Computing the Brauer-Manin obstructions

Martin Bright and Sir Peter Swinnerton-Dyer

1. *Introduction.* Let V be a complete nonsingular projective surface defined over an algebraic number field k, such that the Picard variety of V is trivial and $\mathrm{Pic}(\bar{V})$ is torsion-free. Since our main interest is in necessary conditions for $V(k)$ not to be empty, we shall further assume that $V(k_v)$ is non-empty for every completion k_v of k. We do not assume that $\bar{V}$ is rational, and indeed the case which primarily interests us is when V is a K3 surface. Our objective is to describe effective ways of computing the Brauer-Manin obstructions to the existence of points on V defined over k. Write

$$\mathrm{Br}^0(V) = \{\mathrm{Ker}(\mathrm{Br}(V) \to \mathrm{Br}(\bar{V}))\}/\{\mathrm{Im}(\mathrm{Br}(k) \to \mathrm{Br}(V))\};$$

then it is known that $\mathrm{Br}^0(V)$ is isomorphic to $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$, though to the best of our knowledge there is in general no known algorithm for computing either $\mathrm{Br}^0(V)$ or this isomorphism. It is generally believed that $\mathrm{Br}^0(V)$ contains all the information about the Brauer group $\mathrm{Br}(V)$ which is useful in this context. Most of this paper is concerned with computing groups isomorphic to $\mathrm{Br}^0(V)$, and with describing in terms of these groups the Brauer-Manin obstructions coming from elements of $\mathrm{Br}^0(V)$.

All non-étale cohomology in this paper is continuous; thus cohomology groups for $\mathrm{Gal}(\bar{k}/k)$ are the limits of the corresponding groups for $\mathrm{Gal}(K/k)$ as K runs through finite Galois extensions of k. The exact sequence

$$\mathrm{Br}(k) \to \mathrm{H}^2(k, \bar{k}(V)^*) \to \mathrm{H}^2(k, \bar{k}(V)^*/\bar{k}^*) \to \mathrm{H}^3(k, \bar{k}^*) \tag{1}$$

forms part of the long exact sequence derived from

$$0 \to \bar{k}^* \to \bar{k}(V)^* \to \bar{k}(V)^*/\bar{k}^* \to 0,$$

and $\mathrm{H}^2(k, \bar{k}(V)^*)$ classifies simple algebras on V with centre $k(V)$ which split over $\bar{k}$. Tate[2] has shown that $\mathrm{H}^3(k, \bar{k}^*) = 0$ when k is an algebraic number field; and Lemma 2 below will enable us to identify those elements of $\mathrm{H}^2(k, \bar{k}(V)^*/\bar{k}^*)$ which come from Azumaya algebras on V/k. They form a subgroup which we shall call $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$, and this subgroup is precisely the kernel of the natural map

$$\mathrm{H}^2(k, \bar{k}(V)^*/\bar{k}^*) \longrightarrow \mathrm{H}^2(k, \mathrm{Div}(\bar{V})).$$

Here $\bar{k}(V)^*/\bar{k}^*$ is isomorphic to the group of principal divisors on V defined over $\bar{k}$; we shall as usual denote this isomorphism by $f \mapsto (f)$.

In §2 we introduce the group $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ and show how to calculate it. It is isomorphic to $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$ and therefore to $\mathrm{Br}^0(V)$; and its elements correspond in an obvious way to those classes of Azumaya algebras which split over $\bar{k}$, so that it is a good intermediary for computing the Brauer-Manin obstruction. In §3 we discuss the associated Azumaya algebras and the Brauer-Manin obstructions. If $\mathcal{A}$ is an Azumaya algebra on V defined over k, we write $\mathcal{A}_v = \mathcal{A} \otimes_k k_v$ for each place v of k. We remind the reader that the Brauer-Manin condition for solubility of V in k is that there exists a point $\prod P_v$ in $\prod V(k_v)$ such that

$$\sum_v \mathrm{inv}\mathcal{A}_v(P_v) = 0$$

for every Azumaya algebra $\mathcal{A}$ on V defined over k.

The general theory which underlies much of this paper depends on the existence of lifting processes of the following kind. Let $\mathfrak{G}, \mathfrak{H}$ be commutative groups and $f : \mathfrak{G} \to \mathfrak{H}$ a homomorphism. Let $\mathfrak{h}$ be an element of $\mathfrak{H}$; then a lifting process obtains an element $\mathfrak{g}$ in $\mathfrak{G}$ such that $\mathfrak{h} = f(\mathfrak{g})$. Sometimes the general theory will show (usually in a non-constructive way) that such a $\mathfrak{g}$ exists; at other times the existence of $\mathfrak{g}$ will be an open question. To make the process computable is to provide algorithms which decide whether such $\mathfrak{g}$ exist, and if so which exhibit at least some of them. Such an algorithm will usually be designed so that its primary aim is to find some $\mathfrak{g}$ provided any such exist; if it terminates without finding any $\mathfrak{g}$, it will follow that no such $\mathfrak{g}$ exists. Usually (and in all the cases which occur in this paper) the key step will be to exhibit a finitely generated subgroup $\mathfrak{G}_0 \subset \mathfrak{G}$ depending on $\mathfrak{h}$ such that if $\mathfrak{h} = f(\mathfrak{g})$ is possible at all, then it is possible with $\mathfrak{g}$ in $\mathfrak{G}_0$. Typically, $\mathfrak{G}$ will be associated with the algebraic closure $\bar{k}$ and it will therefore not be possible to express it in a form amenable to computation; but $\mathfrak{G}_0$ will be similarly associated with an explicitly determined finite Galois extension K/k and will therefore be computable. The simplest examples of this are Theorems 2 and 3, and Theorem 1 is almost of the same kind. If we have such a $\mathfrak{G}_0$, let $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$ be a base for $\mathfrak{G}_0$ and write

$$\mathfrak{g} = m_1\mathfrak{g}_1 + \ldots + m_n\mathfrak{g}_n$$

where the m_i are in $\mathbf{Z}$. The condition which we have to satisfy is

$$\mathfrak{h} = m_1 f(\mathfrak{g}_1) + \ldots + m_n f(\mathfrak{g}_n),$$

which is equivalent to a finite set of linear equations and congruences in the m_i. Solving these is routine even if n is quite large.

We shall suppose that we are given both V and $\mathrm{Pic}(\bar{V})$. Obtaining $\mathrm{Pic}(\bar{V})$ from V in an effective way seems to be a number-theoretic problem to which in general no algorithmic answer is yet known. (The critical step in one approach to the problem can be found in [8]. If the Birch/Swinnerton-Dyer conjecture is true, then this approach provides an algorithm which solves the problem; but the algorithm is so laborious that one could not contemplate actually using it.) However, if we only know a subgroup $P \subset \mathrm{Pic}(\bar{V})$ which is mapped to itself by $\mathrm{Gal}(\bar{k}/k)$, then we can give natural meanings to the pseudo-Brauer group associated with P and the Brauer-Manin obstruction associated with this group; and these can be computed by means of the algorithms described in this paper. One particularly interesting case is when we are given a fibration of V and P is generated by the absolutely irreducible components of the curves in this fibration. There is now a natural map

$$\mathrm{H}^1(k, P) \longrightarrow \mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$$

whose image is isomorphic to the vertical part of $\mathrm{Br}^0(V)$ in the sense of [4]; and if we apply to $\mathrm{H}^1(k, P)$ the algorithm which obtains the Brauer-Manin obstruction from $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$, we obtain the vertical part of the Brauer-Manin obstruction.

As far as possible we have denoted elements of $\mathrm{Pic}(\bar{V})$ by α or β, elements of $\mathrm{Div}(\bar{V})$ by $\mathfrak{a}$ or $\mathfrak{b}$, elements of $\bar{k}(V)^*$ by x or y and elements of $\bar{k}(V)^*/\bar{k}^*$ by ξ, η or ζ. These last can be identified with principal divisors; if so, they are enclosed in round brackets.

For clarity, results which belong to the general theory are called lemmas; those which underlie the algorithms are called theorems. Thus the lemmas are related to or identical with what is already known; the most comprehensive account can be found in [3]. But the theorems may well be new.

We are indebted to Jean-Louis Colliot-Thélène and Alexei Skorobogatov for helpful comments and advice. The first author is grateful to EPSRC for financial support, first from a Research Studentship and then from Grant GR/R82975/01.

2. *The Brauer group.* Let Γ be a positive divisor on V, defined and irreducible over a given Galois extension K of k. If $\mathfrak{a}$ is an element of $\mathrm{Div}(V \otimes K)$, we can write

$$\mathfrak{a} = \sum n_i \Gamma_i + \mathfrak{a}'$$

where Γ_i runs through the divisors conjugate to Γ over k and the support of $\mathfrak{a}'$ does not contain any of the Γ_i. We shall call $\sum n_i\Gamma_i$ the Γ-*component* of $\mathfrak{a}$. Because $K(V)^*/K^*$ can be identified with the group of principal divisors on $V \otimes K$, we can in particular define the Γ-component of an element of $K(V)^*/K^*$; it will lie in $\mathrm{Div}(V \otimes K)$ but in general not in $K(V)^*/K^*$. This enables us to define the Γ-components of cochains with values in $\mathrm{Div}(V \otimes K)$ or $K(V)^*/K^*$. The operation of taking Γ-components clearly commutes with the coboundary operator d. By the fundamental equation

$$g\mathfrak{m}(g_1, g_2) = \mathfrak{m}(gg_1, g_2) - \mathfrak{m}(g, g_1g_2) + \mathfrak{m}(g, g_1) \tag{2}$$

for 2-cocycles, if the support of a 2-cocycle $\mathfrak{m}$ with values in $\mathrm{Div}(V \otimes K)$ or $K(V)^*/K^*$ contains $g^{-1}\Gamma$ for some g in $\mathrm{Gal}(K/k)$ then it also contains Γ; so the condition that the support of $\mathfrak{m}$ does not contain Γ is equivalent to the condition that the support of $\mathfrak{m}$ does not contain Γ or any of its conjugates over k. A similar property and proof hold for 1-cocycles. Moreover, all this extends to the tensor products of $\mathrm{Div}(V \otimes K)$ and $K(V)^*/K^*$ with $\mathbf{Q}$.

Let $\mathcal{S}_0$ be a finite subset of $\mathrm{Div}(\bar{V})$ satisfying the following conditions:

- The images of the elements of $\mathcal{S}_0$ generate $\mathrm{Pic}(\bar{V})$.
- If $\mathcal{S}_0$ contains $\mathfrak{a}$ then it contains $g\mathfrak{a}$ for every g in $\mathrm{Gal}(\bar{k}/k)$.

Let $\mathcal{S}_1 \supset \mathcal{S}_0$ be a finite subset of $\mathrm{Div}(\bar{V})$ satisfying the additional condition:

- If $\mathfrak{b}$ is any element of $\mathrm{Div}(\bar{V})$ then there is an $\mathfrak{a}$ in the $\mathbf{Z}$-module spanned by $\mathcal{S}_1$ such that $\mathfrak{b}$ is linearly equivalent to $\mathfrak{a}$ and $\mathfrak{a}$ is defined over the least field of definition for $\mathfrak{b}$ which contains k.

By replacing each element of $\mathcal{S}_0$ by the absolutely irreducible components of its support, and similarly for $\mathcal{S}_1$, we can further suppose that every element of $\mathcal{S}_0$ or $\mathcal{S}_1$ is an absolutely irreducible positive divisor. Having done this, we choose once for all a finite Galois extension K_0 of k which is a field of definition for each divisor in $\mathcal{S}_0$; we shall see shortly that $\mathcal{S}_1$ can be so chosen that K_0 is also a field of definition for each divisor in $\mathcal{S}_1$. From now on, $\mathcal{S}_0, \mathcal{S}_1$ and K_0 will always have this meaning and the additional property just stated.

The construction of $\mathcal{S}_0$ is straightforward provided one knows $\mathrm{Pic}(\bar{V})$. To construct $\mathcal{S}_1$ we proceed as follows. For each field L such that $k \subset L \subset K_0$, choose a finite subset $\mathcal{S}$ of $\mathrm{Div}(V \otimes L)$ whose images generate $\mathrm{Pic}(V \otimes L)$.

To obtain $\mathcal{S}_1$ we adjoin to $\mathcal{S}_0$ all conjugates over k of the elements of the sets $\mathcal{S}$ thus chosen. (This process can be tidied up; but even the most natural choice of $\mathcal{S}_0$ may require the adjunction of some additional elements.)

Since V is everywhere locally soluble, for L as above every element of $\mathrm{Pic}(\bar{V})$ which is fixed by $\mathrm{Gal}(\bar{k}/L)$ lies in $\mathrm{Pic}(V \otimes L)$. For let α in $\mathrm{Pic}(\bar{V})$ be fixed by $\mathrm{Gal}(\bar{k}/L)$. If π is the class of an ample divisor on V, then $n\pi + \alpha$ is an effective divisor class provided n is large enough; and in this case the positive divisors in $n\pi + \alpha$ are classified by the points of some variety W defined over L. Since V is everywhere locally soluble, so is W; and hence W is soluble in L because it is Severi-Brauer.

Lemma 1 *Let G be a finite group and M a torsion-free G-module. Let $g \mapsto \mathfrak{m}(g)$ be a* 1*-cocycle on G with values in M, and let $M_0 \subset M$ be a G-submodule which contains every $\mathfrak{m}(g)$. Then $\mathfrak{m} = d\mu$ for some μ in $M_0 \otimes \mathbf{Q}$.*

Proof Write $\mu = -\{\sum_{g \text{ in } G} \mathfrak{m}(g)\}/[G]$; then $\mathfrak{m}(g_1) = g_1\mu - \mu$ follows from the cocycle rule

$$\mathfrak{m}(g_1) = \mathfrak{m}(g_1 g) - g_1 \mathfrak{m}(g)$$

by summing over all g in G. □

We shall usually only be interested in the class of $\mathfrak{m}$ in $\mathrm{H}^1(G, M)$. Since μ_1 and μ_2 give the same $\mathfrak{m}$ if and only if $\mu_1 - \mu_2$ is fixed under G, they give the same class in $\mathrm{H}^1(G, M)$ if and only if

$$\mu_1 - \mu_2 \quad \text{is in} \quad M + (M \otimes \mathbf{Q})^G.$$

In particular, we can regard a class in $\mathrm{H}^1(G, M)$ as being determined by an element of $M \otimes (\mathbf{Q}/\mathbf{Z})$; and this element is fixed by G and is determined up to the image of an arbitrary element of $(M \otimes \mathbf{Q})^G$.

Corollary 1 *Let K be a Galois extension of k; then*

$$\mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{Div}(V \otimes K)) = 0.$$

Proof Let $\mathfrak{m}$ be a 1-cocycle on $\mathrm{Gal}(K/k)$ with values in $\mathrm{Div}(V \otimes K)$. If K/k is finite, there is an element μ in $(\mathrm{Div}(V \otimes K)) \otimes \mathbf{Q}$ such that $\mathfrak{m} = d\mu$. Let Γ be a positive divisor on V defined and irreducible over K, and let $\mathfrak{m}_0, \mu_0$ be the Γ-components of $\mathfrak{m}$ and μ. Write $\mu_0 = \sum a_i \Gamma_i$ where the sum is taken over the distinct conjugates of Γ over k and the a_i are in $\mathbf{Q}$. Then $\mathfrak{m}_0(g) = \sum_i (a_j - a_i)\Gamma_i$ where $j = j(i, g)$ is such that $g\Gamma_j = \Gamma_i$. For every pair i, j there is at least one such g; so all the $a_i - a_j$ are integers. Choose a so that each $a_i - a$ is an integer, and write $\mu_1 = \sum(a_i - a)\Gamma_i$; thus μ_1 is in $\mathrm{Div}(V \otimes K)$ and $d\mu_1 = d\mu_0 = \mathfrak{m}_0$ because $\sum \Gamma_i$ is fixed by $\mathrm{Gal}(K/k)$. Summing the μ_1 over a complete set of non-conjugate K-irreducible divisors in the support of $\mathfrak{m}$, we obtain μ in $\mathrm{Div}(V \otimes K)$ such that $\mathfrak{m} = d\mu$. The general case now follows because we are using continuous cohomology, so that $\mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{Div}(V \otimes K))$ is the direct limit of the $\mathrm{H}^1(\mathrm{Gal}(L/k), \mathrm{Div}(V \otimes L))$ for finite Galois extensions L/k with $L \subset K$. □

Corollary 2 *Let K_0 be as above, and let K be a Galois extension of k such that $K \supset K_0$. Then the inflation map*

$$\mathrm{H}^1(\mathrm{Gal}(K_0/k), \mathrm{Pic}(\bar{V})) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{Pic}(\bar{V}))$$

is an isomorphism.

Proof Suppose first that K/k is finite. Consider the set of coboundaries $d\alpha$ of those elements α in $(\mathrm{Pic}(\bar{V})) \otimes \mathbf{Q}$ which are such that $d\alpha$ has values in $\mathrm{Pic}(\bar{V})$. This set can be identified both with the set of 1-cocycles on $\mathrm{Gal}(K/k)$ with values in $\mathrm{Pic}(\bar{V})$ and with the corresponding set for $\mathrm{Gal}(K_0/k)$. The general case follows as in the proof of Corollary 1. There is an alternative proof by means of the inflation-restriction exact sequence. □

An argument similar to that of Lemma 1 shows that every 2-cocycle $\mathfrak{m}(g_1, g_2)$ on G with values in M has the form $d\mu$ for some $\mu : g \mapsto \mu(g)$ with values in $M \otimes \mathbf{Q}$. For we need only write

$$\mu(g) = \{\textstyle\sum_{g' \text{ in } G} \mathfrak{m}(g, g')\}/[G]; \tag{3}$$

and apply the cocycle rule (2); summing (2) over all g_2 we obtain

$$g\mu(g_1) = \mu(gg_1) - \mu(g) + \mathfrak{m}(g, g_1).$$

Lemma 2 *Let K be a Galois extension of k and let $\mathcal{C}$ be an element of $\mathrm{H}^2(\mathrm{Gal}(K/k), K(V)^*/K^*)$; then the following five properties are equivalent:*

(i) *Let $\mathcal{T}$ be a finite set of positive divisors on V, each defined and irreducible over K. Then there is an element ξ in $\mathcal{C}$ whose Γ-component is 0 for each Γ in $\mathcal{T}$.*

(ii) *Let Γ be a positive divisor on V, defined and irreducible over K. Then there is an element ξ in $\mathcal{C}$ whose Γ-component is 0.*

(iii) *Let $\{P_1, \ldots, P_n\}$ be any finite set of points on V, not necessarily defined over K or even over $\bar{k}$. Then there is an element ξ in $\mathcal{C}$ whose support does not contain any of the P_i.*

(iv) *Let P be a point on V, not necessarily defined over K or even over $\bar{k}$. Then there is an element ξ in $\mathcal{C}$ whose support does not contain P.*

(v) *$\mathcal{C}$ is in the kernel of the natural map*

$$\mathrm{H}^2(\mathrm{Gal}(K/k), K(V)^*/K^*) \to \mathrm{H}^2(\mathrm{Gal}(K/k), \mathrm{Div}(V \otimes K)).$$

Proof Suppose first that K/k is finite.

(v)⇒(i) and (iii). Suppose that $\mathcal{C}$ satisfies (v) and let ξ_1 be any element of $\mathcal{C}$. The divisor (ξ_1) is the coboundary $d\mathfrak{a}_1$ of a 1-cochain $\mathfrak{a}_1$ with values in $\mathrm{Div}(V \otimes K)$. Let $\mathfrak{a}'_1$ be another 1-cochain with values in $\mathrm{Div}(V \otimes K)$, such that $\mathfrak{a}'_1(g)$ is linearly equivalent to the corresponding $\mathfrak{a}_1(g)$ for each g in $\mathrm{Gal}(K/k)$. If we are trying to prove (i), we further require that the support of each $\mathfrak{a}'_1(g)$ contains no divisor conjugate over k to any of the divisors in $\mathcal{T}$. Let η be a 1-cochain with values in $K(V)^*/K^*$ such that the divisor $(\eta(g)) = \mathfrak{a}_1(g) - \mathfrak{a}'_1(g)$. Then $\xi = \xi_1 - d\eta$ is in $\mathcal{C}$ and its divisor is $d\mathfrak{a}'_1$, which satisfies (i). If instead we are trying to prove (iii), we need to partition the points P_i into three subsets:

- Those which are defined over $\bar{k}$.
- Those which have transcendence degree 1 over $\bar{k}$; the locus of any such P_i over $\bar{k}$ is an absolutely irreducible curve Γ_i defined over $\bar{k}$.
- Those which have transcendence degree greater than 1 over $\bar{k}$, and which therefore do not lie on any curve defined over $\bar{k}$.

The additional requirement on the $\mathfrak{a}'_1(g)$ will now be that their supports do not contain any point conjugate over k to any of the P_i which are of the first kind, and do not contain any curve conjugate over k to the Γ_i associated with the points P_i of the second kind. The rest of the argument is essentially the same as before.

(iii)⇒(i). Let Γ_i run through all the conjugates over k of all the elements of $\mathcal{T}$, and for each i choose a point P_i on Γ_i. If the support of ξ does not contain P_i it cannot contain Γ_i. Again, if Γ is as in (ii) and (iv) holds, we choose any P on Γ. By (iv) there is an element ξ in $\mathcal{C}$ whose support does not contain Γ. But we have already seen that if the support of ξ does not contain Γ then it does not contain any of the conjugates of Γ. Hence (iv)$\Rightarrow$(ii).

(i)$\Rightarrow$(ii) and (iii)$\Rightarrow$(iv) are trivial.

(ii)$\Rightarrow$(v). Suppose that $\mathcal{C}$ satisfies (ii) and let ξ_0 be an element of $\mathcal{C}$. Let Γ be a positive divisor in the support of ξ_0, defined and irreducible over K, and use (ii) to choose ξ in $\mathcal{C}$ with Γ-component 0. The divisor $(\xi_0) - (\xi)$ is a coboundary with values in $\mathrm{Div}(V \otimes K)$; suppose it is $d\mathfrak{a}$ where $\mathfrak{a}$ is a 1-cochain with values in $\mathrm{Div}(V \otimes K)$, and let $\mathfrak{a}_1$ be the Γ-component of $\mathfrak{a}$. Then $d\mathfrak{a}_1$ is the Γ-component of $(\xi_0) - (\xi)$ and hence also of (ξ_0). Carry out this process for a maximal set of non-conjugate divisors in the support of ξ_0, defined and irreducible over K. Let $\mathfrak{a}_0$ be the sum of the corresponding $\mathfrak{a}_1$; then $\mathfrak{a}_0$ is a 1-cochain with values in $\mathrm{Div}(V \otimes K)$ such that $(\xi_0) = d\mathfrak{a}_0$.

The general case of the Lemma now follows because we are dealing with continuous cohomology, so that the cohomology groups in (v) are the direct limits of the corresponding $\mathrm{H}^2(\mathrm{Gal}(L/k), \cdot)$ for finite Galois extensions L/k with $L \subset K$. □

Let K be any Galois extension of k, and let $\mathrm{H}^2_{\mathrm{Az}}(\mathrm{Gal}(K/k), K(V)^*/K^*)$ denote the subgroup of $\mathrm{H}^2(\mathrm{Gal}(K/k), K(V)^*/K^*)$ consisting of those $\mathcal{C}$ which have the properties listed in Lemma 2. Applying (v) and the triviality of $\mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{Div}(V \otimes K))$ to the long exact sequence derived from

$$0 \longrightarrow K(V)^*/K^* \longrightarrow \mathrm{Div}(V \otimes K) \longrightarrow \mathrm{Pic}(\bar{V}) \longrightarrow 0 \tag{4}$$

we obtain an isomorphism

$$\delta : \mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{Pic}(\bar{V})) \to \mathrm{H}^2_{\mathrm{Az}}(\mathrm{Gal}(K/k), K(V)^*/K^*) \tag{5}$$

and in the particular case $K = \bar{k}$ an isomorphism

$$\mathrm{H}^1(k, \mathrm{Pic}(\bar{V})) \longrightarrow \mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*). \tag{6}$$

It follows from Corollary 2 to Lemma 1 that the right hand side of (5) is independent of K provided that $K \supset K_0$. For computational purposes it is clearly advisable to take K to be as small as possible — that is, to take $K = K_0$. However, for notational purposes we shall take $K = \bar{k}$. In contrast with the classical isomorphism $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V})) \simeq \mathrm{Br}^0(V)$, the isomorphism (6) is easily computable. For let $\mathcal{A}$ be an element of $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$ and take any α in $\mathcal{A}$. To obtain $\delta\mathcal{A}$ we first lift α back to a 1-cochain $\mathfrak{a}$ with values in $\mathrm{Div}(\bar{V})$. Since $d\alpha = 0$, $d\mathfrak{a}$ is principal; and $\delta\mathcal{A}$ is defined to be the class of

$d\mathfrak{a}$ in $\mathrm{H}^2(k,\bar{k}(V)^*/\bar{k}^*)$. That $\delta\mathcal{A}$ is in $\mathrm{H}^2_{\mathrm{Az}}(k,\bar{k}(V)^*/\bar{k}^*)$ follows from (v) of Theorem 2.

To define δ^{-1} we proceed as follows. Let $\mathcal{C}$ be a class in $\mathrm{H}^2_{\mathrm{Az}}(k,\bar{k}(V)^*/\bar{k}^*)$ and let ξ be an element of $\mathcal{C}$; then (ξ) is the coboundary of a 1-cochain $\mathfrak{a}$ with values in $\mathrm{Div}(\bar{V})$, and $\mathfrak{a}$ maps to a 1-cochain α with values in $\mathrm{Pic}(\bar{V})$. But the coboundary $d\alpha$ is the image of $d\mathfrak{a}$, so that $d\alpha$ vanishes by the exactness of (4). Hence α is a 1-cocycle. It is trivial to check that the class of α only depends on $\mathcal{C}$ and that the map $\mathcal{C} \mapsto \mathcal{A}$ thus induced is the inverse of the connecting homomorphism (6).

The only step which might cause computational difficulties here is the construction of $\mathfrak{a}$ from ξ. But if Γ is an absolutely irreducible positive divisor on $\bar{V}$, the coboundary of the Γ-component of $\mathfrak{a}$ is just the Γ-component of $d\mathfrak{a}$. Hence we can delete from $\mathfrak{a}$ its Γ-components for all Γ outside the support of ξ. In other words, we can take $\mathfrak{a} = \sum n_i\Gamma_i$ for some n_i, where the sum is over all absolutely irreducible Γ_i in the support of ξ. Hence we can use the process described in the Introduction to find $\mathfrak{a}$. A further simplification is provided by the following Theorem.

Theorem 1 *Each class $\mathcal{C}$ in $\mathrm{H}^2_{\mathrm{Az}}(k,\bar{k}(V)^*/\bar{k}^*)$ contains a 2-cocycle ξ whose support is contained in $\mathcal{S}_0$.*

Proof Let ξ' be a 2-cocycle in $\mathcal{C}$, and suppose that the support of ξ' contains an absolutely irreducible divisor Γ which is not in $\mathcal{S}_0$. By (i) of Lemma 2, there is a 2-cocycle ξ'' in $\mathcal{C}$ whose support does not contain Γ or any of its conjugates over k. Since ξ'/ξ'' is a coboundary, it has the form $d\eta$ for some 1-cochain η with values in $\bar{k}(V)^*/\bar{k}^*$. If we identify η with a 1-cochain whose values are principal divisors, we can write

$$(\eta(g_1)) = \sum n_g(g_1).g\Gamma + \mathfrak{a}(g_1)$$

where the $n_g(g_1)$ are in $\mathbf{Z}$, the sum is taken over all distinct conjugates $g\Gamma$ of Γ and the $\mathfrak{a}(g_1)$ are divisors whose supports do not contain Γ or any of its conjugates. Now let $\mathfrak{c}$ be a divisor linearly equivalent to Γ and with support in $\mathcal{S}_0$. Then $\mathfrak{b}$ defined by

$$\mathfrak{b}(g_1) = \sum n_g(g_1).g(\Gamma - \mathfrak{c})$$

is a 1-cochain whose values are principal divisors, and it contains the same multiple of each $g\Gamma$ as $(\eta(g_1))$ does. Hence $d\mathfrak{b}$ contains the same multiple of each $g\Gamma$ as $d\eta = (\xi'/\xi'')$ does, and the support of $d\mathfrak{b}$ is contained in the union of $\mathcal{S}_0$ and all the $g\Gamma$. Thus $(\xi') - d\mathfrak{b}$ is in $\mathcal{C}$; and its support is a subset of the set derived from the support of ξ' by deleting all the $g\Gamma$ and adjoining $\mathcal{S}_0$. Repeating this process finitely many times, we obtain a 2-cycle in $\mathcal{C}$ whose support is contained in $\mathcal{S}_0$. □

The 2-cochains ξ for $\mathrm{Gal}(K_0/k)$ with values in $K_0(V)^*/K_0^*$ and support in $\mathcal{S}_0$ are specified by $[K_0 : k]^2[\mathcal{S}_0]$ integer-valued parameters; so we can find the set of all such ξ which are actually 2-cocycles. What interests us is which of them lie in some class of $\mathrm{H}^2_{\mathrm{Az}}(\mathrm{Gal}(K_0/k), K_0(V)^*/K_0^*)$ — that is, which of them have images with values in $\mathrm{Div}(V \otimes K_0)$ which are actually coboundaries. To compute $\mathrm{H}^2_{\mathrm{Az}}(\mathrm{Gal}(K_0/k), K_0(V)^*/K_0^*)$ in this way we must find out which such ξ are themselves coboundaries. How to do this is considered in the next paragraph. But in fact we do not need to implement these constructions; for in view of the isomorphism (6) we can obtain $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ from $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$. If we ensure that every element of $\mathrm{Pic}(\bar{V})$ lifts back to a divisor with support contained in $\mathcal{S}_0$, then the representatives of the classes $\mathcal{C}$ which we obtain will automatically have the property in the Theorem.

Computing the set of those ξ with support in $\mathcal{S}_0$ which are actually coboundaries appears to present some difficulties, because the coboundary formula

$$\xi(g, g_1) = g\eta(g_1).\eta(g)/\eta(gg_1) \tag{7}$$

does not appear to imply that we can choose the support of η to be in $\mathcal{S}_0$. But this difficulty can be overcome by working in $\mathcal{S}_1$ rather than in $\mathcal{S}_0$. As the following Theorem shows, to find all the ξ with support in $\mathcal{S}_0$ which lie in the trivial class of $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$, we can further restrict $\mathfrak{a}$ to be principal.

Theorem 2 *Let $\mathcal{C}$ be a class in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ and ξ an element of $\mathcal{C}$ with support in $\mathcal{S}_1$. Then the divisor (ξ) has the form $d\mathfrak{a}$ where $\mathfrak{a}$ is a 1-cochain with values in $\mathrm{Div}(\bar{V})$ and support in $\mathcal{S}_1$. If $\mathcal{C}$ is the trivial class, then $\xi = d\eta$ where η is a 1-cochain with values in $\bar{k}(V)^*/\bar{k}^*$ and support in $\mathcal{S}_1$.*

Proof By Lemma 2, (ξ) is a coboundary $d\mathfrak{a}_0$ where $\mathfrak{a}_0$ is a 1-cochain with values in $\mathrm{Div}(\bar{V})$. Let Γ be an absolutely irreducible curve which is in the support of $\mathfrak{a}_0$ but is not in $\mathcal{S}_1$, and let $\sum n_i(g)\Gamma_i$ be the Γ-component of $\mathfrak{a}_0(g)$, where Γ_i runs through the distinct conjugates of Γ over k. Choose h_i in $\mathrm{Gal}(\bar{k}/k)$ so that $\Gamma_i = h_i\Gamma$. Let L be the least field of definition for Γ which contains k. By the definition of $\mathcal{S}_1$, we can find a divisor $\mathfrak{b}$ in the $\mathbf{Z}$-module spanned by $\mathcal{S}_1$ which is linearly equivalent to Γ and is defined over

L. The Γ-component of $d\mathfrak{a}_0 = \xi$ vanishes, so that

$$\sum\nolimits_i \{n_i(g_2).g_1h_i + (n_i(g_1) - n_i(g_1g_2))h_i\}\Gamma = 0$$

for all g_1, g_2 in $\mathrm{Gal}(\bar{k}/k)$. This is equivalent to

$$n_j(g_2) + n_i(g_1) - n_i(g_1g_2) = 0$$

for all i, g_1, g_2, where j is determined by the condition that the action of h_j on Γ is the same as that of g_1h_i. But this means that the action of h_j on L, and hence also on $\mathfrak{b}$, is the same as that of g_1h_i. Thus

$$\sum\nolimits_i \{n_i(g_2).g_1h_i + (n_i(g_1) - n_i(g_1g_2))h_i\}(\Gamma - \mathfrak{b}) = 0$$

for all g_1, g_2. This is the same as saying that the 1-cochain

$$g \mapsto \sum n_i(g)h_i(\Gamma - \mathfrak{b}) \tag{8}$$

has zero coboundary. Hence we can subtract the 1-cochain (8) from $\mathfrak{a}_0$ without affecting the truth of the equation $(\xi) = d\mathfrak{a}_0$. In this way we eliminate from the support of $\mathfrak{a}_0$ all the conjugates of Γ without bringing in any new divisors which are outside the $\mathbf{Z}$-module spanned by $\mathcal{S}_1$. Repeating this process, we eventually reduce to an $\mathfrak{a}_0$ of the form required. Since the right hand side of (8) is a principal divisor, the argument also proves the last sentence of the Theorem. □

Now let K/k be a finite Galois extension. We saw just before Lemma 2 that we can describe any 2-cocycle ξ on $\mathrm{Gal}(K/k)$ with values in $K(V)^*/K^*$ by a 1-cochain η with values in $(K(V)^*/K^*) \otimes \mathbf{Q}$. Because our cohomology is continuous, this extends to any Galois extension K/k and in particular to $\bar{k}/k$. With the obvious identifications, η is independent of the choice of K. By (3), if the support of ξ is contained in $\mathcal{S}_0$ then so is the support of η. A cochain η with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ and coboundary $d\eta = \xi$ is determined up to a 1-cocycle with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$. Applying Lemma 1 to any such 1-cocycle, it is actually the coboundary of an element ζ in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$. In particular, the class $\mathcal{C}$ of ξ is trivial if and only if ξ is the coboundary of a 1-cocycle η' with values in $\bar{k}(V)^*/\bar{k}^*$. This is the same as saying that if η is given by (3) then there exists ζ in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ such that $\eta/d\zeta$ has values in $\bar{k}(V)^*/\bar{k}^*$. In view of Theorem 2, we can require the support of ζ to lie in $\mathcal{S}_1$.

Suppose now that η is a 1-cochain with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ such that $d\eta$ takes values in $\bar{k}(V)^*/\bar{k}^*$. The following criterion for the class of $d\eta$ to lie in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ is based on (ii) of Theorem 2; there are similar but less useful tests based on each of (i), (iii) and (iv).

Lemma 3 *Let η be a 1-cochain with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ such that its coboundary $\xi = d\eta$ has values in $\bar{k}(V)^*/\bar{k}^*$. Then the class of ξ is in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ if and only if η has the following property: if Γ is any absolutely irreducible positive divisor on $\bar{V}$, there is an element ζ in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ such that the image of $\eta - d\zeta$ as a 1-cochain with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes (\mathbf{Q}/\mathbf{Z})$ has Γ-component 0.*

Proof Suppose first that the class of ξ is in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$. Using (ii) of Lemma 2, choose ξ_1 in the class of ξ so that the Γ-component of ξ_1 vanishes. Let K be a finite Galois extension of k over which ξ, η and ξ_1 are all defined, and let η_1 be obtained from ξ_1 by means of (3); then η and η_1 determine the same class in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$, so that $\eta/\eta_1 = \eta_0 d\zeta$ for some ζ in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ and some 1-cochain η_0 with values in $\bar{k}(V)^*/\bar{k}^*$. The image of $\eta/d\zeta$ as a 1-cochain with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes (\mathbf{Q}/\mathbf{Z})$ is the same as that of $\eta/(\eta_0 d\zeta) = \eta_1$, so it has Γ-component 0.

Conversely, suppose that η has the property in the Lemma. Then we can lift the image of $\eta/d\zeta$ as a 1-cochain with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes (\mathbf{Q}/\mathbf{Z})$ to a 1-cochain η_1 with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ and Γ-component 0. Write $\eta/(\eta_1 d\zeta) = \eta_0$, so that η_0 has values in $\bar{k}(V)^*/\bar{k}^*$; then $d\eta_1 = d\eta/d\eta_0$ is a 2-cocycle which lies in the same class in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ as $\xi = d\eta$. Hence this class satisfies (ii) of Lemma 2. □

We have seen that we can describe the classes $\mathcal{C}$ in $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ and $\mathcal{M}$ in $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$ by means of 1-cochains η with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ and elements α in $(\mathrm{Pic}(\bar{V})) \otimes \mathbf{Q}$ respectively. It is useful to be able to describe the isomorphism (6) in terms of η and α.

To obtain α from η we proceed as follows. By Lemma 2, $(d\eta)$ is a coboundary; so there is a 1-cochain $\mathfrak{a}$ with values in $\mathrm{Div}(\bar{V})$ such that $\mathfrak{a} - (\eta)$ is a 1-cocycle with values in $(\mathrm{Div}(\bar{V})) \otimes \mathbf{Q}$. By Lemma 1, there is an element $\mathfrak{a}_1$ of $(\mathrm{Div}(\bar{V})) \otimes \mathbf{Q}$ such that $d\mathfrak{a}_1 + (\eta)$ has values in $\mathrm{Div}(\bar{V})$; and it is $\mathfrak{a}_1$ rather than $\mathfrak{a}$ which we compute. Since the image of $\mathfrak{a}$ is in $\mathcal{M}$, so is that of $\mathfrak{a} - (\eta)$; so we can take α to be the image of $\mathfrak{a}_1$ in $(\mathrm{Pic}(\bar{V})) \otimes \mathbf{Q}$. By Theorem 1, we can require the support of ξ and hence also of η to be in $\mathcal{S}_0$, and by Theorem 2 we can require the support of $\mathfrak{a}$ and therefore of $\mathfrak{a}_1$ to be in $\mathcal{S}_1$; hence $\mathfrak{a}_1$ is computable.

To obtain η from α we first lift α back to an element $\mathfrak{a}_1$ in $(\mathrm{Div}(\bar{V}))\otimes\mathbf{Q}$ with support in $\mathcal{S}_0$; then we can take η to have divisor $-d\mathfrak{a}_1$.

3. *Central simple algebras over $k(V)$.* There are in the literature two descriptions of the isomorphism between the group of equivalence classes of central simple algebras over a field L and the cohomology group $\mathrm{H}^2(L,\bar{L}^*)$. The one which we use is based on that given by Deuring ([6], Ch V) and Albert ([1], Ch V), because it is the more convenient for computation; the other can be found in Serre [7], Ch X, §5. Fortunately, Deuring's process works on any central simple algebra. We do not have to start by finding an equivalent division algebra — a process indeed which we only know how to implement by going through this isomorphism.

Let K/k be a finite Galois extension and $\mathcal{A}$ a central simple algebra with centre $k(V)$ such that $\mathcal{A}$ contains $K(V)$ and splits over it. We write

$$G=\mathrm{Gal}(K/k)=\mathrm{Gal}(K(V)/k(V)).$$

To each σ in G there corresponds an element $u_\sigma\neq 0$ in $\mathcal{A}$ such that

$$(\sigma x)u_\sigma=u_\sigma x\quad\text{for all } x \text{ in } K(V);\tag{9}$$

u_σ is determined up to left multiplication by an element of $K(V)^*$, and the u_σ form a base for $\mathcal{A}$ regarded as a $K(V)$-vector space. Let $y(\sigma,\tau)$ in $K(V)^*$ be determined for each σ,τ in G by

$$u_\sigma u_\tau=y(\sigma,\tau)u_{\sigma\tau};\tag{10}$$

then the associative law in $\mathcal{A}$ holds if and only if $\sigma,\tau\mapsto y(\sigma,\tau)$ defines a 2-cocycle with values in $K(V)^*$. Varying the u_σ changes this cocycle by an arbitrary coboundary; so the pair $\mathcal{A},K$ determines a class in $\mathrm{H}^2(G,K(V)^*)$. Conversely, given K/k we can in this way derive an algebra $\mathcal{A}$ from any class in $\mathrm{H}^2(G,K(V)^*)$ by means of the composition rules (9) and (10).

The sequence

$$\mathrm{H}^2(G,K^*)\longrightarrow\mathrm{H}^2(G,K(V)^*)\longrightarrow\mathrm{H}^2(G,K(V)^*/K^*)$$

is exact; so on taking limits as K tends to $\bar{k}$ the process above provides a way of implementing the isomorphism

$$\mathrm{Br}(k(V))/\mathrm{Br}(k)\longrightarrow\mathrm{H}^2(k,\bar{k}(V)^*/\bar{k}^*)\tag{11}$$

and more particularly the isomorphism

$$\mathrm{Br}(V)/\mathrm{Br}(k) \longrightarrow \mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*). \tag{12}$$

(The reason why it is useful to be able to implement (11) as well as (12) is that some Azumaya algebras on V are best described as corestrictions of algebras which are not themselves Azumaya.) Implementing the inverse isomorphism is more complicated. The difficulty lies in lifting a 2-cocycle with values in $\bar{k}(V)^*/\bar{k}^*$ to a 2-cocycle with values in $\bar{k}(V)^*$; once we have done this, we can use the argument in the previous paragraph. We do not know whether a class in $\mathrm{H}^2(G, K(V)^*/K^*)$ can always be lifted to a class in $\mathrm{H}^2(G, K(V)^*)$; but this is certainly possible in the most interesting case, as the following Lemma and Corollary show. The Lemma is contained in the Corollary, but for historical reasons we have stated and proved it separately.

Lemma 4 *Let $\mathcal{C}$ be a class in $H^2(G, K(V)^*/K^*)$ and ξ an element of $\mathcal{C}$. If $V(k)$ is not contained in the support of ξ then ξ can be lifted to a 2-cocycle with values in $K(V)^*$.*

Proof Suppose we lift the elements $\xi(g_1, g_2)$ of ξ back to elements $x(g_1, g_2)$ of $K(V)^*$ in any manner; then the difference of the two sides of (2) will lift back to

$$y(g, g_1, g_2) = \frac{gx(g_1, g_2).x(g, g_1g_2)}{x(gg_1, g_2).x(g, g_1)}. \tag{13}$$

These are lifts to $K(V)^*$ of the identity in $K(V)^*/K^*$, so all these expressions lie in K^*. We have to choose the $x(g_1, g_2)$ so that each of these expressions is equal to 1. Now let P be a point of $V(k)$ not in the support of ξ, and choose the $x(g_1, g_2)$ so that each of them has value 1 at P. Then the same is true of all the gx, and hence also of every expression (13). The last sentence of the Lemma now follows from (iv) of Lemma 2. □

Corollary *Let $\mathcal{C}$ be a class in $H^2(G, K(V)^*/K^*)$ and ξ an element of $\mathcal{C}$. If V contains a 0-cycle of degree 1 defined over k then ξ can be lifted to a 2-cocycle with values in $K(V)^*$.*

Proof If the hypothesis holds, standard arguments show that V contains a 0-cycle of degree 1 defined over k, no point of which lies in the support of ξ. Denote this 0-cycle by $\sum P_i - \sum Q_j$. We follow the proof of the Lemma, except that we normalize the $x(g_1, g_2)$ by imposing the condition that

$$\prod x(P_i) / \prod x(Q_j) = 1$$

instead of the condition in the proof of the Lemma. □

Of course this Lemma does not usually help us to carry out the lifting; but it shows that there are really two problems to consider, of which the first is much the more important:

- Determine whether a given 2-cocycle ξ with values in $K(V)^*/K^*$ can be lifted to a 2-cocycle x with values in $K(V)^*$, and if so exhibit such a lifting.
- Given ξ as above, exhibit a finite normal extension L/k with $L \supset K$ such that ξ can be lifted to a 2-cocycle x with values in $L(V)^*$.

As to the second problem, we remark only that it is possible to derive from [2], Ch VII, §4 a recipe for such an extension L/K, depending only on k and K, such that every class in $\mathrm{H}^2(G, K(V)^*/K^*)$ can be lifted to a class in $\mathrm{H}^2(\mathrm{Gal}(L/k), L(V)^*)$. Once L is known, the actual lifting can be carried out by the same algorithm (with L for K) which we use to solve the first problem. But the algorithm for obtaining L is clumsy, and the L which it yields may well be far larger than is really necessary. It is therefore fortunate that the solution of the second problem will seldom if ever be needed; for if we discover that the answer to the first problem is negative, it will follow that $V(k)$ is almost empty and we are likely to lose interest in V.

As we saw in the proof of Lemma 4, if we obtain x by lifting the elements of ξ to elements of $K(V)^*$ in any manner, the expressions $y(g, g_1, g_2)$ given by (13) are constants; and in view of the formula for them, they describe the coboundary of a 2-cochain with values in $K(V)^*$. Hence they describe a 3-cocycle with values in K^*. The most general lift of ξ is to elements x/b where b is a 2-cochain with values in K^*; and x/b is a 2-cocycle if and only if $y = db$. Thus our problem is equivalent to determining whether a given 3-cocycle with values in K^* is the coboundary of a 2-cochain b with values in K^*. The first step is as follows.

Theorem 3 *Let a be a 3-cocycle with values in K^*; then one can construct a finite set $\mathcal{B}$ of primes in K such that if $a = db$, where b is a 2-cochain with values in K^*, then we can choose b to be in $\mathfrak{O}^*_{\mathcal{B}}$.*

Proof We choose $\mathcal{B}$ to satisfy the following conditions:

- Every element of a lies in $\mathfrak{O}^*_{\mathcal{B}}$.
- $\mathcal{B}$ contains all the primes ramified in K/k.

- The primes in $\mathcal{B}$ generate the ideal class group of K.
- If $\mathfrak{P}$ is in $\mathcal{B}$ then so are all its conjugates over k.
- Let H be any cyclic subgroup of $\mathrm{Gal}(K/k)$ and L the fixed field of H. If $\mathfrak{p}$ is a prime in L which is inert in K/L, then there is an ideal $\mathfrak{q}$ in L which lies in the same ideal class as $\mathfrak{p}$ and is such that $\mathrm{conorm}_{K/L}\mathfrak{q}$ is in the group generated by the primes in $\mathcal{B}$ and is not divisible by any prime which ramifies in K/L.

In exhibiting a suitable $\mathcal{B}$, the only potential difficulty comes with the final condition. But since K/L is abelian, we can describe those $\mathfrak{p}$ in any assigned ideal class of L which are inert in K/L by congruence conditions; and if there are any such for a particular ideal class, we need only adjoin to $\mathcal{B}$ the conorm of one of them. However, this is very crude, and for the algorithm which follows the proof of the Theorem it is desirable to make $\mathcal{B}$ as small as possible. Thus in practice one chooses $\mathcal{B}$ in a more sophisticated way, though still subject to the five conditions above.

The rest of the proof is very similar to that of Theorem 2. Let $\mathfrak{P}$ be a prime in K which is not in $\mathcal{B}$ but which occurs in the factorization of some element of b. Let H be the inertia group of $\mathfrak{P}$ and L the fixed field of H. Since $\mathfrak{P}$ is unramified in K/k, H is cyclic and $\mathfrak{P} = \mathrm{conorm}_{K/L}\mathfrak{p}$ for some prime $\mathfrak{p}$ in L. Choose $\mathfrak{a}$ in L as in the final condition on $\mathcal{B}$, and write $\mathfrak{a}\mathfrak{p}^{-1} = (c)$ with c in L^*. We now define an operation $b \mapsto \hat{b}$; we should think of this as finding the component of $\mathfrak{P}$ and its conjugates in b and replacing them by corresponding expressions formed from $\mathfrak{a}$. Let the g_i be such that g_iH runs through the cosets of H in G. For a given element of the 2-cochain b, let $\prod(g_i\mathfrak{P})^{n_i}$ be that product of conjugates of $\mathfrak{P}$ which exactly divides it; and denote by $\hat{b}$ the 2-cochain with values in K^* whose elements are the $\prod(g_ic)^{n_i}$. Thus $\hat{b}$ is independent of the choice of the g_i and $d\hat{b} = \hat{a}$ with the analogous definition of $\hat{a}$. But $\hat{a}$ is trivial because no conjugate of $\mathfrak{P}$ appears in a. We can therefore replace b by $b\hat{b}$ without changing its coboundary; and by doing so we have removed $\mathfrak{P}$ and its conjugates from the set of primes outside $\mathcal{B}$ at which some element of b is a non-unit, without adding any new primes to this set. Repeating this operation for each of a maximal non-conjugate set of such primes, we ensure that any element of b is in $\mathfrak{O}^*_{\mathcal{B}}$. □

Once we have this Theorem, the process described in the Introduction enables us to find b if it exists, and in particular to determine whether $a = db$ for some 2-cochain b with values in K^*.

Nevertheless, this process is somewhat tedious, as is the process of making explicit the Brauer-Manin obstruction corresponding to a given Azumaya algebra expressed as a 2-cocycle. The second step reduces to finding the local invariants of the algebra at the places of bad reduction. Detailed instructions for doing this can be found in [7], Ch XIII, §3. The process described there is algorithmic, but it would be very complicated to program. One is therefore led to ask if there is a subset of algebras which admit a simpler description than by means of a 2-cocycle with values in $\bar{k}(V)^*$ and for which the calculations of local invariants can also be simplified. There is indeed such a set: at the least it contains all sums of corestrictions of quaternion algebras, and subject to a subsidiary condition we can use cyclic algebras instead of quaternion algebras.

We first describe quaternion algebras, which are the case $[G] = 2$ in the construction at (10). Write $G = \{1, \sigma\}$ and let $K = k(\sqrt{c})$ where c is in k. We can choose $u_1 = 1$, so that $y(\sigma, 1) = y(1, \sigma) = y(1, 1) = 1$; thus the algebra is completely determined by $y(\sigma, \sigma) = u_\sigma^2$, and the cocycle law is equivalent to the statement that $y(\sigma, \sigma)$ is in $k(V)^*$. The orthodox notation is to write this algebra as (c, y), where $y = y(\sigma, \sigma)$; but because we wish to regard quaternion algebras as a special case of cyclic algebras, we shall in this paper denote this algebra by $\mathcal{Z}_2(c, y)$.

Next suppose that G is a cyclic group of order $n > 1$; the case $n = 2$ is the one which we have just discussed. Fix a generator σ of G; then we can take $u_{\sigma^\nu} = (u_\sigma)^\nu$ for $1 \leq \nu < n$ and the algebra is completely determined by $u_\sigma^n = y$, which must lie in $k(V)^*$. The associated 2-cocycle is given by

$$y(\sigma^\mu, \sigma^\nu) = \begin{cases} y \text{ if } \mu + \nu \geq n, \\ 1 \text{ if } \mu + \nu < n \end{cases} \tag{14}$$

where $0 \leq \mu, \nu < n$. Such algebras are called *cyclic*; if we denote the algebra just defined by $\mathcal{Z}(K/k, \sigma, y)$ then $\mathcal{Z}(y_1)$ and $\mathcal{Z}(y_2)$ are isomorphic if and only if y_1/y_2 is a norm for $K(V)/k(V)$, and $\mathcal{Z}(y_1) \otimes \mathcal{Z}(y_2)$ is similar to $\mathcal{Z}(y_1 y_2)$. Suppose moreover that k contains the n^{th} roots of unity. Then K has the form $k(c^{1/n})$ for some c in k^*, and we can denote the algebra $\mathcal{Z}(K/k, \sigma, y)$ above by $\mathcal{Z}_n(c, \zeta, y)$, where ζ is the primitive n^{th} root of unity such that $\sigma c^{1/n} = \zeta c^{1/n}$. This is consistent with the notation for quaternion algebras introduced in the previous paragraph.

The algebras constructed in this way are in general not Azumaya; for one of them to be so, it needs to have good reduction at each absolutely irreducible component of the support of (y). Instead we need to consider finite sums $\mathcal{A} = \sum \mathcal{Z}(K_i/k, \sigma_i, y_i)$ or for simplicity

$$\mathcal{A} = \sum \mathcal{Z}_{n_i}(c_i, \zeta_i, y_i). \tag{15}$$

In view of Theorems 1 and 2 and the construction used in the proof of Lemma 1, we can restrict ourselves to the case when every y_i has support in $\mathcal{S}_1$. Let $\mathfrak{a}_j$ run through the absolutely irreducible components of $\mathcal{S}_1$ and write $(y_i) = \sum n_{ij}\mathfrak{a}_j$. Then the condition that $\mathcal{A}$ should have good reduction on $\mathfrak{a}_j$ is that $\prod c_i^{n_{ij}/n_i}$ should be in the least field of definition for $\mathfrak{a}_j$ which contains k; and $\mathcal{A}$ is Azumaya if this holds for all $\mathfrak{a}_j$. But sums (15) will usually be insufficiently general; instead we expect to have to consider sums (16) which involve corestrictions.

The use of the corestriction operator (which extends the trace) also often simplifies the description of a central simple algebra; so we remind the reader of the general description, at least in codimensions 0, 1 and 2. But when they are applicable, a better alternative is to use the projection formulae, for which see [7], p.212.

Let G, H be finite groups such that $H \subset G$, and let M be a G-module; for each $r \geq 0$ the corestriction is a certain homomorphism

$$\text{cores: } \mathrm{H}^r(H, M) \longrightarrow \mathrm{H}^r(G, M).$$

The case which concerns us in this paper is when K/k is a finite Galois extension and ℓ is a field such that $K \supset \ell \supset k$. Now $G = \mathrm{Gal}(K/k)$ and $H = \mathrm{Gal}(K/\ell)$, and the elements of M are defined over K.

Let $g_1, \ldots, g_n$ be representatives of the left cosets of H in G. For $r = 0$, $\mathrm{H}^0(H, M) = M^H$ and the corestriction is defined to be the trace map (norm map if M is multiplicative) $m \mapsto \sum_{i=1}^n g_i m$. When $r = 1$, a class in $\mathrm{H}^1(H, M)$ is represented by a 1-cocycle $h \mapsto m_h$. The corresponding class in $\mathrm{H}^1(G, M)$ is that represented by $g \mapsto m'_g$ where m'_g is defined as follows. For each i with $1 \leq i \leq n$ there exist $j = j(i, g)$ with $1 \leq j \leq n$ and $h = h(i, g)$ in H such that $gg_i = g_j h$; then $m'_g = \sum_{i=1}^n g_j m_h$. When $r = 2$, a class in $\mathrm{H}^2(H, M)$ is represented by a 2-cocycle $h_1, h_2 \mapsto m_{h_1,h_2}$. For each i define j and h'' by $g'' g_i = g_j h''$ and then define k and h' by $g' g_j = g_k h'$. The corresponding class in $\mathrm{H}^2(G, M)$ is represented by $g_1, g_2 \mapsto m'_{g_1,g_2}$ where

$$m'_{g',g''} = \sum\nolimits_{i=1}^n g_k m_{h',h''}.$$

If we replace the sum by a product, these formulae are useful both when $M = K(V)^*$ and when $M = K(V)^*/K^*$.

The natural description of an element of $\mathrm{Br}^0(V)$ is as an element of $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$, so that it is described by means of a 2-cocycle on $\mathrm{Gal}(\bar{k}/k)$ with values in $\bar{k}(V)^*/\bar{k}^*$. But this is not the most convenient description for computational purposes, both because it is rather bulky and for other reasons. Instead we can use the formula (3) to lift this cocycle to a 1-cochain with values in $(\bar{k}(V)^*/\bar{k}^*) \otimes \mathbf{Q}$ and then use the process in the penultimate paragraph of §2 to lift this cochain back to an element of $\mathrm{Pic}(\bar{V}) \otimes \mathbf{Q}$. We obtain the same result if we first lift the element of $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ back to an element of $\mathrm{H}^1(k, \mathrm{Pic}(\bar{V}))$ in the way described just before Theorem 1, and then lift this back to an element of $\mathrm{Pic}(\bar{V}) \otimes \mathbf{Q}$ by means of Lemma 1.

It will often happen that the element of $\mathrm{H}^2_{\mathrm{Az}}(k, \bar{k}(V)^*/\bar{k}^*)$ is the corestriction of an element of $\mathrm{H}^2(\ell, \bar{k}(V)^*/\bar{k}^*)$ where ℓ is a finite extension of k, or the sum of several such corestrictions. As the example in [9], §6 shows, we cannot necessarily expect the underlying elements of $\mathrm{H}^2(\ell, \bar{k}(V)^*/\bar{k}^*)$ to lie in $\mathrm{H}^2_{\mathrm{Az}}(\ell, \bar{k}(V)^*/\bar{k}^*)$. In practice, such an expression is probably only useful when these underlying algebras are cyclic. So we would like a method for deciding whether a given Azumaya algebra $\mathcal{A}$ can be written as a sum of corestrictions of cyclic algebras

$$\mathcal{A} = \sum \mathrm{cores}_{\ell_i/k} \mathcal{Z}_{n_i}(c_i, \zeta_i, y_i) \tag{16}$$

where now c_i is in ℓ_i, y_i is in $\ell_i(V)^*$, ℓ_i contains the n_i^{th} roots of unity and the field $L_i = \ell_i(\sqrt[n_i]{c_i})$. Note that if this is possible at all, it is likely that it can be done in more than one way. Unfortunately we do not know how to find the set of all representations (16) of a given Azumaya algebra $\mathcal{A}$; but what we can do is to write down all the sums of this kind which are equal to some Azumaya algebra on V over k. It would be convenient if we could lift the individual summands back to elements of $\mathrm{Pic}(\bar{V} \otimes \mathbf{Q})$ and then add the result together; but this does not seem to be possible.

As in (15), write $(y_i) = \sum n_{ij} \mathfrak{a}_j$ where $\mathfrak{a}_j$ runs through the absolutely irreducible components of $\mathcal{S}_1$. The condition for $\mathcal{A}$ to have good reduction on $\mathfrak{a}_j$ is that $\prod \mathrm{norm}_{\ell_i/k}(c_i^{n_{ij}/n_i})$ should be in the least field of definition for $\mathfrak{a}_j$ which contains k; and $\mathcal{A}$ is Azumaya if this holds for all $\mathfrak{a}_j$. We can assume that every ℓ_i is contained in K_0; for we can replace ℓ_i by $\ell_i \cap K_0$ and y_i by its norm for $\ell_i/(\ell_i \cap K_0)$. For each of the finitely many such ℓ_i, we choose y_i in $\ell_i(V)^*$ with support in $\mathcal{S}_1$; since the effect of multiplying this y_i by elements of ℓ_i^* or by n_ith powers of elements of $\ell_i(V)^*$ will be trivial, there are only finitely many choices for the y_i. We then choose c_i in ℓ_i^* so that in the notation above

$$\prod \mathrm{norm}_{\ell_i/k}(c_i^{n_{ij}/n_i}) \text{ is in the appropriate field for each } j. \tag{17}$$

We have not tried to implement this process; and in our view, finding the representation (16) is best done by hand rather than by computer. In practice, it is our impression that any relevent sums like the right hand side of (16) will force themselves on our attention, and the real question is which of them are equal. We can for example show that the two apparently quite different Brauer-Manin obstructions described in [9], §6 are actually the same.

For what follows, it is necessary to normalize the maps $\mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z}$ for finite places v; here the choice of sign differs from one author to another. (See [7], p.167.) In this paper we follow Serre [7], Ch. X, §5. For the description (16) to be useful, we need a straightforward way of computing the local invariants $\mathrm{inv}_v\mathcal{A}(P_v)$ of (16) at v-adic points P_v on V. To do this computationally we extend the functions y_i in the notation of (16) from V to the ambient space. If we choose a point P defined over k (but not necessarily lying on V) which is close enough to P_v in the v-adic topology, then $\mathrm{inv}_v\mathcal{A}(P_v) = \mathrm{inv}_v\mathcal{A}(P)$.

It is known that the local invariant $\mathrm{inv}_v\mathcal{A}(P_v)$ is trivial for all P_v in $V(k_v)$ unless v is a bad place of k. In this context the bad places consist of

- the infinite places,
- the primes which divide any n_i,
- the primes below a prime of ℓ_i at which c_i is not a unit or y_i has bad reduction for some i,
- the primes at which V has bad reduction.

The calculation of $\mathrm{inv}_v\mathcal{A}(P_v)$ at a bad place v is often made easier by using the following lemma, in which (i) is a variant of Proposition 1.1.2 of [5] and (ii) can be extracted from Chapters XII to XIV of [7]. A definition of the n^{th}-power residue symbol can be found, for example, in [7], at the beginning of Ch. XIV, §2. It involves the choice of a primitive n^{th} root of unity, and for (ii) below to hold this must be chosen to be the same ζ as appears in the left hand side of (18).

It is enough to consider the individual terms in (16).

Lemma 5 (i) *Let ℓ be a finite extension of k and $\mathcal{A}$ a central simple algebra defined over ℓ. Let v be a place of k. Then*

$$\mathrm{inv}_v(\mathrm{cores}_{\ell/k}\mathcal{A}) = \sum \mathrm{inv}_w\mathcal{A},$$

where the sum is taken over all places w of ℓ above v.

(ii) *Let ℓ be a field containing the n^{th} roots of unity, and let c', c'' be elements of ℓ^* and v a place of ℓ. Then*

$$\mathrm{inv}_v\mathcal{Z}_n(c', \zeta, c'') = (c', c'')_v \tag{18}$$

where the bracket on the right is the n^{th}-power residue symbol.

REFERENCES

[1] Albert, A.A., *Structure of Algebras* (American Mathematical Society Colloquium Publications, vol XXIV, 1939).

[2] Artin, E. and Tate, J., *Class field theory* (Harvard, 1961).

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

[4] Colliot-Thélène, J.-L., Skorobogatov, A.N. and Swinnerton-Dyer, Sir P., Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, *Invent. Math.* **134**(1998), 579-650.

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

[6] Deuring, M., *Algebren* (Springer, 1935).

[7] Serre, J.-P., *Corps Locaux* (Hermann, 1962).

[8] Swinnerton-Dyer, H.P.F., The field of definition of the Néron-Severi group, in *Studies in Pure Mathematics*, pp 719-731 (Birkhäuser, 1983).

[9] Swinnerton-Dyer, Sir Peter, Arithmetic of diagonal quartic surfaces, II, *Proc. London Math. Soc.* (3)**80**(2000), 513-544.

Faulkes Institute for Geometry,
Cambridge University

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