An Alternative Proof of Scheiderer's Theorem on the Hasse Principle for Principal Homogeneous Spaces

Vladimir Chernousov[1]

Received: February 23, 1998
Revised: September 11, 1998

Communicated by Ulf Rehmann

Abstract. We give an alternative proof of the Hasse principle for principal homogeneous spaces defined over fields of virtual cohomological dimension at most one which is based on a special decomposition of elements in Chevalley groups.

1991 Mathematics Subject Classification: Primary 20G10; Secondary 11E72, 12D15.

1. Introduction

Let Y be a smooth irreducible projective curve defined over the real number field $\mathbb{R}$ and $k = \mathbb{R}(Y)$ be the field of $\mathbb{R}$-rational functions on Y. For a point $P \in Y(\mathbb{R})$ we denote the completion of k at the point P by k_P. The present paper is devoted to the Hasse principle for the existence of a rational point on principal homogeneous spaces of a connected linear algebraic group G defined over k. It was Colliot-Thélène who conjectured ([CT], Conjecture 2.9) that for any such space X the Hasse principle holds relative to all local fields k_P, $P \in Y(\mathbb{R})$, i.e. $X(k) \neq \emptyset$ iff $X(k_P) \neq \emptyset$ for each $P \in Y(\mathbb{R})$. Since principal homogeneous spaces of G are in natural one-to-one correspondence with elements of the set $H^1(k, G)$ the latter statement is equivalent to the following: the natural map of pointed sets

$$H^1(k,G) \longrightarrow \prod_{P \in Y(\mathbb{R})} H^1(k_P, G) \tag{1}$$

has trivial kernel ([S]).

In [CT] Colliot-Thélène proved the Hasse principle for algebraic k-tori and reduced the general case to that of a simple simply connected algebraic group G. The case of an arbitrary connected k-group G has been studied by Scheiderer ([Sch1]).

[1]The author gratefully acknowledges the support of the Alexander von Humboldt-Stiftung and SFB 343 "Diskrete Strukturen in der Mathematik" and the hospitality of the University of Bielefeld.

To prove the Hasse principle he first made an important observation (which eventually turned out to be crucial) that local objects k_P can be replaced by real closures k_ξ of k, $\xi \in \Omega_k$, where Ω_k denotes the set of all orderings of k. Indeed, using the description of orderings of k and the so-called Artin-Lang homomorphism theorem ([Srl], Theorem 3.1) it is easy to show that the condition $X(k_P) \neq \emptyset$ for each real point P on Y implies $X(k_\xi) \neq \emptyset$ for each ordering ξ of k and hence the triviality of the kernel of (1) follows immediately from the triviality of the kernel of

$$\theta :\ H^1(k, G) \longrightarrow \prod_{\xi \in \Omega_k} H^1(k_\xi, G) \tag{2}$$

The question whether θ is injective makes sense not only for the function fields of curves but also for an arbitrary field k and it turned out that θ is indeed injective if k has virtual cohomological dimension (vcd) at most 1 (recall that function fields in one variable over $\mathbb{R}$ are such). We have even more.

Theorem 1. (Scheiderer, [Sch1]) *Let K be any field of virtual cohomological dimension ≤ 1. Then the Hasse principle holds for any homogeneous K-space X of a connected linear algebraic K-group G.*

Scheiderer's proof can be divided into two parts. In the first one it is proved that for X as in the theorem (here G may even be not connected) there exists a principal homogeneous space Z which is everywhere locally trivial and dominates X. The strategy of the proof in this part going back to Springer ([S], [Sp]) consists of replacing X by a homogeneous space which dominates X and has a smaller stabilizer. It is worth mentioning that in this part most arguments do not use specific properties of K and so most of them are valid over an arbitrary perfect field.

The second part of Scheiderer's proof is devoted to the case of a principal homogeneous space. To treat such a space Scheiderer first constructs a locally constant sheaf of sets $\mathcal{H}^1(G)$ on Ω_K whose stalks are just the sets $H^1(K_\xi, G)$. Then he shows that there exists a natural bijection between the set of global sections of $\mathcal{H}^1(G)$ and $H^1(K, G)$. As a whole the proof in this part is quite complicated. It is based on using étale machinery and, in particular, strongly relies on results of the book [Sch2].

The aim of this paper is to provide a simpler and shorter self-contained proof which is based only on the Bruhat decomposition in semisimple algebraic groups and the so-called strong approximation property (SAP) of fields (see § 3). We show that in fact the Hasse principle follows immediately modulo two facts. Informally speaking one of them says that the kernel of the natural map $H^1(K, T) \to H^1(K, G)$, where G is an (absolutely) simple simply connected linear K-group and T is a K-torus splitting over $K(\sqrt{-1})$, can be parametrized by "good" rational functions (see § 2) and the other says that any field of virtual cohomological dimension ≤ 1 is an SAP field.

Acknowledgment. *The author is grateful to J.-P. Serre and the referee for remarks that helped to improve the initial exposition.*

2. Algebraic groups splitting over quadratic extensions

Throughout the section K denotes an arbitrary field of characteristic 0. Let G be an (absolutely) simple simply connected algebraic group of rank n defined over K

and splitting over quadratic extension $L = K(\sqrt{d})$. Let

$$\Theta = \mathrm{Gal}(L/K) = \langle \tau \mid \tau^2 = 1 \rangle.$$

Consider a Borel L-subgroup B such that $T = B \cap \tau(B)$ is a maximal torus which will be assumed for simplicity to be K-anisotropic. Since T is splitting over L, one has

$$T \simeq \mathrm{R}^{(1)}_{L/K}(\mathrm{G}_m) \times \ldots \times \mathrm{R}^{(1)}_{L/K}(\mathrm{G}_m).$$

To prove the Hasse principle we need to describe $\mathrm{Ker}\,[H^1(\Theta, T(L)) \to H^1(\Theta, G(L))]$. This description can be easily extracted from [Ch]. However this paper is written in Russian and the translation made by the AMS is unreadable and contains a lot of misprints. So for the sake of expository completeness and the reader's convenience we include here details.

First recall some basic facts about the structure of the group $G(L)$ (for details see [St1]). Let $\Sigma = R(T, G)$ be the root system of G relative to T. The Borel subgroup B determines an ordering on the set Σ and hence a system of simple roots $\Pi = \{\alpha_1, \ldots, \alpha_n\}$. If $\alpha = \sum n_i \alpha_i \in \Sigma^+$, then the number $\mathrm{ht}(\alpha) = \sum n_i$ is called the height of α. If $\{X_\alpha, \alpha \in \Sigma; H_{\alpha_1}, \ldots, H_{\alpha_n}\}$ is a Chevalley basis of the Lie algebra of G, then $G(L)$ is generated by the corresponding root subgroups $G_\alpha = \langle x_{\pm\alpha}(t) \mid t \in L \rangle$, where

$$x_\alpha(t) = \sum_{n=0}^{\infty} t^n X_\alpha^n / n! \ ,$$

and the torus T is generated by $T_\alpha = T \cap G_\alpha = \langle h_\alpha(t) \rangle$, where $h_\alpha(t) = w_\alpha(t) w_\alpha(1)^{-1}$ and $w_\alpha(t) = x_\alpha(t) x_{-\alpha}(-t^{-1}) x_\alpha(t)$.

Furthermore, since G is simply connected the following relations hold in G (cf. [St1], Lemma 28 b), Lemma 20 c), Lemma 15):

A) $T = \langle h_{\alpha_1}(t_1) \rangle \times \cdots \times \langle h_{\alpha_n}(t_n) \rangle$ and for $\alpha \in \Sigma$ we have

(3) $$h_\alpha(t) = \prod_{i=1}^{n} h_{\alpha_i}(t)^{n_i}, \qquad \text{where } H_\alpha = \sum_{i=1}^{n} n_i H_{\alpha_i};$$

B) For $\alpha, \beta \in \Sigma$ let $\langle \beta, \alpha \rangle = 2(\beta, \alpha)/(\alpha, \alpha)$. Then we have

(4) $$h_\alpha(t) x_\beta(u) h_\alpha(t)^{-1} = x_\beta(t^{\langle \beta, \alpha \rangle} u)$$

C) For all $u, v \in L$ such that $1 + uv \neq 0$ we have

(5) $$x_{-\alpha}(u) x_\alpha(v) = x_\alpha(v(1+uv)^{-1}) h_\alpha(1+uv)^{-1} x_{-\alpha}(u(1+uv)^{-1})$$

D) For all $\alpha, \beta \in \Sigma$, $\beta \neq -\alpha$, we have

(6) $$x_\alpha(v) x_\beta(u) x_\alpha(v)^{-1} x_\beta(u)^{-1} = \prod_{i,j>0} x_{i\alpha + j\beta}(c_{i,j} v^i u^j)$$

where the product on the right hand side is taken over all roots of the form $i\alpha + j\beta$ and the $c_{i,j}$ are integers which depend on α, β and on the chosen ordering of the roots but do not depend on v and u.

Since T is K-defined, τ acts on the root system Σ. More exactly, for any $\alpha \in \Sigma$ the character $\alpha + \tau(\alpha)$ is K-defined and hence is zero, i.e. $\tau(\alpha) = -\alpha$, since, by assumption, T is K-anisotropic. It follows that there exists $c_\alpha \in L^*$ such that $\tau(X_\alpha) = c_\alpha X_{-\alpha}$; in particular, the subgroup G_α is K-defined.

The constants c_α actually lie in K and $c_{-\alpha} = c_\alpha^{-1}$. Indeed, for rank one groups, i.e. of the form SL $(1, D)$, where D is a quaternion K-algebra, this fact can be verified directly. The general case easily reduces to the rank one case since G_α is a simple simply connected K-group of rank 1. Thus, we have

LEMMA 1. *There exists constant $c_\alpha \in K^*$ such that for any $u \in L$ one has $\tau(x_\alpha(u)) = x_{-\alpha}(c_\alpha \tau(u))$. Moreover, $G_\alpha \simeq SL(1, D)$, where D is a quaternion algebra over K of the form $D = (d, c_\alpha)$.*

PROOF: Straightforward computations. □

LEMMA 2. *The positive roots $\Sigma^+ = \{\beta_1, \dots, \beta_m\}$ can be ordered in such a way that the following two properties hold:*
1) for any pair of roots β_i, β_j, for which $i < j$ and $\beta_i + \beta_j = \beta_k \in \Sigma^+$, the root β_k is between β_i and β_j, i.e. $i < k < j$;
2) if Σ is a root system of type either A_{2n-1} or D_n or E_6 and σ is the outer automorphism of Σ induced by the non-trivial automorphism of order 2 (resp. 3) of the corresponding Dynkin diagram, then for any root $\beta_i \in \Sigma^+$ the roots β_i and $\sigma(\beta_i)$ (resp. β_i, $\sigma(\beta_i)$, $\sigma^2(\beta_i)$) are neighbours.

PROOF. a) Let $\Sigma = \{\varepsilon_i - \varepsilon_j \mid 1 \leq i \neq j \leq 2n\}$ be a root system of type A_{2n-1}. Let $\alpha_1 = \varepsilon_1 - \varepsilon_2, \dots, \alpha_{2n-1} = \varepsilon_{2n-1} - \varepsilon_{2n}$ be a basis of Σ and Σ_1 be the subsystem generated by the roots $\alpha_2, \dots, \alpha_{2n-2}$. By induction, we can pick an ordering $\Sigma_1^+ = \{\beta_1, \dots, \beta_k\}$ with the required properties. Let $\gamma = \alpha_1 + \cdots + \alpha_{2n-1}$. We number the remaining roots $\Sigma^+ \setminus \{\Sigma_1^+ \cup \gamma\} = \{\beta_{k+1}, \dots, \beta_{m-1}\}$ in the order of decreasing height. If β_i denotes the last root among $\{\beta_{k+1}, \dots, \beta_{m-1}\}$ such that ht $(\beta_i) \geq n$, then the ordering

$$\Sigma^+ = \{\beta_1, \dots, \beta_k, \beta_{k+1}, \dots, \beta_i, \gamma, \beta_{i+1}, \dots, \beta_{m-1}\}$$

is as required.

b) Σ is a root system of type $A_{2n}, B_n, C_n, D_n, E_7$. It follows from the description of root systems of these types that there exists a subsystem Σ_1 generated by $n-1$ simple roots, say $\alpha_1, \dots, \alpha_{n-1}$, such that any root $\beta \in \Sigma^+ \setminus \Sigma_1^+$ can be written as a sum $\beta = m_1\alpha_1 + \cdots + m_{n-1}\alpha_{n-1} + \alpha_n$. If Σ is of type D_n and $|\sigma| = 2$, we may assume in addition that the set $\{\alpha_1, \dots, \alpha_{n-1}\}$ is stable under σ. The root system Σ_1 has rank $n-1$ and so by induction, there exists an ordering of the required type on the set $\Sigma_1^+ = \{\beta_1, \dots, \beta_k\}$. We number the remaining roots $\Sigma^+ \setminus \Sigma_1^+ = \{\beta_{k+1}, \dots, \beta_m\}$ in the order of decreasing height. Then the ordering $\{\beta_1, \dots, \beta_m\}$ is as required.

c) Σ is a root system of type E_6, E_8, F_4, G_2. Here one can argue as in case a). Namely, there exists a subsystem Σ_1 generated by simple roots $\alpha_1, \dots, \alpha_{n-1}$ such that any root $\beta \in \Sigma^+ \setminus \Sigma_1^+$ is of the form $\beta = m_1\alpha_1 + \cdots + m_{n-1}\alpha_{n-1} + \alpha_n$ except for the maximal root $\tilde{\alpha}$ and $\tilde{\alpha}$ is of the form $\tilde{\alpha} = m_1\alpha_1 + \cdots + m_{n-1}\alpha_{n-1} + 2\alpha_n$. Let $b = \text{ht}\,(\tilde{\alpha})$. Again, applying induction we can find an ordering $\Sigma_1^+ = \{\beta_1, \dots, \beta_k\}$ with the desired properties and then we number the roots $\Sigma^+ \setminus \{\Sigma_1^+ \cup \tilde{\alpha}\} = \{\beta_{k+1}, \dots, \beta_{m-1}\}$ in the order of decreasing height. If Σ has type E_6, we may assume in addition that β and $\sigma(\beta)$ are neighbours for all $\beta \in \Sigma^+$. Let β_i be the last root among $\{\beta_{k+1}, \dots, \beta_{m-1}\}$

such that $\mathrm{ht}\,(\beta_i) \geq b/2$. We claim that the ordering

$$\Sigma^+ = \{\beta_1, \dots, \beta_k,\, \beta_{k+1}, \dots, \beta_i,\, \tilde{\alpha},\, \beta_{i+1}, \dots, \beta_{m-1}\}$$

has the desired properties. Indeed, if $\beta_j = \beta_s + \beta_t$, where $s < t$ and $j \in \{k+1, \dots, m-1\}$, then clearly β_s belongs to Σ_1^+. It follows that β_j lies between β_s and β_t, since $\mathrm{ht}\,(\beta_j) \geq \mathrm{ht}\,(\beta_s), \mathrm{ht}\,(\beta_t)$. Now let $\tilde{\alpha} = \beta_s + \beta_t$, $s < t$,. Then $s, t \in \{k+1, \dots, m-1\}$ and $\mathrm{ht}\,(\beta_s) \geq b/2$, $\mathrm{ht}\,(\beta_t) < b/2$ (we use the fact that $\mathrm{ht}(\tilde{\alpha})$ is odd), implying $\tilde{\alpha}$ is also between β_s and β_t.

d) Σ has type D_4 and $|\sigma| = 3$. Let $\alpha_1, \dots, \alpha_4$ be simple roots such that σ permutes $\alpha_1, \alpha_3, \alpha_4$. Then the required ordering is as follows: first we place α_2, then all roots of the height 2, then the maximal root and then the roots of heights 3, 4, 1 respectively. □

Corollary 1. *Let β_i, β_j, $j < i$, be any two positive roots. Then for any positive root β_k of the form $\beta_k = r\beta_j - l\beta_i$, $r, l > 0$, one has $k < j$. Analogously, for any negative root of the form $-\beta_k = r\beta_j - l\beta_i$, $r, l > 0$, one has $k > i$.*

Proof. We distinguish three cases.

a) $\langle \beta_i, \beta_j \rangle_{\mathbb{Q}} \cap \Sigma$ has type A_2. Then $r = l = 1$ and hence if $\beta_k = \beta_j - \beta_i$ is a positive root then $\beta_k + \beta_i = \beta_j$, implying $k < j < i$. Analogously, if $\beta_j - \beta_i = -\beta_k$ then we have $j < i < k$.

b) $\langle \beta_i, \beta_j \rangle_{\mathbb{Q}} \cap \Sigma$ has type B_2. Then either $r = l = 1$ or $r = 1$ and $l = 2$ or $r = 2$ and $l = 1$. The case $r = l = 1$ was already handled in part a). Now let $\beta_k = \beta_j - 2\beta_i$. Then $\beta_j - \beta_i = \beta_s$ is also a positive root implying $s < j$. Futhermore, $\beta_k = \beta_s - \beta_i$ and $s < j < i$. So again we have $k < s < j$. The remaining cases can be handled in a similar way.

c) $\langle \beta_i, \beta_j \rangle_{\mathbb{Q}} \cap \Sigma$ has type G_2. Here the proof is similar to that of case b) and we omit it. □

Proposition 1. *Fix an order in Σ^+ as in Lemma 2. Then the regular map*

$$\omega : \mathbb{G}_m^n \times \mathbb{A}^{2m} \longrightarrow G\,, \qquad (t_1, \dots, t_n, u_1, \dots, u_m, v_1, \dots, v_m) \longrightarrow$$
$$\prod_{i=1}^{n} h_{\alpha_i}(t_i)\, x_{-\beta_1}(u_1) x_{\beta_1}(v_1) \cdots x_{-\beta_m}(u_m) x_{\beta_m}(v_m)$$

is birational over L.

Remark 1. This statement is also true in positive characteristic. There is the only place which require additional work: one need additionally to check that ω is a separable map.

Proof. Both sides have the same dimension and hence it suffices to prove the injectivity of ω on some Zariski open subset, since $\mathrm{char}\, K = 0$.

First we show that for any integer i and any parameters $u_1, \dots, u_i$ and $v_1, \dots, v_i$ from some Zariski open subset the element

$$A_i = x_{-\beta_1}(u_1) x_{\beta_1}(v_1) \cdots x_{-\beta_i}(u_i) x_{\beta_i}(v_i)$$

of the group G can be written in the form

$$A_i = \prod_{k=1}^{n} h_{\alpha_k}(f_k) \prod_{j=1}^{m} x_{-\beta_j}(r_j) \prod_{j=1}^{i-1} x_{\beta_j}(s_j)\, x_{\beta_i}(v_i),$$

where f_k, r_j, s_j are rational functions depending on $u_1, \dots, u_i$, $v_1, \dots, v_{i-1}$.

If $i=1$ there is nothing to prove. By induction, we may write A_{i-1} in the form

$$\prod_{k=1}^{n} h_{\alpha_k}(f_k) \prod_{j=1}^{m} x_{-\beta_j}(r_j) \prod_{j=1}^{i-2} x_{\beta_j}(s_j)\, x_{\beta_{i-1}}(v_{i-1}).$$

To write $A_i = A_{i-1}\, x_{-\beta_i}(u_i)\, x_{\beta_i}(v_i)$ in the same form we have to transpose $x_{-\beta_i}(u_i)$ with each factor in the product $\prod_{j=1}^{i-2} x_{\beta_j}(s_j)\, x_{\beta_{i-1}}(v_{i-1})$. By (6) and by Corollary 1, every time doing so we obtain additional factors $x_{\beta_s}(\,)$ or $x_{-\beta_s}(\,)$, where $s < i-1$ in the first case and $s > i$ in the second case. Collecting together all these factors corresponding to negative roots we can write the element $\prod_{j=1}^{i-2} x_{\beta_j}(s_j)\, x_{\beta_{i-1}}(v_{i-1})\, x_{-\beta_i}(u_i)$ in the form

$$\prod_{k=1}^{n} h_{\alpha_i}(\tilde{f}_k) \prod_{j=1}^{m} x_{-\beta_j}(\tilde{r}_j) \prod_{j=1}^{i-1} x_{\beta_j}(\tilde{s}_j)$$

and so our claim follows.

Now we are ready to prove the injectivity of ω. Suppose that

$$\omega(t_1, \dots, t_n,\, u_1, \dots, u_m,\, v_1, \dots, v_m) = \omega(\tilde{t}_1, \dots, \tilde{t}_n,\, \tilde{u}_1, \dots, \tilde{v}_m) \tag{7}$$

From the above argument and the Bruhat decomposition we get immediately $v_m = \tilde{v}_m$. To show that $u_m = \tilde{u}_m$, we use (4), (5). Namely, it follows from (4), (5) that the left hand side of (7) may be written in the form

$$\prod_{i=1}^{n} h_{\alpha_i}(f_i)\, [x_{\beta_1}(s_1)\, x_{-\beta_1}(r_1)] \cdots [x_{\beta_{m-1}}(s_{m-1})\, x_{-\beta_{m-1}}(r_{m-1})]$$

$$x_{\beta_m}[v_m(1+u_m v_m)]\, x_{-\beta_m}[u_m(1+u_m v_m)^{-1}]\,,$$

where $f_1, \dots, f_n$, $s_1, \dots, s_{m-1}$, $r_1, \dots, r_{m-1}$ are rational functions. Rewriting the right hand side of (7) in the same form we conclude that

$$u_m(1+u_m v_m)^{-1} = \tilde{u}_m(1+\tilde{u}_m \tilde{v}_m)^{-1},$$

hence $u_m = \tilde{u}_m$. After cancelling the factor $x_{-\beta_m}(u_m)\, x_{\beta_m}(v_m)$ in (7) the same argument shows that $v_{m-1} = \tilde{v}_{m-1}$, $u_{m-1} = \tilde{u}_{m-1}$ and so on. □

Now we are in position to formulate the main result of the section.

THEOREM 2. *Let $g \in G(L)$ be such that $g^{1-\tau} \in T(L)$. Then there exist quaternion algebras $D_1, \dots, D_m$ over K and elements $w_1, \dots, w_m \in K$ which are reduced norm of $D_1, \dots, D_m$ respectively and elements $t_1, \dots, t_n \in L$ such that*

$$g^{1-\tau} = \prod_{i=1}^{n} h_{\alpha_i}(t_i \tau(t_i)) \prod_{i=1}^{m} h_{\beta_i}(w_i)$$

PROOF. If $g^{1-\tau} \in T(L)$, then for any $x \in G(K)$ one has $g^{1-\tau} = (gx)^{1-\tau}$. Since $G(K)$ is Zariski dense in G, we may always assume that our element g is in "generic" position by which we mean point in some Zariski open subset $U \subset G$ which can be easily specified from the argument. So let

$$g = \prod_{i=1}^{n} h_{\alpha_i}(t_i)\, x_{-\beta_1}(u_1) x_{\beta_1}(v_1) \cdots x_{-\beta_m}(u_m) x_{\beta_m}(v_m)$$

where $t_i,\ u_i,\ v_i \in L$. Denote $t = \prod_{i=1}^{n} h_{\alpha_i}(t_i)$ and $g_i = x_{-\beta_i}(u_i)x_{\beta_i}(v_i)$, $i = 1, \dots, m$. Let also $t' = g^{1-\tau}$, so that

$$t \cdot g_1 \cdots g_m = t' \cdot \tau(t) \cdot \tau(g_1) \cdots \tau(g_m) \tag{8}$$

By Lemma 1, we have $\tau(g_i) \in G_{\beta_i}$. Then applying Proposition 1 we conclude that g_m and $\tau(g_m)$ coincide modulo $T_{\beta_m}(L) = T(L) \cap G_{\beta_m}$ and so the element $g_m^{\tau - 1}$ is of the form $h_{\beta_m}(w_m)$ for some parameter w_m. We claim that $w_m \in K$ and it is a reduced norm of the quaternion K-algebra $D_m = (d, d_{\beta_m})$, where $d_{\beta_m} = c_{\beta_m}$. Indeed, by construction the cocycle $(g_m^{\tau-1}) \in Z^1(\Theta, T_{\beta_m}(L))$ is trivial in $Z^1(\Theta, G_{\beta_m}(L))$ and by Lemma 1, $G_{\beta_m} \simeq SL(1, D_m)$, hence our claim follows.

Substituting $\tau(g_m) = h_{\beta_m}(w_m) \cdot g$ in (8) and cancelling g, we have then

$$t \cdot g_1 \cdots g_{m-1} = t' \cdot \tau(t) \cdot h_{\beta_m}(w_m) \cdot [h_{\beta_m}(w_m)^{-1}\tau(g_1)h_{\beta_m}(w_m)] \cdots$$
$$\cdots [h_{\beta_m}(w_m)^{-1}\tau(g_{m-1})h_{\beta_m}(w_m)]$$

Applying again Proposition 1 and arguing analogously we have

$$[h_{\beta_m}(w_m)^{-1}\tau(g_{m-1})h_{\beta_m}(w_m)] = h_{\beta_{m-1}}(w_{m-1}) \cdot g_{m-1}$$

for some parameter w_{m-1}, which is again a reduced norm of the quaternion K-algebra $D_{m-1} = (d, d_{\beta_{m-1}})$, where

$$d_{\beta_{m-1}} = c_{\beta_{m-1}} w_m^{\langle \beta_{m-1}, \beta_m \rangle}.$$

To see it, let $\tilde{g}_{m-1} = h_{\beta_m}(w_m)^{-1}\tau(g_{m-1})h_{\beta_m}(w_m)$. Using (4) we have

$$\tilde{g}_{m-1} = x_{\beta_{m-1}}(c_{\beta_{m-1}}^{-1} w_m^{-\langle \beta_{m-1}, \beta_m \rangle}\tau(u_m)) \cdot x_{\beta_{m-1}}(c_{\beta_{m-1}} w_m^{\langle \beta_{m-1}, \beta_m \rangle}\tau(v_m)).$$

It follows that $(h_{\beta_{m-1}}(w_{m-1})) = (\tilde{g}_{m-1} \cdot g_{m-1}^{-1})$ can be viewed as a trivial cocycle in an K-group of rank 1 whose K-structure, i.e. action of τ, is given by the constant $d_{\beta_{m-1}}$. This fact combined with Lemma 1 implies w_{m-1} is a reduced norm of D_{m-1}, as claimed, and so on. Theorem 2 is proved. □

In § 4 we will also deal with a simple simply connected algebraic K-group G which is quasi-split over a quadratic extension L/K and for such a group we also need to describe elements of the form $g^{1-\tau} \in T(L)$, where $g \in G(L)$.

Clearly, K-groups of type ${}^2A_{2n}$ split over a quadratic extension of K. Since this case has been already handled, we may assume that G is an outer form of type not A_{2n}. As above, let B be an L-Borel subgroup B of G such that $T = B \cap \tau(B)$ is a maximal K-anisotropic torus.

Let F/K be the minimal extension over which G is an inner form and let $E = F \cdot L$. Let τ and σ be non-trivial automorphisms of E/K such that $\tau|_F = 1$ and $\sigma|_L = 1$ respectively. In the case ${}^{3,6}D_4$ by σ we denote any automorphism of order 3.

Clearly, σ induces an outer automorphism of the root system $\Sigma = \mathrm{R}\,(T, G)$ which will be denoted by the same letter. Let $\Lambda = \{\gamma_1, \dots, \gamma_s\} \subset \Sigma^+$ (resp. Λ') be a set of representatives of all orbits of σ in Σ^+ (resp. in Π). We divide Λ into two parts: $\Lambda_1 = \{\gamma_i \in \Lambda \mid \sigma(\gamma_i) = \gamma_i\}$ and $\Lambda_2 = \Lambda \setminus \Lambda_1$. Let also $\Lambda_i' = \Lambda' \cap \Lambda_i$, $i = 1, 2$. For $\gamma_i \in \Lambda_1$ (resp. Λ_2) we denote by H_i the subgroup in G generated by G_{γ_i} (resp. G_{γ_i}, $G_{\sigma(\gamma_i)}$ and $G_{\sigma^2(\gamma_i)}$, if $|\sigma| = 3$).

Lemma 3. *H_i is a simple simply connected K-group of type A_1 (resp. $A_1 \times A_1$ or $A_1 \times A_1 \times A_1$) if $\gamma_i \in \Lambda_1$ (resp. $\gamma_i \in \Lambda_2$ and $|\sigma| = 2$ or $|\sigma| = 3$).*

PROOF. It suffices to note that τ acts on Σ as either -1, if Σ has type D_{2n}, or $-\sigma$ otherwise, since it permutes positive and negative roots. Moreover, the combination $\beta_i \pm \sigma(\beta_i)$ is not a root, hence G_{γ_i} and $G_{\sigma(\gamma_i)}$ commute. □

THEOREM 3. *Let $g \in G(L)$ be such that $g^{1-\tau} \in T(L)$. Then there exist quaternion algebras $D_1, \ldots, D_s$ and elements $w_1, \ldots, w_s$ which are reduced norm of $D_1, \ldots, D_s$ respectively and elements $t_1, \ldots, t_p$ such that:*

1) If Σ is not of type ${}^{3,6}D_4$, then

$$g^{1-\tau} = \prod_{\alpha_i \in \Lambda_1'} h_{\alpha_i}(t_i\tau(t_i)) \prod_{\alpha_i \in \Lambda_2'} h_{\alpha_i}(t_i\tau(t_i))h_{\sigma(\alpha_i)}[\sigma(t_i)(\tau\circ\sigma)(t_i)]\cdot$$
$$\prod_{\gamma_i \in \Lambda_1} h_{\gamma_i}(w_i) \prod_{\gamma_i \in \Lambda_2} h_{\gamma_i}(w_i)h_{\sigma(\gamma_i)}(\sigma(w_i))$$

2) If Σ is of type ${}^{3,6}D_4$, then

$$g^{1-\tau} = \prod_{\alpha_i \in \Lambda_2'} h_{\alpha_i}(t_i\tau(t_i))h_{\sigma(\alpha_i)}[\sigma(t_i)(\tau\circ\sigma)(t_i)]h_{\sigma^2(\alpha_i)}[\sigma^2(t_i)(\tau\circ\sigma^2)(t_i)]\cdot$$
$$\prod_{\alpha_i \in \Lambda_1'} h_{\alpha_i}(t_i\tau(t_i)) \prod_{\gamma_i \in \Lambda_1} h_{\gamma_i}(w_i) \prod_{\gamma_i \in \Lambda_2} h_{\gamma_i}(w_i)h_{\sigma(\gamma_i)}(\sigma(w_i))h_{\sigma^2(\gamma_i)}(\sigma^2(w_i))$$

Here D_i is over K (resp. over F) and $w_i \in K$ (resp. F), if $\gamma_i \in \Lambda_1$ (resp. $\gamma_i \in \Lambda_2$), and $t_i \in L$ (resp. E), if $\alpha_i \in \Lambda_1'$ (resp. $\alpha_i \in \Lambda_2'$).

PROOF. As in the L-split case first we may assume that g is in "generic" position and so by property 2 in Lemma 2 and by Proposition 1, it can be written in the form $g = t\,g_1 \cdots g_s$, where $t \in T$, $g_i \in H_i$, $i = 1, \ldots, s$. Then the rest of the proof works exactly as in the L-split case, since by Lemma 3 all subgroups H_i are of the form $\mathrm{R}_{K'/K}(\mathrm{SL}(1, D))$, where D is a quaternion algebra over K' and K' is either F or K. □

3. SOME COHOMOLOGICAL COMPUTATIONS

From now on we assume that $\mathrm{vcd}\,(K) \leq 1$ and we let $L = K(\sqrt{-1})$. We also assume that the set Ω_K of all orderings on K is non-empty; this means, in particular, that char $K = 0$. Recall ([Srl]) that there is a canonical topology on Ω_K under which Ω_K is compact and totally disconnected.

REMARK 2. If $\Omega_K = \emptyset$, then -1 is a sum of squares in K and so $\mathrm{cd}\,(K) = \mathrm{cd}\,(K(\sqrt{-1})) \leq 1$ ([S], Ch. 2, Prop. 10′). Therefore, if $\Omega_K = \emptyset$, then by Steinberg's theorem ([St2]) one has $H^1(K, G) = 1$ for any connected linear algebraic K-group G.

To reduce the proof of the Hasse principle to the case of simply connected semisimple groups we need two auxiliary cohomological statements (Propositions 2 and 4 below) which are very particular cases of the general Theorem 12.13 in [Sch2]. Since we do not need to consider such a generality as in [Sch2] we include here the straightforward proofs of these statements.

Let A be a discrete Γ-module, where $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$, and let

$$\varphi_i : H^i(K, A) \to \prod_{\xi \in \Omega_K} H^i(K_\xi, A)$$

be the canonical map induced by res_{K_ξ}. We want to describe $\mathrm{Ker}\,\varphi_i$, $i \geq 2$, and $\mathrm{Im}\,\varphi_1$. To do so first remind that there is not a canonical way of choosing a real closure of K at $\xi \in \Omega_K$. If K_ξ and K'_ξ are two real closures of K at ξ, then by the theorem of Artin-Schreier ([Srl] Ch. 3, Theorem 2.1) there is a unique K-isomorphism $K_\xi \simeq K'_\xi$, hence there is an element $g \in \Gamma$ such that $g\tau_\xi g^{-1} = \tau'_\xi$, where τ_ξ (resp. τ'_ξ) is the involution (= element of order 2) in Γ corresponding to K_ξ (resp. K'_ξ) (in other words, there is a natural one-to-one correspondence between points of the set Ω_K and conjugacy classes of involutions in Γ).

The element g induces a natural map $\lambda_{i,g} : H^i(K_\xi, A) \to H^i(K'_\xi, A)$ and obviously we have $res_{K'_\xi} = \lambda_{i,g} \circ res_{K_\xi}$. It follows that the question on whether φ_i is injective does not depend on a choice of real closures K_ξ, $\xi \in \Omega_K$.

Clearly, any cocycle from $Z^1(K_\xi, A)$ is determined by the single element $a \in A$ such that $a\tau_\xi(a) = 1$. We will say that an element $\{a_\xi\}_{\xi\in\Omega_K} \in \prod_{\xi\in\Omega_K} H^1(K_\xi, A)$ is locally constant if there are a decomposition $\Omega_K = U_1 \cup \ldots \cup U_l$ into disjoint clopen (= open and closed) sets and elements $\{a_1, \ldots, a_l\}$ of A for which the following condition holds: for any $\xi \in U_i$ there are a cocycle c_ξ representing a_ξ and $g_\xi \in \Gamma$ such that the cocycle $\lambda_{1,g_\xi}(c_\xi)$ is determined by a_i. Analogously, for any $i \geq 1$ one defines the subset of elements in $\prod_{\xi\in\Omega_K} H^i(K_\xi, A)$ which are locally constant. We denote this subset by $\left(\prod_{\xi\in\Omega_K} H^i(K_\xi, A)\right)^{lc}$. Since for any $\zeta \in H^i(K, A)$ the element $\varphi_i(\zeta)$ is locally constant we denote by the same letter the canonical map

$$\varphi_i : H^i(K, A) \longrightarrow \left(\prod_{\xi\in\Omega_K} H^i(K_\xi, A)\right)^{lc} \subset \prod_{\xi\in\Omega_K} H^i(K_\xi, A)$$

Proposition 2. *If A is a finite discrete Γ-module, then the maps φ_i are injective for all integers $i \geq 2$.*

Proof. Since $H^i(L, A) = 1$, $i \geq 2$, the *"res-cores"* argument shows that $H^i(K, A)$ has exponent 2. So replacing A, if necessary, by its 2-Sylow subgroup we may assume that A is a 2-group. First examine the case $A = \mathbb{Z}/2\mathbb{Z}$.

Lemma 4. *Let $A = \mathbb{Z}/2\mathbb{Z}$. Then φ_i is surjective if $i \geq 1$ and injective if $i \geq 2$.*

Proof. Recall ([L], §17) that a field F is said to be an SAP field (strong approximation property) if for any two disjoint closed subsets $A, B \subset \Omega_F$ there exists an element $f \in F$ such that f is positive at all orderings in A, but negative at all orderings in B. We need

Proposition 3. ([L], Theorem 17.9) *If* $\mathrm{vcd}\,(K) \leq 1$, *then K is a SAP field.*

Surjectivity of φ_i, $i \geq 1$. In view of the periodicity of $H^i(K_\xi, \mathbb{Z}/2\mathbb{Z})$ it suffices to consider the cases $i = 1, 2$. If $i = 1$ then $H^1(K, \mathbb{Z}/2\mathbb{Z}) = K^*/K^{*2}$, hence the surjectivity of φ_1 follows immediately from Proposition 3. Furthermore, any element from $H^2(K, \mathbb{Z}/2\mathbb{Z})$ splits over L and so can be represented by a quaternion algebra having L as a maximal subfield. Then clearly, the surjectivity of φ_2 again follows from Proposition 3.

Injectivity of φ_i, $i \geq 2$. The proof is similar to that of [B-P], Lemma 2.3. Namely, by Arason's theorem ([A1], Satz 3), local triviality of $\zeta \in H^i(K, \mathbb{Z}/2\mathbb{Z})$ implies that $\zeta \cup (-1)^r = 0$ for some integer r, where $\cup$ denotes the cup product. On the other hand from the exact sequence

$$H^i(L,\mathbb{Z}/2\mathbb{Z}) \xrightarrow{cor} H^i(K,\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\cup(-1)} H^{i+1}(K,\mathbb{Z}/2\mathbb{Z}) \xrightarrow{res} H^{i+1}(L,\mathbb{Z}/2\mathbb{Z})$$

([A2], Corollary 4.6) and from the equalities

$$H^i(L,\mathbb{Z}/2\mathbb{Z}) = H^{i+1}(L,\mathbb{Z}/2\mathbb{Z}) = 1, \quad i \geq 2$$

we conclude that the product $\cup(-1)$ is an isomorphism. Therefore, $\zeta = 1$, as required. Lemma 4 is proved. □

We come back to an arbitrary finite 2-primary module A. Let Γ_2 be a Sylow 2-subgroup of Γ. Since the restriction map $H^i(K,A) \to H^i(\Gamma_2,A)$ is injective, after replacing Γ by Γ_2 we may assume that Γ is a pro-2-group. But for such a group any irreducible module is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ ([S], §4, Proposition 20). Therefore there exists a submodule $A' \subset A$ such that $A/A' = \mathbb{Z}/2\mathbb{Z}$. It induces the commutative diagram

$$\begin{array}{ccccc} H^i(K,\mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H^{i+1}(K,A') & \longrightarrow \\ \Big\downarrow \theta_1 & & \Big\downarrow \theta_2 & \\ \left(\prod_{\xi\in\Omega_K} H^i(K_\xi,\mathbb{Z}/2\mathbb{Z})\right)^{lc} & \longrightarrow & \left(\prod_{\xi\in\Omega_K} H^{i+1}(K_\xi,A')\right)^{lc} & \longrightarrow \end{array}$$

$$\begin{array}{ccc} H^{i+1}(K,A) & \longrightarrow & H^{i+1}(K,\mathbb{Z}/2\mathbb{Z}) \\ \Big\downarrow \theta_3 & & \Big\downarrow \theta_4 \\ \left(\prod_{\xi\in\Omega_K} H^{i+1}(K_\xi,A)\right)^{lc} & \longrightarrow & \left(\prod_{\xi\in\Omega_K} H^{i+1}(K_\xi,\mathbb{Z}/2\mathbb{Z})\right)^{lc} \end{array}$$

By what has been proved above, θ_1 (resp. θ_4) is surjective (resp. injective) and by induction, θ_2 is injective. It follows that θ_3 is injective as well. Proposition 2 is proved. □

PROPOSITION 4. *If A is a finite discrete Γ-module, then φ_1 is surjective.*

PROOF. Since φ_i, $i \geq 2$, are injective, one can easily verify that if the statement holds both for a submodule $A' \subset A$ and the quotient A/A', then it also holds for A. So we may assume, if necessary, that A is irreducible. It suffices to prove that for a given $\xi \in \Omega_K$ and an element $a \in A$ for which $a\tau_\xi(a) = 1$ there exist a small clopen neighbourhood $U \subset \Omega_K$ of ξ and a cocycle $\zeta \in Z^1(K,A)$ such that for a proper real closure $K_{\xi'}$ of K at ξ' the cocycle $\mathrm{res}_{K_{\xi'}}(\zeta)$ is determined by the element a if $\xi' \in U$, and is trivial otherwise.

We need the following simple property of orderings of K (see [Srl]):

if F/K is an extension of odd degree then for any ordering $\xi \in \Omega_K$ there is an extension of ξ to F; moreover, the restriction map $\phi : \Omega_F \to \Omega_K$ is a local homeomorphism.

Let E be a finite Galois extension of K over which A is a trivial module and let $F \subset E$ be the subfield corresponding to a Sylow 2-subgroup of $\mathrm{Gal}(E/K)$. Denote $\Delta = \mathrm{Gal}(\overline{K}/F)$. Let $\phi^{-1}(\xi) = \{\xi_1, \dots, \xi_t\} \subset \Omega_F$, where, as above, $\phi : \Omega_F \to \Omega_K$ is the restriction map.

By construction, $\phi(\xi_i) = \xi$. So we can pick a small clopen neighbourhood $U \subset \Omega_K$ of ξ and disjoint small clopen neighbourhoods $U_i \subset \Omega_F$ of ξ_i, $i = 1, \dots, t$, such that the restriction map $\phi|_{U_i} : U_i \to U$ is a homeomorphism and $\phi^{-1}(U) = U_1 \cup \dots \cup U_t$. Taking smaller neighbourhoods, if necessary, one can additionally assume that for any $\xi' \in U_1$ there is an involution $\tau_{\xi'} \in \Delta$ corresponding to ξ' for which the following property holds:

(9) if $g \in \Gamma \backslash \Delta$ be such that $\tilde{\tau}_{\xi'} = g\,\tau_{\xi'}\,g^{-1} \in \Delta$ then the point of Ω_F corresponding to the involution $\tilde{\tau}_{\xi'}$ does not lie in U_1.

Indeed, let $I_\Delta \subset \Delta$ be a subset of involutions and $\tau \in I_\Delta$ be an involution which corresponds to ξ_1. Assume the contrary. Since I_Δ, Γ are compact and totally disconnected there exist then in Δ a sequence of involutions $(\tau_1, \tau_2, \dots)$ converging to τ and a converging sequence of elements $(g_1, g_2, \dots)$ in $\Gamma \backslash \Delta$ such that $g_i\,\tau_i\,g_i^{-1} \in \Delta$. Letting $g = \lim g_i$, one has $g \in \Gamma \backslash \Delta$ and $\tau' = g\,\tau\,g^{-1} \in \Delta$. But by assumption, the point ξ' of Ω_F corresponding to τ' lies in U_1 and $\phi(\xi') = \xi$. This means that $\xi' = \xi_1$, hence there is $\delta \in \Delta$ such that $\tau' = \delta\,\tau\,\delta^{-1}$, implying $g^{-1}\delta$ lies in the centralizer $C_\Gamma(\tau)$. But every involution in Γ is self-centralizing, i.e. $C_\Gamma(\tau) = \langle\tau\rangle$,– a contradiction.

The map φ_1 is clearly surjective for the field F, since A can be viewed as $\mathrm{Gal}\,(E/F)$-module and $\mathrm{Gal}\,(E/F)$ is a 2-group, implying that any irreducible $\mathrm{Gal}\,(E/F)$-module is of the form $\mathbb{Z}/2\mathbb{Z}$. Therefore, we can pick $\zeta' \in Z^1(F, A)$ such that for proper real closures the cocycle $res_{F_{\xi'}}(\zeta')$ is determined by the element a if $\xi' \in U_1$ and is trivial otherwise. We claim that the cocycle $\zeta = cor_K^F(\zeta')$ has the same property. To verify it we need

PROPOSITION 5. ([Br], Ch. III, Proposition 9.5) *Let A be a Γ-module and $\Theta \subset \Delta \subset \Gamma$ be subgroups. If $[\Gamma : \Delta] < \infty$ and $z \in H^*(\Delta, A)$ then we have*

$$\mathrm{res}\,_\Theta^\Gamma \circ \mathrm{cor}\,_\Delta^\Gamma(z) = \sum_{g\in\Lambda} \mathrm{cor}\,^{\Theta}_{\Theta\cap g\Delta g^{-1}} \circ \mathrm{res}\,^{g\Delta g^{-1}}_{\Theta\cap g\Delta g^{-1}}(\hat{g}(z)),$$

where Λ is a set of representatives of double cosets $\Theta\, g\, \Delta$ and

$$\hat{g} : H^*(\Delta, A) \to H^*(g\,\Delta\, g^{-1}, A)$$

is the natural map induced by pair $(\,\mathrm{int}(g^{-1}),\, g\,)$.

To prove our claim first take $\eta \in U$. Let $\xi' = \phi^{-1}(\eta) \cap U_1$ and let $\tau_{\xi'} \in \Delta$ be an involution corresponding to ξ' and satisfying (9). Then applying Proposition 5 we have

$$\mathrm{res}_{K_{\xi'}}(\zeta) = \sum \mathrm{res}\,^{g\Delta g^{-1}}_{\Theta_{\xi'}\cap g\Delta g^{-1}}\;(\hat{g}(\zeta')) = \sum \mathrm{res}\,^{\Delta}_{g^{-1}\Theta_{\xi'}\,g\cap\Delta}(\zeta') = \mathrm{res}\,^{\Delta}_{\Theta_{\xi'}}(\zeta')$$

where $\Theta_{\xi'} = \langle\tau_{\xi'}\rangle$, hence $\mathrm{res}_{K_{\xi'}}(\zeta)$ is defined by a. Analogously, one shows that $\mathrm{res}_{K_\eta}(\zeta)$ is trivial if $\eta \notin U$. Proposition 4 is proved. □

COROLLARY 2. *Let A be a commutative connected linear algebraic K-group. Then φ_2 is injective.*

PROOF. One has $H^i(L, A) = 1$, $i \geq 1$. So $H^i(K, A)$ has exponent 2 and hence the map $H^i(K, {}_2A) \to H^i(K, A)$ is surjective, where ${}_2A$ consists of all elements of A killed by 2. By Proposition 4, it gives the surjectivity of φ_1 for A. Then the result follows from the injectivity of φ_2 for ${}_2A$. □

Corollary 3. *The Hasse principle holds for algebraic K-tori.*

Proof. Let T be a K-torus. There exists K-quasi-split torus S and its connected K-subtorus H such that $T = S/H$. Then the commutative diagram

$$\begin{array}{ccccc} H^1(K,S)=1 & \longrightarrow & H^1(K,T) & \longrightarrow & H^2(K,H) \\ \Big\downarrow \theta_1 & & \Big\downarrow \theta_2 & & \Big\downarrow \theta_3 \\ \prod_{\xi\in\Omega_K} H^1(K_\xi,S)=1 & \longrightarrow & \prod_{\xi\in\Omega_K} H^1(K_\xi,T) & \longrightarrow & \prod_{\xi\in\Omega_K} H^2(K_\xi,H) \end{array}$$

shows that the injectivity of θ_2 follows from that of θ_3. □

4. The Hasse principle for principal homogeneous spaces

Let us keep the notations of § 3. In particular, we assume that K is a field with $\mathrm{vcd}\,(K) \le 1$, $L = K(\sqrt{-1}\,)$ and $\Omega_K \ne \emptyset$. Let also τ be the non-trivial element of $\mathrm{Gal}\,(L/K)$. Using the results of the previous sections we may produce a simple proof of the triviality of the kernel of (2).

a) Let G' be a connected linear algebraic K-group, $Z \le G'$ be a finite central K-subgroup and let $G = G'/Z$.

Lemma 5. *If the Hasse principle holds for G' then it also holds for G.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccccc} H^1(K,Z) & \longrightarrow & H^1(K,G') & \longrightarrow & H^1(K,G) & \xrightarrow{\lambda_1} & \\ \Big\downarrow \theta_1 & & \Big\downarrow \theta_2 & & \Big\downarrow \theta_3 & & \\ \prod_{\xi\in\Omega_K} H^1(K_\xi,Z) & \longrightarrow & \prod_{\xi\in\Omega_K} H^1(K_\xi,G') & \longrightarrow & \prod_{\xi\in\Omega_K} H^1(K_\xi,G) & \xrightarrow{\lambda_2} & \\ & & & \xrightarrow{\lambda_1} & H^2(K,Z) & & \\ & & & & \Big\downarrow \theta_4 & & \\ & & & \xrightarrow{\lambda_2} & \prod_{\xi\in\Omega_K} H^2(K_\xi,Z) & & \end{array}$$

By assumption and by Proposition 2, the maps θ_2, θ_4 are injective. Then from the above diagram and from Proposition 4 we have $\mathrm{Ker}\,\theta_3 = 1$. □

b) *Reduction to semisimple groups.* Since unipotent K-groups have trivial cohomology we may assume without loss of generality that G is reductive. Then $G = T \cdot H$ is an almost direct product of the central torus T and the semisimple group $H = [G,G]$. Let $G' = T \times H$. Clearly, the kernel of the natural morphism $G' \to G$ is finite and by induction and by Corollary 3, the Hasse principle holds for H and T. So by Lemma 5, it holds for G as well.

c) *Reduction to simple simply connected groups.* One can again apply Lemma 5 to a simply connected covering G' of G.

d) Let G be an (absolutely) simple simply connected K-group. By Steinberg's theorem ([St2]), G has a Borel subgroup B over L. We may assume that $T = B \cap \tau(B)$ is a maximal K-torus of G. Since $H^1(L,G) = 1$, the map $H^1(L/K, G(L)) \to H^1(K,G)$ is surjective. By Lemma 6.28 [Pl-R], the map $H^1(L/K, T(L)) \to H^1(L/K, G(L))$ is surjective as well, hence any class $[\zeta] \in$

$H^1(K,G)$ can be represented by a cocycle $\zeta' \in Z^1(L/K, T(L))$. Let S be a maximal K-split subtorus of T.

First let $S \neq 1$. Then $C_G(S)$ is a proper connected subgroup of G. Since $C_G(S)$ is a reductive part of some parabolic K-subgroup, one has $\operatorname{Ker}(H^1(E, C_G(S)) \to H^1(E,G)) = 1$ for any extension E/K ([Pr-R], Lemma 5.1). So if in addition $\zeta \in \operatorname{Ker}\theta$, then for each $\xi \in \Omega_K$ the element $\operatorname{res}_{K_\xi}(\zeta')$ is trivial as an element of $H^1(K_\xi, C_G(S))$, hence the claim follows by induction.

e) $S = 1$, *i.e. T is a K-anisotropic torus.* By Steinberg's theorem, G is either split or quasi-split over L. We examine the L-splitting case only, since the L-quasi-splitting case can be handled analogously. Identify $Z^1(\Theta, T(L))$ with $(K^*)^n$. Arguing as in d) we get that any element from $\operatorname{Ker}\theta$ can be represented by a cocycle $\zeta \in Z^1(\Theta, T(L))$. We claim that there exist a maximal K-torus $T' \subset G$ isomorphic to T over K and a cocycle $\zeta' \in Z^1(\Theta, T'(L))$ equivalent to ζ in $Z^1(\Theta, G(L))$ such that ζ' is everywhere locally positive. By Corollary 3, the last would mean that ζ' is trivial as an element of $H^1(\Theta, T'(L))$, hence ζ is trivial in $H^1(\Theta, G(L))$ as well.

To show it, we proceed as in Theorem 2. Namely, we construct inductively quaternion algebras $D_1, \dots, D_m$ over K and elements $g_i \in G_{\beta_i}(L)$ such that for $g = g_1 \cdots g_m$ the element $g^{1-\tau} \in T(L)$ and the components of the cocycles $(g^{1-\tau})$ and ζ everywhere locally have the same signs.

As in Theorem 2, we begin with $D_m = (-1, d_{\beta_m})$, where $d_{\beta_m} = c_{\beta_m}$. For $\xi \in \Omega_K$ let $g_\xi \in G(\overline{K_\xi})$ be such that $\zeta = (g_\xi^{1-\tau})$ (note that T is still anisotropic over K_ξ). We may assume that g_ξ is in "generic" position and so we may write g_ξ as a product $g_\xi = t_\xi\, g_{\xi,1} \cdots g_{\xi,m}$, where $t_\xi \in T$, $g_{\xi,i} \in G_{\beta_i}$, $i = 1, \dots, m$.

We have already known that $\tau(g_{\xi,m}) = h_{\beta_m}(w_{\xi,m})\, g_{\xi,m}$ for some parameter $w_{\xi,m} \in K_\xi$. By virtue of the facts that our field K has the property SAP and the Hasse principle holds for groups of type A_1 ([B-P], [Sch1]) we can pick $w_m \in K$, which has everywhere locally the same sign as $w_{\xi,m}$, and $g_m \in G_{\beta_m}(L)$ such that $h_{\beta_m}(w_m) = g_m^{1-\tau}$.

Next consider the quaternion K-algebra $D_{m-1} = (-1, d_{\beta_{m-1}})$, where

$$d_{\beta_{m-1}} = c_{\beta_{m-1}} w_m^{\langle \beta_{m-1}, \beta_m \rangle}.$$

Let $w_{\xi,m-1} \in K_\xi$ be such that $h_{\beta_{m-1}}(w_{\xi,m-1})\, h_{\beta_m}(w_{\xi,m}) = (g_{\xi,m-1}\, g_{\xi,m})^{1-\tau}$ Again we can pick $w_{m-1} \in K$ such that for all $\xi \in \Omega_K$ the elements w_{m-1} and $w_{\xi,m-1}$ have the same sign. By construction, the equation $h_{\beta_{m-1}}(w_{m-1})\, h_{\beta_m}(w_m) = (x\, g_m)^{1-\tau}$, where $x \in G_{\beta_{m-1}}(L)$, has solution everywhere locally, so it has solution g_{m-1} globally, and so on.

Thus, there exists $g \in G(L)$ such that the components of both cocycles $(g\tau(g^{-1}))$ and ζ have the same signs in K_ξ for each $\xi \in \Omega_K$. To complete the proof of the theorem it remains to notice that the cocycle $\zeta' = \tau(g)^{-1}\zeta\, g$ is equivalent to ζ in $Z^1(\Theta, G(L))$, takes values in the K-defined and L-splitting torus $T' = \tau(g)^{-1} T \tau(g)$ and ζ' is everywhere locally positive. $\square$

Remark 3. The same argument shows that θ is still injective if we replace Ω_K by a dense set of orderings.

References

[A1] J. Arason, Primideale im graduierten Wittring und im mod 2 Cohomologiering, Math. Z. 145 (1975), 139–143.

[A2] J. Arason, Cohomologische Invarianten quadratischer Formen, J. Algebra 36 (1975), 448–491.

[B-P] E. Bayer-Fluckiger, R. Parimala, Classical groups and the Hasse principle, Ann. of Math. 147 (1998), 1–43.

[Br] K. Brown, Cohomology of groups, Springer, 1982.

[Ch] V. Chernousov, On projective simplicity of groups of rational points of some algebraic groups over algebraic number fields, Izvestiya Akad. Nauk SSSR, Ser. Math., 53 (1989), N 2, 398–410 (in Russian).

[CT] J–L. Colliot-Thélène, Groupes linéaires sur les corps de fonctions de courbes réelles, J. reine angew. Math. 474 (1996), 139–167.

[L] T. Y. Lam, Orderings, valuations and quadratic forms, Regional Conference Series in Mathematics 52, AMS, 1983.

[Pr-R] G. Prasad, M. S. Raghunathan, On the Kneser-Tits problem, Comment. Helvetici 60 (1985), 107–121.

[Pl-R] V. P. Platonov, A.S. Rapinchuk, Algebraic groups and number theory, Academic Press, N.Y., 1994.

[S] J–P. Serre, Cohomologie Galoisienne, Springer, 1994.

[Sch1] C. Scheiderer, Hasse principles and approximation theorems for homogeneous spaces over fields of virtual cohomological dimension one, Invent. math. 125 (1996), 307–365.

[Sch2] C. Scheiderer, Real and Étale Cohomology, LNM 1558.

[Srl] W. Scharlau, Quadratic and Hermitian Forms, Grundlehren math., Wiss. 270, Springer-Verlag, Berlin, 1985.

[Sp] T. A. Springer, Nonabelian H^2 in Galois cohomology, in Algebraic groups and discontinuous Subgroups, Proc. Symp. Pure Math. IX, Providence, 1966, 164–182.

[St1] R. Steinberg, Lectures on Chevalley groups, Yale University, 1967.

[St2] R. Steinberg, Regular elements of semisimple algebraic groups, Publ. Math. I.H.E.S. 25 (1965), 281–312.

Vladimir Chernousov
Fakultät für Mathematik
Universität Bielefeld
D 33501 Bielefeld, Germany
chernous@mathematik.uni-bielefeld.de