^{*2}$. Then $\delta_{M_i}((c_1, c_2)) = c_i \in k_i^*/k_i^{*2}$. In particular, $\delta_{M_i}(m) = \alpha_i \in k_i^*/k_i^{*2}$.

Since δ vanishes on the image of $E(k(t))$ under the Kummer map, to describe δ it only remains to compute $\delta((\Delta_{30}(t), \Delta_{30}(t)))$. One finds :

$$\delta_{M_1}(\Delta_{30}(t), \Delta_{30}(t)) = -d_{13}d_{04}d_{14} \in k_1^*/k_1^{*2},$$

$$\delta_{M_2}(\Delta_{30}(t), \Delta_{30}(t)) = -d_{23}d_{04}d_{24} \in k_2^*/k_2^{*2},$$

$$\delta_{M_3}(\Delta_{30}(t), \Delta_{30}(t)) = -d_{13}d_{32}d_{04}d_{34} \in k_3^*/k_3^{*2}.$$

Let $\rho_1 = -d_{13}d_{04}d_{14} \in k^*/k^{*2}$, $\rho_2 = -d_{23}d_{04}d_{24} \in k^*/k^{*2}$ and $\rho_3 = -d_{13}d_{32}d_{04}d_{34} \in k_3^*/k_3^{*2} \in k^*/k^{*2}$. Let $\rho = \rho_1.\rho_2.\rho_3 = \prod_{j\neq 4} d_{4j} \in k^*/k^{*2}$.

Let $\varepsilon \in \{0, 1\}$, and $c, d \in k^*/k^{*2}$. If the class $((\Delta_{30}(t), \Delta_{30}(t)))^{\varepsilon}.(c, d)$ is in the kernel of the composite map

$$\mathfrak{S}_0 \xrightarrow{\delta} \bigoplus_{M\in T} k_M^*/k_M^{*2} \to \bigoplus_{M\in T} k_M^*/ < k_M^{*2}, \delta_M(m) >,$$

then for $i \in \{1, 2, 3\}$ there exist $\varepsilon_i \in \{0, 1\}$ such that $\rho_1^{\varepsilon}.c = \alpha_1^{\varepsilon_1}$, $\rho_2^{\varepsilon}.d = \alpha_2^{\varepsilon_2}$, $\rho_3^{\varepsilon}.c.d = \alpha_3^{\varepsilon_3} = (\alpha_1.\alpha_2)^{\varepsilon_3}$. Elimination yields $\alpha_1^{\varepsilon_1-\varepsilon_3}.\alpha_2^{\varepsilon_2-\varepsilon_3}.\rho^{\varepsilon} = 1$. The assumptions in 1) now imply $\varepsilon = 0$ and $\varepsilon_1 = \varepsilon_2 = \varepsilon_3$, which shows that hypothesis (D) is fulfilled, and completes the proof of (2).

Statement (3) now follows from the main Theorem. □

Remarks 3.2.2

(1) Let k be a number field. For $a_0, \dots, a_4, b_0, \dots, b_4$ in a Hilbert subset of affine space $\mathbf{A}^{10}(k)$, all hypotheses above are fulfilled. Indeed, $K = k(A_0, \dots, A_4, B_0, \dots, B_4)$ be the function field of $\mathbf{A}_k^{10}$ and let $D_{ij} = A_iB_j - A_jB_i$. Looking at divisors, it is an easy matter to check that the elements $-D_{12}D_{13}, D_{21}D_{23}, \prod_{i\neq 4} D_{4i}$ are independent in K^*/K^{*2}. Similarly, if $\{i, j, r\}$ is a permutation of $\{1, 2, 3\}$, then for each $i = 1, 2, 3$, the classes $-D_{i0}D_{i4}, -D_{ij}D_{ir}$ are independent in K^*/K^{*2}. The assertion now follows from Hilbert's irreducibility theorem. Thus for 'general' $a_0, \dots, a_4, b_0, \dots, b_4$, in the number field k, provided the two mentioned conjectures hold, the Hasse principle holds for the corresponding intersection of two quadrics.

(2) Conditions (1) and (2) in the previous proposition are a priori weaker than the original condition (D) (p. 290 of [SwD95]).

(3) Note that there are 10 different obvious ways in which one may transform the original surface W into a pencil of curves of genus one, namely one may set $x_i = tx_j$ for any pair $(i, j), i \neq j$. This leads to 10 versions of condition (D). We have examples where none of these 10 conditions holds, and where nevertheless the quotient $\mathrm{Br}(W)/\mathrm{Br}(k) = 0$. Standard conjectures on rational surfaces suggest that the Hasse principle holds for such a W. However the main theorems of [SwD95] and of the present paper are not enough to prove this. This also indicates that condition (D) is not a necessary condition for the Hasse principle to hold.

3.3 Geometry

Let us consider the surface $X/\mathbf{P}^1$ over the algebraic closure of k. Let T be the set of points of $\mathbf{P}^1$ with singular fibres, and let r be its order. The topological Euler-Poincaré characteristic $e(X)$ of X is given by the formula ([BPV84], Prop. (11.4) p. 97) :

$$e(X) = e(X_\eta)e(\mathbf{P}^1) + \sum_{M\in T} (e(X_M) - e(X_\eta)),$$

where X_η denotes the geometric generic fibre, a curve of genus one, and X_M denotes the fibre at M. We have $e(\mathbf{P}^1) = 2$, $e(X_\eta) = 0$, and $e(X_M) = 2$. Thus $e(X) = 2r$.

(Note : the formula in [BPV84], p. 162 also covers the case of multiple fibres. This is useful when describing 'wild' cases, as in [CT/Sk/SwD97a].)

Let $\chi(X) = \chi(O_X)$ denote the Euler-Poincaré characteristic of the structural sheaf of a proper variety X. Since $p : X \to \mathbf{P}^1$ is a smooth surface fibred into curves of genus one, and has no multiple fibre, the canonical bundle K_X is of the shape $K_X = p^*(L)$ with L a line bundle of degree $\chi(X) - 2\chi(\mathbf{P}^1) = \chi(X) - 2$ on $\mathbf{P}^1$ ([BPV84], Corollary (12.3) p. 162). In particular, $c_1^2(X) = (K_X.K_X) = 0$. From the formula $c_1^2(X) + e(X) = 12\chi(X)$, and from the above result, we deduce

$$r = 6\chi(X).$$

Assume $\chi(X) = 1$, i.e. $r = 6$. We have $K_X = O_X(-X_P)$, where X_P denote a fibre. Thus $2K_X$ has no section and in particular $H^0(X, K_X) = 0$. The vector space $H^2(X, O_X)$ is dual to $H^0(X, K_X)$. Hence the geometric genus $p_g = \dim(H^2(X, O_X))$ vanishes. From $\chi(X) = 1$ we conclude $H^1(X, O_X) = 0$. Castelnuovo's criterion now ensures that the surface is rational.

In terms of simultaneously diagonal equations as above, the possibilities for the degrees of the a_i's and b_i's are ((0,0,0,0) ;(1,1,1,1)) which gives a surface obviously birational to a quadric, or ((0,0,0,2) ;(0,0,0,2)) which is indeed a generalisation of the case considered in [SwD95] and discussed in subsection 3.2 above.

Assume $\chi(X) = 2$, i.e. $r = 12$. Then $K_X = O_X$. Thus $\dim(H^2(X, O_X)) = 1$, hence $\dim(H^1(X, O_X)) = 0$. In this case, X is a $K3$-surface.

In terms of simultaneously diagonal equations as above, the possibilities for the degrees are : ((0,0,0,4) ;(0,0,0,4)), ((0,0,2,2) ;(0,0,2,2)), ((1,1,1,1) ;(1,1,1,1)), ((0,0,0,2) ;(1,1,1,3)), ((0,0,0,0) ;(2,2,2,2)).

Let us discuss the case $((1,1,1,1);(1,1,1,1))$ some more. Let us write

$$a_i(t) = \alpha_{i0}t + \alpha_{i1}, \ \ b_i(t) = \alpha_{i2}t + \alpha_{i3}.$$

In the product $\mathbf{P}^1_k \times \mathbf{P}^3_k$ with bihomogeneous coordinates $(\lambda, \mu; x_0, x_1, x_2, x_3)$, the original surface X is given by the system of equations

$$\sum_{i=0}^{3}(\alpha_{i0}\lambda + \alpha_{i1}\mu)x_i^2 = 0, \ \ \sum_{i=0}^{3}(\alpha_{i2}\lambda + \alpha_{i3}\mu)x_i^2 = 0,$$

projection to $\mathbf{P}^1$ yielding the original fibration $\pi : X \to \mathbf{P}^1$. Let $\mathbf{x} = (x_0, x_1, x_2, x_3)$. For $j = 0, 1, 2, 3$, let

$$A_j(\mathbf{x}) = \alpha_{0j}x_0^2 + \alpha_{1j}x_1^2 + \alpha_{2j}x_2^2 + \alpha_{3j}x_3^2.$$

Then we have

$$\lambda A_0(\mathbf{x}) + \mu A_1(\mathbf{x}) = \lambda A_2(\mathbf{x}) + \mu A_3(\mathbf{x}) = 0$$

and the surface X is isomorphic to the quartic surface $Z \subset \mathbf{P}^3_k$ given by the homogeneous equation

$$A_0(\mathbf{x})A_3(\mathbf{x}) - A_1(\mathbf{x})A_2(\mathbf{x}) = 0.$$

This is also isomorphic to the surface X' given in the product $\mathbf{P}^1_k \times \mathbf{P}^3_k$, with bihomogeneous coordinates $(\sigma, \tau; x_0, x_1, x_2, x_3)$, by the equations :

$$\sigma A_0(\mathbf{x}) + \tau A_2(\mathbf{x}) = \sigma A_1(\mathbf{x}) + \tau A_3(\mathbf{x}) = 0.$$

Thus on Z there is a second fibration into curves of genus one, given by the projection $X' \to \mathbf{P}^1$.

However, there is a natural correspondence between the singular fibres of the two pencils. Geometrically, this is given as follows. Let $C_1 \subset X$ and $C_2 \subset X$ be the two smooth conics which are the components of a singular fibre of the first pencil. Viewed in $Z \subset \mathbf{P}^3$, these curves are still conics. Let $\Pi_i \subset \mathbf{P}^3$ be the plane containing C_i, and let C_i' be the intersection of Π_i and Z residual to C_i. This is a plane conic. An easy calculation with intersection numbers shows that C_i' does not meet the general fibre of the second pencil. So it is a component of some singular fibre of that pencil, and it is now obvious that this singular fibre is $C_1' \cup C_2'$. Algebraically, $(\lambda, \mu) \in k^2 \setminus (0,0)$ corresponds to a singular fibre if and only if there exists $(\sigma, \tau) \in k^2 \setminus (0,0)$ such that

$$\sigma(\lambda A_0(\mathbf{x}) + \mu A_1(\mathbf{x})) + \tau(\lambda A_2(\mathbf{x}) + \mu A_3(\mathbf{x}))$$

is a quadratic form of rank 2 in $\mathbf{x} = (x_0, x_1, x_2, x_3)$; and this condition has an obvious symmetry.

4. Condition (D), Néron models and the Brauer group

In this section we establish a connection between Condition (D) and the structure of the Brauer group of the surface X in the main Theorem. We also give a general definition of the group $\mathfrak{S}$ as 'the geometric Selmer group', as well as an intrinsic interpretation of the maps δ_M.

In this whole section, we let C be an excellent integral Dedekind scheme (= noetherian, normal, of dimension one). We assume that the residue fields at closed points are perfect. (For the purposes of the present paper, the reader may assume C to be a smooth integral curve over a field of characteristic zero, or a localisation of such a scheme.) We let K be the fraction field of C. For a closed point $M \in C$, we denote by O_M the local ring at M, by k_M its residue field, by O_M^h, resp. O_M^{sh}, the henselisation, resp. the strict henselisation of O_M, and we denote by K_M^h, resp. K_M^{sh}, the fraction fields of these rings. We denote by $i_M : \mathrm{Spec}(k_M) \to C$ the natural closed immersion of a closed point M into C, and by $j_K : \mathrm{Spec}(K) \to C$ the natural map of the generic point of C into C.

Given an elliptic curve J_K/K, there exists a unique proper, flat, relatively minimal model J^c/C with J^c integral and regular ([Sha66], [BLR90]). The open set of smooth points for the projection J^c/C is the Néron minimal model J/C of J_K/K. A key rôle in the discussion to follow will be played by the étale cohomology group $H^1(C, J)$.

4.1 Geometric incarnation of $H^1(C, J)$: unramified torsors

The following lemma is well known.

Lemma 4.1.1 *Let X be a regular integral scheme, proper and flat over C, such that the generic fibre of the structural morphism $\pi : X \to C$ is a curve of genus 1. Let K be the function field of C, and let J_K be the jacobian of the generic fibre X_K of π. Assume that the residual characteristics are coprime with the multiplicities of the irreducible components of π. Then the following conditions are equivalent :*

(1) there are no multiple fibres (that is the g.c.d. of the multiplicities of the irreducible components is 1);

(2) for every closed point $M \in C$, the fibre X_M contains an irreducible component of multiplicity 1;

(3) for every closed point $M \in C$ the class $[X_K] \in H^1(K, J_K)$ goes to zero under the restriction to K_M^{sh}.

Proof The question is local for the étale topology on C. One thus reduces to the case where C is the spectrum of a strictly henselian discrete valuation ring. Condition (3) is then equivalent to $X_K(K) \neq \emptyset$, itself equivalent to the existence of a section for $\pi : X \to C$. This section meets the special fibre in a component of multiplicity one. Thus (3) implies (2) which trivially implies (1). If (1) is satisfied, then X_K possesses a zero-cycle of degree one ([BLR90], Corollary 9.1.9), hence a K-point since it is a curve of genus one. Thus (3) holds. $\square$

These conditions depend only on the generic fibre X_K. Condition (3) is the definition of an unramified torsor ([BLR90], p.158). Let $J \to C$ be the Néron model of J_K. By [BLR90], 6.5.3, under this assumption there exists a local Néron model Z_{O_M} of $Z_K = X_K$ (that is, smooth, separated, of finite type, and satisfying the Néron universal mapping property) which can be built by descent from $J_{K^{sh}_M}$. Moreover, Z_{O_M} is a torsor under J_{O_M} ([BLR90], loc.cit.). These local models glue together into a (unique) global Néron model Z/C ([BLR90], 1.4.1) which is a torsor under J/C. To Z one can canonically attach the proper regular relatively minimal model X, also denoted by Z^c. This model is unique [Sha66]. From this model X one can then recover Z as the maximal subscheme of X on which $X \to C$ is smooth.

Thus the unramified torsors are classified by the group

$$H^1(C,J) \xrightarrow{\simeq} H^1_{nr}(K,J) := [\mathrm{Ker}:\ H^1(K,J_K) \longrightarrow \prod_{M\in C} H^1(K^{sh}_M, J_K)]$$

(here and below, the notation $M \in C$ is shorthand for M running through the closed points of C). That the map $H^1(C,J) \to H^1(K,J_K)$ is injective is a consequence of the Néron property. Thus the group $H^1(C,J)$ is a kind of 'geometric' Tate-Shafarevich group for J (cf. [Gr68], III, section 4).

4.2 Geometric Selmer groups

Let J/C and J_K/K be as above. Let $n > 0$ be an integer invertible on C. From the Kummer sequence

$$0 \to {}_nJ_K \to J_K \xrightarrow{n} J_K \to 0$$

we deduce the exact sequence

$$0 \to J(K)/n \to H^1(K, {}_nJ) \to {}_nH^1(K,J) \to 0.$$

For each closed point $M \in C$, we have a similar exact sequence

$$0 \to J(K^{sh}_M)/n \to H^1(K^{sh}_M, {}_nJ) \to {}_nH^1(K^{sh}_M, J) \to 0.$$

Definition 4.2.1 *The 'geometric' n-Selmer group of J/C, denoted $\mathfrak{S}(J,n)$, is the group of elements $\alpha \in H^1(K, {}_nJ)$ such that for each closed point $M \in C$, the image of α in $H^1(K^{sh}_M, {}_nJ)$ lies in the image of $J(K^{sh}_M)/n$.*

For each $M \in C$, let us introduce the group F_M of connected components of the (special fibre of the) Néron model of $J_{O^{sh}_M}$. This is a finite module under the Galois group $\mathrm{Gal}(k^{\mathrm{sep}}_M/k_M)$ and is zero for almost all $M \in C$. We have the exact sequence of $\mathrm{Gal}(k^{\mathrm{sep}}_M/k_M)$-modules

$$0 \to J^0(O^{sh}_M) \to J(O^{sh}_M) \to F_M \to 0,$$

where J^0 denotes the connected component of identity in the Néron model. The group $J^0(O^{sh}_M)$ is divisible by n ([BLR90], subsection 7.3) hence we have $J(O^{sh}_M)/n \xrightarrow{\simeq} F_M/n$. On the other hand, the basic property of the Néron minimal model implies $J(O^{sh}_M)/n \xrightarrow{\simeq} J(K^{sh}_M)/n$. We thus have $J(K^{sh}_M)/n \simeq F_M/n$.

Proposition 4.2.2 *(a) The geometric n-Selmer group $\mathfrak{S}(J,n) \subset H^1(K, {}_nJ)$ is the inverse image in $H^1(K, {}_nJ)$ of ${}_nH^1(C,J) \subset {}_nH^1(K,J)$: it fits into the exact sequence*

$$0 \to J(K)/n \to \mathfrak{S}(J,n) \to {}_nH^1(C,J) \to 0.$$

(b) There is a natural exact sequence

$$0 \to H^1(C, {}_nJ) \to \mathfrak{S}(J,n) \to \oplus_{M \in C} F_M/nF_M.$$

(c) Assume $\mathrm{Pic}(C) = 0$ *and assume that ${}_nJ_K/K$ is isomorphic to the constant group scheme $(\mathbf{Z}/n)^2_K$. Then the previous sequence may be rewritten as :*

$$0 \to (k[C]^*/k[C]^{*2})^2 \to \mathfrak{S}(J,n) \to \oplus_{M \in C} F_M/nF_M \to 0.$$

Proof We claim that there exists a commutative diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & H^1(C, {}_nJ) & & {}_nH^1(C,J) & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J_K(K)/n & \longrightarrow & H^1(K, {}_nJ_K) & \longrightarrow & {}_nH^1(K, J_K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{M \in C} J_K(K_M^{sh})/n & \longrightarrow & \bigoplus_{M \in C} H^1(K_M^{sh}, {}_nJ_{K_M^{sh}}) & \longrightarrow & \bigoplus_{M \in C} {}_nH^1(K_M^{sh}, J_{K_M^{sh}}) & \longrightarrow & 0
\end{array}$$

with exact rows and columns. The horizontal exact sequence has already been discussed, and so has been the bottom one. A class in $H^1(K, {}_nJ)$ comes from a class in $H^1(U, {}_nJ_U)$ for a non-empty open set $U \subset C$. Now $H^1(O_M^{sh}, {}_nJ) = 0$ for any M, for trivial reasons, hence the diagonal map does send the middle exact sequence to the bottom exact sequence (we may write sums rather than products).

The right vertical exact sequence comes from the isomorphism

$$H^1(C,J) \xrightarrow{\simeq} \mathrm{Ker} : \ [H^1(K, J_K) \longrightarrow \prod_{M \in C} H^1(K_M^{sh}, J_K)]$$

mentioned in subsection 4.1. This much of the diagram is enough to give the exact sequence in (a), which, it should be noted, is a 'geometric' analogue of the classical sequence (over number fields) involving the n-Selmer group and the n-torsion of the Tate-Shafarevich group.

Given any Galois-module $\mathcal{F}$ over K, we have the general exact sequence :

$$0 \to H^1(C, j_{K*}\mathcal{F}) \to H^1(K, \mathcal{F}) \to \prod_{M \in C} H^1(K_M^{sh}, \mathcal{F}).$$

Applying this to the module ${}_nJ_K$, we get the exact sequence

$$0 \to H^1(C, j_{K*}({}_nJ_K)) \to H^1(K, {}_nJ_K) \to \prod_{M \in C} H^1(K_M^{sh}, {}_nJ_K),$$

where for reasons as above the right hand side map lands in the direct sum. By the Néron property we have the isomorphism of étale sheaves $J \xrightarrow{\simeq} j_{K*}J_K$ over C, hence also the isomorphism ${}_nJ \xrightarrow{\simeq} j_{K*}({}_nJ_K)$. We thus find that the middle vertical sequence in the diagram is exact. As discussed before the proposition, we have $J(K_M^{sh})/n \simeq F_M/n$ for all $M \in C$. A chase through the diagram now gives the exact sequence in (b).

If ${}_nJ_K/K$ is isomorphic to the constant group scheme $(\mathbf{Z}/n)^2_K$ over K, then

$$ {}_nJ \xrightarrow{\simeq} j_{K*}({}_nJ_K) \simeq j_{K*}((\mathbf{Z}/n)^2_K) = (\mathbf{Z}/n)^2_C. $$

Thus $H^1(C, {}_nJ) = H^1(C, (\mathbf{Z}/n)^2_C)$. That ${}_nJ_K/K$ is isomorphic to the constant group scheme $(\mathbf{Z}/n)^2_K$ over K also implies, via the Weil pairing, that the Galois module of n-th roots of unity $\mu_{n,K}$ is trivial, i.e. isomorphic to $(\mathbf{Z}/n)_K$. If moreover $\mathrm{Pic}(C) = 0$, then the Kummer sequence now yields $(k[C]^*/k[C]^{*n})^2 \simeq H^1(C, {}_nJ)$. In order to prove (c), it only remains to show the surjectivity of the map $\mathfrak{S}(J, n) \to \oplus_{M\in C} F_M/nF_M$. But this follows from the surjectivity of the map $H^1(K, {}_nJ_K) \to \oplus_{M\in C} H^1(K_M^{sh}, {}_nJ_{K_M^{sh}})$, which translates as the valuation map $(K^*/K^{*n})^2 \to \oplus_{M\in C}(\mathbf{Z}/n)^2$, map which is surjective since $\mathrm{Pic}(C) = 0$. □

4.3 Divisors on the special fibres of the Néron model and the map δ

In this subsection, we collect results from Raynaud [Ray70], Artin [Art86], Bosch, Lütkebohmert and Raynaud ([BLR90], subsections 9.5 and 9.6).

Let C be an integral Dedekind scheme whose residue fields are perfect. Let K be the fraction field of K. Let $\pi : X \to C$ be a relatively minimal, proper and flat morphism, with X integral and regular. Assume that the generic fibre is a smooth, geometrically integral curve of genus one over the fraction field K of R, that for each $M \in C$ the multiplicities of the components of the geometric special fibre at M are prime to the characteristic of k, and that the greatest common divisor of these multiplicities is one. Let $J_K = \underline{\mathrm{Pic}}^0_{X_K/K}$ be the jacobian of the smooth projective curve $X_K = X \times_C \mathrm{Spec}(K)$. The Néron minimal model J/C exists and is of finite type over C. Because of the hypotheses on the multiplicities of the special fibres, to X one associates a torsor Z over C under J, which is just the smooth locus of π (subsection 4.1).

Let $\underline{\mathrm{Pic}}_{X/C} = R^1\pi_*\mathbf{G}_m$ be the Picard functor. This is the fppf sheaf on C associated to the presheaf $U \to \mathrm{Pic}(X \times_C U)$. Taking degrees on the generic fibre defines a short exact sequence of fppf sheaves on C

$$ 0 \to P_X \to \underline{\mathrm{Pic}}_{X/C} \to \mathbf{Z}_C \to 0 $$

defining the open and closed fppf subsheaf P_X. Restriction of this sequence to the (small) étale site of C still yields an exact sequence

$$ 0 \to P_X \to Pic_{X/C} \to \mathbf{Z}_C \to 0. \tag{4.3.1} $$

Surjectivity of $Pic_{X/C} \to \mathbf{Z}_C$ follows from the assumptions made on the special fibres.

Let $E_X \subset P_X$ be the schematic closure in P_X of the unit section of $\underline{\mathrm{Pic}}^0_{X_K/K}$. The quotient P_X/E_X (the biggest separated quotient of P_X) is representable by the abelian group scheme J/C. The connected component $\underline{\mathrm{Pic}}^0_{X/C}$ is separated and coincides with the identity component J^0 of J.

Let us assume for a moment that C is the spectrum $C = \mathrm{Spec}(R)$ of a strictly henselian discrete valuation ring R. Let D be the free, finitely generated, abelian group of divisors supported on the special fibre X_s. The subgroup of principal divisors is a free summand, of rank one, generated by the special fibre X_s of X/C (as defined by the divisor of the uniformizing parameter of R). Let $\Delta := D/\mathbf{Z}X_s$. Because of the assumption we made on the multiplicities, this is a finitely generated torsionfree abelian group : there is an exact sequence

$$0 \to \mathbf{Z} \xrightarrow{\{n_Y\}} \oplus_{Y \subset X_s} \mathbf{Z} \to \Delta \to 0,$$

where Y runs through the irreducible components of X_s, and n_Y is the multiplicity of Y. There is a natural isomorphism $\Delta \simeq E_X(C)$, which composed with the map $E_X(C) \subset \mathrm{Pic}(X)$ is the natural map associating to a divisor its class. Intersection of divisors defines a surjective map $\mathrm{Pic}(X) \to D^o = \mathrm{Hom}(D, \mathbf{Z})$, hence a surjective map $P_X(C) \to \Delta^o = \mathrm{Hom}(\Delta, \mathbf{Z})$. This latter map induces a homomorphism $\alpha : \Delta \to \Delta^o$. One has $\mathrm{Coker}(\alpha) \simeq J(R)/J^0(R)$. This latter group is none other than the (finite) group of connected components of (the special fibre of) J, which we have denoted F above.

Let us now go back to the general case of an integral Dedekind scheme C. For each $M \in C$ and each irreducible component $Y \subset X_M$, let n_Y be the multiplicity of Y and let k_Y be the algebraic closure of k_M in the function field $k(Y)$ of Y. Let $\beta_Y : \mathrm{Spec}(k_Y) \to \mathrm{Spec}(k_M)$ be the natural projection. We then have the exact sequence of sheaves on C :

(4.3.2)
$$0 \to i_{M*}\mathbf{Z} \xrightarrow{\{n_Y\}} \oplus_{Y \subset X_M} \beta_{Y*}\mathbf{Z} \to i_{M*}\Delta_M \to 0.$$

The various facts recalled above give us several commutative diagrams of exact sequences of sheaves for the étale topology on C.

The first diagram is

(4.3.3)

$$\begin{array}{ccccccccc}
0 & \to & P_X & \to & Pic_{X/C} & \to & \mathbf{Z} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \oplus_{M \in C} i_{M*}\Delta_M^o & \to & \oplus_{M \in C} i_{M*}D_M^o & \to & \oplus_{M \in C} i_{M*}\mathbf{Z} & \to & 0
\end{array}$$

The next diagram is

(4.3.4)

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & J^0 & = & J^0 & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \oplus_{M \in C} i_{M*}\Delta_M & \xrightarrow{\mathrm{cl}} & P_X & \longrightarrow & J & \longrightarrow & 0 \\
 & & || & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \oplus_{M \in C} i_{M*}\Delta_M & \xrightarrow{\alpha} & \oplus_{M \in C} i_{M*}(\Delta_M^o) & \longrightarrow & \oplus_{M \in C} i_{M*}F_M & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

where cl denotes the map which sends a divisor to its class in the Picard group and the sheaf F_M is the Galois module (over k_M) defined by the components of the geometric special fibre at

M (see subsection 4.2). This diagram is none other than (1.21) in [Art86], where attention is restricted to the case where $X_K(K) \neq \emptyset$.

The last diagram is

(4.3.5)

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & \oplus_{M\in C} i_{M*}\Delta_M & \to & P_X & \to & J & \to & 0 \\
 & & || & & \downarrow & & \downarrow & & \\
0 & \to & \oplus_{M\in C} i_{M*}\Delta_M & \to & Pic_{X/C} & \to & j_{K*}Pic_{X_K/K} & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mathbf{Z}_C & = & \mathbf{Z}_C & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

Surjectivity of $Pic_{X/C} \to j_{K*}Pic_{X_K/K}$ follows from the regularity of X.

Observe that the restrictions of the two right hand side vertical exact sequences to the generic point of C coincide with the exact sequence of étale sheaves on K :

$$0 \to Pic^0_{X_K/K} \to Pic_{X_K/K} \to \mathbf{Z}_K \to 0,$$

i.e.

$$0 \to J_K \to Pic_{X_K/K} \to \mathbf{Z} \to 0,$$

The boundary map $\mathbf{Z} \to H^1(K, J_K)$ maps 1 to the class of the principal homogeneous space $X_K = Z_K$ under J_K. Since the map $H^1(C, J) \to H^1(K, J_K)$ is injective by the Néron property we conclude that the image of 1 under the boundary map $\mathbf{Z} \to H^1(C, J)$ in the cohomology sequence associated to the right hand side exact sequence is the class $[Z]$. From diagram (4.3.5) we see that this boundary map factorizes as $\mathbf{Z} \xrightarrow{d_X} H^1(C, P_X) \to H^1(C, J)$, where the map $d_X : \mathbf{Z} \to H^1(C, P_X)$ is the boundary map in the cohomology sequence associated to the middle vertical exact sequence.

For each $M \in C$, there is a map $\delta_M : H^1(C, J) \to H^1(k_M, F_M)$ coming from diagram (4.3.4) and there is a boundary map $d_M : H^1(C, J) \to H^2(k_M, \Delta_M)$ associated to the exact sequence

(4.3.6) $$0 \to \oplus_{M\in C} i_{M*}\Delta_M \xrightarrow{\mathrm{cl}} P_X \to J \to 0.$$

For the sake of simplicity, let us assume that C is local, with closed point M. Diagram (4.3.4) gives rise to the commutative diagram of exact sequences :

$$\begin{array}{ccccc}
H^1(C, P_X) & \to & H^1(C, J) & \to & H^2(k_M, \Delta_M) \\
\downarrow & & \downarrow \delta_M & & || \\
H^1(k_M, \Delta^o_M) & \to & H^1(k_M, F_M) & \to & H^2(k_M, \Delta_M)
\end{array}$$

In diagram (4.3.3), D_M^o is a permutation module over the absolute Galois group of k_M, hence $H^1(k_M, D_M^o) = 0$. Cohomology of (4.3.3) therefore yields a commutative diagram

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{d_M} & H^1(C, P_X) \\ || & & \downarrow \\ \mathbf{Z} & \longrightarrow & H^1(k_M, \Delta_M^o) \end{array}$$

where the lower map is surjective. Let us now revert to the case of an arbitrary C. Let us now revert to the case of an arbitrary C. We have proved :

Proposition 4.3.1 *For each closed point $M \in C$, the coboundary map $d_M : H^1(C, J) \to H^2(k_M, \Delta_M)$ coming from (4.3.6) factorizes as :*

$$H^1(C, J) \to H^1(C, J)/\mathbf{Z}[Z] \xrightarrow{\delta_M} H^1(k_M, F_M)/\mathbf{Z}\delta_M([Z]) \hookrightarrow H^2(k_M, \Delta_M),$$

the last map being an injection. □

This enables us to give the following definition :

Definition 4.3.2 *Let $\mathcal{D}(X)$ be the subgroup of $H^1(C, J)/\mathbf{Z}[Z]$ defined by either of the equivalent definitions*

$$\mathcal{D}(X) := \mathrm{Ker}[H^1(C, J)/\mathbf{Z}[Z] \xrightarrow{\oplus_{M \in C} \delta_M} \bigoplus_{M \in C} H^1(k_M, F_M)/\mathbf{Z}\delta_M([Z])],$$

where the maps δ_M are induced by the maps $J \to i_{M*}F_M$, or

$$\mathcal{D}(X) := \mathrm{Ker}[H^1(C, J)/\mathbf{Z}[Z] \xrightarrow{\oplus_{M \in C} d_M} \bigoplus_{M \in C} H^2(k_M, \Delta_M)],$$

where d_M comes from (4.3.6). (We have abused notation and denoted by δ_M and d_M maps induced by maps bearing these names.)

The first definition uses the Néron model J/C and the class $[Z] \in H^1(C, J)$. In the second definition, the maps d_M are induced by the coboundary maps $d_M : H^1(C, J) \to H^2(k_M, \Delta_M)$ associated to (4.3.6) ; this exact sequence involves the geometry of X.

4.4 Cohomology of $\mathbf{G}_m$

In this subsection we develop the (hyper)cohomological machinery necessary to establish theorem 4.5.1 below and its various corollaries. Although theorem 4.5.1 could be stated without reference to derived categories, the proof of the stated commutativities in easier to give from this point of view. We refer the reader to [BBD82] and the literature cited there for the necessary background, including the definition and properties of the truncation functors $\tau_{\leq n}$.

Let $\pi : X \to C$ be as in the beginning of subsection 4.3. Note that since π is proper and has geometrically connected fibres one has $\mathbf{G}_{m,C} \xrightarrow{\simeq} \pi_*\mathbf{G}_{m,X}$, and $\mathbf{G}_{m,K} \xrightarrow{\simeq} \pi_*\mathbf{G}_{m,X_K}$. Let $j_{X_K} : X_K \to X$ be the map induced by $j_K : \mathrm{Spec}(K) \to C$.

Lemma 4.4.1 *Let X/C be as above.*
(a) We have $R^n j_{K*}\mathbf{G}_{m,K} = 0$ for all $n \geq 1$;
(b) we have $R^1 j_{X_K*}\mathbf{G}_{m,X_K} = 0$;

(c) *if the local rings of C are Japanese, we have $R^n\pi_*\mathbf{G}_{m,X} = 0$ for $n \geq 2$.*

Proof (a) Recall that we assumed all residue fields of C to be perfect. The result now follows from [Gr68], III, Thm. 1.1 : for $n = 1$ this is a consequence of Hilbert's theorem 90, and for $n \geq 2$ the fraction field of an excellent henselian discrete valuation ring with algebraically closed residue field is a C_1 field (Lang's theorem) – when C is a smooth curve over a field of characteristic zero, the result follows from Tsen's theorem – hence has cohomological dimension 1.

(b) Let P be a point of X. Then on $\mathrm{Spec}(O^{sh}_{X,P})$ the sheaf $R^1j_*\mathbf{G}_{m,X_K}$ is computed as $Pic(O^{sh}_{X,P} \times_C K)$. There is a natural restriction map

$$Pic(O^{sh}_{X,P}) \to Pic(O^{sh}_{X,P} \times_C K).$$

Since X is regular, this map is surjective. It is clear that $Pic(O^{sh}_{X,P}) = 0$. Thus our statement is proved.

(c) This is Artin's theorem ([Gr68], III, Cor. 3.2, p. 98). Here we are using the fact that the fibres have dimension one. □

Given a sheaf $\mathcal{F}$ on C, we denote by $\mathcal{F}^\bullet$ its image in the derived category, under the map which sends it to the class of the complex consisting of $\mathcal{F}$ in degree zero and 0 elsewhere.

Theorem 4.4.2 *Let X/C be as above. In the derived category $\mathrm{D}_+(C_{\text{ét}})$ of bounded below complexes of sheaves for the étale topology on C, there is a commutative diagram of distinguished triangles (arrows will be defined in the proof) :*

$$\begin{array}{ccccc}
\mathbf{G}_{m,C}{}^\bullet & \to & \tau_{\leq 1}(\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^\bullet) & \to & Pic_{X/C}{}^\bullet[-1] \\
\downarrow & & \downarrow & & \downarrow \\
j_{K*}\mathbf{G}_{m,K}{}^\bullet & \to & \tau_{\leq 1}(\mathbf{R}\pi_*)(j_{X_K*}\mathbf{G}_{m,X_K}{}^\bullet) & \to & j_{K*}Pic_{X_K/K}{}^\bullet[-1] \\
\downarrow & & \downarrow & & \downarrow \\
\oplus_{M\in C} i_{M*}\mathbf{Z}_{k(M)}{}^\bullet & \to & \oplus_{M\in C}\oplus_{Y\subset X_M}\tau_{\leq 1}(\mathbf{R}\pi_*)(i_{Y*}\mathbf{Z}_{k(Y)}{}^\bullet) & \to & \oplus_{M\in C} i_{M*}\Delta_M{}^\bullet
\end{array}$$

Proof Given a sheaf $\mathcal{F}$ on X and the complex $(\mathbf{R}\pi_*)(\mathcal{F}^\bullet)$, we have a distinguished triangle :

$$(\pi_*\mathcal{F})^\bullet \to \tau_{\leq 1}(\mathbf{R}\pi_*)(\mathcal{F}^\bullet) \to (R^1\pi_*\mathcal{F})^\bullet[-1]$$

and this associated distinguished triangle is functorial in $\mathcal{F}$.

Let us apply this first to the sheaf $\mathbf{G}_{m,X}$. From $\mathbf{G}_{m,C} \stackrel{\simeq}{\to} \pi_*(\mathbf{G}_{m,X})$ and $R^1\pi_*(\mathbf{G}_{m,X}) = Pic_{X/C}$, we obtain the top distinguished triangle in the diagram.

Let us now apply this to the sheaf $j_{X_K*}(\mathbf{G}_{m,X_K})$. The two maps $\pi \circ j_{X_K}$ and $j_K \circ \pi_K$ coincide, and define a map $\rho : X_K \to C$. We have $\pi_*(j_{X_K*}(\mathbf{G}_{m,X_K})) = \rho_*(\mathbf{G}_{m,X_K}) = j_{K*}(\pi_*(\mathbf{G}_{m,X_K})) = j_{K*}(\mathbf{G}_{m,K})$. This identifies the left term of the middle horizontal distinguished triangle.

Let us show $(R^1\pi_*)(j_{X_K*}\mathbf{G}_{m,X_K}) \stackrel{\simeq}{\to} j_{K*}Pic_{X_K/K}$. The spectral sequence of composite functors $\mathbf{R}\rho_* = \mathbf{R}\pi_* \circ \mathbf{R}j_{X_K*}$ yields the exact sequence of sheaves

$$0 \to R^1\pi_*(j_{X_K*}\mathbf{G}_{m,X_K}) \to R^1\rho_*(\mathbf{G}_{m,X_K}) \to \pi_*(R^1j_{X_K*}(\mathbf{G}_{m,X_K})).$$

By Lemma 4.4.1 (b), we have $R^1j_{X_K*}(\mathbf{G}_{m,X_K}) = 0$, hence $R^1\pi_*(j_{X_K*}\mathbf{G}_{m,X_K}) \stackrel{\simeq}{\to} R^1\rho_*(\mathbf{G}_{m,X_K})$. The spectral sequence of composite functors $\mathbf{R}\rho_* = \mathbf{R}j_{K*} \circ \mathbf{R}\pi_*$ gives rise to the exact sequence

$$0 \to R^1j_{K*}(\mathbf{G}_{m,K}) \to R^1\rho_*(\mathbf{G}_{m,X_K}) \to j_{K*}(R^1\pi_*(\mathbf{G}_{m,X_K})) \to R^2j_{K*}(\mathbf{G}_{m,K}),$$

where we have used $\mathbf{G}_{m,K} \stackrel{\simeq}{\to} \pi_*\mathbf{G}_{m,X_K}$. By Lemma 4.4.1 (a), we have $R^1 j_{K*}(\mathbf{G}_{m,K}) = 0$ and $R^2 j_{K*}(\mathbf{G}_{m,K}) = 0$. We thus have a natural isomorphism $R^1\rho_*(\mathbf{G}_{m,X_K}) \stackrel{\simeq}{\to} j_{K*}(R^1\pi_*(\mathbf{G}_{m,X_K}))$, which composed with $R^1\pi_*(j_*\mathbf{G}_{m,X_K}) \stackrel{\simeq}{\to} R^1\rho_*(\mathbf{G}_{m,X_K})$ yields the announced isomorphism $R^1\pi_*(j_{X_K*}\mathbf{G}_{m,X_K}) \stackrel{\simeq}{\to} j_{K*}Pic_{X_K/K}$ and completes the construction of the middle distinguished triangle in the diagram. It is an easy matter to check that the vertical maps induced by functoriality in $\mathcal{F}$ of the construction above are the obvious ones.

Since C is regular we have an exact sequence of étale sheaves over C :

$$1 \to \mathbf{G}_{m,C} \to j_{K*}\mathbf{G}_{m,K} \to \oplus_{M\in C} i_{M*}\mathbf{Z}_{k(M)} \to 0.$$

Since X is also regular, there is a similar exact sequence of étale sheaves over X :

$$1 \to \mathbf{G}_{m,X} \to j_{X_K*}\mathbf{G}_{m,X_K} \to \oplus_{M\in C} \oplus_{Y\subset X_M} i_{Y*}\mathbf{Z}_{k(Y)} \to 0,$$

where $i_Y : Spec(k(Y)) \to X$ is the inclusion of the generic point of Y.

The second exact sequence gives rise to the following distinguished triangle in the derived category of étale sheaves over C :

$$\mathbf{R}\pi_*(\mathbf{G}_{m,X}{}^\bullet) \to \mathbf{R}\pi_*(j_{X_K*}\mathbf{G}_{m,X_K}{}^\bullet) \to \oplus_{M\in C} \oplus_{Y\subset X_M} \mathbf{R}\pi_*(i_{Y*}\mathbf{Z}_{k(Y)}{}^\bullet).$$

By Artin's theorem (lemma 4.4.1 (c)) we have $R^2\pi_*(\mathbf{G}_{m,X}) = 0$. This implies that if we apply $\tau_{\leq 1}$ to the previous distinguished triangle, we still get a distinguished triangle. By the universal property of truncation, we find that there is a map of distinguished triangles :

$$\begin{array}{ccc}
\mathbf{G}_{m,C}{}^\bullet & \to & \tau_{\leq 1}(\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^\bullet) \\
\downarrow & & \downarrow \\
j_{K*}\mathbf{G}_{m,K}{}^\bullet & \to & \tau_{\leq 1}(\mathbf{R}\pi_*)(j_{X_K*}\mathbf{G}_{m,X_K}{}^\bullet) \\
\downarrow & & \downarrow \\
\oplus_{M\in C} i_{M*}\mathbf{Z}_{k(M)}{}^\bullet & \to & \oplus_{M\in C} \oplus_{Y\subset X_M} \tau_{\leq 1}(\mathbf{R}\pi_*)(i_{Y*}\mathbf{Z}_{k(Y)}{}^\bullet)
\end{array}$$

Let us analyze the map $i_{M*}\mathbf{Z}_{k(M)}{}^\bullet \to \tau_{\leq 1}(\mathbf{R}\pi_*)(i_{Y*}\mathbf{Z}_{k(Y)}{}^\bullet)$. Let $\sigma_Y = \pi \circ i_Y : \mathrm{Spec}(k(Y)) \to C$. This map also factorizes as $\sigma_Y = i_M \circ \beta_Y \circ \alpha_Y$, with $\alpha_Y : \mathrm{Spec}(k(Y)) \to \mathrm{Spec}(k_Y)$ and $\beta_Y = \mathrm{Spec}(k_Y) \to \mathrm{Spec}(k_M)$ the obvious maps. Since β_Y and i_M are finite maps, we have $R^n\beta_{Y*} = 0$ and $R^n i_{M*} = 0$ for $n \geq 1$. By definition, k_Y is algebraically closed in $k(Y)$. Let $k_Y \subset F_Y$ be the embedding of k_Y into a separable closure, and let $F(Y) = k(Y) \otimes_{k_Y} F_Y$, which is a field. We have $H^0(F(Y), \mathbf{Z}) = \mathbf{Z}$ and $H^1(F(Y), \mathbf{Z}) = 0$. Hence the natural map $\mathbf{Z}_{k_Y} \to \alpha_{Y*}\mathbf{Z}_{k(Y)}$ is an isomorphism, and $R^1\alpha_{Y*}\mathbf{Z}_{k(Y)} = 0$. The spectral sequences of composite functors now easily yield : $R^1\pi_*(i_{Y*}\mathbf{Z}_{k(Y)}) = 0$. On the other hand, $\pi_*(i_{Y*}\mathbf{Z}_{k(Y)}) = \sigma_{Y*}(\mathbf{Z}_{k(Y)}) = i_{M*}\beta_{Y*}\mathbf{Z}_{k_Y}$. We thus have a natural quasi-isomorphism

$$(i_{M*}\beta_{Y*}\mathbf{Z}_{k_Y})^\bullet \stackrel{\simeq}{\to} \tau_{\leq 1}(\mathbf{R}\pi_*)(i_{Y*}\mathbf{Z}_{k(Y)}{}^\bullet)$$

hence the bottom map in the above diagram may be rewritten as

$$\oplus_{M\in C}(i_{M*}\mathbf{Z}_{k_M})^\bullet \to \oplus_{M\in C} \oplus_{Y\subset X_M} (i_{M*}\beta_{Y*}\mathbf{Z}_{k_Y})^\bullet.$$

It is an easy matter to check that this map is induced by the maps $n_Y : \mathbf{Z}_{k_M} \to \beta_{Y*}\mathbf{Z}_{k_Y}$. Indeed, for any irreducible component $Y \subset X_M$ with multiplicity n_Y, a valuation computation shows that the following diagram of sheaves is commutative :

$$\begin{array}{ccc} j_{K*}(\mathbf{G}_{m,K}) & \longrightarrow & j_{X_K*}(\mathbf{G}_{m,X_K}) \\ \downarrow & & \downarrow \\ i_{M*}\mathbf{Z}_{k_M} & \xrightarrow{n_Y} & i_{Y*}(\mathbf{Z}_{k(Y)}) \end{array}$$

We have now identified all terms of the above diagram of distinguished triangles. As any such diagram, it may be completed into a diagram 'of the nine' (see [BBD82] Prop. 1.1.11). This diagram of the nine is the one announced in the theorem, except that we have not yet identified the term in the bottom right hand side. This we can do in two ways :

Using the exact sequences

$$0 \to i_{M*}\mathbf{Z} \xrightarrow{\{n_Y\}} \oplus_{Y\subset X_M}\beta_{Y*}\mathbf{Z} \to i_{M*}\Delta_M \to 0,$$

we find that this term is $\oplus_{M\in C} i_{M*}(\Delta_M)^{\bullet}$.

Or we use the exact sequence of sheaves :

$$0 \to \oplus_{M\in C} i_{M*}\Delta_M \to Pic_{X/C} \to j_{K*}Pic_{X_K/K} \to 0$$

which gives us the distinguished triangle

$$Pic_{X/C}{}^{\bullet}[-1] \to (j_{K*}Pic_{X_K/K})^{\bullet}[-1] \to \oplus_{M\in C}(i_{M*}\Delta_M)^{\bullet}.$$

This completes the proof. □

Let us now identify various hypercohomology groups of the complexes appearing in theorem 4.4.2.

Proposition 4.4.3 *Let assumptions be as in theorem 4.4.2.*

(a) For $n \geq 0$, we have $\mathbf{H}^n(C, \mathbf{G}_{m,C}{}^{\bullet}) = H^n(C, \mathbf{G}_{m,C})$.

(b) For $n \geq 0$, we have $\mathbf{H}^n(C, \tau_{\leq 1}(\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^{\bullet})) = H^n(X, \mathbf{G}_{m,X})$.

(c) For $n \geq 0$, we have $\mathbf{H}^n(C, j_{K*}\mathbf{G}_{m,K}{}^{\bullet}) = H^n(C, j_{K*}\mathbf{G}_{m,K}) = H^n(K, \mathbf{G}_{m,K})$.

(d) We have $\mathbf{H}^2(C, Pic^{\bullet}_{X/C}[-1]) = H^1(C, Pic_{X/C}) = H^1(C, P_X)/d(1)$, where the map d is induced by the cohomology of sequence (4.3.1).

(e) We have $\mathbf{H}^2(C, (j_{K*}Pic_{X_K/K})^{\bullet}[-1]) = H^1(C, j_{K*}Pic_{X_K/K}) = H^1(C, J)/[Z]$.

Proof Quite generally, for $\mathcal{F}$ a sheaf on C, we have $\mathbf{H}^i(C, \mathcal{F}^{\bullet}) = H^i(C, \mathcal{F})$. Statement (a) is thus clear. Because of Artin's theorem (Lemma 4.4.1 (c)), the natural map $\tau_{\leq 1}(\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^{\bullet}) \to (\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^{\bullet})$ is a quasi-isomorphism. For any integer n, we therefore have

$$\mathbf{H}^n(C, \tau_{\leq 1}(\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^{\bullet})) \xrightarrow{\simeq} \mathbf{H}^n(C, (\mathbf{R}\pi_*)(\mathbf{G}_{m,X}{}^{\bullet})) = H^n(X, \mathbf{G}_{m,X}),$$

which is claim (b). By Lemma 4.4.1 (a), we have $R^n j_{K*}(\mathbf{G}_{m,K}) = 0$ for $n \geq 1$. Statement (c) follows. Statement (d) is obvious since $H^1(C, \mathbf{Z}_C) = 0$ (since C is regular, hence in particular geometrically unibranch). As for statement (e), the exact sequence of sheaves

$$0 \to J \to j_{K*}Pic_{X_K/K} \to \mathbf{Z}_C \to 0$$

from diagram (4.3.5) gives rise to an exact sequence

$$\mathbf{Z} \to H^1(C, J) \to H^1(C, j_{K*}Pic_{X_K/K}) \to 0$$

(the last zero for the same reason as above). It only remains to use the fact that the image of $1 \in \mathbf{Z}$ is none other than the class of the homogeneous space Z (comments after (4.3.5)). ∎

Theorem 4.4.4 *The following groups are canonically isomorphic :*

(a) the subgroup $\mathrm{Br}^{gnr}(X_K)$ *of the Brauer group* $\mathrm{Br}(X_K)$ *consisting of geometrically unramified elements, that is, elements of* $\mathrm{Br}(X_K)$ *whose image in* $\mathrm{Br}(X_{K_M^{sh}})$ *lies in the subgroup* $\mathrm{Br}(X_{O_M^{sh}})$, *for any closed point* $M \in C$ *;*

(b) the subgroup of the Brauer group $\mathrm{Br}(X_K)$ *consisting of elements of* $\mathrm{Br}(X_K)$ *which vanish in* $\mathrm{Br}(X_{K_M^{sh}})$ *for any closed point* $M \in C$ *;*

(c) the hypercohomology group $\mathbf{H}^2(C, \tau_{\leq 1}(\mathbf{R}\pi_*)j_*\mathbf{G}_{m,X_K})$.

Asssume that C *is a smooth geometrically integral curve over a field* k *of characteristic zero. Then* $\mathrm{Br}^{gnr}(X_K)$ *also coincides with :*

(d) the group of elements $A \in \mathrm{Br}(X_K)$ *such that for each irreducible component* $Y \subset X_M$ *of a fibre* X_M *above a closed point* M, *the residue* $\mathrm{res}_Y(A) \in H^1(k(Y), \mathbf{Q}/\mathbf{Z})$ *is 'constant', i.e. comes from* $H^1(k_Y, \mathbf{Q}/\mathbf{Z})$ *;*

(e) the group of elements $A \in \mathrm{Br}(X_K) = \mathrm{Br}(X_{k(C)})$ *whose image in* $\mathrm{Br}(X_{k^s(C)})$ *is unramified, i.e. comes from* $\mathrm{Br}(X \times_k k^s)$.

Proof Since the relative dimension is one, $\mathrm{Br}(X_{O_M^{sh}}) = 0$ by Artin's theorem. The equivalence of (a) and (b) immediately follows.

By Lemma 4.4.1 (c), we have $R^1 j_{X_K *}\mathbf{G}_{m,X_K} = 0$. Hence the spectral sequence

$$E_2^{pq} = H^p(X, R^q j_{X_K *}\mathbf{G}_{m,X_K}) \Longrightarrow H^n(X_K, \mathbf{G}_{m,X_K})$$

yields the short exact sequence

$$0 \to H^2(X, j_{X_K *}(\mathbf{G}_{m,X_K})) \to H^2(X_K, \mathbf{G}_{m,X_K}) \to H^0(X, R^2 j_{X_K *}(\mathbf{G}_{m,X_K}))$$

and we have a compatible exact sequence for each map $X_{O_M^{sh}} \to X_{K_M^{sh}}$. Thus if $A \in H^2(X_K, \mathbf{G}_{m,X_K})$ lies in $\mathrm{Br}^{gnr}(X_K)$, then its image $b \in H^0(X, R^2 j_{X_K *}(\mathbf{G}_{m,X_K}))$ restricts to zero in each $H^0(X_{O_M^{sh}}, R^2 j_{X_{K_M^{sh}} *}(\mathbf{G}_{m,X_{K_M^{sh}}}))$. We conclude that each closed point of X admits an étale neighbourhood over which the section b vanishes, hence $b = 0$. The exact sequence above now implies that $\mathrm{Br}^{gnr}(X_K)$ actually lies in $H^2(X, j_{X_K *}(\mathbf{G}_{m,X_K})) \subset H^2(X_K, \mathbf{G}_{m,X_K})$, more precisely it coincides with the subgroup of elements of $H^2(X, j_{X_K *}(\mathbf{G}_{m,X_K}))$ which restrict to zero in each $H^2(X_{O_M^{sh}}, j_{X_{K_M^{sh}} *}(\mathbf{G}_{m,X_{K_M^{sh}}}))$.

We have the distinguished triangle

$$\tau_{\leq 1}(\mathbf{R}\pi_*)(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet) \to (\mathbf{R}\pi_*)(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet) \to \tau_{\geq 2}(\mathbf{R}\pi_*)(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet).$$

By the definition of truncation, we have $\mathbf{H}^n(C, \tau_{\geq 2}(\mathbf{R}\pi_*)(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet)) = 0$ for $n \leq 1$ and $\mathbf{H}^2(C, \tau_{\geq 2}(\mathbf{R}\pi_*)(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet)) = H^0(C, R^2\pi_*(j_{X_K *}\mathbf{G}_{m,X_K}))$. Hence the hypercohomology exact sequence associated to the above triangle gives in particular the exact sequence :

$$0 \to \mathbf{H}^2(C, \tau_{\leq 1}(\mathbf{R}\pi_*)(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet)) \to H^2(X, j_{X_K *}\mathbf{G}_{m,X_K}) \to H^0(C, R^2\pi_*(j_{X_K *}\mathbf{G}_{m,X_K})),$$

and we have compatible exact sequences for each $X_{O_M^{sh}}/O_M^{sh}$ in place of X/C. Now a class in $H^2(X, j_{X_K *}\mathbf{G}_{m,X_K})$ which restricts to zero in each $H^2(X_{O_M^{sh}}, j_{X_{K_M^{sh}} *}(\mathbf{G}_{m,X_{K_M^{sh}}}))$ has for image a section of the sheaf $R^2\pi_*(j_{X_K *}\mathbf{G}_{m,X_K})$ with trivial value in a suitable neighbourhood of any closed point of C, hence this image is zero. We conclude that $\mathrm{Br}^{gnr}(X_K)$ is identified with a subgroup of

$$\mathbf{H}^2(C, \tau_{\leq 1}\mathbf{R}\pi_*(j_{X_K *}\mathbf{G}_{m,X_K}{}^\bullet)) \subset H^2(X, j_{X_K *}\mathbf{G}_{m,X_K}) \subset H^2(X_K, \mathbf{G}_m).$$

On the other hand, we may consider a similar and compatible distinguished triangle as the one above over O_M^{sh}. Since a strictly henselian local ring has sheaf cohomology only in degree zero, we clearly have $\mathbf{H}^2(O_M^{sh}, \tau_{\leq 1}\mathbf{R}\pi_*(j_{X_{K_M^{sh}}*}\mathbf{G}_{m,X_{K_M^{sh}}})^\bullet) = 0$ as we would have with any complex concentrated in degrees at most one. Thus the image of the composite map

$$\mathbf{H}^2(C, \tau_{\leq 1}(\mathbf{R}\pi_*)(j_{X_K*}\mathbf{G}_{m,X_K}{}^\bullet) \to H^2(X, j_{X_K*}\mathbf{G}_{m,X_K}) \to H^2(X_K, \mathbf{G}_m)$$

vanishes in each $H^2(X_{K_M^{sh}}, \mathbf{G}_m)$. This completes the proof that the group in (c) is the same as the group in (a) and (b).

Let A be a discrete valuation ring with field of fractions L and perfect residue field κ. Let $j_L : \mathrm{Spec}(L) \to \mathrm{Spec}(A)$ (resp. i_κ) be the inclusion of the generic (resp. special) point. By lemma 4.1.1 we have $R^n j_{L*}\mathbf{G}_{m,L} = 0$ for all $n \geq 1$. From the exact sequence of sheaves

$$1 \to \mathbf{G}_{m,A} \to j_{L*}\mathbf{G}_{m,L} \to i_{\kappa*}\mathbf{Z}_\kappa \to 0$$

we now deduce the exact sequence

$$0 \to \mathrm{Br}(A) \to \mathrm{Br}(L) \xrightarrow{\mathrm{res}} H^1(\kappa, \mathbf{Q}/\mathbf{Z}).$$

Let $\mathcal{X}$ be a two-dimensional, regular, integral scheme whose residue class fields are of characteristic zero. By classical results on the purity of the Brauer group ([Gr68], II, Prop. 2.3) an element α in the Brauer group of the function field of X belongs to $\mathrm{Br}(X)$ if and only if for any closed irreducible subvariety $Y \subset X$ of codimension one with function field $\kappa(Y)$, we have $\mathrm{res}_Y(\alpha) = 0 \in H^1(\kappa(Y), \mathbf{Q}/\mathbf{Z})$.

For any given closed point $M \in C$ we have a natural commutative diagram :

$$\begin{array}{ccccc}
X & \leftarrow & X \times_k k^s & \leftarrow & X_{O_M^{sh}} \\
\downarrow & & \downarrow & & \downarrow \\
C & \leftarrow & C \times_k k^s & \leftarrow & \mathrm{Spec}(O_M^{sh})
\end{array}$$

Since the horizontal maps are limits of étale maps, for $Y \subset X_M$ a component of the fibre X_M, the upper part of the diagram gives rise to the following commutative diagram :

$$\begin{array}{ccccc}
\mathrm{Br}(X_K) & \to & \mathrm{Br}(X_{K\otimes_k k^s}) & \longrightarrow & \mathrm{Br}(X_{K_M^{sh}}) \\
\downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \downarrow \mathrm{res} \\
H^1(k(Y), \mathbf{Q}/\mathbf{Z}) & \to & H^1(k(Y)\otimes_k k^s, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\simeq} & H^1(k(Y)\otimes_k k^s, \mathbf{Q}/\mathbf{Z})
\end{array}$$

The kernel of the map $H^1(k(Y), \mathbf{Q}/\mathbf{Z}) \to H^1(k(Y)\otimes_k k^s, \mathbf{Q}/\mathbf{Z})$ is precisely $H^1(k_Y, \mathbf{Q}/\mathbf{Z})$, where k_Y is the separable closure of k in $k(Y)$. Combining these remarks, we conclude that $\mathrm{Br}^{gnr}(X_K)$ coincides with the groups in (d) and (e). ∎

When the field k is of positive characteristic p, the identification of $\mathrm{Br}^{gnr}(X_K)$ with the groups in (d) and (e) still holds, provided one restricts to the prime-to-p torsion.

4.5 The Brauer group of X, the group $\mathcal{D}(X)$, and the geometric Selmer group

Theorem 4.5.1 *Let X/C be as in the beginning of subsection 4.3, $\mathrm{Br}^{gnr}(X_K)$ as in theorem 4.4.4 and $\mathcal{D}(X)$ as in definition 4.3.2.*
a) There is a commutative diagram

$$\begin{array}{ccccc}
0 & & 0 & & 0 \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Br}(C) & \longrightarrow & \mathrm{Br}(X) & \longrightarrow & \mathcal{D}(X) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Br}(K) & \longrightarrow & \mathrm{Br}^{gnr}(X_K) & \longrightarrow & H^1(C,J)/[Z] \\
\downarrow \mathrm{res} & & \downarrow & & \downarrow \{d_M\} \\
\bigoplus_{M\in C} H^1(k_M,\mathbf{Q}/\mathbf{Z}) & \longrightarrow & \bigoplus_{M\in C}\bigoplus_{Y\subset X_M} H^1(k_Y,\mathbf{Q}/\mathbf{Z}) & \longrightarrow & \bigoplus_{M\in C} H^2(k_M,\Delta_M)
\end{array}$$

with exact columns and exact middle and bottom rows, the map $\mathrm{Br}(X)\to\mathcal{D}(X)$ being induced from the rest of the diagram.
b) If k is a number field and C is a dense open set of $\mathbf{P}^1_k$, then the middle and bottom rows of this diagram are right exact.

Proof Applying hypercohomology to the diagram of theorem 4.4.2 and using the identifications of hypercohomology groups in Proposition 4.4.3 gives a). Note that it gives more, in particular the horizontal middle exact sequence extends to the right, the next term being $H^3(K,\mathbf{G}_m)$, and the bottom exact sequence also extends to the right, the next term being $\oplus_{M\in C}H^3(k_M,\mathbf{Z})\simeq\oplus_{M\in C}H^2(k_M,\mathbf{Q}/\mathbf{Z})$.
If F is a number field, then $H^2(F,\mathbf{Q}/\mathbf{Z})=0$ ([Schn79]). Thus if k is a number field and C an open of $\mathbf{P}^1_k$ the bottom sequence is right exact. Under the same assumptions, $H^3(k(\mathbf{P}^1_k),\mathbf{G}_m)=0$: this is an easy consequence (cf. [Ha94], p. 241) of the previous vanishing result for all finite extensions F/k, together with the vanishing of $H^3(k,\mathbf{G}_m)$ ([ANT67], p. 199). This completes the proof of b). $\square$

Note that if C is a curve over a field of characteristic zero, the map $\mathrm{Br}^{gnr}(X_K)\to H^1(k_Y,\mathbf{Q}/\mathbf{Z})$ in the diagram above is induced by the residue map at the generic point of Y.

Let us define the vertical Brauer group of X (with respect to π) as :

$$\mathrm{Br}_{\mathrm{vert}}(X):=\mathrm{Br}(X)\cap\pi^*(\mathrm{Br}(K))\subset\mathrm{Br}(X_K),$$

and let the 'horizontal' (or rather non-vertical) Brauer group be :

$$\mathrm{Br}_{\mathrm{hor}}(X):=\mathrm{Br}(X)/\mathrm{Br}_{\mathrm{vert}}(X).$$

Theorem 4.5.2 *Let $\pi: X\to C$ be as above, and let $\mathrm{Br}(X)\to\mathcal{D}(X)$ be the map in the above diagram.*
a) This map induces an embedding $\mathrm{Br}_{\mathrm{hor}}(X)\hookrightarrow\mathcal{D}(X)$.
b) Assume that k is a number field and $C=\mathbf{A}^1_k$. Then the map $\mathrm{Br}_{\mathrm{hor}}(X)\hookrightarrow\mathcal{D}(X)$ is an isomorphism.

c) Assume that k is a number field and $C = \mathbf{P}^1_k$. There is an exact sequence

$$0 \to \mathrm{Br}_{\mathrm{hor}}(X) \to \mathcal{D}(X) \to H^1(k, \mathbf{Q}/\mathbf{Z})/[\sum_M t_M(H^1(k_M, \Delta_M))].$$

Here $t_M : H^1(k_M, \Delta_M) \to H^1(k, \mathbf{Q}/\mathbf{Z})$ is the composite map $H^1(k_M, \Delta_M) \to H^2(k_M, \mathbf{Z}) \simeq H^1(k_M, \mathbf{Q}/\mathbf{Z}) \to H^1(k, \mathbf{Q}/\mathbf{Z})$, the first map coming from the exact sequence $0 \to \mathbf{Z} \to D_M \to \Delta_M \to 0$, the last map being the norm map from k_M to k.

d) In the situation of c), let $\mathbf{A}^1_k \subset \mathbf{P}^1_k$ be the complement of a k-point. Then $\mathrm{Br}_{\mathrm{hor}}(X)$ injects into $\mathcal{D}(X \times_{\mathbf{P}^1_k} \mathbf{A}^1_k)$.

Proof This follows from the previous theorem and a chase through the big diagram in that theorem, together with the following facts. Firstly, the bottom exact sequence extends on the left to a map $H^1(k_M, \Delta_M) \to H^2(k_M, \mathbf{Z}) = H^1(k_M, \mathbf{Q}/\mathbf{Z})$. This is clear from the preliminaries. Secondly, we have the following well-known results, which go back to D. K. Faddeev. Let $C = \mathbf{A}^1_k = \mathrm{Spec}(k[t])$. Then the left vertical exact sequence in this diagram extends to an exact sequence :

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}(k(t)) \to \bigoplus_{M \in \mathbf{A}^1_k} H^1(k_M, \mathbf{Q}/\mathbf{Z}) \to 0.$$

Let $C = \mathbf{P}^1_k$. Then the left vertical exact sequence in this diagram extends to an exact sequence :

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}(k(t)) \to \bigoplus_{M \in \mathbf{P}^1_k} H^1(k_M, \mathbf{Q}/\mathbf{Z}) \to H^1(k, \mathbf{Q}/\mathbf{Z}) \to 0,$$

where maps $H^1(k_M, \mathbf{Q}/\mathbf{Z}) \to H^1(k, \mathbf{Q}/\mathbf{Z})$ are norm maps from k_M to k. $\square$

Let us revert to the geometric Selmer groups discussed in subsection 4.2. Let n be the order of $[Z] \in H^1(C, J)$, which is the order of $[X_K] \in H^1(K, J_K)$. Assume $n > 0$, i.e. $X_K(K) = \emptyset$. Let $m \in \mathfrak{S}(J, n)$ be a lift of $[Z]$ under the surjective map $\mathfrak{S}(J, n) \to {}_nH^1(C, J)$. From proposition 4.2.2 a) we get an isomorphism

$$\mathfrak{S}(J, n)/(\mathbf{Z}m + J(K)/n) \xrightarrow{\simeq} ({}_nH^1(C, J))/\mathbf{Z}[Z]$$

which we may compose with the inclusions

$$({}_nH^1(C, J))/\mathbf{Z}[Z] \subset {}_n(H^1(C, J)/\mathbf{Z}[Z]) \subset H^1(C, J)/\mathbf{Z}[Z]$$

and the map

$$H^1(C, J)/\mathbf{Z}[Z] \xrightarrow{\oplus_{M \in C} \delta_M} \bigoplus_{M \in C} H^1(k_M, F_M)/\mathbf{Z}\delta_M([Z])$$

whose kernel is by definition $\mathcal{D}(X)$. Let $\mathcal{D}^n(X)$ be the kernel of this composite map :

$$\mathcal{D}^n(X) := \mathrm{Ker}[\mathfrak{S}(J, n)/(\mathbf{Z}m + J(K)/n) \longrightarrow \bigoplus_{M \in C} H^1(k_M, F_M)/\mathbf{Z}\delta_M([Z])]$$

(the notation $\mathcal{D}^n(X)$ instead of $\mathcal{D}^n(m)$ is legitimate, since the group $\mathfrak{S}(J, n)/(\mathbf{Z}m + J(K)/n)$, hence the above kernel, only depend on the image of m in ${}_nH^1(K, J)$, which is the class of $Z_K = X_K$).

Corollary 4.5.3 *Let notation be as above.*

a) Assume that $n = l$ is a prime number and that $[Z]$ is not divisible by l in $H^1(C, J)$. Then the group ${}_l\mathrm{Br}_{\mathrm{hor}}(X)$ injects into $\mathcal{D}^l(X)$. In particular, if $\mathcal{D}^l(X) = 0$, then ${}_l\mathrm{Br}_{\mathrm{hor}}(X) = 0$, and the whole l-primary part of the Brauer group of X is vertical : $\mathrm{Br}(X)_{\mathrm{vert}}\{l\} = \mathrm{Br}(X)\{l\}$.

b) Assume that k is a number field and $C = \mathbf{A}^1_k$. If ${}_n\mathrm{Br}_{\mathrm{hor}}(X) = 0$, i.e. if $\mathrm{Br}(X)_{\mathrm{vert}}\{l\} = \mathrm{Br}(X)\{l\}$ for each prime l dividing n, then we have $\mathcal{D}^n(X) = 0$.

Proof That $\mathcal{D}^n(X)$ injects into ${}_n\mathcal{D}(X)$ is clear from the definitions. If $n = l$ is prime, one immediately checks that this injection is an isomorphism if $[Z]$ is not divisible by l in $H^1(C, J)$. By the previous theorem, ${}_n\mathrm{Br}_{\mathrm{hor}}(X)$ injects into ${}_n\mathcal{D}(X)$, and under the hypothesis of b), this map is an isomorphism. Since $\mathrm{Br}(X)$ is a torsion group, $\mathrm{Br}(X)/\mathrm{Br}_{\mathrm{vert}}(X)$ is l-torsion free if and only if the inclusion $\mathrm{Br}_{\mathrm{vert}}(X) \subset \mathrm{Br}(X)$ induces an isomorphism on l-primary subgroups. $\square$

4.6 The Brauer group of the Jacobian fibration

We shall now discuss the special case where $X_K(K) \neq \emptyset$. In this subsection, we thus assume $X = J^c$ and $Z = J$.

Let $\mathrm{Br}_0(J) \subset \mathrm{Br}(J)$ be the subgroup consisting of elements which vanish when restricted to the zero section of J/C, and let similarly $\mathrm{Br}_0(J_K) \subset \mathrm{Br}(J_K)$ consist of elements vanishing at $0 \in J_K(K)$. The following proposition gives an *algebraic incarnation* of the elements in $H^1(C, J)$ in terms of the Brauer group of J_K.

Proposition 4.6.1 *The following groups are naturally isomorphic :*

a) the group $H^1(C, J)$ of C-torsors under J ;

b) the group $H^1_{nr}(K, J_K)$ of unramified K-torsors under J_K ;

c) the subgroup of $\mathrm{Br}_0(J_K)$ consisting of elements α such that for every closed point $M \in C$ the image of α in $\mathrm{Br}_0(J_{K^{sh}_M})$ is zero.

Asssume that C is a smooth geometrically integral curve over a field k of characteristic zero. Then these groups also coincide with

d) the subgroup of $\mathrm{Br}_0(J_K)$ consisting of elements whose residues at components of fibres of J^c/C are constant ;

e) the subgroup $\mathrm{Br}_0^{gnr}(J^c_K) \subset \mathrm{Br}_0(J^c_K) = \mathrm{Br}_0(J_K)$ consisting of elements whose image in $\mathrm{Br}(J^c_{K\otimes_k k^s})$ is unramified, i.e. lies in $\mathrm{Br}(J^c \times_k k^s)$. $\square$

The exact sequence
$$0 \to \mathbf{Z} \to D_M \to \Delta_M \to 0$$
is split, and one may identify Δ_M with the permutation module on components which do not meet the zero section $\sigma_0 \subset J$. The commutative square of theorem 4.5.1

$$\begin{array}{ccc} Br^{gnr}(J_K) & \longrightarrow & H^1(C, J) \\ \downarrow & & \downarrow d_M \\ \bigoplus_{Y \subset X_M} H^1(k_Y, \mathbf{Q}/\mathbf{Z}) & \longrightarrow & H^2(k_M, \Delta_M) \end{array}$$

gives here rise to the commutative square

$$\begin{array}{ccc} Br_0^{gnr}(J_K) & \xrightarrow{\simeq} & H^1(C,J) \\ \downarrow & & \downarrow d_M \\ \bigoplus_{Y\subset X_M, Y\cap\sigma_0=\emptyset} H^1(k_Y,\mathbf{Q}/\mathbf{Z}) & \xrightarrow{\simeq} & H^2(k_M,\Delta_M) \end{array}$$

We thus have two ways of viewing the map $H^1(C,J) \to \bigoplus_{Y\subset X_M, Y\cap\sigma_0=\emptyset} H^1(k_Y,\mathbf{Q}/\mathbf{Z})$: from the geometric point of view, it comes from the composition

$$H^1(C,J) \to H^1(k_M,F_M) \to H^2(k_M,\Delta_M),$$

where F_M is the (geometric) group of connected components of the special fibre at M. From the algebraic point of view, where $H^1(C,J)$ is identified with a subgroup of the Brauer group, it corresponds to residue maps at the generic points of components of the special fibre of J^c.

The middle and bottom exact sequences in the main diagram of theorem 4.5.1 are here left and right exact. They are in fact split in a compatible way, the splitting being given by the zero section. From the mentioned diagram one deduces

$$\mathrm{Br}(J^c) \simeq \mathrm{Br}(C) \oplus \mathcal{D}(J^c).$$

4.7 The case under study in this paper : glossary

For the family of elliptic curves $E/\mathbf{P}^1_k$ under consideration in the introduction, let $J_K = E_K$ denote the generic fibre over $K = k(\mathbf{P}^1)$, let J^c/C be the regular minimal model over $C = \mathbf{P}^1_k$, and let J/C be the Néron minimal model.

One easily checks that the singular fibres J^c_M of J^c/C are reduced and consist of two components, which are two smooth curves of genus zero meeting transversally in two points (over the algebraic closure of k_M). The special fibres J_M of J are thus extensions of $F_M = \mathbf{Z}/2$ (with a clearly trivial Galois action) by a one-dimensional k_M-torus. In particular, we have $H^1(k_M,F_M) = k^*_M/k^{*2}_M$. The group ${}_2J/C$ is equal to the constant group scheme $(\mathbf{Z}/2)^2_C$. The map $(K^*/K^{*2})^2 = H^1(K, {}_2J_K) \to {}_2H^1(K,J_K)$ associates to the pair (m_1,m_2) the class of the curve $X(m)$ given by the equations

$$m_1X_1^2 + c_1X_0^2 = m_2X_2^2 + c_2X_0^2 = m_1m_2X_3^2 + c_3X_0^2$$

in $\mathbf{P}^3_K$, which is a principal homogeneous space under J_K.

Easy valuation computations show that the group $\mathfrak{S} \subset (K^*/K^{*2})^2$, resp. $\mathfrak{S}_0 \subset (K^*/K^{*2})^2$, of the introduction coincides with the group $\mathfrak{S}(J/\mathbf{A}^1_k,2) \subset H^1(K,{}_2J_K)$, resp. $\mathfrak{S}(J/\mathbf{P}^1_k,2) \subset H^1(K,{}_2J_K)$. If m lies in $\mathfrak{S}_0$, then $X(m)$ extends to a torsor Z over $\mathbf{P}^1_k$ under J.

Next, one checks that for any point M of bad reduction for J_K/K (hence $M \in \mathbf{A}^1_k$), the composite map

$$\mathfrak{S} = \mathfrak{S}(J/\mathbf{A}^1_k,2) \to {}_2H^1(\mathbf{A}^1_k,J) \xrightarrow{\delta_M} H^1(k_M,F_M) = k^*_M/k^{*2}_M$$

coincides with the map δ_M defined in the introduction.

Let us now look at the statement of the main Theorem. We start from $m \in \mathfrak{S}_0 \subset \mathfrak{S}$. We assume that m is not in the image of ${}_2J_K(K)/2$. If m lies in the image of $J_K(K)$ under the

Kummer map, then the rank of $J_K(K)$ is at least one, and $J_K \simeq X(m)_K$. In this case, rational points are clearly Zariski dense on X.

Let $E/\mathbf{P}^1_k$, m, $X = X(m)$ be as in the main Theorem. Assume that $m \in \mathfrak{S}_0$ does not lie in the image of $J_K(K)/2$. Let us consider the following statements.

(i) Condition (3) (=(D)) of the main Theorem holds.

(ii) $\mathcal{D}^2(X/\mathbf{P}^1_k) = 0$.

(iii) ${}_2\mathcal{D}(X/\mathbf{P}^1_k) = 0$.

(iv) The 2-primary subgroups $\mathrm{Br}_{\mathrm{vert}}(X)\{2\}$ and $\mathrm{Br}(X)\{2\}$ coincide.

Statement (i) holds if and only if (ii) holds and the rank of $J(K)$ is zero. Statement (iii) implies (ii) and the converse holds as soon as the class of Z is not divisible by 2 in $H^1(\mathbf{P}^1_k, J)$. Statement (iii) implies (iv).

Most of this is immediate from subsection 4.5. Let us simply note that the image of $J_K(K)/2$ in $\mathfrak{S}_0 \subset \mathfrak{S}$ lies in the kernel of the map $\mathfrak{S} \to \bigoplus_{M\in T} k_M^*/k_M^{*2}$. If (D) holds, then the inclusion ${}_2J_K(K) \subset J_K(K)$ induces an isomorphism ${}_2J_K(K) \simeq J_K(K)/2$ (see (iii) in the proof of proposition 2.1.3), and the rank of $J_K(K)$ is zero. Note that the class $[Z]$ is not divisible by 2 if $\delta_M(m) \neq 0$ for some $M \in T$.

The situation over the affine line is somewhat simpler.

Let $E/\mathbf{P}^1_k$, m, $X = X(m)$ be as in the main theorem. Assume that $m \in \mathfrak{S}_0$ does not lie in the image of $J_K(K)/2$. Let $X_{\mathrm{aff}} := X \times_{\mathbf{P}^1_k} \mathbf{A}^1_k$.

Let us consider the following statements.

(i) Condition (D_0) in Remark 2.5.4 (iv) holds.

(ii) $\mathcal{D}^2(X_{\mathrm{aff}}/\mathbf{A}^1_k) = 0$.

(iii) ${}_2\mathcal{D}(X_{\mathrm{aff}}/\mathbf{A}^1_k) = 0$.

(iv) The 2-primary subgroups $\mathrm{Br}_{\mathrm{vert}}(X_{\mathrm{aff}})\{2\}$ and $\mathrm{Br}(X_{\mathrm{aff}})\{2\}$ coincide.

Statement (i) holds if and only if (ii) holds and the rank of $J(K)$ is zero. Statement (iii) implies (ii) and the converse holds as soon as the class of Z_{aff} is not divisible by 2 in $H^1(\mathbf{A}^1_k, J)$. Statement (iii) is equivalent to (iv).

Acknowledgements

A. N. Skorobogatov acknowledges support from Centre National de la Recherche Scientifique, Ecole Normale Supérieure (Paris) and the Russian Foundation for Basic Research (project 96-01-01378). He also thanks l'Institut de Mathématiques de Luminy and l'Université de Paris-Sud for their hospitality.

REFERENCES

[Art86] M. Artin, Néron models, in *Arithmetic geometry*, G. Cornell and J. Silverman ed., Springer (1986) 213-230.

[ANT67] *Algebraic number theory*, J. W. S. Cassels and A. Fröhlich ed., Academic Press (London, 1967).

[BBD82] A. A. Beilinson, J. Bernstein, P. Deligne, Faisceaux pervers, in *Analyse et topologie sur les espaces singuliers*, vol. **I**, Astérisque **100** (1982).

[BPV84] W. Barth, C. Peters, A. Van de Ven, *Compact complex surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band **4**, Springer-Verlag 1984.

[BLR90] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band **21**, Springer-Verlag 1990.

[Cass62] J. W. S. Cassels, Arithmetic on Curves of Genus One. IV. Proof of the Hauptvermutung, J. reine angew. Math. **211** (1962) 95-112.

[CT97] J.-L. Colliot-Thélène, The Hasse principle in a pencil of algebraic varieties, in Proceedings of a conference held at Tiruchirapalli, India, January 1996, K. Murty and M. Waldschmidt ed., to appear in the Contemporary Mathematics series of the A.M.S.

[CT/SwD94] J.-L. Colliot-Thélène and Sir Peter Swinnerton-Dyer, Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, J. reine angew. Math. **453** (1994) 49-112.

[CT/Sk/SwD97a] 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.

[CT/Sk/SwD97b] J.-L. Colliot-Thélène, A. N. Skorobogatov and Sir Peter Swinnerton-Dyer, Rational points and zero-cycles on fibred varieties : Schinzel's hypothesis and Salberger's device, Prépublication **97-03**, Université de Paris-Sud.

[Gr68] A. Grothendieck, Le groupe de Brauer I, II, III, in *Dix exposés sur la cohomologie des schémas*, Masson & Cie, Paris, North-Holland, Amsterdam, 1968.

[Ha94] D. Harari, Méthode des fibrations et obstruction de Manin, Duke Math. J. **75** (1994) 221-260.

[Milne86] J. S. Milne, Arithmetic Duality Theorems, Perspect. Math. **1**, Academic Press, Boston, 1986.

[Ray70] M. Raynaud, Spécialisation du foncteur de Picard, Publ. Math. I. H. E. S. **38** (1970) 27-76.

[Schn79] P. Schneider, Über gewisse Galoiscohomologiegruppen, Math. Zeit. **168** (1979) 180-205.

[Sha66] I. R. Shafarevich, *Lectures on minimal models and birational transformations of two-dimensional schemes*, Tata Institute of Fundamental Research, **37**, Bombay, 1966.

[Sk96] A. N. Skorobogatov, Descent on fibrations over the projective line, Amer. J. Math. **118** (1996) 905-923.

[SwD94] Sir Peter Swinnerton-Dyer, Rational points on pencils of conics and on pencils of quadrics, J. London Math. Soc. (2) **50** (1994) 231-242.

[SwD95] Sir Peter Swinnerton-Dyer, Rational points on certain intersections of two quadrics, in *Abelian varieties*, Barth, Hulek and Lange ed., Walter de Gruyter, Berlin, New York, 1995.

[Ta72] J. Tate, Algorithm for determining the type of a singular fibre in an elliptic pencil, in *Modular Functions of One Variable IV*, B. J. Birch and W. Kuyk ed., Lecture Notes in Math. 476, Springer-Verlag 1975.

J.-L. Colliot-Thélène,

C.N.R.S.,
URA D0752, Mathématiques,
Bâtiment 425,
Université de Paris-Sud,
F-91405 Orsay
France

e-mail : colliot@math.u-psud.fr

A. N. Skorobogatov,

Institute for Problems of Information Transmission,
Russian Academy of Sciences,
19, Bolshoi Karetnyi
Moscow 101447
Russia

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-53225 Bonn
Deutschland

e-mail : skoro@mpim-bonn.mpg.de

Sir Peter Swinnerton-Dyer,

Isaac Newton Institute,
20 Clarkson Road,
Cambridge CB3 0EH
United Kingdom

e-mail : hpfs100@newton.cam.ac.uk