Zeitschrift: Commentarii Mathematici Helvetici
Band: 59 (1984)

Artikel: On algebraic tori of norm type.
Autor: Hürlimann, W.
DOI: https://doi.org/10.5169/seals-45408

Comment. Math. Helvetici 59 (1984) 539–549 0010-2571/84/040539-11$01.50 + 0.20/0

On algebraic tori of norm type

W. HÜRLIMANN*

Introduction

We study algebraic norm tori T arising from norm forms of subextensions of a finite Galois extension of global fields (see definition in section 1). Even in that special case, the arithmetic structure of the Tate–Shafarevich group Ш(T), measuring the deviation from the validity of the Hasse principle, is far from being understood. The first section has preliminary character. In section 2, we prove that certain tori are stably birationally equivalent. From this we deduce new types of linear algebraic groups whose non-trivial arithmetical Tate–Shafarevich group structure is explicitly known. As an illustration for the applications of algebraic tori to Diophantine geometry, we deal in section 3 with a class of tori satisfying the Hasse principle and the weak approximation. Its simplest special case provides a new proof of the well-known Hasse principle for quadratic forms in 4 variables. More generally, a subclass of these tori give a necessary criterion for a diagonal surface of arbitrary degree to be a counterexample to the Hasse principle.

The methods used in section 2 are based on the techniques developed by Voskresenskii, Endo and Miyata, Lenstra. The proper geometric setting of these techniques is splendidly demonstrated by Colliot-Thélène and Sansuc in [3]. So we will assume the reader is familiar with this basic work, especially section 1, 2, 8.

1. Preliminary remarks and notations

Throughout this paper, unless mentioned, we let K/k be a finite Galois extension of arbitrary fields with group G. By L_G we mean the category of finitely generated $\mathbb{Z}G$-modules which are free as abelian groups. A $\mathbb{Z}G$-module will be called simply a G-module. The $\mathbb{Z}G$-module $M^0 = \mathrm{Hom}\,(M, \mathbb{Z})$ is the $\mathbb{Z}$-dual of M.

---

* This work was done at MPI für Mathematik in Bonn. Financial support from the Swiss N.F. for scientific research.

We know (for example [1]) that L_G is in duality with the category $T(K/k)$ of algebraic tori defined over k and split by K. A k-torus $T \in T(K/k)$ corresponds in this duality to the dual $X(T)^0$ of the character module $X(T) = \mathrm{Hom}\,(T, \mathbb{G}_m)$. Two algebraic k-tori T_1 and T_2 are called *k-stably birationally equivalent* if the k-varieties $T_1 x_k \mathbb{A}^r(k)$ and $T_2 x_k \mathbb{A}^s(k)$ are k-birationally equivalent for appropriate choices of r and s. We let $Z(K/k)$ be the set of stable birational equivalence classes of tori in $T(K/k)$. For an arbitrary G-module A, we understand by $H^n(G, A)$ the *Tate* cohomology groups defined for all integers n.

Following Colliot-Thélène and Sansuc (see [3]), we outline how $Z(K/k)$ can be studied via flasque resolutions of G-modules. A *permutation* module is a G-module which has a $\mathbb{Z}$-basis permuted by G. Permutation modules are sums of modules of the form $\mathbb{Z}[G/H]$ where H is a subgroup of G and G acts by permuting cosets. A direct summand of a permutation module is called an *invertible* module (also permutation projective in the literature). A G-module M is called a *flasque* module if $H^{-1}(H, M) = 0$ for all subgroups $H \subset G$. For any G-module M, there exists an exact sequence, called *flasque resolution,*

$$0 \to M \to P \to F \to 0,$$

where P is a permutation module and F is a flasque module ([2], lemma 3). Two modules M, M' are defined to be *similar* if there exists permutation modules P, P' such that $M \oplus P = M' \oplus P'$. The similarity class of a module M is written $[M]$. A module similar to 0 is called a *stably permutation* module. The similarity classes of modules in L_G build a commutative semigroup S_G with respect to direct sums. Let F_G be its sub-semigroup of similarity classes of flasque G-modules. If $0 \to M \to P \to F \to 0$ and $0 \to M \to P' \to F' \to 0$ are two flasque resolutions of M, then F is similar to F' ([3], lemme 5) and F depends only on the class of M. Therefore, defining $\rho(M)$ to be the similarity class of F, the map ρ from S_G to F_G is well-defined. Let now $T \in T(K/k)$ be a k-torus. If $\rho(T)$ is defined to be $\rho(X(T))$, it is shown in ([3], prop. 5, 6) that the invariant ρ characterizes the equivalence classes of k-stably birational equivalent tori. More precisely, the map $\rho: T(K/k) \to F_G$, $T \mapsto \rho(T) = \rho(X(T))$, induces an isomorphism of semigroups $\rho: Z(K/k) \cong F_G$. In section 2, we will use freely this characterization.

We recall now some standard notations from algebraic number theory. Let K/k be a Galois extension of global fields with group G. Let P be the set of all places v of k and let G_v in G be the decomposition group of a place w above v. If M is an arbitrary G-module, we write $Ш^i(G, M)$ for the kernel of the restriction map $H^i(G, M) \to \prod_{v \in P} H^i(G_v, M)$ for all integers i. If $M \in L_G$ or if M and i are such that $H^i(G_v, M) = 0$ for almost all $v \in P$, we denote by $Ч^i(G, M)$ the cokernel of this same restriction map. For a torus $T \in T(K/k)$, we write $Ш^i(T)$ for the kernel of the restriction map $H^i(G, T(K)) \to \prod_{v \in P} H^i(G_v, T(K_w))$, where $T(L)$ denotes the rational points of T in the field L containing k. The group $Ш^1(T)$, written $Ш(T)$, is the so-called Tate–Shafarevich group of T. It is the obstruction to the validity of the Hasse principle for the principal homogeneous spaces under T. The obstruction to the weak approximation for T is the quotient $A(T)$ of $\prod_{v \in P} T(k_v)$ by the closure of the image of $T(k)$ via the diagonal embedding. In this context, we assume the reader is acquainted with the fundamental theorems of Tate and Nakayama on local and global duality (see the references [21], [32] in [3]).

Finally, the objects of study in this paper are tori of norm type. An algebraic k-torus $T \in T(K/k)$ is said to be a *norm torus* if the dual $X(T)^0$ of its character module $X(T)$ belongs to an exact sequence of G-modules

$$0 \to X(T)^0 \to \bigoplus_{H \in S} \mathbb{Z}[G/H] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

where S is a finite set of subgroups of G and ε is the sum of the augmentation maps $\varepsilon_{G/H}: \mathbb{Z}[G/H] \to \mathbb{Z}$, $H \in S$.

2. Stable birational equivalence of some algebraic tori

Let K/k be a Galois extension of bicyclic group $G = C_m \times C_n$ generated by s and t. We assume that $m, n \neq 1$. Denote by K_1, respectively K_2, the fixed field by s, respectively t, and by K_i the fixed field by st^{i-2} for $i = 3, \dots, n+1$. The norms from K_i to k are written N_i, $i = 1, \dots, n+1$.

Let us introduce the relevant tori. Let I_G be the augmentation ideal of G and consider the exact sequences of G-modules

$$0 \to X(T_2') \to \mathbb{Z}G \cdot u(s) \oplus \mathbb{Z}G \cdot u(t) \xrightarrow{d} I_G \to 0, \tag{2.1}$$

$$0 \to X(T_2) \to \bigoplus_{r \in G} \mathbb{Z}G \cdot u(r) \xrightarrow{d'} I_G \to 0, \tag{2.2}$$

where the $u(r)$, $r \in G$, are indeterminates and d, d' are defined by $du(s) = s - 1$, $du(t) = t - 1$, $d'u(r) = r - 1$, $r \in G$. The G-modules $X(T_2')$, $X(T_2)$ define by duality the algebraic k-tori T_2', T_2. In the special case $m = n = 2$, the exact sequence of G-modules

$$0 \to X(S)^0 \to \mathbb{Z}[G/st] \oplus \mathbb{Z}[G/s] \oplus \mathbb{Z}[G/t] \xrightarrow{\varepsilon} \mathbb{Z} \to 0, \tag{2.3}$$

where ε is the sum of augmentations, defines the norm torus S. We will show that these tori are closely related to the norm torus $R^1_{K/k}G_m$ associated to the Chevalley module $J_G = I^0_G$. The key of our results lies in the construction of short exact sequences relating these modules.

We begin with $X(S)^0$. This module possesses the $\mathbb{Z}$-basis $e_1=(1-t,0,0)$, $e_2=(0,1-t,0)$, $e_3=(0,0,1-s)$, $e_4=(1,-1,0)$, $e_5=(1,0,-1)$. The map $f:\mathbb{Z}[G/st]\oplus\mathbb{Z}[G/s]\oplus\mathbb{Z}[G/t]\to\mathbb{Z}G$ such that $f(1,0,0)=1+s$, $f(0,1,0)=1+t$, $f(0,0,1)=1+st$, defines a homomorphism of G-modules $f:X(S)^0\to I_G$. This homomorphism is surjective since $1-s=f(e_3-e_4+e_5)$, $1-t=f(e_3+e_5)$ and $1-st=f(e_1-e_4)$. A routine computation shows that

$$\operatorname{Ker} f=\mathbb{Z}\cdot(e_1-e_2-2e_4)\oplus\mathbb{Z}\cdot(e_1-e_3-2e_5)\cong\mathbb{Z}\oplus\mathbb{Z}$$

is a trivial G-module. Therefore we have by duality the exact sequence of G-modules

$$0\to J_G\to X(S)\to\mathbb{Z}\oplus\mathbb{Z}\to 0. \tag{2.4}$$

We look now at $X(T_2')$. The exact sequence of G-modules

$$0\to\mathbb{Z}\xrightarrow{\alpha}\mathbb{Z}G\xrightarrow{\beta}\mathbb{Z}G\oplus\mathbb{Z}G\to X(Q)^0\to 0,$$

where $\alpha(1)=\sum_{r\in G} r$, $\beta(1)=(s-1,t-1)$, defines the module $X(Q)^0$. Since $\operatorname{Coker}\alpha = J_G$, we have short exact sequences

$$0\to\mathbb{Z}\to\mathbb{Z}G\to J_G\to 0, \tag{2.5}$$

$$0\to J_G\to\mathbb{Z}G\oplus\mathbb{Z}G\to X(Q)^0\to 0. \tag{2.6}$$

In particular, we have the identifications $X(T_2')^0=X(Q)^0=(\mathbb{Z}G\oplus\mathbb{Z}G)/U$ where U is the left submodule generated by $(s-1,t-1)$. The map $g:(\mathbb{Z}G\oplus\mathbb{Z}G)/U\to I_G$ such that $g((1,0)+U)=t-1$, $g((0,1)+U)=1-s$, defines a surjective homomorphism of G-modules whose kernel is the trivial G-module

$$\operatorname{Ker} g=\mathbb{Z}\cdot\left(\left(\sum_{i=0}^{n-1} t^i,0\right)+U\right)\oplus\mathbb{Z}\cdot\left(\left(0,\sum_{i=0}^{m-1} s^i\right)+U\right)\cong\mathbb{Z}\oplus\mathbb{Z}.$$

Therefore, we obtain the exact sequence of G-modules (by duality)

$$0\to J_G\to X(T_2')\to\mathbb{Z}\oplus\mathbb{Z}\to 0. \tag{2.7}$$

We are ready to show

THEOREM 2.8. *Let K/k be a Galois extension of arbitrary fields with bicyclic group $G = C_m \times C_n$. Then the k-tori $R^1_{K/k}G_m$, T_2' and T_2 are k-stably birationally equivalent. If $m = n = 2$, the torus $R^1_{K/k}\mathbb{G}_m$ is also k-stably birationally equivalent to the torus S.*

Proof. From the exact sequences (2.1), (2.2), we get the commutative diagram of G-modules with exact rows

$$\begin{array}{ccccccc} & X(T_2') & \longrightarrow & \mathbb{Z}G\cdot u(s)\oplus \mathbb{Z}G\cdot u(t) & \xrightarrow{d} & I_G & \longrightarrow 0 \\ & \downarrow{\scriptstyle res(u)} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle id.} & \\ 0\longrightarrow & X(T_2) & \longrightarrow & \bigoplus_{r\in G}\mathbb{Z}G\cdot u(r) & \xrightarrow{d'} & I_G & \end{array}$$

where u is the obvious inclusion. Using the snake lemma, we get the exact sequence

$$0 \to X(T_2') \to X(T_2) \to \bigoplus_{r\neq s,t} \mathbb{Z}G\cdot u(r) \to 0. \tag{2.9}$$

From the sequences (2.7), (2.9) and the criterion ([3], lemme 7), we see that $\rho(J_G) = \rho(X(T_2')) = \rho(X(T_2))$, which proves the first assertion (cf. section 1). The same goes for the statement about $m = n = 2$ using sequence (2.4).

COROLLARY 2.10. *Let K/k be a Galois extension of global fields with bicyclic group $G = C_m \times C_n$. Then we have the identifications $\text{Ш}(R^1_{K/k}\mathbb{G}_m) = \text{Ш}(T_2') = \text{Ш}(T_2) = H^3(G, K^*)$. If $m = n = 2$, we have moreover $\text{Ш}(R^1_{K/k}\mathbb{G}_m) = \text{Ш}(S) = H^1(G, S(K))$.*

Proof. This follows from the invariance of Ш under k-stable birational equivalence of algebraic tori ([3], prop. 18). The identification $\text{Ш}(T_2) = H^3(G, K^*)$ is obtained as follows. We have the exact sequences

$$0 \to X(T_1) = I_G \to \mathbb{Z}G \to \mathbb{Z} \to 0,$$

$$0 \to X(T_2) \to \bigoplus_{r\in G} \mathbb{Z}G\cdot u(r) \to X(T_1) \to 0.$$

By application of the functor Hom $(\cdot, K^*)$ we obtain the exact sequences $(U(\cdot) =$

functor "units")

$$0 \to K^* \to U(K \otimes_k K) \to T_1(K) \to 0,$$

$$0 \to T_1(K) \to \prod_{|G| \text{times}} U(K \otimes_k K) \to T_2(K) \to 0.$$

Since $H^n(G, U(K \otimes_k K)) = 0$ for all n, we deduce from the long exact sequences of cohomology that $H^1(G, T_2(K)) = H^2(G, T_1(K)) = H^3(G, K^*)$. Let A_k be the adele ring of K and let J_K be the idele group of K. By the same chain of arguments as above (application of the functor Hom $(\cdot, J_K)$), we get

$$\prod_{v \in P} H^1(G_v, T_2(K_w)) = H^1(G, T_2(A_K)) = H^2(G, T_1(A_K)) = H^3(G, J_K).$$

From class field theory, we have that $H^3(G, J_K) = 0$. It follows that $\text{Ш}(T_2) = H^1(G, T_2(K)) = H^3(G, K^*)$. The identification $\text{Ш}(S) = H^1(G, S(K))$ is the fact that the principcal homogeneous spaces under S have everywhere locally rational points (e.g. [2], exercise 5).

Remark 2.11. Concerning the case $m = n = 2$, we observe that the arithmetic structure of $H^1(G, S(K)) = k^*/\prod_{i=1}^3 N_i K_i^*$ is known ([2], exercise 5). The author thinks that the norm torus $S = T_2'$ (see prop. 2.12), the Klein norm torus $R^1_{K/k}\mathbb{G}_m$ and the corresponding T_2, are the only examples of (linear) algebraic groups whose non-trivial Tate–Shafarevich group structure is entirely understood. A more detailed analysis of the situation leads even to a complete solution of the Hasse problem for norm forms in the biquadratic bicyclic case. A study on this subject will appear elsewhere.

We conclude this section with a more precise result when $m = n = 2$.

PROPOSITION 2.12. *Let K/k be a Galois extension of fields with group $G = C_2 \times C_2$. Then the algebraic k-tori T_2' and S are k-isomorphic.*

Proof. It suffices to show that $X(Q)^0$ and $X(S)^0$ are isomorphic G-modules. The integral representation associated to the basis $(e_i)_{1 \leq i \leq 5}$ of $X(S)^0$ is expressed in matrix form by

$$s \mapsto \begin{pmatrix} T(s) & L_1(s) \\ 0 & U(s) \end{pmatrix}, \qquad t \mapsto \begin{pmatrix} T(t) & L_1(t) \\ 0 & U(t) \end{pmatrix},$$

where

$$T(s)=\begin{pmatrix}-1 & & 0\\ & 1 & \\ 0 & & -1\end{pmatrix},\quad T(t)=\begin{pmatrix}-1 & & 0\\ & -1 & \\ 0 & & 1\end{pmatrix},$$

$$L_1(s)=\begin{pmatrix}-1 & -1\\ 0 & 0\\ 0 & 1\end{pmatrix},\quad L_1(t)=\begin{pmatrix}-1 & -1\\ 1 & 0\\ 0 & 0\end{pmatrix},$$

and $U(s)=U(t)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. On the other hand, the $\mathbb{Z}$-basis of $X(Q)^0$ $(1-s,0)+U$, $(s-t,0)+U$, $(1-s,1-s)+U$, $(t,1+s)+U$, $(0,1)+U$, provides the matrices

$$s\mapsto\begin{pmatrix}T(s) & L_2(s)\\ 0 & U(s)\end{pmatrix},\quad t\mapsto\begin{pmatrix}T(t) & L_2(t)\\ 0 & U(t)\end{pmatrix},$$

where

$$L_2(s)=\begin{pmatrix}1 & 1\\ 0 & 0\\ 0 & -1\end{pmatrix},\quad L_2(t)=\begin{pmatrix}1 & 1\\ 1 & 0\\ 0 & 0\end{pmatrix}.$$

It is immediate that $L_2(s)-L_1(s)=T(s)D-DU(s)$, $L_2(t)-L_1(t)=T(t)D-DU(t)$, where

$$D=\begin{pmatrix}-1 & -1\\ 0 & 0\\ 0 & 1\end{pmatrix}.$$

Using the criterion ([4], (73.21)), we see that the representations $\begin{pmatrix}T & L_1\\ 0 & U\end{pmatrix}$ and $\begin{pmatrix}T & L_2\\ 0 & U\end{pmatrix}$ are $\mathbb{Z}$-equivalent, that is $X(S)^0$ and $X(Q)^0$ are isomorphic G-modules.

3. A norm torus satisfying the Hasse principle and the weak approximation

Let K/k be a finite Galois extension of group $G=C\times H$ where C is cyclic and H is a finite group. Let $K_1=K^C$, $K_2=K^H$, $N_1=N_{K_1/k}$ and $N_2=N_{K_2/k}$. For an abelian group A, we denote its dual $\operatorname{Hom}(A,\mathbb{Q}/\mathbb{Z})$ by $\tilde{A}$.

The exact sequence of G-modules

$$0 \to \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}[G/C] \oplus \mathbb{Z}[G/H] \to X(T) \to 0, \tag{3.1}$$

where $\varphi(1) = (\sum_{h \in H} h, -\sum_{c \in C} c)$, defines the k-torus T corresponding to the norm equation $N_1(x) \cdot N_2(y) = 1$, x, y indeterminates in K_1 repsectively K_2. We let

$$0 \to X(T) \to P \to X(S) \to 0 \tag{3.2}$$

be a flasque resolution of $X(T)$, i.e. P is a permutation module and $X(S)$ is a flasque module.

The following simple result is appropriate to demonstrate the usefulness of algebraic tori for the problem of existence of rational points in Diophantine geometry.

PROPOSITION 3.3. *Let K/k be a finite Galois extension of global fields with group $G = C \times H$, C cyclic. Then the norm k-torus T corresponding to $N_1N_2 = 1$ satisfies the Hasse principle and the weak approximation, i.e.* $Ш(T) = A(T) = 0$.

Proof (following a method due to J.-J. Sansuc, private communication). Since $X(S)$ is flasque, we have $H^{-1}(G', X(S)) = H^1(G', X(S)) = 0$ for all cyclic subgroups G' of G. From the long exact sequence of cohomology associated to (3.2), we get the commutative square

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1(G, X(S)) & \xrightarrow{\delta} & H^2(G, X(T)) \\ & & \downarrow{\scriptstyle \mathrm{res}_1} & & \downarrow{\scriptstyle \mathrm{res}_2} \\ 0 & = & H^1(C, X(S)) & \xrightarrow{\delta'} & H^2(C, X(T)). \end{array}$$

It suffices to show that res_2 is injective. We have then $H^1(G, X(S)) = 0$ and the assertion follows in view of the exact sequence ([3], prop. 19):

$$0 \to A(T) \to H^1(G, X(S))^{\sim} \to Ш(T) \to 0.$$

Now the exact sequence of Hochschild–Serre (e.g. [5], p. 355) tells that $\mathrm{Ker}(\mathrm{res}_2) = H^2(G/H, X(T)^C)$ (use that $H^1(C, X(T)) = 0$: the sequence (3.1) as a sequence of C-modules is split). As $H^1(C, \mathbb{Z}) = 0$, we have from (3.1) the exact sequence of G/C-modules

$$0 \to \mathbb{Z} \to \mathbb{Z}[G/C] \oplus \mathbb{Z} \to X(T)^C \to 0, \tag{3.4}$$

which is split as a sequence of G/C-modules. Therefore we have $\mathbb{Z} \oplus X(T)^C \cong \mathbb{Z} \oplus \mathbb{Z}[G/C]$. As $\mathbb{Z}[G/C]$ is G/C-induced, we have in particular $H^2(G/C, \mathbb{Z}[G/C]) = 0$. It follows easily that $H^2(G/C, X(T)^C) = 0$ as wanted.

Remark 3.5. Concretely, this proposition says that the equation $N_1(x)N_2(y) = c$, $c \in k^*$, which is a principal homogeneous space under T, satisfies the Hasse principle and that for $c = 1$ weak approximation holds. The referee of "Inventiones mathematicae", which I thank here warmly for his useful remarks, has suggested to generalize prop. 3.3 to norm equations $N_{K_1/k}(x)N_{K_2/k}(y) = c$, $c \in k^*$, K_1/k cyclic, K_2/k arbitrary (not necessarily Galois). For this, extend our proof by looking at the method developed by Tasaka in *Remarks on the validity of Hasse's norm theorem*, J. Math. Soc. Japan *22* (1970), 330–341.

We come to our applications. Let $n \geq 2$ be a natural number and let $G = C_n \times C_n$ be a bicyclic group of order n^2. The class of all diagonal surfaces in $\mathbb{P}^3(k)$ of the form

$$ax^n + by^n + cz^n + dw^n = 0, \tag{3.6}$$

where a, b, c, $d \in k^*$, is certainly of fundamental interest. Using a trick of Selmer (case of cubic surfaces), we can write (3.6) in the form

$$x^n + (b/a)y^n + (c/a)(z^n + (d/c)w^n) = 0. \tag{3.7}$$

Define α, β by

$$\alpha^n = \pm(d/c),\ \beta^n = \pm(b/a) \text{ (choice of sign below)}, \tag{3.8}$$

and assume that the extension of fields $K = k(\alpha, \beta)$ is Galois over k of degree n^2. After appropriate choice of sign in (3.8), the equation (3.7) can be written as

$$-(c/a)N_1(z + \alpha w) = N_2(x + \beta y). \tag{3.9}$$

Let $L \supset k$ be a field extension. An equation of the form $0 \neq rN_1 = N_2$, $r \in k^*$, has a L-rational point if and only if the equation $r = N_1N_2$ has a L-rational point. This remark plays an important role in the subsequent results. First of all, we obtain a new proof of the classical Hasse principle for quadratic forms in 4 variables.

COROLLARY 3.10. *Let a, b, c, d belong to the global field k and assume* $abcd \neq 0$. *Then the quadratic form* $ax^2+by^2+cz^2+dw^2=0$ *satisfies the Hasse principle.*

Proof. If K/k is of degree 4, the assertion follows from the validity of Hasse's principle for the norm torus T associated to $N_1N_2=1$ (prop. 3.3). Indeed an equation of the form $N_1N_2=r$, $r \in k^*$, is a principcal homogeneous space under T, and its class in the Tate–Shafarevich group $Ш(T)=0$ is trivial, so it satisfies the Hasse principle. Otherwise (except for trivial cases), the equation (3.7) for $n=2$ can be reduced, using composition of binary quadratic forms, to a norm form of a quadratic extension, which satisfies the Hasse principle.

Remark 3.11. We note that the proof does not depend on Dirichlet's theorem on the existence of prime numbers in arithmetic progressions, which is usually the case (see the proofs by Borevich and Shafarevich in "Number Theory" and Serre in "A Course in Arithmetic"). However our point of view is heavily based on Tate–Nakayama duality, one of the non-trivial facts of class field theory. Another proof, which does not use Dirichlet's theorem, is given in ([2], exercise 4): reduction to the case of 3 variables and then Hasse norm theorem for quadratic extensions.

In general, we obtain a criterion of non-existence of rational points in completions of global fields.

COROLLARY 3.12. *Let a, b, c, d belong to the global field k and assume* $abcd \neq 0$, K/k *Galois of degree* n^2. *If* $-(c/a) \notin N_1K_1^* \cdot N_2K_2^*$, *then there exists some completion* k_v *of k such that the diagonal surface* $ax^n+by^n+cz^n+dw^n=0$ *has no* k_v*-rational point.*

Proof. We show the contraposition. Assume that the diagonal surface $ax^n+by^n+cz^n+dw^n=0$ has k_v-rational points for all places v of k. Then the equation (3.9) as well as the equation $N_1(x)N_2(y)=-(c/a)$ have everywhere locally points. But this last equation is a principal homogeneous space under the norm k-torus associated to the norm form $N_1(x)N_2(y)=1$. By prop. 3.3 (validity of the Hasse principle), the equation $N_1(x)N_2(y)=-(c/a)$ has a solution, i.e. $-(c/a) \in N_1K_1^* \cdot N_2K_2^*$.

Remark 3.13. Though obvious, this result is of some interest. Indeed, it asserts that the candidates to counterexamples to Hasse's principle for diagonal surfaces of arbitrary degree are among those equations for which $-(c/a) \in N_1K_1^* \cdot N_2K_2^*$. The interested reader should for example look at the counterexamples of Cassels and Guy (1966) and Bremner (1978) for diagonal cubic surfaces.

REFERENCES

[1] A. Borel, Linear Algebraic Groups, New York (1969).

[2] J. W. S. Cassels and A. Fröhlich (editors), Algebraic Number Theory, Academic Press, London and Thompson Publ. Co., Washington (1967).

[3] J.-L. Colliot-Thélène et J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Scient. Ecole Norm. Sup. (4) *10*, 175–229 (1977).

[4] C. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, New York, Interscience (1962).

[5] S. MacLane, Homology, Berlin and New York, Springer (1963).

Forschungsinstitut für Mathematik
ETH-Zentrum
CH 8092 Zürich

Received November 29, 1983