Beyond the Manin obstruction

Alexei N. Skorobogatov

1. Introduction

Let X be a smooth variety over a field k, and $\mathrm{Br}(X)$ be the (cohomological) Brauer–Grothendieck group of X, $\mathrm{Br}(X) = H^2(X, \mathbf{G}_m)$. Let $\overline{k}$ be a separable closure of k, $G = Gal(\overline{k}/k)$, and let $\overline{X} = X \times_k \overline{k}$. Let $\mathrm{Br}_0(X)$ (resp. $\mathrm{Br}_1(X)$) be the image of the natural map $\mathrm{Br}(k) \to \mathrm{Br}(X)$ (resp. the kernel of the natural map $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})^G$). For any extension K/k let

$$X(K) \times \mathrm{Br}(X) \to \mathrm{Br}(K), \quad (A, P) \mapsto A(P)$$

be the pairing obtained by specializing elements of $\mathrm{Br}(X)$ at K-rational points. Now let k be a number field, Ω the set of places of k, $\mathbf{A}_k$ the adèle ring of k. Let

$$\mathrm{inv}_v : \mathrm{Br}(k_v) \hookrightarrow \mathbf{Q}/\mathbf{Z}$$

be the local invariant. In [M] Manin considered the pairing between $\mathrm{Br}(X)$ and $X(\mathbf{A}_k)$ with values in $\mathbf{Q}/\mathbf{Z}$ given by

$$\sum_{v \in \Omega} \mathrm{inv}_v(A(P_v)),$$

for $A \in \mathrm{Br}(X)$, $\{P_v\} \in X(\mathbf{A}_k)$, the sum which is well known to be finite (for almost all v the specialization $A(P_v)$ belongs to $\mathrm{Br}(\mathcal{O}_v) = 0$). By the global reciprocity this pairing is trivial on the algebras coming from $\mathrm{Br}(k)$, so it could be regarded as a pairing

$$\mathrm{Br}(X)/\mathrm{Br}_0(X) \times X(\mathbf{A}_k) \to \mathbf{Q}/\mathbf{Z}.$$

We shall call this *the Brauer–Manin pairing*. Let us define $X(\mathbf{A}_k)^{\mathrm{Br}}$ as "the right kernel" of this pairing, that is, the subset of points of $X(\mathbf{A}_k)$ orthogonal to all elements of $\mathrm{Br}(X)$. Manin made an important observation that by the global reciprocity law the image of $X(k)$ under the diagonal embedding $X(k) \hookrightarrow X(\mathbf{A}_k)$ is contained in $X(\mathbf{A}_k)^{\mathrm{Br}}$. A variety X such that $X(\mathbf{A}_k) \neq \emptyset$ whereas $X(k) = \emptyset$ is *a counterexample to the Hasse principle*. Such a counterexample is accounted for by *the Manin obstruction* if already $X(\mathbf{A}_k)^{\mathrm{Br}}$ is empty. For a long time most known counterexamples to the Hasse principle could be explained by means of the Manin obstruction (to the best of my knowledge the case of the Bremner–Lewis–Morton curve $3x^4 + 4y^4 - 19z^4 = 0$ remains undecided). Recently Sarnak and L.Wang [SW] showed that the Manin obstruction is not the only obstruction to the Hasse principle for smooth hypersurfaces of degree 1130 in $\mathbf{P}^4_{\mathbf{Q}}$ if one assumes Lang's conjecture that $X(\mathbf{Q})$ is finite if $X_{\mathbf{C}}$ is hyperbolic.

The aim of this note is to construct a smooth proper surface over $k = \mathbf{Q}$ of Kodaira dimension 0 which is a counterexample to the Hasse principle but for which the Manin obstruction is not sufficient to explain the absence of $\mathbf{Q}$-rational points. We exploit the same kind of surfaces which has been recently used to produce counterexamples to a conjecture of Mazur [AA]. These surfaces are quotients of a product of two curves of genus one by a fixed point free involution.

Although in our example the Manin obstruction fails to provide a finite decision process for determining the existence of rational points there still is such a process. We propose a refinement of the Manin obstruction and show that for surfaces of our type it is the only obstruction to the Hasse principle. To define it we use a combination of the Manin obstruction and a descent very similar to the classical descent on elliptic curves. The point is that unlike in that classical case in the case of surfaces the Brauer group can become substantially bigger after passing to a finite unramified covering, thus the Manin obstruction can become finer.

We construct our example in Section 2. A refinement of the Manin obstruction is defined in Section 3. There we also formulate the underlying descent statement, which is then proved in Section 4. The construction of the example relies on the existence of elliptic curves over $\mathbf{Q}$ with no rational 2-torsion and an element of exact order 4 in the Tate–Shafarevich group. In the appendix to this paper S. Siksek writes down explicitly an everywhere locally soluble 4-covering of the curve $y^2 = x^3 - 1221$, and shows that it does represent an element of exact order 4.

2. A counterexample to the Hasse principle not accounted for by the Manin obstruction

Let J be an elliptic curve over $\mathbf{Q}$ whose Tate-Shafarevich group $Ш(J)$ contains an element of order 4, and such that J contains no non-trivial point of order 2 defined over $\mathbf{Q}$. For example, take J to be the curve

$$y^2 = x^3 - 1221.$$

Then $J(\mathbf{Q}) = 0$ and $Ш(J) = \mathbf{Z}/4 \times \mathbf{Z}/4$ (the last property is conditional on the Birch - Swinnerton-Dyer conjecture, [GPZ], Tables 3 and 4). We shall only use the (unconditional) result proved in the appendix to this paper that $Ш(J)$ contains an element of exact order 4. Let C' be a principal homogeneous space under J whose class $[C'] \in H^1(\mathbf{Q}, J)$ belongs to $Ш(J)$ and has exact order 4.

Let C be a principal homogeneous space under J such that $[C] = 2[C']$. Let $\xi : C' \to C$ be the corresponding unramified Galois covering with Galois group $J[2]$. In particular, the inverse image on the Jacobians, $\xi^* : J \to J$, is multiplication by 2.

By a lemma of Swinnerton-Dyer ([B/SwD], Lemmas 1 and 2, [C], IV, Thm. 1.3) any element of order 2 in $Ш(J)$ can be represented as a double cover of $\mathbf{P}^1_{\mathbf{Q}}$. In particular, C can be given by the equation

$$u^2 = g(t)$$

for some polynomial $g(t)$ of degree 4 with integral coefficients (see (A.2) for an explicit expression of $g(t)$). Let $\sigma : C \to C$ be the corresponding hyperelliptic involution. In particular, σ_* acts on the Jacobian J of C as multiplication by -1.

Let us fix once and for all two monic quadratic polymomials $p(x)$ and $q(x)$ with integer coefficients such that $Res(p(x), q(x)) = \pm 1$, and such that both $p(x)$ and $q(x)$ take only positive values on $\mathbf{Q}$. Let $D \subset \mathbf{P}^3_{\mathbf{Q}}$ be the smooth proper curve of genus one given by its affine equations

$$y^2 = p(x), \;\; z^2 = q(x).$$

This curve D has obvious rational points at infinity. We fix one of them, say, Q, and take it as the neutral element of the group law on D.

Let $\rho : D \to D$ be the involution sending (x, y, z) to $(x, -y, -z)$. One sees easily that ρ has no fixed point. Then $D' = D/\rho$ is an elliptic curve given by

$$w^2 = p(x)q(x).$$

Let $\psi : D \to D'$ be the natural surjection. Take $Q' = \psi(Q)$ as the neutral element for the group law on D'. Then ψ becomes an isogeny whose kernel is generated by a point of order 2. In particular, the action of ρ_* on the Jacobian of D is trivial. (After the choice of Q and Q' we can identify D and D' with their Jacobians.)

Let X be the quotient of $Y = C \times D$ by the fixed point free involution (σ, ρ), $f : Y \to X$. This is a surface classically known as hyperelliptic (or bielliptic), see [Sh], Ch. VII.8, [B], Ch. VI. Its geometric invariants are $\kappa = 0$, $p_g = 0$, $q = 1$, $(K_X^2) = 0$, $b_1 = b_2 = 2$. (Recall that surfaces with such invariants together with $K3$, Enriques and Abelian surfaces exhaust all surfaces of Kodaira dimension zero.) An affine model of X can be given by equations

$$y^2 = g(t)p(x), \ z^2 = g(t)q(x). \tag{2.1}$$

Finally, let $Y' = C' \times D$, and let $\pi : Y' \to D$ be the second projection. Let $f' : Y' \to X$ be the composition of the unramified covering $(\xi, Id) : Y' \to Y$ with f.

Theorem. (a) *We have* $X(\mathbf{Q}) = \emptyset$.

(b) $f'^*(\mathrm{Br}(X)) \subset \mathrm{Br}(Y')$ *is contained in* $\pi^*(\mathrm{Br}(D))$. *Therefore for any* $R \in D(\mathbf{Q})$, *and any* $\{P_v\} \in C'(\mathbf{A_Q})$, *the map* f' *sends* $\{(P_v, R)\} \in Y'(\mathbf{A_Q})$ *to* $X(\mathbf{A_Q})^{\mathrm{Br}}$, *in particular we have* $X(\mathbf{A_Q})^{\mathrm{Br}} \neq \emptyset$.

Proof. (a) An easy valuation argument (the same as in [AA], Prop. 5.1) shows that for any prime p and any $\mathbf{Q}_p$-rational point of X for which $yz \neq 0$ the p-adic valuation $val_p(g(t))$ is even. Thus $g(t) = \pm 1$ modulo squares in $\mathbf{Q}^*$. This extends to the whole of X (see *loc. cit.*), and we get a decomposition

$$X(\mathbf{Q}) = f(Y(\mathbf{Q})) \cup f^-(Y^-(\mathbf{Q})),$$

where $f^- : Y^- = C^- \times D^- \to X$ is a "twisted form" of f, and C^- (resp. D^-) is obtained by inverting the sign of $g(t)$ (resp. of $p(x)$ and $q(x)$). Note that $Y = C \times D$ clearly has no rational point since $C(\mathbf{Q})$ is empty. The curve D^- given by the equations $y^2 + p(x) = z^2 + q(x) = 0$ has no real point by the positivity condition on $p(x)$ and $q(x)$, hence Y^- has no real point. This completes the proof of (a).

(b) The second statement of (b) follows from the first one : by projection formula it is enough to show that $\{(P_v, R)\}$ is Brauer–Manin orthogonal to $f'^*(\mathrm{Br}(X))$, and this follows from the first statement by the global reciprocity law.

Our first goal will be to study $f^*(\mathrm{Br}(X))$.

Consider the Hochschild–Serre spectral sequence ([Mi2], III.2.20) :

$$H^p(G, H^q(\overline{X}, \mathbf{G}_m)) \Rightarrow H^{p+q}(X, \mathbf{G}_m) \tag{2.2}$$

When $H^0(\overline{X}, \mathbf{G}_m) = \overline{k}^*$, for example when X is proper, the exact sequence of low degree terms writes down as follows :

$$0 \to \mathrm{Br}_0(X) \to \mathrm{Br}_1(X) \to H^1(G, Pic(\overline{X})) \to H^3(\mathbf{Q}, \mathbf{G}_m) = 0,$$

where the last equality is provided by the class field theory (and holds also with $\mathbf{Q}$ replaced by any number field or any local field). We shall employ the notation $r : \mathrm{Br}_1(X) \to H^1(G, Pic(\overline{X}))$ for the corresponding canonical map.

For surfaces the structure of $\mathrm{Br}(\overline{X})$ was determined by Grothendieck ([G], II, Cor. 3.4, III, (8.12)) : the divisible subgroup $\mathrm{Br}(\overline{X})_{div}$ is isomorphic to $(\mathbf{Q}/\mathbf{Z})^{b_2-\rho}$ as an abelian group, and the quotient $\mathrm{Br}(\overline{X})/\mathrm{Br}(\overline{X})_{div}$ is isomorphic to $Hom(NS(\overline{X})_{tors}, \mathbf{Q}/\mathbf{Z})$ as a G-module. Here $b_2 = rk(H^2(X_{\mathbf{C}}, \mathbf{Z}))$, $\rho = cork(Pic(\overline{X}) \otimes \mathbf{Q}/\mathbf{Z})$, and $NS(\overline{X})$ is the Néron–Severi group of $\overline{X}$, finitely generated and isomorphic to the quotient of $Pic(\overline{X})$ by its divisible subgroup. Since in our case the geometric genus of X is zero, we have $b_2 = \rho$, hence $\mathrm{Br}(\overline{X})$ is dual to the torsion subgroup of $NS(\overline{X})$.

We now analyse the structure of the G-module $Pic(\overline{X})$ and of the map $f^* : Pic(\overline{X}) \to Pic(\overline{Y})$.

Consider the following commutative diagram :

$$
\begin{array}{ccccc}
C & \xleftarrow{\pi_1} & Y & \xrightarrow{\pi_2} & D \\
\downarrow & & f \downarrow & & \psi \downarrow \\
\mathbf{P}^1_{\mathbf{Q}} & \longleftarrow & X & \longrightarrow & D'
\end{array}
$$

Here $X \to D'$ is the Albanese map ([AA], Prop. 3.1 (3)). Let $\psi^* : D' \to D$ be the isogeny dual to $\psi : D \to D'$. By the choice of $Q' \in D'(\mathbf{Q})$ the G-module $D'(\overline{k})$ is identified with $Pic^0(\overline{X})$. Let Γ be the cyclic group of automorphisms of Y generated by (σ, ρ). Since $f^* : Pic(\overline{X}) \to Pic(\overline{Y})$ factors through the inclusion $Pic(\overline{Y})^\Gamma \hookrightarrow Pic(\overline{Y})$ we get a commutative diagram of G-modules with exact rows :

$$
\begin{array}{ccccccccc}
0 & \to & D'(\overline{k}) & \to & Pic(\overline{X}) & \to & NS(\overline{X}) & \to & 0 \\
 & & {\scriptstyle (0,\psi^*)} \downarrow & & {\scriptstyle f^*} \downarrow & & {\scriptstyle f^*} \downarrow & & \\
0 & \to & J[2](\overline{k}) \times D(\overline{k}) & \to & Pic(\overline{Y})^\Gamma & \to & NS(\overline{Y})^\Gamma & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & J(\overline{k}) \times D(\overline{k}) & \to & Pic(\overline{Y}) & \to & NS(\overline{Y}) & \to & 0
\end{array}
\tag{2.3}
$$

We used the fact that (σ_*, ρ_*) acts on the product of two Jacobians $J(\overline{k}) \times D(\overline{k})$ as multiplication by $(-1, 1)$.

Lemma 1. *There is an isomorphism of G-modules $NS(\overline{X})_{tors} = J[2](\overline{k})$.*

Proof. Let us denote the kernel of $f^* : NS(\overline{X}) \to NS(\overline{Y})$ by K. Since $NS(\overline{Y})$ is torsion-free, we have $NS(\overline{X})_{tors} = K_{tors}$. Thus it will be enough to show that the G-modules K and $J[2]$ are isomorphic. The Hochschild–Serre spectral sequence

$$H^p(\Gamma, H^q(\overline{Y}, \mathbf{G}_m)) \Rightarrow H^{p+q}(\overline{X}, \mathbf{G}_m)$$

yields an exact sequence

$$0 \to H^1(\Gamma, \overline{\mathbf{Q}}^*) \to Pic(\overline{X}) \xrightarrow{f^*} Pic(\overline{Y})^\Gamma \to H^2(\Gamma, \overline{\mathbf{Q}}^*)$$

We have $H^1(\Gamma, \overline{\mathbf{Q}}^*) = Hom(\Gamma, \overline{\mathbf{Q}}^*) = \mathbf{Z}/2$, and $H^2(\Gamma, \overline{\mathbf{Q}}^*) = 0$ by periodicity. On the other hand, $Ker(\psi^*) = \mathbf{Z}/2$. The snake lemma applied to the upper part of diagram (2.3) now gives rise to the exact sequence of G-modules

$$0 \to \mathbf{Z}/2 \to \mathbf{Z}/2 \to K \to J[2] \to 0.$$

This proves Lemma 1. QED

Corollary. *We have* $\mathrm{Br}(\overline{X})^G = 0$, *thus* $\mathrm{Br}(X) = \mathrm{Br}_1(X)$.

Proof. This follows from Lemma 1 since $\mathrm{Br}(\overline{X})^G = Hom_G(J[2](\overline{k}), \mathbf{Z}/2) = 0$. QED

Lemma 2. *The group* $f^*(\mathrm{Br}(X))/\mathrm{Br}_0(Y) \subset \mathrm{Br}_1(Y)/\mathrm{Br}_0(Y) = H^1(G, Pic(\overline{Y}))$ *is contained in the image of* $H^1(\mathbf{Q}, J)[2] \times H^1(\mathbf{Q}, D)$ *under the map induced by the natural inclusion* $J(\overline{k}) \times D(\overline{k}) = Pic^0(\overline{Y}) \hookrightarrow Pic(\overline{Y})$.

Proof. By Corollary we have a canonical functorial isomorphism

$$\mathrm{Br}(X)/\mathrm{Br}_0(X) \xrightarrow{=} H^1(G, Pic(\overline{X})).$$

By functoriality of spectral sequence (2.2) we have to consider the subgroup of $\mathrm{Br}_1(Y)/\mathrm{Br}_0(Y)$ isomorphic to the image of the map

$$f^* : H^1(G, Pic(\overline{X})) \to H^1(G, Pic(\overline{Y})).$$

Observe that $NS(\overline{Y})^\Gamma \subset NS(\overline{Y})$ is torsion free. We have $f_*f^*(x) = 2x$, for any $x \in NS(\overline{X})$, and $y+(\sigma,\rho)y = f^*f_*(y)$, for any $y \in NS(\overline{Y})$. Therefore the G-modules $NS(\overline{X})\otimes\mathbf{Q}$ and $NS(\overline{Y})^\Gamma\otimes\mathbf{Q}$ are isomorphic. Since $X_{\mathbf{C}}$ has second Betti number $b_2 = 2$, we have $dim(NS(\overline{Y})^\Gamma \otimes \mathbf{Q}) = 2$. The classes of fibres of canonical projections $\pi_1 : \overline{Y} \to \overline{C}$ and $\pi_2 : \overline{Y} \to \overline{D}$ give two linearly independent G-invariant elements of this vector space, implying that it carries trivial G-action. Thus $NS(\overline{Y})^\Gamma = \mathbf{Z} \oplus \mathbf{Z}$ as a G-module. Consider again diagram (2.3). Note that on replacing $NS(\overline{Y})^\Gamma$ by the image of $Pic(\overline{Y})^\Gamma \to NS(\overline{Y})^\Gamma$ we obtain from (2.3) a commutative diagram whose middle row is right exact. This image is a submodule of $NS(\overline{Y})^\Gamma = \mathbf{Z} \oplus \mathbf{Z}$, and hence is a free abelian group with trivial G-action. Since $H^1(G, \mathbf{Z}) = 0$ the modified diagram (2.3) gives rise to the following commutative diagram with exact rows :

$$\begin{array}{ccccc}
H^1(\mathbf{Q}, D') & \to & H^1(G, Pic(\overline{X})) & \to & H^1(G, NS(\overline{X})) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(\mathbf{Q}, J[2]) \times H^1(\mathbf{Q}, D) & \to & H^1(G, Pic(\overline{Y})^\Gamma) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow \\
H^1(\mathbf{Q}, J) \times H^1(\mathbf{Q}, D) & \to & H^1(G, Pic(\overline{C} \times \overline{D})) & \to & H^1(G, NS(\overline{Y}))
\end{array}$$

The statement of Lemma 2 follows from the commutativity of this diagram. QED

Now we can finish the proof of the theorem.

We claim that the group $f'^*(\mathrm{Br}(X))/\mathrm{Br}_0(Y') \subset \mathrm{Br}_1(Y')/\mathrm{Br}_0(Y) = H^1(G, Pic(\overline{Y'}))$ is contained in the image of $H^1(\mathbf{Q}, D)$ under the map induced by the natural inclusion $J(\overline{k}) \times D(\overline{k}) = Pic^0(\overline{Y'}) \hookrightarrow Pic(\overline{Y'})$. After Lemma 2 and by functoriality of spectral sequence (2.2) in order to prove this we only have to remark that the inverse image map $Pic^0(\overline{Y}) \to Pic^0(\overline{Y'})$ is multiplication by $(2, 1)$ on $J(\overline{k}) \times D(\overline{k})$. The first statement of (b) now follows. The theorem is proved. QED

J.-L. Colliot-Thélène conjectured that the Manin obstruction to the Hasse principle for zero-cycles of degree one is the only obstruction for all varieties over a number field k ([CT], Conj. 1.5 (a), this statement was also formulated and discussed by S. Saito in [Sa], Sect. 8). This would imply the existence of a K-point on X for some odd degree extension $K/\mathbf{Q}$.

3. Refinement of the Manin obstruction

Let us now combine the theory of descent and Manin's treatment of the Brauer–Grothendieck group to define an "iterated Manin obstruction". The descent with respect to algebraic tori and its relation to the algebraic part of the Manin obstruction was studied in detail by J.-L. Colliot-Thélène and J.-J. Sansuc [CS]. We follow this work in a more general context of groups of multiplicative type, which also covers the classical descent on abelian varieties.

Let X be a variety over a number field k. A reasonable class of varieties for which the descent method works well are those satisfying the condition

$$H^0(\overline{X}, \mathbf{G}_m) = \overline{k}^*. \tag{3.1}$$

This condition is satisfied by all proper varieties.

Let M be a finitely generated G-module, and let $S = Hom_{k-groups}(M, \mathbf{G}_m)$ be the k-group of multiplcative type dual to M. There are two important cases : if M is finite, then S is finite, and if M is torsion-free, then S is an algebraic k-torus.

The obstruction that we are going to define is attached to a G-homomorphism

$$\lambda : M \longrightarrow Pic(\overline{X}).$$

Let $\mathrm{Br}_\lambda(X) := r^{-1}\lambda_*(H^1(G, M)) \subset \mathrm{Br}_1(X)$ (the map r comes from spectral sequence (2.2)), and define $X(\mathbf{A}_k)^{\mathrm{Br}_\lambda} \subset X(\mathbf{A}_k)$ as the set of adelic points orthogonal to $\mathrm{Br}_\lambda(X)$ with respect to the Brauer–Manin pairing.

If Y is an X-torsor under S, and $\sigma \in H^1(X, S)$, then the "twist" $f_\sigma : Y_\sigma \to X$ is defined as the X-torsor under S whose class is $[Y_\sigma] = [Y] - \sigma \in H^1(X, S)$.

For $p : X \to Spec(k)$ satisfying (3.1) there is the following fundamental exact sequence ([CS], Thm. 1.5.1) :

$$0 \to H^1(k, S) \to H^1(X, S) \to Hom_G(M, Pic(\overline{X})) \xrightarrow{\partial} H^2(k, S) \to H^2(X, S) \tag{3.2}$$

This is the sequence of low degree terms of the spectral sequence

$$Ext^p_k(M, R^q p_* \mathbf{G}_m) \Rightarrow Ext^{p+q}_X(p^* M, \mathbf{G}_m).$$

If Y is an X-torsor under S, then the image of the class of Y under the map $H^1(X, S) \to Hom_G(M, Pic(\overline{X}))$ in (3.2) is called *the type* of Y. By (3.2) a torsor of a given type is unique up to twist by an element of $H^1(k, S)$.

Proposition. (a) *Let X be a smooth geometrically integral variety over a number field k satisfying condition (3.1). Suppose that $X(\mathbf{A}_k)^{\mathrm{Br}_\lambda} \neq \emptyset$. Then there exists an X-torsor Y under S of type λ, $f : Y \to X$, such that*

$$X(\mathbf{A}_k)^{\mathrm{Br}_\lambda} = \cup_{\sigma \in H^1(k,S)} f_\sigma(Y_\sigma(\mathbf{A}_k)).$$

(b) *When X is proper there exists a finite subset $\Sigma \subset H^1(k, S)$ such that*

$$X(\mathbf{A}_k)^{\mathrm{Br}_\lambda} = \cup_{\sigma \in \Sigma} f_\sigma(Y_\sigma(\mathbf{A}_k)), \quad X(k) = \cup_{\sigma \in \Sigma} f_\sigma(Y_\sigma(k)).$$

(c) *Suppose there exists an X-torsor Y under S of type λ such that $Y_\sigma(\mathbf{A}_k) \neq \emptyset$, then $X(\mathbf{A}_k)^{\mathrm{Br}_\lambda} \neq \emptyset$.*

The proof will be given in the next section.

We define an iterated version of the Manin obstruction related to $\lambda : M \to Pic(\overline{X})$ as follows. Define

$$X(\mathbf{A}_k)^{\lambda} := \cup_{\sigma \in H^1(k,S)} f_\sigma(Y_\sigma(\mathbf{A}_k)^{\mathrm{Br}}).$$

For each $\sigma \in H^1(k,S)$ we have the following obvious inclusions :

$$Y_\sigma(k) \subset Y_\sigma(\mathbf{A}_k)^{\mathrm{Br}} \subset Y_\sigma(\mathbf{A}_k)^{f_\sigma^*(\mathrm{Br}(X))} \subset Y_\sigma(\mathbf{A}_k).$$

Applying f_σ and taking the union for all $\sigma \in H^1(k,S)$ we obtain

$$X(k) \subset X(\mathbf{A}_k)^\lambda \subset X(\mathbf{A}_k)^{\mathrm{Br}} \subset X(\mathbf{A}_k)^{\mathrm{Br}_\lambda} \subset X(\mathbf{A}_k).$$

Thus the emptiness of $X(\mathbf{A}_k)^\lambda$ is an obstruction to the Hasse principle which is a refinement of the Manin obstruction related to the whole of $\mathrm{Br}(X)$.

In our example consider $D \in Div(X)$ such that the divisor of the function $g(t)$ on X is $2D$ (cf. (2.1)). Let $\lambda : \mathbf{Z}/2 \hookrightarrow Pic(\overline{X})$ be the inclusion of the cyclic subgroup generated by D. Then $f: Y \to X$ is "a torsor of type λ" (by the local description of torsors, [CS], 2.3, 2.4.1). By the proof of the assertion (a) of the theorem, we can take $\Sigma = \{1\} \subset H^1(\mathbf{Q}, \mathbf{Z}/2) = \mathbf{Q}^*/\mathbf{Q}^{*2}$. We have $Y(\mathbf{A_Q})^{\mathrm{Br}} = \emptyset$ since the Manin obstruction is the only obstruction to the Hasse principle for curves of genus one. This implies $X(\mathbf{A_Q})^\lambda = \emptyset$, whereas $X(\mathbf{A_Q})^{\mathrm{Br}} \neq \emptyset$ by assertion (b) of the theorem.

The proposition implies that if the descent varieties Y_σ's have the property that the Manin obstruction associated to some finite subgroup of $\mathrm{Br}(Y_\sigma)/\mathrm{Br}_0(Y_\sigma)$ is the only obstruction to the Hasse principle, then there still is a finite process to decide whether $X(k)$ is empty or not. This is what happens for varieties X given by (2.1) : testing the Manin obstruction on Y is reduced to testing it on C and D. By the classical result of Manin ([M], Thm. 6) one is led to consider the conjecturally finite group $Ш(J)$, and check whether there is $\beta \in Ш(J)$ such that the Cassels–Tate pairing $< [C], \beta >$ is not zero. By the conjectural non-degeneracy of the Cassels–Tate pairing ([Mi], Thm. 6.13 (a)) such a β exists if and only if $[C] = 0$, that is, precisely when C has rational points. If $[C] \neq 0$, then the Manin obstruction on C is not empty, *a fortiori* the same is true for Y.

4. Descent with respect to groups of multiplicative type

In this section we summarize the analysis of relations between X-torsors under multiplicative groups and the algebraic part of $\mathrm{Br}(X)$ undertaken in [CS]. Our treatment is somewhat more general since we do not assume that the elementary obstruction for the existence of k-points on X vanishes.

The statement *(ii)* of the following lemma is a complement to [CS] clarifying the relation between the fundamental exact sequence (3.2) and the sequence of low degree terms of (2.2). It also provides an explicit construction of Azumaya algebras as cup-products via the pairing

$$H^1(k,M) \times H^1(X,S) \xrightarrow{(p^*,id)} H^1(X,M) \times H^1(X,S) \to \mathrm{Br}(X).$$

Recall that $r : \mathrm{Br}_1(X) \to H^1(G, Pic(\overline{X}))$ is the canonical map from spectral sequence (2.2).

Lemma 3. *Let X be a variety over a field k satisfying (3.1), M be a finitely generated G-module, S be the dual k-group of multiplicative type. Let $\lambda \in Hom_k(M, Pic(\overline{X}))$. Suppose there exists an X-torsor T under S of type λ. Then for $\alpha \in H^1(k,M)$ we have*

(i) $p^*(\alpha) \cup [T] \in \mathrm{Br}_1(X)$,

(ii) $r(p^*(\alpha) \cup [T]) = \lambda_*(\alpha)$,

(iii) let $A = p^*(\alpha) \cup [T] \in H^2(X, \mathbf{G}_m)$, then for $P \in X(k)$ the specialization $A(P) \in \mathrm{Br}(k)$ equals $\alpha \cup T(P)$ with respect to the natural pairing $H^1(k,M) \times H^1(k,S) \to \mathrm{Br}(k)$,

(iv) for any $A \in \mathrm{Br}_\lambda(X)$ and any $\alpha \in H^1(k,M)$ such that $r(A) = \lambda_*(\alpha)$, there exists $a_0 \in \mathrm{Br}(k)$ such that for any point $P \in X(K)$ over an extension $k \subset K$ we have

$$Res_{k,K}(\alpha) \cup T(P) = A(P) + Res_{k,K}(a_0) \quad \in \mathrm{Br}(K).$$

Proof. (i) is trivial.

(ii) We have $Ext^n_X(p^*M, \mathbf{G}_m) = H^n(X,S)$ ([CS], Prop. 1.4.1), and also $Ext^n_X(\mathbf{Z}, p^*M) = H^n(X, p^*M)$. There are Yoneda cup-products

$$H^1(X, p^*M) \times Ext^n_X(p^*M, \mathbf{G}_m) \to H^{n+1}(X, \mathbf{G}_m) \tag{4.1}$$

and

$$H^1(k, M) \times Ext^n_k(M, Pic(\overline{X})) \to H^{n+1}(k, Pic(\overline{X})). \tag{4.2}$$

Let

$$0 \to M \to N \to \mathbf{Z} \to 0 \tag{4.3}$$

be an exact sequence of G-modules whose class in $Ext^1_k(\mathbf{Z}, M) = H^1(G, M)$ is α. Let d be the connecting homomorphism in the long exact sequence of Ext's in the first variable assotiated to (4.3). By the definition of Yoneda cup-product (4.1), for $\xi \in Ext^n_X(p^*M, \mathbf{G}_m)$ we have $p^*(\alpha) \cup \xi = d(\xi)$. In case of (4.2) we have for $\zeta \in Ext^n_k(M, Pic(\overline{X}))$ the analogous formula $\alpha \cup \zeta = d(\zeta)$.

We claim that there is the following commutative diagram :

$$\begin{array}{ccc} Ext^1_X(p^*M, \mathbf{G}_m) & \longrightarrow & Hom_k(M, Pic(\overline{X})) \\ {\scriptstyle d}\downarrow & & {\scriptstyle d}\downarrow \\ \mathrm{Br}_1(X) & \longrightarrow & H^1(G, Pic(\overline{X})) \end{array} \tag{4.4}$$

Here the upper arrow is the map in (3.1) which associates to a torsor its type, and the lower arrow is the map r obtained from the spectral sequence (2.2). The statement *(ii)* is a consequence of the commutativity of this diagram.

In order to prove this commutativity it will be convenient to place ourselves in a more general context. Let

$$0 \to A \to B \to C \to 0 \tag{4.5}$$

be an exact sequence of G-modules. Let $\mathcal{D}^+$ be the derived category of bounded below complexes of G-modules, and

$$\ldots \to C^\bullet[-1] \to A^\bullet \to B^\bullet \to C^\bullet \to \ldots$$

be the corresponding distinguished triangle in $\mathcal{D}^+$. For any $F \in \mathcal{D}^+$, $i \in \mathbf{Z}$, the truncation functors provide distinguished triangles

$$\ldots \to \tau_{\leq i}(F) \to F \to \tau_{\geq i+1}(F) \to \ldots$$

We have a commutative diagram

$$(4.6)\qquad \begin{array}{ccc} Hom(A^\bullet, F) & \longrightarrow & Hom(A^\bullet, \tau_{\geq 1}(F)) \\ {\scriptstyle d}\downarrow & & {\scriptstyle d}\downarrow \\ Hom(C^\bullet, F)[1] & \longrightarrow & Hom(C^\bullet, \tau_{\geq 1}(F))[1] \end{array}$$

Applying this to $F = \tau_{\leq 1}(Rp_*\mathbf{G}_m)$ and the sequence (4.3) as (4.5) we obtain the commutative diagram

$$\begin{array}{ccc} Hom(M^\bullet, \tau_{\leq 1}(Rp_*\mathbf{G}_m)) & \longrightarrow & Hom(M^\bullet, \tau_{\geq 1}(\tau_{\leq 1}(Rp_*\mathbf{G}_m))) \\ {\scriptstyle d}\downarrow & & {\scriptstyle d}\downarrow \\ \tau_{\leq 1}(Rp_*\mathbf{G}_m)[1] & \longrightarrow & \tau_{\geq 1}(\tau_{\leq 1}(Rp_*\mathbf{G}_m))[1] \end{array}$$

On taking the first hypercohomology groups we get the desired diagram (4.4). Indeed, quite generally $\mathbf{H}^n(Hom(M^\bullet, Rp_*\mathbf{G}_m)) = Ext^n_X(p^*M, \mathbf{G}_m)$. This implies that

$$\mathbf{H}^1(Hom(M^\bullet, \tau_{\leq 1}(Rp_*\mathbf{G}_m))) = Ext^1_X(p^*M, \mathbf{G}_m)$$

since obviously $\mathbf{H}^0(Hom(M^\bullet, \tau_{\geq 2}(Rp_*\mathbf{G}_m))) = \mathbf{H}^1(Hom(M^\bullet, \tau_{\geq 2}(Rp_*\mathbf{G}_m))) = 0$. Similarly, we have $\mathbf{H}^1(\tau_{\geq 2}(Rp_*\mathbf{G}_m)) = 0$, and also $\mathbf{H}^2(\tau_{\geq 2}(Rp_*\mathbf{G}_m)) = H^2(\overline{X}, \mathbf{G}_m)^G$, hence we get an exact sequence

$$0 \to \mathbf{H}^2(\tau_{\leq 1}(Rp_*\mathbf{G}_m)) \to H^2(X, \mathbf{G}_m) \to H^2(\overline{X}, \mathbf{G}_m)^G$$

which identifies $\mathbf{H}^1(\tau_{\leq 1}(Rp_*\mathbf{G}_m)[1])$ with $\mathrm{Br}_1(X)$. Next, we have

$$\tau_{\geq 1}(\tau_{\leq 1}(Rp_*\mathbf{G}_m)) = Pic(\overline{X})^\bullet[-1],$$

hence

$$\mathbf{H}^1(Hom(M^\bullet, \tau_{\geq 1}(\tau_{\leq 1}(Rp_*\mathbf{G}_m)))) = \mathbf{H}^1(Hom(M, Pic(\overline{X}))^\bullet[-1]) = Hom_k(M, Pic(\overline{X})),$$

and similarly

$$\mathbf{H}^1(\tau_{\geq 1}(\tau_{\leq 1}(Rp_*\mathbf{G}_m))[1]) = \mathbf{H}^1(Pic(\overline{X})^\bullet) = H^1(G, Pic(\overline{X})).$$

Comparing (4.6) with (4.4) one sees also that the arrows in these diagrams are identical. The proof of *(ii)* is now complete.

(iii) This follows from the functoriality of the cup-product.

(iv) Take any $\alpha \in H^1(G, M)$ such that $r(A) = \lambda_*(\alpha)$. Then by *(ii)* we have that

$$A - p^*(\alpha) \cup [T] \in \mathrm{Br}_0(X),$$

thus it is the image of some element $a_0 \in \mathrm{Br}(k)$. Now apply *(iii)*. (Cf. [CS], Lemme 3.5.2.) QED

Proof of the proposition. (a) and (b)

There are three steps :

(1) If there exists an adelic point which is Brauer–Manin orthogonal to $\lambda_*(\text{Ш}^1(M)) \subset \mathrm{Br}_1(X)/\mathrm{Br}_0(X)$, then there exists a torsor $f : Y \to X$ of type λ.

(2) If an adelic point is Brauer–Manin orthogonal to $\mathrm{Br}_\lambda(X)$, then there exists $\sigma \in H^1(k,S)$ such that this point lifts to an adelic point on Y_σ; the similar assertion for k-points is evident.
(3) If X is proper, then a finite set $\Sigma \subset H^1(k,S)$ would suffice to cover all points in $X(\mathbf{A}_k)^{\mathrm{Br}_\lambda}$.

The statement (1) is very similar to Prop. 3.3.2 of [CS]. The case under consideration in *loc. cit.* is that of $Pic(\overline{X})$ of finite type and $\lambda : M \to Pic(\overline{X})$ the identity map. We establish (1) along the lines of that proof.

It follows from (3.2) that there exists an X-torsor under S of type λ if and only if the image $\partial(\lambda)$ of λ in $H^2(k,S)$ is zero.

Let $b_X \in Ext^2_G(Pic(\overline{X}), \overline{k}^*)$ be the class of the 2-extension

$$1 \to \overline{k}^* \to \overline{k}(X)^* \to Div(\overline{X}) \to Pic(\overline{X}) \to 0 \tag{4.7}$$

Since $X(\mathbf{A}_k) \neq \emptyset$ this class goes to 0 under the restrictions from k to k_v ([CS], Prop. 2.2.4, 2.2.2 (b)), so that

$$b_X \in Ш(Ext^2_G(Pic(\overline{X}), \overline{k}^*)).$$

Recall that $Ext^i_G(M, \overline{k}^*) = H^i(k,S)$ ([Mi], I.4.12 (a)). By ([CS], Prop. 1.5.2 *iv*) we have

$$\partial(\lambda) = \lambda^*(b_X) \in Ext^2_G(M, \overline{k}^*).$$

One can reinterpret the proof of Lemma 3.3.3 of [CS] as follows. Let $A \in \mathrm{Br}_1(X)$ be such that $a = r(A) \in Ш^1(G, Pic(\overline{X}))$. Therefore A is "locally constant" : $i(A) := \sum_{v\in\Omega} \mathrm{inv}_v(A(P_v))$ does not depend on the choice of $\{P_v\}$. By the global reciprocity $i(A)$ depends only on $a = r(A)$, so that we adopt the notation $i(a) = i(A)$. Let $a = \lambda_*(\alpha)$ for some $\alpha \in Ш^1(G,M)$. Colliot-Thélène and Sansuc actually prove the following formula :

$$i(\lambda_*(\alpha)) =< \lambda^*(b_X), \alpha >, \tag{4.8}$$

where $<,>$ is the canonical duality pairing ([Mi], I.4.20 (a))

$$Ш^2(G,S) \times Ш^1(G,M) \to \mathbf{Q}/\mathbf{Z}$$

(The proof of Lemma 3.3.3 of [CS] rewrites $i(a)$ in the form which imitates the explicit description of $<,>$ in ([Mi], p.79) thus establishing (4.8). Note that (4.8) is completely analogous to a result of Manin ([M], Thm. 6). Assume that X is a k-torsor under an abelian variety S, S^t is the dual of S, $\lambda : S^t = Pic^0(\overline{X}) \hookrightarrow Pic(\overline{X})$ is the natural inclusion. Then presumably $\lambda^*(b_X) \in Ext^2_k(S^t, \mathbf{G}_m)$ coincides up to a sign with the class $[X] \in H^1(k,S) = Ext^2_k(S^t, \mathbf{G}_m)$, where the last isomorphism is in ([Mi], I.3.1). If $X(\mathbf{A}_k) \neq \emptyset$, and $a = r(A) = \lambda_*(\alpha)$ for some $\alpha \in Ш^1(k, S^t)$, then (4.8) with $<,>$ understood as the canonical Cassels–Tate pairing $Ш^1(k,S) \times Ш^1(k,S^t) \to \mathbf{Q}/\mathbf{Z}$ becomes Manin's formula $\sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) =< [X], \alpha >$.)

By the assumption of (1) there exists an adelic point $\{P_v\}$ such that for any $\alpha \in Ш^1(G,M)$ we have

$$< \partial(\lambda), \alpha >=< \lambda^*(b_X), \alpha >= i(\lambda_*(\alpha)) = 0.$$

By the non-degeneracy of the pairing $<,>$ we conclude that $\partial(\lambda) = 0$. This proves (1).

Inverting a finite number of primes in the ring of integers $\mathcal{O}_k \subset k$ one obtains a ring $\mathcal{O} \subset k$ such that M is unramified over $\mathcal{O}$. Let $\mathcal{S} = Hom_{\mathcal{O}-groups}(M, \mathbf{G}_m)$. Let $\mathcal{O}_v$ be the completion of $\mathcal{O}$ at a prime $v \in Spec(\mathcal{O})$, $\mathcal{S}_v := \mathcal{S} \times_{\mathcal{O}} \mathcal{O}_v$. To siplify the notation we shall write $H^i(R, \cdot)$ for $H^i(Spec(R), \cdot)$ when R is a ring. We denote $N^* = Hom(N, \mathbf{Q}/\mathbf{Z})$. The cup-product

$$H^1(k_v, S) \times H^1(k_v, M) \to \mathrm{Br}(k_v) \xrightarrow{\mathrm{inv}_v} \mathbf{Q}/\mathbf{Z}$$

defines an isomorphism (local duality) of finite groups $H^1(k_v, S) = H^1(k_v, M)^*$ ([Mi], I.2.3).

Consider the exact sequence (cf. [Mi], I.4.20 (b))

$$0 \to Ш^1(k, S) \to H^1(k, S) \to P^1(k, S) \to H^1(G, M)^* \tag{4.9}$$

where $P^1(k, S)$ is the restricted product of $H^1(k_v, S)$ for all places v with respect to subgroups $H^1(\mathcal{O}_v, \mathcal{S}_v)$ defined for $v \in Spec(\mathcal{O})$, that is, for almost all v. The right arrow in (4.9) is the sum of

$$\tau_v : H^1(k_v, S) = H^1(k_v, M)^* \to H^1(k, M)^*$$

which is the composition of the local duality isomorphism and the dual of the restriction map. Any element of $H^1(k, M)$ for almost all places v restricts to an element of $H^1(\mathcal{O}_v, M) \subset H^1(k_v, M)$ ([Mi], I.4.8), the group orthogonal to $H^1(\mathcal{O}_v, \mathcal{S}_v)$ with respect to the local duality pairing. Thus the second arrow in (4.9) is given by a finite sum and hence is well defined.

Let Y be an X-torsor under S of type λ whose existence was established in (1). Let $Y(P)$ denote the element in $H^1(k(P), Y)$ given by the fibre of Y at a closed point P. The map $X(\mathbf{A}_k) \to \prod_{v\in\Omega} H^1(k_v, S)$ sending $\{P_v\}$ to $\{Y(P_v)\}$ has its image in $P^1(k, S)$. (Indeed, up to inverting a finite number of primes in $\mathcal{O}$ depending on X, Y, and $\{P_v\}$, there exists an integral, regular model $\mathcal{X}/\mathcal{O}$ and an $\mathcal{X}$-torsor $\mathcal{Y}$ under $\mathcal{S}$ which give X, S, and Y at the generic point $Spec(k)$ of $Spec(\mathcal{O})$. Moreover, we can assume that $P_v \in \mathcal{X}(\mathcal{O}_v)$ for $v \in Spec(\mathcal{O})$, thus $\mathcal{Y}(P_v) \in H^1(\mathcal{O}_v, \mathcal{S}_v)$ for such v.) Thus we can define the map (cf. [CS], Def. 3.4.1)

$$X(\mathbf{A}_k) \to H^1(k, M)^*, \text{ by } \{P_v\} \mapsto \sum_{v\in\Omega} \tau_v(Y(P_v)).$$

¿From Lemma 3 *(iv)* it follows that for any $A \in \mathrm{Br}_\lambda(X)$ and any $\alpha \in H^1(G, M)$ such that $r(A) = \lambda_*(\alpha)$ there exists $a_0 \in \mathrm{Br}(k)$ such that for any $P_v \in X(k_v)$ we have

$$Res_{k,k_v}(\alpha) \cup Y(P_v) = A(P_v) + Res_{k,k_v}(a_0) \in \mathrm{Br}(k_v).$$

This equality combined with global reciprocity implies (cf. [CS], Cor. 3.5.3) that

$$\sum_{v\in\Omega} \tau_v(Y(P_v))(\alpha) = \sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)), \tag{4.10}$$

which is just the Brauer–Manin pairing. Let us now complete the proof of (2). If $\{P_v\} \in X(\mathbf{A}_k)$ is Brauer–Manin orthogonal to $\mathrm{Br}_\lambda(X)$, then we see that $\{Y(P_v)\}$ goes to zero under the right arrow of (4.9) thus is the image of some $\sigma \in H^1(k, S)$. Therefore $Y_\sigma(P_v) = 0$ for all v, and the fibre of $f_\sigma : Y_\sigma \to X$ over $\{P_v\}$ contains an adelic point, which proves (2).

If X is proper one can moreover assume that $\mathcal{X}$ is proper over $Spec(\mathcal{O})$. The choice of $\mathcal{O}$, $\mathcal{X}$, and $\mathcal{Y}$ is now independent on $\{P_v\}$. By the properness of X we have $\mathcal{X}(\mathcal{O}_v) = X(k_v)$, and thus $\mathcal{Y}(P_v) \in H^1(\mathcal{O}_v, \mathcal{S}_v)$ for $v \in Spec(\mathcal{O})$. It follows that an element of $H^1(k, S)$ mapping to $\{Y(P_v)\} \in P^1(k, S)$ actually lands in the subset $\prod_{v\notin Spec(\mathcal{O})} H^1(k_v, S) \times \prod_{v\in Spec(\mathcal{O})} H^1(O_v, S_v)$. Let us show that this implies that $x \in H^1(\mathcal{O}, \mathcal{S})$, the group which is well known to be finite. (This is done by reduction to the case of a finite group and of a torus. The finiteness in these cases is proved in [M], II.2.13, and II.4.6.) Let $\mathbf{F}_v$ be the residue field at v. Consider the following commutative diagram whose upper row is the exact sequence of the pair $Spec(k) \subset Spec(\mathcal{O})$, the lower row is the one of the pair $Spec(k_v) \subset Spec(\mathcal{O}_v)$, and the vertical arrows are the natural restrictions :

$$\begin{array}{ccccc}
H^1(\mathcal{O},\mathcal{S}) & \longrightarrow & H^1(k,S) & \longrightarrow & \prod_{v\in Spec(\mathcal{O})} H^2_{Spec(\mathbf{F}_v)}(\mathcal{O},\mathcal{S}) \\
\downarrow & & \downarrow & & \downarrow \\
\prod_{v\in Spec(\mathcal{O})} H^1(\mathcal{O}_v,\mathcal{S}_v) & \longrightarrow & \prod_{v\in Spec(\mathcal{O})} H^1(k_v,S) & \longrightarrow & \prod_{v\in Spec(\mathcal{O})} H^2_{Spec(\mathbf{F}_v)}(\mathcal{O}_v,\mathcal{S}_v)
\end{array}$$

By the étale excision theorem combined with Greenberg's theorem one concludes that the right vertical arrow is an isomorphism, which proves what we need. (I am grateful to J.-L. Colliot-Thélène for this argument.) This completes the proof of statement (3). Hence the parts (a) and (b) of the proposition are proved.

Proof of the proposition. (c)

Let $\{P_v\} \in X(\mathbf{A}_k)$ be the image of an adelic point on Y. Then $Y(P_v) = 0$, and (4.10) implies that $\{P_v\}$ is contained in $X(\mathbf{A}_k)^{\mathrm{Br}_\lambda}$. QED

Acknowledgement. The author thanks J.-L. Colliot-Thélène for pointing out a gap in the first draft of the example, and D. Zagier for bringing the paper [GPZ] to his attention. I thank S. Siksek for the appendix. This work was done while the author enjoyed the warm hospitality of Max-Planck-Institut für Mathematik in Bonn.

Appendix, by S. Siksek

4-descent

Let us fix our notation. Let E be an elliptic curve over a field k of characteristic zero. Let C be a principal homogeneous space under E over k with the action of E given by the map $\mu : E \times C \to C$. Then C is called an n-covering if there is a map $\psi : C \to E$ such that the following diagram commutes (cf. [S], Sect. 2) :

$$\begin{array}{ccc}
E\times C & \xrightarrow{(n,\psi)} & E\times E \\
{\scriptstyle\mu}\downarrow & & {\scriptstyle +}\downarrow \\
C & \xrightarrow{\psi} & E
\end{array}$$

An nm-covering $\psi' : C' \to E$ is a lifting of $\psi : C \to E$ if the analogous diagram for C' factorizes through this one. A principal homogeneous space C under E can be endowed with a structure of n-covering if and only if its class $[C] \in H^1(k,E)$ belongs to the n-torsion. This is precisely when $[C]$ can be lifted to a cocycle of $H^1(k,E[n])$ (see [C], III, Sect. 2). By ([C], III, Sect. 4) the nm-covering $\psi' : C' \to E$ is a lifting of the n-covering $\psi : C \to E$ if and only if the corresponding cocycles are related by the map $m_* : H^1(k,E[mn]) \to H^1(k,E[n])$. This implies that $m[C'] = [C] \in H^1(k,E)$.

We shall consider more closely the case when $n = m = 2$ and C is given by

$$y^2 = ax^4 + cx^2 + dx + e.$$

Let K be the k-algebra $k[x]/(ax^4+cx^2+dx+e)$, and let θ be the image of x in K. Let $C' \in \mathbf{P}^3_k$ be the intersection of two quadrics obtained by equating the coefficients of θ^2 and θ^3 in the following formula

$$(A.1) \qquad X - \theta Z = \epsilon(x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3)^2,$$

for some $\epsilon \in K^*$ such that $a^{-1}N_{K/k}(\epsilon) \in k^{*2}$. The following lemma is well known and is given here for the sake of completeness, cf. [B/SwD], [MSS], [Ca].

Lemma. *(a) C can be equipped with a structure of 2-covering ψ of the elliptic curve $E : u^2 = v^3 - 27Iv - 27J$, where $I = 12ae + c^2$, $J = 72ace - 27ad^2 - 2c^3$, such that $\psi^{-1}(0) \subset C$ is given by $y = 0$.*

(b) C' can be equipped with a structure of 4-covering of E which is a lifting of $\psi : C \to E$.

(c) If $C(k) = \emptyset$, then $[C']$ is of exact order 4.

Note that when $a = 1$ the passage from the equation of C to that of E is precisely the passage from a quartic polynomial to its cubic resolvent.

Recall the following well known geometric observation. Let $X \subset \mathbf{P}^4_k$ be the intersection of two quadrics given by $Q(\mathbf{x}) = Q'(\mathbf{x}) = 0$. The corresponding discriminantal curve Y defined by $\mu^2 = det(\lambda Q + Q')$ is naturally identified with $Pic^2(X)$. Indeed, the curve Y parametrizes families of lines on the quadrics of the pencil spanned by Q and Q'. Then Y is identified with $Pic^2(X)$ by the map which associates to a family of lines on a quadric the divisor class of the intersection of any line of this family with X. The curve Y comes with the map $\xi : X \to Y = Pic^2(X)$ sending a point P to the divisor class of $2P$ (geometrically this is the family of lines containing the tangent to X at P).

Proof of the lemma. (a) The curve C is isomorphic to the following intersection of two quadrics in $\mathbf{P}^4_k$:

$$Q = ut - x^2, \quad Q' = -y^2 + au^2 + cut + dxt + et^2.$$

One computes that

$$det(\lambda Q - Q') = (1/4)(\lambda^3 - 2c\lambda^2 + (c^2 - 4ae)\lambda + ad^2),$$

which gives the equation of E after an obvious change of variables. Thus $Y = E$. Let us choose the origin of the group law of E at $\lambda = \infty$ (this point corresponds to the hyperelliptic divisor on C). The map $\psi = \xi$ is a 2-covering, and it is easy to see that $\psi^{-1}(0)$ is as required.

(b) Let $\theta_i \in \overline{k}$ be the roots of the equation $ax^4 + cx^2 + dx + e = 0$. Let $\epsilon_i \in \overline{k}$ be the image of ϵ under the map $K \to \overline{k}$ which sends θ to θ_i. Let us denote by δ_i the Van der Monde determinant associated to $\theta_1, \ldots, \theta_4$ with the exception of θ_i, multiplied by $(-1)^i$. Let

$$\Delta = \prod_{1 \le i < j \le 4} (\theta_i - \theta_j)^2 \ \in k$$

be the discriminant of $a^{-1}(ax^4 + cx^2 + dx + e)$.

In the pencil of quadrics containing C' we choose the following two quadrics individually defined over k :

$$Q(\mathbf{x}) = \sum_{i=1,2,3,4} \delta_i\epsilon_i(\sum_{j=1,2,3,4} x_j\theta_i^j)^2,$$

$$Q'(\mathbf{x}) = \sum_{i=1,2,3,4} \theta_i\delta_i\epsilon_i(\sum_{j=1,2,3,4} x_j\theta_i^j)^2.$$

One computes that
$$det(\lambda Q - Q') = N_{K/k}(\epsilon)\Delta^2 \prod_{i=1,2,3,4} (\lambda - \theta_i).$$

Thus $Y = C$, and we have the map $\xi : C' \to C = Pic^2(C')$. A structure of 4-covering $\psi' : C' \to E$ is defined by the map sending a point P to the divisor class of $4P$, and identifying $Pic^4(C')$ with E by choosing the hyperplane section class as the origin of the group law. Then $\psi' = \psi \circ \xi$, so that ψ' is a lifting of ψ. See ([W], App. III, [MSS], [Ca]) for more on this classical subject.

(c) Since ψ' is a lifting of ψ we have $2[C'] = [C] \in H^1(k, E)$. When C has no k-point, $[C] \neq 0$, and our statement is proved. QED

Let us apply this to the curve

$$C: \ y^2 = g(x), \quad g(x) = 3(x^4 - 54x^2 - 117x - 243) \tag{A.2}$$

defined over $\mathbf{Q}$. Using (a) one computes that this is a 2-covering of

$$J: \ y^2 = x^3 - 1221.$$

(C is in fact everywhere locally soluble, and was initially found using Cremona's program `mwrank` [Cr]. By ([B/SwD], Lemmas 1 and 2, [C], IV, Thm. 1.3) any 2-covering which is everywhere locally soluble can be given by a double cover of $\mathbf{P}^1_{\mathbf{Q}}$.) It is computed in [GPZ] that J has analytic rank zero. The authors point out that the rank of $J(\mathbf{Q})$ is unconditionally 0 by the work of Rubin and Kolyvagin. The classical computation of torsion of such curves implies that $E(\mathbf{Q}) = \{0\}$. This together with irreducibility of $g(x)$ implies that $C(\mathbf{Q}) = \emptyset$. It is also computed in [GPZ] that Ш(J) is predicted to be isomorphic to $\mathbf{Z}/4 \times \mathbf{Z}/4$ by the conjectures of Birch and Swinnerton-Dyer. We shall now exhibit an everywhere locally solvable 4-covering $C' \to J$ which is a lifting of the 2-covering $C \to J$. By (c) of the above lemma this gives an element of order exactly 4 in Ш(J).

It is observed that the element $\epsilon = -\theta^3/3 - \theta^2 + 29\theta + 27 \in K = \mathbf{Q}(\theta)$, where $g(\theta) = 0$, has norm $243 = 3 \times 9^2$. We construct a 4-covering C' as the intersection of two quadrics (A.1), which can be written down explicitly :

$$\mathbf{x}A\mathbf{x}^t = 0, \quad \mathbf{x}B\mathbf{x}^t = 0$$

where $\mathbf{x} = (x_1, x_2, x_3, x_4)$ and the entries of A and B are respectively

$$\begin{matrix} -1 & 11 & -66 & 396 \\ 11 & -66 & 396 & -2520 \\ -66 & 396 & -2520 & 16335 \\ 396 & -2520 & 16335 & -105786 \end{matrix}$$

and

$$\begin{matrix} -1 & -3 & 33 & -198 \\ -3 & 33 & -198 & 1188 \\ 33 & -198 & 1188 & -7560 \\ -198 & 1188 & -7560 & 49005 \end{matrix}$$

Let us show that $[C'] \in$ Ш(J). Criteria for testing intersections of 2 quadrics in $\mathbf{P}^3$ for everywhere local solubility are given in [MSS]. By ([MSS], Lemma 7) we know that it is soluble over **R**, and by ([MSS], Thm. 4) that it is necessary to test for solubility only at the finite primes 2, 3, 11, 37 (2 and the divisors of 1221). This result also tells us that the following will lift to p-adic points on C' for $p = 2, 3, 11, 37$ respectively : $(0,2,1,0) mod(2^3), (12,21,1,0) mod(3^3), (0,1,0,0) mod(11)(0,1,9,16) mod(37)$. This completes our proof that C' represents an element of order exactly 4 in the the Tate–Shafarevich group of J.

We would like to draw the reader's attention to an explicit form of the Cassels–Tate bilinear pairing on the 2-Selmer group given in [Ca]. This could have been used to show that the Tate–Shafarevich group does contain an element of exact order 4, though that method would not have allowed us to write down the equations for the curve representing such an element.

We thank J. Cremona and N. Smart for their comments on an earlier version of this appendix.

References

[B] A. Beauville. *Surfaces algebriques complexes.* Astérisque **54** (1978).

[B/SwD] B. J. Birch and H. P. F. Swinnerton-Dyer. *Notes on elliptic curves. I.* J. reine angew. Math. **212** (1963) 7-25.

[C] J. W. S. Cassels. *Arithmetic on Curves of Genus 1. III. The Tate-Shafarevich and Selmer Groups.* Proc. London Math. Soc. **12** (1962) 259-296 ; *IV. Proof of the Hauptvermutung.* J. reine angew. Math. **211** (1962) 95-112.

[Ca] J. W. S. Cassels. *Second descents for elliptic curves.* To appear.

[CT] J.-L. Colliot-Thélène. *L'arithmétique du groupe de Chow des zéro-cycles.* J. théorie des nombres de Bordeaux **7** (1995) 51-73.

[CS] J.-L. Colliot-Thélène et J.-J. Sansuc. *La descente sur les variétés rationnelles. II.* Duke Math. J. **54** (1987) 375-492.

[AA] J.-L. Colliot-Thélène, A. N. Skorobogatov and Sir Peter Swinnerton-Dyer. *Double fibres and double covers : paucity of rational points.* Acta Arithm. **79** (1997) 113-135.

[Cr] J. E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992.

[GPZ] J. Gebel, A. Pethő, H. G. Zimmer. *On Mordell's Equation.* Comp. Math., to appear.

[G] A. Grothendieck. *Le groupe de Brauer. I, II, III.* Dans : *Dix exposés sur la cohomologie des schémas.* A. Grothendieck, N. H. Kuipers, Eds. North-Holland (1968) 46-188.

[M] Yu. I. Manin. *Le groupe de Brauer-Grothendieck en géometrie diophantienne.* Actes Congrès Int. Math. Nice 1970, tome **I**, Gauthier-Villars, Paris (1971) 401-411.

[MSS] J. R. Merriman, S. Siksek and N. P. Smart, *Explicit* 4*-Descents on an Elliptic Curve.* Acta Arith. **77** (1996) 385–404.

[Mi] J. S. Milne. *Arithmetic Duality Theorems.* Persp. Math. **1**, Academic Press, Boston (1986).

[Mi2] J. S. Milne. *Étale Cohomology.* Princeton Univ. Press (1980).

[Sa] S. Saito. *Some observations on motivic cohomology of arithmetic schemes.* Inv. Math. **98** (1989) 371-404.

[SW] P. Sarnak and L. Wang. *Some hypersurfaces in* $\mathbf{P}^4$ *and the Hasse-principle.* C. R. Acad. Sci. Paris **321** (1995) 319-322.

[Sh] I. R. Shafarevich *et al. Algebraic surfaces.* Proc. Steklov Inst. Math. **75** (1967).

[S] Sir Peter Swinnerton-Dyer. *Rational points on certain intersections of two quadrics.* In : *Abelian Varieties.* Barth, Hulek, Lange, Eds. Walter de Gruyter (1995) 273-292.

[W] A. Weil. *Number Theory. An approach through history.* Birkhäuser, Boston (1983).