COMPOSITIO MATHEMATICA

Brauer–Manin obstruction for integral points of homogeneous spaces and representation by integral quadratic forms

Jean-Louis Colliot-Thélène and Fei Xu

Compositio Math. **145** (2009), 309–363.

doi:10.1112/S0010437X0800376X

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

Compositio Math. 145 (2009) 309–363
doi:10.1112/S0010437X0800376X

Brauer–Manin obstruction for integral points of homogeneous spaces and representation by integral quadratic forms

Jean-Louis Colliot-Thélène and Fei Xu

De toute façon, les considérations exposées ici se prêtent à des généralisations variées, qu'il n'entrait pas dans notre propos d'examiner pour l'instant.
A. Weil [Wei62]

Abstract

An integer may be represented by a quadratic form over each ring of p-adic integers and over the reals without being represented by this quadratic form over the integers. More generally, such failure of a local-global principle may occur for the representation of one integral quadratic form by another integral quadratic form. We show that many such examples may be accounted for by a Brauer–Manin obstruction for the existence of integral points on schemes defined over the integers. For several types of homogeneous spaces of linear algebraic groups, this obstruction is shown to be the only obstruction to the existence of integral points.

Résumé

Une forme quadratique entière peut être représentée par une autre forme quadratique entière sur tous les anneaux d'entiers p-adiques et sur les réels, sans l'être sur les entiers. On en trouve de nombreux exemples dans la littérature. Nous montrons qu'une partie de ces exemples s'explique au moyen d'une obstruction de type Brauer–Manin pour les points entiers. Pour plusieurs types d'espaces homogènes de groupes algébriques linéaires, cette obstruction est la seule obstruction à l'existence d'un point entier.

Introduction

Representation of an integral quadratic form, of rank n, by another integral quadratic form, of rank $m \geq n$, has been a subject of investigation for many years. The most natural question is that of the representation of an integer by a given integral quadratic form ($n = 1$, m arbitrary).

Scattered in the literature one finds many examples where the problem can be solved locally, that is over the reals and over all the rings $\mathbb{Z}_p$ of p-adic integers, but the problem cannot be solved over $\mathbb{Z}$: these are counterexamples to a local-global principle for the problem of integral representation. One here encounters such concepts as that of 'spinor exceptions'.

It is the purpose of the present paper to give a conceptual framework for entire series of such counterexamples.

Received 4 February 2008, accepted in final form 4 June 2008, published online 10 March 2009.
2000 Mathematics Subject Classification 11D85, 11E12, 11E20, 11E57, 11E72, 11G35, 14G25, 14F22, 20G30.
Keywords: integral quadratic forms, integral points, Hasse principle, Brauer–Manin obstruction, spinor exceptions, homogeneous spaces of linear algebraic groups, Galois cohomology.

The situation resembles the one which Manin encountered in 1970 regarding the classical Hasse principle, namely the question of existence of a rational point on a variety defined over the rationals when one knows that there are points in each completion of $\mathbb{Q}$. Manin analyzed most of the then known counterexamples by means of the Brauer group of varieties.

Our key tool is a straightforward variation on the Brauer–Manin obstruction, which we call the integral Brauer–Manin obstruction. We are over a number field k, with ring of integers O, and we are interested in the integral points of a certain O-scheme $\mathbf{X}$ associated to the representation problem. An important point is that, even though we are interested in the set of integral points of the scheme $\mathbf{X}$, the Brauer group which we use is the Brauer group of the k-variety $X = \mathbf{X} \times_O k$, and not the Brauer group of $\mathbf{X}$, as one would naively imagine. This obstruction is defined in § 1.

In this paper we restrict attention to the problem of representation of a form g of rank $n \geq 1$ by a form f of rank $m \geq 3$. Then the k-varieties which underly the problem are homogeneous spaces of spinor groups.

In § 2 we discuss Brauer groups and Brauer pairings on homogeneous spaces of connected linear algebraic groups over an arbitrary field.

In the next two sections we discuss rational and integral points on homogeneous spaces under an arbitrary connected linear group G. There are two types of results, depending on whether the geometric stabilizer is connected (§ 3) or whether it is a finite commutative group (§ 4). For integral points, the main results, Theorems 3.7 and 4.5, assert that the integral Brauer–Manin obstruction to the existence of an integral point is the only obstruction provided the group G is simply connected and satisfies an isotropy condition at the archimedean places. These conditions ensure that the group G satisfies the strong approximation theorem.

The tools we use have already been used most efficiently in the study of rational points, by Sansuc [San81] and Borovoi [Bor96]. Our results on rational points are very slight extensions of their results. Some results on integral points already appear in a paper by Borovoi and Rudnick [BR95]. It has recently come to our attention that further related results appear in the appendix of a paper by Erovenko and Rapinchuk [ER06].

For the representation problem of quadratic forms over the integers, the isotropy condition is that the form f is 'indefinite', i.e. isotropic at some archimedean completion of the number field k. In this case, if there is no integral Brauer–Manin obstruction, as defined in the present paper, then the form g is represented by f over the integers. As may be expected, the cases $m - n \geq 3$ (Theorem 6.1), $m - n = 2$ (Theorem 6.3) and $1 \geq m - n \geq 0$ (Theorem 6.4) each require a separate discussion. For $m - n \geq 3$, the geometric stabilizer is simply connected, there are no Brauer–Manin obstructions, the result on representation by indefinite forms is classical. For $m - n = 2$, the geometric stabilizer is a one-dimensional torus. For $1 \geq m - n \geq 0$, the geometric stabilizer is $\mathbb{Z}/2$.

In § 7 we compare the results obtained in § 6 with classical results in terms of genera and spinor genera. We take a new look at the notion of 'spinor exception'.

In § 8 we show how various examples in the literature can all be interpreted in terms of the integral Brauer–Manin obstruction. We also illustrate the general results by a theorem, a special case of which is: Let $f(x_1, \ldots, x_n)$, respectively $l(x_1, \ldots, x_n)$, be a polynomial of total degree 2, respectively total degree 1, with coefficients in $\mathbb{Z}$. Assume that l does not divide f, that the affine $\mathbb{Q}$-variety defined by $f = l = 0$ is smooth, and that its set of real points is noncompact. For $n \geq 5$, the existence of solutions to $f = l = 0$ in all $\mathbb{Z}_p$ implies the existence of solutions in $\mathbb{Z}$. For $n = 4$, this is so if and only if there is no Brauer–Manin obstruction (a condition which in this case can easily be checked).

In § 9 we apply the technique to recover a theorem characterizing sums of three squares in the ring of integers of an imaginary quadratic field – without using computation of integral spinor norms and Gauss genus theory. In Appendix A, this kind of argument also enables Dasheng Wei and the second named author to establish a local-global principle for sums of three squares in the ring of integers of an arbitrary cyclotomic field.

1. Notation; the integral Brauer–Manin obstruction

For an arbitrary scheme X, with structural sheaf O_X, we let $\mathrm{Pic}\, X = H^1_{\mathrm{Zar}}(X, O_X^*)$ denote the Picard group of X. Given a sheaf $\mathcal{F}$ on the étale site of X, we let $H^r_{\text{ét}}(X, \mathcal{F})$ denote the étale cohomology groups of the sheaf $\mathcal{F}$. There is a natural isomorphism $\mathrm{Pic}\, X \simeq H^1_{\text{ét}}(X, \mathbb{G}_m)$, where $\mathbb{G}_m$ is the étale sheaf associated to the multiplicative group $\mathbb{G}_m$ over X. The Brauer group of X is $\mathrm{Br}\, X = H^2_{\text{ét}}(X, \mathbb{G}_m)$. For background on the Brauer group, we refer to Grothendieck's exposés [Gro68].

Let k be a field. A k-variety is a separated k-scheme of finite type. Given a k-variety X and a field extension K/k we set $X_K = X \times_k K$. For $K = \overline{k}$ a separable closure of k we write $\overline{X} = X \times_k \overline{k}$. We let $K[X] = H^0(X_K, O_{X_K})$ be the ring of global functions on X_K. We let $K[X]^*$ be the group of units in that ring. We let $X(K)$ be the set of K-rational points of X, that is $X(K) = \mathrm{Hom}_k(\mathrm{Spec}\, K, X)$.

Let k be a number field and O its ring of integers. Let Ω_k denote the set of places of k. For $v \in \Omega_k$ we let k_v denote the completion of k at v. For v nonarchimedean we let O_v denote the ring of integers in k_v. For each place v, class field theory yields an embedding $\mathrm{inv}_v : \mathrm{Br}\, k_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$.

Let S be a finite set of places of k containing all archimedean places. Let $O_S \subset k$ be the rings of elements which are integral outside of S, also known as the ring of S-integers. Let $\mathbf{X}$ be a scheme separated and of finite type over the ring O_S. The set $\mathbf{X}(O_S)$ is the set of S-integral points of $\mathbf{X}$.

Let $X = \mathbf{X} \times_{O_S} k$. For any commutative integral O_S-algebra A with field of fractions F, the natural map

$$\mathbf{X}(A) = \mathrm{Hom}_{O_S}(\mathrm{Spec}\, A, \mathbf{X}) \to X(F) = \mathrm{Hom}_k(\mathrm{Spec}\, F, X)$$

is an injection. If $\mathbf{Y} \subset \mathbf{X}$ denotes the schematic closure of X in $\mathbf{X}$ then $\mathbf{Y}(A) = \mathbf{X}(A)$. For all problems considered here, we could thus replace $\mathbf{X}$ (which may have very bad special fibres) by the flat O-scheme $\mathbf{Y}$.

We may thus view the set $\mathbf{X}(O_S)$ as a subset of $X(k)$ and for each place $v \notin S$ of k we may view $\mathbf{X}(O_v)$ as a subset of $X(k_v)$. The latter space is given the topology induced by that of the local field k_v. As one easily checks, $\mathbf{X}(O_v)$ is open in $X(k_v)$. If $U \subset X$ is a dense Zariski open set of X, if X/k is smooth, the implicit function theorem implies that $U(k_v)$ is dense in $X(k_v)$. This implies that $\mathbf{X}(O_v) \cap U(k_v)$ is dense in $\mathbf{X}(O_v)$.

An adèle of the k-variety X is a family $\{x_v\} \in \prod_{v \in \Omega_k} X(k_v)$ such that, for almost all v, the point x_v belongs to $\mathbf{X}(O_v)$. This definition does not depend on the model $\mathbf{X}/O_S$. The set of adèles of X is denoted $X(\mathcal{A}_k)$. There is a natural diagonal embedding $X(k) \subset X(\mathcal{A}_k)$.

There is a natural pairing between $X(\mathcal{A}_k)$ and the Brauer group $\mathrm{Br}\, X = H^2_{\text{ét}}(X, \mathbb{G}_m)$ of X:

$$X(\mathcal{A}_k) \times \mathrm{Br}\, X \to \mathbb{Q}/\mathbb{Z},$$
$$(\{x_v\}, \alpha) \mapsto \sum_v \mathrm{inv}_v(\alpha(x_v)).$$

This pairing is known as the Brauer–Manin pairing.

Any element of $X(k)$ is in the left kernel of that pairing. The image of $\mathrm{Br}\, k \to \mathrm{Br}\, X$ is in the right kernel of that pairing.

When X/k is proper, for a given element $\alpha \in \mathrm{Br}\, X$, there exists a finite set S_α of places of k such that, for $v \notin S_\alpha$ and any $M_v \in X(k_v)$, $\alpha(M_v) = 0$. This enables one to produce and analyze counterexamples to the Hasse principle. For background on the Brauer–Manin obstruction, we refer the reader to [Sko01] and the literature cited there.

When X/k is not proper, for $\alpha \in \mathrm{Br}\, X$, there is in general no such finite set S_α of places; the pairing seems to be useless. The situation changes when one restricts attention to integral points.

The above pairing induces a pairing

$$\left[\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)\right] \times \mathrm{Br}\, X \to \mathbb{Q}/\mathbb{Z},$$

which vanishes on the image of $X(k)$ on the left hand side and vanishes on the image of $\mathrm{Br}\, k \to \mathrm{Br}\, X$ on the right hand side. That is, we have an induced pairing

$$\left[\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)\right] \times \mathrm{Br}\, X/\mathrm{Br}\, k \to \mathbb{Q}/\mathbb{Z}.$$

In the present context, the Brauer–Manin set

$$\left(\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)\right)^{\mathrm{Br}\, X}$$

is by definition the left kernel of either of the above pairings. We have the inclusions

$$\mathbf{X}(O_S) \subset \left(\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)\right)^{\mathrm{Br}\, X} \subset \left(\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)\right).$$

If the product $(\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v))$ is not empty but the Brauer–Manin set is empty, we say there is a Brauer–Manin obstruction to the existence of an S-integral point on $\mathbf{X}$.

For a given $\alpha \in \mathrm{Br}\, X$, there exists a finite set $S_{\alpha,\mathbf{X}}$ of places v of k with $S \subset S_{\alpha,\mathbf{X}}$ such that, for any $v \notin S_{\alpha,\mathbf{X}}$ and $M_v \in \mathbf{X}(O_v)$, we have $\alpha(M_v) = 0$ (see [Sko01, § 5.2, p. 101]). For a given $\alpha \in \mathrm{Br}\, X$, computing the image of the evaluation map

$$ev(\alpha) : \left(\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)\right) \to \mathbb{Q}/\mathbb{Z}$$

is thus reduced to a finite amount of computations.

If the quotient $\mathrm{Br}\, X/\mathrm{Br}\, k$ is finite, only finitely many computations are needed to decide if the Brauer–Manin set is empty or not.

Cohomology in this paper will mostly be étale cohomology. Over a field k with separable closure $\overline{k}$ and Galois group $\mathfrak{g} = \mathrm{Gal}(\overline{k}/k)$, étale cohomology is just Galois cohomology. For a continuous discrete $\mathfrak{g}$-module M, we shall denote by $H^r(\mathfrak{g}, M)$ or $H^r(k, M)$ the Galois cohomology groups. Given a linear algebraic group H over k, one has the pointed cohomology set $H^1(k, H)$. This set classifies (right) principal homogeneous spaces under H, up to nonunique isomorphism. Over an arbitrary k-scheme X, one has the pointed cohomology set $H^1_{\text{ét}}(X, H)$. This set classifies (right) principal homogeneous spaces over X under the group H, up to nonunique isomorphism. In this relative context, (right) principal homogeneous spaces will be referred to as torsors.

2. Brauer groups and Brauer–Manin pairing for homogeneous spaces

In this whole section, k denotes a field of characteristic zero, $\overline{k}$ an algebraic closure of k, and $\mathfrak{g}$ the Galois group of $\overline{k}$ over k.

For any k-variety X, let

$$\mathrm{Br}_1\, X = \mathrm{Ker}[\mathrm{Br}\, X \to \mathrm{Br}\, \overline{X}].$$

Let us first recall some known results.

Lemma 2.1. *One has a natural exact sequence*

$$0 \to H^1(\mathfrak{g}, \overline{k}[Y]^*) \to \mathrm{Pic}\, Y \to (\mathrm{Pic}\, \overline{Y})^{\mathfrak{g}} \to H^2(\mathfrak{g}, \overline{k}[Y]^*) \\ \to \mathrm{Br}_1\, Y \to H^1(\mathfrak{g}, \mathrm{Pic}\, \overline{Y}) \to H^3(\mathfrak{g}, \overline{k}[Y]^*)$$

and the last map in this sequence is zero if the natural map $H^3(\mathfrak{g}, \overline{k}[Y]^*) \to H^3_{\text{ét}}(Y, \mathbb{G}_m)$ is injective.

Proof. This is the exact sequence of terms of low degree attached to the spectral sequence $E_2^{pq} = H^p(k, H^q_{\text{ét}}(\overline{Y}, \mathbb{G}_m)) \Longrightarrow H^n_{\text{ét}}(Y, \mathbb{G}_m)$. □

Proposition 2.2 (Sansuc). *Let H/k be a connected linear algebraic group. Let $\hat{H}$ denote the (geometric) character group of H. This is a finitely generated, $\mathbb{Z}$-free, discrete Galois module. Let X be a smooth connected k-variety and $p : Y \to X$ be a torsor over X under H. There is a natural exact sequence of abelian groups*

$$0 \to k[X]^*/k^* \to k[Y]^*/k^* \to \hat{H}(k) \to \mathrm{Pic}\, X \to \mathrm{Pic}\, Y \to \mathrm{Pic}\, H \to \mathrm{Br}\, X \to \mathrm{Br}\, Y. \tag{2.1}$$

In this sequence, the abelian groups $k[X]^*/k^*$, $k[Y]^*/k^*$ and $\hat{H}(k)$ are finitely generated and free, and the group $\mathrm{Pic}\, H$ is finite.

Proof. This is [San81, Proposition 6.10]. □

The map $\nu(Y)(k) : \hat{H}(k) \to \mathrm{Pic}\, X$ is the obvious map: given a character χ of H and the H-torsor Y over X, one produces a $\mathbb{G}_m$-torsor over X by the change of structural group defined by χ. We let $\nu(Y) : \hat{H} \to \mathrm{Pic}\, \overline{X}$ be the associated Galois-equivariant map over $\overline{k}$.

Any extension

$$1 \to \mathbb{G}_m \to H_1 \to H \to 1$$

of a group H by the torus $\mathbb{G}_m$ defines a $\mathbb{G}_m$-torsor over H, hence a class in $\mathrm{Pic}\, H$. The induced map

$$\mathrm{Ext}_{k\text{-gp}}(H, \mathbb{G}_m) \to \mathrm{Pic}\, H$$

is functorial in the group H.

Assume that H is a connected linear algebraic group. Then the extension is automatically central, and the above map is an isomorphism

$$\mathrm{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_{m,k}) \xrightarrow{\simeq} \mathrm{Pic}\, H$$

(see [Col08, Corollary 5.7]). Here $\mathrm{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_m)$ denotes the abelian group of isomorphism classes of central extensions of k-algebraic groups of H by $\mathbb{G}_m$.

Let H be an algebraic group over k, let X be a k-variety and $p : Y \to X$ be a torsor over X under H. There is an associated class ξ in the cohomology set $H^1_{\text{ét}}(X, H)$. Given any central extension of algebraic groups

$$1 \to \mathbb{G}_m \to H_1 \to H \to 1,$$

there is a natural exact sequence of pointed sets

$$H^1_{\text{ét}}(X, H_1) \to H^1_{\text{ét}}(X, H) \to H^2_{\text{ét}}(X, \mathbb{G}_m) = \text{Br}\, X.$$

We thus have a natural pairing

$$H^1_{\text{ét}}(X, H) \times \text{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_m) \to \text{Br}\, X$$

and this pairing is linear on the right hand side, functorial in the k-scheme X and functorial in the k-group H. To the torsor Y there is thus associated a homomorphism of abelian groups

$$\rho_{\text{tors}}(Y) : \text{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_m) \to \text{Br}\, X.$$

If H is connected this map induces a homomorphism

$$\delta_{\text{tors}}(Y) : \text{Pic}\, H \to \text{Br}\, X.$$

Proposition 2.3. *Let H be a connected linear algebraic group over k. Let H_1, X, Y be as above. Assume* $\text{Pic}\, Y = 0$ *and $Y(k) \neq \emptyset$. Then $\rho_{\text{tors}}(Y)$ and $\delta_{\text{tors}}(Y)$ are injective.*

Proof. If the class of the central extension

$$1 \to \mathbb{G}_m \to H_1 \to H \to 1$$

is in the kernel of $\rho_{\text{tors}}(Y)$ then the class of Y in $H^1_{\text{ét}}(X, H)$ is in the kernel of the map $H^1_{\text{ét}}(X, H) \to H^2_{\text{ét}}(X, \mathbb{G}_m) = \text{Br}\, X$. There thus exists a torsor Z/X under the k-group H_1 such that the H-torsor $Z \times^{H_1} H/X$ is H-isomorphic to the H-torsor Y/X. The projection map $Z \to Y$ makes Z into a $\mathbb{G}_m$-torsor over Y. Since $\text{Pic}\, Y = 0$, there exists a k-morphism $\sigma : Y \to Z$ which is a section of the projection $p : Z \to Y$. Fix $y \in Y(k)$. Let $z = \sigma(y) \in Z(k)$ and let $x \in X(k)$ be the image of y under $Y \to X$. Taking fibres over x, we get an H_1-torsor Z_x over k with the k-point z, an H-torsor Y_x with the k-point y, a projection $Z_x \to Y_x$ compatible with the actions of H_1 and H and a section $\sigma_x : Y_x \to Z_x$ sending y to z. The k-homomorphism $H_1 \to H$ thus admits a scheme-theoretic section $\tau : H \to H_1$.

At this point we can appeal to the injectivity of $\text{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_{m,k}) \xrightarrow{\simeq} \text{Pic}\, H$ (see [Col08, Corollary 5.7]) to conclude. Alternatively, we observe that the section τ sends the unit element of H to the unit element of H_1. It is *a priori* just a k-morphism of varieties. Because H_1 is a central extension of the connected k-group H by a torus, this implies that τ is a homomorphism of algebraic groups (this is a consequence of Rosenlicht's lemma, see [Col08, proof of Proposition 3.2]). Thus the central extension is split. □

Remark 2.4. If we assume X is geometrically integral, hence also Y, or if H is characterfree, one may dispense with the assumption $Y(k) \neq \emptyset$.

With notation as in the proposition, Sansuc's Proposition 2.2 yields an exact sequence $\text{Pic}\, Y \to \text{Pic}\, H \to \text{Br}\, X$. If one could prove that the map $\text{Pic}\, H \to \text{Br}\, X$ in that sequence coincides (up to a sign) with the map $\delta_{\text{tors}}(Y)$, this would give another proof of Proposition 2.3.

Proposition 2.5. *Let G be a connected linear algebraic group over k and let $H \subset G$ be a closed subgroup, not necessarily connected. Let $X = G/H$. Then there is a natural exact sequence*

$$\hat{G}(k) \to \hat{H}(k) \to \text{Pic}\, X \to \text{Pic}\, G.$$

Proof. See Proposition 3.2 of the paper *The Picard group of a G-variety*, by H. Knop, H.-P. Kraft and T. Vust in [KSS89, pp. 77–87]. The proof there is given over an algebraically closed field.

One checks that it extends to the above statement. The map $\hat{H}(k) \to \operatorname{Pic} X$ is the map $\nu(G)(k)$ associated to the H-torsor G over $X = G/H$. □

Proposition 2.6. *Let G/k be a semisimple simply connected group. Let Y/k be a k-variety. Assume there exists an isomorphism of $\overline{k}$-varieties $\overline{G} \simeq \overline{Y}$. We have*

(i) *the natural map $k^* \to k[Y]^*$ is an isomorphism;*

(ii) $\operatorname{Pic} Y = 0$;

(iii) *the natural map $\operatorname{Br} k \to \operatorname{Br} Y$ is bijective.*

Proof. First consider the case $Y = G$ semisimple simply connected and $k = \overline{k}$. In this case it is well known that $k^* = k[G]^*$ and that $\operatorname{Pic} G = 0$. Let us give details for the slightly less known vanishing of $\operatorname{Br} \overline{G}$. One reduces to the case $\overline{k} = \mathbb{C}$ and uses $\pi_1 \overline{G} = 0$ and $\pi_2 \overline{G} = 0$ (Élie Cartan). The universal coefficient theorem then implies $H^2_{\text{top}}(\overline{G}, \mathbb{Z}/n) = 0$ for any positive integer n. The comparison theorem then implies $H^2_{\text{ét}}(\overline{G}, \mu_n) = 0$ for all n, hence ${}_n\operatorname{Br} \overline{G} = 0$ for all n, hence $\operatorname{Br} \overline{G} = 0$ since that group is a torsion group (as is the Brauer group of any regular scheme, see [Gro68, II, Proposition 1.4]). All statements now follow from the results over $\overline{k}$ and Lemma 2.1. □

Let H be a (not necessarily connected) linear algebraic group over k. Let $M = H^{\text{mult}}$ denote the maximal quotient of H which is a group of multiplicative type. Let $\hat{M} = \hat{H}$ denote the (geometric) character group of H. This is a finitely generated discrete $\mathfrak{g}$-module, which we view as a commutative k-group scheme locally of finite type. It coincides with the (geometric) character group of H^{mult}. If H is connected, $M = H^{\text{mult}}$ is a k-torus, which is then denoted H^{tor}, and $\hat{H}$ is $\mathbb{Z}$-torsionfree.

Proposition 2.7. *Let $Y \to X$ be an H-torsor. With notation as above, the diagram*

$$\begin{array}{ccccc}
X(k) & \times & \operatorname{Br} X & \longrightarrow & \operatorname{Br} k \\
\downarrow{\scriptstyle ev_Y} & & \uparrow{\scriptstyle \rho_{\text{tors}}(Y)} & & \| \\
H^1(k, H) & \times & \operatorname{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_m) & \longrightarrow & \operatorname{Br} k \\
\downarrow & & \uparrow & & \| \\
H^1(k, M) & \times & \operatorname{Ext}^c_{k\text{-gp}}(M, \mathbb{G}_m) & \longrightarrow & \operatorname{Br} k \\
\| & & \uparrow & & \| \\
H^1(k, M) & \times & \operatorname{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m) & \longrightarrow & \operatorname{Br} k \\
\| & & \uparrow{\scriptstyle \simeq} & & \| \\
H^1(k, M) & \times & H^1(k, \hat{M}) & \longrightarrow & \operatorname{Br} k
\end{array} \tag{2.2}$$

is commutative.

Proof. Commutativity of the first diagram follows from functoriality. Commutativity of the second and third diagrams, where $\operatorname{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m)$ denotes the group of isomorphism classes of extensions of M by $\mathbb{G}_m$ in the category of abelian k-group schemes, is also a matter of functoriality.

For the construction of the last diagram and the proof of its commutativity, most ingredients may be found in Chapter I, § 0 of Milne's book [Mil86]. Proposition 0.14 *op. cit.* establishes a similar diagram at the level of Galois modules, Galois cohomology and extensions of Galois modules. In the present context of commutative algebraic groups, the definition of maps and pairing must be adapted. The map $H^1(k, \hat{M}) \to \mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m)$ comes from the spectral sequence in Proposition 0.17 *op. cit.* For the pairings, see Proposition 0.16 *op. cit.* For the commutativity, one uses [Mil80] V.1.20, which produces a variant of the above mentioned Proposition 0.14 in the more general context required here (see the comments in the proof of the quoted proposition). □

The group $\mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m)$ classifies extensions

$$1 \to \mathbb{G}_m \to E \to M \to 1,$$

where E is a commutative algebraic group over k. The group E is then a k-group of multiplicative type. Over $\overline{k}$ any such extension is split.

The injective map $\mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m) \to \mathrm{Ext}^c_{k\text{-gp}}(M, \mathbb{G}_m)$ has for its image the group of central extensions of M by $\mathbb{G}_m$ which split over $\overline{k}$.

Thus the composite map

$$H^1(k, \hat{M}) \to \mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m) \to \mathrm{Ext}^c_{k\text{-gp}}(M, \mathbb{G}_m) \to \mathrm{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_m)$$

has its image in the subgroup of extensions split over $\overline{k}$, and the composite map

$$H^1(k, \hat{M}) \to \mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m) \to \mathrm{Ext}^c_{k\text{-gp}}(M, \mathbb{G}_m) \to \mathrm{Ext}^c_{k\text{-gp}}(H, \mathbb{G}_m) \to \mathrm{Br}\, X$$

has its image in the subgroup $\mathrm{Br}_1\, X \subset \mathrm{Br}\, X$. Since $\hat{M} \simeq \hat{H}$ this gives rise to a map

$$\theta(Y) : H^1(k, \hat{H}) \to \mathrm{Br}_1\, X.$$

We are indebted to T. Szamuely for a discussion of the following proposition.

PROPOSITION 2.8. *Let H be a not necessarily connected linear algebraic group, let $M = H^{\mathrm{mult}}$ and let $Y \to X$ be an H-torsor. Let $\nu(Y) : \hat{H} \to \mathrm{Pic}\, \overline{X}$ be the associated homomorphism. The induced map $H^1(k, \hat{H}) \to H^1(k, \mathrm{Pic}\, \overline{X})$ coincides with the composite of the map $\theta(Y)$: $H^1(k, \hat{H}) \to \mathrm{Br}_1\, X$ with the map $\mathrm{Br}_1\, X \to H^1(k, \mathrm{Pic}\, \overline{X})$ in Lemma 2.1.*

Proof. To prove this proposition one may replace the H-torsor Y by the M-torsor $Y \times^H M$. In other words, it is enough to prove the proposition in the case $H = M$ is a k-group of multiplicative type.

The map $\theta(Y)$ here is induced by the composite map

$$H^1(k, \hat{M}) \to \mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m) \to \mathrm{Br}\, X,$$

where the map $\mathrm{Ext}_{k\text{-abgp}}(M, \mathbb{G}_m) \to \mathrm{Br}\, X$ is given by the M-torsor Y (see the discussion before Proposition 2.3). The composite map clearly has its image in $\mathrm{Br}_1\, X$. One first observes that the map $\theta(Y) : H^1(k, \hat{M}) \to \mathrm{Br}_1\, X$ as defined above coincides with the map given by cup-product with the class of the torsor Y in $H^1_{\text{ét}}(X, M)$. For this we refer to [GH70, GH71] and to [Mil80, Proposition 1.20 in Chapter V]. (The case $X = \mathrm{Spec}\, k$ already appears in Proposition 2.7.)

We have a natural pairing of sheaves $\hat{M} \times M \to \mathbb{G}_m$ on the big étale site of Spec k. Consider the following diagram.

$$\begin{array}{ccccc} H^1(k, \hat{M}) & \times & H^1_{\text{ét}}(X, M) & \longrightarrow & \mathrm{Br}_1\, X \\ \downarrow = & & \downarrow & & \downarrow \\ H^1(k, \hat{M}) & \times & \mathrm{Hom}_k(\hat{M}, \mathrm{Pic}\, \overline{X}) & \longrightarrow & H^1(k, \mathrm{Pic}\, \overline{X}) \end{array} \tag{2.3}$$

In this diagram the top pairing is induced by cup-product. The map $H^1_{\text{ét}}(X, M) \to \mathrm{Hom}_k(\hat{M}, \mathrm{Pic}\, \overline{X})$ is the natural map associating to an M-torsor Y over X its type $\nu(Y)$. Given $\alpha \in H^1(k, \hat{M})$, the bottom map sends it to the map which sends $\nu \in \mathrm{Hom}_k(\hat{M}, \mathrm{Pic}\, \overline{X})$ to $\nu(\alpha)$. The map $\mathrm{Br}_1\, X \to H^1(k, \mathrm{Pic}\, \overline{X})$ is the map coming from the Hochschild–Serre spectral sequence. Theorem 4.1.1 of Skorobogatov's book [Sko01], the proof of which is rather elaborate, shows that this diagram is commutative. Combining this with the above compatibility establishes the result. □

Proposition 2.9. *Let H be a connected linear algebraic group over the field k. With notation as above, the group $M = H^{\mathrm{mult}}$ is a torus. Any algebraic group extension of H by $\mathbb{G}_m$ is central and any algebraic group extension of the k-torus M by $\mathbb{G}_m$ is commutative. There are natural compatible isomorphisms of finite groups*

$$\mathrm{Ext}_{k\text{-gp}}(H, \mathbb{G}_m) \xrightarrow{\simeq} \mathrm{Pic}\, H$$

and

$$\mathrm{Ext}_{k\text{-gp}}(M, \mathbb{G}_m) \xrightarrow{\simeq} \mathrm{Pic}\, M.$$

Let $Y \to X$ be an H-torsor. The diagram in the previous proposition yields a commutative diagram as follows.

$$\begin{array}{ccccc} X(k) & \times & \mathrm{Br}\, X & \longrightarrow & \mathrm{Br}\, k \\ \downarrow ev_Y & & \uparrow \delta_{\mathrm{tors}}(Y) & & \| \\ H^1(k, H) & \times & \mathrm{Pic}\, H & \longrightarrow & \mathrm{Br}\, k \\ \downarrow & & \uparrow & & \| \\ H^1(k, M) & \times & \mathrm{Ker}[\mathrm{Pic}\, H \to \mathrm{Pic}\, \overline{H}] & \longrightarrow & \mathrm{Br}\, k \\ \| & & \uparrow \simeq & & \| \\ H^1(k, M) & \times & H^1(k, \hat{M}) & \longrightarrow & \mathrm{Br}\, k \end{array} \tag{2.4}$$

Proof. The first two statements are well known. The two isomorphisms have been discussed above.

That $\mathrm{Pic}\, H$ is a finite group is a well known fact (see [Col08], Rappel 0.5, Proposition 3.3, Proposition 6.3 and the literature cited there). Part of the right vertical map in the previous diagram now reads

$$H^1(k, \hat{M}) \simeq \mathrm{Pic}\, M \to \mathrm{Pic}\, H.$$

The statement now follows from Proposition 2.7 provided we show that the map $\mathrm{Pic}\, M \to \mathrm{Pic}\, H$ induces an isomorphism $\mathrm{Pic}\, M \to \mathrm{Ker}[\mathrm{Pic}\, H \to \mathrm{Pic}\, \overline{H}]$. We have the exact sequence of connected algebraic groups

$$1 \to H_1 \to H \to M \to 1,$$

where H_1 is a smooth connected characterfree algebraic group. Applying Proposition 2.2 to this sequence we get the exact sequences

$$0 \to \mathrm{Pic}\, M \to \mathrm{Pic}\, H \to \mathrm{Pic}\, H_1$$

and

$$0 \to \mathrm{Pic}\, \overline{M} \to \mathrm{Pic}\, \overline{H} \to \mathrm{Pic}\, \overline{H}_1,$$

which simply reads $\mathrm{Pic}\, \overline{H} \hookrightarrow \mathrm{Pic}\, \overline{H}_1$. Moreover Rosenlicht's lemma and Lemma 2.1 show that the obvious map $\mathrm{Pic}\, H_1 \to \mathrm{Pic}\, \overline{H}_1$ is injective. This is enough to conclude. □

Proposition 2.10. *Let G be a semisimple, simply connected algebraic group over k and $H \subset G$ a connected k-subgroup. Let $X = G/H$. Projection $G \to G/H$ makes G into a right H-torsor $Y \to X$. Let $\mathrm{Br}_* X \subset \mathrm{Br}\, X$ be the group of elements vanishing at the point of $X(k)$ which is the image of $1 \in G(k)$. Projection $\mathrm{Br}\, X \to \mathrm{Br}\, X/\mathrm{Br}\, k$ induces an isomorphism $\mathrm{Br}_* X \to \mathrm{Br}\, X/\mathrm{Br}\, k$.*

(i) *The natural map $\nu(G) : \hat{H}(k) \to \mathrm{Pic}\, X$ is an isomorphism.*

(ii) *The map $\delta_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \to \mathrm{Br}\, X$ attached to the torsor $G \to G/H = X$ induces isomorphisms*

$$\delta'_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \xrightarrow{\simeq} \mathrm{Br}_* X \simeq \mathrm{Br}\, X/\mathrm{Br}\, k.$$

(iii) *Let X_c be a smooth compactification of X. There is an isomorphism between $\mathrm{Br}\, X_c$ and the group of elements of $H^1(\mathfrak{g}, \hat{H})$ whose restriction to each procyclic subgroup of $\mathfrak{g}$ is zero.*

Proof. For (i) use either Proposition 2.2 or 2.5.

Let us prove (ii). The map $\delta_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \to \mathrm{Br}\, X$ sends $\mathrm{Pic}\, H$ to $\mathrm{Br}_* X \subset \mathrm{Br}\, X$. By Proposition 2.3, the map $\delta_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \to \mathrm{Br}\, X$ is injective. We thus have an injective homomorphism $\mathrm{Pic}\, H \to \mathrm{Br}_* X$. By Proposition 2.6, $\mathrm{Pic}\, G = 0$ and the natural map $\mathrm{Br}\, k \to \mathrm{Br}\, G$ is an isomorphism. Sansuc's Proposition 2.2 gives *some* isomorphism $\mathrm{Pic}\, H \simeq \mathrm{Br}_* X$. Since the group $\mathrm{Pic}\, H$ is finite, we conclude that $\delta_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \to \mathrm{Br}_* X$ is an isomorphism.

Statement (iii) is a special case of [CK06, main theorem]. □

Remark 2.11. If the connected group H has no characters, then the map $\mathrm{Pic}\, H \to \mathrm{Pic}\, \overline{H}$ is injective. As soon as $\mathrm{Pic}\, H \neq 0$, we thus get 'transcendental elements' in the Brauer group of X, i.e. elements of the Brauer group of X whose image in $\mathrm{Br}\, \overline{X}$ is nonzero.

Proposition 2.12. *Let G be a semisimple, simply connected algebraic group over k and $H \subset G$ be a closed k-subgroup, not necessarily connected. Let $X = G/H$. Then:*

(i) *the natural map $\nu(G) : \hat{H}(k) \to \mathrm{Pic}\, X$ is an isomorphism;*

(ii) *the map $\theta(G) : H^1(k, \hat{H}) \to \mathrm{Br}_1\, X$ induces an isomorphism $H^1(k, \hat{H}) \simeq \mathrm{Br}_1\, X/\mathrm{Br}\, k$.*

Proof. Using Propositions 2.5 and 2.6 we obtain isomorphisms $\nu(G)(k) : \hat{H}(k) \xrightarrow{\simeq} \mathrm{Pic}\, X$ and $\nu(G) : \hat{H} \xrightarrow{\simeq} \mathrm{Pic}\, \overline{X}$. The first one gives (i), the second one induces an isomorphism $H^1(k, \hat{H}) \xrightarrow{\simeq} H^1(k, \mathrm{Pic}\, \overline{X})$. Proposition 2.6 gives $\overline{k}^* = \overline{k}[X]^*$. By Lemma 2.1 this implies $\mathrm{Br}_1\, X/\mathrm{Br}\, k \xrightarrow{\simeq} H^1(k, \mathrm{Pic}\, \overline{X})$. Combining this with Proposition 2.8 we get (ii). □

3. The Brauer–Manin obstruction for rational and integral points of homogeneous spaces with connected stabilizers

Let k be a number field and H/k be a connected linear algebraic group. Since H is connected, the image of the diagonal map $H^1(k,H) \to \prod_v H^1(k_v,H)$ lies in the subset $\bigoplus_v H^1(k_v,H)$ of elements which are equal to the trivial class $1 \in H^1(k_v,H)$ for all but a finite number of places v of k. For each place v, the pairing

$$H^1(k_v,H) \times \mathrm{Pic}\, H_{k_v} \to \mathrm{Br}\, k_v \subset \mathbb{Q}/\mathbb{Z}$$

from Proposition 2.9 induces a map $H^1(k_v,H) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$.

The following theorem is essentially due to Kottwitz ([Kot86, 2.5, 2.6]; see also [BR95]). It extends the Tate–Nakayama theory (case when H is a torus). With the maps as defined above, a proof of the theorem is given in [Col08, Theorem 9.4] (handling the real places is a delicate point; in [Col08] one refers to an argument of Borovoi).

Theorem 3.1. *Let k be a number field and H a connected linear algebraic group over k. The above maps induce a natural exact sequence of pointed sets*

$$H^1(k,H) \to \bigoplus_v H^1(k_v,H) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z}).$$

Let G be a connected linear algebraic group over k and $H \subset G$ a connected subgroup. Let $X = G/H$. Projection $G \to G/H$ makes G into a right torsor over X under the group H.

We have the following natural commutative diagram.

$$\begin{array}{ccccc}
G(k) & \longrightarrow & G(\mathcal{A}_k) & & \\
\downarrow & & \downarrow & & \\
X(k) & \longrightarrow & X(\mathcal{A}_k) & \longrightarrow & \mathrm{Hom}(\mathrm{Br}\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z}) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(k,H) & \longrightarrow & \bigoplus_v H^1(k_v,H) & \longrightarrow & \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z}) \\
\downarrow & & \downarrow & & \\
H^1(k,G) & \longrightarrow & \bigoplus_v H^1(k_v,G) & &
\end{array} \tag{3.1}$$

In this diagram the two left vertical sequences are exact sequences of pointed sets ([Ser65, Chapter I, § 5.4, Proposition 36]). The map $\mathrm{Hom}(\mathrm{Br}\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$ is induced by the map $\delta_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \to \mathrm{Br}\, X$. The commutativity of this diagram follows from Proposition 2.9.

A finite set S of places of k will be called *big enough for* (G,H) if it contains all the archimedean places, there exists a closed immersion of smooth affine O_S-group schemes with connected fibres $\mathbf{H} \subset \mathbf{G}$ extending the embedding $H \subset G$ and the quotient O_S-scheme $\mathbf{X} = \mathbf{G}/\mathbf{H}$ exists and is separated. There always exists such a finite set S.

Theorem 3.2. *Let k be a number field, $H \subset G$ connected linear algebraic groups over k and $X = G/H$.*

(i) *With notation as above, the kernel of the map*

$$X(\mathcal{A}_k) \to \mathrm{Hom}(\mathrm{Br}\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z})$$

is included in the kernel of the composite map

$$X(\mathcal{A}_k) \to \bigoplus_v H^1(k_v, H) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z}).$$

(ii) *If G is semisimple and simply connected, the kernels of these two maps coincide.*

(iii) *Let the finite set S of places be big enough for (G, H). A point $\{M_v\}_{v\in\Omega_k}$ in the product $\prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)$ is in the kernel of the composite map*

$$X(\mathcal{A}_k) \to \bigoplus_v H^1(k_v, H) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$$

if and only if the point $\{M_v\}_{v\in S}$ is in the kernel of the composite map

$$\prod_{v\in S} X(k_v) \to \prod_{v\in S} H^1(k_v, H) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z}).$$

Proof. Statement (i) follows from diagram (3.1).

If G is semisimple and simply connected, Proposition 2.10 implies that the composite map $\delta'_{\mathrm{tors}}(G) : \mathrm{Pic}\, H \to \mathrm{Br}\, X \to \mathrm{Br}\, X/\mathrm{Br}\, k$ is an isomorphism. This gives (ii).

In the situation of (iii), for each $v \notin S$, the composite map $\mathbf{X}(O_v) \to X(k_v) \to H^1(k_v, H)$ factorizes as $\mathbf{X}(O_v) \to H^1_{\text{ét}}(O_v, \mathbf{H}) \to H^1(k_v, H)$ and $H^1_{\text{ét}}(O_v, \mathbf{H}) = 1$ by Hensel's lemma together with Lang's theorem. □

In the case where the group G is semisimple and simply connected, the hypotheses of the next three theorems are fulfilled. In that case these theorems are due to Borovoi [Bor96] and Borovoi and Rudnick [BR95].

Theorem 3.3 (Compare [BR95, Theorem 3.6]). *Let G be a connected linear algebraic group over a number field k and $H \subset G$ a connected k-subgroup. Let $X = G/H$. Assume $Ш^1(k, G) = 0$. If $\{M_v\}_{v\in\Omega} \in X(\mathcal{A}_k)$ is orthogonal to the image of the (finite) group* Pic H *in* Br X *with respect to the Brauer–Manin pairing, then there exist $\{g_v\} \in G(\mathcal{A}_k)$ and $M \in X(k)$ such that for each place v of k*

$$g_v M = M_v \in X(k_v).$$

Proof. This immediately follows from diagram (3.1). □

Theorem 3.4. *Let G be a connected linear algebraic group over a number field k and $H \subset G$ a connected k-subgroup. Let $X = G/H$. Assume $Ш^1(k, G) = 0$ and assume that G satisfies weak approximation.*

(a) *Let $\{M_v\}_{v\in\Omega} \in X(\mathcal{A}_k)$ be orthogonal to the image of the (finite) group* Pic H *in* Br X *with respect to the Brauer–Manin pairing. Then for each finite set S of places of k and open sets $U_v \subset X(k_v)$ with $M_v \in U_v$ there exists $M \in X(k)$ such that $M \in U_v$ for $v \in S$.*

(b) *(Borovoi) If G is semisimple and simply connected and H is geometrically characterfree, then X satisfies weak approximation.*

Proof. (a) Let $\{g_v\} \in G(\mathcal{A}_k)$ and $M \in X(k)$ be as in the conclusion of the previous theorem. If $g \in G(k)$ is close enough to each g_v for $v \in S$, then $gM \in X(k)$ belongs to each U_v for each $v \in S$.

(b) Since H is geometrically characterfree, Lemma 2.1 and Rosenlicht's lemma ensure that the natural map $\mathrm{Pic}\, H \to \mathrm{Pic}\, \overline{H}$ is injective. This implies that for any field K containing k the natural map of finite abelian groups $\mathrm{Pic}\, H \to \mathrm{Pic}\, H_K$ is injective. Thus the dual map $\mathrm{Hom}(\mathrm{Pic}\, H_K, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$ is onto. For any nonarchimedean place w of k the natural map

$$H^1(k_w, H) \to \mathrm{Hom}(\mathrm{Pic}\, H_{k_w}, \mathbb{Q}/\mathbb{Z})$$

is a bijection (Kottwitz, see [Col08, Theorem 9.1(ii)]). Since G is semisimple and simply connected and w nonarchimedean, $H^1(k_w, G) = 1$ (Kneser), hence the map $X(k_w) \to H^1(k_w, H)$ is onto. Thus the composite map

$$X(k_w) \to H^1(k_w, H) \to \mathrm{Hom}(\mathrm{Pic}\, H_{k_w}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$$

is onto. Let S be a finite set of places of k, let $\{M_v\}_{v\in S} \in \prod_{v\in S} X(k_v)$ and for each place v let $U_v \subset X(k_v)$ be a neighbourhood of M_v. Let $\varphi \in \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$ be the image of $\{M_v\}_{v\in S}$ under the map $\prod_{v\in S} X(k_v) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$. Choose a nonarchimedean place $w \notin S$ and a point $M_w \in X(k_w)$ whose image in the group $\mathrm{Hom}(\mathrm{Pic}\, H_{k_w}, \mathbb{Q}/\mathbb{Z})$ induces $-\varphi \in \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$. At places v not in $S \cup \{w\}$ take $M_v \in X(k_v)$ to be the image of $1 \in G(k_v)$ under the projection map $G(k_v) \to X(k_v)$. Then the family $\{M_v\}_{v\in\Omega_k}$ satisfies the hypothesis in (a), which is enough to conclude. □

THEOREM 3.5. *Let G be a connected linear algebraic group over a number field k and $H \subset G$ a connected k-subgroup. Let $X = G/H$. Let X_c be a smooth compactification of X. The closure of the image of the diagonal map $X_c(k) \to X_c(\mathcal{A}_k)$ is exactly the Brauer–Manin set $X_c(\mathcal{A}_k)^{\mathrm{Br}\, X_c}$ consisting of elements of $X_c(\mathcal{A}_k)$ which are orthogonal to* $\mathrm{Br}\, X_c$.

Proof. After changing both G and H one may assume that the group G is 'quasi-trivial' (see [CK06, Lemme 1.5]). For any such group G, weak approximation holds, and $Ш^1(k, G) = 0$ (see [Col08, Proposition 9.2]). Let $\{M_v\} \in X_c(\mathcal{A}_k)$ be orthogonal to $\mathrm{Br}\, X_c$. Since $\overline{G}$ is a rational variety, the smooth, projective, geometrically integral variety X_c is geometrically unirational. This implies that the quotient $\mathrm{Br}\, X_c/\mathrm{Br}\, k$ is finite. Any element of $X_c(\mathcal{A}_k)^{\mathrm{Br}\, X_c}$ may thus be approximated by an $\{M_v\} \in X(\mathcal{A}_k)$ which is orthogonal to $\mathrm{Br}\, X_c$. Let S be a finite set of places of k. The group $\mathrm{Pic}\, H$ is finite, its image $B \subset \mathrm{Br}\, X$ is thus a finite group and we have $\{M_v\} \in X(\mathcal{A}_k)^{B\cap \mathrm{Br}\, X_c}$. According to a theorem of Harari ([Har94, Corollary 2.6.1], see also [Col03, Theorem 1.4]), there exists a family $\{P_v\} \in X(\mathcal{A}_k)$ with $P_v = M_v$ for $v \in S$ which is orthogonal to $B \subset \mathrm{Br}\, X$. By Theorem 3.4 we may find $M \in X(k)$ as close as we wish to each M_v for $v \in S$. □

Remark 3.6. Some of the results in [Bor96], [Bor99] and the references quoted therein are not covered by the previous two theorems. M. Borovoi tells us that in Theorem 3.5 one may replace $\mathrm{Br}\, X_c$ by $\mathrm{Br}_1\, X_c$.

We now discuss integral points of homogeneous spaces. Let Y be a variety over a number field k. Let S_0 be a finite set of places of k (these may be arbitrary places of k). We let O_{S_0} denote the subring of elements x of k which are v-integral at each nonarchimedean place v not in S_0. One says that Y satisfies strong approximation with respect to S_0 if the diagonal image of $Y(k)$ in the set of S_0-adèles of Y is dense. The S_0-adèles of Y is the subset of $\prod_{v\notin S_0} Y(k_v)$ consisting of elements which are integral at almost all places of k. This set is equipped with a natural restricted topology. The definition does not depend on the choice of an integral model for Y. For a discussion of various properties of strong approximation, see [PR91, § 7.1]. If G/k

is a connected linear algebraic group, G satisfies strong approximation with respect to S_0 if and only if $G(k).(\prod_{v\in S_0} G(k_v))$ is dense in the group of all adèles $G(\mathcal{A}_k)$.

On first reading the statement of the following theorem, the reader is invited to take S to be just the set of archimedean places.

Theorem 3.7. *Let k be a number field, O its ring of integers, S a finite set of places of k containing all archimedean places, and O_S the ring of S-integers. Let G/k be a semisimple, simply connected group. Let $H\subset G$ be a connected subgroup. Let $\mathbf{X}$ be a separated O_S-scheme of finite type such that $X=\mathbf{X}\times_{O_S} k$ is k-isomorphic to G/H.*

(a) *For a point $\{M_v\}\in\prod_{v\in S} X(k_v)\times\prod_{v\notin S}\mathbf{X}(O_v)\subset X(\mathcal{A}_k)$ the following conditions are equivalent:*
   (i) *it is in the kernel of the map $X(\mathcal{A}_k)\to \mathrm{Hom}(\mathrm{Br}\, X,\mathbb{Q}/\mathbb{Z})$;*
   (ii) *it is in the kernel of the composite map*
$$X(\mathcal{A}_k)\to\bigoplus_v H^1(k_v,H)\to \mathrm{Hom}(\mathrm{Pic}\, H,\mathbb{Q}/Z).$$
   Let S_1 with $S\subset S_1$ be big enough for (G,H) and $\mathbf{X}$. More precisely assume that there exists a semisimple O_{S_1}-group scheme $\mathbf{G}$ extending G/k, a smooth, fibrewise connected, O_{S_1}-subgroup scheme $\mathbf{H}\subset\mathbf{G}$ over O_{S_1} extending H and an O_{S_1}-isomorphism $\mathbf{X}\times_{O_S} O_{S_1}\simeq \mathbf{G}/\mathbf{H}$ extending $X\simeq G/H$. Then the above conditions are equivalent to:
   (iii) *the S_1-projection $\{M_v\}_{v\in S_1}$ of $\{M_v\}$ is in the kernel of the composite map*
$$\prod_{v\in S_1} X(k_v)\to\prod_{v\in S_1} H^1(k_v,H)\to \mathrm{Hom}(\mathrm{Pic}\, H,\mathbb{Q}/\mathbb{Z}).$$

(b) *Let S_0 be a finite set of places of k such that for each almost simple k-factor G' of G there exists a place $v\in S_0$ such that $G'(k_v)$ is not compact. Let S_2 be a finite set of places of k. If $\{M_v\}\in\prod_{v\in S} X(k_v)\times\prod_{v\notin S}\mathbf{X}(O_v)\subset X(\mathcal{A}_k)$ satisfies one of the three conditions above, then there exists $M\in\mathbf{X}(O_{S_0\cup S})$ arbitrarily close to each M_v for $v\in S_2\setminus S_0$. In particular, we then have $\mathbf{X}(O_{S\cup S_0})\neq\emptyset$.*

Proof. The assumption on G ensures that $Ш^1(k,G)=0$ and that G satisfies strong approximation with respect to S_0 (Kneser [Kne65]; Platonov and Rapinchuk [PR91, Russian edition, Chapter 7.4, Teor. 12, p. 466; English edition, § 7.4, Theorem 7.12, p. 427]).

Statement (a) then follows from Theorem 3.2.

Let us prove (b). We may assume that S_2 contains S_1. According to Theorem 3.3, whose hypotheses are fulfilled, there exist $N\in X(k)$ and a family $\{g_v\}\in G(\mathcal{A}_k)$ such that $g_v.N=M_v$ for each place v. By strong approximation with respect to S_0, there exist $g\in G(k)$ such that g is very close to g_v for $v\in S_2\setminus S_0$ and $g\in\mathbf{G}(O_v)$ for $v\notin S_2\cup S_0$. Now the point $M=gN\in X(k)$ belongs to $\mathbf{X}(O_v)$ for $v\notin S_2\cup S_0$ and it is very close to $M_v\in\mathbf{X}(k_v)$ for $v\in S_2\setminus S_0$. Hence it also belongs to $\mathbf{X}(O_v)$ for $v\notin S\cup S_0$ (the set $\mathbf{X}(O_v)$ is open in $X(k_v)$). We thus have found $M\in\mathbf{X}(O_{S\cup S_0})$ very close to each M_v for $v\in S_2\setminus S_0$. □

The existence of an $\{M_v\}\in\prod_{v\in S} X(k_v)\times\prod_{v\notin S}\mathbf{X}(O_v)$ satisfying hypothesis (i) or (ii) is reduced to the existence of an $\{M_v\}\in\prod_{v\in S_1}\mathbf{X}(k_v)$ as in hypothesis (iii). This can be checked by a finite amount of computations involving the pairings $H^1(k_v,H)\times\mathrm{Pic}\, H\to\mathbb{Q}/\mathbb{Z}$.

If one uses the Brauer pairing, one can also check hypothesis (i) by means of a finite amount of computations. For any $\alpha \in \mathrm{Br}\, X$ there exists a finite set S_α of places of k such that α vanishes on $\mathbf{X}(O_v)$ for any $v \notin S_\alpha$. Let T be the union of S and the S_α for a finite set E of the α spanning the finite group $\mathrm{Br}\, X/\mathrm{Br}\, k$. To decide if there exists $\{M_v\}$ as in hypothesis (i) one only has to see whether there exists an element $\{M_v\} \in \prod_{v\in S} \mathbf{X}(k_v) \times \prod_{v \in T\setminus S} \mathbf{X}(O_v)$ which is orthogonal to each α in the finite set E, the sum in the Brauer–Manin pairing being taken only over the places in T.

Remark 3.8. In view of Remark 2.11, the Brauer–Manin obstruction involved in this section may involve transcendental elements in the Brauer group of the homogeneous spaces $X = G/H$ under consideration.

4. The Brauer–Manin obstruction for rational and integral points of homogeneous spaces with finite, commutative stabilizers

Let k be a number field and μ/k be a finite commutative k-group scheme. The image of the diagonal map $H^1(k,\mu) \to \prod_v H^1(k_v,\mu)$ lies in the restricted direct product $\prod'_v H^1(k_v,\mu)$. For each place v, we have the cup-product pairing

$$H^1(k_v,\mu) \times H^1(k_v,\hat{\mu}) \to \mathrm{Br}\, k_v \subset \mathbb{Q}/\mathbb{Z}.$$

Theorem 4.1 (Poitou, Tate). *The above pairings induce a natural exact sequence of commutative groups*

$$H^1(k,\mu) \to {\prod_v}' H^1(k_v,\mu) \to \mathrm{Hom}(H^1(k,\hat{\mu}),\mathbb{Q}/\mathbb{Z}). \tag{4.1}$$

Let S be a finite set of places of k containing all the archimedean places, such that the finite étale k-group scheme μ extends to a finite étale group scheme over O_S of order invertible in O_S, so that $\hat{\mu}$ also extends to a finite étale group scheme over O_S. Then there is an exact sequence of finite abelian groups

$$H^1_{\text{ét}}(O_S,\mu) \to \prod_{v\in S} H^1(k_v,\mu) \to \mathrm{Hom}(H^1_{\text{ét}}(O_S,\hat{\mu}),\mathbb{Q}/\mathbb{Z}). \tag{4.2}$$

See Milne's book [Mil86], Chapter I, § 4, Theorem 4.10 p. 70 (for both sequences) and Chapter II, § 4, Proposition 4.13(c) p. 239 (for the second sequence).

Let G be a connected linear algebraic group over k and $\mu \subset G$ a finite commutative k-subgroup, not necessarily normal in G. Let $X = G/\mu$.

We have the following natural commutative diagram.

$$\begin{array}{ccccc}
G(k) & \longrightarrow & G(\mathcal{A}_k) & & \\
\downarrow & & \downarrow & & \\
X(k) & \longrightarrow & X(\mathcal{A}_k) & \longrightarrow & \mathrm{Hom}(\mathrm{Br}_1\, X/\mathrm{Br}\, k,\mathbb{Q}/\mathbb{Z}) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(k,\mu) & \longrightarrow & \prod'_v H^1(k_v,\mu) & \longrightarrow & \mathrm{Hom}(H^1(k,\hat{\mu}),\mathbb{Q}/\mathbb{Z}) \\
\downarrow & & \downarrow & & \\
H^1(k,G) & \longrightarrow & \prod'_v H^1(k_v,G) & &
\end{array} \tag{4.3}$$

In this diagram the two left vertical sequences are exact sequences of pointed sets [Ser65, Chapter I, § 5.4, Proposition 36]. The map

$$\mathrm{Hom}(\mathrm{Br}_1\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(H^1(k, \hat{\mu}), \mathbb{Q}/\mathbb{Z})$$

is induced by the map $\theta(G) : H^1(k, \hat{\mu}) \to \mathrm{Br}_1\, X \subset \mathrm{Br}\, X$ associated to the μ-torsor $G \to G/\mu = X$, as defined in Proposition 2.7 and the comments following that proposition. The commutativity of the right hand side square follows from Proposition 2.7.

Let S be a finite set of places of k which contains all the archimedean places, and is large enough so that all the following properties hold: there exists a smooth, linear O_S-group $\mathbf{G}$ with connected fibres, the group μ comes from a finite, étale O_S-group scheme $\mu \subset \mathbf{G}$, the group $\hat{\mu}$ comes from a finite, étale O_S-group scheme $\hat{\mu}$, the k-variety X comes from a smooth O_S-scheme $\mathbf{X}$ and there is a finite étale map $\mathbf{G} \to \mathbf{X}$ extending $G \to X = G/\mu$ and making $\mathbf{G}$ into a μ-torsor over $\mathbf{X}$. In the rest of this section, we shall simply say that such an S is 'big enough for (G, μ)'.

One then has the following commutative diagram.

$$\begin{array}{ccccc}
\mathbf{G}(O_S) & \longrightarrow & \prod_{v\in S} G(k_v) & & \\
\downarrow & & \downarrow & & \\
\mathbf{X}(O_S) & \longrightarrow & \prod_{v\in S} X(k_v) & \longrightarrow & \mathrm{Hom}(\mathrm{Br}_1\, X, \mathbb{Q}/\mathbb{Z}) \\
\downarrow & & \downarrow & & \downarrow \\
H^1_{\text{ét}}(O_S, \mu) & \longrightarrow & \prod_{v\in S} H^1(k_v, \mu) & \longrightarrow & \mathrm{Hom}(H^1_{\text{ét}}(O_S, \hat{\mu}), \mathbb{Q}/\mathbb{Z}) \\
\downarrow & & \downarrow & & \\
H^1_{\text{ét}}(O_S, \mathbf{G}) & \longrightarrow & \prod_{v\in S} H^1(k_v, G) & &
\end{array} \tag{4.4}$$

The map $\mathrm{Hom}(\mathrm{Br}_1\, X, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(H^1_{\text{ét}}(O_S, \hat{\mu}), \mathbb{Q}/\mathbb{Z})$ is induced by the composite map $H^1_{\text{ét}}(O_S, \hat{\mu}) \to H^1(k, \hat{\mu}) \to \mathrm{Br}_1\, X$. By Theorem 4.1, the sequence on the third line, which is a sequence of finite abelian groups, is exact. The middle and left vertical maps are exact sequences of pointed sets.

Theorem 4.2.

(i) *With notation as above, the kernel of the map*

$$X(\mathcal{A}_k) \to \mathrm{Hom}(\mathrm{Br}_1\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z})$$

is included in the kernel of the composite map

$$X(\mathcal{A}_k) \to {\prod_v}' H^1(k_v, \mu) \to \mathrm{Hom}(H^1(k, \hat{\mu}), \mathbb{Q}/\mathbb{Z}).$$

(ii) *If G is simply connected, the kernels of these two maps coincide.*

(iii) *Let the finite set S of places be big enough for (G, μ). If the point $\{M_v\} \in \prod_{v\in S} X(k_v) \times \prod_{v\notin S} \mathbf{X}(O_v)$ is in the kernel of the composite map*

$$X(\mathcal{A}_k) \to {\prod_v}' H^1(k_v, \mu) \to \mathrm{Hom}(H^1(k, \hat{\mu}), \mathbb{Q}/\mathbb{Z})$$

then its projection $\{M_v\}_{v\in S}$ is in the kernel of the composite map

$$\prod_{v\in S} X(k_v) \to \prod_{v\in S} H^1(k_v, \mu) \to \mathrm{Hom}(H^1_{\text{ét}}(O_S, \hat{\mu}), \mathbb{Q}/\mathbb{Z}).$$

Proof. Statement (i) follows from diagram (4.3). If G is simply connected, then by Proposition 2.12 the composite map $H^1(k,\hat{\mu}) \to \mathrm{Br}_1\, X \to \mathrm{Br}_1\, X/\mathrm{Br}\, k$ is an isomorphism. This proves (ii). For $v \notin S$, the image of the composite map

$$\mathbf{X}(O_v) \to X(k_v) \to H^1(k_v, \mu)$$

lies in $H^1_{\text{ét}}(O_v, \mu)$. Since the cup-product $H^1_{\text{ét}}(O_v, \mu) \times H^1_{\text{ét}}(O_v, \hat{\mu}) \to \mathrm{Br}\, k_v$ vanishes, this proves (iii). □

Proceeding as in the previous section we get the first statement in each of the following results. Here the (generally infinite) group $H^1(k,\hat{\mu})$ plays the rôle of the (finite) group $\mathrm{Pic}\, H$. The second statement in each of the following results has the advantage of involving only finitely many computations.

Theorem 4.3. *Let G/k be a connected linear algebraic group over a number field k. Let $\mu \subset G$ be a finite, commutative k-subgroup. Assume $Ш^1(k, G) = 0$.*

(a) *If $\{M_v\} \in X(\mathcal{A}_k)$ is orthogonal to the image of the group $H^1(k,\hat{\mu})$ in $\mathrm{Br}\, X$ with respect to the Brauer–Manin pairing, then there exist $\{g_v\} \in G(\mathcal{A}_k)$ and $M \in X(k)$ such that for each place v of k*

$$g_v M = M_v \in X(k_v).$$

(b) *Let S be big enough for (G, μ). If $\{M_v\} \in \prod_{v\in S} X(k_v)$ is orthogonal to the image of the composite map $H^1_{\text{ét}}(O_S, \hat{\mu}) \to H^1(k, \hat{\mu}) \to \mathrm{Br}\, X$ with respect to the Brauer–Manin pairing (where the pairing is restricted to the places in S), then there exist $\{g_v\} \in \prod_{v\in S} G(k_v)$ and $M \in X(k)$ such that for each place $v \in S$*

$$g_v M = M_v \in X(k_v).$$

Proof. (a) This is the same as the proof of Theorem 3.3, using diagram (4.3).

(b) Chasing through the diagram (4.4) one first produces a class ξ in $H^1_{\text{ét}}(O_S, \mu)$ whose image in $H^1_{\text{ét}}(O_S, \mathbf{G})$ has trivial image in each $H^1(k_v, G)$ for $v \in S$. For $v \notin S$, the image of an element of $H^1_{\text{ét}}(O_S, \mathbf{G})$ in $H^1(k_v, G)$ is trivial by Lang's theorem and Hensel's lemma. Thus the image of ξ in $H^1(k, G)$ has trivial image in each $H^1(k_v, G)$, hence is trivial in $H^1(k, G)$. This implies that the image of ξ in $H^1(k, \mu)$ lies in the image of $X(k)$ and one concludes the argument just as before. □

Theorem 4.4. *Let G/k be a connected linear algebraic group over a number field k. Let $\mu \subset G$ be a finite, commutative k-subgroup. Assume $Ш^1(k, G) = 0$ and assume that G satisfies weak approximation.*

(a) *Let $\{M_v\} \in X(\mathcal{A}_k)$ be orthogonal to the image of the group $H^1(k,\hat{\mu})$ in $\mathrm{Br}\, X$ with respect to the Brauer–Manin pairing. Then for each finite set S of places of k and open sets $U_v \subset X(k_v)$ with $M_v \in U_v$ there exists $M \in X(k)$ such that $M \in U_v$ for $v \in S$.*

(b) *Let S be big enough for (G, μ). If $\{M_v\} \in \prod_{v\in S} X(k_v)$ is orthogonal to the image of the composite map $H^1_{\text{ét}}(O_S, \hat{\mu}) \to H^1(k, \hat{\mu}) \to \mathrm{Br}\, X$ with respect to the Brauer–Manin pairing (where the pairing is restricted to the places in S), then for each family of open sets $U_v \subset X(k_v)$ with $M_v \in U_v$ for $v \in S$ there exists $M \in X(k)$ such that $M \in U_v$ for $v \in S$.*

Proof. This immediately follows from the previous theorem. □

On first reading the statement of the following theorem, the reader is invited to take S to be just the set of archimedean places.

THEOREM 4.5. *Let k be a number field, O its ring of integers, S a finite set of places of k containing all archimedean places, and O_S the ring of S-integers. Let G/k be a semisimple, simply connected group. Let $\mu \subset G$ be a finite, commutative k-subgroup. Let $\mathbf{X}$ be a separated O_S-scheme of finite type such that $X = \mathbf{X} \times_{O_S} k$ is k-isomorphic to G/μ.*

(a) *For a point $\{M_v\} \in \prod_{v \in S} X(k_v) \times \prod_{v \notin S} \mathbf{X}(O_v) \subset X(\mathcal{A}_k)$, the following conditions are equivalent:*
   (i) *it is in the kernel of the map $X(\mathcal{A}_k) \to \mathrm{Hom}(\mathrm{Br}_1 X, \mathbb{Q}/\mathbb{Z})$;*
   (ii) *it is in the kernel of the composite map*
$$X(\mathcal{A}_k) \to \prod{}' H^1(k_v, \mu) \to \mathrm{Hom}(H^1(k, \hat{\mu}), \mathbb{Q}/Z).$$
   Let S_1 with $S \subset S_1$ be big enough for (G, μ) and $\mathbf{X}$. More precisely assume that S_1 contains S and there exists a semisimple O_{S_1}-group scheme $\mathbf{G}$ extending G/k, a finite, commutative étale subgroup scheme $\mu \subset \mathbf{G}$ over O_{S_1} extending μ and an isomorphism of O_{S_1}-schemes $\mathbf{X} \times_{O_S} O_{S_1} \simeq \mathbf{G}/\mu$ extending $X \simeq G/\mu$. Then the above conditions imply:
   (iii) *the point $\{M_v\}_{v \in S_1}$ is in the kernel of the composite map*
$$\prod_{v \in S_1} X(k_v) \to \prod_{v \in S_1} H^1(k_v, \mu) \to \mathrm{Hom}(H^1_{\text{ét}}(O_{S_1}, \hat{\mu}), \mathbb{Q}/\mathbb{Z}).$$

(b) *Let S_0 be a finite set of places of k such that for each almost simple k-factor G' of G there exists a place $v \in S_0$ such that $G'(k_v)$ is not compact. Let S_2 be a finite set of places of k. If $\{M_v\} \in \prod_{v \in S} X(k_v) \times \prod_{v \notin S} \mathbf{X}(O_v)$ satisfies condition (i) or (ii) above, then there exists $M \in \mathbf{X}(O_{S_0 \cup S})$ arbitrarily close to each M_v for $v \in S_2 \setminus S_0$. In particular $\mathbf{X}(O_{S \cup S_0}) \neq \emptyset$.*

(c) *If the finite set S_1 of places is as above and contains S_0 and if $\{M_v\}$ in the product $\prod_{v \in S} X(k_v) \times \prod_{v \notin S} \mathbf{X}(O_v)$ satisfies condition (iii) above, then there exists $M \in \mathbf{X}(O_{S \cup S_0})$ arbitrarily close to each M_v for $v \in S_1 \setminus S_0$. In particular $\mathbf{X}(O_{S \cup S_0}) \neq \emptyset$.*

Proof. (a) This is just a special case of Theorem 4.2.

(b) We may assume that S_2 contains S_1. By Theorem 4.3 there exist $N \in X(k)$ and a family $\{g_v\} \in G(\mathcal{A}_k)$ such that for each place v of k we have $g_v N = M_v \in X(k_v)$. By the strong approximation theorem for G with respect to S_0, there exists $g \in \mathbf{G}(O_{S_2 \cup S_0})$ such that g is very close to $g_v \in G(k_v)$ for $v \in S_2 \setminus S_0$. We may thus arrange that the point $M = gN$ is very close to M_v for $v \in S_2 \setminus S_0$, and in particular lies in $\mathbf{X}(O_v)$ for each $v \in S_2 \setminus (S \cup S_0)$. It also lies in $\mathbf{X}(O_v)$ for $v \notin S_2 \cup S_0$. Hence it lies in $\mathbf{X}(O_{S \cup S_0})$.

(c) The proof here is more delicate than the proof of the statement (b) in Theorem 3.7. Let $\{M_v\} \in \prod_{v \in S_1} X(k_v)$ satisfy condition (iii). By a theorem of Nisnevich [Nis84], the kernel of the map
$$H^1_{\text{ét}}(O_{S_1}, \mathbf{G}) \to H^1(k, G)$$
is $H^1_{\text{Zar}}(O_{S_1}, \mathbf{G})$. Under our assumptions on G, we have $\text{Ш}^1(k, G) = 0$ and the group G satisfies strong approximation with respect to S_1: the set $G(k).(\prod_{v \in S_1} G(k_v))$ is dense in $G(\mathcal{A}_k)$. By a theorem of Harder [Har67, Korollar 2.3.2, p. 179] this implies $H^1_{\text{Zar}}(O_{S_1}, \mathbf{G}) = 0$.

For $v \notin S_1$, we have $H^1_{\text{ét}}(O_v, \mathbf{G}) = 0$ (Hensel's lemma and Lang's theorem). Thus the kernel of the map $H^1_{\text{ét}}(O_{S_1}, \mathbf{G}) \to \prod_{v \in S_1} H^1(k_v, G)$ is the same as the kernel of the map $H^1_{\text{ét}}(O_{S_1}, \mathbf{G}) \to \prod_v H^1(k_v, G)$ and under our assumptions, by the above argument, that kernel is trivial (note in passing that the only places where $H^1(k_v, G)$ may not be trivial are the real places of k). Chasing through diagram (4.4) with S replaced by S_1 one finds that there exist a point $N \in \mathbf{X}(O_{S_1})$ and a family $\{g_v\}$ in $\prod_{v \in S_1} G(k_v)$ such that $g_v.N = M_v$ for each $v \in S_1$. By strong approximation with respect to S_0 there exists $g \in \mathbf{G}(O_{S_1}) \subset G(k)$ such that g is very close to $g_v \in G(k_v)$ for $v \in S_1 \setminus S_0$ and $g \in \mathbf{G}(O_v)$ for $v \notin S_1$. Now the point $M = gN \in X(k)$ belongs to $\mathbf{X}(O_v)$ for $v \notin S_1$ and it is very close to $M_v \in \mathbf{X}(k_v)$ for $v \in S_1 \setminus S_0$, hence lies in $\mathbf{X}(O_v)$ for $v \notin S \cup S_0$. □

Remark 4.6. Under the assumption on G made in (c), the proof of the above theorem shows, in a very indirect fashion, that the existence of a point $\{M_v\}_{v \in \Omega_k}$ as in (i) or (ii) is equivalent to the existence of a point $\{M_v\}_{v \in S_1}$ as in (iii).

The group $H^1(k, \hat{\mu})$ is in general infinite, hence the conditions appearing in (i) and (ii) do not lead to a finite decision process for the existence of S-integral points. However for any finite set $S \subset \Omega_k$ such that μ and its dual are finite étale over O_S, the group $H^1_{\text{ét}}(O_S, \hat{\mu})$ is a finite group: this is a consequence of Dirichlet's theorem on units and of the finiteness of the class number of number fields. Thus for $S = S_1$ as in (c), only finitely many computations are required to decide whether there exists a family $\{M_v\}_{v \in S_1}$ as in (iii), hence ultimately to decide if there exists an S-integral point on $\mathbf{X}$, which additionally may be chosen arbitrarily close to each $M_v \in X(k_v)$ for $v \in S \setminus S_0$.

5. Representation of a quadratic form by a quadratic form over a field

5.1 Let k be a field of characteristic different from 2. Let $n \leq m$ be natural integers. A classical problem asks for the representation of a nondegenerate quadratic form g over k, of rank $n \geq 1$, by a nondegenerate quadratic form f of rank $m \geq 2$, over k, i.e. one looks for linear forms $l_1, \dots, l_m$ with coefficients in k in the variables $x_1, \dots, x_n$, such that

$$g(x_1, \dots, x_n) = f(l_1(x_1, \dots, x_n), \dots, l_m(x_1, \dots, x_n)).$$

This equation in the coefficients of the forms l_i defines an affine k-variety X.

In an equivalent fashion, X is the variety of linear maps of $W = k^n$ into $V = k^m$ such that the quadratic form f on V induces the quadratic form g on W. The linear map is then necessarily an embedding.

Let $B_f(v_1, v_2)$ be the symmetric bilinear form on V such that $B_f(v, v) = f(v)$ for $v \in V$. Thus $B_f(v_1, v_2) = \frac{1}{2}(f(v_1 + v_2) - f(v_1) - f(v_2))$. In concrete terms, a k-point of X is given by a set of n vectors $v_1, \dots, v_n \in V = k^m$, such that the bilinear form B_f satisfies: the matrix

$$B_f(v_i, v_j)_{i=1,\dots,n; j=1,\dots,n}$$

is the matrix of the bilinear form on $W = k^n$ attached to g.

The k-variety X has a k-point if and only if there exists a nondegenerate quadratic form h over k in $m - n$ variables and an isomorphism of quadratic forms $f \simeq g \perp h$ over k. The quadratic form h is then well defined up to (nonunique) isomorphism (Witt's cancellation theorem).

By another of Witt's theorems [O'Me71, Theorem 42:17, p. 98], over any field K containing k the set $X(K)$ is empty or a homogeneous space of $O(f)(K)$, and the stabilizer of a point of $X(K)$ is isomorphic to the group $O(h_K)(K)$, where h_K is a nondegenerate quadratic form over K such that $f_K \simeq g_K \perp h_K$. Thus the k-variety X is a homogeneous space of the k-group $O(f)$. If $X(k) \neq \emptyset$, the stabilizer of a k-point of X, up to nonunique isomorphism, does not depend on the k-point, it is k-isomorphic to the k-group $O(h)$ for a quadratic form h over k as above.

For $n < m$, the group $SO(f)(k)$ acts transitively on $X(k)$. If $X(k) \neq \emptyset$, the stabilizer of a k-point of X, up to nonunique isomorphism, does not depend on the k-point, it is k-isomorphic to the k-group $SO(h)$ for a quadratic form h as above. For $n = m - 1$, the k-variety X is a principal homogeneous space of $SO(f)$.

For $n = m$, the k-variety X is a principal homogeneous space of $O(f)$. If it has a k-point, it breaks up into two connected components X' and X'', each of which is a principal homogeneous space of $SO(f)$.

Let us fix a k-point of X, i.e. an embedding $\lambda : (W, g) \hookrightarrow (V, f)$ of quadratic spaces as above. If $n = m$, the k-point determines a connected component of X, say X'. Such a k-point $M \in X(k)$ defines a k-morphism $SO(f) \to X$ which sends $\sigma \in SO(f)$ to $\sigma \circ \lambda$. For $n = m$ this factorizes through a k-morphism $SO(f) \to X'$. By Witt's results, for $n < m$ over any field K containing k, the induced map $SO(f)(K) \to X(K)$ is onto. For $n = m - 1$ it is a bijection. For $n = m$ the map $SO(f)(K) \to X'(K)$ is a bijection.

In this paper we restrict attention to $m \geq 3$, which we henceforth assume. We then have the exact sequence

$$1 \to \mu_2 \to Spin(f) \to SO(f) \to 1. \tag{5.1}$$

Let $G = Spin(f)$. Assume $char(k) = 0$. Proposition 2.6 gives $k^* = k[G]^*$, $\mathrm{Pic}\, G = 0$ and $\mathrm{Br}\, k = \mathrm{Br}\, G$.

We thus have $k^* = k[SO(f)]^*$ and $\overline{k}^* = \overline{k}[SO(f)]^*$. Proposition 2.5 gives natural isomorphisms

$$\nu(Spin(f))(h) : \mathbb{Z}/2 \xrightarrow{\simeq} \mathrm{Pic}\, SO(f), \quad \nu(Spin(f)) : \mathbb{Z}/2 \xrightarrow{\simeq} \mathrm{Pic}\, SO(f) \times_k \overline{k}.$$

This induces an isomorphism $k^*/k^{*2} = H^1(k, \mathbb{Z}/2) \xrightarrow{\simeq} H^1(k, \mathrm{Pic}\, SO(f) \times_k \overline{k})$, which combined with the inverse of the isomorphism $\mathrm{Br}_1\, X/\mathrm{Br}\, k \xrightarrow{\simeq} H^1(k, \mathrm{Pic}\, SO(f) \times_k \overline{k})$ yields an isomorphism

$$k^*/k^{*2} \simeq \mathrm{Br}_1\, X/\mathrm{Br}\, k.$$

This isomorphism is the one provided by Proposition 2.12.

Given a k-isogeny $1 \to \mu \to G \to G' \to 1$ with G semisimple simply connected, Proposition 2.6 and the Hochschild–Serre spectral sequence

$$E_2^{pq} = H^p(\hat{\mu}(\overline{k}), H^q(\overline{G}, \mathbb{G}_m)) \Longrightarrow H^n(\overline{G}', \mathbb{G}_m)$$

yield an isomorphism $H^2(\hat{\mu}(\overline{k}), \overline{k}^*) \simeq \mathrm{Br}\, \overline{G}'$. If the group $\hat{\mu}(\overline{k})$ is cyclic, as is the case here, this implies $\mathrm{Br}\, \overline{G}' = 0$. Thus

$$\mathrm{Br}_1\, SO(f) = \mathrm{Br}\, SO(f).$$

5.2 Applying Galois cohomology to sequence (5.1) and using Kummer's isomorphism we get a homomorphism of groups, the spinor norm map

$$\theta : SO(f)(k) \to k^*/k^{*2}.$$

There are various ways to compute this map. One is well known: any element $\sigma \in SO(V)(k)$ is a product of reflections with respect to an even number of anisotropic vectors $v_1, \dots, v_n$. The product $\prod_i f(v_i) \in k$ is nonzero; its class in k^*/k^{*2} is equal to $\theta(\sigma)$.

The following result, due to Zassenhaus, is quoted in [O'Me71, p. 137]. We thank P. Gille for help with the proof.

Proposition 5.1. *For an element $\tau \in SO(V)(k) \subset GL(V)(k)$ such that $\det(1 + \tau) \neq 0$, we have $\theta(\tau) = \det((1 + \tau)/2) \in k^*/k^{*2}$.*

Proof. Let $\sigma : End(V) \to End(V)$ denote the adjoint involution attached to the quadratic form f (if one fixes a basis $V = k^m$ and A is the matrix of f in this basis, then for $M \in M_m(k)$ we have $\sigma(M) = A^{-1}.{}^{\mathrm{t}}M.A$).

We have the following inclusions of k-varieties:

$$U \subset SO(f) \subset O(f) \subset GL(V) \subset End(V),$$

where $O(f) = \{a \in End(V), \sigma(a).a = 1\}$, and $U = \{a \in O(f), (1 + a) \in GL(V)\}$. The open set $U \subset O(f)$ is contained in the irreducible open set $SO(f) \subset O(f)$.

We also have the following inclusions of k-varieties:

$$W \subset Alt(f) \subset End(V),$$

where $Alt(f) = \{b \in End(V), \sigma(b) + b = 0\}$ and

$$W = \{b \in End(V), \sigma(b) + b = 0, 1 + b \in GL(V)\}.$$

The k-variety $Alt(f)$, which is the Lie algebra of $SO(f)$, is an affine space $\mathbb{A}^{m(m-1)/2}$. One checks that the polynomial function $\det(1 + b)$ on $End(V)$ induces a nonzero (geometrically) irreducible function h_W on $Alt(f) \simeq \mathbb{A}^{m(m-1)/2}$. Thus the open set $W \subset Alt(f)$ satisfies $\mathrm{Pic}(W) = 0$ and $k[W]^* = k^*.h_W^{\mathbb{Z}}$.

The maps $b \mapsto (1 - b)(1 + b)^{-1}$, respectively $a \mapsto (1 + a)^{-1}(1 - a)$, define k-morphisms $W \to U$, respectively $U \to W$, which are the inverse of each other (this is the well-known Cayley parametrization of the orthogonal group). On $U \subset SO(f)$, the invertible function h_U which is the inverse image of h_W sends $\tau \in U \subset SO(f)$ to $\det(2(1 + \tau)^{-1})$. We have $\mathrm{Pic}(U) = 0$ and $k[U]^* = k^*.h_U^{\mathbb{Z}}$. From the Kummer sequence in étale cohomology we have $k[U]^*/k[U]^{*2} \simeq H^1_{\text{ét}}(U, \mu_2)$. Thus any étale μ_2-cover of U is given by an equation $c.h_U^r = z^2$, with $c \in k^*$ and $r = 0$ or 1. If the total space of the cover is geometrically irreducible, then $r = 1$. The restriction of the étale μ_2-cover $Spin(f) \to SO(f)$ on U is thus given by an equation $c.h_U = z^2$. The point $\tau = 1$ belongs to U and $h_U(1) = 1$. There exists a k-point in $Spin(f)$ above $\tau = 1 \in SO(f)$. Thus the restriction of $c.h_U = z^2$ on $\tau = 1$, which is simply $c = z^2$, has a k-point. Hence c is a square in k.

The spinor map $\theta : SO(f)(k) \to k^*/k^{*2}$ thus restricts to the map $U(k) \to k^*/k^{*2}$ induced by $\tau \mapsto \det(2(1 + \tau)^{-1})$. □

5.3 If $m - n \geq 3$, the geometric stabilizers of the $Spin(f)$ action on X are of the shape $Spin(h)$ for h a quadratic form over $\overline{k}$ of rank $m - n \geq 3$. Assume $X(k) \neq \emptyset$. The stabilizer $H \subset G = Spin(f)$ of this k-point is then isomorphic to a k-group $H = Spin(h)$ for h a quadratic form over k of rank $m - n \geq 3$. Assume $char(k) = 0$. Then $\hat{H} = 0$, $\mathrm{Pic}\, H = 0$ and $\mathrm{Br}\, k = \mathrm{Br}\, H$ (Proposition 2.6). From Proposition 2.2 we conclude that

$$k^* = k[X]^*, \quad \mathrm{Pic}\, X = 0, \quad \mathrm{Br}\, k = \mathrm{Br}\, X.$$

5.4 If $m - n = 1$, the stabilizers of the $SO(f)$-action on X are trivial, X is a principal homogeneous space of $SO(f)$, and the geometric stabilizers of the $Spin(f)$ action on X are of the shape μ_2. Assume X has a k-point, and fix such a k-point. This determines an isomorphism of k-varieties $\phi : SO(f) \xrightarrow{\simeq} X$ sending 1 to the given k-point. The composite map $Spin(f) \to SO(f) \to X$ makes $Spin(f)$ into a μ_2-torsor over X. As explained in § 5.1 we then get

$$k^* = k[X]^*, \quad \mathbb{Z}/2 = \mathrm{Pic}\, X$$

and

$$k^*/k^{*2} = H^1(k, \mathbb{Z}/2) \simeq \mathrm{Br}_1\, X/\mathrm{Br}\, k = \mathrm{Br}\, X/\mathrm{Br}\, k.$$

Let $\xi \in H^1_{\text{ét}}(X, \mu_2)$ be the class of the μ_2-torsor $\mathit{Spin}(f) \to X$. There is an associated map $\psi : X(k) \to H^1(k, \mu_2) = k^*/k^{*2}$. The composite map $SO(f)(k) \to X(k) \to k^*/k^{*2}$ is the spinor map $\theta : SO(f)(k) \to k^*/k^{*2}$.

For any $\alpha \in k^*/k^{*2} = H^1(k, \mathbb{Z}/2)$ we have the cup-product $\xi \cup \alpha \in H^2_{\text{ét}}(X, \mu_2)$ and we may consider the image $A_\alpha \in {}_2\mathrm{Br}\, X$ of this element in the 2-torsion subgroup of $\mathrm{Br}\, X$ under the natural map induced by $\mu_2 \to \mathbb{G}_m$. Using Propositions 2.7 and 2.8, one sees that the map $\alpha \mapsto A_\alpha$ induces the isomorphism $k^*/k^{*2} \simeq \mathrm{Br}\, X/\mathrm{Br}\, k$ described above, and that for any k-point $N \in SO(f)(k) = X(k)$, and any $\alpha \in k^*/k^{*2}$, the evaluation of A_α at $\phi(N) \in X(k)$ is the class of the quaternion algebra $(\psi(\phi(N)), \alpha) = (\theta(N), \alpha) \in \mathrm{Br}\, k$.

5.5 If $m = n$ and $X(k) \neq \emptyset$, then § 5.4 applies to each of the two connected components X' and X'' of X.

5.6 If $m - n = 2$, the geometric stabilizers, be they for the $SO(f)$-action or the $\mathit{Spin}(f)$-action on X, are one-dimensional tori. Assume X has a k-point M. This fixes a morphism $\phi : SO(f) \to X$. This also corresponds to a decomposition $f \simeq g \perp h$ for some two-dimensional quadratic form h over k. The stabilizer of the k-point M for the $SO(f)$-action is the k-torus $T_1 = R^1_{K/k}\mathbb{G}_m$, where $K = k[t]/(t^2 - d)$ and $\mathrm{disc}(f) = -\mathrm{disc}(g).d$. If d is a square in k then $T_1 \simeq \mathbb{G}_{m,k}$. The stabilizer of the k-point M for the $\mathit{Spin}(f)$-action is a k-torus T which fits into an exact sequence

$$1 \to \mu_2 \to T \to T_1 \to 1.$$

This implies that the k-torus T_1 is k-isomorphic to the k-torus T. For clarity, we keep the index 1 for the torus T_1. Thus from the k-point $M \in X(k)$ one builds a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & T & \longrightarrow & T_1 & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathit{Spin}(f) & \longrightarrow & SO(f) & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & X & = & X & &
\end{array}$$

where the bottom vertical maps define torsors and the horizontal sequences are exact sequences of algebraic groups over k.

By Proposition 2.6, we have $k^* = k[\mathit{Spin}(f)]^*$, $\mathrm{Pic}\, \mathit{Spin}(f) = 0$, $\mathrm{Br}\, k = \mathrm{Br}\, \mathit{Spin}(f)$ and the analogous statements over $\overline{k}$.

This immediately implies $k^* = k[X]^*$ and $\overline{k}^* = \overline{k}[X]^*$.

Applying Propositions 2.2 or 2.5 to the T-torsor $\mathit{Spin}(f) \to X$, we get isomorphisms

$$\nu(\mathit{Spin}(f))(k) : \hat{T}(k) \xrightarrow{\simeq} \mathrm{Pic}\, X, \quad \nu(\mathit{Spin}(f)) : \hat{T} \xrightarrow{\simeq} \mathrm{Pic}\, \overline{X}.$$

The latter map induces an isomorphism $H^1(k, \hat{T}) \xrightarrow{\simeq} H^1(k, \mathrm{Pic}\, \overline{X})$. If we compose this isomorphism with the inverse of the isomorphism $\mathrm{Br}_1\, X/\mathrm{Br}\, k \xrightarrow{\simeq} H^1(k, \mathrm{Pic}\, \overline{X})$ coming from Lemma 2.1, we get an isomorphism $H^1(k, \hat{T}) \xrightarrow{\simeq} \mathrm{Br}_1\, X/\mathrm{Br}\, k$ which is the one in Proposition 2.12, i.e. is induced by $\theta(\mathit{Spin}(f)) : H^1(k, \hat{T}) \to \mathrm{Br}_1\, X$.

Since T is a torus, it is a connected group and $\mathrm{Pic}\,\overline{T}=0$. Proposition 2.9 shows that the map $\theta(Spin(f)):H^1(k,\hat{T})\to \mathrm{Br}_1\,X$ factorizes as

$$H^1(k,\hat{T})\xrightarrow{\simeq}\mathrm{Pic}\,T\to \mathrm{Br}_1\,X.$$

If d is a square, we get

$$\mathbb{Z}\simeq \mathrm{Pic}\,X,\quad \mathrm{Br}\,X/\mathrm{Br}\,k=0.$$

If d is not a square in k, then

$$\mathrm{Pic}\,X=0,\quad \mathbb{Z}/2\simeq \mathrm{Br}_1\,X/\mathrm{Br}\,k\simeq \mathrm{Br}\,X/\mathrm{Br}\,k.$$

Indeed, in the first case, $\hat{T}=\mathbb{Z}$ with the trivial Galois action, thus $\mathrm{Pic}\,T\simeq H^1(k,\hat{T})=0$. In the second case, $\hat{T}=\mathbb{Z}[G]/\mathbb{Z}(1+\sigma)$ where $G=\mathrm{Gal}(K/k)=\{1,\sigma\}=\mathbb{Z}/2$, hence $\mathrm{Pic}\,T\simeq H^1(k,\hat{T})=H^1(G,\hat{T})=\mathbb{Z}/2$.

Taking Galois cohomology one gets the commutative diagram

$$\begin{array}{ccc}
\theta: SO(f)(k) & \longrightarrow & k^*/k^{*2}\\
\downarrow{\scriptstyle \phi_k} & & \downarrow\\
\psi: X(k) & \longrightarrow & H^1(k,T)=k^*/N_{K/k}K^*\\
\downarrow & & \downarrow\\
\mathrm{Hom}(\mathrm{Br}\,X,\mathrm{Br}\,k) & \longrightarrow & \mathrm{Hom}(H^1(k,\hat{T}),\mathrm{Br}\,k)
\end{array}$$

where the bottom right hand side vertical map is given by cup-product and the bottom horizontal map is induced by

$$\theta(Spin(f)):H^1(k,\hat{T})\xrightarrow{\simeq}\mathrm{Pic}\,T\to \mathrm{Br}_1\,X\subset \mathrm{Br}\,X.$$

Let us check that this diagram is commutative. Given a point in $a\in SO(f)(k)$, one lifts it to $b\in Spin(f)(k_s)$, where k_s is a separable closure of k. The 1-cocycle $\sigma\mapsto {}^{\sigma}b.b^{-1}\in\mu_2$ defines a class in $H^1(k,\mu_2)=k^*/k^{*2}$ which is exactly $\theta(a)$, i.e. the image of the spinor map. On the other hand the image $c\in X(k_s)$ of b under the map $Spin(f)(k_s)\to X(k_s)$ is precisely the same as the image of a under the map $SO(f)(k)\to X(k)$. Thus the image of c in $H^1(k,T)$ under ψ is given by the class of the cocycle ${}^{\sigma}b.b^{-1}$ viewed in $T(k_s)$ rather than in $\mu_2\subset T(k_s)$. That is, the top diagram is commutative. The commutativity of the bottom square is a special case of Proposition 2.7.

The natural map $\psi:X(k)\to k^*/NK^*$ associated to the torsor $Spin(f)\to X$ under the k-torus T can thus be defined in a more concrete fashion. By Witt's theorem a point in $X(k)$ may be lifted to some element σ in $SO(f)(k)$. One may then send this element σ to $k^*/k^{*2}=H^1(k,\mu_2)$ using the middle horizontal exact sequence. That is, one sends σ to its spinor norm $\theta(\sigma)\in k^*/k^{*2}$. The top horizontal sequence defines a map $H^1(k,\mu_2)\to H^1(k,T)$, which may be identified with the obvious map $k^*/k^{*2}\to k^*/NK^*$. Using this map, one gets an element in $H^1(k,T)$ which one immediately checks does not depend on the choice of the lift σ in $SO(k)$.

Let us assume that d is not a square in k. The torsor $Spin(f)\to X$ is associated to the choice of a k-point M of X. The above discussion yields a map $\mathbb{Z}/2=\mathrm{Pic}\,T\to \mathrm{Br}\,X$. The image of $1\in\mathbb{Z}/2$ is the class of an element $\alpha\in\mathrm{Br}\,X$ which is trivial at M, vanishes when pulled back to $Spin(f)$ and also vanishes when pulled back to $\mathrm{Br}\,X_K$. There thus exists a rational function $\rho\in k(X)^*$ whose divisor on X is the norm of a divisor on X_K and such that the image of α under the embedding $\mathrm{Br}\,X\hookrightarrow \mathrm{Br}\,k(X)$ is the class of the quaternion algebra $(K/k,\rho)$. Let U be the complement of the divisor of ρ. On the subset $U(k) \subset X(k)$ the map $X(k) \to \mathrm{Br}\, k$ defined by α is induced by the evaluation of the function ρ, which yields a map $U(k) \to k^*/N_{K/k}K^* \subset \mathrm{Br}\, k$. In order to implement the results of the previous section it is thus useful to compute such a function ρ. Here is a general way to do it. Let $F = k(X)$ be the function field of X. By Witt's theorem the map $SO(f)(F) \to X(F)$ is onto. One may thus lift the generic point of X to an F-point $\xi \in SO(f)(F)$, which one may write as an even product of reflections τ_{v_i} with respect to anisotropic vectors v_i with F-coordinates. One computes the image of $\xi \in SO(f)(F)$ in $H^1(F, \mu_2) = F^*/F^{*2}$ under the boundary map, that is one computes the spinor norm of ξ. The image of ξ is thus the class of the product $\prod_i f(v_i) \in F^*$. This product yields a desired function ρ.

For later use, it will be useful to give complete recipes for the computation of the map $X(k) \to k^*/NK^*$.

5.7 We start with the general case $m = n+2$. We fix a k-point $M \in X(k)$. As recalled above, this is equivalent to giving n vectors $v_1, \ldots, v_n \in V = k^m$ such that the matrix $\{B_f(v_i, v_j)\}_{i=1,\ldots,n; j=1,\ldots,n}$ gives the coefficients of the quadratic form $g(x_1, \ldots, x_n)$ on $W = k^n$. We may and shall assume $f(v_1) \neq 0$. Let us henceforth write $B(x, y) = B_f(x, y)$.

Let now P be an arbitrary k-point of X, given by a linear map from $W = k^n$ to $V = k^m$ compatible with the bilinear forms. Let $w_1, \ldots, w_n \in k^m$ be the image of the standard basis of W. There exists $\sigma \in SO(f)(k)$ such that $\sigma(M) = P$, i.e. $\sigma(v_i) = w_i$ for each $i = 1, \ldots, n$. Let τ_y be the reflection along the vector $y \in V$ with $f(y) \neq 0$ which is given by

$$\tau_y(x) = x - 2\frac{B(x, y)}{f(y)} y.$$

Over a Zariski open set U of $SO(f)$ such that all the following related reflections are defined, we define $\sigma_1 = \sigma$ and $\sigma_2 = \tau_{v_1}\tau_{\sigma_1 v_1 + v_1}\sigma_1$ if n is odd and $\sigma_2 = \tau_{\sigma_1 v_1 - v_1}\sigma_1$ if n is even. Let

$$\sigma_3 = \tau_{\sigma_2 v_2 - v_2}\sigma_2, \ldots, \sigma_n = \tau_{\sigma_{n-1}v_{n-1} - v_{n-1}}\sigma_{n-1}$$

inductively. Let us prove

$$B(v_i, \sigma_j v_j - v_j) = 0 \tag{5.2}$$

for all $j > i$ with $1 \le i \le n$. Indeed, if $j = i+1 > 2$ or n is even, then

$$\begin{aligned} B(v_i,\ \sigma_{i+1}v_{i+1} - v_{i+1}) &= B(v_i, \tau_{\sigma_i v_i - v_i}\sigma_i v_{i+1}) - B(v_i, v_{i+1}) \\ &= B(\tau_{\sigma_i v_i - v_i} v_i, \sigma_i v_{i+1}) - B(v_i, v_{i+1}) = B(\sigma_i v_i, \sigma_i v_{i+1}) - B(v_i, v_{i+1}) = 0. \end{aligned}$$

If $j = i+1 = 2$ and n is odd, then

$$\begin{aligned} B(v_i, \sigma_{i+1}v_{i+1} - v_{i+1}) &= B(v_1, \tau_{v_1}\tau_{\sigma_1 v_1 + v_1}\sigma_1 v_2 - v_2) \\ &= B(\tau_{\sigma_1 v_1 + v_1}\tau_{v_1} v_1, \sigma_1 v_2) - B(v_1, v_2) = 0. \end{aligned}$$

Suppose (5.2) is true for values less than j. Then

$$\begin{aligned} B(v_i, \sigma_j v_j - v_j) &= B(v_i, \tau_{\sigma_{j-1}v_{j-1} - v_{j-1}} \cdots \tau_{\sigma_i v_i - v_i}\sigma_i v_j) - B(v_i, v_j) \\ &= B(\tau_{\sigma_i v_i - v_i} \cdots \tau_{\sigma_{j-1}v_{j-1} - v_{j-1}} v_i, \sigma_i v_j) - B(v_i, v_j). \end{aligned}$$

By the induction hypothesis, one has

$$\tau_{\sigma_i v_i - v_i} \cdots \tau_{\sigma_{j-1}v_{j-1} - v_{j-1}} v_i = \tau_{\sigma_i v_i - v_i} v_i = \sigma_i v_i$$

and (5.2) follows. From (5.2) we deduce

$$\sigma v_i = \tau_{\sigma_1 v_1 - v_1} \tau_{\sigma_2 v_2 - v_2} \cdots \tau_{\sigma_n v_n - v_n} v_i$$

for all $1 \leq i \leq n$ if n is even and

$$\sigma v_i = \tau_{v_1} \tau_{\sigma v_1 + v_1} \tau_{\sigma_2 v_2 - v_2} \cdots \tau_{\sigma_n v_n - v_n} v_i$$

for all $1 \leq i \leq n$ if n is odd.

For n even, the even product of reflections $\tau_{\sigma_1 v_1 - v_1} \tau_{\sigma_2 v_2 - v_2} \cdots \tau_{\sigma_n v_n - v_n}$ is a lift of P under the map $SO(f) \to X$ associated to M. For n odd, the even product of reflections $\tau_{v_1} \tau_{\sigma_1 v_1 + v_1} \tau_{\sigma_2 v_2 - v_2} \cdots \tau_{\sigma_n v_n - v_n}$ is a lift of P under the map $SO(f) \to X$ associated to M.

The spinor norm of this lift is thus the class of the product $\prod_{i=1}^{n} f(\sigma_i v_i - v_i) \in k^*/k^{*2}$ if n is even or $f(v_1) f(\sigma v_1 + v_1) \prod_{i=2}^{n} f(\sigma_i v_i - v_i) \in k^*/k^{*2}$ if n is odd. Hence the image of $P \in X(k)$ in k^*/NK^* is the class

$$\prod_{i=1}^{n} f(\sigma_i v_i - v_i) \in k^*/N_{K/k} K^*$$

if n is even or

$$f(v_1) f(\sigma v_1 + v_1) \prod_{i=2}^{n} f(\sigma_i v_i - v_i) \in k^*/N_{K/k} K^*$$

if n is odd.

5.8 We now specialize to the case $m = 3$, $n = 1$. This is the classical problem of representing an element $a \in k^*$ by a ternary quadratic form $f(x, y, z)$. The k-variety X is the affine quadric given by the equation

$$f(x, y, z) = a.$$

Assume $d = -a.\operatorname{disc}(f)$ is not a square and $X(k) \neq \emptyset$. Let $K = k(\sqrt{d})$. The general considerations above, or direct ones, show that $\operatorname{Br} X/\operatorname{Br} k = \operatorname{Br}_1 X/\operatorname{Br} k$ has order 2. Here is a more direct way to produce a function ρ with divisor a norm for the extension K/k, such that the quaternion algebra $(\rho, d) \in \operatorname{Br} k(X)$ comes from $\operatorname{Br} X$ and yields a generator of $\operatorname{Br} X/\operatorname{Br} k$. Let $Y \subset \mathbb{P}^3_k$ be the smooth projective quadric given by the homogeneous equation

$$f(x, y, z) = at^2.$$

Suppose a k-rational point M of Y is given. Let $l_1(x, y, z, t)$ be a linear form with coefficients in k defining the tangent plane to Y at M. There then exist linear forms l_2, l_3, l_4, a constant $c \in k^*$ and an identity

$$f(x, y, z) - at^2 = l_1.l_2 + c(l_3^2 - dl_4^2).$$

Such linear forms (and the constant c) are easy to determine. The linear forms l_i are linearly independent. Conversely, if we have such an identity, $l_1 = 0$ is an equation for the tangent plane at the k-point $l_1 = l_3 = l_4 = 0$. Define $\rho = l_1(x, y, z, t)/t \in k(X)$. Consider the quaternion algebra $\alpha = (\rho, d) = (l_1(x, y, z, t)/t, d) \in \operatorname{Br} k(X)$. We have $(l_1(x, y, z, t)/t, d) = (l_2(x, y, z, t)/t, d) \in \operatorname{Br} k(X)$. Thus α is unramified on X_k away from the plane at infinity $t = 0$, and the finitely many closed points given by $l_1 = l_2 = 0$. By the purity theorem for the Brauer group of smooth varieties [Gro68, II, Theorem 2.1 and III, Theorem 6.1], we see that this class is unramified on the affine quadric X, i.e. belongs to $\operatorname{Br} X \subset \operatorname{Br} k(X)$. The complement of X in Y is the smooth projective conic C over k given by $q(x, y, z) = 0$. An easy computation shows that the residue of α at the generic point of this conic is the class of d in $k^*/k^{*2} = H^1(k, \mathbb{Z}/2) \subset H^1(k(C), \mathbb{Z}/2) \subset H^1(k(C), \mathbb{Q}/\mathbb{Z})$ (note that k is algebraically closed in $k(C)$). Since d is not a square in k, this class is not trivial. Thus $\alpha = (\rho, d) \in \mathrm{Br}\, X \subset \mathrm{Br}\, k(X)$ does not lie in the image of $\mathrm{Br}\, k$. It is thus a generator of $\mathrm{Br}\, X/\mathrm{Br}\, k$. Note that, at any k-point of X, either l_1 or l_2 is not zero. The map $X(k) \to \mathrm{Br}\, k$ associated to α can thus be computed by means of the map $X(k) \to k^*/N_{K/k}K^*$ given by either the function $\rho = l_1(x, y, z, t)/t$ or the function $\sigma = l_2(x, y, z, t)/t$.

For later use, let (V, Q) denote the three-dimensional quadratic space which in the given basis $V = k^3$ is defined by $Q(u) = f(x, y, z)$ for $u = (x, y, z)$. Let $B(u, v) = \frac{1}{2}(Q(u + v) - Q(u) - Q(v))$ be the associated bilinear form. Let $v_0 \in V$ correspond to a point M of the affine quadric $f(x, y, z) = a$. Then the affine linear map $\rho : V \to k$ is given by $v \mapsto B(v_0, v) - a$. Thus on the open set $B(v_0, v) - a \neq 0$ of X the restriction of α is given by the quaternion algebra $(B(v_0, v) - a, -a.\, \mathrm{disc}(f))$.

6. Representation of a quadratic form by a quadratic form over a ring of integers

Let k be a number field, and O its ring of integers. Let f and g be quadratic forms over O. Assume g_k and f_k are nondegenerate, of respective ranks $n \geq 1$ and $m \geq n$.

A classical problem raises the question of the representability of g by f, i.e. the existence of linear forms $l_1, \ldots, l_m$ with coefficients in O in the variables $x_1, \ldots, x_n$, such that one has the identity

$$g(x_1, \ldots, x_n) = f(l_1(x_1, \ldots, x_n), \ldots, l_m(x_1, \ldots, x_n)).$$

Such an identity corresponds to a point with O-coordinates of a certain O-scheme $\mathbf{X}$.

There are variants of this question. For instance, when g is of rank one, i.e. of the shape ax^2, in which case one simply asks for the existence of an integral point $y_i = b_i$, $i = 1, \ldots, n$ of the scheme

$$a = f(y_1, \ldots, y_n),$$

one sometimes demands that the ideal spanned by the b_i be the whole ring O (this is a so-called primitive solution of the equation). This simply corresponds to choosing a different O-scheme $\mathbf{X}$, but one with the same generic fibre $X = \mathbf{X} \times_O k$. More precisely one takes the new O-scheme to be the complement of the closed set $y_1 = \cdots = y_n = 0$ in the old $\mathbf{X}$.

In the case $n = m$ and $X(k) \neq \emptyset$ we shall replace the natural X, which is disconnected, by one of its connected components over k, and we shall consider O-schemes $\mathbf{X}$ with generic fibre this component.

Quite generally the following problem may be considered.

Problem. Let k be a number field, and O its ring of integers. Let f and g be nondegenerate quadratic forms over k, of respective ranks m and $n \leq m$. Let $\mathbf{X}$ be a separated O-scheme of finite type equipped with an isomorphism of $X = \mathbf{X} \times_O k$ with the closed k-subvariety of $\mathbb{A}_k^{mn}$ which the identity

$$g(x_1, \ldots, x_n) = f(l_1(x_1, \ldots, x_n), \ldots, l_m(x_1, \ldots, x_n))$$

defines – here the l_i are linear forms. Assume $\prod_v \mathbf{X}(O_v) \neq \emptyset$. Does this imply $\mathbf{X}(O) \neq \emptyset$?

We have adopted the following convention: for v archimedean we set $\mathbf{X}(O_v) = X(k_v)$. One could also naturally address the question of existence and density of S-integral solutions for an arbitrary finite set S of places, as we did in §§ 3 and 4. In the interest of simplicity, in the rest of this paper, when discussing representation of quadratic forms by quadratic forms, we restrict attention to integral representations, as opposed to S-integral representations as considered in earlier sections. Also, we concentrate on the *existence* of integral points and do not systematically state the strongest approximation results. The reader will have no difficulty in applying the general theorems of earlier sections to get the most general results.

According to a well-known result of Hasse, the hypothesis $\prod_v X(k_v) \neq \emptyset$ implies $X(k) \neq \emptyset$.

If $m \geq 3$, then as explained in § 5, we may fix an isomorphism $X \simeq Spin(f)/H$. Here H is a connected linear algebraic group if $m-n \geq 2$, $H = \mu_2$ is $m-n \leq 1$ (as usual, in the case $n=m$, we replace X by one of its connected components).

We shall say that a finite set S of places of k is big enough for $\{f, g\}$ if S contains all the archimedean places, all the dyadic places and all the nonarchimedean places such that $\mathrm{disc}(f)$ or $\mathrm{disc}(g)$ is not a unit.

The following result is well known (Kneser). It is most often stated under the assumption that v_0 is an archimedean place, in which case the above integral representation problem has a positive answer.

Theorem 6.1. *Let f, g and $\mathbf{X}/O$ be as above, with $m-n \geq 3$. Let v_0 be a place of k such that $f_{k_{v_0}}$ is isotropic. If $\prod_v \mathbf{X}(O_v) \neq \emptyset$ then $\mathbf{X}(O_{\{v_0\}}) \neq \emptyset$: there is a point which is integral away from v_0. Moreover $\mathbf{X}(O_{\{v_0\}})$ is dense in the topological product $\prod_{v \neq v_0} \mathbf{X}(O_v)$.*

Proof. In this case $X \simeq Spin(f)/H$ with $\mathrm{Pic}\, H = 0$ and $\mathrm{Br}\, X/\mathrm{Br}\, k = 0$ (§ 5.3). The hypothesis $f_{k_{v_0}}$ isotropic is equivalent to the hypothesis that $SO(f)(k_{v_0})$ or equivalently $Spin(f)(k_{v_0})$ is not compact. The group $Spin(f)$ is almost k-simple except if $m=4$ and the determinant of f is a square. In this special case, there is a quaternion algebra A over k such that $Spin(f) \simeq SL_1(A) \times_k SL_1(A)$ and the algebra A splits over a field F if and only if the quadratic form f is isotropic over F. Thus in all cases Theorem 3.7 with $S_0 = \{v_0\}$ yields the result. □

Remark 6.2. One may prove the above theorem without ever mentioning the Brauer group. One uses the left hand side of diagram (3.1), strong approximation for $G = Spin(f)$ and the Hasse principle: for G semisimple and simply connected, the map $H^1(k, G) \to \prod'_{v \in \Omega_k} H^1(k_v, G)$ reduces to a bijection $H^1(k, G) \to \prod_{v \in S_\infty} H^1(k_v, G)$, where S_∞ denotes the set of archimedean places of k. Surjectivity of the map is used for $H = Spin(h)$, injectivity for $G = Spin(f)$.

When $m-n \leq 2$, examples in the literature, some of which will be mentioned in later sections, show that the existence of local integral solutions is not a sufficient condition for the existence of an integral solution.

Theorem 6.3. *Let f, g and $\mathbf{X}/O$ be as above, with $m-n=2$. Let $d = -\mathrm{disc}(f).\, \mathrm{disc}(g) \in k^*$. Let $K = k[t]/(t^2-d)$. Let T denote the k-torus $R^1_{K/k} G_m$. Assume $\prod_v \mathbf{X}(O_v) \neq \emptyset$. Then $X(k) \neq \emptyset$. Fix $M \in X(k)$. The choice of M defines a k-morphism $SO(f) \to X$. Let $\xi \in H^1_{\text{ét}}(X, T)$ be the class of the T-torsor defined by the composite map $Spin(f) \to SO(f) \to X$. For any field F containing k we have the map $\psi_F : X(F) \to H^1(F, T) = F^*/N(FK)^*$. The quotient $\mathrm{Br}\, X/\mathrm{Br}\, k$ is of order 1 if d is a square, of order 2 if d is not a square. In the latter case it is spanned by the class of an element $\alpha \in \mathrm{Br}\, X$ of order 2, well defined up to addition of an element of $\mathrm{Br}\, k$.*

For a point $\{M_v\} \in \prod_{v\in\Omega_k} \mathbf{X}(O_v)$ the following conditions are equivalent:

(i) *$\{M_v\}$ is orthogonal to* $\operatorname{Br} X$ *for the Brauer–Manin pairing;*

(ii) $\sum_{v\in\Omega_k} \operatorname{inv}_v(\alpha(M_v)) = 0$;

(iii) *$\{M_v\}$ is in the kernel of the composite map*

$$X(\mathcal{A}_k) \to \bigoplus_{v\in\Omega_k} k_v^*/NK_v^* \to \mathbb{Z}/2,$$

where the first map is defined by the various ψ_{k_v} and the second map is the sum of the local Artin maps $k_v^*/NK_v^* \to \operatorname{Gal}(K_v/k_v) \subset \operatorname{Gal}(K/k) = \mathbb{Z}/2$.

Let S be a finite set of places of k, big enough for $\{f, g\}$, and such that there exists an isomorphism $\mathbf{X} \times_O O_S \simeq \mathbf{Spin}(f)/\mathbf{T}$ over O_S. Here $\mathbf{T}$ is an O_S-torus such that $\mathbf{T} \times_{O_S} k = T$.

Then the above conditions on $\{M_v\} \in \prod_{v\in\Omega_k} \mathbf{X}(O_v)$ are equivalent to:

(iv) *the projection $\{M_v\}_{v\in S}$ is in the kernel of the composite map*

$$\prod_{v\in S} X(k_v) \to \bigoplus_{v\in S} k_v^*/NK_v^* \to \mathbb{Z}/2.$$

Let v_0 be a place of k such that $f_{k_{v_0}}$ is isotropic. Under any of the above conditions the element $\{M_v\} \in \prod_{v\in\Omega_k\setminus v_0} \mathbf{X}(O_v)$ can be approximated arbitrarily closely by an element of $\mathbf{X}(O_{\{v_0\}})$. In particular $\mathbf{X}(O_{\{v_0\}}) \neq \emptyset$.

Proof. Just combine § 5.6 with Theorem 3.7. □

Computational recipes

(i) To be in a position to apply the above theorem, one must first exhibit a k-rational point of X. Starting from such a k-point, one determines a finite set S of places as in the theorem. To decide if an $\{M_v\}_{v\in S}$ satisfies (iv), or even if there is such an $\{M_v\}_{v\in S}$, is then the matter of finitely many computations. Indeed one only needs to give a concrete description of the maps $\psi_{k_v} : X(k_v) \to k_v^*/NK_v^*$ for each $v \in S$. This has already been given in § 5.6, with complements in §§ 5.2 and 5.7 for the computation of the spinor norm map.

Given any point $M_v \in X(k_v)$, there exists an element $\sigma_v \in SO(f)(k_v)$ such that $\sigma_v(M) = M_v$. To $\sigma_v \in SO(k_v)$ one associates its spinor norm $\theta(\sigma_v) \in k_v^*/k_v^{*2}$. Then $\psi_{k_v}(M_v)$ is the image of this element under projection $k_v^*/k_v^{*2} \to k_v^*/NK_v^*$.

(ii) In the case $m = 3, n = 1$, that is when X is given by an equation $f(x, y, z) = a$, the discussion in § 5.8 leads to an alternative, possibly more efficient, recipe. Compare the comments after Theorem 3.7.

Theorem 6.4. *Let f, g and $\mathbf{X}/O$ be as above, with $m \geq 3$ and $1 \geq m - n \geq 0$. Assume $\prod_v \mathbf{X}(O_v) \neq \emptyset$. Then $X(k) \neq \emptyset$. The choice of a k-point $M \in X(k)$ defines a k-isomorphism $SO(f) \simeq X$. Let $\xi \in H^1_{\text{ét}}(X, \mu_2)$ be the class of the μ_2-torsor defined by $Spin(f) \to SO(f) \simeq X$. For any field F containing k this torsor defines a map $\psi_F : X(F) \to H^1(F, \mu_2) = F^*/F^{*2}$. The composite map $SO(f)(F) \simeq X(F) \to F^*/F^{*2}$ is the spinor norm map.*

(a) *For a point $\{M_v\} \in \prod_{v\in\Omega_k} \mathbf{X}(O_v)$, the following conditions are equivalent:*

  (i) *$\{M_v\}$ is the kernel of the map $X(\mathcal{A}_k) \to \operatorname{Hom}(\operatorname{Br} X, \mathbb{Q}/\mathbb{Z})$;*

  (ii) *$\{M_v\}$ is in the kernel of the composite map*

$$X(\mathcal{A}_k) \to {\prod}' k_v^*/k_v^{*2} \to \operatorname{Hom}(k^*/k^{*2}, \mathbb{Z}/2),$$

  where the last map is given by the sum over all v of Hilbert symbols.

Assume that the finite set of places S is big enough for (G, μ_2) and that there is an isomorphism $\mathbf{SO}(f) \simeq \mathbf{X} \times_O O_S$ extending $SO(f) \simeq X$. Conditions (i) and (ii) on $\{M_v\} \in \prod_{v \in \Omega_k} \mathbf{X}(O_v)$ imply:

(iii) *the point $\{M_v\}_{v \in S} \in \prod_{v \in S} \mathbf{X}(O_v)$ is in the kernel of the map*

$$\prod_{v \in S} X(k_v) \to \prod_{v \in S} k_v^*/k_v^{*2} \to \mathrm{Hom}(H^1_{\text{ét}}(O_S, \mu_2), \mathbb{Z}/2).$$

Let v_0 be a place of k such that $f_{k_{v_0}}$ is isotropic.

(b) *If $\{M_v\} \in \prod_{v \in \Omega_k} \mathbf{X}(O_v)$ satisfies condition (i) or (ii) and S_1 is a finite set of places containing v_0, then there exists $M \in \mathbf{X}(O_{\{v_0\}})$ arbitrarily close to each M_v for $v \in S_1 \setminus S_0$. In particular $\mathbf{X}(O_{\{v_0\}}) \neq \emptyset$.*

(c) *If the finite set S of places is as above and contains v_0 and if $\{M_v\}_{v \in S} \in \prod_{v \in S} \mathbf{X}(O_v)$ is as in condition (iii), then there exists $M \in \mathbf{X}(O_{\{v_0\}})$ arbitrarily close to each M_v for $v \in S \setminus S_0$. In particular $\mathbf{X}(O_{\{v_0\}}) \neq \emptyset$.*

Proof. Just combine §§ 5.4 and 5.5 with Theorem 4.5. □

Computational recipe

One first exhibits some point $M \in X(k)$. Using this point one determines S as in the theorem. One enlarges S so that the 2-torsion of the class group of O_S vanishes. One then has $O_S^*/O_S^{*2} \simeq H^1_{\text{ét}}(O_S, \mu_2)$. The group O_S^*/O_S^{*2} is finite.

First method. To each element $\eta \in O_S^*/O_S^{*2}$ one associates the cup-product $\xi \cup \eta \in H^2(X, \mu_2)$ which one then pushes into $\mathrm{Br}\, X$. This produces finitely many elements $\{\beta_j\}_{j \in J}$ of order 2 in $\mathrm{Br}\, X$, which actually are classes of quaternion Azumaya algebras over $\mathbf{X} \times_O O_S$. For a given j one considers the map

$$\prod_{v \in S} \mathbf{X}(O_v) \to \mathbb{Z}/2$$

given by $\{M_v\}_{v \in S} \mapsto \sum_{v \in S} \mathrm{inv}_v(\beta_j(M_v)) \in \mathbb{Z}/2$. One then checks whether there exists a point $\{M_v\} \in \prod_{v \in S} \mathbf{X}(O_v)$ which simultaneously lies in the kernel of these finitely many maps.

Second method. One considers the map $X(k) \to H^1(k, \mu_2) = k^*/k^{*2}$ associated to ξ. For S as above, the image of $\mathbf{X}(O_S)$ lies in the finite group $C = H^1_{\text{ét}}(O_S, \mu_2) = O_S^*/O_S^{*2}$. For each element $\rho \in C$, one considers the μ_2-torsor Y^ρ over X obtained by twisting Y by a representant of $\rho^{-1} \in O_S^*/O_S^{*2} \subset k^*/k^{*2}$. Then the kernel in (iii) is not empty if and only if there exists at least one $\rho \in C$ and a family $\{M_v\} \in \prod_{v \in S} \mathbf{X}(O_v)$ such that there exists a family $\{N_v\} \in \prod_{v \in S} Y^\rho(k_v)$ which maps to $\{M_v\} \in \prod_{v \in S} X(k_v)$ under the structural map $Y^\rho \to X$.

7. Genera and spinor genera

A necessary condition for an integral quadratic form g to be represented by an integral quadratic form f (of rank at least 3) over the integers is that it be represented by f over each completion of the integers and at the infinite places. If that is the case, g is said to be represented by the genus of f. A further, classical necessary condition, considered by Eichler [Eic52] and Kneser [Kne56], is that g be represented by the spinor genus of f (see [O'Me71]). In this section we first recall the classical language of lattices. We then show how the spinor genus condition boils down to an integral Brauer–Manin condition of the type considered in the previous section. Finally, we compare the results in terms of the Brauer–Manin obstruction with some results obtained in [CX04, HSX98, Kne61, Xu05, SX04]. With hindsight, we see that some version of the Brauer–Manin condition had already been encountered in these papers.

7.1 Classical parlance

Let k be a number field and O its ring of integers. Let V be a finite-dimensional vector space over k equipped with a nondegenerate quadratic form f with associated bilinear form B_f. A quadratic lattice $L \subset V$ is a finitely generated, hence projective, O-module such that $f(L) \subset O$ and such that the restriction of the quadratic form f on $L_k = L \otimes_O k \subset V$ is nondegenerate. Given any element $\sigma \in O(f)(k)$ the O-module $\sigma.L$ is a quadratic lattice. A quadratic lattice L is called full if its rank is maximal, i.e. $L_k = V$.

Two full quadratic lattices L_1 and L_2 are in the same class, respectively the same proper class, if there exists $\sigma \in O(f)(k)$, respectively $\sigma \in SO(f)(k)$, such that $L_1 = \sigma.L_2$.

Given a quadratic lattice $N \subset V$ of rank n and a full quadratic lattice $M \subset V$ of rank $m = \dim_k V$, one asks whether there exists $\sigma \in O(f)(k)$, respectively $\sigma \in SO(f)(k)$, such that $N \subset \sigma.M$. If the rank of N is strictly less than the rank of M, i.e. if N is not full, the two statements are equivalent.

If that is the case, one says that the quadratic lattice N is represented by the class, respectively the proper class, of the quadratic lattice M. One sometimes writes $N \to cls(M)$, respectively $N \to cls^+(M)$.

From now on we assume $m = \dim V \geq 3$. (The case $m = 2$ is very interesting but requires other techniques.)

There is an action of the group of adèles $O(f)(\mathcal{A}_k)$ (via the finite components) on the set of full quadratic lattices in V. Indeed, given an adèle $\{\sigma_v\} \in O(f)(\mathcal{A}_k)$ and a full quadratic lattice $L \subset V$, one shows [O'Me71, 81:14] that there exists a unique full quadratic lattice $L_1 \subset V$ such that $L_1 \otimes_O O_v = \sigma_v(L \otimes_O O_v) \subset V \otimes_k k_v$ for each finite place v.

Two full quadratic lattices in (V, f) in the same orbit of $O(f)(\mathcal{A}_k)$ are said to be in the same genus. They automatically lie in the same orbit of $SO(f)(\mathcal{A}_k) \subset O(f)(\mathcal{A}_k)$ (see [O'Me71, § 102 A]).

One says that a quadratic lattice $N \subset V$ is represented by the genus of the full quadratic lattice $M \subset V$ if there exists at least one quadratic lattice $M_1 \subset V$ in the genus of M such that $N \subset M_1 \subset V$. One sometimes writes $N \to gen(M)$.

We have the natural isogeny $\varphi : Spin(f) \to SO(f)$, with kernel μ_2. The group $Spin(f)(\mathcal{A}_k)$ acts on the set of maximal quadratic lattices in V through φ. The group $\varphi(Spin(f)(\mathcal{A}_k))$ is a normal subgroup in $SO(f)(\mathcal{A}_k)$. One therefore has an action of the group

$$O(f)(k) \cdot \varphi(Spin(f)(\mathcal{A}_k)) = \varphi(Spin(f)(\mathcal{A}_k)) \cdot O(f)(k)$$

on the set of such lattices. One says that two full quadratic lattices are in the same spinor genus, respectively in the same proper spinor genus, if they are in the same orbit of the group $O(f)(k) \cdot \varphi(Spin(f)(\mathcal{A}_k))$, respectively of the group $SO(f)(k) \cdot \varphi(Spin(f)(\mathcal{A}_k))$.

One says that a quadratic lattice $N \subset V$ is represented by the spinor genus, respectively the proper spinor genus of the full quadratic lattice M if there exists at least one quadratic lattice $M_1 \subset V$ in the spinor genus, respectively in the proper spinor genus of M, such that $N \subset M_1$. One sometimes writes $N \to spn(M)$, respectively $N \to spn^+(M)$.

Let $N \subset V$ and $M \subset V$ be quadratic lattices in (V, f), with M a full lattice. There is an induced quadratic form f on M and an induced quadratic form g on N. We may then consider (N, g) and (M, f) as abstract quadratic spaces over O (with associated bilinear form nondegenerate over k, but not necessarily over O). We let $N_k = N \otimes_O k$ and $M_k = M \otimes_O k = V$.

Let $\mathrm{Hom}_O(N, M)$ be the scheme of linear maps from N into M. Let $\mathbf{X}/O$ be the closed subscheme defined by the linear maps compatible with the quadratic forms on N and M. Let $X = \mathbf{X} \times_O k$. As explained in § 1, for the purposes of this paper we may if we wish replace $\mathbf{X}$, which need not be flat over O (dimensions of fibres may jump), by the schematic closure of X in $\mathbf{X}$, which is integral and flat over O. This does not change the generic fibre X, and it does not change the sets $\mathbf{X}(O)$ and $\mathbf{X}(O_v)$.

Since we are given quadratic lattices $N \subset V$ and $M \subset V$ in the same quadratic space (V, f) over k, we are actually given a k-point $\rho \in X(k)$, that is a k-linear map $\rho : N_k \to M_k$ which is compatible with the quadratic forms f and g. Conversely such a map defines a point of $X(k)$. If $n < m$ then the k-variety X is connected and is a homogeneous space of $SO(f)$. If $n = m$, we shall henceforth replace X by the connected component to which the given k-point belongs and $\mathbf{X}$ by the schematic closure of that connected component; the new X is a (principal) homogeneous space of $SO(f)$. In all cases, we shall view the k-variety X as a homogeneous space of the k-group $Spin(f)$.

7.2 Classical parlance versus integral Brauer–Manin obstruction

Proposition 7.1. *With notation as in § 7.1, the following conditions are equivalent.*

(i) *The quadratic lattice N is represented by the proper class of the quadratic lattice M.*

(ii) *We have $\mathbf{X}(O) \neq \emptyset$.*

Proof. Assume (i). Thus there exists $\sigma \in SO(f)(k)$ such that $\sigma(N) \subset M \subset V$. The linear map $\sigma(\rho) : N_k \to M_k$ sends N to M and is compatible with the quadratic forms. It is thus a point of $\mathbf{X}(O)$.

Assume (ii). There exists an O-linear map $\lambda : N \to M$ which is compatible with the quadratic forms f and g. We also have the given k-point $\rho \in X(k)$. By a theorem of Witt and the definition of $\mathbf{X}$ in the case $n = m$ there exists $\sigma \in SO(f)(k)$ such that $\sigma(\rho) = \lambda_k$ over k. Thus $\sigma(N) \subset M \subset V$. □

Proposition 7.2. *With notation as in § 7.1, the following conditions are equivalent.*

(i) *The quadratic lattice N is represented by the genus of the quadratic lattice M.*

(ii) *We have $\prod_{v \in \Omega_k} \mathbf{X}(O_v) \neq \emptyset$.*

Proof. For any place v of k let $N_v = N \otimes_O O_v$ and $M_v = M \otimes_O O_v$.

Assume (i). Let $\{\sigma_v\} \in SO(f)(\mathcal{A}_k)$ be such that $\sigma_v(N_v) \subset M_v \subset V \otimes_k k_v$. For each finite place v the linear map $\sigma_v(\rho) : N \otimes_k k_v \to M \otimes_k k_v$ sends N_v to M_v and is compatible with the quadratic forms. It is thus a point of $\mathbf{X}(O_v)$. By assumption $\rho \in X(k)$. Thus for v archimedean $\mathbf{X}(O_v) = X(k_v) \neq \emptyset$.

Assume (ii). The argument given in the proof of the previous proposition shows that for each place $v \in \Omega_k$ there exists $\tau_v \in SO(f)(k_v)$ such that $N_v \subset \tau_v(M_v)$. For all places v of k not in a finite set $S \subset \Omega_k$, the discriminant of g and the discriminant of f are units in O_v, N_v is an orthogonal factor of the unimodular O_v-lattice M_v and it is also an orthogonal factor in the unimodular O_v-lattice $\tau_v(M_v)$. For each place $v \notin S$ there thus exists $\varsigma_v \in SO(f)(k_v)$ which sends isomorphically $\tau_v(M_v)$ to $M_v \subset V \otimes_k k_v$ and induces the identity map on $N_v \subset M_v \subset V \otimes_k k_v$

(see [O'Me71, Theorem 92:3]). Therefore $\varsigma_v \tau_v M_v = M_v$ for all $v \notin S$. Let $\varsigma_v = 1$ for $v \in S$. Then $\{\varsigma_v \tau_v\} \in SO(f)(\mathcal{A}_k)$ and $N_v \subset \varsigma_v \tau_v M_v$ for all v. Therefore N is represented by the genus of M. □

Proposition 7.3. *With notation as in § 7.1, the following conditions are equivalent.*

(i) *The quadratic lattice N is represented by the proper spinor genus of the quadratic lattice M.*

(ii) *We have $(\prod_{v\in\Omega_k} \mathbf{X}(O_v))^{\mathrm{Br}\, X} \neq \emptyset$.*

Proof. Assume (i). Let $\sigma \in SO(f)(k)$ and $\{\tau_v\} \in \varphi(Spin(\mathcal{A}_k))$ be such that $N_v \subset \{\tau_v\}\sigma M_v$ for each $v \in \Omega_k$. The map $\sigma(\rho) : N_k \to M_k$ defines a k-point $p \in X(k)$, which itself defines a point $\{p_v\} \in X(\mathcal{A}_k)$. One then applies the element $\{\tau_v\} \in \varphi(Spin(\mathcal{A}_k))$ to get the point $\{x_v\} = \{\tau_v.p\} \in X(\mathcal{A}_k)$. By hypothesis, the element $\{x_v\}$ lies in $\prod_{v\in\Omega_k} \mathbf{X}(O_v)$. Since $\{p_v\} \in X(\mathcal{A}_k)$ is the diagonal image of an element of $X(k)$, it is orthogonal to $\mathrm{Br}\, X$. Consider diagram (3.1) after Theorem 3.1 if $m - n \geq 2$, respectively diagram (4.3) after Theorem 4.1 if $0 \leq m - n \leq 1$. The commutativity of those diagrams implies that the image of $\{x_v\} = \{\tau_v.p\}$ in $\mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$, respectively $\mathrm{Hom}(H^1(k, \hat{\mu}), \mathbb{Q}/\mathbb{Z})$, is zero. If $m - n \geq 2$ we know from §§ 5.3 and 5.6 that the map $\mathrm{Hom}(\mathrm{Br}\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\mathrm{Pic}\, H, \mathbb{Q}/\mathbb{Z})$ is an isomorphism. If $0 \leq m - n \leq 1$ we know from §§ 5.4 and 5.5 that the map $\mathrm{Hom}(\mathrm{Br}\, X/\mathrm{Br}\, k, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(H^1(k, \hat{\mu}), \mathbb{Q}/\mathbb{Z})$ is an isomorphism. Thus in all cases we find that $\{x_v\}$ lies in $(\prod_{v\in\Omega_k} \mathbf{X}(O_v))^{\mathrm{Br}\, X}$.

Assume (ii). Let $\{x_v\}$ belong to $(\prod_{v\in\Omega_k} \mathbf{X}(O_v))^{\mathrm{Br}\, X}$. Each x_v corresponds to an O_v-linear map $N_v \to M_v$ which respects the quadratic forms f and g. We have $X = G/H$ with $G = Spin(f)$ and H semisimple simply connected if $m - n \geq 3$, H a one-dimensional k-torus T if $m - n = 2$ and $H = \mu_2$ if $0 \leq m - n \leq 1$. Applying Theorem 3.3 when H is connected and Theorem 4.3 when $H = \mu_2$, we see that there exists a rational point $p \in X(k)$, with associated linear map $N_k \to M_k$ and $\{\tau_v\} \in \varphi(Spin(\mathcal{A}_k))$ such that $\tau_v p = x_v \in \mathbf{X}(O_v)$ for all v. By Witt's theorem there exists $\sigma \in SO(f)(k)$ such that $\sigma(\rho) : N_k \to M_k$ is given by the point p. Then $\tau_v\sigma(N_v) \subset M_v$ for all v. Thus N is represented by the proper spinor genus of M. □

Remark 7.4. Let N, M be quadratic lattices in the quadratic space (V, f), with M a full lattice. Let us assume there exists an archimedean place v_0 of k such that f is isotropic over k_{v_0}, that is $Spin(f)(k_{v_0})$ is not compact.

Using the above propositions, we recover the classical result: for such an f and $m - n \geq 3$, Theorem 6.1 implies that any quadratic lattice N represented by the genus of M is represented by the proper class of M.

In the cases $m - n \leq 2$, Theorems 6.3 and 6.4 show that the representation of a given quadratic lattice N by the proper class of M may be decided after a finite amount of computation.

7.3 Relation with some earlier literature

We keep notation as in § 7.1. We thus have a finite-dimensional vector space V over k of rank $m \geq 3$, equipped with a nondegenerate quadratic form f. We are given two quadratic lattices $N \subset V$ and $M \subset V$, with M a full lattice.

We let $\mathbf{X}/O$ be the closed subscheme of $\mathrm{Hom}_O(N, M)$ consisting of maps which respect the quadratic form f on M and the form g it induces on N. We let $X = \mathbf{X} \times_O k$. The natural inclusion $N_k \subset M_k = V$ determines a k-point $\rho \in X(k)$. When $n = m$ we replace X by the connected component of ρ and $\mathbf{X}$ by the schematic closure of that component in $\mathbf{X}$. If we wish, when $n < m$, we may perform the same replacement.

In this subsection we work under the standard assumption $\prod_v \mathbf{X}(O_v) \neq \emptyset$.

We have the natural homogeneous map

$$\phi : SO(f) \to X$$

sending 1 to the point ρ. For any field K containing k, the induced map $SO(f)(K) \to X(K)$ is surjective (Witt).

In earlier studies of the representation of N by M (see [CX04, p. 287] and [Xu05, p. 38]), the following sets played an important rôle. For any place v of k, one lets

$$X(M_v/N_v) = \{\sigma \in SO(f)(k_v) : N_v \subset \sigma(M_v)\}.$$

For almost all places v, the form f is nondegenerate over O_v and there is an inclusion $N_v \subset M_v$ over O_v which over k_v yields $\rho \otimes_k k_v$. For almost all v we therefore have

$$SO(f)(O_v) \subset X(M_v/N_v).$$

The set $X(M_v/N_v)$ is not empty if and only if $\mathbf{X}(O_v) \neq \emptyset$. As a matter of fact,

$$X(M_v/N_v) = \phi^{-1}(\mathbf{X}(O_v)) \subset SO(f)(k_v).$$

The spinor maps induce maps

$$\theta_v : X(M_v/N_v) \to k_v^*/k_v^{*2}.$$

With notation as in Theorem 6.3 we have the following theorem.

Theorem 7.5. *Assume $m - n = 2$. Let $d = -\mathrm{disc}(f).\,\mathrm{disc}(g)$ and $K = k[t]/(t^2 - d)$. The following conditions are equivalent.*

(i) *The quadratic lattice N is represented by the proper spinor genus of the quadratic lattice M.*

(ii) *We have $(\prod_{v\in\Omega_k} \mathbf{X}(O_v))^{\mathrm{Br}\,X} \neq \emptyset$.*

(iii) *There exists a point in the kernel of the composite map*

$$\prod\nolimits'_{v\in\Omega_k} X(M_v/N_v) \to \prod\nolimits'_{v\in\Omega_k} k_v^*/k_v^{*2} \to \bigoplus_{v\in\Omega_k} k_v^*/N_{K/k}K_v^* \to \mathbb{Z}/2.$$

The restricted product on the left hand side is taken with respect to the subsets $SO(f)(O_v) \subset X(M_v/N_v)$ at places of good reduction.

Let S be a finite set of places containing all archimedean places, all dyadic places, all finite places v at which either disc(f) *or* disc(g) *is not a unit. Assume moreover that at each finite nondyadic place $v \notin S$ the natural injection $N_{k_v} \subset M_{k_v}$, which is given by ρ_{k_v}, comes from an injection $N_v \subset M_v$. Then the above conditions are equivalent to the following.*

(iv) *There exists a point in the kernel of the composite map*

$$\prod_{v\in S} X(M_v/N_v) \to \prod_{v\in S} k_v^*/k_v^{*2} \to \bigoplus_{v\in S} k_v^*/N_{K/k}K_v^* \to \mathbb{Z}/2.$$

If the form f is isotropic at an archimedean place of k, these conditions are equivalent to the following.

(v) *The quadratic lattice N is represented by the proper class of M.*

Proof. Combine Proposition 7.3 and Theorem 6.3. Note that the assumption on S ensures that $\rho \in X(k)$ actually belongs to $\mathbf{X}(O_S)$ and defines an O_S-isomorphism $\mathbf{Spin}(f)/\mathbf{T} \simeq \mathbf{X} \times_O O_S$, for $\mathbf{T}$ as in Theorem 6.3. □

With notation as in Theorem 6.4 we have the following theorem.

Theorem 7.6. *Assume $0 \le m-n \le 1$. With notation as above, the following three conditions are equivalent.*

(i) *The quadratic lattice N is represented by the proper spinor genus of the quadratic lattice M.*

(ii) *We have $(\prod_{v\in\Omega_k} \mathbf{X}(O_v))^{\mathrm{Br}\, X} \neq \emptyset$.*

(iii) *There exists a point in the kernel of the composite map*

$$\prod\nolimits'_{v\in\Omega_k} X(M_v/N_v) \to \prod\nolimits'_{v\in\Omega_k} k_v^*/k_v^{*2} \to \mathrm{Hom}(k^*/k^{*2}, \mathbb{Z}/2).$$

Let S be a finite set of places containing all archimedean places, all dyadic places, all finite places v at which disc(f) *or* disc(g) *is not a unit. Suppose the form f is isotropic at an archimedean place of k. Then these conditions are equivalent to the following.*

(iv) *There exists a point in the kernel of the composite map*

$$\prod_{v\in S} X(M_v/N_v) \to \prod_{v\in S} k_v^*/k_v^{*2} \to \mathrm{Hom}(H^1_{\text{ét}}(O_S,\mu_2), \mathbb{Z}/2).$$

(v) *The quadratic lattice N is represented by the proper class of M.*

Proof. Combine Proposition 7.3 and Theorem 6.4. Note that the assumption on S ensures that $\rho \in X(k)$ actually belongs to $\mathbf{X}(O_S)$. Note that the assumption on S ensures that $\rho \in X(k)$ actually belongs to $\mathbf{X}(O_S)$ and defines an O_S-isomorphism $\mathbf{SO}(f) \simeq \mathbf{X} \times_O O_S$. □

Remark 7.7. The equivalence of (i) and (iii) in each of the last two theorems appears in various guises in the literature. Let us here quote Eichler [Eic52], Kneser [Kne61, see Satz 2, p. 93], Jones and Watson [JW56], Schulze-Pillot [Sch80, see Satz 1, Satz 2], [Sch00, Sch04], and most particularly Hsia, Shao and Xu [HSX98, Theorem 4.1]. See also [Xu00], [CX04, Theorem 3.6, p. 292], [SX04, Proposition 7.1] and [Xu05, (5.4) and Corollary 5.5, p. 50].

One may rephrase Theorems 7.5 and 7.6 in terms of the *spinor class fields* defined in [HSX98, p. 131]. The construction of such spinor class fields is based on the following fact, which is proved by *ad hoc* computations [HSX98, Theorem 2.1].

Fact. *Let v be a finite place of k. If $N_v \subseteq M_v$, then the set $\theta(X(M_v/N_v))$ is a subgroup of k_v^*/k_v^{*2}.*

Assume that $\prod_{v\in\Omega_k} \mathbf{X}(O_v) \neq \emptyset$. There is $\sigma \in SO(f)(k_v)$ such that $\sigma N_v \subseteq M_v$. Then $\theta(X(\sigma^{-1}M_v/N_v))$ is a subgroup of k_v^*/k_v^{*2} by the above fact. Let $\tau \in SO(f)(k_v)$ such that $\tau N_v \subseteq M_v$. Then

$$X(\sigma^{-1}M_v/N_v)\sigma^{-1} = X(\tau^{-1}M_v/N_v)\tau^{-1} \subset SO(f)(k_v).$$

This implies that the group $\theta(X(\sigma^{-1}M_v/N_v)) \subset k_v^*/k_v^{*2}$ is independent of the choice of σ. For all v such that $2\det(N)\det(M)$ is a unit, this subgroup contains O_v^*/O_v^{*2}. One lets $\theta(M_v,N_v) \subset k_v^*$ denote its inverse image under the map $k_v^* \to k_v^*/k_v^{*2}$.

The finite Kummer 2-extension $\Sigma_{M/N}$ of k corresponding to

$$k^* \prod\nolimits'_{v\in\Omega_k} \theta(M_v, N_v)$$

is called the *spinor class field* of M and N. The notation $\prod'$ here means the trace of $\prod'_{v\in\Omega_k}\theta(M_v,N_v)\subset\prod_v k_v^*$ on the group of idèles of k.

In the situation of Theorem 7.5 ($m-n=2$), one has $k\subset\Sigma_{M/N}\subset K=k(\sqrt{d})$. In the situation of Theorem 7.6 ($m-n\leq 1$), the field extension $\Sigma_{M/N}/k$ is a subfield of the maximal Kummer 2-extension of k which is ramified only at primes with $v|2\det(M)$ and at the archimedean primes.

The detailed comparison with the results of [HSX98] is left to the reader.

There are several articles devoted to explicit computations of the group $\theta(M_v,N_v)$ in terms of the local Jordan splitting of M_v and N_v. In the case $rank(M_v)=3$, $rank(N_v)=1$, the group $\theta(M_v,N_v)$ is computed in [Sch80] for v nondyadic or 2-adic and it is computed in [Xu00] for the general dyadic case. In [HSX98], the group $\theta(M_v,N_v)$ is computed for general M_v and N_v with nondyadic v.

7.4 Spinor exceptions

In this subsection we assume $m=n+2$.

Definition 7.8. Suppose the quadratic lattice N is represented by the genus of the quadratic lattice M. The lattice N is called a spinor exception for the genus of M if there is a proper spinor genus in $gen(M)$ such that no lattice in that proper spinor genus represents N.

That is to say, there exists a lattice M' in $gen(M)$ such that N is represented by $gen(M')$ but no lattice in the proper spinor genus of M' represents N.

We let $\mathbf{X}$ and X be associated to the pair N,M as in the beginning of § 7.3. If N is a spinor exception for $gen(M)$, then Proposition 7.3 and § 5.6 imply

$$d=-\det(M)\cdot\det(N)\notin k^{*2}$$

and $\mathrm{Br}\,X/\mathrm{Br}\,k\cong\mathbb{Z}/2$.

Proposition 7.9. *Suppose the lattice N is represented by $gen(M)$. Suppose we have $d=-\det(M)\cdot\det(N)\notin k^{*2}$. Let $K=k(\sqrt{d})$. Let $A\in\mathrm{Br}\,X$ generate the group $\mathrm{Br}\,X/\mathrm{Br}\,k\cong\mathbb{Z}/2$. The following conditions are equivalent.*

- (i) *N is a spinor exception for $gen(M)$.*
- (ii) *For each $v\in\Omega_k$, A assumes only a single value on $\mathbf{X}(O_v)$.*

Proof. The condition in (ii) does not depend on the representant A. Since $X(k)\neq\emptyset$, there exists an element $A\in\mathrm{Br}\,X$ which is of exponent 2 in $\mathrm{Br}\,X$ and which generates $\mathrm{Br}\,X/\mathrm{Br}\,k\cong\mathbb{Z}/2$. We fix such an element $A\in\mathrm{Br}\,X$.

Assume that, for some place v, A takes two distinct values on $\mathbf{X}(O_v)$. This implies that A has a nontrivial image in the group $\mathrm{Br}\,X_{k_v}/\mathrm{Br}\,k_v$, which is of order at most 2. The natural map $\mathbb{Z}/2=\mathrm{Br}\,X/\mathrm{Br}\,k\to\mathrm{Br}\,X_{k_v}/\mathrm{Br}\,k_v$ is thus an isomorphism. Let M' be a lattice in the genus of M. Let $\mathbf{X}'$ be the O-scheme attached to the pair N,M'. The hypothesis that M' is in the genus of M implies that there exists an isomorphism of k_v-schemes $X'_{k_v}=\mathbf{X}'\times_O k_v\cong\mathbf{X}\times_O k_v=X_{k_v}$. The latter map induces an isomorphism $\mathrm{Br}\,X_{k_v}/\mathrm{Br}\,k_v\cong\mathrm{Br}\,X'_{k_v}/\mathrm{Br}\,k_v$. The inverse image $B\in\mathrm{Br}\,X'_{k_v}$ of $A\in\mathrm{Br}\,X$ under the composite map $X'_{k_v}\cong X_{k_v}\to X$ takes two distinct values on $\mathbf{X}'(O_v)$. We also have a natural map $\mathrm{Br}\,X'/\mathrm{Br}\,k\to\mathrm{Br}\,X'_{k_v}/\mathrm{Br}\,k_v$. Since M' is in the genus of M, there exists an isomorphism of k-varieties $X\cong X'$. The map $\mathrm{Br}\,X'/\mathrm{Br}\,k\to\mathrm{Br}\,X'_{k_v}/\mathrm{Br}\,k_v$ is therefore an isomorphism, and both groups are isomorphic to $\mathbb{Z}/2$. There thus exists an element A' of order 2 in $\mathrm{Br}\,X'$ whose image in $\mathrm{Br}\,X'_{k_v}$ differs from B by an element in $\mathrm{Br}\,k_v$. Thus A' takes two distinct values on $\mathbf{X}'(O_v)$. This implies $(\prod_{v\in\Omega_k}\mathbf{X}'(O_v))^{\mathrm{Br}\,X'}\neq\emptyset$. By Proposition 7.3 this shows that N is represented by the proper spinor genus of the quadratic lattice M'. Since M' is an arbitrary lattice in the genus of M, this shows that (i) implies (ii).

Assume (ii). If the sum of the values of A on each $\mathbf{X}(O_v)$ is nonzero, then by Proposition 7.3 N is not represented by the proper spinor genus of M so N is a spinor exception. Let us assume otherwise. Thus the value $\mathrm{inv}_v(A(\mathbf{X}(O_v)))\in\mathbb{Z}/2$ is well defined and we have

$$\sum_{v\in\Omega_k}\mathrm{inv}_v(A(\mathbf{X}(O_v)))=0\in\mathbb{Z}/2.$$

For any smooth compactification X_c of X, we have $\mathrm{Br}\,k=\mathrm{Br}\,X_c$. This is easy to show in the case $n=1, m=3$. In the general case, this follows from [CK06] (see Proposition 2.10(iii) above) together with the easy computation that for the k-torus $T=R^1_{K/k}\mathbb{G}_m$ any class in $H^1(\mathfrak{g},\hat{T})$ whose restriction to procyclic subgroups of $\mathfrak{g}$ vanishes must itself vanish. Thus the class $A\in\mathrm{Br}\,X$ does not extend to a class on a smooth compactification of X. By a result of Harari [Har94, Corollaire 2.6.1], this implies that there exist infinitely many primes $v_0\in\Omega_k$ such that A takes at least two distinct values over $X(k_{v_0})$. We choose such a prime v_0, nonarchimedean and such that ρ_{v_0} sends N_{v_0} into M_{v_0}, i.e. $\rho_{v_0}\in\mathbf{X}(O_{v_0})$.

Let $P\in X(k_{v_0})$ be such that

$$\mathrm{inv}_{v_0}(A(P))\neq\mathrm{inv}_{v_0}(A(\mathbf{X}(O_{v_0})))\in\mathbb{Z}/2.$$

By Witt's theorem, there exists $\sigma\in SO(V\otimes_k k_{v_0})$ sending the point $\rho\in X(k)$ to $P\in X(k_{v_0})$.

Let the quadratic lattice $M'\subset V$ be defined by the conditions $M'_v=M_v$ over O_v for each $v\neq v_0$ and $M'_{v_0}=\sigma M_{v_0}$ over O_{v_0}. The lattice M' is in the genus of M.

Let $\mathbf{X}'$ be the O-scheme attached to the pair of lattices N, M'. We have equalities $\mathbf{X}\times_O k=X$ and $\mathbf{X}'\times_O k=X$. For each $v\neq v_0$ we have an equality $\mathbf{X}\times_O O_v=\mathbf{X}'\times_O O_v$. For $v=v_0$, the k_{v_0}-isomorphism $\sigma: X\times_k k_{v_0}\simeq X\times_k k_{v_0}$ induces a bijection between $\mathbf{X}(O_{v_0})$ and $\mathbf{X}'(O_{v_0})$. Let $Q\in\mathbf{X}'(O_{v_0})$ be the image of ρ under this bijection. The image of Q under the natural embedding $\mathbf{X}'(O_{v_0})\subset X(k_{v_0})$ is the point P.

For $v\neq v_0$, for trivial reasons, the element A takes on $\mathbf{X}'(O_v)$ the same value as A on $\mathbf{X}(O_v)$. For $v=v_0$, the values taken by A on $\mathbf{X}'(O_{v_0})$ are those taken by $\sigma^*(A)$ on $\mathbf{X}(O_{v_0})$. Since σ is an automorphism of the k_{v_0}-scheme $X\times_k k_{v_0}$, the element $\sigma^*(A)\in\mathrm{Br}(X\times_k k_{v_0})$ is of order 2 and its class generates $\mathrm{Br}(X\times_k k_{v_0})/\mathrm{Br}(k_{v_0})=\mathbb{Z}/2$. Thus $\sigma^*(A)$ differs from A by an element in $\mathrm{Br}(k_{v_0})$. In particular it takes a single value on $\mathbf{X}(O_{v_0})$, thus A takes a single value on $\mathbf{X}'(O_{v_0})$. That value is the one taken on P.

Thus for any $\{M_v\}\in\prod_{v\in\Omega_k}\mathbf{X}'(O_v)$ we have

$$\sum_{v\in\Omega_k}\mathrm{inv}_v(A'(M_v))\neq 0\in\mathbb{Z}/2,$$

hence

$$\left(\prod_{v\in\Omega_k}\mathbf{X}'(O_v)\right)^{\mathrm{Br}\,X'}=\emptyset.$$

By Proposition 7.3 this implies that N is not represented by the proper spinor genus of M'. Therefore N is a spinor exception for $gen(M)$. □

With notation as in § 7.3 (see especially Remark 7.7), the above result and [HSX98, Theorem 4.1] give the following corollary.

COROLLARY 7.10. *With notation as in this and the previous section the following conditions are equivalent:*

(i) *N is a spinor exception for the genus of M;*

(ii) $\Sigma_{M/N} = K$*;*

(iii) $\theta(M_v, N_v) = N_{K_w/k_v}(K_w^*)$ *for all* $v \in \Omega_k$ *and* $w|v$*;*

(iv) *for any* $A \in \operatorname{Br} X$ *which generates* $\operatorname{Br} X/\operatorname{Br} k$*,* $\operatorname{inv}_v(A)$ *takes a single value over* $\mathbf{X}(O_v)$ *for all* $v \in \Omega_k$.

Remark 7.11. If these conditions are fulfilled, then it is known that N is represented by exactly half the spinor genera in $gen(M)$.

It is a purely local problem to determine whether N is a spinor exception for $gen(M)$. Moreover the finiteness of the set of extensions $\Sigma_{M/N}$ for a given M implies that the determinants $\det(N)$ of spinor exception lattices N for $gen(M)$ belong to finitely many square classes of k^*/k^{*2}.

In particular, spinor exception integers for a given ternary genus belong to finitely many square classes, a fact which has been known for a long time [Kne61]. For a proof in terms of the Brauer group, see the next-but-one paragraph.

Suppose N is a spinor exception for $gen(M)$. Then N is represented by $spn(M)$ if and only if the number of places v of k satisfying

$$\theta_v(X(N_v/M_v)) \neq \theta(M_v, N_v)$$

is even: this follows from Theorem 7.5(iii) and statement (iii) in the above corollary. This is the exact statement of [SX04, Proposition 7.1].

Let us discuss the finiteness of square classes associated to spinor exceptions in the case $n = 1, m = 3$. Let O be the ring of integers in a number field k, and let $f(x, y, z)$ be a quadratic form in three variables defined over O, nondegenerate over k. Let $a \in O, a \neq 0$. Let v be a finite nondyadic place such that $v(\operatorname{disc}(f))$ is even and $v(a)$ is odd. Let $\mathbf{X}_a$ be the O-scheme defined by $f(x, y, z) = a$. Let X_a/k be the affine quadric with equation $q(x, y, z) = a$. Over O_v the quadratic form f is isomorphic to the form $uv - \det(f)w^2$. In these last coordinates a generator of $\operatorname{Br} X_{k_v}/\operatorname{Br} k_v$ is given by $\alpha = (u, -a.\operatorname{disc}(f))$. There are integral O_v-points on $\mathbf{X}_a$ with $w = 0$ and $u \in O_v^*$ either a square or a nonsquare in the residue field. Thus α takes two distinct values on $\mathbf{X}_a(O_v)$. This implies that there is no Brauer–Manin obstruction.

We thus see that, if $a \in O$ is such that $f(x, y, z) = a$ has solutions in all O_v, then there may exist a Brauer–Manin obstruction to the existence of an integral point only if for each nonarchimedean nondyadic v with $v(\operatorname{disc}(f))$ even – and these are almost all places – we have $v(a)$ even. This implies that, for given f, such an a belongs to a finite number of classes in k^*/k^{*2}.

8. Representation of an integral quadratic form by another integral quadratic form: some examples from the literature

8.1 Some numerical examples from the literature

8.1.1 In Cassels' book [Cas78, p. 168], we find Example 23. Let $m \equiv \pm 3 \bmod 8$. Then m^2 is represented *primitively* by the indefinite form $x^2 - 2y^2 + 64z^2$ over every $\mathbb{Z}_p$ but not over $\mathbb{Z}$. The equation for $\mathbf{X}/\mathbb{Z}$ is the complement of $x = y = z = 0$ in the affine $\mathbb{Z}$-scheme with equation

$$x^2 - 2y^2 = (m + 8z)(m - 8z).$$

One considers the algebra $\alpha = (m+8z, 2) = (m-8z, 2)$ over $X = \mathbf{X} \times_{\mathbb{Z}} \mathbb{Q}$. Over (primitive) solutions in $\mathbf{X}(\mathbb{Z}_p)$ for p odd or infinity one checks that α vanishes whereas it never vanishes on points in $X(\mathbb{Z}_2)$. For this, one uses the obvious equalities $(m+8z)+(m-8z) = 2m$ and $(m+8z)-(m-8z) = 16z$. (Note that for primes p which do not divide m, any $\mathbb{Z}_p$-solution is primitive.)

8.1.2 In the same book [Cas78, Example 7, p. 252], we find two examples of positive definite forms and elements which are primitively represented locally but not globally. Cassels refers to papers by G. L. Watson; the hint he gives can certainly be reinterpreted in terms of the law of quadratic reciprocity.

Here is one of these examples. If m is odd and positive and $m \equiv 1 \bmod 3$ then $4m^2$ is not represented primitively by $x^2+xy+y^2+9z^2$ over $\mathbb{Z}$, although it is primitively represented over each $\mathbb{Z}_p$. We can write the equation of $X/\mathbb{Q}$ as

$$x^2+xy+y^2 = (2m+3z)(2m-3z).$$

The $\mathbb{Z}$-scheme $\mathbf{X}$ under consideration here is the complement of $x=y=z=0$ in the $\mathbb{Z}$-scheme given by the same equation. For any $\mathbb{Z}$-algebra A, the points of $\mathbf{X}(A)$ are the primitive solutions of the above equation, with coordinates in A. We consider the algebra $\alpha = (2m+3z, -3) = (2m-3z, -3)$ over X. Using $(2m+3z)+(2m-3z) = 4m$ and $(2m+3z)-(2m-3z) = 6z$, one checks that α vanishes on points of $\mathbf{X}(\mathbb{Z}_p)$ for $p \neq 2, 3, \infty$. It also vanishes on points of $\mathbf{X}(\mathbb{Z}_2)$. Indeed, $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is unramified at 2. For a point of $\mathbf{X}(\mathbb{Z}_2)$, one checks that $z \in \mathbb{Z}_2^*$. Thus $2m+3z \in \mathbb{Z}_2^*$ and $2m+3z$ is a local norm at 2 for the unramified extension $\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2$. Over $\mathbb{R}$, either $2m+3z$ or $2m-3z$ is positive, but since their product is positive both must be positive. Hence α vanishes on $X(\mathbb{R})$.

The assumption $m \equiv 1 \bmod 3$ implies $2m+3z \equiv 2 \bmod 3$. But the units in $\mathbb{Z}_3$ which are norms for the ramified extension $\mathbb{Q}_3(\sqrt{-3})/\mathbb{Q}_3$ are precisely those which are congruent to $1 \bmod 3$. Thus α never vanishes on $\mathbf{X}(\mathbb{Z}_3)$.

8.1.3 One may also give such examples with a positive definite form, excluding the existence of integral solutions – not only primitive integral solutions. Over $\mathbb{Q}(\sqrt{35})$, Schulze-Pillot in [Sch04] gives an example (Example 5.3). Let us show that this example can be accounted for by the Brauer–Manin condition.

Proposition 8.1. *Let $k = \mathbb{Q}(\sqrt{35})$. Then $7p^2$ where p is a prime with $(p/7) = 1$ is not a sum of three integral squares over the ring of integers $O = \mathbb{Z}[\sqrt{35}]$ but is a sum of three integral squares over O_v for all primes v of F.*

Proof. The tangent plane through the rational point $((7/\sqrt{35})p, (14/\sqrt{35})p, 0)$ of

$$x^2+y^2+z^2 = 7p^2$$

is given by $x+2y-\sqrt{35}p = 0$.

By § 5.8, one can consider the following quaternion algebra $(x+2y-\sqrt{35}p, -7)$ over the integral points of $x^2+y^2+z^2 = 7p^2$ at each local completion.

If v is a finite prime away from 2, 5, 7 and p, we claim that

$$\mathrm{ord}_v(x+2y-\sqrt{35}p) \equiv 0 \bmod 2 \quad \text{or } -7 \in (k_v^*)^2.$$

This implies that $\mathrm{inv}_v((x+2y-\sqrt{35}p, -7)) = 0$. Indeed, one can write

$$x+2y-\sqrt{35}p = u_v \pi_v^{n_v}$$

with $u_v \in O_v^*$ and one may assume $n_v > 0$ and $-7 \notin (k_v^*)^2$.

Suppose $(2y - \sqrt{35}p) \in O_v^*$. Then

$$z^2 + 7\left(2p - \frac{\sqrt{35}}{7}y\right)^2 = 2(2y - \sqrt{35}p)u_v\pi_v^{n_v} - u_v^2\pi_v^{2n_v}$$

by plugging x into the above quadric. Since the left hand side is a norm of the unramified extension $k_v(\sqrt{-7})/k_v$, one concludes that n_v is even.

Otherwise $2y \equiv \sqrt{35}p \bmod \pi_v$. Then $z^2 \equiv -7(p/2)^2 \bmod \pi_v$. By Hensel's lemma, $-7 \in (k_v^*)^2$ which is a contradiction. The claim follows.

If $v \mid p$, one has

$$\left(\frac{-7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}(-1)^{((p-1)/2)((7-1)/2)}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right) = 1$$

and $-7 \in (\mathbb{Q}_p^*)^2 \subset (k_v^*)^2$. Then $\mathrm{inv}_v((x + 2y - \sqrt{35}p, -7)) = 0$.

If $v \mid 2$, then $-7 \in (\mathbb{Q}_2^*)^2 \subset (k_v^*)^2$ and $\mathrm{inv}_v((x + 2y - \sqrt{35}p, -7)) = 0$.

If $v \mid 5$ and $x + 2y - \sqrt{35}p \equiv 0 \bmod \pi_v$, then

$$7p^2 = x^2 + y^2 + z^2 \equiv 2^2y^2 + y^2 + z^2 \equiv z^2 \bmod \pi_v.$$

Since 5 is ramified in $k/\mathbb{Q}$, the above equation implies that 7 is a square modulo 5, which is a contradiction. Therefore $x + 2y - \sqrt{35}p$ is a unit and $\mathrm{inv}_v((x + 2y - \sqrt{35}p, -7)) = 0$.

Since $-7 = (\sqrt{35}/5)^2(-5)$ and $(-5/7) = 1$, if $v \mid 7$, then one has $-7 \in (k_v^*)^2$ and one has $\mathrm{inv}_v((x + 2y - \sqrt{35}p, -7)) = 0$.

The algebra is $(x + 2y - \sqrt{35}p, -7)$ at one real place ∞_1 and $(x + 2y + \sqrt{35}p, -7)$ at the other real place ∞_2. Since $x + 2y - \sqrt{35} \leq 0$ and $x + 2y + \sqrt{35} \geq 0$ for $x^2 + y^2 + z^2 = 7p$ over $\mathbb{R}$, one has

$$\mathrm{inv}_{\infty_1}((x + 2y - \sqrt{35}p, -7)) = \tfrac{1}{2} \quad \text{and} \quad \mathrm{inv}_{\infty_2}((x + 2y + \sqrt{35}p, -7)) = 0.$$

Therefore

$$\left(\prod_v \mathbf{X}(O_v)\right)^{\mathrm{Br}\,X} = \emptyset$$

hence there are no integral points. □

8.1.4 We leave it to the reader to handle the following example with $(n, m) = (1, 3)$ (see [Bor01, BR95]):

$$-9x^2 + 2xy + 7y^2 + 2z^2 = 1.$$

More generally, one may give a criterion for an integer to be represented by the indefinite form $-9x^2 + 2xy + 7y^2 + 2z^2$ (see [Xu05, 6.4]). As an exercise, the reader should recover the results of [Xu05] from the present point of view and give a criterion for primitive representation of integers by the above form.

8.1.5 Here is an example with $(n, m) = (2, 4)$ which goes back to Siegel. This is Example 5.7 in [Xu05, p. 50]. Over $\mathbb{Z}$, the form $g(x, y) = x^2 + 32y^2$ is not represented by the form $f(x, y, z, t) = x^2 + 128y^2 + 128yz + 544z^2 - 64t^2$, even though it is represented over each $\mathbb{Z}_p$ and $\mathbb{R}$.

Let us explain how this example can be explained from the present point of view. Let $B(u,v)$ denote the bilinear form with coefficients in $\mathbb{Z}$ such that $B(u,u)=f(u)$. Let $\mathbf{X}/\mathbb{Z}$ be the closed $\mathbb{Z}$-scheme of $\mathbb{A}^8_{\mathbb{Z}}$ given by the identity

$$g(x,y)=f(l_1(x,y),\dots,l_4(x,y)).$$

Let $X=\mathbf{X}\times_{\mathbb{Z}}\mathbb{Q}$. For any commutative ring A a point of $\mathbf{X}(A)$ is given by a pair of vectors $u_1,u_2\in A^4$ with

$$B(u_1,u_1)=1,\quad B(u_1,u_2)=0,\quad B(u_2,u_2)=32.$$

The standard basis for A^4 will be denoted e_1,e_2,e_3,e_4. The discriminant of g is 2^5, and the discriminant of f is -2^{22}. In the notation of the previous section, we may take $d=2$, $K=\mathbb{Q}(\sqrt{2})$. On X we find the $\mathbb{Q}$-point M given by the pair

$$v_1=(1,0,0,0)=e_1,\quad v_2=(0,\tfrac{1}{5},\tfrac{1}{5},0)=\tfrac{1}{5}(e_2+e_3).$$

We also have the $\mathbb{Q}$-point given by the pair

$$(1,0,0,0);\quad (0,\tfrac{1}{2},0,0).$$

This ensures $\mathbf{X}(\mathbb{Z}_p)\neq\emptyset$ for all p.

The $\mathbb{Q}$-point M gives rise to a morphism $SO(f)\to X$ over $\mathbb{Q}$ and for each field extension $F/\mathbf{Q}$ to a map $X(F)\to F^*/N((FK)^*)$, hence for each prime p to a map

$$\theta_p:\mathbf{X}(\mathbb{Z}_p)\to\mathbb{Q}_p^*/NK_p^*.$$

Each of these maps is computed in the following fashion: given a point of $\mathbf{X}(\mathbb{Z}_p)$ represented by a pair of vectors $w_1,w_2\in(\mathbb{Z}_p)^4$, one picks up $\sigma\in SO(f)(\mathbb{Q}_p)$ such that simultaneously $\sigma v_1=w_1$ and $\sigma v_2=w_2$. One then computes the spinor class of σ, which is an element in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ and one takes its image in $\mathbb{Q}_p^*/NK_p^*$.

Assertion. For each prime $p\neq 5$ the image of θ_p is reduced to $1\in\mathbb{Q}_p^*/NK_p^*$. For $p=5$ the image of θ_5 is reduced to the nontrivial class $5\in\mathbb{Q}_5^*/NK_5^*$.

The reciprocity law then implies that there is no point in $\mathbf{X}(\mathbb{Z})$: the form f does not represent g over $\mathbb{Z}$.

Let us prove the assertion. The system $\mathbf{X},M$ has good reduction away from $S=\{2,5,\infty\}$. We also have $\mathbb{R}^*/N_{K/\mathbb{Q}}K_\infty^*=1$. To prove the assertion we could restrict ourselves to considering the primes $p=2$ and $p=5$ but as we shall see the recipe we apply easily yields the triviality of all maps θ_p for $p\neq 2,5$.

In § 5.7 we gave a recipe for writing the rotation σ as an even product of reflections, so as to be able to compute the spinor norm of σ. This recipe works provided the pair $\{w_1,w_2\}$ lies in a certain Zariski open set. Typically one wants some $f(x-\sigma x)$ to be nonzero in order to use the reflection with respect to $x-\sigma x$. There are however many ways to write a rotation as a product of reflections. We shall use the basic equality

$$f(x+\sigma x)+f(x-\sigma x)=4f(x).$$

This equality ensures that if $f(x)\neq 0$ then one of $f(x+\sigma x)$ or $f(x-\sigma x)$ is nonzero. For $x\in\mathbb{Z}_p^4$ with $p\neq 2$ and $f(x)\in\mathbb{Z}_p^*$ it ensures that at least one of $f(x+\sigma x)$ or $f(x-\sigma x)$ is in $\mathbb{Z}_p^*$.

With notation as in § 5.7 whenever the appropriate reflections are defined we have for each of $i=1,2$ the equalities

$$\tau_{\sigma v_1 - v_1}\tau_{[\tau_{\sigma v_1 - v_1}\sigma v_2 - v_2]} v_i = \sigma v_i,$$
$$\tau_{\sigma v_1 + v_1}\tau_{v_1}\tau_{[\tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma v_2 - v_2]} v_i = \sigma v_i,$$
$$\tau_{\sigma v_1 - v_1}\tau_{[\tau_{\sigma v_1 - v_1}\sigma v_2 + v_2]}\tau_{v_2} v_i = \sigma v_i,$$
$$\tau_{\sigma v_1 + v_1}\tau_{v_1}\tau_{[\tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma v_2 + v_2]}\tau_{v_2} v_i = \sigma v_i.$$

(To check these formulas, use the property $\tau_{x-y}(y) = x$ is $f(x) = f(y)$.)

Note that the form f represents 1. Thus for any point $P \in X(F)$ with lift $\sigma \in SO(f)(F)$ the image of P in $F^*/N(FK)^*$ is the class of any nonzero element among

$$h_1 = f(\sigma v_1 - v_1) f(\tau_{\sigma v_1 - v_1}\sigma v_2 - v_2),$$
$$h_2 = f(\sigma v_1 + v_1) f(v_1) f(\tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma v_2 - v_2),$$
$$h_3 = f(\sigma v_1 - v_1) f(\tau_{\sigma v_1 - v_1}\sigma v_2 + v_2) f(v_2),$$
$$h_4 = f(\sigma v_1 + v_1) f(v_1) f(\tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma v_2 + v_2) f(v_2).$$

The extension $K = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is ramified only at 2.

Suppose $p \neq 2$ and $p \neq 5$. Then $f(v_1)$ is in $\mathbb{Z}_p^*$. This implies that at least one of $f(\sigma v_1 - v_1)$ or $f(\sigma v_1 + v_1)$ is in $\mathbb{Z}_p^*$. Since $f(v_2)$ is in $\mathbb{Z}_p^*$ for $p \neq 2$ and 5, one has that at least one of $f(\tau_{\sigma v_1 - v_1}\sigma v_2 - v_2)$ or $f(\tau_{\sigma v_1 - v_1}\sigma v_2 + v_2)$ is in $\mathbb{Z}_p^*$, and one of $f(\tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma v_2 - v_2)$ or $f(\tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma v_2 + v_2)$ is in $\mathbb{Z}_p^*$. This combination implies that at least one of h_i for $1 \leq i \leq 4$ is in $\mathbb{Z}_p^*$, hence has trivial image in $\mathbb{Q}_p^*/NK_p^*$. This proves the assertion for such p.

Consider the case $p = 5$. Let $\{w_1, w_2\} \in \mathbf{X}(\mathbb{Z}_5)$. Thus w_1, w_2 are in $\mathbb{Z}_5 e_1 + \mathbb{Z}_5 e_2 + \mathbb{Z}_5 e_3 + \mathbb{Z}_5 e_4$ and there exists $\sigma \in SO(f)(\mathbb{Q}_5)$ such that $\sigma v_1 = w_1$ and $\sigma v_2 = w_2$. Since $f(v_1) = 1$ from the basic equality we deduce that at least one of $f(\sigma v_1 - v_1)$ and $f(\sigma v_1 + v_1)$ belongs to $\mathbb{Z}_5^*$. Let

$$\varrho = \begin{cases} \tau_{\sigma v_1 - v_1}\sigma & \text{if } f(\sigma v_1 - v_1) \in \mathbb{Z}_5^*, \\ \tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma & \text{otherwise.} \end{cases}$$

Then $\varrho v_1 = v_1$. As for ϱv_2, it is integral and orthogonal to ϱv_1 hence it belongs to the group $\mathbb{Z}_5 e_2 + \mathbb{Z}_5 e_3 + \mathbb{Z}_5 e_4$.

There exists $\varepsilon \in (\mathbb{Z}_5)^4$ with $\mathbb{Z}_5 e_2 + \mathbb{Z}_5 e_3 = \mathbb{Z}_5(e_2 + e_3) + \mathbb{Z}_5 \varepsilon$ such that $f(\varepsilon) = 0$ and moreover $B(\varepsilon, e_2 + e_3) = 1$. Write $\varrho v_2 = a(e_2 + e_3) + b\varepsilon + c e_4$ with a, b and $c \in \mathbb{Z}_5$. Then $a, b \in \mathbb{Z}_5^*$. Otherwise one would have $32 = f(\varrho v_2) \equiv -64c^2 \bmod 5$, but 2 is not a square modulo 5. Immediate computation now yields $B(\varrho v_2, v_2) \in 5^{-1}\mathbb{Z}_5^*$. This implies h_1 or $h_2 \in 5^{-1}\mathbb{Z}_5^*$. Since $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ is an unramified quadratic field extension, this proves the assertion for $p = 5$.

Let $p = 2$ and $\{w_1, w_2\} \in \mathbf{X}(\mathbb{Z}_2)$. Thus w_1, w_2 belong to $\mathbb{Z}_2 e_1 + \mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$ and there exists $\sigma \in SO(f)(\mathbb{Q}_2)$ such that $\sigma v_1 = w_1$ and $\sigma v_2 = w_2$.

Write $\sigma v_1 = \alpha v_1 + w$ with $\alpha \in \mathbb{Z}_2$ and $w \in \mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$. Then $1 - \alpha^2 = f(w) \in 2^5\mathbb{Z}_2$. Therefore $\min\{\operatorname{ord}(1-\alpha), \operatorname{ord}(1+\alpha)\} = 1$ and $\operatorname{ord}(1-\alpha) + \operatorname{ord}(1+\alpha) \geq 5$. We have

$$f(\sigma v_1 + v_1) = f((1+\alpha)v_1 + w) = (1+\alpha)^2 + f(w) = (1+\alpha)^2 + (1-\alpha^2) = 2(1+\alpha),$$
$$f(\sigma v_1 - v_1) = f((\alpha-1)v_1 + w) = (\alpha-1)^2 + f(w) = (1-\alpha)^2 + (1-\alpha^2) = 2(1-\alpha).$$

We have $1 \pm \alpha = 2 - (1 \mp \alpha) = 2(1 - 2^{-1}(1 \mp \alpha))$. If $\operatorname{ord}(1+\alpha) \geq 4$ (first case) then $1 - \alpha \in 2(\mathbb{Z}_2^*)^2$, hence $f(\sigma v_1 - v_1) \in 4(\mathbb{Z}_2^*)^2$. If $\operatorname{ord}(1-\alpha) \geq 4$ (second case) then $1 + \alpha \in 2(\mathbb{Z}_2^*)^2$, hence $f(\sigma v_1 + v_1) \in 4(\mathbb{Z}_2^*)^2$.

In the first case set $\varrho = \tau_{\sigma v_1 - v_1}\sigma$. We have $\varrho v_1 = v_1$. The element $\sigma v_1 - v_1$ belongs to $2\mathbb{Z}_2 e_1 + \mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$. This implies that ϱv_2 belongs to $\mathbb{Z}_2 e_1 + \mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$. It actually lies in $\mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$, because ϱv_2 is orthogonal to $\varrho v_1 = v_1$.

In the second case set $\varrho = \tau_{v_1}\tau_{\sigma v_1 + v_1}\sigma$. We have $\varrho v_1 = v_1$. The element $\sigma v_1 + v_1$ belongs to $2\mathbb{Z}_2 e_1 + \mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$. This implies that ϱv_2 belongs to $\mathbb{Z}_2 e_1 + \mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$. It actually lies in $\mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 + \mathbb{Z}_2 e_4$, because ϱv_2 is orthogonal to $\varrho v_1 = v_1$.

In the first case we have $h_1 = f(\sigma v_1 - v_1) f(\varrho v_2 - v_2)$ and $h_3 = f(\sigma v_1 - v_1) f(\varrho v_2 + v_2) f(v_2)$. In the second case we have $h_2 = f(\sigma v_1 + v_1) f(\varrho v_2 - v_2)$ and $h_4 = f(\sigma v_1 + v_1) f(\varrho v_2 + v_2) f(v_2)$.

There exists ε such that $\mathbb{Z}_2 e_2 + \mathbb{Z}_2 e_3 = \mathbb{Z}_2 v_2 \perp \mathbb{Z}_2 \varepsilon$ with $f(\varepsilon) = 2^{11}$. Write $\varrho v_2 = a v_2 + b\varepsilon + c e_4$ with a, b and $c \in \mathbb{Z}_2$. We have $2^5 = f(v_2) = f(\varrho v_2) = 2^5 a^2 + 2^{11} b^2 - 2^6 c^2$. From this we deduce that $a \in \mathbb{Z}_2^*$ and $\mathrm{ord}(c) \geq 1$. Set $c = 2d$ with $d \in \mathbb{Z}_2$. From $a \in \mathbb{Z}_2^*$ we deduce that $\min\{\mathrm{ord}(1+a), \mathrm{ord}(1-a)\} = 1$ and $\mathrm{ord}(1+a) + \mathrm{ord}(1-a) \geq 3$. We have

$$f(\varrho v_2 - v_2) = 2^5 (a-1)^2 + 2^{11} b^2 - 2^8 d^2 \quad \text{and} \quad f(\varrho v_2 + v_2) = 2^5 (a+1)^2 + 2^{11} b^2 - 2^8 d^2.$$

Suppose $\mathrm{ord}(1-a) = 1$. Then $f(\varrho v_2 - v_2) \neq 0$ is a norm for the extension $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$. If we are in the first case we find that $h_1 = f(\sigma v_1 - v_1) f(\varrho v_2 - v_2)$ is a norm. If we are in the second case we find that $h_2 = f(\sigma v_1 + v_1) f(\varrho v_2 - v_2)$ is a norm.

Suppose $\mathrm{ord}(1+a) = 1$. Then $f(\varrho v_2 + v_2) \neq 0$ is a norm for the extension $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$. If we are in the first case we find that $h_3 = f(\sigma v_1 - v_1) f(\varrho v_2 + v_2) f(v_2)$ is a norm (recall $f(v_2) = 2^5$). If we are in the second case we find that $h_4 = f(\sigma v_1 + v_1) f(\varrho v_2 + v_2)$ is a norm.

This completes the proof of the assertion.

8.1.6 Starting from the previous example one immediately gets an example with $(n, m) = (2, 3)$. Indeed the form $x^2 + 32y^2$ is represented by the form $x^2 + 128y^2 + 128yz + 544z^2$ over each $\mathbb{Z}_p$ and it certainly is not represented by this form over $\mathbb{Z}$ since it is not represented by the form $x^2 + 128y^2 + 128yz + 544z^2 - 64t^2$.

We leave it to the reader to analyze [CX04, Example 2.9]: the form $5x^2 + 16y^2$ is represented by $4x^2 + 45y^2 - 10yz + 45z^2$ over each $\mathbb{Z}_p$ but not over $\mathbb{Z}$.

8.2 Representation of an integer by a three-dimensional form: a two-parameter family

In [SX04, p. 324, Example 1.2] we find the following result.

Proposition 8.2. *Let $n, m, k \geq 1$ be positive integers. The diophantine equation*

$$m^2 x^2 + n^{2k} y^2 - n z^2 = 1$$

is solvable over each $\mathbb{Z}_p$ and $\mathbb{R}$ except if $(n, m) \neq 1$. It is solvable over $\mathbb{Z}$ except in the following cases:

(i) $(n, m) \neq 1$;

(ii) $n \equiv 5 \bmod 8$ *and* 2 *divides* m;

(iii) $n \equiv 3 \bmod 8$ *and* 4 *divides* m.

Let us prove this result with the method of the present paper.

Proof. Let us denote by $\mathbf{X}$ the affine scheme over $\mathbb{Z}$ defined by $m^2 x^2 + n^{2k} y^2 - n z^2 = 1$ and by X the $\mathbb{Q}$-scheme $\mathbf{X} \times_{\mathbb{Z}} \mathbb{Q}$.

Let us first discuss the existence of local solutions. If $(n, m) \neq 1$ then there is a prime p such that $\mathbf{X}(\mathbb{Z}_p) = \emptyset$. We now assume $(n, m) = 1$. Over $\mathbb{Q}$, we have the point $(x, y, z) = (1/m, 0, 0)$ and the point $(x, y, z) = (0, 1/n^k, 0)$. For each prime p, at least one of these two points lies in $\mathbf{X}(\mathbb{Z}_p)$. Both lie in $X(\mathbb{R})$.

One has the equation

$$(1 + n^k y)(1 - n^k y) = m^2x^2 - nz^2, \tag{E1}$$

and the second equation

$$(1 + n^k y) + (1 - n^k y) = 2. \tag{E2}$$

One introduces $\alpha = (1 + n^k y, n)$ (note that $1 + n^k y = 0$ is the tangent plane to the quadric X at the obvious rational point $(0, -1/n^k, 0)$). As explained above, α belongs to $\mathrm{Br}_1\, X$ and induces the nontrivial element in $\mathrm{Br}_1\, X/\mathrm{Br}(\mathbb{Q})$. Let us restrict attention to the open set $U \subset X$ defined by

$$(1 + n^k y)(1 - n^k y) = m^2x^2 - nz^2 \neq 0. \tag{E3}$$

First note that over any field F containing $\mathbb{Q}$ and any point $(x, y, z) \in U(F)$, the equation (E3) implies

$$(1 + n^k y, n) = (1 - n^k y, n) \in \mathrm{Br}(F). \tag{E4}$$

Claim: for any prime $p \neq 2$, α vanishes on $\mathbf{X}(\mathbb{Z}_p)$. Let $(x, y, z) \in \mathbf{X}(\mathbb{Z}_p) \cap U(\mathbb{Q}_p)$. If p divides n, then $1 + n^k y$ is a square in $\mathbb{Z}_p$, hence α vanishes. Suppose that p does not divide n. If n is a square mod p there is nothing to prove. Suppose n is not a square mod p. If $v_p(1 + n^k y) = 0$ then each entry in $(1 + n^k y, n)_p \in \mathrm{Br}(\mathbb{Q}_p)$ is a unit, hence $(1 + n^k y, n)_p = 0$. Suppose $v_p(1 + n^k y) > 0$. Then from (E2) we get $v_p(1 - n^k y) = 0$, hence $(1 - n^k y, n)_p = 0$, which using (E4) shows $(1 + n^k y, n)_p = 0$.

From $n > 0$ we see that α vanishes on $X(\mathbb{R})$.

It remains to discuss the value of α on $\mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$.

By Theorem 6.3 together with § 5.8, there is an integral solution, i.e. a point in $\mathbf{X}(\mathbb{Z})$, if and only if there exists a point of $\mathbf{X}(\mathbb{Z}_2)$ on which α vanishes.

If m is odd, then the point M with coordinates $(x, y, z) = (1/m, 0, 0)$ belongs to the set $\mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$, and $\alpha(M) = (1, n)_2 = 0 \in \mathrm{Br}(\mathbb{Q}_2)$.

Assume now m even, hence n odd.

If $n \equiv 1 \bmod 8$ then n is a square in $\mathbb{Z}_2$, hence $(1 + n^k y, n)_2 = 0$ for any point of the set $X(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$.

If $n \equiv -1 \bmod 8$ then there exists a point $M \in \mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$ with coordinates $(x, y) = (0, 0)$, hence $\alpha(M) = (1, n)_2 = 0$.

Let us consider the remaining cases, i.e. m even and $n \equiv \pm 3 \bmod 8$.

Let us recall the following values of the Hilbert symbol at the prime 2. We have $(r, 5)_2 = 0$ if r is an odd integer and $(2, 5)_2 = 1 \in \mathbb{Z}/2$. We have $(3, 3)_2 = (3, 7)_2 = 1 \in \mathbb{Z}/2$ and $(2, 3)_2 = 1 \in \mathbb{Z}/2$.

Assume that $n \equiv 3 \bmod 8$ and $m = 2m_0$ with m_0 odd. The equation $1 - 4m_0^2 = -nz^2$ has a solution with $z \in \mathbb{Z}_2$. The point M with coordinates $(x, y, z) = (1, 0, z)$ belongs to the set $\mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$, and $\alpha(M) = (1, n)_2 = 0$.

Assume that $n \equiv 3 \bmod 8$ and 4 divides m. Let $M = (x, y, z)$ be a point of the set $\mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$. We have $1 - y^2 \equiv -3z^2 \bmod 8$. If $v_2(y) > 0$ then $z \in \mathbb{Z}_2^*$ and the last equality implies $1 - y^2 \equiv -3 \bmod 8$, hence $y = 2y_0$ with $y_0 \in \mathbb{Z}_2^*$. Thus $1 + n^k y \equiv 3$ or $7 \bmod 8$. This implies $(1 + n^k y, n)_2 = (3, 3)_2$ or $(7, 3)_2 = 1 \in \mathbb{Z}/2$. Assume $y \in \mathbb{Z}_2^*$. Then (E1) implies

$0 \equiv -3z^2 \bmod 8$. Hence 4 divides z. Hence $1 - n^{2k}y^2 \equiv 0 \bmod 16$. This implies $n^k y \equiv \pm 1 \bmod 8$. Thus either $1 + n^k y \equiv 2 \bmod 8$ which implies $(1 + n^k y, n)_2 = 1 \in \mathbb{Z}/2$ or $1 - n^k y \equiv 2 \bmod 8$ which implies $(1 - n^k y, n)_2 = 1 \in \mathbb{Z}/2$, hence using (E4) $(1 + n^k y, n)_2 = 1 \in \mathbb{Z}/2$. That is, α is never zero on $\mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$.

Assume that $n \equiv 5 \bmod 8$ and 2 divides m. Let $M = (x, y, z)$ be a point of $\mathbf{X}(\mathbb{Z}_2) \cap U(\mathbb{Q}_2)$. We have $1 - y^2 \equiv 3z^2 \bmod 4$. This implies $y \in \mathbb{Z}_2^*$ and $v_2(z) > 0$ even. Each of $1 + n^k y$ and $1 - n^k y$ has positive 2-adic valuation. Since their sum is 2, one of them is of the shape $2r$ with $r \in \mathbb{Z}_2^*$. Now $(r, 5)_2 = 0$ for $r \in \mathbb{Z}_2^*$, so $(2r, 5)_2 = (2, 5)_2 = 1 \in \mathbb{Z}/2$. Thus at least one of $(1 + n^k y, n)_2$ or $(1 - n^k y, n)_2$ is nonzero, hence both are nonzero. □

8.3 Quadratic diophantine equations

In this section we illustrate how our insistence on arbitrary integral models, as opposed to the classical ones, immediately leads to results which in the classical literature would have required some work.

Theorem 8.3. *Let k be a number field, O its ring of integers, $f(x_1, \ldots, x_n)$ a polynomial of total degree 2 and $l(x_1, \ldots, x_n)$ a polynomial of total degree 1 which does not divide f.*

Let $\mathbf{X}/O$ be the affine closed O-subscheme of $\mathbb{A}^n_O$ defined by

$$f(x_1, \ldots, x_n) = 0, \quad l(x_1, \ldots, x_n) = 0.$$

Assume that $X = \mathbf{X} \times_O k$ is smooth. Let v_0 be a place of k such that $X(k_{v_0})$ is noncompact. Let $O_{\{v_0\}}$ be the ring of integers away from v_0.

(i) *If $n \geq 5$, i.e. the dimension of X is at least 3, then $\mathbf{X}(O_{\{v_0\}})$ is dense in $\prod_{v \neq v_0} \mathbf{X}(O_v)$.*

(ii) *If $n = 4$, i.e. the dimension of X is 2, and if $\{M_v\} \in \prod_v \mathbf{X}(O_v)$ is orthogonal to the group $\mathrm{Br}\, X/\mathrm{Br}\, k \subset \mathbb{Z}/2$, then $\{M_v\} \in \prod_{v \neq v_0} \mathbf{X}(O_v)$ may be approximated arbitrarily closely by an element of $\mathbf{X}(O_{\{v_0\}})$.*

Proof. The hypothesis on X guarantees that X is k-isomorphic to a smooth affine quadric of dimension $n - 2$. Such a quadric is of the shape G/H for G a spinor group attached to a quadratic form of rank $n - 1$ and $H \subset G$ a spinor group if $n \geq 5$, a torus if $n = 4$ (see §§ 5.3 and 5.6). The result is a special case of Theorem 3.7 (see also Theorem 6.1 if $n \geq 5$ and Theorem 6.3 if $n = 4$). □

Remark 8.4. One may write a more general statement, where one gives oneself a finite set of places containing v_0 and one approximates elements in $\prod_{v \in S \setminus v_0} X(k_v) \times \prod_{v \notin S} \mathbf{X}(O_v)$ by points in $\mathbf{X}(O_S)$.

Remark 8.5. Watson proved a result [Wat61, Theorem 2] closely related to the case $n \geq 5$ of the above theorem. It would be interesting to revisit his paper [Wat67].

9. Sums of three squares in an imaginary quadratic field

Let $k = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. We may and will assume that d is a negative squarefree integer. Let O denote the ring of integers of k. In this section we give a proof based on Theorem 6.3 of the following theorem due to Ji, Wang and Xu [JWX06].

Theorem 9.1. *Suppose $a \in O$ can be expressed as a sum of three integral squares at each local completion O_v. If a is not a sum of three integral squares in O, then all the following conditions are fulfilled:*

(i) $d \not\equiv 1 \bmod 8$;

(ii) *there is a squarefree positive integer* d_0 *such that* $a = d_0\alpha^2$ *for some* $\alpha \in k$*; such a* d_0 *is then uniquely determined;*

(iii) $d = d_0.d_1$ *with* $d_1 \in \mathbb{Z}$;

(iv) $d_0 \equiv 7$ *mod* 8;

(v) *for any odd prime* p *which divides* $N_{F/\mathbb{Q}}(a)$*, at least one of* $(-d_0/p), (-d_1/p)$ *is equal to 1.*

If conditions (i) to (v) are fulfilled, then a *is not a sum of three squares in* O*.*

Remark 9.2. (1) For v nondyadic, -1 is a sum of two squares in O_v, hence any element in O_v is a sum of three squares (use the formula $x = ((x+1)/2)^2 - ((x-1)/2)^2$). The local condition on a in the theorem only has to be checked for the dyadic valuations.

(2) Let us explain the comment on uniqueness of the positive squarefree d_0 in (ii). Let $a = d_0'.\beta^2$ be another representation. Then $d_0/d_0' = (n + m\sqrt{d})^2$ with $n, m \in \mathbb{Q}$, which implies $d_0/d_0' = n^2$ or $d_0/d_0' = m^2.d$. From $d < 0$ we conclude that we are in the first case and then $d_0 = d_0'$.

(3) An easy application of Hilbert's theorem 90 implies that (ii) holds if and only if $N_{k/Q}(a) = r^2$ for some integer $r \in \mathbb{Z}$.

(4) There is a big difference with the family of examples discussed in Proposition 8.2. Given an integer $a \in k$ which is a good candidate, there is in general no obvious rational point on $a = x^2 + y^2 + z^2$ – unless d is such that -1 is an explicit sum of two squares in k.

(5) Earlier results on the representation of an integer in a quadratic imaginary field as a sum of three squares are due to Estes and Hsia [EH83].

Before we begin the proof let us fix some notation and recall facts from § 5.8.

Let k be a field of characteristic not 2, let (V, Q) be a three-dimensional quadratic space over k which in a given basis $V \simeq k^3$ associates $Q(v) = f(x, y, z)$ to $v = (x, y, z)$. Let $B(v, w) = \frac{1}{2}(Q(v+w) - Q(v) - Q(w))$ be the associated bilinear form. Let $a \in k^*$. We let $X \subset \mathbb{A}^3_k$ be the smooth affine quadric defined by the equation $Q(v) - a = 0$. We let $Y \subset \mathbb{P}^3_k$ be the smooth projective quadric given by the homogeneous equation $Q(v) - at^2 = 0$. Suppose $-a$ is not a square in k. Then according to § 5.8 we have $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbb{Z}/2$. Let $M \in X(k)$, which we may view as an element $v_0 \in V$. The trace on X of the tangent plane to Y at M is given by $B(v_0, v) - a = 0$. Let $U_M \subset X \subset V$ be the complement in X of that plane.

By § 5.8 the class of the quaternion algebra

$$A = (B(v_0, v) - a, -a.\, \mathrm{disc}(f)) \in \mathrm{Br}\, U_M$$

is the restriction to the open set U_M of an element α of $\mathrm{Br}\, X$ which generates $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbb{Z}/2$.

For $X(k) \neq \emptyset$ that very statement implies that, for F any field extension of k such that $-a \notin F^{*2}$, the restriction map $\mathbb{Z}/2 = \mathrm{Br}\, X/\mathrm{Br}\, k \to \mathrm{Br}\, X_F/\mathrm{Br}\, F = \mathbb{Z}/2$ is an isomorphism.

If we start from a point $M \in Y(k) \setminus X(k)$, which may be given by an element $v_0 \in V \setminus 0$ with $Q(v_0) = 0$, the same construction yields the algebra

$$A = (B(v_0, v), -a.\, \mathrm{disc}(f)) \in \mathrm{Br}\, U_M.$$

Proof. We thus assume that $a \in O$ is a sum of three squares in each O_v.

If $-a$ is a square in k then according to Theorem 6.3 a is a sum of three squares in O. If $-a$ is a square in k and (ii) holds then $-d_0$ is a square in $k = \mathbb{Q}(\sqrt{d})$ hence $-d_0 = d$. Then (i) and (iv) may not simultaneously hold.

To prove the theorem it is thus enough to restrict to the case where $-a$ is not a square in k. In that case $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbb{Z}/2$. Let $A \in \mathrm{Br}\, X$ be a 2-torsion element which spans $\mathrm{Br}\, X/\mathrm{Br}\, k$. By Theorem 6.3 we know that $\mathbf{X}(O) \neq \emptyset$ if and only if there exists a family $\{M_v\} \in \prod \mathbf{X}(O_v)$ such that

$$\sum_v \mathrm{inv}_v(A(M_v)) = 0 \in \mathbb{Z}/2.$$

For this to happen, it suffices that for some place v the map $\mathbf{X}(O_v) \to \mathbb{Z}/2$ given by evaluation of A is onto.

In the next three lemmas we discuss purely local situations.

If $O \subset k$ is a discrete valuation ring with field of fractions k, we shall write $L = L_O \subset V$ for the trace of $O^3 \subset k^3 \simeq V$.

LEMMA 9.3. *Let k be a nonarchimedean, nondyadic local field, O its ring of integers, $a \in O^*$. Let $\mathbf{X} \subset \mathbb{A}^3_O$ be the O-scheme with affine equation $x^2 + y^2 + z^2 = a$ and let $X = \mathbf{X} \times_O k$. Then $\mathbf{X}(O) \neq \emptyset$. For any element $A \in \mathrm{Br}\, X$, the image of the map $\mathbf{X}(O) \to \mathbb{Q}/\mathbb{Z}$ given by $P \mapsto \mathrm{inv}(A(P))$ is reduced to one element.*

Proof. The quadratic form $x^2 + y^2 + z^2$ is O-isomorphic to the quadratic form $2uv - w^2$, and the scheme $\mathbf{X} \subset \mathbb{A}^3_O$ is given by the equation $2uv - w^2 = a$. In particular $\mathbf{X}(O) \neq \emptyset$. Its natural compactification is the smooth O-quadric $\mathbf{Y} \subset \mathbb{P}^3_O$ given by the homogeneous equation $2uv - w^2 = at^2$.

If $-a$ is a square, then $\mathrm{Br}\, X/\mathrm{Br}\, k = 0$ and the result is obvious. Assume $-a$ is not a square. The point $(u, v, w, t) = (0, 1, 0, 0)$ is a point of $Y(k)$. Its tangent plane is given by $u = 0$. Thus there exists an element of order 2 in $\mathrm{Br}\, X$ whose restriction to the open set $u \neq 0$ of $X \subset \mathbb{A}^3_k$ is given by the quaternion algebra $(u, -a)$, and which spans $\mathrm{Br}\, X/\mathrm{Br}\, k$. Given any point $(\alpha, \beta, \gamma) \in \mathbf{X}(O)$, from $2\alpha\beta - \gamma^2 = a$ we deduce that α and β are in O^*. Thus α is a norm for the unramified extension $k(\sqrt{-a})/k$ and $\mathrm{inv}(\alpha, -a) = 0 \in \mathbb{Z}/2$. □

LEMMA 9.4. *Let k be a nonarchimedean, nondyadic local field, O its ring of integers, $a \in O$. Let $\mathbf{X} \subset \mathbb{A}^3_O$ be the O-scheme with affine equation $x^2 + y^2 + z^2 = a$ and let $X = \mathbf{X} \times_O k$. Then $\mathbf{X}(O) \neq \emptyset$. Assume $-a$ is not a square in k and $v(a) > 0$. Then $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbb{Z}/2$ and there exists an element A of order 2 in $\mathrm{Br}\, X$ which spans $\mathrm{Br}\, X/\mathrm{Br}\, k$. For any such element the image of the map $\mathbf{X}(O) \to \mathbb{Z}/2$ given by $P \mapsto \mathrm{inv}(A(P)) \in \mathbb{Z}/2$ is the whole group $\mathbb{Z}/2$.*

Proof. Since the local field k is not dyadic, the quadratic form $x^2 + y^2 + z^2$ is O-isomorphic to the quadratic form $2xy - z^2$, and $\mathbf{X} \subset \mathbb{A}^3_O$ is given by the equation $2xy - z^2 = a$ which we now only consider. We clearly have $\mathbf{X}(O) \neq \emptyset$.

The assumption $-a$ is not a square yields $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbb{Z}/2$ as recalled above, that group being generated by the class of an algebra A whose restriction to a suitable open set is given by a quaternion algebra A computed from the equation of the tangent plane at a k-point.

Let ν denote the valuation of k. If $\nu(a)$ is odd, let us set $v_0 = (\frac{1}{2}a, 1, 0) \in \mathbf{X}(O) \subset X(k)$. For given $\epsilon \in O^*$ set $v = v(\epsilon) = (\epsilon, \frac{1}{2}a\epsilon^{-1}, 0) \in \mathbf{X}(O)$. Since $B(v_0, v) - a = \epsilon + \frac{1}{4}\epsilon^{-1}a^2 - a = \epsilon\eta^2$ for some $\eta \in O^*$ by Hensel's lemma, one has

$$\mathrm{inv}(B(v_0, v) - a, -a) = \mathrm{inv}(\epsilon, -a) \in \mathbb{Z}/2.$$

This is equal to 0 if ϵ is a square and to 1 otherwise.

Fix π a uniformizing parameter for O. If $\nu(a) > 1$ is even, and $-a \notin k^{*2}$, set $v_0 = ((\pi/2)a, \pi^{-1}, 0) \in X(k)$. Let $v_1 = (1, a/2, 0) \in \mathbf{X}(O)$ and $v_2 = (\pi, (a/2\pi), 0) \in \mathbf{X}(O)$. Then $B(v_0, v_1) = \pi^{-1} + (a^2/4)\pi$ and $B(v_0, v_2) = 1 + (a^2/4)$. Thus

$$\mathrm{inv}(B(v_0, v_1) - a, -a) = \mathrm{inv}(\pi^{-1}, -a) = 1 \in \mathbb{Z}/2$$

and

$$\mathrm{inv}(B(v_0, v_2) - a, -a) = \mathrm{inv}(1, -a) = 0 \in \mathbb{Z}/2.$$

Lemma 9.5. *Let k be a finite extension of $\mathbb{Q}_2$ and O its ring of integers. Let $a \in O$. Let $\mathbf{X} \subset \mathbb{A}^3_O$ be the O-scheme with affine equation $x^2 + y^2 + z^2 = a$ and let $X = \mathbf{X} \times_O k$. Assume $\mathbf{X}(O) \neq \emptyset$, i.e. a is a sum of three squares in O. Assume $-a$ is not a square in k. Then* $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbb{Z}/2$ *and there exists an element A of order 2 in* $\mathrm{Br}\, X$ *which spans* $\mathrm{Br}\, X/\mathrm{Br}\, k$. *For any such element A the image of the map $\mathbf{X}(O) \to \mathbb{Z}/2$ given by $P \mapsto \mathrm{inv}(A(P)) \in \mathbb{Z}/2$ is the whole group $\mathbb{Z}/2$.*

Proof. We let ν denote the valuation on k and π be a uniformizing parameter for O. We shall use the following facts from the theory of local fields. Let K/k be a quadratic field extension of local fields. The subgroup of norms $N_{K/k}K^* \subset k^*$ is of index 2. This subgroup coincides with the group of elements of k of even valuation if and only if K/k is the unramified quadratic extension of k. If $K = k(\sqrt{a})$ and $b \in k^*$, then b is a norm from K if and only if the Hilbert symbol $(a, b) = 0 \in \mathbb{Z}/2$.

Suppose $x^2 + y^2 + z^2$ is O-isomorphic to $2xy - z^2$ and $\mathbf{X} \subset \mathbb{A}^3_O$ is given by the equation $2xy - z^2 = a$ which we now first consider.

Since $\mathbf{X}(O) \neq \emptyset$, there is $(x_0, y_0, z_0) \in \mathbf{X}(O)$. Let $v_0 = (x_0 y_0, 1, z_0) \in \mathbf{X}(O)$ and let $v = (\epsilon^{-1}, \epsilon x_0 y_0, z_0) \in \mathbf{X}(O)$ for any $\epsilon \in O^*$. Then

$$\mathrm{inv}(B(v_0, v) - a, -a) = (\epsilon^{-1}(\epsilon x_0 y_0 - 1)^2, -a) = (\epsilon, -a)$$

takes both values 0 and 1 in $\mathbb{Z}/2$ if $k(\sqrt{-a})/k$ is ramified.

If $k(\sqrt{-a})/k$ is unramified, then $\nu(a)$ is even and there are infinitely many ξ and η in O^* such that $-a\pi^{-\nu(a)} = \xi^2 + 4\eta$ by [O'Me71, 63:3].

Let $v_0 = (-2\eta\pi^{\nu(a)}, 1, \xi\pi^{\nu(a)/2})$ be such that

$$\pi^{-1}B((\pi, 1, 0), v_0) = \pi^{-1}(\pi - 2\eta\pi^{v(a)}) = 1 - 2\pi^{v(a)-1}\eta \in O$$

is nonzero.

Since the above v only produces the value 0 in this case, one needs

$$v' = v_0 - \pi^{-1}B((\pi, 1, 0), v_0)(\pi, 1, 0) \in \mathbf{X}(O)$$

and

$$\mathrm{inv}(B(v_0, v') - a, -a) = (-\pi^{-1}(B((\pi, 1, 0), v_0))^2, -a) = (-\pi, -a) = 1 \in \mathbb{Z}/2.$$

Next we assume that $x^2 + y^2 + z^2$ is not isomorphic to $2xy - z^2$ over O. Since $x^2 + y^2 + z^2$ is isomorphic to $2x^2 + 2xy + 2y^2 + 3z^2$ over O by $x \mapsto x - z$, $y \mapsto y - z$ and $z \mapsto x + y + z$, we consider that $\mathbf{X} \subset \mathbb{A}^3_O$ is given by the equation $2x^2 + 2xy + 2y^2 + 3z^2 = a$. Since $\mathbf{X}(O) \neq \emptyset$, one can fix $v_0 = (x_0, y_0, z_0) \in \mathbf{X}(O)$ such that at least one of x_0 or y_0 is nonzero by Hensel's lemma. For any $\epsilon \in O^*$, there are infinitely many $\eta \in O^*$ such that $\epsilon \equiv \eta^2 \bmod \pi$. By Hensel's lemma, for each η there is $\xi \in O$ such that $\xi^2 + \xi\eta + \eta^2 = \epsilon$. Since there are at most two η satisfying $B(v_0, (\xi, \eta, 0)) = 0$ for the given v_0, one can choose η such that $B(v_0, (\xi, \eta, 0)) \neq 0$. Let

$$v = v_0 - \epsilon^{-1}B(v_0, (\xi, \eta, 0))(\xi, \eta, 0) \in \mathbf{X}(O).$$

Then

$$\mathrm{inv}(B(v_0, v) - a, -a) = (-\epsilon^{-1} B(v_0, (\xi, \eta, 0))^2, -a) = (-\epsilon, -a)$$

takes both values 0 and 1 in $\mathbb{Z}/2$ if $k(\sqrt{-a})/k$ is ramified.

If $k(\sqrt{-a})/k$ is unramified, then $\nu(a)$ is even. We claim $\nu(2x^2+2xy+2y^2)$ is odd for all $x, y \in O$. First we show that $\nu(2)$ is odd. Suppose it is not; then there exists $\alpha \in O^*$ such that $2 + 3\alpha^2\pi^{\nu(2)} \equiv 0 \bmod 2\pi$ by the perfectness of the residue field. Then

$$2x^2 + 2xy + 2y^2 + 3z^2 \sim (2 + 3\alpha^2\pi^{\nu(2)})x^2 + 2xy + 2y^2 + (3 + 6\alpha^2\pi^{\nu(2)})z^2$$

over O by

$$x \mapsto x - 2\alpha\pi^{\nu(2)/2} z, \quad y \mapsto y + \alpha\pi^{\nu(2)/2} z, \quad z \mapsto z + \alpha\pi^{\nu(2)/2} x.$$

By Hensel's lemma, one has

$$(2 + 3\alpha^2\pi^{\nu(2)})x^2 + 2xy + 2y^2 \sim 2xy$$

over O (see [O'Me71, 93:11]). This contradicts our assumption. Suppose the claim is not true. Then there are $\alpha, \beta \in O^*$ such that $\alpha^2 + \alpha\beta + \beta^2 \equiv 0 \bmod \pi$. By Hensel's lemma and [O'Me71, 93:11], one has $2x^2 + 2xy + 2y^2 \sim 2xy$ over O which contradicts our assumption. The claim is proved.

By the claim, one obtains that $z_0 \neq 0$. Since the above v only produces the value 0 in this case, one needs $v' = (x_0, y_0, -z_0) \in \mathbf{X}(O)$ and

$$\mathrm{inv}(B(v_0, v') - a, -a) = (-2z_0^2, -a) = (-2, -a) = 1 \in \mathbb{Z}/2.$$

The proof is complete. □

Lemma 9.6. *Let $d < 0$ be a squarefree negative integer. Let $k = \mathbb{Q}(\sqrt{d})$. Let a be a nonzero element in the ring O of integers of k. Assume that, for each place v, a is a sum of three squares in O_v. Then the set of conditions:*

(a) *for each nondyadic valuation v with $v(a) > 0$, $-a$ is a square in k_v;*

(b) *for each dyadic valuation v, $-a$ is a square in k_v;*

is equivalent to the set of conditions:

(i) $d \not\equiv 1 \bmod 8$;

(ii) *there is a squarefree integer $d_0 \in \mathbb{Z}$ such that $a = d_0\alpha^2$ for some $\alpha \in k$;*

(iii) $d = d_0.d_1$ *with* $d_1 \in \mathbb{Z}$;

(iv) $d_0 \equiv 7 \bmod 8$;

(v) *for any odd prime p which divides $N_{k/\mathbb{Q}}(a)$ one at least of $(-d_0/p), (-d_1/p)$ is equal to 1.*

Note that the only difference between the second list of conditions and the list in Theorem 9.1 is that we do not demand $d_0 > 0$.

Proof. From (b) we deduce that -1 is a sum of three squares in each dyadic field k_v. Since -1 is not a sum of three squares in $\mathbb{Q}_2$, this implies that the prime 2 is not split in the extension $k/\mathbb{Q}$, i.e. $d \not\equiv 1$ mod 8, which proves (i).

Hypotheses (a) and (b) imply:

(c) *for any (nonarchimedean) valuation v of k, $v(a)$ is even.*

Thus for any prime p, the p-adic valuation of the positive integer $N_{k/\mathbb{Q}}(a)$ is even. Thus $N_{k/\mathbb{Q}}(a) \in \mathbb{N}$ is a square. An application of Hilbert's theorem 90 shows that there exist an integer $r \in \mathbb{N}$ and an element $\xi \in k$ such that $a = r.\xi^2$. We may and will take r squarefree. From (a) and (b) we conclude that r consists only of primes ramified in the extension $k/\mathbb{Q}$, i.e. r divides the discriminant D of $k/\mathbb{Q}$. In particular r divides $4d$. Since r is squarefree, r divides $2d$.

As we have seen, there is just one valuation v of k above the prime 2. In the dyadic field $k_v = \mathbb{Q}_2(\sqrt{d})$, $-a$ is a square, hence so is $-r$. This implies that either $-r$ or $-d/r$ is a square in $\mathbb{Q}_2$.

If $-r \in \mathbb{Z}$, which is squarefree, is a square in $\mathbb{Q}_2$, then $-r$ is odd and $-r \equiv 1$ mod 8. We set $d_0 = r > 0$. The integer d_0 is squarefree, divides $2d$ and is odd, hence divides d. It satisfies $d_0 \equiv 7$ mod 8. Let $\alpha = \xi$. Then $a = d_0.\alpha^2$.

Assume that $-r$ is not a square in $\mathbb{Q}_2$. Then $-d/r$ is a square in $\mathbb{Q}_2$. Since r divides $2d$ in $\mathbb{Z}$ and d is squarefree, the 2-adic valuation of $-d/r$ is -1, 0 or 1. It must therefore be 0, and $-d/r$ is a positive squarefree integer congruent to 1 mod 8. We set $d_0 = d/r \in \mathbb{Z}$, $d_0 < 0$. The integer d_0 is squarefree, divides d and satisfies $d_0 \equiv 7$ mod 8. Let $\alpha = r.\xi$. Then $a = r.\xi^2 = (d/r).\alpha^2 = d_0.\alpha^2$.

Since d is squarefree, we may write $d = d_0 d_1$ with $d_1 \in \mathbb{Z}$ and d_0, d_1 coprime and squarefree.

Let p be an odd prime which divides $N_{F/\mathbb{Q}}(a) \in \mathbb{N}$. There exists a place v of k above p such that $v(a) > 0$. By hypothesis (b), $-a$ is a square in k_v. Thus $-d_0$ is a square in k_v. If p splits in $k = \mathbb{Q}(\sqrt{d})$, then $k_v \simeq \mathbb{Q}_p$, the squarefree integer $-d_0$ is a square in $\mathbb{Q}_p$, hence is prime to p and satisfies $(-d_0/p) = 1$. If p is inert or ramified in k, then $-d_0$ is a square in the quadratic extension $\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$. Thus one of the squarefree integers $-d_0$ or $-d_1 = -d/d_0$ is a square in $\mathbb{Q}_p$, hence is the square of a unit in $\mathbb{Z}_p$.

Thus the second set of conditions is implied by the first one.

Suppose (i) to (v) hold. From (ii) and (iv), we get (b). From (ii) and (iii) we see that we may write $-a = -d_0\alpha^2$ and $a = -d_1\beta^2$ with $\alpha, \beta \in k$. If v is a place of k above an odd prime p and $v(a) > 0$ then p divides $N_{k/\mathbb{Q}}(a)$. From (v) we then get that either $-d_0$ or $-d_1$ is a square in $\mathbb{Q}_p$, hence $-a$ is a square in k_v. □

Let us go back to the global situation. Thus a lies in the ring of integers of $k = \mathbb{Q}(\sqrt{d})$ and $a \in O$ is a sum of three squares in O_v for each place v. Moreover, $-a$ is not a square in k. Let $A \in \operatorname{Br} X$ be a 2-torsion element which spans $\operatorname{Br} X/\operatorname{Br} k = \mathbb{Z}/2$. Let us consider the two conditions:

(1) for each nondyadic valuation v with $v(a) > 0$, $-a$ is a square in k_v;

(2) for each dyadic valuation v, $-a$ is a square in k_v.

From Lemmas 9.3, 9.4 and 9.5 we deduce the following result.

If one of these two conditions does not hold, then there exists a place v such that the image of $\mathbf{X}(O_v) \to \mathbb{Z}/2$ given by evaluation of A is the whole group $\mathbb{Z}/2$, hence $\mathbf{X}(O) \neq \emptyset$.

For any given $A \in \operatorname{Br} X$ as above, we thus have that, for each place v of k, the image of the evaluation map $\mathbf{X}(O_v) \to \mathbb{Z}/2$ given by $M_v \mapsto \operatorname{inv}_v(A(M_v))$ is reduced to one element, say $\alpha_v \in \mathbb{Z}/2$, and $\mathbf{X}(O) = \emptyset$ if and only if $\sum_v \alpha_v = 1 \in \mathbb{Z}/2$.

For given a satisfying the two conditions above, let us produce a convenient A. Under our assumptions, $-1 = a/(-a)$ is a sum of three squares, hence of two squares, in each dyadic field k_v. It is a sum of two squares in any other completion k_v. By Hasse's principle it is a sum of two squares in k. There thus exists $\rho, \sigma, \tau \in O$, which we may take all nonzero, such that $\rho^2 + \sigma^2 + \tau^2 = 0$. This defines a point (at infinity) on $Y(k)$. Starting from this point, the technique recalled at the beginning of the proof shows that the quaternion algebra $(\rho x + \sigma y + \tau z, -a)$ is the restriction to the open set $\rho x + \sigma y + \tau z \neq 0$ of a 2-torsion element A of $\mathrm{Br}\, X$ which spans $\mathrm{Br}\, X/\mathrm{Br}\, k$.

Let v be a place of k and π a uniformizing parameter. If $-a$ is a square in k_v, then $A = 0$. That is thus the case for v dyadic and for v nondyadic such that $v(a) > 0$.

Assume that $-a$ is not a square in k_v. For v nondyadic with $v(a) = 0$, for $b \in k_v^*$, we have $\mathrm{inv}(b, -a) = 0 \in \mathbb{Z}/2$ if and only if $v(b)$ is even. Let $n = \inf(v(\rho), v(\sigma), v(\tau))$. Let $\rho = \rho_v \pi^n$, $\sigma = \sigma_v \pi^n$, $\tau = \tau_v \pi^n$. Assume $v(\rho_v) = 0$. Let

$$M_v = (\rho_v, \sigma_v, \tau_v) + (a/2\rho_v^2)(\rho_v, -\tau_v, \sigma_v) \in O_v^3.$$

We have $M_v \in \mathbf{X}(O_v)$. Thus $\alpha_v = \mathrm{inv}_v(A(M_v)) = \mathrm{inv}_v(\frac{1}{2}\pi^n a, -a) \in \mathbb{Z}/2$ is 0 or 1 depending on whether n is even or odd. By symmetry in ρ, σ, τ, the result holds whichever is the smallest of $v(\rho), v(\sigma), v(\tau)$.

We thus conclude as follows.

Assume that for each nondyadic valuation v with $v(a) > 0$, $-a$ is a square in k_v and that for each dyadic valuation v, $-a$ is a square in k_v. There exist $\rho, \sigma, \tau \in O$, none of them zero, such that $\rho^2 + \sigma^2 + \tau^2 = 0$. Fix such a triple. Then the set $\mathbf{X}(O)$ is not empty if and only if the number of places v such that:

(1) *$-a$ is not a square in k_v,*

(2) *$\inf(v(\rho), v(\sigma), v(\tau))$ is odd,*

is even.

Let us now look for values of $\rho, \sigma, \tau \in O$. We know that -1 is a sum of two squares in k. Since it is not a sum of two squares in $\mathbb{Q}_2$, this implies that the prime 2 is not split in the extension $k/\mathbb{Q}$, i.e. the squarefree integer d satisfies $d \not\equiv 1 \bmod 8$, hence the squarefree integer $-d$ satisfies $-d \not\equiv 7 \bmod 8$. Thus there exist $\alpha, \beta, \gamma, \delta$ in $\mathbb{Z}$, not all zero, such that $\alpha^2 + \beta^2 + \gamma^2 + d\delta^2 = 0$. We may choose them so that none of $\alpha, \beta, \gamma, \delta, \alpha^2 + \beta^2$ is zero. Then

$$(\alpha^2 + \beta^2)^2 + (\alpha\gamma + \beta\delta\sqrt{d})^2 + (\beta\gamma - \alpha\delta\sqrt{d})^2 = 0.$$

We may thus take

$$(\rho, \sigma, \tau) = (\alpha^2 + \beta^2, \alpha\gamma + \beta\delta\sqrt{d}, \beta\gamma - \alpha\delta\sqrt{d}).$$

To produce convenient $\alpha, \beta, \gamma, \delta$, we shall use Hecke's results on primes represented by a binary quadratic form.

PROPOSITION 9.7. *Let $d < 0$ be a squarefree integer, $d \not\equiv 1 \bmod 8$. Then there exists a prime $l \equiv 1 \bmod 4$ which does not divide d and which is represented over $\mathbb{Z}$ as:*

(a) *$l = -2i^2 + 2ij - ((d+1)/2)j^2$ if $d \equiv 5 \bmod 8$;*

(b) *$l = -i^2 - dj^2$ if $d \equiv 2 \bmod 4$;*

(c) *$l = -i^2 + ij - ((d+1)/4)j^2$ if $d \equiv 3 \bmod 4$.*

Proof. Let us denote by $q(x, y)$ the quadratic form on the right hand side. This is a form of discriminant $-4d$, hence over the reals it breaks up as a product of two linear forms. In each of the above cases one checks that there exist $i_0, j_0 \in \mathbb{Z}$ such that $q(i_0, j_0) \equiv 1 \bmod 4$. Let $\Delta \subset \mathbb{R} \times \mathbb{R}$ be a convex cone with vertex at the origin in the open set defined by $q(x, y) > 0$. In each of the above cases the quadratic form $q(x, y)$ is primitive: there is no prime which divides all its coefficients. A direct application of Hecke's result as made explicit in [CCS80, Theorem 2.4, p. 162] shows that there exist $i, j \in \mathbb{Z}$ and l a prime number such that $(i, j) \in \Delta$, hence $q(i, j) > 0$, with $q(i, j) = \pm l$, hence $q(i, j) = l$ such that moreover $(i, j) \equiv (i_0, j_0) \bmod 4$, hence $l \equiv 1 \bmod 4$. □

Remark 9.8. Earlier papers on the subject [EH83, JWX06] already use special representations as provided by the above proposition. For their purposes, Dirichlet's theorem (for number fields) was enough.

Fix l as above. Fix $\alpha, \beta \in \mathbb{Z}$ such that:

(a) $\alpha^2 + \beta^2 = 2l$ if $d \equiv 5 \bmod 8$;
(b) $\alpha^2 + \beta^2 = l$ if $d \equiv 2 \bmod 4$;
(c) $\alpha^2 + \beta^2 = 4l$ if $d \equiv 3 \bmod 4$.

For i, j as above set:

(a) $\gamma = 2i - j, \delta = j$ if $d \equiv 5 \bmod 8$;
(b) $\gamma = i, \delta = j$ if $d \equiv 2 \bmod 4$;
(c) $\gamma = 2i - j, \delta = j$ if $d \equiv 3 \bmod 4$.

Then $\alpha^2 + \beta^2 + \gamma^2 + d\delta^2 = 0$ and $(l, \alpha\beta\gamma\delta) = 1$.

The prime l splits in $k/\mathbb{Q}$. Let v_1 and v_2 be the two places of k above l. We have $N_{k/\mathbb{Q}}(\beta\gamma - \alpha\delta\sqrt{d}) = 2l(\alpha^2 + \gamma^2)$ if $d \equiv 5 \bmod 8$, $N_{k/\mathbb{Q}}(\beta\gamma - \alpha\delta\sqrt{d}) = l(\alpha^2 + \gamma^2)$ if $d \equiv 2 \bmod 4$, and $N_{k/\mathbb{Q}}(\beta\gamma - \alpha\delta\sqrt{d}) = 4l(\alpha^2 + \gamma^2)$ if $d \equiv 3 \bmod 4$. We have $N_{k/\mathbb{Q}}(\alpha\gamma + \beta\delta\sqrt{d}) = 2l(\beta^2 + \gamma^2)$ if $d \equiv 5 \bmod 8$, $N_{k/\mathbb{Q}}(\alpha\gamma + \beta\delta\sqrt{d}) = l(\beta^2 + \gamma^2)$ if $d \equiv 2 \bmod 4$, and $N_{k/\mathbb{Q}}(\alpha\gamma + \beta\delta\sqrt{d}) = 4l(\beta^2 + \gamma^2)$ if $d \equiv 3 \bmod 4$.

Thus

$$\mathrm{ord}_{v_1}(\beta\gamma - \alpha\delta\sqrt{d}) + \mathrm{ord}_{v_2}(\beta\gamma - \alpha\delta\sqrt{d}) \geq 1$$

and

$$\mathrm{ord}_{v_1}(\alpha\gamma + \beta\delta\sqrt{d}) + \mathrm{ord}_{v_2}(\alpha\gamma + \beta\delta\sqrt{d}) \geq 1.$$

Since $\beta(\beta\gamma - \alpha\delta\sqrt{d}) + \alpha(\alpha\gamma + \beta\delta\sqrt{d})$ is equal to $2l\gamma$ if $d \equiv 5 \bmod 8$, is equal to $l\gamma$ if $d \equiv 2 \bmod 4$ and is equal to $4l\gamma$ if $d \equiv 3 \bmod 4$, one has

$$\mathrm{ord}_{v_1}(\beta\gamma - \alpha\delta\sqrt{d}) \geq 1 \Leftrightarrow \mathrm{ord}_{v_1}(\alpha\gamma + \beta\delta\sqrt{d}) \geq 1$$

and

$$\mathrm{ord}_{v_2}(\beta\gamma - \alpha\delta\sqrt{d}) \geq 1 \Leftrightarrow \mathrm{ord}_{v_2}(\alpha\gamma + \beta\delta\sqrt{d}) \geq 1.$$

Since

$$N_{k/\mathbb{Q}}(\alpha\delta\sqrt{d} - \beta\gamma) + N_{k/\mathbb{Q}}(\alpha\gamma + \beta\delta\sqrt{d})$$

is equal to $4l(l + \gamma^2)$ if $d \equiv 5 \bmod 8$, to $l(l + 2\gamma^2)$ if $d \equiv 2 \bmod 4$ and to $8l(2l + \gamma^2)$ if $d \equiv 3 \bmod 4$, one has

$$\mathrm{ord}_{v_1}(\beta\gamma - \alpha\delta\sqrt{d}) + \mathrm{ord}_{v_2}(\beta\gamma - \alpha\delta\sqrt{d}) = 1$$

or

$$\mathrm{ord}_{v_1}(\alpha\gamma + \beta\delta\sqrt{d}) + \mathrm{ord}_{v_2}(\alpha\gamma + \beta\delta\sqrt{d}) = 1.$$

Without loss of generality, one can assume that

$$\mathrm{ord}_{v_1}(\beta\gamma - \alpha\delta\sqrt{d}) = 0 \quad \text{and} \quad \mathrm{ord}_{v_2}(\beta\gamma - \alpha\delta\sqrt{d}) = 1.$$

Then

$$\mathrm{ord}_{v_1}(\alpha\gamma+\beta\delta\sqrt{d})=0 \quad \text{and} \quad \mathrm{ord}_{v_2}(\alpha\gamma+\beta\delta\sqrt{d})\geq 1.$$

For

$$(\rho,\sigma,\tau)=(\alpha^2+\beta^2,\alpha\gamma+\beta\delta\sqrt{d},\beta\gamma-\alpha\delta\sqrt{d})$$

we thus have

$$\inf(v_1(\rho),v_1(\sigma),v_1(\tau))=0,$$
$$\inf(v_2(\rho),v_2(\sigma),v_2(\tau))=1$$

and

$$\inf(v(\rho),v(\sigma),v(\tau))=0$$

for any other nondyadic prime v.

Assume $\mathbf{X}(O)=\emptyset$. From Lemmas 9.3, 9.4 and 9.5 we know that hypotheses (a) and (b) in Lemma 9.6 hold. In particular $a=d_0\zeta^2$ for some $\zeta\in k$. Also, the squarefree integer d is not congruent to 1 mod 8. We may thus produce (ρ,σ,τ) as above. For A associated to (ρ,σ,τ), we have $\alpha_v=0$ for any $v\neq v_2$ and $\alpha_{v_2}=1$ if and only if $-a$ is not a square in k_{v_2}, i.e. if and only if $-d_0$ is not a square in $\mathbb{Q}_l$, i.e. if and only if $-1=(-d_0/l)$.

From Lemma 9.6 we have $d\neq 0,1,4$ mod 8. Thus

$$-1=\left(\frac{-d_0}{l}\right)=\prod_{p|d_0}\left(\frac{l}{p}\right)=\prod_{p|d_0}\left(\frac{-1}{p}\right)$$

if $d\equiv 2$ or 3 mod 4, where the second equality follows from the quadratic reciprocity law and the third equality follows from Proposition 9.7. This implies that there is an odd number of primes congruent to 3 mod 4 which divide the squarefree integer d_0. Hence d_0 is congruent to its sign times 3 modulo 4. From Lemma 9.6 we have d_0 congruent to 7 mod 8, hence to 3 mod 4. We now conclude $d_0>0$.

Similarly

$$-1=\left(\frac{-d_0}{l}\right)=\prod_{p|d_0}\left(\frac{l}{p}\right)=\prod_{p|d_0}\left(\frac{-2}{p}\right)$$

if $d\equiv 5$ mod 8, and we deduce $d_0>0$.

Together with Lemma 9.6, this completes the proof of one half of Theorem 9.1: if $\mathbf{X}(O)$ is empty, then conditions (i) to (v) in that theorem are fulfilled.

Assume that hypotheses (i) to (v) in Theorem 9.1 hold. Then from Lemma 9.6 we deduce: for each nondyadic valuation v with $v(a)>0$, $-a$ is a square in k_v and for each dyadic valuation v, $-a$ is a square in k_v. Proceeding as above one finds suitable $\alpha,\beta,\gamma,\delta$ with associated ρ,σ,τ, and a prime l congruent to 1 mod 4 such that $\mathbf{X}(O)=\emptyset$ if and only if $-d_0$ is not a square in $\mathbb{Q}_l$. The same computation as above now shows that $d_0>0$ implies that $-d_0$ is not a square in $\mathbb{Q}_l$. □

Acknowledgements

The work on this paper started at the Conference on Arithmetic Geometry and Automorphic Forms held at Nankai Institute of Mathematics, Tianjin, in August 2005. It was pursued over e-mail and during stays of the first named author at Tsinghua University, Beijing (August 2005) and at the Morning Centre of Mathematics, Beijing (April 2007) and of the second named author at I.H.É.S, Bures-sur-Yvette (July 2006). We thank David Harari and Mikhail Borovoi for comments on our text.

Appendix A. Sum of three squares in a cyclotomic field, by Dasheng Wei and Fei Xu

In this appendix, we will show that the local-global principle holds for the sum of three squares over the ring of integers of cyclotomic fields. First we need the following lemma which appears in [Raj93, Exercises 2 and 3, p. 70]. For completeness, we provide the proof.

LEMMA A.1. *Suppose R is a commutative ring with identity 1_R. If -1_R can be written as a sum of two squares over R, then any element which can be written as a sum of squares over R is a sum of three squares over R.*

Proof. Suppose $\alpha \in R$ can be written as a sum of squares. Since -1_R can be written as a sum of squares, one has that $-\alpha$ can be written as a sum of squares as well. Let $-\alpha = \sum_{i=1}^{s} x_i^2$. Then

$$\alpha = \Big(\prod_{1\le i<j\le s} x_i x_j + \sum_{i=1}^{s} x_i + 1\Big)^2 - \Big[\Big(\prod_{1\le i<j\le s} x_i x_j + \sum_{i=1}^{s} x_i\Big)^2 + \Big(1 + \sum_{i=1}^{s} x_i\Big)^2\Big].$$

Since -1_R is a sum of two squares and

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2,$$

one concludes that α is a sum of three squares. □

Let $k = \mathbb{Q}(\zeta_n)$ be a cyclotomic field, where ζ_n is a primitive nth root of unity. Let O be the ring of integers of k.

THEOREM A.2. *An integer $x \in O$ is a sum of three squares over O if and only if x is a sum of three squares over all local completions O_v.*

Proof. If 2 is ramified in $k/\mathbb{Q}$, then $4 \mid n$ and -1 is a square in O. By Theorem 6.1, one has x is a sum of four squares. By Lemma A.1, one concludes that x is a sum of three squares as well.

Now one only needs to consider the case that 2 is unramified. Therefore one can assume that n is odd. Let f be the order of the Frobenius of 2 in $\mathrm{Gal}(k/\mathbb{Q}) = (\mathbb{Z}/n)^*$.

If f is even, there is a prime $p \mid n$ such that the order of 2 in $(\mathbb{Z}/p)^*$ is even by the Chinese remainder theorem, which is denoted by $2t$. Then $2^t \equiv -1 \bmod p$. Let $\zeta_p \in O$ be a pth primitive root of unity. One has

$$\prod_{i=1}^{t} (1+\zeta_p^{2^i}) = \frac{1-(\zeta_p^{2^t})^2}{1-\zeta_p^2} = \frac{1-(\zeta_p^{-1})^2}{1-\zeta_p^2} = -\zeta_p^{-2}.$$

This implies that -1 can be written as a sum of two squares over O. By the same argument as above, x is a sum of three squares.

Otherwise $f = [\mathbb{Q}_2(\zeta_n) : \mathbb{Q}_2]$ is odd. Suppose x is not a sum of three squares over O. By Lemma 9.5 and Theorem 6.3, one obtains that $-x$ is a square in $\mathbb{Q}_2(\zeta_n)$. This implies -1 is a sum of three squares over $\mathbb{Q}_2(\zeta_n)$. By Springer's theorem (see [Sch86, Chapter 2, § 5.3]), -1 is a sum of three squares over $\mathbb{Q}_2$. Therefore -1 is a sum of two squares by Pfister's theorem (see [Sch86, Chapter 2, § 10.8]) over $\mathbb{Q}_2$. A contradiction is derived. □

REFERENCES

Bor96 M. Borovoi, *The Brauer–Manin obstructions for homogeneous spaces with connected or abelian stabilizer*, J. reine angew. Math. **473** (1996), 181–194.

Bor99 M. Borovoi, *The defect of weak approximation for homogeneous spaces*, Ann. Fac. Sci. Toulouse **8** (1999), 219–233.

Bor01 M. Borovoi, *On representations of integers by indefinite ternary quadratic forms*, J. Number Theory **90** (2001), 281–293.

BR95 M. Borovoi and Z. Rudnick, *Hardy–Littlewood varieties and semisimple groups*, Invent. Math. **119** (1995), 37–66.

Cas78 J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13 (Academic Press, London, 1978).

CX04 W. K. Chan and F. Xu, *On representations of spinor genera*, Compositio Math. **140** (2004), 287–300.

Col08 J.-L. Colliot-Thélène, *Résolutions flasques des groupes linéaires connexes*, J. reine angew. Math. **618** (2008), 77–133.

CCS80 J.-L. Colliot-Thélène, D. Coray and J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. reine angew. Math. **320** (1980), 150–191.

CS87 J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles II*, Duke Math. J. **54** (1987), 375–492.

Col03 J.-L. Colliot-Thélène, *Points rationnels sur les fibrations*, in *Higher dimensional varieties and rational points*, Budapest, 2001, Bolyai Society of Mathematical Studies, vol. 12 (Springer, Berlin, 2003), 171–221.

CK06 J.-L. Colliot-Thélène and B. È. Kunyavskiĭ, *Groupe de Picard et groupe de Brauer des compactifications lisses d'espaces homogènes*, J. Algebraic Geometry **15** (2006), 733–752.

Eic52 M. Eichler, *Die Ähnlichkeitsklassen indefiniter Gitter*, Math. Z. **55** (1952), 216–252.

ER06 I. V. Erovenko and A. S. Rapinchuk, *Bounded generation of S-arithmetic subgroups of isotropic orthogonal groups over number fields*, J. Number Theory **119** (2006), 28–48.

EH83 D. R. Estes and J. S. Hsia, *Sum of three integer squares in complex quadratic fields*, Proc. Amer. Math. Soc. **89** (1983), 211–214.

GH70 J. Gamst and K. Hoechsmann, *Products in sheaf cohomology*, Tôhoku Math. J. **22** (1970), 143–162.

GH71 J. Gamst and K. Hoechsmann, *Ext-products and edge-morphisms*, Tôhoku Math. J. **23** (1971), 581–588.

Gro68 A. Grothendieck, Le groupe de Brauer, I, II, III, in *Dix exposés sur la cohomologie des schémas* (Masson, Paris; North-Holland, Amsterdam, 1968).

Har94 D. Harari, *Méthode des fibrations et obstruction de Manin*, Duke Math. J. **75** (1994), 221–260.

Har67 G. Harder, *Halbeinfache Gruppenschemata über Dedekindringen*, Invent. Math. **4** (1967), 165–191.

HSX98 J. S. Hsia, Y. Y. Shao and F. Xu, *Representations of indefinite quadratic forms*, J. reine angew. Math. **494** (1998), 129–140.

JWX06 C. Ji, Y. Wang and F. Xu, *Sums of three squares over imaginary quadratic fields*, Forum Math. **18** (2006), 585–601.

JW56 B. W. Jones and G. L. Watson, *On indefinite ternary quadratic forms*, Canad. J. Math. **8** (1956), 592–608.

Kne56 M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. **VII** (1956), 323–332.

Kne61 M. Kneser, *Darstellungsmasse indefiniter quadratischer Formen*, Math. Z. **77** (1961), 188–194.

Kne65 M. Kneser, *Starke Approximation in algebraischen Gruppen, I*, J. reine angew. Math. **218** (1965), 190–203.

KSS89 H. Kraft, P. Slodowy and T. A. Springer, *Algebraische Transformationsgruppen und Invariantentheorie*, DMV Seminar, vol. 13 (Birkhäuser, Basel, 1989).

Kot86 R. E. Kottwitz, *Stable trace formula: elliptic singular terms*, Math. Ann. **275** (1986), 365–399.

Mil80 J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33 (Princeton University Press, Princeton, NJ, 1980).

Mil86 J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1 (Academic Press, New York, 1986).

Nis84 Ye. A. Nisnevich, *Espaces homogènes principaux rationnellement triviaux et arithmétique des schémas en groupes réductifs sur les anneaux de Dedekind*, C. R. Acad. Sci. Paris Sér. I **299** (1984), 5–8.

O'Me71 O. T. O'Meara, *Introduction to quadratic forms*, Grundlehren der Mathematik, vol. 117 (Springer, Berlin, 1971).

PR91 V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory* (Nauka, Moscow, 1991), (Engl. trans. *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139 (Academic Press, Inc., Boston, MA, 1994)).

Raj93 A. R. Rajwade, *Squares*, London Mathematical Society Lecture Note Series, vol. 171 (Cambridge University Press, Cambridge, 1993).

San81 J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. reine angew. Math. **327** (1981), 12–80.

Sch86 W. Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematik, vol. 270 (Springer, Berlin, 1986).

Sch80 R. Schulze-Pillot, *Darstellung durch Spinorgeschlechter ternärer quadratischer Formen*, J. Number Theory **12** (1980), 529–540.

Sch00 R. Schulze-Pillot, *Exceptional integers for genera of integral ternary positive definite quadratic forms*, Duke Math. J. **102** (2000), 351–357.

Sch04 R. Schulze-Pillot, *Representation by integral quadratic forms—a survey. Algebraic and arithmetic theory of quadratic forms*, Contemp. Math. **344** (2004), 323–337.

SX04 R. Schulze-Pillot and F. Xu, *Representations by spinor genera of ternary quadratic forms*, Contemp. Math. **344** (2004), 323–337.

Ser65 J.-P. Serre, *Cohomologie Galoisienne (Cinquième édition, révisée et complétée)*, Lecture Notes in Mathematics, vol. 5 (Springer, Berlin, 1965).

Sko01 A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144 (Cambridge University Press, Cambridge, 2001).

Wat61 G. L. Watson, *Indefinite quadratic diophantine equations*, Mathematika **8** (1961), 32–38.

Wat67 G. L. Watson, *Diophantine equations reducible to quadratics*, Proc. London Math. Soc. **17** (1967), 26–44.

Wei62 A. Weil, *Sur la théorie des formes quadratiques*, in *Colloque sur la théorie des groupes algébriques* (CBRM, Bruxelles, 1962), 9–22.

Xu00 F. Xu, *Representations of indefinite ternary quadratic forms over number fields*, Math. Z. **234** (2000), 115–144.

Xu05 F. Xu, *On representations of spinor genera II*, Math. Ann. **332** (2005), 37–53.

Jean-Louis Colliot-Thélène jlct@math.u-psud.fr
CNRS, UMR 8628, Mathématiques, Bâtiment 425, Université Paris-Sud, F-91405 Orsay, France

Fei Xu xufei@math.ac.cn
Academy of Mathematics and System Science, CAS, Beijing 100080, P.R. China