Lectures On
Galois Cohomology of Classical Groups

By

M. Kneser

Tata Institute of Fundamental Research, Bombay

1969

Lectures On
Galois Cohomology of Classical Groups

By

M. Kneser

Notes by

P. Jothilingam

Tata Institute of Fundamental Research
Bombay
1969

Preface

These notes reproduce the contents of lectures given at the Tata Institute in January and February 1967, with some details added which had not been given in the lectures. The main result is the Hasse principle for the one-dimensional Galois cohomology of simply connected classical groups over number fields. For most groups, this result is closely related to other types of Hasse principle. Some of these are well known, in particular those for quadratic forms. Two less well known cases are:

i) Hermitian forms over a division algebra with an involution of the second kind; here the result is connected with (but not equivalent to) a theorem of Landherr. The simplified proof of Landherr's theorem, given in §5.5, has been obtained independently by T. Springer;

ii) Skew-hermitian forms over a quaternion division algebra; here a proof by T. Springer, different from the one given in the lectures in §5.10, is reproduced as an appendix.

I wish to thank the Tata Institute for its hospitality and P. Jothilingam for taking notes and filling in some of the details.

Martin Kneser

Contents

Chapter 1

Galois Cohomology

In this chapter we shall collect the fundamental facts about Galois Cohomology. Proofs are mostly straightforwards and therefore omitted. Moreover they can be found in the basic reference [19]. 1

1.1 Non-commutative cohomology

Let G be a group operating on a set A; the image of (s, a) under the map $G \times A \to A$ defining the operation of G on A will be denoted by ${}^s a$. A set is called a G-set if G acts on it. If the G-set A has in addition the structure of group and if the operation of G respects this structure then we say A is a G-group.

Definition of $H^0(G, A)$: If A is any G-set then $H^0(G, A)$ is defined to be the set A^G of elements left fixed by the operation of G on A, i.e. $H^0(G, A) = A^G = \{a \in A | {}^s a = a \ \forall s \in G\}$.

Definition of $H^1(G, A)$: This definition will be given only for a G-group A. Accordingly let A be a G-group. A mapping $s \to a_s$ of G into A is said to be a 1-cocycle of G in A if the relation $a_{st} = a_s {}^s a_t$ holds for all $s, t \in G$. Two 1-cocycles (a_s) and (b_s) are said to be equivalent if for a suitable $c \in A$ the relation $b_s = c^{-1} a_s {}^s c$ holds for all $s \in G$. This is an equivalence relation on the set of 1-cocycles of G in A. $H^1(G, A)$ is by definition the set of equivalence classes of 1-cocycles. If A is a commu- 2

tative group we have the usual definition of $H^i(G, A)$, $i = 0, 1, 2, 3, \ldots$ by means of cocycles and coboundaries. We write it down here only for $i = 2$. If A is commutative the definitions of $H^i(G, A)$, $i = 0, 1$ given above coincide with the usual definition of these groups.

Definition of $H^2(G, A)$: Here A is any commutative G-group. A 2-cocycle of G in A is a mapping $(s, t) \to a_{s,t}$ of $G \times G$ into A satisfying the relation $r_{a_{s,t}}\ a^{-1}_{rs,t}\ a_{r,st}\ a^{-1}_{r,s} = 1$ for all $r, s, t \in G$. A 2-coboundary is a 2-cocycle of the form $s_{c_t}\ c^{-1}_{st}\ c_s$ with $c_s \in A$. If the product of two cocycles $(a_{s,t})$ and $(b_{s,t})$ is defined as $(a_{s,t}\ b_{s,t})$ the 2-cocycles will form a multiplicative group and the 2-coboundaries will form a subgroup; by definition the quotient group is then $H^2(G, A)$.

Let A be a G-group and B an H-group. Two homomorphisms $f : A \to B$, $g : H \to G$ are said to be compatible if $f({}^{g(s)}a) = {}^s(f(a))$ holds for every $s \in H$, $a \in A$; if $H = G$ and g is identity then f is said to be a G-homomorphism. Mapping a 1-cocycle (a_s) of G in A onto the 1-cocycle (b_s) of H in B defined by $b_s = f(a_{g(s)})$ induces a mapping $H^1(G, A) \to H^1(H, B)$; this will be a group homomorphism in case A and B are commutative. If H is a subgroup of G and g is the inclusion the map $H^1(G, A) \to H^1(H, B)$ defined above is called the restriction map. This definition can be carried over to higher dimensional cohomology groups when A and B are commutative.

3 For non-commutative G-group A, the set $H^1(G, A)$ is not a group in general but it has a distinguished element namely the class of 1-cocycles of the form $b^{-1}{}^s b$, with $b \in A$. The existence of this element enables one to define the kernel of a map $H^1(G, A) \to H^1(H, B)$ such as we have obtained above and also to attach meaning to the term 'exact sequence of cohomology sets'.

1.2 Profinite groups

Definition. *A topological group G is said to be profinite if it is a projective limit of finite groups the latter carrying discrete topology.*

A profinite group is then compact and totally disconnected, it possesses a base of neighbourhoods of the identity formed by open normal

subgroups. Conversely if a compact topological group G has a base of neighbourhoods of $1 \in G$ formed by open normal subgroups U then the quotients G/U are finite and $G \cong \varprojlim G/U$; hence G is profinite.

Let G be profinite and A any G-group with discrete topology. In such a case we shall always assume that the action of G on A is continuous. This is equivalent to the requirement $A = \bigcup_U A^U$ the union being taken over the set of open normal subgroups U of G. We shall modify the definition of $H^i(G, A)$ in this case by requiring the cocycles to be continuous. In the sequel this new definition of $H^i(G, A)$ will be adhered to whenever we consider profinite groups G and G-sets. If $U \subset V$ are open normal subgroups of G then the inclusion $A^V \hookrightarrow A^U$ **4**
and natural projection $G/U \to G/V$ are compatible, hence we get the induced map $\varrho_U^V : H^i(G/V, A^V) \to H^i(G/U, A^U)$ called inflation. The sets $H^i(G/U, A^U)$ together with the maps ϱ_U^V form an inductive system and $H^i(G, A) \cong \varinjlim H^i(G/U, A^U)$.

1.3 Induction

Let G be a profinite group, H an open subgroup of G and let B be any H-set. Let $\bar{A}$ denote the set of mappings $a : G \to B$ which map $s \in G$ onto $a(s) \in B$ satisfying the condition $a(ts) = {}^t a(s)$ for all $t \in H$, $s \in G$. $\bar{A}$ is made into a G-set by defining r_a for $a \in \bar{A}$, $r \in G$ by the rule $({}^r a)(s) = a(sr)$; we then say that $\bar{A}$ is induced from B; more generally, we call every G-set A isomorphic to $\bar{A}$ a $G - H$ induced set; if B is an H-group, A is a G-group. Suppose A is $G-H$ induced from B so that we can identify A with $\bar{A}$. Mapping $a \in \bar{A}$ onto $a(1) \in B$ we get a mapping $A \cong \bar{A} \to B$ which is compatible with the inclusion $H \hookrightarrow G$; passing to cohomology we get a map $H^i(G, A) \to H^i(H, B)$ whenever $H^i(H, B)$ (and therefore $H^i(G, A)$) is defined. We then have the

Lemma 1. *The mapping $H^i(G, A) \to H^i(H, B)$ defined above is an isomorphism.*

For commutative A and B, see [19] 1 §2.5. For completeness sake, we give the proof for $i = 0, 1$ in the general case.

Proof. First let $i = 0$; if $a \in \bar{A}^G$, $(r_a)(s) = a(s)$ for every, $r, s \in G$, taking 5
$s = 1$ we find that a is a constant function $G \longrightarrow B$. Hence the mapping $H^\circ(G, A) \longrightarrow H^\circ(H, B)$ is injective. If $c \in B$ the constant function $G \longrightarrow B$ mapping every $s \in G$ onto c is an element of $\bar{A}^G$; this shows that the mapping in question is also surjective and hence bijective. □

Now let $i = 1$; suppose two elements (a_r), (b_r) of $H^1(G, A)$ have the same image under the mapping $H^1(G, A) \longrightarrow H^1(H, B)$; then for a suitable $c \in B$ we must have $a_r(1) = c^{-1}b_r(1)r_c$ for all $r \in H$. Now we find an element $d \in \bar{A}$ with $d(1) = c$ by taking a set of representatives of gH including 1 and mapping 1 onto c and the other representatives onto arbitrarily chosen elements of B; replacing the cocycle b_r by the equivalent cocycle $d^{-1}b_r r_d$ we can assume $a_r(1) = b_R(1)$ for all $r \in H$. Using the cocycle condition we have for all $r, s, t \in G$

$$a_{rs}(t) = a_r(t)r_{a_s}(t) = a_r(t)a_s(tr)$$
$$b_{rs}(t) = b_r(t)r_{b_s}(t) = b_r(t)b_s(tr)$$

Setting $r = t^{-1}$ in (1) and (2) we get $a_{t^{-1}s}(t) = a_{t^{-1}(t)a_s(1)}$ and $b_{t^{-1}s}(t) = b_{t^{-1}}(t)b_s(1)$; since $a_s(1) = b_s(1)$ for all $s \in H$ we get $a_{t^{-1}s}(t)b_{t^{-1}s}(t) = a_{t^{-1}}(t)b_{t^{-1}}(t)$ holding for all $s \in H$; hence if we define $c(t) \in B$ for every $t \in G$ by the rule $c(t) = b_{t^{-1}}(t)a_{t^{-1}}(t)$ then by what precedes we get for

$$s \in H, c(st) = b_{t^{-1}s^{-1}}(st)a_{t^{-1}s^{-1}}(st)^{-1} = {}^s b_{t^{-1}s^{-1}}(t)\,{}^s a_{t^{-1}s^{-1}}(t)^{-1} =$$
$$= {}^s(b_{t^{-1}s^{-1}}(t)a_{t^{-1}s^{-1}}(t)^{-1}) = {}^s(b_{t^{-1}}(t)a_{t^{-1}}(t)^{-1}) = {}^s c(t),$$

6 and hence c belongs to $\bar{A}$. Given elements r and t in G choose $s \in G$ such that $trs = 1$; then we have

$$a_{rs}(t) = a_{t^{-1}}(t) = c(t)^{-1}b_{t^{-1}}(t) = c(t)^{-1}b_{rs}(t)$$
$$\text{and } a_s(tr)^{-1} = a_{r^{-1}t^{-1}}(tr)^{-1} = b_{r^{-1}t^{-1}}(tr)^{-1}c(tr) = b_s(tr)^{-1}c(tr).$$

From equations (1) and (2) together with the foregoing it follows that $a_r(t) = a_{rs}(t)a_s(tr)^{-1} = c(t)^{-1}b_{rs}(t)b_s(tr)^{-1}c(tr) = c(t)^{-1}b_r(t)^r c(t)$ i.e. $a_r = c^{-1}b_r r_c$, hence the cocycles a_r and b_r are equivalent; this means that the mapping $H^1(G, A) \to H^1(H, B)$ is injective. Now suppose $b = (b_s) \in H^1(H, B)$ is given. Let V be a system of right representatives of

G mod H, $v(s)$ the representative in V of the coset Hs, and therefore $w(s) = sv(s)^{-1} \in H$. Define $a_s : G \to \bar{A}$ by $a_s(t) = {}^{w(s)} b_{w(v(t)s)}$. It is straight forward to verify that $a_s(t)$ is indeed an element of A and that (a_s) is a 1-cocycle of G in $\bar{A}$ whose image is (b_s) under the mapping $H^1(G, A) \to H^1(H, B)$; this proves the surjectivity and so bijectivity of the mapping in question.

Remark. If B is a H-group and $\bar{A}$ is $G - H$ induced from B (so that $\bar{A}$ 7
is a G-group) then the projection $\bar{A} \to B$ induces an isomorphism of B with the subgroup of those $a \in \bar{A}$ which are equal to 1 outside H; if we identify B with this subgroup, then s_B depends only on the coset Hs and we have $\bar{A} \cong \prod_{s \in H/G} {}^s B$. The converse is also true, i.e. we have the lemma whose proof is straight forward and so omitted.

Lemma 2. *A G-group A is $G - H$ induced if and only if there exists an H-subgroup B of A such that A is the direct product of the subgroups ${}^s B (s \in H/G)$.*

1.4 Twisting

In the sequel we shall be considering a G-group A and a G-set E on which A operates; for $x \in A$ and $a \in E$ we denote by $x.a$ the result of operating x on a. We assume that the action of A on E satisfies the condition ${}^s(x.a) = s_x.s_a$ for $s \in G$, $x \in A$ and $a \in E$. If E, F are G-sets and $f : E \to F$ is a map of sets not necessarily of G-sets we define the map $s_f : E \to F$ for $s \in G$ by the rule $({}^s f)(a) = {}^s(f({}^{s^{-1}}a))$ so that $({}^s f)({}^s a) = {}^s(f(a))$; taking $F = E$ this definition makes Aut E (the group of bijections of E onto itself as a set) into a G-group. Associating to $x \in A$ the automorphism of E defined by the action of x on E we get a G-homomorphism $A \to Aut\ E$ which induces a mapping of cohomologies

$$H^i(G, A) \to H^i(G, Aut\ E).$$

If $f : E \to F$ is a bijection of G-sets then $a_s = f^{-1} \circ {}^s f$ is a 1- 8
cocycle of G in $Aut\ E$; changing f through and automorphism of E we get an equivalent cocycle. Hence any bijection $f : E \to F$ modulo

automorphism of E defines an element of $H^1(G, Aut\ E)$. Moreover if E and F carry additional structures and f preserves these then so does a_s. Conversely starting with a G-group A, a G-set E on which A operates G-compatibly and a 1-cocycle (a_s) with values in A we can construct a G-set F and a bijection $f : E \to F$ such that if b_s denotes the image of a_s under the mapping $A \to Aut\ E$ then $b_s = f^{-1} \circ {}^s f$. To do this we take F to be a copy of E with a bijection $f : E \to F$ namely the identity and define the operation of G on F by ${}^s(f(x)) = f(a_s {}^s x)$ for $x \in E$ and $s \in G$; with this operation F is a G-set and F together with the mapping $f : E \to F$ solves our problem. We then say that F is obtained from E by twisting with the cocycle (a_s) and denote it by ${}_aE$; replacing a_s by an equivalent cocycle changes f by an automorphism of E. If E has in addition algebraic structures and a_s preserves these then the twisted set ${}_aE$ will carry the same algebraic structures. In particular taking $E = A$ and operating A on itself by inner automorphisms we get a twisted group ${}_aA$; again if A carries additional algebraic structures and a_s preserves these then ${}_aA$ will carry the same algebraic structures.

Example. ([18] X §2, [19] III §1.1). Let us consider the universal do-
9 main Ω in the sense of algebraic geometry and select a ground field K; let V be a Ω-vector space. We say that V is defined over K if there is given a K-subspace V_K of V such that $V \cong V_K \otimes_K \Omega$. As in algebraic geometry we shall say that V_K is the space of K-rational points on V. Let L be a finite Galois extension of K with Galois group $g_{L/K}$; then $g_{L/K}$ acts on $V_L = V_K \otimes_K L$ by the rule ${}^s(a \otimes x) = a \otimes {}^s x$ if $a \in V_K$, $x \in L$ and $s \in g_{L/K}$. Let $(Aut\ V)_L$ denote the group of L-linear automorphisms of V_L. Suppose (a_s) is a 1-cocycle of $g_{L/K}$ in $(Aut\ V)_L$. We can then twist the vector space V_L by the 1-cocycle $a = (a_s)$ to get a new L-vector space, say V' with the same underlying set as V_L. If now W is the fixed space of V' under the twisted action of $g_{L/K}$ then it is well known that W is a K-space and that $V' \cong W \otimes_K L$. Suppose $t, t', \ldots$ are given tensors in the tensor space $T(V_K)$ of V_K. If these tensors are invariant under the canonical extensions of all the a_s to $T(V_L) \cong T(V_K) \otimes_K L$, denoting by $i : V \to V'$ the identity map and its extension to $T(V)$ the tensors $i(t), i(t') \ldots$ are then invariant under the twisted action of $g_{L/K}$ so that they belong to $T(W)$. This shows for example that if we have a

hermitian or quadratic form on V_L defined over K and that if they are invariant under all the automorphisms a_s then the twisted space V' will also carry a hermitian or quadratic form defined over K. Again if V is an algebra with involution and if all the automorphisms a_s preserve the algebra structure and the involution then the twisted space will be an algebra with involution.

Let A be a G-group, (a_s) a 1-cocycle of G in A. **10**

Lemma . *There exists a bijection of* $H^1(G,_a A)$ *onto* $H^1(G, A)$ *which maps the class of (1) onto the class* (a_s)*.*

Proof. Identify the set ${}_aA$ with A by means of the bijection $f : A \to_a A$ and map the 1-cocycle (b_s) of G in A onto the 1-cocycle (b_s, a_s) of G in A. This gives a mapping of $H^1(G,_a A)$ into $H^1(G, A)$ which takes the distinguished element of $H^1(G,_a A)$ onto the cocycle (a_s). This mapping has an inverse defined by $(c_s) \to (c_s.a_s^{-1})$ where c_s is a 1-cocycle of G in A. This proves the lemma. □

This can be seen in another way as follows: Let F be a set with some structure whose automorphism group is A. The twisted group ${}_aA$ acts naturally on the twisted set ${}_aF$. Moreover ${}_aA$ will be the automorphism group of ${}_aF$. Hence the elements of $H^1(G,_a A)$ correspond bijectively with G-isomorphism classes of G-sets E (with structure) for which there is an isomorphism $h :_a F \to E$; let $g : F \to_a F$ be the bijection corresponding to a. Then $h\ o\ g : E \to E$ will determine an element of $H^1(G, A)$, the corresponding cocycle will be $(hog)^{-1}o^s(hog) = g^{-1}oh^{-1}o^s ho^s g = g^{-1}ob_s{}^s g = f^{-1}(b_s) \cdot a_s$ where (b_s) is the 1-cocycle of G in ${}^aA$ corresponding to $h :_a F \to F$ and f is the bijection $f : A \to {}_aA$ corresponding to the twisting by a. This process in naturally reversible and so we get a bijection of $H^1(G, {}_aA)$ onto $H^1(G, A)$. Evidently the distinguished element (1) of $H^1(G, {}_aA)$ goes onto (a_s) under this mapping.

Let A, B be G-groups and $g : A \to B$ be a G-homomorphism. If (a_s) **11**
is a 1-cocycle of G in A define $b_s = g(a_s)$; then (b_s) is a 1-cocycle of G in B and g induces a G-homomorphism also denoted by g of a^A into b^B.

The commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle f}\downarrow & & \downarrow \\ {}_aA & \xrightarrow[g]{} & {}_bB \end{array}$$

gives rise to the following commutative diagram:

$$\begin{array}{ccc} H^1(G,A) & \longrightarrow & H^1(G,B) \\ \downarrow & & \downarrow \\ H^1(G,{}_aA) & \longrightarrow & H^1(G,{}_bB) \end{array}$$

1.5 Exact Sequences

In what follows A, B, C will be G-groups and homomorphisms will be G-homomorphisms

a) Let $A \to B$ be a monomorphism of G-groups. Let B/A be the homogeneous space of left cosets of B in A; this is a G-set and one can define $H^0(G, B/A)$. Given an element in $H^0(G, B/A)$ choose a representative b of it in B; define $a_s = b^{-1s}b$; then $a_s \in A$ and (a_s) is a 1-cocycle of G in A; moreover (a_s) depends only on the element of $H^o(G, B/A)$ under consideration and not on the particular representative chosen. In this way we get a map $\delta : H^0(G, B/A) \to H^1(G, A)$. Then the following sequence with maps the natural ones and δ as defined above, is exact:

12

$$1 \to H^o(G,A) \to H^o(G,B) \to H^o(G,B/A) \xrightarrow{\delta} H^1(G,A) \to H^1(G,B).$$

b) Let A be a normal subgroup of B and let $C = B/A$; then C is a G-group and the exact sequence $1 \to A \to B \to C \to 1$ gives rise to an

exact cohomology sequence

$$1 \to H^o(G,A) \to H^o(G,B) \to H^o(G,C) \to H^1(G,A) \\ \to H^1(G,B) \to H^1(G,C)$$

here the definition of δ is the same as before and all other maps are natural ones.

c) Let A be a subgroup of the centre of B so that $H^2(G,A)$ is defined. As in *b*) we let $C = B/A$. We can then define a map $\partial : H^1(G,G) \to H^2(G,A)$ which will make the following sequence exact:

$$1 \to H^o(G,A) \to H^o(G,B) \to H^o(G,C) \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \\ \to H^1(G,C) \xrightarrow{\partial} H^2(G,A).$$

The map δ is the same as in *a*) and the maps other than δ, ∂ are the natural ones. The definition of ∂ is as follows: let $c = (c_s) \in H^1(G,C)$ be given; lift c to a mapping $b : G \to B$ (if G is profinite this lift can be chosen to be continuous which we assume is done); define $a_{s,t} = b_s{}^s b_t b_{st}^{-1}$; then $a_{s,t} \in A$ and is a 2-cocycle of G in A whose class is by definition ∂c.

The proofs of the above exact sequences and the propositions below will be found in [19] *I*§ 5.

Let B be a G-group and A a $G-$subgroup of B; the injection of A **13**
in B gives rise to a map $H^1(G,A) \to H^1(G,B)$; let $(b_s) \in H^1(G,B)$ be given. Then we have the following proposition

Proposition 1. *In order that* (b_s) *may belong to the image of* $H^1(G,A)$ *under the above map it is necessary and sufficient that the twisted homogeneous space* ${}_b(B/A)$ *has an element invariant under* G.

Suppose B is a $G-$group, A a $G-$subgroup of B contained in the center of B; then we have the exact sequence $1 \to A \to B \to C \to 1$, where $C = B/A$; let (a_s) be a 1-cocycle of G in C. The group C operates on B through inner automorphisms by a system of representatives of B/A. Hence we can twist both C and B by the cocycle (a_s); the twisted group ${}_aA$ will be A itself since A is central. The sequence $1 \to A \to_a B \to_a C \to 1$ is then exact.

1.6 Galois Cohomology

Let A be an algebraic variety defined over a field K; let L/K be a Galois extension finite or infinite. If A_L denotes the set of points of A rational over L then the Galois group $g_{L/K}$ of L/K acts on A_L; this action moreover is continuous, since any $L-$rational point of A generates a finite extension of K and so $A_L = \cup A_M$, the union being taken over the set of subfields M of L containing K such that $[M : K] < \infty$. If A is an algebraic group then since group multiplication is a morphism de-
14 fined over K, the set A_L is a group; we are interested in the study of $H^i(g_{L/K}, A_L)$ which is also denoted by $H^i(L/K, A)$ or by $H^i(K, A)$ if L is the separable closure K_s of K. We shall be dealing only with fields of characteristic 0 so that $K_s = \bar{K}$, the algebraic closure of K. Obviously $H^0(L/K, A) = A_K$. If A, B, C are algebraic groups defined over K and if we have morphisms $f : A \to B$, $g : B \to C$ defined over K then we shall say that $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ is an exact sequence if the following sequence $1 \to A_{\bar{K}} \to B_{\bar{K}} \to C_{\bar{K}} \to 1$ induced by it is exact in the usual sense. One should note that this is not a good definition in the case of characteristic $\neq 0$. Suppose $1 \to A \to B \to C \to 1$ is a sequence of morphisms of algebraic groups and that the induced sequence $1 \to A_L \to B_L \to C_L \to 1$ is exact. Then we get an exact sequence $1 \to A_K \to B_K \to C_K \to H^1(L/K, B) \to H^1(L/K, C)$. In particular if $1 \to A \to B \to C \to 1$ is exact then the sequence $1 \to A_{\bar{K}} \to B_{\bar{K}} \to C_{\bar{K}} \to H^1(K, A) \to H^1(K, B) \to H^1(K, C)$ is exact.

Let A, B be algebraic varieties defined over $\bar{K}$ and let $f : A \to B$ be an isomorphism defined over L. Then with the usual notations $a_s = f^{-1} o^s f$ is a 1-cocycle of G in the group $(\mathrm{Aut}\, A)_L$ of automorphisms of A defined over L. Suppose we fix A. An algebraic variety B defined over K and isomorphic to A over L is called a L/K-form of A, or simply a K-form. We have seen that any L/K-form of A determines a 1-cocycle
15 of $g_{L/K}$ in $(\mathrm{Aut}\, A)_L$. If two L/K-forms are K-isomorphic it is easy to see that the 1-cocycles defined by them are equivalent. Conversely it can be proved that if A is quasi projective (i.e. isomorphic to a locally closed subvariety of some projective space) then any 1-cocycle of g_L/K in $(\mathrm{Aut} A)_L$ defines a L/K-form and that equivalent 1-cocycles define K-

isomorphic forms. Hence we see that $H^1(L/K,\ \mathrm{Aut}\ A))$ is isomorphic to the set of K-isomorphic classes of L/K-forms of A, in case A is quasi projective [S_2] III §1.3, [W_1].

If A is an algebraic group defined over K, by an L/K-form of A we mean an algebraic group defined over K and isomorphic to A as an algebraic group over L. Again let V be a vector space defined over K and x a certain tensor of type $(p.q)$ defined over K. By an L/K-form of (V, x) we mean a pair (W, y) formed by a K-vector space W, a tensor y of type (p, q) of W such that there exists an L-linear isomorphism $f : V \otimes_K L \to W \otimes_K L$ for which $f(x) = y$; here x, y are considered as tensors in $V \otimes_K L$ and $W \otimes_K L$ respectively through the natural maps $V \to V \otimes_K L, W \to W \otimes_K L$. Here again if L/K is Galois $H^1(L/K,\ \mathrm{Aut}\ V)_L)$ is bijective with the set of K-isomorphism classes of L/K-forms of (V, x).

Change of Base. Let A be an algebraic group defined over K; let L/K be a Galois extension and K' any extension of K. Let L' be a Galois extension of K' containing an isomorphic image of L which we identify with L. The canonical homomorphism $g_{L'/K'} \to g_{L/K}$ obtained by restriction of K'-automorphisms of L' to L is compatible with the injection **16**
$A_L \to A_L$, and so we get an induced map $H^1(L/K, A) \to H^1(L'/K'A)$. If now L is the separable closure of K, L' that of K' there exists an injection $L \to L'$ and again L can be assumed to be contained in L'. By what precedes we then get a map $H^1(K, A) \to H^1(K', A)$; it can be proved that this mapping is independent of the particular imbedding of L in L' chosen [18] X§ 4, [19] II § 1.1.

1.7 Three Examples

Example 1. Let A be a finite dimensional K-algebra; for any extension L of K we denote by aA_L^* the group of units of the L-algebra $A_L = A \otimes_K L$; if L/K is Galois then $g_{L/K}$ acts on $A \otimes_K L$ and hence it acts it acts on A_L^*. We claim that $H^1(L/K, A_L^*) = 1$. It is enough to give the proof for finite Galois extensions, since $H^1(L/K, A_L^*) = \varinjlim_{\vec{M}} H^1(M/K, A_M^*)$ the inductive limit is with respect to inflation mappings and M runs through finite Galois extensions of K contained in L. We treat A as a right A-module

and consider the L/K forms of A; the L/K forms are right A-modules B of finite dimension over K such that $A_L \cong B_L$ this being a right A_L-module is given by left multiplication by an element of A_L^* we know from 1.6 that $H^1(L/K, A_L^*)$ is bijective with the K-isomorphism classes of L/K forms of the right A-module A; hence we have only to verify that
17 any L/K form B is isomorphic to A over K i.e. $B_K \cong A_K = A$. Now $B_L \cong B_K \otimes_K L \cong A_L$ as right A_L-modules. The A_l-isomorphism $A_L \cong B_L$ being also an A_K-module isomorphism we get the A_K-isomorphism $[L : K]A_K \cong [L : B]B_K[L : K]\ A_K$ stands for the direct sum of $[L : K]$ copies of A_K). Since A_K and B_K are Artinian A_K-modules Krull - Schmidt theorem applies so that A_K and B_K must have isomorphic in decomposable components. Hence $A_K \cong B_K$ as A_K-modules.

Example 2. Let K be a field and $A = K^n$, the direct sum of n copies of K considered as a K-algebra; the only $\bar{K}$-algebra automorphisms of $A_{\bar{K}}$ correspond to permuting the components so that $(AutA)_{\bar{K}} = \gamma_n$ the symmetric group on n symbols; the action of $g_{\bar{K}/K}$ is trivial on $(AutA)_{\bar{k}}$ so that any 1-cocycle of $g_{\bar{K}/K}$ in $(AutA)_{\bar{k}}$ is actually a group homomorphism of $g_{\bar{K}/K}$ into γ_n. We contend that $H^1(K, \gamma_n)$ is bijective with the isomorphism classes of commutative separable K-algebras of degree n. Because we noted in 1.6 that $H^1(K, AutA)$ is isomorphic to the set of K-isomorphism classes of K-forms of A, we have only to prove that K-forms of the algebra $A = K^n$ are exactly the commutative separable K-algebras of degree n, *i.e.* that a commutative K-algebra B of degree n is separable if and only if $B \otimes \bar{K} \cong \bar{K}^n$; but this is well known ([2] Chap. 8).

Example 3. Let $\mathscr{G}$ be a non-degenerate quadratic form on a finite dimensional K-vector space V; then $\mathscr{G}$ corresponds to a tensor of type $(2, 0)$.
18 In this case for any extension L of $K, (AutV)_L$ i.e. the group of L-linear automorphisms of V fixing the tensor in the notation of 1.6 is just the orthogonal group of $\mathscr{G}$ considered as quadratic form over V_L; let us denote the latter by $o(\mathscr{G})_L$. $o(\mathscr{G})_L$. is an algebraic group defined over K. By the considerations of 1.6 for any Galois extension L/K, $H^1(L/K, O(\mathscr{G}_L))$ is bijective with the K-equivalent classes of quadratic forms which become isometric to $\mathscr{G}$ when we extend the scalars to L.Over the alge-

braic closure $\bar{K}$ of K any quadratic form Q has the orthogonal splitting $V_{\bar{K}} = \bar{K}x_1 \perp \bar{K}x_2 \perp \ldots \perp \bar{K}x_n$ with $Q(x_i) = 1$ for all i; this is because if we take any orthogonal splitting $V_{\bar{K}} = \bar{K}y_1 \perp \bar{K}y_2 + \cdots + \bar{K}y_n$ with $Q(y_i) = \alpha_i$ then $(\frac{y_1}{\sqrt{\alpha_1}}, \frac{y_2}{\sqrt{\alpha_2}}, \ldots, \frac{y_n}{\sqrt{\alpha_n}})$ will be an orthogonal $\bar{K}$-basis with the desired properties. Hence any two quadratic forms on $V_{\bar{K}}$ are equivalent. This shows that $H^1(K, O(\mathscr{G}))$ is just the set of K-equivalent classes of quadratic forms. Again any nondegenerate skew-symmetric bilinear form on V is given by a tensor of type $(2, 0)$ and the corresponding algebraic group is the symplectic group S_p; here the dimension of V must be even since the form is assumed to be non-degenerate; let $\dim V = 2n$; then it is well known that the matrix of the form can be brought to the form $\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ by a change of basis. Hence any two non-degenerate skew-symmetric bilinear forms on V are K-equivalent. This implies that $H^1(K, S\,p) = (1)$ or $H^1(L/K, S\,p) = (1)$ for any Galois extension L of K.

Chapter 2

Classical Groups

Throughout the rest of these lectures we shall assume the characteristic of the ground field K to be zero. In the first three paragraphs of this chapter we collect the basic facts on semi-simple linear algebraic groups (basic references [6], [7]). The last three paragraphs contain a survey of classical groups ([9], [24]). **19**

2.1 Linear algebraic groups

By a linear algebraic group G over K we mean an affine algebraic variety G defined over K together with K-morphisms $G \times G \to G$ denoted by $(x, y) \to x.y$ and $G \to G$ denoted by $x \to x^{-1}$ which satisfy the group axioms. Whenever we talk of open or closed sets in a variety we shall always assume that they are so in the Zariski topology. For any field of definition L the group of points of G rational over L will be denoted by G_L.

Example. $G = GL_n$ the general linear group; if Ω is the universal domain over K this is the algebraic group $GL_n(\Omega)$ of non-singular $n \times n$ matrices with entries in Ω. If $x = (x_{ij}) \in GL_n(\Omega)$ the mapping $(x_{ij}) \to (x_{11}, x_{12}, \ldots, \ldots x_{nn}, (\det x)^{-1})$ gives an imbedding of G in Ω^{n^2+1} as a closed subvariety of Ω^{n^2+1}, GL_n is an algebraic group defined over the prime field and for any field L, $(GL_n)_L = GL_n(L)$.

20 Next if $\mathscr{G}$ is a non-degenerate quadratic form over K its orthogonal group $0(\mathscr{G})$ is a closed subgroup of GL_n and is an algebraic group defined over K. It is known that any linear algebraic group is isomorphic (i.e biregular isomorphism) to an algebraic (i.e. closed) subgroup of GL_n for some n. The connected component of the identity of the algebraic group G is denoted by $G_\circ; G_o$ is a closed, normal and connected subgroup of G with $[G : G_\circ] < \infty$; conversely any closed normal and connected subgroup of G of finite index must be $G_\circ$. In the example above the connected component of the identity of $0(\mathscr{G})$ is $S \circ (\mathscr{G})$ the special orthogonal group of $\mathscr{G}$ i.e. the subgroup of elements of $0(\mathscr{G})$ with determinant $1; S\,0(\mathscr{G})$ is of index two in $0(\mathscr{G})$. For any linear algebraic group G there exists a unique maximal normal, connected and solvable subgroup G_1, called the radical of G. We make the following

Definition 1. *A linear algebraic group G is said to be semi-simple if its radical* $G_1 = \{1\}$.

Example 2. It is known that SL_n. the subgroup of elements of GL_n with determinant 1 is a semi-simple algebraic group.

Example 3. The orthogonal group $0(\mathscr{G})$ of a non-degenerate quadratic form in at least three variables is semi-simple.

Let H be a connected linear algebraic group defined over K. Then we have the following

21 **Definition 2.** *A covering of H is a pair* (G, f)*, where G is a connected linear algebraic group and* $f : G \to H$ *is a homomorphism (i.e. rational homomorphism) which is surjective and with finite kernel, (for the definition of surjectivity, exactness etc, see 1.6);*

Definition. *A linear algebraic group G is said to be simply connected if it is connected and every covering of it is an isomorphism.*

Remark 1. In the case of non-zero characteristic p, this definition is not reasonable; SL_n would not be simply connected in the above definition because $(x_{ij}) \to (x_{ij}^p)$ is surjective with finite kernel but is not an iso-

morphism. But SL_n is simply connected in the above definition if the characteristic is zero.

Remark 2. If (G, f) is a covering of the connected linear algebraic group H then $ker f \subset$ center G; for let $N = \ker f$: then N is a finite group and so the Zariski topology on N is discrete. For every $n \in N$ consider the morphism $G \to N$ given by $x \to xnx^{-1}n^{-1}$; since G is connected and N discrete this must be a constant map; taking $x = n$, this constant value must be 1; i.e. $xnx^{-1}n^{-1} = 1 \forall x \in G$; since $n \in N$ may be quite arbitrary N must be in the center of G.

Definition . *A linear algebraic group G is said to be simple if its only closed normal subgroups are the identity and G itself.*

Example . The projective linear group PGL_n which is the quotient of GL_n by its center is a simple group.

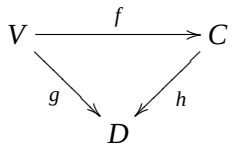
2.2 Semi-simple groups

If G is any linear algebraic group the adjoint group $\bar{G}$ is defined to be the quotient of G by its centre. It is known that a semi-simple linear **22**
algebraic group has finite center. If G is a connected semi-simple linear algebraic group defined over K there exists a covering $\tilde{G} \to G$ defined over K such that $\tilde{G}$ is simply connected and that $\tilde{G}$ is unique upto K-isomorphism; $\tilde{G}$ is called the universal covering group of G.

Example 1. The adjoint group of SL_n is the projective linear group PGL_n.

Example 2. Let $\mathscr{G}$ be a non-degenerate quadratic form on a finite dimensional K-vector space V. The proper orthogonal group $S0(\mathscr{G})$ is semi-simple and connected; and it has a two fold covering namely the Spin group which is constructed using the Clifford algebra of $\mathscr{G}$; we merely state the definition and properties of Clifford algebra and refer the reader to the standard works [2] Chap. 9 and [4]. A Clifford algebra of $\mathscr{G}$ is a pair (C, f) where C is an associative K-algebra with unity and $f : V \to C$ is a K-linear map with $\{f(x)\}^2 = q(x) \cdot 1$ for every $x \in V$

and satisfying the following universal property: Whenever a pair (D, g) is given with D an associative K-algebra with unity and $g : V \to D$ is a K-linear map such that $\{g(x)\}^2 = \mathscr{G}(x).1$ there exists a unique K-algebra homomorphism $h : C \to D$ making the diagram



23 commutative. It is known that such an algebra C exists and is unique upto K-isomorphism; evidently $f(V)$ must generate C. The algebra C is called the Clifford algebra of $\mathscr{G}$ and is denoted by $C(\mathscr{G})$. It turns out that the map f is injective, so we can identify $f(V)$ with V; then if $e_1, \ldots, e_n$ is a basis of V, the products $e_{i_1} \ldots e_{i_m} (1 \leq i_1 < i_2 < \ldots < i_m \leq n, 1 \leq m \leq n)$ together with 1 form a basis of $C(\mathscr{G})$ so its dimension is 2^n. If n is even C a simple algebra with centre K; if n is odd the algebra C is a separable algebra, its centre being of dimension two over K; C is either simple or the direct sum of two simple algebras. We denote by C^+ the subalgebra of C generated by products of an even number of vectors of V; then $\dim C^+ = 2^{n-1}$.

In case $n = \dim V$ is even and $n > 0$ it is known that $C^+(\mathscr{G})$ is separable its centre Z is of dimension 2 over K; Z is either a quadratic extension of K or a direct sum of two copies of K; in the first case $C^+(\mathscr{G})$ is a simple algebra while in the second case it is a direct sum of two simple algebras. If n is odd then $C^+(\mathscr{G})$ is always central simple; if in addition $\mathscr{G}$ has maximal Witt index then $C^+(\mathscr{G})$ is isomorphic to the ring $M_{\frac{n-1}{2}}(K)$, of $\frac{n-1}{2} \times \frac{n-1}{2}$ matrices over K. If L is any extension of K then the quadratic form $\mathscr{G}$ can be extended to a quadratic form $\mathscr{G}_L$ of V_L in a natural way by passing to the associated bilinear form of $\mathscr{G}$ and extending it to V_L; then the Clifford algebra $C(\mathscr{G}_L) \cong C(\mathscr{G}) \otimes_K L$. Let $\sigma \in 0(\mathscr{G})$ be given; σ then determines an automorphism of $C(\mathscr{G})$ in
24 the following way; $(f\mathscr{G}\sigma(x))^2 = \mathscr{G}(\sigma(x)).1 = \mathscr{G}(x).1$ for every $x \in V$. Hence by the universal property there is a K-algebra homomorphism

$g : C \to C$ making the diagram below commutative

$$\begin{array}{ccc} V & \xrightarrow{f} & C \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle g} \\ V & \xrightarrow[f]{} & C \end{array}$$

Working with σ^{-1} we see that g is an automorphism. If $\sigma \in S0(\mathscr{G})$ it is known that the corresponding automorphism of $C(\mathscr{G})$ is inner automorphism by an invertible element of $C^+(\mathscr{G})$. Conversely if $t \in C^+(\mathscr{G})$ is an invertible element such that $tVt^{-1} = V$ then the mapping $x \to txt^{-1}$ of V into itself is a proper orthogonal transformation. It is known that if we define a map $\alpha : C \to C$ by the rule $\alpha(e_{i_1} \ldots e_{i_r}) = e_{i_r} e_{i_{r-1}} \ldots e_{i_1}$ on the generators $e_{i_1} \ldots e_{i_r} (1 \leq i_1 < i_2 < \ldots < i_r \leq n; 1 \leq r \leq n)$ and $\alpha(1) = 1$ we get an anti- automorphism of C of degree 2. We shall denote $\alpha(t)$ by t^*. If t is an invertible element of C^+ such that $tVt^{-1} = V$ then it is wellknown that $tt^* \in K.1$. We now define Spin $(\mathscr{G})_{\bar{K}} = \left\{ t \in C^+_{\bar{K}} / tV_{\bar{K}} t^{-1} = V_{\bar{K}}, tt^* = 1 \right\}$; then for any field L, $(\text{Spin}\,\mathscr{G})_L$ will be the set of invertible elements t of C^+_L such that $tV_L t^{-1} = V_L$ and $tt^* = 1$. $\text{Spin}\,\mathscr{G}$ defined in this way is clearly a linear algebraic group over K. It is known that $\text{Spin}\,\mathscr{G}$ is simply connected and that for any $t \in (\text{Spin}\,\mathscr{G})_L$ the mapping $x \to txt^{-1}$ of V_L into itself is an element of $S0(\mathscr{V})_L$. This mapping of $\text{Spin}\,\mathscr{G}$ into $S0(\mathscr{G})$ is a K-homomorphism and **25**
is known to be surjective (c.f. Chapter 1 1.6 for the definition). Hence $\text{Spin}\,\mathscr{G} \to S0(\mathscr{G})$ is a covering. The kernel consists of those $t \leq \text{Spin}\,\mathscr{G}$ such that $txt^{-1} = x$ holds for every $x \in V$. Since V generates C, the inner automorphism by t must be the identity automorphism of C; hence tC^+ must be an element of the centre of C and so must be in K; the condition $tt^* = 1$ then implies $t = \pm 1$. Hence the kernel of $(\text{Spin}\,\mathscr{G})_{\bar{K}} \to S0(\mathscr{G})_{\bar{K}}$ is Z_2 the cyclic group $\{\pm 1\}$. $Spin\mathscr{G} \to S0(\mathscr{G})$ is the universal covering of $S0(\mathscr{G})$; it is two-fold with kernel $\{-1, 1\}$.

Definition. *Let G be a linear algebraic group defined over K; we say that G is K-almost simple if it has finite centre and all proper normal K-almost simple if it has finite centre and all proper normal K-subgroups*

are contained in the centre. In particular if K is algebraically closed we say that G is almost simple.

Let G be a semi-simple and simply connected linear algebraic group defined over an algebraically closed field K. Then

$$G = G_1 \times \ldots \times G_r \tag{1}$$

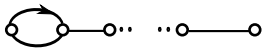
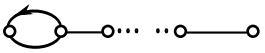
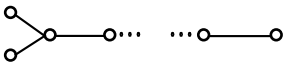
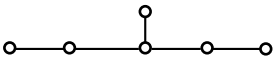
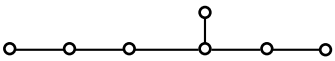
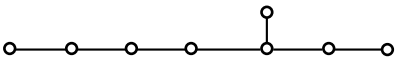
where the $G_i's$ are absolutely almost simple groups and this decomposition is unique upto permutation..

Let now K be arbitrary and G be a semisimple simply connected linear algebraic group defined over K; let (1) be the decomposition of G over $\bar{K}$; the Galois group $g_{\bar{K}/K}$ acts on either side of (1). Since the left
26 hand side is unaltered by the action of $g_{\bar{K}/K}$ the strong uniqueness theorem quoted above implies that the action of any element $g_{\bar{K}/K}$ is simply a permutation of the components G_i. Hence if $H_1, \ldots, H_s$ denote the products of components in the transitive classes modulo the action of $g_{\bar{K}/K}$ the $H_i's$ are defined over K and $G = H_1 \times \cdots \times H_s$. The groups H_i are K-almost simple. Hence we have shown that any semi-simple simply connected groups defined over K is the direct product of K-almost simple groups.

Let G be K-almost simple and let $G = G_1 \times \cdots \times G_r$ be a decomposition of G over $\bar{K}$ into the direct product of almost simple groups. Let L be the fixed field of the subgroup of $g_{\bar{K}/K}$ of elements leaving G_1 fixed. Then G_1 is a $g_{\bar{K}/L}$-subgroup of G and if s runs through a fixed system of representatives of right cosets of $g_{\bar{K}/K}$ modulo $g_{\bar{K}/L}$ we have $G = \prod_{G_1}^{s}$. This shows that G is $g_{\bar{K}/K}$-induced from G_1 (cf. Chapter 1 1.3). Lemma 1 of 1.3 then reduces the cohomology of G over K to that of G_1 over L. In the proofs later on, we may therefore assume that G is absolutely almost simple, *i.e.* remains almost simple over the algebraic closure.

2.3 Simple groups

Every semisimple linear algebraic group determines a certain graph consisting of points and lines called the Dynkin diagram. Absolutely almost simple groups correspond to connected graphs and are classified into the following types:

Types	**Dynkin Diagram**	**Chevalley Groups**
$A_n (n \geq 1)$		SL_{n+1}
$B_n (n \geq 3)$		Spin_{2n+1}
$C_n (n \geq 2)$		Sp_{2n}
$D_n (n \geq 4)$		Spin_{2n}
E_6		
E_7		
E_8		
F_4		
G_2		

27

Two simply connected almost simple groups over an algebraically closed field are isomorphic if and only if they have isomorphic Dynkin diagrams. The simply connected groups of types A_n, B_n, C_n, D_n are given in the last column; for types B_n and D_n the corresponding quadratic from must have maximal index. The spin groups of dimensions 3 to 6 and Sp_2 which are not contained in this list are semisimple too and have the following Dynkin diagrams:

Spin_3	
Spin_4	
Spin_5	
Spin_6	
Sp_2	

28

Looking for isomorphic Dynkin diagrams in our list, we get the following well known isomorphisms which can otherwise also be proved without using Dynkin diagrams. (cf. [9]):

$\mathrm{Spin}_3 \cong Sp_2 \cong SL_2$

$\mathrm{Spin}_4 \cong Sp_2 \times SL_2$

$\mathrm{Spin}_5 \cong Sp_4$

$\mathrm{Spin}_6 \cong SL_4$.

It is known that over an arbitrary ground field corresponding to any of the above types there exists a simply connected group defined over K, having a maximal torus that is defined and split over K, it is unique upto K-isomorphism and is called the simply connected Chevalley group of that type (cf. [5], [7]).

29 The group Aut G of automorphisms of a simply connected group G can also be read off from the Dynkin diagram. It contains the normal subgroup of inner automorphisms which is isomorphic to the adjoint group $Ad\ G$, the quotient being the group Symm (G) of symmetries of the Dynkin diagram. For Chevalley groups G the Galois group $g_{\bar{K}/K}$ acts trivially on Symm (G) and the exact sequence

$$1 \longrightarrow Ad\ G \longrightarrow Aut\ G \longrightarrow Symm\ (G) \longrightarrow 1 \qquad (*)$$

splits over K. Hence the corresponding cohomology sequence gives a surjection $H^1(K,\ \mathrm{Aut}\, G) \longrightarrow H^1(K, Symm(G)) \longrightarrow 1$. Let G' be any K-form of a Chevalley group G belonging to type X_y; it determines an element of $H^1(K, \mathrm{Aut}G)$ and taking its image in $H^1(K, Symm(G))$ under the map constructed above we get an element of $H^1(K, Symm(G)$ say a. Since $g_{\bar{K}/K}$ acts trivially on Symm (G) a is a homomorphism of $g_{\bar{K}/K}$ into Symm (G); let L be the fixed field of the kernel of the homomorphism $a : g_{\bar{K}/K} \longrightarrow Symm(G)$. Since Symm (G) is finite $[L : K] < \infty$. Let $z = [L : K]$. We then say that G' belongs to the sub type ${}^zX_Y$. We are now in a position to define classical groups.

Definition. *An absolutely almost simple simply connected group is side*

to be a classical group if it belongs to one of the types A_n, B_n, C_n, D_n but not to the subtypes ${}^3D_4$ and ${}^6D_4$. A connected semi-simple group is called a classical group if in the product decomposition described above of the simply connected covering group [cf. this Chapter 2.2] only classical groups occur as components.

We then see that the simply connected almost simple classical groups defined over K are K-forms of SL_{n+1}, Sp_{2n} and Spin_n (except for some K-forms of Spin_8) here Spin_n corresponds to the Spin group of a non-degenerate quadratic form of maximal Witt index. **30**

2.4 Classical Groups

Following Weil [24] we can describe the simply connected almost simple classical groups over K in terms of algebras with involution, K being an arbitrary ground field. Let G be a K-form of SL_{n+1} belonging to the subtype ${}^1A_n$ and let $f : SL_{n+1} \longrightarrow G$ be the corresponding isomorphism defined over $\bar{K}$. Then for any $s \in g_{\bar{K}/K}$, $a_s = f^{-1} \circ {}^s f \in \mathrm{Aut}GL_{n+1}$; since G is of subtype ${}^1A_n$ the exact sequence $(*)$ of 2.3 shows that a_3 actually belongs to the adjoint group of SL_{n+1} namely the projectives linear group PGL_{n+1} [cf. 2.2 example 1] (a_s) is a 1-cocycle of $g_{\bar{K}/K}$ in PGL_n. Now PGL_n is also the automorphism group of M_{n+1}, the full matrix ring. Hence $(a_s) \in H^1(K, \mathrm{Aut}\,(M_{n+1}))$. Twisting M_{n+1} by the 1-cocycle (a_s) we get a central simple K-algebra A and an isomorphism $g : M_{n+1} \otimes \bar{K} \longrightarrow A \otimes \bar{K}$ such that $a_s = g^{-1} \circ s_g$. Let H be the image of SL_{n+1} under g. H is an algebraic group defined over K. By the definition of the reduced norm N in A, $N(g(X)) = \det X$, hence $H_{\bar{K}} = \left\{ x \in A_{\bar{K}} \middle| NX = 1 \right\}$. Hence H is the algebraic group $\left\{ x \in A \middle| NX = 1 \right\}$. On the other hand by means of g, H is obtained from SL_{n+1} by twisting with the 1-cocycle (a_s) so that H is isomorphic to G. Hence the K-forms of SL_{n+1} belonging to subtype ${}^1A_n$ are the algebraic groups of elements of reduced norm 1 in central simple K-algebras.

Next we consider then case when the K-from G of SL_{n+1} belongs to **31**

the subtype ${}^2A_n$. We can describe G by means of algebras with involution.

Definition. *An antiautomorphism of period 2 of an associative K-algebra is called an involution. An involution is said to be of the first kind if it fixes every element of the center of the algebra, otherwise it is said to be of the second kind. An algebra A with involution I is denoted by (A, I). In what follows algebras A will be assumed finite dimensional over K. We shall prove that the K-forms G of SL_{n+1} belonging to subtype ${}^2A_n$ correspond bijectively with isomorphism classes of simple K-algebras A with involution I of the second kind such that the center is a quadratic extension of K; if G corresponds to (A, I) then G is isomorphic to the K-group $\left\{ z \in A \middle/ zz^I = 1, Nz = 1 \right\}$. Consider the algebra $M_{n+1} \otimes M_{n+1}$; this has an involution I of the second kind given by $(X, Y) \to ({}^tY, {}^tX)$ (t denotes transpose). We shall denote the image of any element $z \in M_{n+1} \otimes M_{n+1}$ under I by z^*. We shall determine all the automorphisms of $M_{n+1} \oplus M_{n+1}$ which commute with I; now the automorphism group of $M_{n+1} \otimes M_{n+1}$ is generated by inner automorphisms and by the automorphism $(X, Y) \longrightarrow (Y, X)$ of which the latter obviously commutes with I. If the inner automorphism by the element a commutes with I it is easy to check that aa^I must be in the center $K \oplus K$ of $M_{n+1}(K) \otimes M_{n+1}(K)$; since aa^I is invariant under I its components in $K \oplus K$ must be equal so that aa^I is an element of K.*1

32 If K is algebraically closed we can assume we can without loss of generality that $aa^I = 1$, the identity element of $K \oplus K$. Hence the group of automorphisms of $M_{n+1} \oplus M_{n+1}$ commuting with I is generated by automorphisms of the types: 1) the automorphisms $(X, Y) \longrightarrow (Y, X)$ *ii*) inner automorphisms by elements of the type $X, {}^tX^{-1}$. Now it is well know [9] that the automorphism group of SL_{n+1} is generated by inner automorphisms and by the automorphism $X \longrightarrow^t X^{-1}$. Hence the imbedding $SL_{n+1} \longrightarrow M_{n+1} \oplus M_{n+1}$ given by $X \longrightarrow (X, {}^tX^{-1})$ gives an isomorphism of the automorphism group of SL_{n+1} with the group of those automorphisms of $M_{n+1} \oplus M_{n+1}$ commuting with the involution I. We shall denote the latter group by Aut $(M_{n+1} \oplus M_{n+1}, I)$. Let G be a K-form of SL_{n+1} of subtype ${}^2A_n$. Then there exists an isomor-

phism $f : SL_{n+1} \longrightarrow G$ over $\bar{K}$ and if $s \in g_{\bar{K}/K}$, $a_s = f^{-1} \circ {}^s f$ is a 1-cocycle of $g_{\bar{K}/K}$ in $(\text{Aut } SL_{n+1})_{\bar{K}}$; but we have seen that $(\text{Aut } SL_{n+1})_{\bar{K}} = \text{Aut } (M_{n+1}(\bar{K}) \oplus M_{n+1}(\bar{K}), I$. Hence (a_s) is a 1-cocycle of $g_{\bar{K}/K}$ in Aut $(M_{n+1}(\bar{K}) \oplus M_{n+1}(\bar{K}), I$ so that we can twist $M_{n+1} \oplus M_{n+1}$ by the cocycle (a_s); the twisted algebra A will carry an involution J of the second kind; in this process the center $K \oplus K$ of $M_{n+1} \oplus M_{n+1}$ will get twisted into the center of A; now Symm $(SL_{n+1}) = Z_2$ and since G is of type ${}^2A_n$ the homomorphism $s \longrightarrow \lambda(a_s)$ of $g_{\bar{K}/K}$ into Symm $(SL_{n+1}) = Z_2$ is non-trivial where λ is the homomorphism $\lambda : \text{Aut}(SL_{n+1}) \longrightarrow Symm(SL_{n+1})$ appearing in the split sequence. **33**

$$1 \to Ad(SL_{n+1}) \to Aut(SL_{n+1}) \to Symn(SL_{n+1}) \to 1$$

.

Hence by 1.7 example 2 Chapter 1 we conclude that the centre $K \oplus K$ of $M_{n+1} \oplus M_{n+1}$ gets twisted into a quadratic extension L of K. Hence A is a simple K-algebra with involution J of the second kind with center a quadratic extension L of K. Now the image of SL_{n+1} under the imbedding $\varphi : SL_{n+1} \longrightarrow M_{n+1} \oplus M_{n+1}$ constructed above is given by $\left\{ z \in M_{n+1} \oplus M_{n+1} \middle/ zz^J = 1, Nz = 1 \right\}$; the image of this group under the isomorphism $g : M_{n+1} \oplus M_{n+1} \longrightarrow A$ got by the twisting process is $\left\{ z \in A \middle/ zz^J = 1, Nz = 1 \right\}$. Hence taking into consideration the various identifications constructed above we see that G is isomorphic to the algebraic group $\left\{ z \in A \middle/ zz^J = 1, Nz = 1 \right\}$ where A is a simple K-algebra with an involution of the second kind with center a quadratic extension of K.

Next we shall consider the K-forms of the Chevally group of type C_n. Hence the Chevalley group is the symplectic group $Sp_{2n} = \left\{ X \in M_{2n} \middle/ XS\,{}^tX = S \right\}$ where S is a non-degenerate skew-symmetric matrix over K. We shall show that the K-forms of Sp_{2n} are given by $\left\{ x \in A \middle/ xx^J = 1 \right\}$ where A is an algebra with involution of the first kind J, simple with center K and which becomes isomorphic to (M_{2n}, I) over

$\bar{K}$, I being the involution $X \longrightarrow S^t X S^{-1}$. The automorphisms of M_{2n} are all inner automorphisms and the inner automorphism $X \longrightarrow uXu^{-1}$ commutes with I and only if $uu^I \in K$ above, and again over $\bar{K}$ we may assume $uu^I = 1$, which means that $u \in Sp_{2n}$.

34 On the other hand it is known that the only automorphisms of Sp_{2n} are inner automorphisms; hence Aut Sp_{2n} Aut (M_{2n}, I). We can then apply the foregoing method to characterise the K-forms of Sp_{2n}, the result being as indicated in the beginning of this paragraph.

Finally we shall consider the K-forms of Chevalley groups of types B and D. Here the Chevalley group is $\mathrm{Spin}_n(\mathscr{G})$; n may be even or odd $n \neq 1, 2, 3, 4, 5, 6$; and $\mathscr{G}$ is a non-degenerate quadratic form of maximal index. Now any automorphism of $SO(\mathscr{G})$ is obtained as transformation by an element of $O(\mathscr{G})$ i.e. there exists $t \in O(\mathscr{G})$ such that $x \to txt^{-1}$ is the automorphism in question; but we have seen that any $t \in O(\mathscr{G})$ gives an automorphism of the Clifford algebra of $(\mathscr{G})$ (cf. 2.2) and so an automorphism of the spin group. All the automorphisms of $\mathrm{Spin}(\mathscr{G})$ are obtained in this way through automorphisms of $SO(\mathscr{G})$ except in case D_4 i.e. Spin_8. This is seen as follows: it is clear that the mapping τ : Aut $(SO) \to$ Aut (Spin) constructed above is injective; we have seen in 2.2 that an inner automorphism of Spin $(\mathscr{G})$ by an element t corresponds to an element u of SC and by construction $\tau(\mathrm{int}\, u) = \mathrm{int}\, t$ so that τ induces an isomorphism of $Ad(SO)$ onto Ad(Spin); the index of Ad(Spin)*in* Aut (Spin) is equal to the number of symmetries of the Dynkin diagram of the Spin group which is equal to 1 if the dimension is odd; if n is even $\neq 8$, the number of symmetries is 2, but also the index of $AD(SO)$ in Aut $(SO) = Ad(O)$ is 2 because transformation by a reflection is not an inner automorphism of SO. Hence τ is a bijection in these cases.

35 This shows that the simply connected almost simple classical groups of type B and D are two fold coverings of the K-forms of the special orthogonal group except when the dimension =8 i.e. in the case D_4. For type D_4, every two fold covering of an orthogonal group SO_8 is easily seen to be of type ${}^1D_4$ or ${}^2D_4$. Conversely, in the homomorphism of $g_{\bar{K}/K}$ into Symm G obtained from the twisting cocycle of a group of type D_4 has image of order 1 or 2 this image can be transformed by an inner

automorphism into the group of automorphisms induced by $O(\mathscr{G})$, and therefore these K-forms are coverings of K-forms of $SO(\mathscr{G})$. Hence classical groups of dimension 8 which are K-forms of Spin_8 are two-fold coverings of the K-forms of SO_8. Hence in all cases we find that the classical groups which are K-forms of Chevalley groups of type B and D are two fold coverings of the K-forms of the special orthogonal group. So we have only to find the K-forms of $SO(\mathscr{G})$. Let a be the matrix of the quadratic from $(\mathscr{G})$ in some basis; on M_n define the involution I by $X^I = a^t X a^{-1}$, $a \in M_n$. Using the fact that the automorphisms of M_n are all inner we can prove as before that the only automorphisms of M_n commuting with I are inner automorphisms by elements of $0(\mathscr{G})$. Moreover one knows that the automorphisms of SO are given by transformation by elements of $O(\mathscr{G})$; hence over $\bar{K}$ we have an isomorphism Aut $SO(\mathscr{G}) \cong$ Aut (M_n, I). Carrying out exactly the same procedure as before it is easily seen that the K-forms of $SO(\mathscr{G})$ are given by $G = \left\{ x \in A \middle| xx^J = 1, Nx = 1 \right\}$ where A is a simple K-algebra with involution J of the first kind which becomes isomorphic over $\bar{K}$ to (M_n, I). Hence we have proved that simply connected almost simple **36** classical groups of types B and D are two fold coverings of groups G given above.

2.5 Algebras with involution (cf. [1] Chap X)

Let A be a simple K-algebra with center L; let I be an involution on A. If J is another involution on A coinciding with I on L then by the theorem of Skolem-Noether we can find an invertible element $a \in A$ such that $x^J = a x^I a^{-1}$ holds for every $x \in A$. Now, $x = x^{JJ} = a(a x^I a^{-1})^I a^{-1} = (a a^{-I}).x(a a^{-I})^{-1}$ for every $x \in A$, so that $a a^{-1} \in L$. Let $a^I = ca$ where $c \in L$; applying I to both sides we get $cc^I = 1$. If the involution is of the first kind (See 2.4 for the definition) $cc^I = 1$ implies $c^2 = 1$ i.e. $c = \pm 1$ so that $a^I = \pm a$. Suppose now that I is of the second kind, let F be the fixed field of I in A; then since I is of period 2, L is a quadratic extension of F and the condition $cc^I = 1$ is equivalent to $N_{L/F}(c) = 1$. Hence by Hilbert's theorem 90, there exists $d \in L^*$ such that $c = d^I d^{-1}$.

Therefore $a^I = ca = d^I d^{-1}a$, i.e $(d^{-1}a)^I = d^{-1}a$. Moreover the equation $x^J = ax^I a^{-1}$ is unaltered if we replace a by $d^{-1}a$ since $d \in L$. Hence if I is of the second kind we can assume in the equation $x^J = ax^I a^{-1}$ that $a^I = a$.

Examples of algebras with involution: A quaternion algebra with the standard involution $x \to \bar{x}$, the conjugate of x, is a simple algebra and the standard involution is of the first kind. If D is any division algebra over K then $M_n(D)$ has an involution of the r^{th} kind ($r = 1, 2$) if and
37 only if D has an involution of the r^{th} kind; for if I in an involution of the rth kind on D then if we define X^J for $X = (x_{ij}) \in M_n(D)$ as $X^J = (x_{ji}^I)$ we get an involution of the r^{th} kind; the converse follows from Theorem 1 below by taking $A = M_n(D)$, $B = M_n(K)$.

Next let A be a simple K-algebra with an involution I; let L be the center of A. Suppose B is a given K-subalgebra of A containing L and assume moreover that B carries an involution J coinciding with I on L. When can J be extended to an involution on A? Sufficient conditions under which this is possible are given by the following

Theorem. *With the notations as above J can be extended to an involution on A in the following cases:*

i) B is a simple algebra

ii) B is a maximal commutative semi-simple subalgebra of A and I is of the second kind.

Proof. I o J is an isomorphism of the L-algebra B into the simple algebra A with center L so that in case i) by the theorem of Skolem-Noether we can find an invertible element $t \in A$ such that $x^{IoJ} = (x^J)^I = txt^{-1}$ for every $x \in B$; this conclusion holds true also when B is a maximal commutative semi-simple subalgebra of A [15] Hilfssatz 3.5. Let B' be the commutant of B in A; let $L(u)$ be the K-subalgebra generated by $u = t^{-I}t$. If v is any element of B' and if we replace t by tv in $x^J = (txt^{-1})^I x \in B$
38 found above this equality is unaltered; we shall choose a suitable $v \in B'$ and replace t by tv in the final stage to obtain an involution extending J; for the moment let $u = t^{-I}t$ with t as given above. Define for every

$x \in A$, $x^{\widetilde{J}} = (\mathrm{txt}^{-1})^I$; then by what precedes $\widetilde{J}$ coincides with J on B; moreover if $x \in B$, $x^{\widetilde{J}^2} = (tx^J t^{-1})^I = t^{-I}\cdot(x^J)^I\cdot t^I = t^{-I}(txt^{-1})\cdot t^I = uxu^{-1}$; but $x^{\widetilde{J}^2} = x^{J^2} = x$ since $x \in B$ so that $uxu^{-1} = x$ implying that $u \in B'$ and hence $L(u) \subset B'$. It will turn out the we can choose $v \in L(u)$ suitably so that when t is replaced by tv, and $\widetilde{J}$ defined as above with this new t then $\widetilde{J}$ will be an involution on A, extending J on B. The equation $x^{\widetilde{J}^2} = uxu^{-1}$ shows that if we choose $v \in B'$ to satisfy $(tv)^{-I}(tv) = \pm 1$ then with tv in place of t the equation $x^{\widetilde{J}^2} = x$ will hold for all $x \in A$ and consequently $\widetilde{J}$ will be an involution on A; evidently $\widetilde{J}$ will then be an extension of J on B. We shall prove that $v \in L(u)$ can be chosen so as to satisfy $(tv)^{-I}(tv) = \pm 1$. Observe that

$$u^{\widetilde{J}}u = (tut^{-1})^I.u = (t^{-I}.u^I.t^I).(t^{-I}.t) = t^{-I}u^I.t = t^{-I}.t^I.t^{-I}.t = 1$$

hence $u^{\widetilde{J}} = u^{-1}$. Consider case *i*) first. If $u = -1$, then evidently the choice $v = 1$ will do, so assume $u \neq -1$. To start with assume B' to be a division algebra; the condition $(tv)^{-I}tv = 1$, is equivalent to $v^{-\widetilde{J}}uv = 1$; we claim that $v = (1+u)^{-1}$ which is obviously an element of $L(u)$ will work; for $v^{-\widetilde{J}} = 1 + u^{\widetilde{J}} = 1 + u^{-1} = (1+u)\cdot u^{-1} = v^{-1}.u^{-1}$ so that $v^{-\widetilde{J}}uv = 1$. Suppose now B' is not necessarily a division algebra, we can write $B' \cong D \otimes M_n$ where M_n is the full matrix ring of dimension n^2 for some n and D is a division algebra. We can then consider D, M_n **39** as subalgebras of A; the commutant of the subalgebra BM_n is equal to the commutant of M_n is B', i.e. to D. Now the involution J on B can be extended to BM_N by defining $(bX)^{J'} = b^{Jt}X$, $b \in B$, $X \in M_n$. Moreover BM_n is a simple algebra being L-isomorphic to $B \otimes_L M_n$ which is simple. Hence by the case already considered the involution J' can be extended to an involution of A; this extension clearly coincides with J on B.

Next consider case *ii*). Here again we shall find $v \in L(u)$ to satisfy $(tv)^{-I}(tv) = 1$ i.e. $v^{-\widetilde{J}}uv = 1$. Since $u^{\widetilde{J}} = u^{-1}$, $\widetilde{J}$ maps $L(u)$ onto itself; it is an involution of $L(u)$ of the second kind. Let F be the fixed field of $\widetilde{J}$ in L. Let C^+ be the subalgebra of elements of $L(u)$ fixed by $\widetilde{J}$; since $\widetilde{J}$ is not the identity on L, $L(u) \cong C^+ \oplus_F L$; moreover under this isomorphism the action of $\widetilde{J}$ on $L(u)$ goes over into the natural action of the Galosi group $g_{L/F}$ of L/F on $C + \otimes_F L$. The elements of $g_{L/F}$ are 1 and $\tilde{J}$; the correspondence $\tilde{J} \to u^{-1}$, $1 \to 1$ defines a 1-cocycle of $g_{L/F}$

in $(C^+ \otimes_F L)^*$. By 1.7 Chapter 1 we know that $H^1(L/K, (C^+)^*) = 1$; hence there exists $v \in L(u)$ such that $v^{-1}u^{-1}v^{\bar{J}} = 1$, i.e. $v^{-\bar{J}}uv = 1$. But this is what we wanted. Hence the theorem is completely proved.

If A is a central simple algebra over K and if A has an involution I of the first kind then A is of order 1 or 2 in the Brauer group of K; for I gives an isomorphism of A with its opposite algebra A^o hence $A \otimes_k A \cong A \otimes_k A^0$
40 splits. But if I is of the second kind A is not necessarily isomorphic over the centre to its opposite algebra, so may not have order 2 in the Brauer group (for an example see §5.1). But let us consider the particular case where A is a quaternion algebra with centre L and assume that I is an involution of the second kind. Let K be the subfield of L fixed by I so that L is a quadratic extension of K. Let J be the standard involution on A namely conjugation; this is the only involution on A which fixes exactly the elements of L. The involution IJI^{-1} fixes the centre so that $IJI^{-1} = J$, i.e. $(IJ)^2 =$ identity. Let B be the fixed space of IJ in A; then B is a K-subalgebra of A, and $A \cong B \otimes_K L$ since IJ is not the identity L. Hence we have proved the following □

Proposition 1. *If A is a quaternion algebra of centre L and has an involution I of the second kind then $A \cong B \otimes_K L$ where B is an algebra over the fixed field K of I. Moreover I coincides with the standard involution on B and on L it coincides with the non-trivial K-automorphism.*

2.6 Bilinear and hermitian forms; discriminants

Let D be a division algebra; let $x \to \bar{x}$ be an involution; let V be a n-dimensional left vector space over D. A sesquilinear form on V is a function $B : V \times V \to D$ taking (x, y) to $B(x, y)$ which is linear in x and anti linear in y (i.e. $B(x, \alpha y) = B(x, y)\bar{\alpha}$ for every $x, y \in V, \alpha \in D$), B is called hermitian if we have $B(x, y) = \overline{B(y, x)}$ for every pair
41 of vectors $x, y \in V$; B is called skew hermitian if $B(x, y) = -\overline{B(y, x)}$ for every pair of vectors $x, y \in V$. Let $h(x) = B(x, x)$; we shall call h a hermitian or skew hermitian form according as B is a hermitian or skew-hermitian sesquilinear form. If $e_1, \ldots, e_n$ is a D-basis of V, then the matrix $(B(e_i, e_j))$ is said to be the matrix of B relative to this basis.

Call this matrix M. If $e'_1, \ldots, e'_n$ is any other basis of V let $e'_i = \sum_{i=1}^{n} \alpha_{ji} e_i$ and denote the matrix (α_{ij}) by the letter T; then the matrix of B in the basis $e'_1, \ldots, e'_n$ is just ${}^tT M \bar{T}$. We define the radical of V as the space of elements $x \in V$ such that $B(x, y) = 0$ for every $y \in V$. B is said to be non-degenerate if the radical is zero. Any hermitian space V has an orthogonal basis i.e. a basis $e_1, \ldots, e_n$ such that $B(e_i, e_j) = 0$ if $i \neq j$; for e_1 one can choose any anisotropic vector i.e such that $B(e_1, e_1) \neq 0$. If V, V' are two hermitian spaces over D withe corresponding hermitian form B, B' then a D-linear transformation $\sigma : V \to V'$ is called an isometry if σ is bijective and $B(x, y) = B(\sigma x, \sigma y)$ for every $x, y \in V$. In particular if $V = V'$ the set of isometries of V onto itself will be a group called the unitary group of the hermitian form. We have similar notions for skew-hermitian forms over D.

Let V be a finite dimensional vector space over K endowed with a quadratic form $\mathscr{G}$ which we assume to be non-degenerate. The determinant of the matrix of $(V, \mathscr{G})$ with respect to any basis of V/K is unique modulo squares of K^*, i.e. it is a well defined element of K^*/K^{*2}. We call this element of K^*/K^{*2} the discriminant of V. Quite frequently a **42**
representative in K^* will be called the discriminant of V; this will not involve any confusion as the context will make it clear what we have in mind. Let D be a quaternion division algebra over K with the standard involution; let V be a finite dimensional left vector space over D. If h is a hermitian of skew hermitian form on V the discriminant of h is by definition the reduced norm of a matrix representing h, modulo squares of elements of K^*. We shall state and prove a number of lemmas which we shall need in the sequel.

Lemma 1. *a) Let D be a quaternion algebra over K; let h be a non-degenerate hermitian or skew hermitian form on a finite dimensional vector space V of D. Then if D does not split, the special unitary group $SU(h, D)$ of h coincides with the unitary group $U(h, D)$. More generally we shall prove the following*

Lemma 1. *b) Let A be a simple central K-algebra with an involution I of the first kind. If there exists an element $x \in A$ satisfying $xx^I = 1$ and $Nx = -1$, then $A \cong M_n(K)$.*

Proof. We look at the eigen values of x considered as an element of $A \otimes_K \bar{K} \cong M_n(\bar{K})$. Since every involution of $M_n(\bar{K})$ is transposition followed by an inner automorphism, x and x^I have the same eigenvalues. But $x^I = x^{-1}$, so x and x^{-1} have the same set of eigenvalues and with equal multiplicities. This implies that the eigenvalues of x different from ± 1 occur in pairs (λ, λ^{-1}). Since the product of the eigenvalues is equal to the reduced norm of x, -1 must occur as eigenvalue with odd multiplicity. □

43 This shows that 0 is an eigen value of $x+e$ (e denoting the identity of A) of odd multiplicity. Hence if the integer m is sufficiently large the null space of $(x+e)^m$ is of odd dimension.

Now go back to the ground field K. We can write $A \cong M_k(D)$. Let $n^2 = [A : K]$; we then have $[D : K] = (n/k)^2$. The lemma will be proved if we show that $[D : K] = 1$. For this we compute the dimension over K of the K-space $\Lambda = \{y \in M_k(D) | (x+e)^m . y = 0\}$, in two different ways and compare them.

Let V be a K-dimensional left vector space over D. We can then interpret $(x+e)^m, y$ as linear transformations on V. Then $y \in \Lambda$ if and only if y maps V into the kernel of $(x+e)^m$. From this description of the elements of Λ it is easy to see that $[\Lambda : D] = k.r$, where r denotes the dimension over D of the kernel of $(x+e)^m$. Hence $[\Lambda : K] = k.r[D : K] = k.r(n/k)^2 = nr(n/k)$. On the other hand $[\Lambda : K] = [\Lambda_{\bar{K}} : \bar{K}]$. Now $\Lambda_{\bar{K}}$ is equal to $\left\{y \in M_n(\bar{K}) / (x+e)^m y = 0\right\}$ so that by the same argument as above with D replaced by $\bar{K}$ we get $[\Lambda_{\bar{K}} : \bar{K}] = n(\dim_{\bar{K}} \ker(x+e)^m)$. But by the first part of the proof $\dim_{\bar{K}} \ker(x+e)^m$ is an odd integer. Hence $[\Lambda : K] = nx$ an odd integer. Comparing the two values of $[\Lambda : K]$ obtained we get $nxodd$ integer $= n.r(n/k)$. This implies n/k is odd integer. i.e. $[D : K]$ is an odd integer. Now A being an algebra with involution of the first kind it has order two in the Brauer group. But one knows that the prime divisors of the order of A in the Brauer group and those of $[D : K]$ are the same. The last two conclusions can hold simultaneously only when $[D : K] = 1$.

This proves the lemma.

44 **Lemma 2.** *Let D be a quaternion algebra over K with an involution I,*

$A = M_n(D)$; for $Z = (z_{ij}) \in A$ denote by Z^* the element (z^I_{ji}). Let $a \in A$ be a non-singular skew-hermitian matrix, i.e. $a^* = -a$. Then if X, Y are $1 \times n$ matrices over D such that $XaX^* = YaY^* = C$ is non-singular in D, there exists a proper a-unitary matrix $t \in A$ such that $Y = Xt$.

Proof. If D is a division algebra, this follows immediately from Witt's theorem and lemma 1. If $D = M_2(K)$, the action of I is as follows: $\alpha \to S^t \alpha S^{-1}$ where S is some fixed 2×2 skew-symmetric matrix in $M_2(K)$. Denoting by P the $2n \times 2n$ matrix $\begin{pmatrix} S & & \\ & S & \\ & & \cdot S \end{pmatrix}$ we have $X^* = P^t X S^{-1}$, $Y^* = p^t Y S^{-1}$ and $a^* = p^t a p^{-1}$. Now since $a^* = -a$, we have $p^t a p^{-1} = -a$ which implies that $aP = -P^t a = {}^t(ap)$. This shows that aP is a symmetric $2n \times 2n$ matrix. The condition $XaX^* = c$ then gives $X(aP)^t X = cS$; similarly the condition $YaY^* = c$ gives $Y(aP)^t Y = cS$. The matrix aP gives a $2n \times 2n$ dimensional quadratic space over K and the above two equations imply that the two dimensional subspaces generated by the two rows of X and Y respectively are isometric. Hence by Witt's theorem on quadratic form there exists an isometry t of the above quadratic space transforming X into Y. If t is not proper then by multiplying t on the right by a reflection in a suitable subspace containing the two rows of X we can make the product proper. Hence t can be assumed proper. This t then defines a proper unitary transformation changing X into Y. □

Lemma 3. *Let D be a quaternion division algebra with standard involution; (V, h) and (V', h') are two skew hermitian spaces over D. Let $f : (V_{\bar{K}}, h) \to (V'_{\bar{K}}, h')$ be an isomorphism over $\bar{K}$; then the 1-cocycle $a_s = f^{-1} o^s f$ which belongs to $H^1(K, U)$ comes from $H^1(K, SU)$ if and only if the discriminants of (V, h) and (V', h') are equal; here U denotes the unitary group and SU denotes the special unitary group of h.* 45

Proof. Consider the exact sequence $1 \to SU \to U \to Z_2 \to 1$ where $U \to Z_2$ is the norm mapping; this gives rise to an exact sequence $H^1(SU) \to H'(U) \to H^1(Z_2)$; but clearly $H^1(Z_2) \cong K^*/K^{*2}$ and $H^1(U) \to K^*/K^{*2}$ is the map associating with each K-form (V', h') of

(V, h) the quotient of the discriminants of h' and h. This shows that (a_s) comes from $H^1(SU)$ if and only if V' has the same discriminant as V.

Next we shall determine the simply connected absolutely almost simple classical groups of types B_n, C_n, D_n over fields K satisfying the property that every division of order 2 in the Brauer group B_L for any algebraic extension L is a quaternion algebra. Examples of such fields are the $\mathscr{P}$-adic fields and number fields [8]. If A is a central simple involutorial algebra over such a field K then since its order in Brauer group is either 1 or 2 we conclude that either A is a matrix algebra over K or a matrix ring over a quaternion division algebra over K. We make use of the classification given in 2.4. Consider $G = \{x \in A / xx^I = 1\}$ where A
46 is a central simple K-algebra with involution I of the first kind. There are two possibilities *i*)$A \cong M_r(K)$ or *ii*)$A \cong M_s(C)$ where C is a quaternion division algebra over K. In the first case there exists an invertible $a \in M_r(K)$ either symmetric of skew-symmetric such that $X^I = a^t X a^{-1}$ for every $X \in M_r(K)$. If a is skew-symmetric G is the symplectic group of the alternating form a and so belongs to type C_n; but if a is symmetric we get the orthogonal group which will correspond to type B_n, D_n by taking two-fold coverings of the special orthogonal group. In the second case when $A \cong M_s(C)$, C being quaternion division algebra we get $x^I = a x^* a^{-1}$ where $x \to x^*$ is the involution on $M_s(C)$ given by $(x_{ij}) \to (\bar{x}_{ji})$, denoting the standard involution on C and where a is either hermitian or skew hermitian with respect to *. In the first case $xx^I = 1$ means that x is in the unitary group of the hermitian form while in the second case it means that x is in the unitary group of the skew-hermitian form a. Consideration of the dimension of the space of symmetric elements will show that the former corresponds to type C_n while the latter to type D_n. Hence we have the □

Theorem. *The only simply connected absolutely almost simple Classical groups of types B_n, C_n, D_n over a field with the properties stated above are*
C_n: Symplectic groups and unitary groups of hermitian forms over quaternion division algebras
B_n, D_n: Spin groups of quadratic forms and of skew hermitian forms over quaternion division algebras.

Chapter 3

Algebraic Tori

3.1 Definitions and examples ([6], [7])

Definition of G_m. This is the algebraic group defined over the prime field of the universal domain such that for any field K, the K-rational points of G_m is K^*.

Notation If G is an algebraic group and L a field of definition we denote by G_L the group of L-rational points of G.

Definition. *An algebraic group G is said to be a torus if it is isomorphic to a product of copies of G_m; a field L is said to be a splitting field of G if this isomorphism is defined over L.*

Example. 1) Let L/K be a finite separable extension of fields. We define an algebraic group L^* as follows: $(L^*)_{\bar{K}}$ = units of $L \otimes_K \bar{K}$; choosing a basis of L/K we get a basis for $L \otimes_K \bar{K}$ over $\bar{K}$ and with respect to this basis multiplication by a unit of $L \otimes_K \bar{K}$ is an element of $GL(n, \bar{K})$ where $n = [L : K]$. This makes $(L^*)_{\bar{K}}$ into a closed subgroup of $GL(n, \bar{K})$. Now $L \otimes_K \bar{K} \tilde{=} \bar{K} \otimes \cdots \otimes \bar{K}$. (Here we use the fact that L/K is separable). Hence $L^*_{\bar{K}} \tilde{=} (\bar{K}^*)^n$; this shows that L^* is an algebraic torus. Any Galois extension of K containing L is a splitting field of L^*.

2) Let L/K be as above; define an algebraic group G by the requirement $G_{\bar{K}} = \{x \in (L \otimes_K \bar{K})^* / Nx = 1\}$; this consists of those elements $(x_1, \ldots, x_n)$ of $(\bar{K}^*)^n$ with $x_1 \cdots x_n = 1$. Hence G is an algebraic torus isomorphic to G_m^{n-1} over $\bar{K}$.

48 **Example 3.** SO_2 for a non-degenerate quadratic form $\mathscr{G}$ is an algebraic torus.

Let V be the corresponding quadratic space. Let e_1, e_2 be an orthogonal basis of V with $q(e_2) = cq(e_1)$. Then the orthogonal group of V consists of matrices of the form $\begin{pmatrix} \lambda_1 & \lambda_2 \\ -c\lambda_2 & \lambda_1 \end{pmatrix}, \begin{pmatrix} \lambda_1 & \lambda_2 \\ +c\lambda_2 & -\lambda_1 \end{pmatrix}$ with λ_1, $\lambda_2 \in K$ and $\lambda_1^2 + c\lambda_2^2 = 1$; hence the special orthogonal group of V consists of the matrices $\begin{pmatrix} \lambda_1 & \lambda_2 \\ -c\lambda_2 & \lambda_1 \end{pmatrix}$ with $\lambda_1^2 + c\lambda_2^2 = 1$. Such matrices are isomorphic to the group of elements of norm 1 in the quadratic extension $K[X]/_{(x^2+c)}$ of K; hence SO_2 is an algebraic torus.

Another example is the following.

Example 4. If h is a skew hermitian form on the quaternion division algebra C over K then $SU_1(C/K, h)$, the special unitary group is an algebraic torus.

If T is a torus defined over K then there exists a finite Galois extension L of K which is a splitting field of T. This is because the rational functions defining the isomorphism $T \cong G_m^n$ are finite in number and we can adjoin the coefficients of these to K to get a field L'; the field we require can be taken to be some finite normal extension L of K containing the field L'.

Theorem 1. *Suppose T is an algebraic torus defined over K; let L be a splitting field of T; then if $X = \mathrm{Hom}(G_m, T)$ we have $T_L \cong X \otimes_Z L^*$.*

49 *Here* $\mathrm{Hom}(G_m, T)$ *denotes the set of morphisms of G_m into T defined over L and which are also group homomorphisms.*

Proof. Consider the map $L^* \otimes_Z \mathrm{Hom}(G_m, T) \to T_L$ defined by $x \otimes f \to f(x)$. This makes sense since f is defined over L so that $f(x) \in T_L$. This is an isomorphism. For if $T \cong G_m^n$ over L, $T_L \cong G_m(L)^n = (L^*)^n$; also

$L^* \otimes_Z \mathrm{Hom}(G_m, T) \tilde{=} L^* \otimes_Z Z^n \tilde{=} (L^*)^n$; after these identifications the map defined above becomes the identity map of $(L^*)^n$ onto itself. This proves the theorem. □

Remark. If L/K is a Galois extension then $g_{L/K}$ acts on $X = \mathrm{Hom}(G_m, T)$ so that if $f : G_m \to T$ is an element of X, ${}^s f({}^s x) = {}^s(f(x))$; it therefore acts on $X \otimes_Z L^*$ too. Then the above isomorphism is an isomorphism of $g_{L/K}$-modules $L^* \otimes_Z X$ and T_L.

If T is an algebraic torus and $\widetilde{T}$ is a connected commutative group which is a covering of T, then $\widetilde{T}$ is also an algebraic torus. For if $0 : \widetilde{T} \to T$ is the covering an if $x \in \widetilde{T}$ is unipotent then $p(x)$ will be unipotent and since T is a torus $p(x) = 1$; hence $\widetilde{T}_u$, the unipotent part of T is contained in the kernel of p which is finite. Hence $\widetilde{T}_u$ being connected, it is $\{1\}$, and so $\widetilde{T}$ consists only of semisimple elements and being commutative and connected it is an algebraic torus.

3.2 Class Field Theory

In this section we shall list some of the results of class field theory we require without proofs. For proofs see the references S_1, T_a

a) Local class field Theory. **50**

Let K be any field. We denote by B_K the Brauer group of K; it is defined to be the inductive limit of $H^2(g_{L/K}, L^*)$ where L/K runs through the set of finite Galois extensions and the limit is taken with respect to the inflation homomorphisms. Alternatively, consider the class ℓ of simple algebras over K with centre K. If A, A' are two such algebras we know by Wedderburn's theorem that $A \cong M_n(D)$, $A' \cong M_{n'}(D')$ where D, D' are division algebras. The integer n and the isomorphism class of D characterise A upto isomorphism; similarly n' and the isomorphism class of D' characterise A', upto isomorphism; We shall say $A \sim A'$ if $D \cong D'$. Let $B_K = \ell/\sim$ be the set of equivalence classes; B_K is then made into a group as follows: if A, B are representatives of two classes of B_K then the equivalence class of $A \otimes_K B$ depends only on those of A and B so that we get a map $B_K \times B_K \to B_K$. This composition

makes B_K into a group, the identity element being the equivalence class of K and the inverse of a class with representative A is the class with representative A^o, the opposite algebra of A.

Now let K be a p-adic field, i.e. a field complete under a discrete valuation, with finite residue class field.

Theorem 2 (cf. [8])**.** *There is a canonical isomorphism $B_K \cong Q/Z$. If A is a simple algebra over K with center K then the image of its class under the above isomorphism is called the Hasse - invariant of A; if we denote this invariant by $inv_K(A)$ then for any finite extension L of K. We have $inv_L(A \otimes_K L) = [L : K] inv_K(A)$. We have further*

51 **Theorem 3.** *If A is a central simple algebra over K then it is split by an extension L of K with the property $[L : K]^2 = [A : K]$.*

Another theorem which we will need is the following theorem of Tate and Nakayama ([18], IX, §8):

Theorem 4 (Nakayama-Tate)**.** *Let G be a finite group, A a G-module, an (a) an element of $H^2(G, A)$. For each prime number P let G_P be a p-Sylow subgroup of G, and suppose that*

1) $H^1(G_p, A) = 0$

2) $H^2(G_p, A)$ is generated by Res $G/G_p(a)$ and the order of $H^2(G_p, A)$ is equal to that of G_p.

Then, if D is a G-module such that for $(A, D) = 0$, the cup multiplication by $(a_g) = ResG/g(a)$ induces an isomorphism

$$\hat{H}^n(g, D) \to \hat{H}^{n+2}(g, A \otimes D)$$

for every $n \in Z$ and every subgroup g of G.

In this theorem the Tate cohomology groups $\hat{H}$ are defined as follows ([18], VIII, §1):

$$\hat{H}^n(G, A) = H^n(G, A) \text{ for } n \geq 1$$
$$\hat{H}^o(G, A) = A^G/NA \text{ where } N : A \to A$$
is the norm homomorphism defined

$$\text{by } N(a) = \sum_{s \in G} s_a$$
$$\hat{H}^{-1}(G, A) = {}_N A / IA$$

where ${}_N A$ denotes the kernel of the norm mapping and I is the augmentation ideal of $Z(G)$ generated by the elements $1 - s$ with $s \in G$.

$\hat{H}^{-n-1}(G, A) = H_n(G, A)$, the n^{th} homology group for $n \geq 1$.
If L/K is a finite Galois extension of the adic field K then $H^2(g_{L/K}, L^*)$ is **52**
a cyclic group generated by the 'fundamental class' (a) and is of order equal to $[L : K]$. Condition 2) of the present theorem for $g = g_{L/K}$, $A = L^*$ is an easy consequence of the property of Hasse invariant stated under theorem 2.

Using the theorem we can prove the following

Theorem 5. *Let T be an algebraic torus over K split by the finite Galois extension L; with the notations of theorem 1 we have $\hat{H}^{n+2}(g_{L/K}, T) \cong \hat{H}^n(g_{L/K}, X)$.*

Proof. By theorem 1 we know that $\hat{H}^{n+2}(g_{L/K}, T) \cong \hat{H}^{n+2}(g_{L/K}, X \otimes_Z L^*)$. We shall apply theorem 4. Condition 1) is Hilbert's theorem 90 (cf. §1.7, example 1). We have just seen that conditions 2) is satisfied. Since X is a free abelian group $\mathrm{Tor}_l(X, L^*)$ is zero. Hence cup multiplication by the fundamental class of $H^2(g_{L/K}, L^*)$ induces by theorem 3 an isomorphism

$$\hat{H}^{n+2}(g_{L/K}, X \otimes_Z L^*) \simeq \hat{H}^n(g_{L/K}, X)$$

which proves the result. □

3.3 Global class field Theory.

Let K be a number field and N a finite Galois extension with Galois group g; we shall employ the following notations:
$I = I_N$ - the idele group of N

$C = C_N$ - the idele class group of N, i.e. I_{N/N^*} where N^* is imbedded in I_N by the map $a \to (\ldots, a, \ldots)$.
$\overline{v}$ - places of N **53**
v - place of K
∞ - the set of infinite places.

To any given place v of K we choose an extension $\overline{v}$ of v to N and keep it fixed; this extension is denoted by $h(v)$; $g_{h(v)}$ is then used to denote the Galois group of the extension $N_{h(v)}/K_v$, which is the decomposition group of $h(v)$.
Z - the ring of rational integers
Y - the free abelian group generated by the set of places of N.
If $s \in g$ and $\overline{v}$ a place of N then ${}^s\overline{v}$ denotes the place of N defined by $|x|_{{}^s\overline{v}} = |x|_{\overline{v}}$; g acts on Y by the rule ${}^s(\sum n_{\overline{v}}\overline{v}) = \sum n_{\overline{V}^{\overline{s}}}$; W - kernel of the surjective g-homomorphism $Y \to Z$ defined by

$$\sum n_{\overline{v}}.\overline{v} \to \sum n_{\overline{v}}.$$

With these notations we shall explain a result of Nakayama and Tate which we shall use in the study of 'Hasse Principle' in number fields.

We compare the two exact sequences of g-modules:

$$1 \longrightarrow N^* \longrightarrow I \longrightarrow C \longrightarrow 1 \tag{1}$$
$$1 \longrightarrow W \longrightarrow Y \longrightarrow Z \longrightarrow 1 \tag{2}$$

Tate's theorem then asserts that we can find elements $\alpha_1 \in H^2(g, \mathrm{Hom}(Z, C)), \alpha_2 \in H^2(g, \mathrm{Hom}(Y, I))$ and $\alpha_3 \in H^2(g, \mathrm{Hom}(W, N^*))$ such **54** that cup multiplication by these cohomology classes induce isomorphisms $\hat{H}^i(g, Z) \cong \hat{H}^{i+2}(g, C), \hat{H}^i(g, Y) \cong \hat{H}^{i+2}(g, I), \hat{H}^i(g, W) \cong \hat{H}^{i+2}(g, N^*)$; moreover there exists a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & \bar{H}^{i+2}(g, N^*) & \longrightarrow & \bar{H}^{i+2}(g, I) & \longrightarrow & \bar{H}^{i+2}(g, C) & \longrightarrow & \cdots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
\cdots & \longrightarrow & \hat{H}^i(g, X) & \longrightarrow & \hat{H}^i(g, Y) & \longrightarrow & \hat{H}^i(g, Z) & \longrightarrow & \cdots
\end{array} \tag{3}$$

where the vertical maps are the isomorphisms mentioned above.

Let M be a torsian free g-module; tensoring (1) and (2) with M we get exact sequences of g-modules:

$$1 \longrightarrow M \otimes N^* \longrightarrow M \otimes I \longrightarrow M \otimes C \longrightarrow 1 \qquad (1')$$

$$1 \longrightarrow M \otimes N \longrightarrow M \otimes Y \longrightarrow M \otimes Z \longrightarrow 1 \qquad (2')$$

Then Cohomology classes $\bar{\alpha}_1 \in \hat{H}^2(g, \mathrm{Hom}(M \otimes Z, M \otimes C))$, $\bar{\alpha}_2 \in \hat{H}^2(g, \mathrm{Hom}(M \otimes Y, M \otimes I))$ and $\bar{\alpha}_3 \in \hat{H}^2(g, \mathrm{Hom}(M \otimes W, M \otimes N^*))$ are constructed from α_1, α_2 and α_3 such that the cup-multiplication by these cohomology classes give isomorphisms

$$\hat{H}^i(g, M \otimes Z) \cong \hat{H}^{i+2}(g, M \otimes C)$$

$$\hat{H}^i(g, M \otimes Y) \cong \hat{H}^{i+2}(g, M \otimes I)$$

and $\hat{H}^i(g, M \otimes W) \cong \hat{H}^{i+2}(g, M \otimes N^*)$; moreover there exists a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\cdots \longrightarrow & \hat{H}^{i+2}(g, M \otimes N^*) & \longrightarrow & \hat{H}^{i+2}(g, M \otimes I) & \longrightarrow & \hat{H}^{i+2}(g, M \otimes C) & \longrightarrow \cdots \\
 & \uparrow & & \uparrow & & \uparrow & \\
\cdots \longrightarrow & \hat{H}^{i}(g, M \otimes W) & \longrightarrow & \hat{H}^{i}(g, M \otimes Y) & \longrightarrow & \hat{H}^{i}(g, M \otimes Z) & \longrightarrow \cdots
\end{array} \qquad (3')$$

where the vertical maps are the isomorphisms quoted above. **55**

Another result which we shall need is the following isomorphisms also proved in Tate's paper:

$$\hat{H}^i(g, M \otimes Y) \cong \otimes_v \hat{H}^i(g_{h(v)}, M \otimes Z) \qquad (4)$$

$$\hat{H}^i(g, M \otimes I) \cong \otimes_v \hat{H}^i(g_{h(v)}, M \otimes N_{h(v)}) \qquad (5)$$

With these preliminary discussion we shall go on to prove

Theorem 6 (a)**.** *Let T/K be an algebraic torus split by the finite Galois extension N of K; suppose N/K is cyclic or there exists a place w of K which is such that $N \otimes_K K_w$ is a field, i.e. there exists a unique extension of w to N; then for any i the canonical map*

$$\hat{H}^i(g, T_N) \longrightarrow \prod_v \hat{H}^i(g_{h(v)}, T_{N_{h(v)}}) \qquad (6)$$

is injective; here the product on the right hand side is taken over all places v of K.

Theorem 6 (b)**.** *With the notations of theorem 6 a) let S be a finite set of places of K containing the infinite places. If the decomposition groups $g_{h(v)}$, $v \in S$ are all cyclic then the canonical map*

$$\hat{H}^i(g, T_N) \cdots \prod_{v \in S} \hat{H}^i(g_{h(v)}, T_{N_{h(v)}}) \tag{7}$$

is surjective.

Corollary. *With the above notations the canonical map*

$$H^1(K, T) \longrightarrow \prod_{v \in \infty} H^1(K_v, T)$$

is surjective.

56 **Proof of theorem 6.** a). By theorem 1, we know that $T_N \cong X \otimes N^*$ where $X = \mathrm{Hom}(G_m, T)$ this being a g-isomorphism; so that $\hat{H}^i(g, T_N) \cong \hat{H}^i(g, X \otimes N^*)$. Similarly $\hat{H}^i(g_{h(v)}, T_{N_{h(v)}}) \cong \hat{H}^i(g_{h(v)}, X \otimes N^*_{h(v)})$. Hence we have only to prove that the mapping

$$\hat{H}^i(g, X \otimes N^*) \longrightarrow \prod_v \hat{H}^i(g_{h(v)}, X \otimes N^*_{h(v)})$$

is injective. By the isomorphism (5) applied to $M = X$ we are reduced to proving the injectivity of the map

$$\hat{H}^i(g, X \otimes N^*) \longrightarrow \hat{H}^i(g, X \otimes I).$$

By (3′) this is equivalent to proving the injectivity of

$$\hat{H}^{i-2}(g, X \otimes W) \longrightarrow \hat{H}^{i-2}(g, X \otimes Y);$$

again by (3′) the latter will follow if we prove that the map

$$\hat{H}^{i-3}(g, X \otimes Y) \longrightarrow \hat{H}^{i-3}(g, X \otimes Z)$$

is surjective. We shall prove that the map

$$\hat{H}^i(g, X \otimes Y) \longrightarrow \hat{H}^i(g, X \otimes Z)$$

is surjective for all i and this will establish our result. We know by Frobenius theorem resp. by assumption there exists a place w with decomposition group $g_{h(w)} = g$; but then in (4) (with $M = X$ one component on the right hand side is $\hat{H}^i(g, X \otimes Z)$. This proves the result.

Proof of theorem 6. b). The right hand side of 7 is contained in $\otimes_v \hat{H}^i(g_{h(v)}, T_{N_{h(v)}})$. Using (3′) and (5) we are reduced to proving the following: given elements $\alpha_v \in \hat{H}^i(g_{h(v)}, T_{N_{h(v)}})$ for $v \in S$ to find elements **57**
$\alpha_v \in \hat{H}^i(g_{h(v)}, T_{N_{h(v)}})$ for $v \in S$ such that the image of the element (α_v) of $\otimes \hat{H}^i(g_{h(v)}, T_{N_{h(v)}})$ under the map $\hat{H}^i(g, X \otimes I) \to \hat{H}^i(g, X \otimes C)$ is zero; the latter question is equivalent to the following: given finitely many components corresponding to $v \in S$ in $\oplus \hat{H}^{i-2}(g_{h(v)} X \otimes Z)$ to find other components so that the resulting element of $\hat{H}^{i-2}(g, X \otimes Y)$ will have image zero under the map

$$\hat{H}^{i-2}(g, X \otimes Y) \longrightarrow \hat{H}^{i-2}(g, X \otimes Z),$$

we shall prove that this is possible for every i.

By a theorem of Frobenius since all $g_{h(v)}$'s are cyclic for $v \in S$ to any given $v \in S$ we can find a place $\overline{v}$ of N not dividing any place belonging to S such that $g_{\overline{v}} = g_{h(v)}$; such a choice is possible in infinitely many ways; let $\overline{v} = h(\hat{v})$ where $\hat{v}$ is a place of K. We can moreover assume that the $\hat{v}$'s are all different; let S^1 be the set of places $\hat{v}$ obtained in this way. Suppose we are given elements $\beta_v \in \hat{H}^i(g_{h(v)}, X)$ for $v \in S$; define an element $(x_v) \in \otimes \hat{H}^i(g_{h(v)}, X) \cong \hat{H}^i(g, X \otimes Y)$ by the requirements

$x_v = \beta_v$ for $v \in S$.

$x_{\hat{v}} = -\beta_v$ if $\hat{v}$ is such that $h(\hat{v}) = \overline{v}, v \in S$

$x_v = 0$ if $v \notin S \cup S'$

Then this element has image zero under the map $\hat{H}^i(g, X \otimes Y) \to \hat{H}^i(g, X \otimes Z)$. This proves the result.

Theorem 7. *Let K be a number field and T an algebraic torus defined* **58**
over K and split by the finite Galois extension; suppose there exists a place v of K for which there exists no non-trivial homomorphism of G_m into T defined over K_v. Then the canonical map

$$H^2(g, T_N) \longrightarrow \prod_v H^2(g_{h(v)}, T_{N_{h(v)}})$$

is injective.

Proof. With the notations of theorem 6 *a*) we have only to prove the surjectivity of the map

$$\hat{H}^{-1}(g, X \otimes Y) \longrightarrow \hat{H}^{-1}(g, X \otimes Z).$$

By (4) we have

$$\hat{H}^{-1}(g, X \otimes Y) \cong \oplus \hat{H}^{-1}(g_{h(v)}, X \otimes Z) \cong N_v^X / I_v X$$

where N_v denotes the norm mapping of $g_{h(v)}$, I_v denotes the augmentation ideal of $g_{h(v)}$ and ${}_{N_v}X$ denotes the kernel of the norm mapping. Similarly $\hat{H}^{-1}(g, X \otimes Z) \cong {}_{N_g}X / I_g X$, N_g denoting the norm mapping of g and I_g the augmentation ideal of g. If η_v denotes the map $\hat{H}^{-1}(g_{h(v)}, X) \to \hat{H}^{-1}(g, X)$ got by passage to quotients in the natural inclusion ${}_{N_v}X \to {}_{N_g}X$ then the map $\hat{H}^{-1}(g, X \otimes Y) \to \hat{H}^{-1}(g, X \otimes Z)$ is given after the above identification by the rule

$$(x_v) \to \sum \eta_v x_v$$

This shows that the proof of the theorem will be completed if we can
59 show the existence of a place v for which ${}_{N_v}X = {}_{N_g}X$ holds; we claim that the place v given in the statement of the theorem will suffice; for by assumption $(X)^{g_{h(v)}} = (\mathrm{Hom}(G_m, T))^{g_{h(v)}} = (1)$; since image $N_v \subset (X)^{g_{h(v)}}$ we must have image $N_v = (1)$ which implies that ${}_{N_v}X = X$ but then ${}_{N_g}X = X$ and so we are through. □

Chapter 4

$\mathscr{P}$-adic group

4.1 Statement of results

60

In this chapter by a $\mathscr{P}$-adic field we mean a discrete valuated complete field of characteristic zero with finite residue class field. We shall first state two theorems

Theorem 1. *Let G be a linear algebraic group defined over a $\mathscr{P}$-adic field K and assume G to be semi - simple and simply connected; then $H^1(K, G) = \{1\}$*

Theorem 2. *Let G be a semisimple and connected algebraic group defined over K; let $\tilde{G} \to G$ be the simply connected covering with kernel F. Then the mapping $\delta : H^1(K, G) \to H^2(K, F)$ obtained from the exact sequence of algebraic groups $1 \to F \to \tilde{G} \to G \to 1$ is surjective.*

Putting these together we can conclude that δ of theorem 2 is actually bijective. For $H^1(K, \tilde{G}) = \{1\}$ by theorem 1, so that only the distinguished element of $H^1(K, G)$ gets mapped into the distinguished element of $H^2(K, F)$ by δ . Now suppose two elements (a_s), (b_s) of $H^1(K, G)$ get mapped into the element of $H^2(K, F)$ by δ. Twist G by the cocycle (a_s) and call the twisted group ${}_aG$. Since G operates on $\tilde{G}$ by inner automorphisms $\tilde{G}$ can be twisted by (a_s); let ${}_a\tilde{G}$ be the twisted group. The resulting sequence $1 \to F \to {}_a\tilde{G} \to {}_aG \to 1$ is again exact;

moreover since ${}_a\tilde{G}$ is the simply connected covering of the semisimple group ${}_aG$ by the first part of the argument the images of the cohomology
61 classes (a_s) and (b_s) under the bijective mapping $H^1(K,G) \to H^1(K,{}_aG)$ are both the distinguished element of $H^1(K,{}_aG)$ and so (a_s) and (b_s) are cohomologous. Hence δ is bijective. This shows that a knowledge of the cohomology of the finite abelian group F will enable us to determine the cohomology of G.

We shall prove these theorems only for the classical groups, following the first part of [16]; the second part of that paper contains a case by case proof for exceptional groups. More satisfactory is the general theory of semisimple groups over $\mathscr{P}$-adic fields by F. Bruhat and J. Tits [3] of which theorem 1 is a consequence.

We start by classifying the $\mathscr{P}$-adic classical groups. By the results of chapter 2, this reduces to the classification of simple algebras A over K with involution I. Let (A,I) be a central simple algebra over K with involution I. If A^o is the opposite algebra I gives an isomorphism of A onto A^o so that $inv_K A = inv_K A^o$, even if I is of the second kind, and so the isomorphism between A and A^o is not a K-isomorphism; but since A^o is the inverse of A in the Brauer group B_K by §3.2, theorem 2 we gave $inv_K A = -inv_K A^o$ so that $inv_K A = 0$ or $\frac{1}{2}$; in the first case A is a matrix algebra over K. In the second case let $A = D \otimes_K M_\Gamma(K)$ where D is a division algebra over K. Since $inv_K M_\Gamma(K) = 0$ and $inv_K A = inv_K D + inv_K M(K) \mod 1$ we have $inv_K D = \frac{1}{2}$, i.e. D is a quaternion division algebra so that A is a matrix ring over the quaternion division algebra D. This gives the following

62 **Proposition 1.** *Any central simple K-algebra with involution is either a matrix algebra over K or a matrix ring over quaternion division algebra. Using these results we shall prove the following classification theorem.*

Theorem. *The only simply connected absolutely almost simple classical groups over K are the following :*

${}^1A_n$ *-Norm-one group of simple K-algebras*

${}^2A_n$ *-Special unitary groups of hermitian forms over quadratic extensions of K*

C_n*-Sympletitic groups and unitary groups of hermitian forms over quaternion division algebras.*

B_n, D_n*-Spin groups of quadratic forms, spin groups of skew hermitian forms over quaternion algebras*

Proof. For type ${}^1A_n$ there is nothing to prove anew. For subtype ${}^2A_n$ we know the corresponding groups are $\left\{x \in A / xx^I = 1; Nx = 1\right\}$ where A is a simple K-algebra with involution I of the second kind and N stands for the reduced norm. We know by §2.5 that $A \cong M_r(L)$ where L is a quadratic extension of K. If $x = (x_{ij}) \in M_r(L)$ let $x^* = (x^I_{ji})$; then $x \to x^*$ is an involution of the second kind on $M_r(L)$. Since the restrictions of I and $*$ to L are the same there exists an invertible element $a \in A$ such that $x^I = ax^*a^{-1}$ for every $x \in A$. We saw in §2.5 that a can be chosen to satisfy $a^* = a$, i.e. hermitian. The condition $xx^I = 1$ means that $xax^* = a$, i.e x is an element of the unitary group of a; the condition $Nx = 1$ means $\det x = 1$ under the identification $AM_r(L)$. Hence x is **63** actually an element of the special unitary group of the hermitian form defined by a. Conversely groups defined in this way belong to subtype ${}^2A_n$. The other types are classified in §2.6. □

4.2 Proof of theorem 2

We shall now prove theorem 2. We shall construct a commutative subgroup $\tilde{T} \subset \tilde{G}$ such that $\tilde{T} \supset F$ and such that $H^2(K, \tilde{T}) = \{1\}$. Then the diagram below is commutative with exact rows.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & F & \longrightarrow & \tilde{T} & \longrightarrow & T & \longrightarrow & 1 \end{array}$$

Here T is the quotient of $\tilde{T}$ by F and the vertical maps are inclusions. Using $H^2(K, \tilde{T}) = \{1\}$ we then get a commutative diagram

$$\begin{array}{ccccc} H^1(K,G) & \xrightarrow{\delta} & H^2(K,F) & & \\ \uparrow & & \uparrow & & \\ H^1(K,T) & \xrightarrow{\delta} & H^2(K,F) & \longrightarrow & 1 \end{array}$$

which shows that $\delta : H^1(K,G) \to H^2(K,F)$ is surjective, hence the theorem will be proved if we can construct such a $\tilde{T}$. For this we have the following

Lemma 1. *$\tilde{G}$ contains an algebraic torus $\tilde{T}$ defined over K and containing F such that $H^2(K, \tilde{T}) = \{1\}$.*

By the results of §2.2, it suffices to prove lemma 1 for $\tilde{G}$ absolutely
64 *almost simple. We know by §3.2, theorem 5 that if $\tilde{T}$ is a torus of $\tilde{G}$ over K split by the Galois extension L of finite degree over K then*

$$H^2(g_{L/K}\tilde{T}) \cong \hat{H}^o(g_{L/K}X_{\tilde{T}}) \text{ where } X_{\tilde{T}} = \mathrm{Hom}(G_m, \tilde{T})$$

is the set of homomorphisms of G_m into $\tilde{T}$ defined over L. Since center $\tilde{G} \supset F$, if we can construct a torus $\tilde{T}$ such that i) $\tilde{T} \supset$ centre of $\tilde{G}$ and ii) there exists no nontrivial rational homomorphism of G_m into $\tilde{T}$ defined over K, then it will follow that $\hat{H}^o(g_{L/K}X_{\tilde{T}}) = \{1\}$ and by what precedes lemma 1 will be proved after passing to the inductive limit. Hence lemma 1 is a consequence of the following

Lemma 2. *If G is a simply connected absolutely almost simple classical group over K there exists a torus T/K containing the centre such that there exists no non-trivial homomorphism of G_m into T over K.*

Type ${}^1A_n$: here $G = \{x \in A/Nx = 1\}$ where A is a simple K-algebra. Let L be a maximal commutative subfield of A and define $T = \{x \in L/Nx = 1\}$; we saw in §3.2 Example 2 that T is a torus; clearly $T \subset G$ and contains the center of G.

We claim that T satisfies our requirements: let L^* be the torus defined in §3.1 Example 1 let $f : L^* \to G_m^{n+1}$ be the isomorphism defined

over $\bar{K}$. Let for each i such that $1 \leq i \leq n+1$, u_i be the homomorphism $u_i : G_m \to G_m^{n+1}$ defined by $x \to (1, \ldots, x \cdots 1)$. These u_i's generate $\mathrm{Hom}_{\bar{K}}(G_m, G_m^{n+1})$ this being the set of rational homomorphisms of G_m into G_m^{n+1}, defined over $\bar{K}$. Hence $\bar{f}^{-1} \cdot u_i$ generate $\mathrm{Hom}_{\bar{K}}(G_m, T)$; **65**
moreover these $\bar{f}' o u_i' s$ are free generators of the free abelian group $\mathrm{Hom}_{\bar{K}}(G_m, T)$. The isomorphism $f : L_{\bar{K}}^* \to (\bar{K}^*)^{n+1}$ is defined in the following way; let $s_1, \ldots, s_{n+1}$ be the distinct K-isomorphisms of L into $\bar{K}$; then f is induced by the map $L \otimes_K \bar{K} \to \bar{K} \oplus \cdots \oplus \bar{K}$ given by $x \otimes y \to ({}^{s_1}x.y, {}^{s_2}x.y, \ldots, {}^{s_{n+1}}x.y)$. Using this it follows that if F is a finite Galois extension of K which splits T then $g_{F/K}$ acts transitively on the set of $f^{-1} o u_i' s$ and that its action is simply to permute them. This implies if $\prod (f^{-1} o u_i)^{r_i} \in \mathrm{Hom}_K(G_m, L^*)$ then $r_i = r$ for all i. The image of $\prod (f^{-1} o u_i)^{r_i}$ will be in T if and only $\sum r_i = 0$; these two conditions can be satisfied only when all the r_i are zero. Hence there exists no non-trivial homomorphism of G_m into T defined over $\bar{K}$. This proves the lemma for the subtype ${}^1A_n$.

Next consider the subtype ${}^2A_n$; these are special unitary groups of hermitian forms over quadratic extensions L of K. Let $G = SU(h)$ accordingly; choose an orthogonal basis $e_1, e_2, \ldots, e_{n+1}$ of the corresponding vector space. Define $T = \{x \in G / xe_i = \lambda_i e_i\}$ where the $\lambda_i' s$ are scalars; the $\lambda_i' s$ satisfy the conditions $\prod \lambda_i = 1$ and $N_{N/K} \lambda_i = 1$; this shows that T is isomorphic to a product of groups of the previous type considered and we can repeat the argument for each of the components of this product.

Next consider the type C_n: Here we have to consider *i*) $G = Sp_{2n}$ *ii*) G=unitary group of hermitian form over quaternion division algebra.

Case (i). We have $Sp_{2n} \supset Sp_2 \times \cdots \times Sp_2 \cong SL_2 \times \cdots \times SL_2$; since **66**
SL_2

n factors $\qquad$ n factors

is of type ${}^1A_n$ we can construct a torus T_1 of dimension one in SL_2 containing the centre of SL_2 for which $\mathrm{Hom}_K(G_m, T_1) = \{1\}$.

Then $T = T_1 \times \cdots \times T_1$ will be a torus of the desired kind; for

n factors

$\mathrm{Hom}_K(G_m, T) \cong \{\mathrm{Hom}_K(G_m, T_1)\}^n = \{1\}$. The centre of Sp_{2n} is $\{\pm 1\}$ which is contained in the centre of Sp_2^n; hence centre $Sp_{2n} \subset$ centre SL_2^n but $T_1^n \supset$ centre of SL_2^n; hence $T \supset$ centre Sp_{2n}: this proves the result in this case.

Case (ii). The argument is similar; let $G = U_n(C/K, h)$ where C is a quaternion division algebra over K and h is a non-degenerate hermitian form over C. Taking an orthogonal basis for the corres ponding vector space we see that $U_n(C/K, h)$ contains the product of n one-dimensional unitary groups operating on C as a left vector space over itself with $h(x, y) = xay^I$; here I is the standard involution on C and $a \in K$. Any C-linear automorphism of C is of the form $x \to x\lambda$ with $\lambda \in C^*.h(x\lambda, y\lambda) = h(x, y) \Longleftrightarrow \lambda\lambda^I = 1$.

Hence $U_1(C/K, h)$ is isomorphic to the group of elements of C with norm 1 and so U_1 is a group of type ${}^1A_n$. Hence by what we have proved there exists a torus T_1 of dimension one defined over K containing the centre of $U_1(C/K, h)$ and such that $\mathrm{Hom}_K(G_m, T_1) = \{1\}$. Define $T = T_1^n$; as in the last case considered T will be a torus having the requisite properties.

67 Next consider types B_n, D_n:
i) $G = SO_{2n}(n \geq 2)$; we need the following

Lemma 3. *Let V be a non-degenerate quadratic space over K of dimension $2n$ with $n \geq 2$. Then there exists an orthogonal splitting $V = V_1 \perp V_2 \perp \cdots \perp V_n$ where the V's are two dimensional anisotropic subspaces.*

We shall assume this lemma for the moment. Let T_i be the special orthogonal group of the quadratic space V_i; then $SO_{2n} \supset T_1 \times \cdots \times T_n$; we have shown in §3.1 Example 3 that the T_i's are algebraic tori; define $T = T_1 \times \cdots \times T_n$; we claim that this torus satisfies our requirements. The proof of this is exactly the same as in the case of Sp_{2n}; we have only to use the fact that the centre of SO_{2n} is ± 1. Consider the spin group now; let $p : \mathrm{Spin}_{2n} \to SO_{2n}$ be the covering homomorphism. If T is the torus of SO_{2n} constructed as above then we claim that $\tilde{T} = p^{-1}(T)$ has the required properties; firstly since $p|\tilde{T} : \tilde{T} \to T$ is a surjective morphism

with finite kernel if we prove that $\tilde{T}$ is connected it will follow from §3.1. Remark 2 that $\tilde{T}$ is an algebraic torus.

Let V_1 be a two dimensional anisotropic quadratic space. Then the Clifford algebra $C(V_1)$ is of dimension 4 and $C^+(V_1)$ is just $K(\sqrt{c})$ where c is the discriminant of V_1 and the $*$ automorphism is the non-trivial K-automorphism of $K(\sqrt{c})$. Hence we have $\mathrm{Spin}_2(V_1) = \{x \in C^+ / xx^* = 1\}$ is isomorphic to the group of elements of $K(\sqrt{c})/K$ with norm 1 which is a torus. In particular $\mathrm{Spin}_2(V_1)$ is connected. Moreover if **68**
$T_i' = \mathrm{Spin}(V_i)$ is considered as a subgroup of $\mathrm{Spin}(V)$ then $p^{-1}(T) = p^{-1}(T_1 \times \cdots \times T_n) = T_1' \times \cdots \times T_n'$ is connected. Hence as said before $\tilde{T}$ is a torus. Evidently $\tilde{T} \supset$ center of Spin_{2n} since $T \supset$ center of SO_{2n}. Next if $f : G_m \to \tilde{T}$ is a non-trivial homomorphism defined over K, $f(G_m)$ is one-dimensional; since the kernel of $p|\tilde{T} : \tilde{T} \to T$ is zero dimensional the composite $p|\tilde{T} \circ f$ will be a non-trivial homomorphism of G_m into T defined over K which contradicts the property of T; hence $\mathrm{Hom}_K(G_m, \tilde{T}) = \{1\}$ and so $\tilde{T}$ has the required properties. For type D_n we need the following

Lemma 4. *If h is a skew-hermitian form on the quaternion division algebra C over K then $SU_1(C, h)$ is a torus T without non-trivial homomorphism of G into T over K.*

Proof. If $h(x, y) = xay^I$ with $a^I = -a$, then $SU_1(C, h) = \{x \in C / xax^I = a, Nx = 1\} = \{x \in C / xa = ax, Nx = 1\}$, i.e. the elements of norm 1 in the quadratic extension $K(a)$. □

Since our groups of type D_n are isomorphic to the unitary group of a skew-hermitian form over a quaternion division algebra say $U_n(C/K, h)$ we can carry out the procedure adopted for SO_{2n} to construct a torus with the requisite properties for $U_n(C/K; h)$.

Proof of Lemma 3. To start with let the quadratic space V be of dimension four. There certainly exists a decomposition $V = V_1 \perp V_2$ with V_1, V_2 two dimensional and V_2 containing an anisotropic vector e_2; let $\mathscr{G}$ be the quadratic form associated with V. If both V_1 and V_2 are **69**
anisotropic there is nothing to prove. So suppose V_1 is isotropic. Using

the fact that the quadratic form of an isotropic space represents any non-zero element of K we can choose $e_1 \in V_1$ so that $\mathscr{G}(e_1, e_1) = \dfrac{-a}{\mathscr{G}(e_2, e_2)}$ where a is some element of K^* which is not a square and not equal to the discriminant of V modulo squares, the choice of such an a being always possible in the $\mathscr{P}$-adic field. Then the two dimensional subspace $V_1' = Ke_1 \oplus Ke_2$ of V has discriminant equal to $-a$ modulo squares; by the choice of a, V_1' is anisotropic; if V_2' it the orthogonal complement of V_1' it is also anisotropic since by choice $a \not\equiv -d(V) \mod \text{squares}$.

Hence $V = V_1' \perp V_2'$ is the required decomposition. The general case is proved by induction on the integer $2n$. If $n = 2$ we have just seen that the lemma is true. So we can assume that $n \geq 3$ and that the lemma is true for all subspaces of V of dimension $2m$ with $2 \leq m < n$. Let U be a four dimensional non-degenerate subspace of V. Let $V = U \perp W$ be an orthogonal splitting. For U we have a decomposition $U = V_1 \perp V_2$ with V_1 and V_2 both anisotropic. The subspace $V_2 \perp W$ is of dimension $2(n-1) \geq 4$ so induction assumption can be applied.
Hence there exists an orthogonal splitting $V_2 \perp W = V_2' \perp V_3' \perp \cdots \perp V_n'$ where $V_2', V_3', \ldots V_n'$ are anisotropic subspaces of dimension two. Hence $V = V_1 \perp V_2' \perp V_3' \perp \cdots \perp V_n'$ is a splitting of the required kind for V. This proves the lemma.

Now consider SO_{2n+1} for odd dimension. In this case we can prove that the corresponding vector space has a decomposition $V_1 \perp \cdots \perp$
70 $V_n \perp W$ with V_i's two dimensional anisotropic and W one dimensional. As before we can prove that $p : \text{Spin}_{2n+1} \to SO_{2n+1}$ is the covering homomorphism and $T = SO(V_1) \times \cdots \times SO(V_n)$ then $p^{-1}(T)$ will be the torus with the required properties. This completes the proof of theorem 2.

4.3 Proof of theorem 1

Type ${}^1A_n$: The classical group of this type is $G = \{x \in A / Nx = 1\}$ where A is a simple K-algebra. From the exact sequence $1 \to G \to A^* \to G_m \to 1$ and from the fact $H^1(K, A^*) = \{1\}$ proved in 1.7. Example 1 we

get the following exact sequence of cohomology sets:

$$A_K^* \xrightarrow{N} K^* \to H^1(K, G) \to 1.$$

To show that $H^1(K, A^*) = \{1\}$ we have only to prove the

Lemma 1. *$A_K^* \xrightarrow{N} K^*$ is surjective.*

Proof. Let $t \in K^*$ be a prime element i.e. an element of order 1 in the discrete valuation. The polynomial $f(x) = x^{n+1} + (-1)^{n+1}t$ is an Eisenstein's polynomial over K and consequently irreducible. Hence $\frac{K[X]}{(f)}$ is a field extension of K of degree $(n + 1)$ so that by theorem 3, §3.2. A is split by the extension $\frac{K[x]}{(f)}$. Hence there exists a K-isomorphism of $\frac{K[x]}{(f)}$ onto a subfield L of A; the reduced norm of an element of L is the usual norm $N_{L/K}$; since the residue class of x in $\frac{K[x]}{(f)}$ has norm over K equal to t we see that t is the reduced norm of an element of A^*. Next if ε be any unit of K^* both t and $t\varepsilon$ are prime elements and so they are reduced norms of elements of A^*; consequently ε is the reduced norm of element of A^*. Since any element of K^* can be **71**
written as $t^r\varepsilon$ where $r \in Z$ and ε is a unit the lemma follows. □

Type ^2A_n. Here $G = SU_{n+1}(L/K, h)$ where $[L : K] = 2$ and h is a hermitian form over L. Since we have seen from the Dynkin diagram that there is no subtype $^2A_1$, $SU_2(L/K, h)$ is isomorphic to a group belonging to type $^1A_n \cdot A$ simple direct proof will be as follows.

Lemma 2. *Let A be a quaternion K-algebra with involution I of the second kind; let L be the centre of A so that $[L : K] = 2$. Then the group $G_1 = \left\{x \in A / xx^I = 1, Nx = 1\right\}$ is isomorphic to the group $G_2 = \{x \in B / Nx = 1\}$ where B is a quaternion algebra of centre K.*

Proof. We proved in §2.5 proposition 1 that there exists a quaternion algebra B of centre K such that $A \cong B \otimes_K L$, that I induces the standard involution on B and on L the action of I is the non-trivial K-automorphism.

Let $L = K(\sqrt{d})$ Then any $x \in A$ can be written as $x = x_1 \otimes 1 + x_2 \otimes \sqrt{d}$. Then □

$xx^I = (x_1 \otimes 1 + x_2 \otimes \sqrt{d})(x_1^I \otimes 1 - x_2^I \otimes \sqrt{d}) = (x_1 x_1^I - d x_2 x_2^I) \otimes 1 + (x_2 x_1^I - x_1 x_2^I) \otimes \sqrt{d}$; the condition $xx^I = 1$ implies $(x_1^{-1} x_2)^I = x_1^{-1} x_2$, hence $x_2 = t x_1$ with $t \in K$. Then $x = x_1 \otimes 1 + t x_1 \otimes \sqrt{d} = x_1 \otimes (1 + t\sqrt{d}) = x_1 \otimes z$, say where $z \in L$. Now $xx^I = 1$ is equivalent to $x_1 x_1^I \otimes z z^I = 1$; the condition $Nx = 1$ is equivalent to $x_1 x_1^I \otimes z^2 = 1$ (because in B, $x_1 x_1^I$ is the reduced norm; the term z^2 accounts for the fact that in A the reduced norm is taken with respect to L). The last two conditions give $z = z^I$;
72 i.e. $z \in K$; hence if $x \in G_1$ we have proved that $x = x_1 z \otimes 1$ i.e. $x \in B$; but then B, $xx^I = 1$ and $Nx = 1$ are equivalent; hence the lemma.

The lemma implies by case ${}^1A_n$ that $H^1(K, SU_2(h)) = \{1\}$. Let V be the vector space of $(n+1)$ dimension over L corresponding to this hermitian from h; choose a vector $a \in V$ such that $h(a,a) \neq 0$. Let H be the subgroup of G consisting of those elements which fix the vector a. Then H is the unitary group SU_n of dimension n corresponding to the orthogonal complement of a in V. Applying induction on n we have only to prove the following.

Lemma 3. *The map $i : H^1(K, SU_n) \to H^1(K, SU_{n+1})$ induced by the injection $SU_n \to SU_{n+1}$ is surjective for $n \geq 2$.*

Proof. Let $a = (a_s) \in H^1(K, SU_{n+1})$; (a) is in the image of i if and only if the twisted homogeneous space ${}_a(SU_{n+1}/SU_n)$ has a K-rational point by §1.5. Proposition 1. Now $SU_{n+1}/SU_n \cong U_{n+1}/U_n$. Let $T = \left\{ x \in V / h(x,x) = c \right\}$ where $c = h(a,a)$, U_{n+1} acts transitively on T and the subgroup of U_{n+1} fixing T is U_n; hence $U_{n+1}/U_n \cong T$ so that ${}_a(SU_{n+1}/SU_n) \cong a^T$, □

Since G is a group of L-automorphisms of V and that the hermitian from h is fixed by all these automorphisms we can twist both V and h by the cocycle (a_s) to get a vector space V' and a hermitian form h' and an isomorphism $f : V \otimes_K \bar{K} \to V' \otimes_K \bar{K}$ such that $f^{-1} o^s f = a_s$. Let $T' = \left\{ x \in V' / h'(x,x) = c \right\}$; then $f(T) = T'$ holds; and $f^{-1} o^s f = a_s$
73 show that $T' \cong_a T$. We have only to shows that T' has a K-rational

point. But this follows from the fact that any non-degenerate hermitian form of dim ≥ 2 is a quadratic form of dimension ≥ 4, and so over a local field represents any non-zero element of the field. Hence the lemma is proved and consequently theorem *I* for type ${}^2A_n$.

Type C_n i) $G = Sp_{2n}$; we proved in §1.7. Example 3 that $H^1(K, Sp_{2n}) = 1$. ii) $G = U_n(C/K, h)$ where C/K is a quaternion algebra of centre K and h is a non-degenerate hermitian form over C; let V be the corresponding n-dimensional vector space. For $n = 1 U_1(C/K, h)$ is isomorphic to a group of type ${}^1A_n$ so that $H^1(K, U_1(C/K, h)) = \{1\}$ by theorem 1 for type ${}^1A_n$. Let $U_{n-1}(C/K, h)$ be the subgroup of $U_n(C/K, h)$ fixing an anisotropic vector of V; then just as in the discussion of type ${}^2A_n$, the map $H^1(K, U_{n-1}(C/K, h)) \to H^1(K, U_n(C/K, h))$ is surjective. Here we have only to use the fact that any hermitian form h with respect to the standard involution on C represents any non-zero element of the local field K. Applying induction on n we see the truth of theorem 1 in this case.

Types B_n **and** D_n. First consider SO_n and its universal covering Spin n; for $n \leq 6$ the theorem follows by the isomorphism of Spin_n with group of the previous types considered; for example Spin_3 is the norm-one group of the second Clifford algebra which is a quaternion algebra (§2.3, [9], [12]) and so $H^1(K, \mathrm{Spin}_3) = \{1\}$; we can assume $n \geq 4$ and apply induction; let 0_{n-1} be the subgroup of 0_n fixing an anisotropic vec- **74**
tor; then $\mathrm{Spin}_n / \mathrm{Spin}_{n-1} = SO_n/SO_{n-1} \cong O_n/O_{n-1}$; by Witt's theorem $O_{n/O_{n-1}} = \left\{ x \in V / \mathscr{G}(x, x) = \mathscr{G}(a, a) \right\}$ have V is the vector space corresponding to the quadratic form $\mathscr{G}$ and a is the anisotropic vector chosen. Applying the twisting argument and the fact that any quadratic form over a $\mathscr{P}$-adic field K in at least four variables represents any non-zero element of K it will follow that the map $H^1(K, \mathrm{Spin}_{n-1}) \to H^1(K, \mathrm{Spin}_n)$ is surjective for $n \geq 4$. Induction now works for the proof of theorem 1.

Finally consider the remaining classical groups of type D_n; they are $G = \mathrm{Spin}_n(C/K, h)$ where C is a quaternion algebra over K and h is a skew hermitian form over C with respect to the standard involution on C. Let V be the corresponding vector space over C. Then G is the simply connected covering of $SU_n(C/K, h)$ the special unitary group. Now for $n = 3$ this group is isomorphic over K to a group of type A_3 so that

its Galois cohomology is trivial. This can be used to apply induction on n. If U_{n-1} is the subgroup of U_n fixing an anisotropic vector of V then $\mathrm{Spin}_n / \mathrm{Spin}_{n-1} \cong SU_n / SU_{n-1} \cong U_n / U_{n-1}$; in this case also U_n / U_{n-1} is a sphere; by the methods previously employed it is now evident that the truth of theorem 1 will be guaranteed by the following

Lemma 4. *Any skew-hermitian form $h'(x, y)$ over C of dimension at least three represents any non-zero skew-quaternion of C. For proofs* 75 *see [14], [16], [22]. We shall give here one more proof, using the isomorphisms of SU with groups of type $A_1 \times A_1$, A_3.*

Proof. Let $c \in C$ be the skew quaternion of the theorem. It is sufficient to consider vector spaces of dimension 3. Let V' be the vector space corresponding to $h'(x, y)$; we have to shows that the sphere $S' = \left\{ x' \in V' / h'(x, x) = c \right\}$ has a K-rational point. Construct a vector space V of dimension 3 over C with a skew-hermitian form h which represents c K-rationally. V can also be constructed to have discriminant equal to that of V. This is assured by the following □

sublemma. Any non-zero element of a quaternion algebra C over any field K can be written as the product of two skew symmetric elements of C with respect to the standard involution.

Proof. Let $c \in C$, $c \neq 0$ be given; let $\bar{C}$ denote the space of skew symmetric elements of C; the intersection $c\bar{C} \cap \bar{C}$ is non-zero since both C^- and cC^- are of dimension three whereas C is of dimension 4; hence there exists two non-zero elements $c_1, c_2 \in C^-$ such that $cc_1 = c_2$; i.e, $c = c_1^{-1} c_2$; here both c_1^{-1} and c_2 are skew symmetric. This proves the sublemma. □

We know that any non-zero element of K is the reduced norm of an element of C; choose $d \in C$ so that $Nd = \dfrac{d(V')}{Nc}$; write $d = d_1 d_2$ where d_1 and d_2 are skew symmetric; the matrix $\begin{pmatrix} c & 0 & 0 \\ 0 & d_1 & 0 \\ 0 & 0 & d_2 \end{pmatrix}$ is skew

hermitian and if the vector space V is provided with the hermitian form h corresponding to this matrix then h represents c and that discriminant **76**
of V'. Now (v, h), and (V', h') are isomorphic over $\bar{K}$; let $f : V_{\bar{K}} \to V'_{\bar{K}}$ be this isomorphism, then $f^{-1}o^s f = a_s \in U_3(V, h)$ where U denotes the unitary group of h; since the discriminants of V and V' are equal we have by §2.6 lemma 3 that $a_s \in SU_3(V, h)$; let U_2 be the unitary group of the orthogonal complement of a chosen vector representing c; let S be the homogeneous space SU_3/SU_2 which is the sphere $\left\{x \in V / h(x, x) = c\right\}$; then the sphere S is just the twisted sphere ${}_aS$. The proof of the theorem will be achieved once we prove that the cocycle (a_s) is in the image of the map $H^1(K, SU_2) \to H^1(K, SU_3)$; we shall actually prove that this map is bijective. The commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z_2 & \longrightarrow & \mathrm{Spin}_3 & \longrightarrow & SU_3 & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & Z_2 & \longrightarrow & \mathrm{Spin}_2 & \longrightarrow & SU_2 & \longrightarrow & 1 \end{array}$$

with exact rows and whose vertical maps are the natural ones, gives rise to the commutative diagram

$$\begin{array}{ccc} H^1(K, SU_3) & \xrightarrow{\delta} & H^2(K, Z_2) \\ \uparrow & & \uparrow \text{identity} \\ H^1(K, SU_2) & \xrightarrow{\delta} & H^2(K, Z_2) \end{array}$$

By theorems (1) and (2) the rows are isomorphisms; since the righthand column is an isomorphism the left hand column is also an isomorphism. This proves the result. Hence theorem 1 is proved completely.

Chapter 5

Number fields

5.1 Statement of results

77

Let G be a semi-simple and simply connected classical group defined over a number field K.

Theorem 1. *The canonical map* $i : H^1(K, G) \to \prod_{V \in \infty} H^1(K_v, G)$ *is bijective*

Theorem 1 a. *The mapping i above is injective*

Theorem 1 b. *The mapping i above is surjective; this is true even for connected semisimple groups but not necessarily simply connected.*

Theorems 1a and 1b b) together imply theorem 1.

Let G/K be a semisimple and connected classical group; let $p : \tilde{G} \to G$ be the universal covering with kernel F. The exact sequence

$$1 \longrightarrow F \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

defines a map $\delta : H^1(K, G) \to H^2(K, F)$.

Theorem 2. *The map* δ *defined above is surjective.*

In theorem 1 we any replace $\prod_{v \in \infty}$ *by* $\prod_{v}$, *since* $H^1(K_v, G) = 1$ *for* $v \notin \infty$ *by theorem 1 of chapter 4. The injectivity of the map* $H^1(K, G) \to$

$\prod_v H^1(K_v, G)$ *is known as the Hasse principle for* H^1 *of* G. *Harder* [H] *has proved theorem 1 for any simply connected semi-simple group* G/K *not containing any factor of type* E_∞. *If* G *is semi-simple and connected and if* $\P : \tilde{G} \to G$ *be its simply connected covering with kernel* F *then Hasse-Principle for* H^1 *of* G *is equivalent to the Hasse Principle for* H^2 *of* F. *The proof of this makes use of a simple lemma in diagram chasing which we shall state without proof for future reference.*

78 **Lemma 1.** *Let* $A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4$ *be sets with distinguished elements and suppose we have a commutative diagram with exact rows*

$$\begin{array}{ccccccc} A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} \\ B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 \end{array}$$

Let f_1 *be surjective,* f_2 *injective and* f_4 *has trivial kernel then* f_3 *has trivial kernel.*

For the present assume theorem 1, 2; if Hasse-principle for H^1 of G is valid then in the diagram below β is injective;

$$\begin{array}{ccccccc} H^1(K, \tilde{G}) & \longrightarrow & H^1(K, G) & \longrightarrow & H^2(K, F) & \longrightarrow & 1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ \prod H^1(K_v, \tilde{G}) & \longrightarrow & \prod H^1(K_v, G) & \longrightarrow & \prod H^1(K_v, F) & & \end{array}$$

The top row is exact by theorem 2; α is surjective by theorem 1. Clearly the bottom row is exact. Hence by lemma 1, γ has trivial kernel; *i.e.* Hasse-Principle for H^2 of F holds. Conversely suppose Hasse-Principle for H^2 of F holds; the diagram below is commutative with exact rows

$$\begin{array}{ccccccc} H^1(K, F) & \longrightarrow & H^1(K, \tilde{G}) & \longrightarrow & H^1(K, G) & \longrightarrow & H^2(K, F) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \eta} \\ \prod_{v\in\infty} H^1(K_v, F) & \longrightarrow & \prod_{v\in\infty} H^1(K_v, \tilde{G}) & \longrightarrow & \prod H^1(K_v, G) & \longrightarrow & \prod H^2(K_v, F) \end{array}$$

79 where ∞ denotes the set of archimedean places; in view of theorem 1,

β is bijective; by assumption η is injective; also α can be shown to be surjective; hence by lemma 1, γ has trivial kernel, by a twisting argument which we have used several times it follows that γ is injective i.e. Hasse-Principle for H^1 of G holds.

The first step in the proof of theorem 1 is reduction to the case of absolutely almost simple groups which we shall now carry out; G is a finite product of K-almost simple groups say $G = \prod G_i$; since $H^1(K, G) \cong H^1(K, G_i)$, $H^1(K_v, G) \cong \prod H^1(K_v, G_i)$, for the proof of theorem 1 it is enough to consider K-almost simple groups. So suppose G is K-almost simple. By § 2.2 (1) we know that $G = \prod_{i=1}^{r} H_i$ where $H_i's$ are $\bar{K}$-almost simple groups and that $g_{\bar{K}/K}$ acts on the set of the $H_i's$ by permuting them; moreover this action is transitive; hence if h denotes the isotropy group of $H = H_1$ in $g = g_{\bar{K}/K}$ we have $G = \prod_{s \in g/h} {}^sH$; let L be the fixed field of h and let M be any finite Galois extension of K containing L. For any K-algebra A we denote by G_A the set of A-valued points of G i.e. if $G = \operatorname{Spec} B$ then $G_A = \operatorname{Hom}(\operatorname{Spec} A, \operatorname{Spec} B) = \operatorname{Hom}_{K-alg}(B, A)$. Consider the diagram below

$$\begin{array}{ccc} H^1(g_{m/K}, G_M) & \xrightarrow{f_1} & H^1(g_{M/K}, G_{M\otimes_K K_v}) \\ \alpha \downarrow & & \beta \downarrow \\ H^1(g_{M/L}, H_M) & \xrightarrow[g_1]{} & H^1(g_{M/L}, H_{M\otimes_K K_v}) \end{array}$$

where α, β are the isomorphisms given by lemma 1 of § 1.3; f_1, g_1 **80** are the natural homomorphisms obtained from the canonical mappings $G_M \to G_{M\otimes_K K_v}$ and $H_M \to H_{M\otimes_K K_v}$; now $M \otimes_K K_v \cong \oplus M_{\bar{v}}$ where $\bar{v}$ runs through all places of M extending v and $g_{M/K}$ permutes the components $M_{\bar{v}}$ transitively, the isotropy group of one particular $M_{\bar{v}}$ being its decomposition group $g_{M_{\bar{v}/}K_v}$. By lemma 1 of 1.3, $H^1(g_{M/K}, G_{M\otimes K_v}) \cong H^1(g_{M_{\bar{v}}/K_v}, G_{M_{\bar{v}}}$ and with this identification, f_1 becomes the canonical map $H^1(g_{M/K}, G_M) \to H^1(g_{M_{\bar{v}}/K_v}, G_{M_{\bar{v}}})$. Similarly $M \otimes K_v \cong M \otimes_L (L \otimes_K K_v) \cong \underset{w/v}{\oplus} M \otimes_L L_w \cong \underset{w/v}{\oplus} \underset{\bar{w}/w}{\oplus} M_{\bar{w}}$, and so

$$H^1(g_{M/L}, H_{M\otimes_K K_v}) \cong \prod_{w/v} H^1(g_{M/L}, H_{M\otimes_L L_w}) \cong \prod_{w/v} H^1(g_{M_{\bar{w}/L_w}}, H_{M_{\bar{w}}}),$$

where for each w, $\bar{w}$ is an extension of w to M. Therefore the Hasse Principle for H^1 of G will follow if we can prove the same for H; hence for the proof of theorem 1 we can restrict ourselves to absolutely almost simple and simply connected classical groups.

Before proceeding with the proofs of theorems 1 and 2 we shall discuss the types of involutory algebras (A, I) over K. If I is of the first kind, $A \cong A^o$, so A is of order 2 in the Brauer group and therefore A is either a matrix algebra over K or a matrix ring over a quaternion division algebra (*cf. De , e.g.*). In the case of $\mathscr{P}$-adic field we saw (§ 4.1, proposition 1) that the only division algebra with involution of the second kind and with centre L is the field L itself. But in the case of number fields the situation is different. In fact we shall prove the following

81 **Proposition 1.** *There exists a division algebra over K of any given degree m with an involution of the second kind.*

Proof. Choose extensions L/F and M/K such that i) $[L : K] = 2$ ii) M/K is cyclic of degree m iii) L and M are linearly disjoint over K. Such a choice is always possible. Then ML/L is again a cyclic extension and if σ is a generator of $g_{ML/L}$ then σ/M is a generator of $g_{M/K}$. We shall construct A as a crossed product $A = (ML/L, \sigma, a)$ where $a \in L^*$ to be suitably chosen; this is by definition a left free module over ML with basis $1 = u^o, u^1, \ldots, u^{m-1}$ and the multiplication rules are given by

$$\begin{aligned} ux &= \sigma_x \cdot u \text{ for } x \in ML \\ u^i, u^j &= u^{i+j} \text{ if } i + j < m, \\ u^i.u^j &= au^{i+j-m} \text{ if } i + j \geq m. \end{aligned}$$

□

A is a simple algebra with centre L; we then require $a^I = a^{-1}$ and define $I : A \to A$ as follows: $I|M$ is the identity, $I|L$ is the non-trivial K-automorphism of L and $u^I = u^{-1}$; if $x = \sum x_i u^i$ is any element of A with $x_i \in ML$ we define $x^I = \sum u^{-i} x_i^I$; with this definition for any $x \in ML$,

$(\sigma_x)^I = {}^{\sigma}(x^I)$; using this it follows that I is an involution; clearly I is of the second kind. We seek an additional condition on a to make A into a division algebra. $a^I = a^{-1}$ is equivalent to $N_{L/K}a = 1$ which by Hilbert's theorem 90 implies $a = b^I/b$ for some $b \in L$. We have only to choose b properly. By Frobenius theorem we can choose a prime divisor $\mathfrak{p}$ in K with the properties *i*) if $\mathfrak{p}$ is any prime divisor of M dividing $\mathfrak{P}$ then **82**
$[M_{\mathfrak{p}} : K_{\mathfrak{P}}] = m$ and $M_{\mathfrak{p}}/K_{\mathfrak{P}}$ is unramified; ii) $\mathfrak{p}$ splits into two distinct prime divisors $\mathscr{G}_1$ and $\mathscr{G}_2$ in L. Next choose $b \in L$ such that $b \in \mathscr{G}$ but $b \notin \mathscr{G}_1^2$, $b \notin \mathscr{G}_2$ and b integral at $\mathscr{G}_2$. We claim that with this choice of a, A is a division algebra. For ML/L is unramified at $\mathscr{G}_2$ and for σ one can take the Frobenius automorphism; we shall calculate the $\mathscr{G}_2$-invariant of $(ML/L, \sigma, a)$; $ord_{\mathscr{G}_2} a = 1$ by the choice of b in $a = b^I/b$; hence the $\mathscr{G}_2$ -invariant will be $\frac{1}{m}$ since the local degree of ML/L at $\mathscr{G}_2$ is m by our choice of $\mathfrak{P}$. Hence $(ML/L, \sigma, a)$ has order m in the Brauer group. Now the index of an algebra being a multiple of the exponent the index of $(ML/L, \sigma, a)$ is m, so that it is a division algebra.

By §§2.4 and 2.6, the absolutely almost simple simply connected classical groups are classified as follows:

Type ${}^1A_n$: Norm-one-group of simple algebras "${}^2A_n$: Groups belonging to this type are $G = \left\{x \in A/Nx = 1, xx^I = 1\right\}$ where A is simple K-algebra with involution I of the second kind, the centre L of A being a quadratic extension of K.

Type C_n: Symplectic groups of the special unitary groups of hermitian forms over quaternion algebras;

Types B_n, D_n: Spin groups of quadratic forms

Spin groups of skew hermitian forms over quaternion algebras.

5.2 Proof of theorem 2

The ideal of the proof can be explained as follows: **83**

1. Prove that an element in $H^2(K, F)$ is trivial locally at all places outside a finite set S of places of K.

2. Construct a torus $\tilde{T} \subset \tilde{G}$ containing F such that $H^2(K_v, \tilde{T}) = \{1\}$ for $v \in S$ and such that the Hasse principle for H^2 of $\tilde{T}$ holds.

Assuming 1) and 2) have been achieved we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F & \longrightarrow & \tilde{T} & \longrightarrow & T & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & F & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

T is the quotient of $\tilde{T}$ by F and the vertical maps are the natural ones. This gives on passing to cohomology a commutative diagram in which the top row is exact:

$$\begin{array}{ccccc} H^1(K,T) & \xrightarrow{\delta_2} & H^2(K,F) & \xrightarrow{h} & H^2(K,\tilde{T}) \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle \text{identity}} & & \\ H^1(K,G) & \xrightarrow[\delta_1]{1} & H^2(K,F) & & \end{array}$$

Given a 2-cohomology class $a = (a_s) \in H^2(K,F)$ construct the set S of places as in 1) and $\tilde{T}$ as in 2). By 1) and 2) $h(a)$ is locally trivial at all places; since the Hesse principle for H^2 of $\tilde{T}$ holds by construction $h(a)$ must be trivial; hence a is in the image of δ_2 and hence of δ_1. This proves the theorem provided we can ensure steps 1) and 2).

84 **Step 1.** Let $(a_s) \in H^2(K,F)$ be given; we have $H^2(K,F) = \varinjlim_L H^2(g_{L/K}, F_L)$ where L runs through the set of finite Galois extensions of K; by choosing L big enough assume that (a_s) comes from $H^2(g_{L/K}, F_L)$ and that $F_L = F_{\bar{K}}$; this being possible by the finiteness of F. We define S to be the set consisting of archimedean places and all those places v of K which are ramified in L/K; we shall show that this S satisfies our requirements; let $v \notin S$ and suppose w is an extension of v to L; let l, k be the residue fields of L_w and K_v respectively; since v is unramified in L/K, $g_{\ell/k} \cong g_{L_w/K_v}$ and we have an isomorphism $H^2(g_{L_w/K_v}, F_{\bar{k}}) \cong H^2(g_{1/k}, F_{\bar{k}})$. Since the cohomological dimension of the finite field k is

one ([19], II § 3) we have $H^2(g_{\bar{k}/k}, F_{\bar{K}}) = 0$; hence there exists a finite extension say l' of k containing l such that the inflation map

$$H^2(g_{l/k}, F_{\bar{k}}) \longrightarrow H^2(g_{l'/k}, F_{\bar{k}})$$

is zero. We can find a finite Galois extension say L'_w of K_v containing L_w and unramified at v with residue field isomorphic to l'; we then have $H^2(G_{l'/k}, F) \cong H^2(g_{L'_w/K_v}, F)$ and the inflation map $H^2(g_{L_{v'}/K_v}, F) \longrightarrow H^1(g_{L'_w/K_v}, F)$ is zero, so $a = 0$. This completes the proof of step 1).

Step 2. To any given $v \in S$ we construct a maximal torus $\tilde{T}_v \subset \tilde{G}$ containing F and defined over K_v such that $H^2(K_v, \tilde{T}_v) = \{1\}$; by § 4.2, lemma 1, this is possible for every non-archimedean $v \in S$; moreover **85**
we can assume that S contains at least one non-archimedean place v and remark that for this v by the construction of § 4.2, lemma 1, there is no non-trivial homomorphism of G_m into $\tilde{T}_v$ over K_v. For archimedean v, the same lemma 1 holds, but we omit the proof. By an approximation argument, we can then find a torus $\tilde{T}$ defined over K such that $\tilde{T} \cong \tilde{T}_v$ over K_v for every $v \in S$. Hence $H^2(K_v, \tilde{T}) = (1)$ and $\tilde{T}$ evidently contains F. We have only to establish the Hasse Principle for H^2 of $\tilde{T}$. Suppose $(a_s) \in H^2(K, \tilde{T})$ has trivial image in $H^2(K_v, \tilde{T})$ for all places v of K; given v we can find a finite Galois extension L/K which splits $\tilde{T}$ such that (a_s) comes from an element of $H^2(g_{L/K}; \tilde{T}_L)$ and that the image of (a_s) under the map $H^2(g_{L/K}, \tilde{T}_L) \to H^2(g_{L\bar{v}/K_v}, \tilde{T}_{L\bar{v}})$ is zero; here $\bar{v}$ denotes some extension of v to L; this follows from the expression of $H^2()$ as inductive limit. Since any cohomology class of $H^2(g_{L/K}, \tilde{T})$ is trivial locally for all but a finite number of places (this follows from the results of chapter 3, in particular theorem 1 and the isomorphism (5)) we can assume that the extension L has been so chosen that the image of $(a_s) \in H^2(g_{L/K}\tilde{T})$ under the map $H^2(g_{L/K}, \tilde{T}) \to H^2(g_{L_{\bar{v}}/K_v}, \tilde{T})$ is zero for all v. § 3.2 theorem 7 then implies (a_s) is trivial.

This proves theorem 2.

5.3 Proof of theorem 1b

We have to prove that if G is semi-simple and connected then the mapping $H^1(K,G) \to \prod_v H^1(K_v,G)$ is surjective; on the right hand side
86 we have only to consider real infinite places since for complex places $H^1(K_v,G) = \{1\}$. Hence assume $K_v \cong \mathbb{R}$, then by definition $H^1(K_v,G) = H^1(Z_2,G_c)$ where $\mathbb{C}$ denotes the field of complex numbers. Let $(a_s) \in H^1(Z_2,G_{\mathbb{C}})$ be given; if $Z_2 = \{e,s\}$ we have $1 = a_e = a_{s^2} = a_s \cdot {}^s a_s$ i.e. ${}^s a_s = a_s^{-1}$; by the general theory of algebraic group we can write $a_s = a'_s.a''_s$ where a'_s is semisimple, a''_s is unipotent and a'_s and a''_s commute; moreover this representation is unique. Since $s_{a_s} = s_{a'_s} s_{a''_s}$ we have $a_s^{-1} = {}^s a'_s.{}^s a''_s$; but $a_s^{-1} = a_s'^{-1}.a_s''^{-1}$ so that $a_s'^{-1}.a_s''^{-1} = {}^s a'_s.{}^s a''_s$; by uniqueness this implies ${}^s a''_s = a_s''^{-1}$ i.e. a''_s defines a 1-cocycle. The algebraic subgroup generated by a''_s is isomorphic to the additive group G_a; but since the additive group is cohomologically trivial, the cocycle a''_s splits; hence for the proof of the theorem we can assume without loss of generality that a_s is semi-simple; but any semi-simple elements of G is contained in a maximal torus. So any element in $\prod_{v\in\infty} H^1(K_v,G)$ is contained in the image of $\prod_{v\in\infty} H^1(K_v,T_v)$ for suitably chosen maximal tori T_v of G over K_v. Now by an approximation argument, we construct a maximal torus T of G over K which is conjugate to T_v by an element of G_{K_v}. Then $H^1(K_v,T_v)$ can be replaced by $H^1(K_v,T)$ and theorem 1 b, follows from the corollary to theorem 6 b), § 3.3 and the commutativity of the diagram

$$\begin{array}{ccc} H^1(K,T) & \longrightarrow & \prod_{v\in\infty} H^1(K_v,T) \\ \downarrow & & \downarrow \\ H^1(K,G) & \longrightarrow & \prod_{v\in\infty} H^1(K_v,G) \end{array}$$

5.4 Proof of theorem 1a, for type ${}^1A_n$

87 The classical group of this type is $G = \left\{ u \in A \middle/ Nu = 1 \right\}$ where A is a

simple algebra with centre K and N stands for the reduced norm. The exact sequence of algebraic groups

$$1 \to G \to A^* \xrightarrow{N} G_m$$

gives rise to a commutative diagram with exact rows:

$$\begin{array}{ccccccc} A_K^* & \xrightarrow{N} & K^* & \longrightarrow & H^1(K,G) & \longrightarrow & H^1(K,A^*) = \{1\} \\ \downarrow & & \downarrow & & \downarrow & & \\ \prod_{v\in\infty} A_{K_v}^* & \xrightarrow{N} & \prod_{v\in\infty} K_v^* & \longrightarrow & \prod_{v\in\infty} H^1(K_v,G) & \longrightarrow & \prod_{v\in\infty} H^1(K_v,A^*) = \{1\} \end{array}$$

$H^1(K,A^*) = \{1\}$ and $H^1(K_v,A^*) = \{1\}$ by § 1.7, Example 1. By the usual twisting argument injectivity of $H^1(K,G) \to \prod_{v\in\infty} H^1(K_v,G)$ is equivalent to kernel being trivial for all twisted groups. By diagram chasing we are reduced to proving the following.

Proposition. (Norm theorem for simple algebras). *If an element x of K^* is the reduced norm of an element in A_{K_v} for all places v of K then it is the reduced norm of an element in A.*

We shall give Eichler's proof [E_1] with slight modifications. First we shall introduce some terminology; the principal polynomial of an elements a in a central simple algebra A is by definition the characteristic polynomial of $a \otimes 1$ in an isomorphism $A \otimes_K L \cong M_n(L)$ where L is a splitting field of A. This polynomial has coefficients in K and is independent of the splitting of the splitting field L and the chosen isomorphism $A \otimes_K L \cong M_n(L)$. An element $a \in A$ is said to be a regular element if its principle polynomial is separable. **88**

The proof of the proposition depends on the following lemmas:

Lemma a. *Let K be an infinite field and A a simple algebra with centre K. If $x \in K$ is the reduced norm of an element $z \in A$ then one can find a regular element $\bar{z} \in A$ whose reduced norm is x.*

Proof. Since $A_{\bar{K}}$ is a matrix algebra over $\bar{K}$ we can find a regular diagonal matrix y with determinant x. $N(zy^{-1}) = 1$, which implies $y =$

$z[a_1, b_1] \cdots [a_r, b_r]$ where $[a_1, b_1], \ldots, [a_r, b_r]$ are certain commutators in $A_{\bar{K}}$; let $e_1, \ldots, e_M$ be a basis of A/K where $M = [A : K] = n^2$. Let $\alpha_1^{(i)}, \ldots, \alpha_M^{(i)}, \beta_1^{(j)}, \ldots, \beta_M^{(j)}$, i, j taking the values $1, 2, \ldots, r$ independently be a set of independent variables. Write $x_i = \sum_{t=1}^{M} \alpha_t^{(i)} e_t$, $y_j = \sum_{t=1}^{M} \beta_t^{(j)} e_t$. Consider the generic element $z[x_1, y_1]M[x_r, y_r]$ of $A_{\bar{K}}$. The discriminant of its characteristic polynomial is not identically zero since for the choice $x_i = a_i$, $y_j = b_j$ the above generic element specializes to the regular element y. This discriminant can be written as P/Q where P and Q are polynomials in the variables $\alpha_t^{(i)}, \beta_{t'}^{(j)}$ and by what we said above P, Q are not identically zero. Since K is infinite we can specialize $\alpha_t^{(i)}$, $\beta_{t'}^{(j)}$ to elements of K for which $P \neq 0$ and $Q \neq 0$; if x_i specializes to x_i' and y_j to y_j' under this specialisation of $\alpha_t^{(i)}, \beta_{t'}^{(j)}$ then $z[x_1', y_1'] \cdots [x_r', y_r']$ is a regular element of A with reduced norm equal to that of z, i.e. its reduced norm is x. This proves the lemma. □

89 **Lemma b.** *Let A/K be a simple algebra of degree n^2 over its centre K, K being any field; then A contains an element with principal polynomial equal to a given separable polynomial $f(X)$ of degree n if and only if for every irreducible factor $g(X)$ of $f(X)$ the algebra $A \otimes_K K[X]/g(X)$ splits.*

If f is irreducible, this is standard. The proof for the general case is similar to the usual one (*cf.*[K_1]).

Lemma c. *Let K be a number field and $f(X) \in K[X]$ a separable polynomial; let A be a simple algebra with centre K; then A contains an element with principal polynomial $f(X)$ if and only if AK_v contains an element with principal polynomial equal to $f(X)$ for every place v of K.*

Proof. We shall make use of lemma b); let $g(X)$ be an irreducible factor of $f(X)$ and suppose $L = K[X]/g(X)$; let $g(X) = g_1(X)g_2(X) \cdots g_r(X)$ be the decomposition of g into irreducible factors over K_v; then we have

$$(A \otimes_K L) \otimes_K K_v \cong \oplus A \otimes_K K_v[X]/g_i(X) \cong \oplus A_{K_v} \otimes_{K_v} K_v[X]/g_i(X)$$

By assumption and lemma b), $A_{K_v} \otimes_{K_v} K_v[X]/g_i(X)$ is a matrix algebra over $K_v[X]/g_i(X)$ so that $(A \otimes_K L) \otimes_K K_v$ is a direct sum of matrix algebras. Also $L \otimes_K K_v \cong \oplus_{w/v} L_w$, the direct sum extended over all the extensions of v to w; hence $A \otimes_K L \otimes_K K_v \cong \oplus_{w/v} A \otimes_K L_w \cong \oplus_w (A \otimes_K L) \otimes_L L_w =$

$\oplus_w A_L \otimes L_w$ say where $A_L = A \otimes_K L$. From the splitting criterion for simple algebras over number fields it follows that $A \otimes_K L$ is a matrix algebra. **90**
Since $g(X)$ is any irreducible factor of $f(X)$ by lemma b) it follows that A contains an element with principal polynomial equal to $f(X)$. This proves the lemma. □

Proof of Proposition 1. By lemma a) we can find regular elements z_v of A_{K_v} such that $x = Nz_v$ for every place v of K. Let $f_v(X) = X_n - \cdots + \cdots + (-1)^n x$ be the principal polynomial of z_v. Let T denote the set of places v of K for which A_{K_v} is not a matrix algebra over K_v; then T is a finite set. Construct the polynomial $f(X) = X^n - \cdots + \cdots (-1)^n x$ with the constant term x such that its coefficients approximate those of $f_v(X)$ for $v \in T$. If the approximation is close enough $f(X)$ will be separable and $K_v[X]/f(X) \cong K_v[X]/f_v(X)$ for $v \in T$; this can be proved by Newton's method of approximating roots of polynomial; here one has to use the fact that the $f_v(X)'s$ are separable polynomials; we therefore assume $K_v[X]/f(X) \cong K_v[X]/f_v(X)$ for $v \in T$. Now since $f_v(X)$ is the principal polynomial of z in A_{K_v} there is an isomorphism of $K_v[X]/f_v(X)$ into A_{K_v} and from $K_v[X]/f(X) \cong K_V[X]/f_v(X)$ we conclude that there exists an isomorphism of $K_v[X]/f(X)$ into A_{K_v} for $v \in T$. Hence there exists an elements an element in A_{K_v} whose principal polynomial is equal to $f(X)$; this is true fro every $v \in T$. If $v \notin T$ then by the definition of T, A_{K_v} is a matrix algebra so that there always exists a matrix in A_{K_v} with characteristic polynomial $f(X)$. Hence the conditions of lemma c) are satisfied and we conclude that $f(X)$ is the principal polynomial of some **91**
element z of A; but then $Nz = x$ so that x is needed the reduced norm of the element z of A. This proves the proposition and so theorem 1a) is proved for groups of type ${}^1A_n$.

5.5 Proof of theorem 1a for type ${}^2A_n$; reductions (Landherr's theorem)

The classical group in this case is $G = \left\{ x \in A / xx^I = 1, Nx = 1 \right\}$ where A is a simple K-algebra with involution I of the second kind the centre L of

A being a quadratic extension of K. Consider the map $\eta : x \to (xx^I, Nx)$ of G into $A^* \times L^*$, the latter being considered as an algebraic variety over K as explained in § 3.1 Example 1 $y = xx^I$ and $z = Nx$ satisfy the relations $y^I = y$ and $Ny = zz^I$, define $H = \left\{(y,z) \in A^* \times L^* \middle| y^I = y, Ny = zz^I\right\}$; this H is not an algebraic group; but it becomes a homogeneous space for A^* under the operation given by $x : (y,z) \to (xyx^I, zNx)$. The sequence $1 \to G \to A^* \to H \to 1$ is then an exact sequence and we get the following commutative diagram:

$$\begin{array}{ccccccc} A_K^* & \xrightarrow{\eta} & H_K & \xrightarrow{\delta} & H^1(K,G) & \longrightarrow & H^1(K,A^*) = \{1\} \\ \downarrow & & \downarrow & & \downarrow \mathfrak{h} & & \\ \prod A_{K_v}^* & \xrightarrow{\eta} & \prod H_{K_v} & \xrightarrow{\delta} & \prod H^1(K_v,G) & \longrightarrow & \prod H^1(K_v,A^*) = \{1\} \end{array}$$

The mapping $\delta's$ are surjective since by § 1.7 Example 1 $H^1(K,A^*) = \{1\}$ and $H^1(K_v,A^*) = \{1\}$ for every place v of K. As in the previous paragraph we see that the kernel of h is trivial if and only if every element $b \in H_K$ which is in $\eta(A_{K_v}^*)$ for all v actually is in $\eta(A_K^*)$. So we have to prove the

92 **Proposition 1.** *Let $y \in A_K^*$, $z \in L_K^* = L^*$ be such that $y^1 = y$ and $N_y = zz^I$; suppose the equations $y = xx^I$, $z = Nx$, $x \in A^*$ are solvable locally at all places v of K i.e. with $x = x_v \in A_{K_v}^*$; then they can be solved globally in K, i.e. with $x \in A_K^*$. For the proof of this proposition we shall first carry out several reductions.*

Reduction 1. Write $z = Nx_v$, $x_v \in A_{K_v}^*$; *i*) if v extends uniquely to a place w of L then $A_{K_v} = A \otimes_K K_v \cong B$ where B is a simple algebra over L_w; this is because $A \otimes_K K_v$ is a direct sum of simple algebras and since its center $L \otimes_K K_v$ is a field, there is only one simple component; moreover, we have $A_{K_v} \cong A \otimes_L L_w$. ii) On the other hand if v extends to two different places w_1, w_2 of L then $A_{K_v} \cong A_1 \oplus A_2$ where A_1 and A_2 are simple algebras over L_{w_1} and L_{w_2} respectively; this is because in this case $L \otimes_K K_v \cong L_{w_1} \oplus L_{w_2}$ and since $A_{K_v} \cong A \otimes_L (L \otimes_K K_v)$ we have $A_{K_v} \cong A_1 \oplus A_2$ where $A_1 = A \otimes_L L_{w_1}$ and $A_2 = A \otimes_L L_{w_1}$. In the first case z is the reduce norm of an element of $A \otimes_L L_w$. while in the second

case z is a reduced norm from both A_1 and A_2. Hence z is local norm of the algebra A/L at all places of L; by the norm theorem for simple algebras (§ 5.4) we conclude that $z = Nt$ where $t \in A_K^*$. Replace (y, z) by $(t^{-1}yt^{-I}, zNt^{-1})$. The components $t^{-1}yt^{-I}$ and zNt^{-1} satisfy the same condition as (y, z); if the proposition is true for the pair $(t^{-1}yt^{-I}, zNt^{-1})$ then it is true also for the pair (y, z); now $zNt^{-1} = 1$ by the choice of t; hence we are reduce to proving the proposition in the case when $z = 1$.

Reduction 2. To carry out this reduction we need the following.

Lemma 1. *If $y \in A_K^*$ is such that $y^I = y, Ny = 1$ and if the equation $y = xx^I, x \in A^*$ is solvable locally at all places then it is solvable globally. To start with assume this lemma. The element y of proposition 1 after reduction 1) satisfies all the conditions of lemma 1. Let $x \in A$ be a solution of $y = xx^I$ assured by lemma 1. Replace (y, z) in the proposition by $(x^{-1}yx^{-1}, zNx^{-1})$. This shows that for the proof of the Proposition 1 we can assume without loss of generality that $y = 1$; but we can no longer assume $z = 1$.* **93**

We shall now prove lemma 1. Let us start by explaining our notation to be used in this paragraph. The dimension $[A : L]$ is denoted by the integer n^2. If v is any place of K then two cases occurs i) $L_{K_v} \cong L_{w_1} \oplus L_{w_2}$ if v extends to two different places w_1 and w_2 in L. ii) L_{K_v} is a field if v extends uniquely to a place w of L; in this case $L_{K_v} \cong L_w$. In case i) $A_{K_v} \cong A_1 \oplus A_2$ where $A_1 \cong A \otimes_L L_{w_1}$ and $A_2 \cong A \otimes_L L_{w_2}$; the action of I is to interchange the component. In case ii) $A_{K_v} \cong A \otimes_L L_w$ is simple algebra with center L_w. If u is an element of A_{K_v} we denote its components in case i) by $u^{(1)}$ and $u^{(2)}$; in case ii) u considered as an element of $A \underset{L}{\otimes} L_w$ is denoted by $u^{(1)}$; the two uses of the symbol $u^{(1)}$ corresponding to the different cases will be evident from the context and will not lead to any confusion. In case i) N stands for the reduced norm of A_{K_v}, i.e if $u = (u^{(1)}, u^{(2)}) \in A_{K_v}$ then $Nu = (N_1u^{(1)}, N_2u^{(2)})$ where N_1, N_2 are the reduced norm mapping of the simple algebras A_1 and A_2 respectively; in case ii) N shall denote the reduced norm of the simple algebra $A \otimes_L L_w$. By an order in a simple algebra A/K we mean a subring of A which is finitely generated as a module over the ring of integers of K **94**

and such that it generates A as a K-vector space. The algebra A_{K_v} being finite dimensional over the complete field K_v it is a normed algebra and that all its norm inducing v-topology on K_v are equivalent; when we talk of approximation of elements in A_{K_v} we mean this in the sense of the norm topology on A_{K_v}. If $\mathcal{O}$ is an order in A its completion at the place v is denote by $\mathcal{O}_v$. We shall state without proof two sublemmas which we shall use; the first one is a special case of a more general theorem of Hasee:

Sublemma a. *(Norm theorem for quadratic extensions). If L/K is a quadratic extension of the number field K then an element of K is a norm from L to K if and only if it is locally a norm at all places of K.*

Sublemma b. *(Strong approximation theorem for simple algebras, cf [11], [15]). Let G be the norm one group of the simple algebra A with center K, a number field, and $\mathcal{O}$ an order in A; let $S \supseteq \infty$ be a finite set of places of K. Suppose given a place $v_o \in S$ such that A_{v_o} is not a division algebra, and element $a_v \in G_{K_v}$; then there exists $x \in G_K$ such that $x \cong a_v$ in the v-topology for $v \in S$, $v \neq v_o$ and $x \in \mathcal{O}_v$ for $v \notin S$.*

Proof of Lemma 1. The idea of the proof can be explained thus: Replace y by the element $t_J t^I$ where $t \in A_K^*$ and $Nt = 1$; choose t in such
95 a way that $K(tyt^I)$ becomes a separable algebra of maximal degree; and then seek a solution of $tyt^I = xx^I$ with $x \in L(tyt^I)$. If the latter is possible then clearly the lemma will be proved. The actual construction of t will be the last step of the proof. In two preliminary steps we shall assume that $K(tyt^I)$ is a separable algebra of maximal degree, and investigate conditions for solvability of $tyt^I = xx^I$. In step 1) we show, by means of the quadratic norm theorem, that solvability is assured, once we know the solvability with $x \in L(tyt^I) \otimes K_v$ for every place v of K. step 2) is preparatory to step 3) in which we derive several sufficient conditions for the local solvability at v. In the final step 4) we construct t by means of the approximation theorem in such a way that for every place v at least one of these conditions is satisfied. Clearly the proof of the lemma will then be complete.

As outlined above we shall assume that $K(tyt^I)$ is a separable algebra

of maximal degree. Since I is identity on $K(tyt^I)$ and not the identity on $L(tyt^I)$, the latter is the direct sum of the spaces of symmetric elements and antisymmetric elements; if $L = K(\sqrt{d})$ then $K(tyt^I)$ is the space of symmetric elements while $\sqrt{d}K(tyt^I)$ is the space of antisymmetric elements; hence

$$L(tyt^I) \cong K(tyt^I) \oplus \sqrt{d}K(tyt^I) \cong (K \oplus \sqrt{d}K) \otimes K(tyt^I) \cong L \otimes K(tyt^I).$$

Since $K(tyt^I)$ is a commutative separable algebra it is the direct sum of separable extension fields $K_i (i = 1, 2, \dots r)$ of K. If K_1 is one such component then $L \otimes_K K_1$ being an algebra of degree two over K_1 must be either a quadratic extension of K_1 or a direct sum of two algebras isomorphic to K_1; in the former case I is the nontrivial K_1-automorphic **96**
of $L \otimes K_1$ while in the latter case I interchanges the components of any element of $K_1 \oplus K_1$. Accordingly let $K_1, \dots, K_s$ be those field among $K_i (i = 1, 2, \dots r)$ for which $L \otimes_K K_j$ is a quadratic extension of $K_j (j = 1, 2, \dots, s)$. Then we have $L(tyt^I) \cong (L \otimes K_1 \oplus \cdots \oplus L \otimes K_s) \oplus (K_{s+1} \oplus K_{s+1}) \oplus \cdots \oplus (K_r \oplus K_r)$. Let $x = (x_1, \dots, x_s, x_{s+1}, x'_{s+1}, \dots, x_r, x'_r)$ be any element of $L(tyt^I)$; $x^I = (x^I_1, \dots, x^I_s, x'_{s+1}, x_{s+1}, \dots, x'_r, x_r)$ so that we have $xx^I = (Nx_1, \dots, Nx_s, x_{s+1}x'_{s+1}, x'_{s+1}x'_{s+1}, \dots, x_r x'_r, x_r x^1_r)$. We want to solve $tyt^I = xx^I$ with $x \in L(tyt^I)$; for this assume $tyt^I = (a_1, a_2, \dots, a_s, a_{s+1}, a^1_{s+1}, \dots, a_r, a'_r)$; since tyt^I is symmetric we have $a^I_j = a_j (j = 1, 2, \dots s)$ and $a'_l = a_l (l = s + 1, \dots, r)$. From what precedes we are reduced to solving the following system of equations;

α) $Nx_j = a_j$, $j = 1, 2, \dots s$ where $a_i \in K_i$ and N denoted the norm map of the extension fields $L \otimes K_j / K_j$.

β) $x_l x'_l = a_l$, $l = s + 1, \dots r a_l \in K_i$

of these β) is trivial. For solving α) by Sublemma a it is enough to know the local solvability of the equations α at all places of K_j. Now if v is any place of K then

$(L \otimes K_j) \otimes K_v \cong \underset{w/v}{\oplus} (L \otimes K_j)_w$ where w runs through all extensions of v to the field $L \otimes K_j (j = 1, 2, \dots s)$. This implies $L(tyt^I) \otimes K_v \overset{s}{\underset{i=1}{\oplus}} \underset{w/v}{\otimes} (L \otimes K_i)_w \overset{r}{\underset{j=s+1}{\oplus}} L \otimes K_j \otimes K_v$. This shows that if the equation $tyt^I = xx^I$ is solvable with $x \in L(tyt^I) \otimes K_v$ for all places v of K then system of equation α) **97**

will be solvable locally at all places of K_j. As observed before this will imply the global solvability of equations α). This proves step 1).

Proof of Step 2. Let $u_v \in A^*_{K_v}$ be a solution of $u_v u_v^I = y$. We claim that u_v can be so chosen that $Nu_v = 1$. To see this replace u_v by $u_v.v_v$; the condition $y = (u_v v_v)(u_v v_v)^I$ then means $v_v v_v^I = 1$ and $N(u_v v_v) = 1$ means $Nv_v = Nu_v^{-1} = c$ say. From $Ny = 1$ we get $c_v c_v^I = 1$. Hence our claim will be achieved if the following problems is solved: given $c_v \in L \otimes K_v$ such that $c_v c_v^I = 1$ and that c_v is norm of $A \otimes K_v$ to find $r_v \in \otimes K_v$ satisfying the conditions $Nr_v = c_v$. This we shall do now. In case *i*), this is immediate. In case *ii*) $A_{K_v} \cong A \otimes_L L_w$ is an algebra over L_w with an involution of the second kind. If v is non-archimedean A_{K_v} must be a matrix algebra; the same holds for archimedean v, since then $L_w \cong \mathbb{C}$; moreover if x is a matrix of this algebra say $x = (x_{ij})$ then $x^I = ax^*a^{-1}$ where $x^* = (x_{ij}^I)$ and a is a hermitian matrix. The condition $r_v r_v^I = 1$ means that r_v is a unitary matrix corresponding to a. Hence we have to find a unitary matrix of a with given determinant c_v; by choosing
98 an orthogonal basis one can assume that a is diagonal $\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$;
since $c_v c_v^I = N_{L_{w/K_v}} c_v = 1$ we can find elements $d_1, \ldots, d_n$ of L_w^* such that $N_{L_{w/K_v}} d_i = d_i d_i^I = 1$ and that $d_1 \cdots d_n = c_v$ (for we can arbitrarily choose d_1, d_2, d_{n-1} to satisfy $N_{L_{w/K_v}}(d_i) = 1$ and then d_n by the condition $d_1 \cdots d_n = c_v$). The matrix $\begin{pmatrix} d_1 & .. & \\ & \ddots & \\ & & d_n \end{pmatrix}$ can then be taken for u_v. This finishes step 2).

Step 3. We shall describe three situations in which $tyt^I = xx^I$ is solvable with $x \in L(tyt^I) \otimes K_v$. Situation a) $t \cong u_v^{-1}$ in A_{K_v} in the sense of the norm topology on A_{K_v}. Suppose $\mathcal{O}$ is any order in A_K; we can assume $\mathcal{O}^I = \mathcal{O}$ since otherwise we can replace $\mathcal{O}$ by the order $\mathcal{O} \cap \mathcal{O}^I$ which will satisfy this condition. Situation *b*) v non archimedean unramified in L/K and $tyt^I \in \mathcal{O}_v$. Situation *c*) v decomposes into two places in L. In situation *a*) $tyt^I \cong u_v^{-1} y u_v^{-I}$. $= 1$ so that by the binomial theorem tyt^I is

the square of an element of $K(tyt^I) \otimes K_v$; hence we can write $tyt^I = x_v x_v^I$ with $x_v \in K(tyt^I) \otimes K_v$; this is what we wanted. In situation *b*) since $tyt^I \in \mathcal{O}_v \cap K(tyt^I)$, the components of tyt^I in $K(tyt^I) \otimes K_v$ are integers; **99**
these components are moreover units as follows from $Ntyt^I = 1$. Since L/K is unramified at v the components $L \otimes K_i (i = 1, 2, \ldots s)$ of $L(tyt^I)$ are also unramified at v. Since in an unramified local extension any unit is a local norm we conclude tyt^I can be written as $x_v x_v^I$ with $x_v \in L(tyt^I) \otimes K_v$. In situation *c*), the place v of K decomposes into two distinct places in each of the components $L \otimes K_i (i = 1, 2, \ldots, s)$ of $L(tyt^I)$. This shows that the local degree corresponding to v of the extension field $L \otimes K_i / K_i$ are all unity and so we can find in this case too elements $x_v \in L(tyt^I) \otimes K_v$ with property $tyt^I = x_v x_v^I$. This completes the proof of step 3.

Proof of Step 4. Let S be a finite set of places of K containing all v which are either archimedean or non-archimedean ramified in L, or non-archimedean and $y \notin \mathcal{O}_v$, and two further places v_o, v_1 for which A_{K_v} is the direct sum of two matrix algebras over K_v. We claim that $t_{v_1} \in A_{K_{v_1}}$ can be so chosen that $K_{v_1}(t_{v_1} y t_{v_1}^I)/K_{v_1}$ is a separable algebra of maximal degree and such that $NT_{v_1} = 1$. By the choice of v_1 if v_1 splits into the places w_1, w_2 in L/K we have $A_{K_v} \cong M_n(L_{w_1}) \oplus M_n(L_{w_2})$. Let $y = (y_1, y_2)$ and set $t_{v_1} = (t_{w_1}, 1)$; then $t_{v_1} y t_{v_1}^I = (t_{w_1} y_1, y_2 t_{w_1}^I)$. We have to choose t_{w_1} such that $N t_{w_1} y_1 = 1$ and such that the characteristic polynomial of $t_{w_1} y_1$ is separable. With this choice of t_{w_1}, the resulting t_{v_1} will satisfying our requirements. To construct t_{w_1} we have only to find element $d_1, \ldots, d_n$ in L_{v_1} which are different and such that their **100**
product is equal to 1; this is clearly possible; we can then take $t_{w_1} = \frac{1}{y_1} \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$. We have therefore constructed $t_{v_1} \in A_{K_{V_1}}$ such that $N t_{v_1} = 1$ and such that $K_{v_1}(t_{v_1} y t_{v_1}^I)/K$ is a separable algebra of maximal degree. To complete step 4 we find $t \in A_K^*$ such that i) $Nt = 1$ 2) $t \approx u_v^{-1}$ in the v-topology for $v \in S$, $v \neq v_0$, v_1 and $t \simeq t_{V_1}$ in the v_1-topology. 3) $t \in \mathcal{O}_v$ for all $v \notin S$. Then the principal polynomial of tyt^I is separable so $K(tyt^I)$ is a separable algebra of maximal degree. For this choice of t any place v will satisfy one of the conditions a), b) or c) stated in step 3

and we shall be through. The existence of t follows from sublemma bb) applied to the simple algebra A with centre L; namely an approximation condition in the v-topology is equivalent to similar conditions in the w-topologies for the extensions w_1 of v of L, and $t \in \mathcal{O}_v$ is equivalent to $t \in \mathcal{O}_w$ for the same $w's$.

Corollary . *Finitely many local solutions of $y = xx^I$ can be approximated by a global solution, i.e. if T is a finite set of places and if $y = x_v x_v^I$ with $x_v \in A_{K_v}$, $v \in T$ then there is an $x \in A_K$ with $xx^I = y$ and $x \approx x_v$ in the v-topology.*

Proof. Let $u \in A$ satisfy $y = uu^I$; the existence of this u is guaranteed by lemma 1. Write $x_v = us_v$; from $uu^I = x_v x_v^I$ we get $s_v s_v^I = 1$. If we can find $s \in A_K^*$ such that $ss^I = 1$ and $s \approx s_v$ for $v \in T$ then writing $x = us$ we see that $x \approx us_v$ and that $y = xx^I$ so that the corollary will be proved; hence we have only to find such an s. For this we make use of the Cayley
101 transform: in the representation $A_{K_v} \cong M_P(D_1) \oplus M_q(D_2)$ or $A_{K_v} \cong M_P(D)$ suppose to start with that the eigenvalues of the components of s_v are all different from -1; then $(1 + s_v)^{-1}$ exists. The relation $s_v s_v^I = 1$ then shows that $(1 - s_v)(1 + s_v)^{-1}$ is skew symmetric; call this p_v; then $p_v^I = -p_v$; we can now approximate the skew symmetric elements p_v by a skew symmetric element p of A since we have only to approximate the entries. Going back by the inverse transformation we can define $s = \dfrac{1 - p}{1 + p}$; then $ss^I = 1$ and $s \approx s_v$ for $v \in T$. If the eigen values of the components of s_v are not all different from -1 then we can write s_v as a product of two elements for which the eigenvalues are all different from -1 and we can proceed as before, This proves the corollary. □

The lemma just proved is the essential step in providing the following more general theorem due to Landherr [L]; a proof of this along the same lines as the one given here has been found independently by T. Springer.

Landherr's theorem (Form I): Let $y \in A_K^*$ be an element such that $y^I = y$. Suppose the equation $y = xx^I$ is solvable with $x \in A_{K_v}$ for every infinite place v; assume moreover that for every non archimedean

place v there exists $z_v \in L_{K_v}$ satisfying the equation $Ny = z_v z_v^I$. Then the equation $y = xx^I$ is solvable with $x \in A_K^*$.

Proof of Landherr's theorem. Let v be archimedean and let $x_v \in A_{K_v}$ is such that $y = x_v x_v^I$ holds. Taking norms on both sides we get $Ny = u_v u_v^I$ with $u_v \in L_{K_v}$. If v is non archimedean we are given that $Ny = z_v z_v^I$. **102**
These two equations clearly show that Ny is a local norm in the extension L/K at all places v of K. Hence by the quadratic norm theorem (stated in sublemma a) we can find $z \in L$ such that $Ny = zz^I$. Now suppose v is an infinite place. Write $Nx_v = z.u_v$ where $u_v \in L_{K_v}$. The condition $Ny = zz^I$ then implies $u_v u_v^I = 1$. Now apply the corollary to lemma 1 for the set of infinite places and the local solutions u_v of the equation $uu^I = 1$. Hence if $u \approx u_v$, $u \in L_K$ then $z.u \approx Nx_v$ which implies that $z.u/Nx_v$ is an n^{th} power; this is easily proved by the binomial theorem. Hence $z.u/Nx_v$ is a reduced norm from A_{K_v}, i.e. $z.u$ is a reduced norm from A_{K_v}. This is true for every archimedean place. At a non archimedean place $v, z.u$ is again a local reduced norm as we have seen in § 4.3, lemma 1. Hence by the norm theorem for simple algebras we can find $t \in A$ such that $z.u = Nt$. We shall prove that the conditions of lemma 1 are satisfied for $t^{-1}yt^{-I}$ in place of y. Clearly $t^{-1}yt^I$ is symmetric. $Ny = (zu).(zu)^I$ implies $N(t^{-1}yt^{-I}) = 1$. We have to prove that $t^{-1}yt^{-I}$ is of the form $y_v y_v^I$ for every place v of K, with $y_v \in A_{K_v}$. If v is infinite then $t^{-1}yt^{-I} = t^{-1}x_v x_v^I t^{-I} = (t^{-1}x_v)(t^{-1}x_v)^I$ and this case is settled. Let v be non-archimedean. We shall use the notations of the beginning of the paragraph § 5.5. Since by § 4.1 theorem 1 the one dimensional Galois cohomology $H^1(K_v, G)$ is trivial the mapping $A_{K_v} \longrightarrow H_{K_v}$ is surjective.The element $(t^{-1}yt^{-I}, 1)$ is clearly an element of H_{K_v}; hence there exists $y_v \in A_{K_v}^*$ such that $t^{-1}yt^{-I} = y_v y_v^I$. This proves that the condition of lemma 1 are satisfied for this $t^{-1}yt^{-I}$. Hence by that lemma **103**
there exists $x \in A_K$ satisfying $t^{-1}yt^{-I} = xx^I$; this implies $y = (tx)(tx)^I$ and so Landherr's theorem is proved. There is a second formulation of Landherr's theorem which runs as follows:

Landherr's theorem (2nd formulation). If $y \in A_K^*$ is I-symmetric and if $y = xx^I$ is solvable with $x \in A_{K_v}$ for every place v of K then it is solvable with $x \in A_K$.

Proof. Let $y = x_v x_v^I$; then taking norms we have $Ny = z_v z_v^I$ where $z_v = Nx_v \in L_{K_v}$. Hence the assumption of the first formulation are satisfied and so $y = xx^I$ can be solved with $x \in A_K$. □

5.6 Proof of Proposition 1 when *n* is odd

The proof of lemma 1 concludes the second reduction of proposition 1; accordingly for providing proposition 1 we can assume $y = 1$. The proposition then takes the form

Proposition a. *Let $z \in L_K^*$ be such that $zz^I = 1$; if the equations $z = Nx$ and $xx^I = 1$ are solvable simultaneously with $x \in A_{K_v}$ for all places v of K then they can be solved simultaneously with $x \in A_K$. This is proved by means of mathematical induction on n and the inductive proof makes use of another*

Proposition b. *Let $z \in L_K^*$ be I-symmetric; if the equations $x^I = x$ and $z = Nx$ are solvable simultaneously with $x \in A_{K_v}$ for all places v of K then they can be solved simultaneously with $x \in A_K$.*

We shall prove these propositions now. We first consider the case when n is odd. The idea of the proof may be explained as follows:

104

1) *Construct a commutative separable L-algebra B of degree n and an involution J on B which coincides with I on L such that $B = L(x)$ and $z = N_l^B(x)$, $xx^J = 1$ (or $x^J = x$ in the case (b)). Here N_L^B denotes the usual algebra norm got by the regular representation.*

   Involutions which coincide with I on L will be called I- involutions in future.

2) *Imbed B in A, the imbedding being identity on L.*

3) *Change the imbedding given in 2) by an inner automorphism of A so as to get an imbedding of algebras with involution. If we grant 1), 2) and 3) then the proofs of propositions a) and b) are simple. For since B is a separable algebra of dimension n, $N_L^B(x)$ is just the reduced norm of x and by construction $z = Nx$, $xx^I = 1$ (or $x^I = x$).*

Step 1 (Construction of B)**.** Here again for any place v we consider the two cases i) and ii) mentioned in § 5.5, namely $L_{K_v} \cong L_{w_1} \oplus L_{w_2}$ or $L_{K_v} \cong L_w$; corresponding to these two cases we have either $A_{K_v} \cong A_1 \oplus A_2$ where $A_1 = A \otimes_L L_{w_1}$, $A_2 = A \otimes_L L_{w_2}$ or $A_{K_v} \cong A \otimes_L L_w$. We claim that the local solutions x_v of the equations $z = Nx\ xx^I = 1$ (resp. $x^I = x, z = Nx$) can be assumed to be regular. This is done as follows:

Case i. (Corresponding to proposition a). *Let* $z = (z_1, z_2)$, $x_v = (x_v^{(1)}, x_v^{(2)})$ *then clearly* $z_1 = Nx^{(1)}$, $z_2 = Nx_v^{(2)}$*; as in the proof of Eichler's norm theorem* $x_v^{(1)}$ *can be replaced by a regular element also denoted by* **105** $x_v^{(1)}$ *of norm* z_1*. The condition* $x_v x_v^I = 1$ *give* $x_v^{(1)} x_v^{(2)} = 1$*; so if* $x_v^{(2)}$ *is determined by this condition both* $x_v^{(1)}$ *and* $x_v^{(2)}$ *will be regular. Hence* x_v *can be assumed regular.*

Case i. (corresponding to proposition b). $z^I = z$ *implies* $z_1 = z_2$ *and* $z = Nx$ *implies* $z_1 = Nx_v^{(1)}$*; by the same argument as above* $x_v^{(1)}$ *can be assumed to be regular; since* $x_v^I = x_v$ *implies* $x_v^{(1)} = x_v^{(2)}, x_v^{(2)}$ *is also regular; hence* x_v *can be assumed regular.*

Case ii. (corresponding to proposition a). *Here* $A_{K_v} \cong M_n(L_w)$*, a matrix algebra over* L_w*; if* $x = (x_{ij}) \in M_n(L_w)$ *and if* $x^* = (x_{ji}^I)$ *then there is a hermitian matrix a, i.e. a matrix such that* $a^* = a$ *for which* $x^I = ax^*a^{-1}$ *holds;* $xx^I = 1$ *implies that x is unitary with respect to a. This case occurred in the course of the proof of lemma 1 in § 5.5. As explained in that place we can find a regular unitary matrix* x_v *with norm equal to z.*

Case ii. (corresponding to proposition b). *In the notations above a can be assumed to be diagonal by a choice of orthogonal basis. It is then easy to find a regular diagonal matrix* x_v *with entries in K and of determinant z;* x_v *will then be I-symmetric and* $z = Nx_v$*. Hence the claim is proved and the local solutions* x_v *can be assumed to be all regular.*

Remark . It is to be noted that the only essential local condition on z occurs when $L_{K_v} \cong L_{w_1} \oplus L_{w_2}$, v real infinite and A_{K_v} is a direct sum of matrix rings over quaternion algebras; at all other places the equations in question are automatically solvable.

Let the principal polynomial $f_v(X)$ of x_v over L_{K_v} be given by **106**

$f_v(X) = X^n - a_1^{(v)}X^{n-1} + \cdots +$, where we write the coefficients $a_1^{(v)}, a_2^{(v)}, \ldots$, alternatively with positive and negative signs. Applying I to f_v we will get the principal polynomial of x_v^I; in the case of Proposition a) $x_v^I = x_v^{-1}$; the principal polynomial of x_v^{-1} is equal to $X^n - a_{n-1/z}X^{n-1} + \cdots - \frac{1}{z}$; this must be the same as f_v so that we get $a_{n-i}^v = z(a_i^{(v)})^I$. In the case of Proposition b)since $x_v^I = x_v$ we have $f_v^I = f_v$ so that $(a_i^{(v)})^I = a_i^{(v)}$. Let S be the set of places v which are either archimedean or such that A_{K_v} is not isomorphic to a direct sum of matrix algebras or itself a matrix algebra. The set S is finite. Approximate the $a_i^{(v)}$ for $v \epsilon S$ by $a_i \epsilon L$ with $a_{n-i} = za_i^I$ in the case of Proposition a) and $a_i^I = a_i$ in the case of Proposition b); since the equations for the a_i are linear, this is possible by ordinary approximation theorem; define $f(X)$ by $f(X) = X^n - a_1X^{n-1} + \cdots + (-1)_z^n$. Finally define $B = L[X]/(f(X))$. Since the $f_v(X)$ are separable (because x_v are regular) by taking close approximations we can assume $f(X)$ to be separable. Hence B is a separable algebra of degree n; again depending on the closeness of the approximation we can assume $L[X]/(f(X) \otimes_{K_v} = L_v[X]/(f(X))$ to be isomorphic to $L_{K_v}[X]/(f_v(X))$ for $v \in S$; this can be done as observed in the proof of norm theorem for simple algebras by using Newton's method of approximating roots of polynomials. We then define an involution J on B by the requirement $(X \mod f(X))^I = X^{-1} \mod f(X)$ (and resp $(X \mod f(X))^I = X$
107 $\mod f(X)$) and J restricted to L is I. Then J is an I-involution of B. By construction if x denotes the residue class of $X \mod f(X)$ then $B = L(x)$ and $z = N_L^B(x)$, $xx^J = 1$ (resp. $x^J = x$). This completes the proof of step 1).

Step 2. For $v \in S$ let B_v denote the algebra $L_{K_v}[X]/(f_v(X)) = L_{K_v}(x_v)$; we saw in step 1, that there is an isomorphism of algebras $B_{K_v} \cong B_v$; we claim that by taking approximations of step 1 close enough we get an isomorphism $(B_{K_v}, J) \cong (B_v, I)$. This is seen as follows. Let $\bar{x}$ be the image of x_v under the isomorphism θ^{-1}. To get an isomorphism af algebras with involution we require $\theta(\bar{x}^J) = x_v^{-1}$. Now since B_v is separable it has only finitely many automorphisms; hence the composite of two involution being an automorphism we conclude that B_v has only finitely many involution. Since $x_v \to \theta(\bar{x}^J)$ is an involution of B_v the set

of image $\theta(\bar{x}^J)$ corresponding to the various isomorphisms $\theta B_{K_v} \cong B_v$is finite; clearly $x \simeq \bar{x}$ which implies that $\bar{x}^J \approx x^{-1}$; i.e. $\bar{x}^J \approx \bar{x}^{-1}$; hence $\theta(\bar{x}^J)$ approximates x_v^{-1}. But since the number of $\theta(\bar{x}^J)$ that can occur is finite we see that for a sufficiently good approximation $\theta(\bar{x}^J) = x_v^{-1}$ so that we have actually an isomorphism $(B_{K_v}, j) \cong (B_v, I)$ for $v \in S$. This shows that (B, J) can be imbedded in (A, I) locally at all places $v \in S$. If $v \notin S$, A_{K_v} splits and B_{K_v} can be imbedded in A_{K_v} by regular representation. But this need not respect the involutions J and I. In any case we find that B is embeddable in A locally at all places of K. Hence B can imbedded in A; since the local imbeddings are identity on L, B can be imbedded in A such *a* way that this imbedding is identity on L. **108** This finishes the proof of step 2. corresponding to proposition a). The same can be done corresponding to proposition b) too.

Proof of Step 3. By step 2 we can assume $B \subset A$; the involution J on the maximal commutative semisimple subalgebra B can be extended to A by § 2.5 theorem 1. We denote the extension by the same symbol J. By Skolem- Noether's theorem there exists $t \epsilon A_K^*$, $t^I = t$ such that $x^J = tx^I t^{-1}$ for all $x \epsilon B$. We shall choose $s \epsilon A_K^*$ such that $x \to s^{-1}xs$ gives an imbedding of (B, J) in (A, I). In order this is true it is necessary and sufficient that we have $s^{-1}x^J s = (s^{-1}xs)^I$ for $x \epsilon B$. Now $x^I = t^{-1}x^J t$ so that $x^J = ss^I x^I s^{-I} s^{-1} = (ss^I t^{-1})x^J (ss^I t^{-1})^{-1}$.

This means we should that $ss^I t^{-1} \epsilon B^1$, the commutant of B which is B itself since B is maximal commutative. Hence we require $ss^I = bt$ with $b \epsilon B, s \epsilon A_K^*$. We shall first find b and then s. We showed above that (B, J) can be imbedded in (A, I) locally at all places $v \epsilon S$, in particular at the infinite places. Hence the equation $ss^I = bt$ is satisfied for some $s_v \epsilon A_{K_v}^*$, $b_v \epsilon B_{K_v}$ for every infinite place v. Approximate the finitely many I-symmetric elements $b_v t$ by an I-symmetric element $b_o t$ in Bt. Then $ss^I = b_o t$ is solvable with $s \epsilon A_{K_v}^*$ for all infinite places v. By taking norms $c = N(b_0 t) \epsilon K$ is a norm from $L \otimes K_v / K_v$, and therefore $ss^I = c^{-1} b_0 t = bt$ is solvable with $s \in A_{K_v}^*$. On the other hand $N(bt) = N(c^{-1} b_0 t) = c^{1-n} = c^{(1-n)/2} (c^{(1-n)/2})^I$. So by Langherr's theorem $ss^I = bt$ is solvable globally. Hence the mapping $x \to s^{-1}xs$ gives an imbedding of (B, J) in **109** (A, I). The same can be done for proposition b) Hence step 3 is complete

and so proposition a and b are proved when n is odd.

5.7 Proof of Propositions a), b) when n is even

The idea is the following

I) Construct an I-invariant quadratic extension N of L, $N \subset A$ and a primitive element y of N/L i.e. an element for which $N = L(y)$ such that 1) $N_L^N y = z$, $yy^I = 1$ (resp $y^I = y$), 2) the equations $y = \bar{N}x$, $xx^I = 1$ (resp. $x^I = x$) are solvable locally in N', the commutant of N in A; here $\bar{N}$ denotes the reduced norm mapping of the simple algebra N' with centre N. Observe that if M denotes the field $M = \{a \in N / a^I = a\}$ then M is quadratic over K and that N is the composite of M and L; the latter shows that the commutant of N is the intersection of those of M and L i.e. $N' = M'$, M' being the commutant of M in A. The proof of the proposition will be by induction on the power of 2 contained in n as factor. This is justified as we have proved the propositions for odd n; since $[N^1 : N] = \frac{[N' : L]}{2} = \frac{[A : L]}{2(N : L)} = (\frac{n}{2})^2$ and the hypothesis of the propositions are satisfied for N' and y in the place A and z respectively induction applies; by induction we can therefore assume the truth of the proposition for N'; hence the equations in 2) are solvable globally; let x be a global solution; then since reduced norm of x in A is equal to $N_L^N y = z$ we find that this x gives a global
110 solution of the equations $Nx = z$ (N denotes reduced norm in A), $xx^I = 1$ (resp. $x^I = x$); we have remarked in § 5.6 that for local solvability of our problem the only conditions come from those real infinite places for which the algebra is isomorphic to a direct sum of two matrix rings over the quaternions. We shall take care of the local conditions 2) by constructing N in such a way that this critical case does not occur for any place w of M. Let w be an extension of the place v of K. If $K_v \cong \mathbb{C}$, or $N \otimes K_v \cong \mathbb{C}$, then w is certainly not critical. If $A \otimes K_v$ is isomorphic to the direct sum of two matrix rings over K_v then $N' \otimes_M M_w$ is isomorphic to the direct sum of two matrix rings over M_w. If finally $A \otimes K_v$ is isomorphic

to a direct sum of two matrix rings over the quaternions, then we shall construct N such that $N_w \cong \mathbb{C}$, and so w is not critical either.

II) We shall construct N abstractly to start with; we then construct a commutative separable L-algebra B of maximal degree with an I-involution J such that i) (N, I) is imbeddable in (B, J) so that N can be identified with a subfield of B and then $J/N = I/N$ ii) $B = N(x)$ for a suitable x.

III) Imbed B in A; extend J to A by the theorem on extension of involutions, and then change the imbedding by an inner automorphism to get an imbedding of algebras with involution. The constructions outlined in I, II and III will be achieved once we prove the following lemmas.

Lemma 1. *There exists a finite set S of places of K including the archimedean places such that for $v \notin S$ and any commutative separable L_{K_v}-algebra with I-involution J say B_v of dimension n there exists an imbedding of (B_v, J) into (A_{K_V}, I).* 111

Lemma 2. *For every $v \in S$ there exists y_v, x_v in A_{K_v} such that*

i) $N_v = L_{K_v}(y_v)$, $B_v = N_v(x_v)$ *are commutative separable algebras*

ii) $N_v \cong L_{K_v}[Y]/_{Y^2-\lambda_v Y+z}$ *under the mapping which takes the residue class of Y onto y_v.*

iii) such that $y_v y_V^I = 1$ *(Resp* $y_V^I = y_v$*) and*

iv) $B_v \cong N_v[X]/_{(x^{\frac{n}{2}}+\cdots)}$ *under the mapping taking the residue class of X on to x_v, the coefficients of $X^{\frac{n}{2}} + \cdots$ being in L_{K_v}. If A_{K_v} is a direct sum of matrix rings over quaternion algebras then y_v can be so chosen that the field M_v of I-invariance N_v is isomorphic to $\mathbb{C}$.*

Lemma 3. *After possibly replacing z by zNu^{-1} with $u \in A_K$, $uu^I = 1$ (resp. by $zNuNu^I$ with $u \in A_K^*$) there exists a place $w \notin S$ with L_{K_w} a field and a quadratic field extension N_w with an I-involution J_{N_W}*

such that $N_w = L_{K_w}(y_w)$ with y_w satisfying the conditions $N_{L_{K_w}}(y_w) = z$, $y_w y_w^J = 1$ (resp $y_w^J = y_w$).

Lemma 4. *Let K be a number field, L, M two different quadratic extensions of it; let N be the composite of L and M. Suppose there exists a place w of K such that N_{K_w} is a field; then for a given $c \in K^*$, if the equation $(N_{L_K} l) = (N_K^M m)c$ is solvable locally then it is solvable*
112 *globally. Finitely many local solutions can be approximated. We shall assume these lemmas and show how N, B and J can be constructed; first we make the replacement necessitated by lemma 3. This does not affect local and global solvability. Now let $Y^2 - \lambda_w Y + z$ be the minimal polynomial of y_w in N_w/L_w; where N_w is constructed as in lemma 3. Let $\lambda \in L$ approximate the λ_v's for $v \in S$ and λ_w. Define $N = L[Y]/Y^2 - \lambda Y + z$; since $Y^2 - \lambda_w Y + z$ is irreducible so is $Y^2 - \lambda Y + z$ irreducible over L; hence N is a filed; let y be the residue class of Y modulo $(Y^2 - \lambda Y + z)$; then $N = L(y)$. As in the proof of step 2 of Proposition a) and b) of § 5.6 if the approximation is good enough then the stipulation $J/L = I/L$, $y^J = y^{-1}$ (reap. $y^J = y$) will define an I-involution J on N; similarly approximating the coefficients of the polynomial $X^{\frac{n}{2}} + \cdots +$ given for B_v, $v \in S$ in lemma 2 we get a polynomial with coefficients in N and a maximal commutative separable algebra $B = N[X]/X^{\frac{n}{2}} + \cdots$ with an involution also denoted by J extending the involution J on N; if our approximations are good enough we have as in the proof of step of 1 of Propositions a) and b) of § 5.6 that $B_{K_v} \cong B_v$ for $v \in S$ so that B_{K_v} is imbeddable in A_{K_v} for $v \in S$; by lemma 1 this is true even if $v \notin S$; hence B is locally imbeddable in A at places v of K. Hence B is imbeddable in A globally. Since N is imbeddable in B this simultaneously gives an imbedding of N in A so that we can assume hereafter that $L \subset N \subset B \subset A$. Next we extend the involution J on B to A by the theorem on extensions of involutions; we denote the extension also by the same letter J. By Skolem Noether's theorem we can find $t \in A$, $t^I = t$ such that $x^J = t x^I t^{-1}$ holds for every $x \in A$. We want to choose an $s \in A^*$ such that $x \to s^{-1} x s$ given an*
113 *imbedding of (N, J) into (A, I); this replaces N by $s^{-1} N s$; the necessary and sufficient condition for this is that the following equations hold as*

in the proof of the case of odd n : $ss^I = ut$, $u \in N'$ and $u^J = u$. We claim that these equations are solvable locally with $s \in A_{K_v}$, $u \in N'_{K_v}$ for all v; this is seen as follows: if $v \in S$ we know that $N_{K_v} \cong L_{K_v}[Y]/(Y^2 - \lambda_v Y + z)$ in the notations of lemma 2, and this will moreover be an isomorphism of algebras with involution if the approximations are close enough as we saw in the case of odd dimension. By lemma 2 then $(N_{K_v,J})$ is imbeddable in (A_{K_v}, I) for $v \in S$. If $v \notin S$ lemma 1 asserts that the algebra (B_{K_v}, J) can be imbedded in (A_{K_v}, I); this then gives an imbedding of (N_{K_v}, J) in (A_{K_v}, I); hence (N, J) is imbeddable locally in (A, I) so that the equations $ss^I = ut$, $u \in N'$, $u^J = u$ are solvable locally everywhere; if (s_v, u_v) are local solutions at the place v taking reduced norms on both sides of the equation $s_v s_v^I = u_v t$ we get $l_v l_v^I = (N_L^N m_v)$. Nt where $l_v = Ns_v$ and $m_v = \bar{N}u_v$ ($\bar{N}$ denotes the reduced norm of N' over N). Since L and M are linearly disjoint over K we have $N_L^N m_v = N_K^M m_v$; Moreover $l_v l_v^I = N_K^L l_v$; hence $N_K^L l_v = (N_K^M m_v)(Nt)$. This shows that the equations $N_K^L l = (N_K^M m)(Nt)$ are solvable locally everywhere; applying lemma 4 we can approximate the local solutions (l_v, m_v) for v at infinity by a global solution say (l, m); write $1 - \alpha_v = \dfrac{m}{m_v}$; if the approximations is close enough $(1 - \alpha_v)^{\frac{1}{n}}$ can be developed by a power series and since $\alpha_v^J = \alpha_v$ applying J to the terms of this power series we get $(1 - \alpha)^{\frac{1}{n}}$ is J-invariant; hence $\dfrac{m}{m_v}$ is the reduced norm in N' of a J-invariant element; since $m_v = \bar{N}u_v$ with $u_v^J = u_v$ we see that the equation $m = \bar{N}u$ **114** *is solvable locally at infinity by J-invariant elements; we shall now apply Proposition b); the local conditions for the solvability of $m = \bar{N}u$ come only from the infinite places and we have shown that the equation is solvable locally at infinity. Since the maximum power of 2 dividing $[N' : N]$ is less than the corresponding number for $[A : L]$ we can apply the induction hypothesis to N', $m \in N'$ which is J-symmetric; hence we can find $u \in N'$ with $m = \bar{N}u$ and $u^J = u$.*

Next the equation $ss^I = ut$ will be solved by using Landherr's theorem first formulation; we have proved that this is solvable locally at the places in S, in particular at infinity; next by construction of m we have

$N(ut) = N_K^L l = ll^I$; moreover $(ut)^I = t^I u^I = t.t^{-1}.u^j.t = ut$. Hence the conditions of Landherr's theorem are satisfied and so we can find $s \in A_K$ with $ss^I = ut$. This solves the problem of imbedding (N, J) globally in (A, I). Identifying N with its image we can write $N = L(y)$; by construction this N and y have all properties required in 1) of the beginning of the proof. As for the requirement 2) the local conditions necessary to ensure the local solvability are void in view of lemma 2.

We shall now go on to the proofs of the lemmas 1 - 4.

Proof of Lemma 1. Let $\mathcal{O}$ be an order in A which we assume to be I-invariant (otherwise take $\mathcal{O} \cap \mathcal{O}^I$). If v is some place of K and B a separable algebra over L_{K_v} we shall denote the set of integers of B of $\mathcal{O}(B)$.
115 Let S be the set of these places v of K which are either archimedean or ramified in L/K or such that $\mathcal{O}_v$ is not a matrix over $\mathcal{O}(L_{K_v})$; the non-archimedean places which satisfy the property are divisors of the discriminant of $\mathcal{O}$ and so finite in number; since the places satisfying either the first or second property are also finite in S is a finite set. We claim this S will have the property stated in the lemma: Let $v \notin S$.

Case i. *$L_{K_v} \cong K_v \oplus K_v$; in this case $A_{K_v} \cong A_1 \oplus A_2$ where A_1, A_2 are matrix rings over K_v and I interchanges the components. Similarly $B_v \cong B_1 \oplus B_2$ and J interchanges the components; by the regular representation B_1 can be imbedded in A_1; if f is this imbedding and $b \in B_1$ then $f(b^J) = f(b)^I$ extend this to an imbedding of (B_v, J) into (A_{K_v}, I).*

Case ii. *L_{K_v} is a field; in this case $A_{K_v} \cong M_n(L_{K_v})$ and if $x \in A_{K_v}$ is considered as a matrix (x_{ij}) over L_{K_v} then $x^I = ax^*a^{-1}$ where $x^* = (x_{ji}^I)$ and a is a fixed hermitian matrix i.e., $a^* = a$. Since $\mathcal{O}^I = \mathcal{O}$ we have $a\,\mathcal{O}_v a^{-1} = \mathcal{O}_v$; now a is determined up to a scalar matrix over K_v, multiplying a by a suitable scalar matrix over K_v multiplying a by a suitable scalar matrix over K_v, since v is unramified in L/K, we can assume a to be a primitive matrix; the condition $a\mathcal{O}_v a^{-1} = \mathcal{O}_v$ will then imply that $a, a^{-1} \in \mathcal{O}_v$. Hence the discriminant of the hermitian form corresponding to a, namely delta is a unit in L_{K_v}; but since $a^* = a$ deta is invariant under I which implies that deta $\in K_v$. Using the fact that*
116 *L_{K_v}/K_v is unramified we can write $\det a = \lambda\lambda^I$ with $\lambda \in L_{K_v}$. Now*

over a p-adic field any hermitian from is determined by its discriminant and dimension; choosing a matrix $u \in M_n(L_{K_v})$ with determinant λ the matrix uu^I is hermitian with discriminant equal to det a; hence we have shown that a can be written as uu^I.

Write A_{K_v} as End (V), where V is a n-dimensional vector space over L_{K_v} and End (V) means the endomorphism ring. The action of I on End (V) can be described as follows; let u, v be two vectors of V; we consider them as n-tuples over L_{K_v}; let $(u, v) = uav^*$; take $x \in$ End V then we have $(ux, v) = (uxav^*) = ua(vax^*a^{-1})^* = (u, vx^I)$. We have to construct an embedding of (B_v, J) into the endomorphism ring of such a vector space with hermitian form. On the space B_v we introduce the hermitian form defined by $(u, v) = Tr_{L_{K_v}}^{B_v}(uv^J c)$ where c is an invertible element in B_v to be chosen properly to satisfy $c^J = c$ and to make the discriminant of (u, v) a unit. This is a non-degenerate hermitian form since trace map in a separable algebra in non-trivial. Let $\mathcal{O}(B_v)^* = \{u \in B_v | (u, v) \in \mathcal{O}(L_{K_v})\ \forall v \in \mathcal{O}(B_v)\}$. The hermitian form is unimodular (i.e., discriminant a unit) if and only if $\mathcal{O}(B_v) = \mathcal{O}(B_v)^*$ (a nonzero regular lattice in a quadratic space is unimodular if and only if it is equal to its dual). As v runs through elements of $\mathcal{O}(B_v)$, $v^J c$ runs through elements of $\mathcal{O}(B_v).c$; hence $\mathcal{O}(B_v)^* c$ is just the dual of $\mathcal{O}(B_v)$ with respect to Tr and so is equal to $\vartheta^{-1}_{B_v/L_{K_v}}$, the inverse different of $B_v.B_v$ is a direct sum of local fields and $\mathcal{O}(B_v)$ is the direct sum of rings of integers in these fields each of which is a principal ideal ring and so $\mathcal{O}(B_v)$ itself is a **117** principal ideal ring; hence $\vartheta^{-1}_{B_v/L_{K_v}}$ can be written as $\mathcal{O}(B_v)c$ with $c \in B_v$; since $\vartheta^{-1}_{B_v/L_{K_v}}$ is invariant under J and L_{K_v}/K_v is unramified we can take c to satisfy $c^J = c$. The dimensions of the vector spaces B_v and V are the same and by this choice of c the hermitian form (u, v) and B_v and the hermitian form coming from the matrix a on V are isomorphic.

Next imbed B_v in End (B_v) by regular representation; we then claim that J goes into the involution $*$ with respect to the matrix of (u, v); for if $x \in B_v$ and u, v are vectors of B_v then $(ux, v) = Tr(uxv^J c) = Tr(u(x^J v)^J c) = (u, x^J v)$. This proves lemma 1.

Lemma 2.

Case i. *v non-archimedean and $L_{K_v} \cong K_v \oplus K_v$ and consequently $A_{K_v} \cong A_1 \oplus A_2$ the involution I interchanging the components. The problem reduces to one concerning A_1, i.e., if $y_v = (y_1, y_2)$ we have to construct y_1 so that $K_v(y_1)$ will be a separable sub-algebra of A_1 and then fix y_2 by the condition $y_v y_v^I = 1$ (resp $y_v^I = 1$). Let D be the quaternion division algebra over K_v; if $z = (z_1, z_2)$ then we know that z_1 is the reduced norm of a regular element of the division algebra D and so the principal polynomial of z say $Y^2 - \lambda_1 Y + z_1$ is irreducible over K_v; let $N_1 = \dfrac{K_v[Y]}{(Y^2 - \lambda_1 Y + z_1)}$ then N_1 is a field extension of K_v of degree 2. Since the degree n of A_1 is even by local theory of central simple algebras the field N_1, can be imbedded in A_1; let y_1 be the image of the residue class of Y; then we can write $N_1 = K_v(Y_1)$; choosing y_2 to*
118 *satisfy the condition $y_2 = y_1^{-1}$ (resp $y_2 = y_1$) $K_v(y_1) \oplus K_v(y_2)$ will be the separable algebra N_v sought.*

Case ii. *v archimedean and $L_{K_v} \cong K_v \oplus K_v$. If $K_v \cong \mathbb{R}$ and $z = (z_1, z_2)$ with $z > 0$, essentially the same argument as in case i applies. In particular by the local solvability condition, this happens if A_{K_v} is the direct sum of two matrix rings over the quaternions, and then by construction N_1 and so the algebra of I-invariant elements in N_v is isomorphic to $\mathbb{C}$. In all other cases $A_{K_v} \cong A_1 \oplus A_2$ with A_1, A_2 isomorphic to $M_n(K_v)$ the $n \times n$ matrix ring over K_v. In the construction of case i we may then use an arbitrary λ_1, but now N_1 is not necessarily a field, but may be isomorphic to $K_v \oplus K_v$. If so we have to be careful with the embedding of N_1 into A_1 and we do it by mapping $(u, v) \in K_v \oplus K_v = N_1$ into $\begin{pmatrix} u & & \\ & \ddots & \\ & & v \end{pmatrix} \in M_n(K_v) = A_1$. For X_1 we take any regular diagonal matrix.*

Case iii. *L_{K_v} is a field; here $A_{K_v} \cong M_n(L_{K_v})$ and I has the action $x^I = a x^* a^{-1}$ where a is a fixed hermitian matrix with the usual notations; by choosing an orthogonal basis we can assume the hermitian form to be diagonal; choose $c \in L_{K_v}$ such that $cc^I = 1$ (resp $c^I = c$) and such that $c \neq z/c$; take for y_v the matrix*

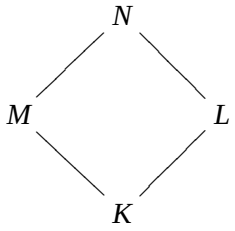
$$\left(\begin{array}{c|c} o & O \\ \hline O & \pi/\varepsilon_{z/c} \end{array} \right\}_n^n ;$$

then $y_v y_v^I = 1$ (resp $y_v^I = y_v$); the principal polynomial of this matrix is $(Y - c)(Y - z/c)$ which is separable; consequently the algebra **119**
$\frac{L_{K_v}[Y]}{(Y-c)(Y-z/c)}$ *is separable and is isomorphic to $L_{K_v} \oplus L_{K_v}$. We can take this algebra for N_v and any regular diagonal matrix for x_v.*

Proof of Lemma 3. By algebraic number theory there exists infinitely many places for which L_{K_w} is a field. Choose such a $w \notin S$. In the case of Proposition a) approximate the local solution x of $z = Nx$ by $u \in A_K$ with u having the property $uu^I = 1$; then $z \approx Nu$ and so z/Nu can be assumed to be a square r^2 say where $r \in L_K$; now $zz^I = 1$ and Nuu^I so that $rr^I = \pm 1$. Since r can be taken to approximate 1 we can have $rr^I = 1$. Replacing z by z/Nu we have only to prove the lemma for this new z. Let M_w be a quadratic extension of K_w different from L_{K_w} which exists for the $\mathcal{P}$-adic field K_w. Then if N_w denotes the composite of L_w and $M_w, \ldots N_w$ is quadratic over L_w and we have $z = N_{L_w}^w(r)$; we put $y_{w_N} = rs$ with s in N_w but not in L_{K_w} satisfying the conditions $N_{L_w}^w(s) = 1$ and $N_{M_w}^{N_w}(s) = 1$; if H resp. J are the non-trivial automorphisms of N_w over L_w resp. M_w, $s = \frac{tt^{HJ}}{t^H t^J}$ with suitable $t \in N_w$ satisfies these conditions. This y_w clearly satisfies all the requirements of the lemma. In the case of proposition b), if z is a norm from L_w/K_w, we may first change z to $zNuNu^I$ and so assume $z = r^2$ with $r^I = r$, similar to case *a*) and then put $N_w = L_w M_w$ and $y_w = rs$ with s in M_w but not in K_w, $N_{K_w}^{M_w}(s) = 1$. On the otherhand if z is not a norm from L_w/K_w choose a quadratic extension M_w/K_w from which z is a norm $z = N_{K_w}^{M_w}(y_w)$. Then **120**
necessarily L_w is different from M_w and $y_w \in K_w$ so we are through.

We shall now go to the proof of lemma 4 which is the only remaining thing to be proved for establishing theorem a a) for groups of type ${}^2A_n$.

Consider the diagram below



here M and L are quadratic extensions of K and N is the composite of M and L; we are given $c \in K^*$ and our assumptions are i) the equation $N_K^L l = cN_K^M m$ is solvable locally; i.e. given a place v of K the equation is solvable with $l \in L \otimes K_v$ and $m \in M \otimes K_v$; ii) there is at least one place w of K such that M_{K_w} is a field. We then want to assert the solvability of $N_K^L l = cN_K^M m$ globally, i.e. with $l \in L$ and $m \in M$. Let G_m be the 1-dimensional multiplicative group; consider L^*, M^* as two dimensional tori over K and let $T = L^* \times M^*$ be their product which is again a torus. Since N is a splitting field for both L^* and M^* it is a splitting field T; consider a map $T \to G_m$ defined by $(x, y) \to (N_K^L x)(N_K^M y^{-1})$. This map is defined over N and using the fact that N splits T one can see that the map is surjective; Let T' be the kernel; then T' will be again a torus over K split by N.

$$1 \to T' \to T \to G_m \to 1 \qquad \cdots . \tag{1}$$

121 will be an exact sequence defined over N; the ground field being of characteristic zero the homomorphism $T \to G_m$ will be separable; hence taking rational points over N we get an exact sequence

$$1 \to T'_N \to T_N \to (G_m)_N \to 1$$

The homomorphisms involved in this sequence are g-homomorphisms where g denotes the Galois group of N/K. To any given place v of K we select arbitrarily a place v' of N extending v and keep it fixed throughout; the decomposition group of v' depends only on v and not on the extension v' chosen since N/K is abelian; hence we can denote it by g_v: then g_v will be the Galois group of $N_{K_{v'}}/K_v$. Passing to $N_{v'}$-rational

points in (1) we will get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T'_N & \longrightarrow & T_N & \longrightarrow & (G_m)_N & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & T_{N_{v'}} & \longrightarrow & T_{N_{v'}} & \longrightarrow & (G_m)_{N_{v'}} & \longrightarrow & 1 \end{array}$$

where the vertical maps are inclusions; here the rows are respectively g-exact and g_v-exact sequences; and the vertical maps are compatible with the inclusion $g_v \to g$; hence passing to cohomology we get the following commutative diagram:

$$\begin{array}{ccccc} T_K & \xrightarrow{\alpha} & K^* & \xrightarrow{\beta} & H^1(g_{N/K}, T'_N) \\ \downarrow f & & \downarrow g & & \downarrow h \\ T_{K_v} & \xrightarrow[\bar{\alpha}]{} & K_v^* & \xrightarrow[\bar{\beta}]{} & H'(g_v, T'_{N_v}) \end{array}$$

Now $g(c)$ is in the image of $\bar{\alpha}$ by assumption of local solvability of **122**
$N_K^L l = cN_K^M m$; hence $\bar{\beta}$ maps $g(c)$ into (1) which implies that h maps $\beta(c)$ into (1); the lemma is equivalent to proving that c is in the image of α, i.e. we have to show that $\beta(c) = (1)$: hence the proof of the lemma will be achieved if the product map $H^1(g_{N/K}, T_N^1) \to \prod_v H(g_v, T'_{N'_v})$ is injective. But this we have proved in § 3.2, theorem 6 a).

If finally (l_v, m_v) are finitely many local solutions and (l, m) is a global solution, then $(a_v, b_v) = (l_v l^{-1}, m_v m^{-1})$ are local solutions of $N_K^L a = N_K^M b$. If we can approximate these by a global solution (a, b), then (al, bm) will be a global solution of our original equation approximating the given local solutions (l_v, m_v). Now it can be shown that every solution (a_v, b_v) is of the form $a_v = c_v N_L^N d_v$, $b_v = c_v N_M^N d_v$ with $c_v \in K_v$, $d_v \in N \otimes K_v$; so we can put $a = cN_L^N d$, $b = cN_M^N d$ with $c \in K$, $d \in N$ approximating c_v, d_v. This completes the proof of lemma 4 and of theorem a a) for groups of type ${}^2_{A_n}$.

5.8 Proof of theorem 1a for groups of type C_n

By the classification given in §5.1, groups of type C_n are either the symplectic groups or the special unitary groups of hermitian forms over quaternion algebras. In the case of symplectic group the theorem is a consequence of §1.7, Example 3. In the second case since the special unitary group coincides with the unitary group, we have to consider
123 $G = U_n(C/K, h)$ where C is a quaternion algebra and h is a hermitian form. The proof for this case is given by induction on the integer n. For $n = 1, U_1(C/K, h)$ is isomorphic to a group of type A_1 and by our proof for groups of the latter type theorem a a) holds for $U_1(C/K, h)$. Hence by induction assume theorem a a) is proved for unitary groups in $(n-1)$ dimension, $n \geq 2$. Let V be the vector-space on which the unitary group U_n operates. This space V will be of dimension $4n$ over K. Let x_o be an anisotropic vector of V. Let $h(x_o) = c$ where $c \in K^*$. Let U_{n-1} be the unitary group corresponding to the orthogonal complement of x_o; let $H = U_{n-1}$; consider the following commutative diagram:

$$\begin{array}{ccc} H^1(K,H) & \longrightarrow & H^1(K,G) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ \prod H^1(K_v,H) & \longrightarrow & \prod H^1(K_v,G) \end{array}$$

we have to prove that β is injective; let $(a) \in H^1(K,G)$ be mapped onto (1) by (β); then $\beta(a)$ is in the image of ψ; hence by proposition 1 of § 1.5 the twisted homogeneous space ${}_a(G/H)$ has a K_v-rational point for every $v \in \infty$; we shall prove that this implies ${}_a(G/H)$ has a K-rational point; we shall also prove that ψ is injective. Granting these we apply proposition 1 of § 1.5 again; hence there exists $(b) \in H^1(K,H)$ such that $\varphi(b) = a$; now $\psi \circ \alpha(b) = \beta \circ \varphi(b) = (1)$, so that by the injectivity of ψ we have $\alpha(b) = (1)$; but by induction assumption α is injective hence $b = (1)$ which implies $a = (1)$ which is what is required to be
124 proved; we shall now prove the two assertions made. The group G operates transitively on the sphere $\left\{x \in V \middle| h(X) = c\right\}$ over $\bar{K}$ and H is the isotropy subgroup of $x_\circ$ of this sphere; hence G/H is isomorphic to this

sphere over $\bar{K}$; we can twist both V and h by the cocycle a since h is invariant under all the automorphism a_s, $s \in (\bar{K}/K)$; let the twisted sphere be $\{x \in V'/h'(x) = c\}$ which is then isomorphic to ${}_a(G/H)$ over $\bar{K}$. Since ${}_a(G/H)$ has a K_v-rational point for every place v of K the preceding isomorphism implies that $h'(X) = c$ is solvable locally at all completion K_v of K; now h' can be considered as a quadratic form over K in $4n$ variables; this quadratic form over K represents the nonzero c locally at K_v for all places v of K by assumption; hence Minkowski-Hasse's theorem it presents c globally in K and so ${}_a(G/H)$ has a K-rational points. Next we shall prove the injectivity of ψ; from the exact sequence $1 \to H \to G \to (G/H) \to 1$ of $g_{\bar{K}_v/K_v}$-sets we get exact sequence

$$G_{K_v} \to (G/H)_{K_v} \to H^1(K_v, H) \to H^1(K_v, G) \tag{1}$$

Now the map $G_{K_v} \to (G/H)_{K_v}$ is defined through the operation of G on the homogeneous space G/H; by lemma 2 of § 2.6 the operation of G_{K_v} on $(G/H)_{K_v}$ is transitive; hence the map $G_{K_v} \to (G/H)_{K_v}$ is surjective which then implies by the exactness of (1) that the map $h^1(K_v, H) \to H^1(K_v, G)$ is injective. Hence the map ψ is injective.

5.9 Quadratic forms

If $G = \mathrm{Spin}_n$, $n = 3$, by considering the Dynkin diagram we get isomor- **125**
phisms of G onto groups of type A_m or C_m so that theorem a a) is true for these $n's$. So assume $n \geq 4$; choose a non-isotropic vector $x_\circ \in V$, V being the vector space on which the quadratic form is given; let 0_{n-1} be the orthogonal group of its orthogonal complement; let H be its simply connected covering; then H is Spin_{n-1}; for proving theorem a) we use induction on n; so assume the theorem for $n-1$; consider the comutative diagram below.

$$\begin{array}{ccccc} (G/H)_K & \xrightarrow{\varphi} & H^1(K,H) & \xrightarrow{\psi} & H^1(K,G) \\ \downarrow f & & \downarrow g & & \downarrow h \\ \prod_{v\in\infty} (G/H)_{K_v} & \xrightarrow{\alpha} & \prod_{v\in\infty} H^1(K_v,H) & \xrightarrow{\beta} & \prod_{v\in\infty} H^1(K,G) \end{array} \tag{2}$$

Let $(a) \in H^1(K, G)$ be mapped onto (1) by h; then as in the discussion of C_n, ${}_a(G/H)$ has K_v-rational point for every v; now we have $\mathrm{Spin}/\mathrm{Spin}_{n-1} \cong SO_n/SO_{n-1} \cong O_n/O_{n-1}$ which is isomorphic to the sphere $\{x \in V/\mathscr{G}(x) = c\}$ where $c = \mathscr{G}(x_o)$; hence over $\bar{K}$ ${}_a(G/H) \cong \left\{x \in V' \middle/ \mathscr{G}'(x) = c\right\}$ where $(V', \mathscr{G}')$ is got by twisting $(V, \mathscr{G})$ by the cocycle a; by assumption the quadratic form $\mathscr{G}'(x)$ represents c locally at infinity. Since $n \geq 4$ the quadratic form $\mathscr{G}'(x)$ represents c locally at the non-archimedean completion of K as well; hence c is represented by $\mathscr{G}'(x)$ locally in all K_v; applying Hasse-Minkowski's theorem $\mathscr{G}'(x)$ represent c globally; hence ${}_a(G/H)$ has a K-rational point; this implies
126 the existence of $b \in H^1(K, H)$ such that $\psi(b) = a$; then $\beta(g(b)) = (1)$ so that there exists $c \in \prod_{v \in \infty}$ which $\alpha(c) = g(b)_1$; we shall prove presently that c can be so chosen that it is in the image of f; granting this there exists $d \in (G/H)_K$ such that $f(d) = c$; then $g(\varphi(d)) = g(b)$; by induction assumption g is injective so that $b = \varphi(d)$; but then $a = \varphi(b) = \varphi o \varphi(d) = (1)$ and so h will be injective; hence we have only to prove c can be chosen as required above. By the exactness of the bottom row in (2) two elements of $\prod_{v \in \infty} (G/K)_{K_v}$ will go into the same element under the map $\prod (G/H)_{K_v} \to \prod H^1(k_v, H)$ if and only if there differ by an element of $\prod G_{K_v}$ as factor hence the fact that c can be chosen to lie in the image of f will follow from the lemma below:

Lemma 1. *Given elements $x_v \in (G/H)_{K_v}$ for archimedean there exist elements $u_v \subset G_{K_v}$ such that $u_v x_v \in (G/H)_K$ and are the same for all v.*

Proof. Here G/H is the sphere $T = \left\{x \in V \middle/ \mathscr{G}(x) = c\right\}$ and so $(G/H)_{K_v}$ is the set of solutions of $\mathscr{G}(x) = c$ rational over K_v. By Witt's theorem $(O_n)_{K_v} = O_{K_v}$ acts transitively on the sphere T; since $x_o \in T$ we can find $t_v \in O_{K_v}$ such that $x_v = t_v x_o$; if t_v is improper by multiplying t_v on the right by a reflection in a plane containing x_o we can make product proper and $t_v x_o$ is not disturbed by this change; hence without loss of generality we can assume $t_v \in SO_{K_v}$; let a be the matrix of the quadratic form $\mathscr{G}$ with respect to some basis; let $x^I = a^t x a^{-1}$ for $x \in O_n$; then $x x^I = 1$ by definition of O_n; approximate the $t_v's$ by a $t \in SO_K$ and put $x = t x_o$ so that $x \in (G/H)_K$ and $x \simeq x_v$; we shall now show that x is in

$G_{K_v}x_v$; the orbit of x_v under the action of G_{K_v} is just $(G/H)_{K_v}$ by Witt's **127**
theorem; now $\mathrm{Spin}_n \to SO_n$ is surjective and is a local isomorphism over $\bar{K}_v$ since it is a covering; hence $(\mathrm{Spin}_n)_{\bar{K}_v}$ is local isomorphism; this homomorphism is compatible with the action of the Galois group $g_{\bar{K}_v/K_v}$; hence forming the group of fixed points under the action of $g_{\bar{K}_v/K_v}$ in the above groups we get a local isomorphism $(\mathrm{Spin}_n)_{K_v} \to (SO_n)_{K_v}$; this shows that the latter map is surjective onto a neighbourhood of 1 in $(SO_n)_{K_v}$; now by construction $t_v t^{-1} \approx 1$ and $t_v t^{-1} \in (SO_n)_{K_v}$ hence $t_v t^{-1}$ is the image of some element $u_v^{-1} \in (Spin_n)_{K_v}$ under the above homomorphism; then $x = tx_o = tt_v^{-1}x_v$; going back from T to G/H by the isomorphism $G/H \cong T$ we get $x = u_v x_v$ with $u_v \in G_{K_v}$; hence the lemma is proved and consequently theorem a a) is proved for the group under consideration. □

5.10 Skew hermitian forms over quaternion division algebras

Write $G = \mathrm{Spin}_n(D/K, h)$ where D is a quaternion division algebra and h is a skew-hermitian form. If $n = 2$ or 3, G is isomorphic to a group of type $A_1 \times A_1$ or A_3 and the theorem is proved for these types. Hence we can assume $n \geq 4$. We can then carry out the procedure adopted for spin groups of quadratic forms almost word for word; for this we need to know the analogue of Witt's theorem, i.e. Given two anisotropic vectors x and y of the same length meaning $h(x) = h(y)$ there exists a proper unitary matrix t transforming x into y; this we proved in § 2.6, lemma 2.

We also need to know the Minkowski- Hasse's theorem for skewher- **128**
mitian forms. This we shall state and prove as a proposition.

Proposition. *Let D be a quaternion division algebra over K; let h be a skew hermitian form in $n \geq 2$ variables over D; let c be a nonzero skew quaternion of D; then is the equation $h'(x) = c$ has a solution locally at all places v of K then it has a global solution.*

Clearly the proof of this proposition will complete the proof of theorem a a) for G.

Proof of the Proposition. We shall first prove the proposition for $n = 2$ and 3. Let V' be the vector space on which h' is given. We shall construct a vector space V with a hermitian form h such that both V and V' have the same dimension and discriminants and such that $V = Wl(x_o)$ with $h(x_o) = c$. This is done as follows; first let $n = 2$. We shall find a skew quaternion b such that the reduced norm of $\begin{pmatrix} b & o \\ o & c \end{pmatrix}$ shall be equal to the discrimination d of V'; this is equivalent to requiring $bb^I = \dfrac{d}{cc^I}$. Expressing b in terms of a basis of D/K, bb^I becomes a ternary form over K. Hence we require the form bb^I to represent $\dfrac{d}{cc^I}$. By the Minkowski-Hasse's theorem for quadratic forms it is enough to check the local solvability of the equation $bb^I = \dfrac{d}{cc^I}$. Now suppose x'_v are the given solution of $h'(x) = c$ at the places v of K. If $D_v y_v$ denotes the orthogonal complements of x'_v in V'_{K_v}, then $h(y_v)H^{-1})^I = d/cc^I$. This proves the local
129 solvability of $bb^I = d/cc^I$. Hence as observed above it is also globally solvable with $b \in D$. Then $\begin{pmatrix} b & o \\ o & c \end{pmatrix}$ define a hermitian form h on a 2-dimensional vector space V/D; clearly h represents the skew quaternion c. If $n \geq 3$ we can carry out a similar procedure using lemma 4 of § 4.3. Let U_{n-1} denote the unitary group of (W, h). By construction (V, h) is isomorphic to (V', h') over $\bar{K}$. Let $f : V \to V'$ be this isomorphism. Then $a_s = f^{-1} \circ {}^s f$ is a 1-cocycle of $g_{\bar{K}/K}$ with values in $U_n(V)$, the unitary group of V. The discriminants of V and V' being equal by § 2.6 lemma 3 we know that (a_s) comes from $H^1(K, SU_n)$ so that we can assume $a_s \in SU_n$. Let $T = \left\{ x \in V \middle| h(x) = c \right\}, T' = \left\{ x \in V' \middle| h'(x) = c \right\}$ be spheres in V, V' respectively. Clearly T is got by twisting the sphere T with the 1-cocycle (a_s). Our problem is to show that $h'(x) = c$ has a global solution i.e. the sphere T' has a K-rational point. Now by lemma 2 of § 2.6 T is isomorphic over $\bar{K}$ to the homogeneous space SU_n/SU_{n-1}. Hence the sphere T' is isomorphic to the twisted homogeneous space ${}_a(SU_n/SU_{n-1})$. The problem therefore reduces to showing that the latter has a K-rational point. By § 1.5 proposition 1, this is equivalent to proving that the 1-cocycle a_s comes from SU_{n-1}. The lo-

cal solvability of $h'(X) = c$ implies that locally at all places the cocycle a_s comes from SU_{n-1}. Hence for the proof of the proposition we are reduce to proving the following: given $(a_s) \in H^1(K, SU_n)$ such that its image (b_s) in $H^1(K_v, SU_n)$, is contained in the image of $H^1(K_v, SU_{n-1}) \to H^1(K_v, SU_n)$ for all places v of K to show that (a_s) is in the image of $H^1(K, SU_{n-1}) \to H^1(K, SU_n)$. We shall prove this now. In the diagram **130**
below we write $H^1(SU_n)$ to mean both $H^1(K, SU_n)$ and $H^1(K_v, SU_n)$; let $1 \to Z_2 \to \mathrm{Spin}_n \to SU_n \to 1, 1 \to Z_2 \to \mathrm{Spin}_{n-1} \to SU_{n-1} \to 1$ be the covering maps. From these we get a commutative diagram

$$\begin{array}{ccc} H^1(SU_{n-1}) & \xrightarrow{g} & H^1(SU_n) \\ \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} \\ H^1(Z_2) & \xrightarrow{\text{identity}} & H^2(Z_2) \end{array}$$

By assumption $\delta_2(a_s) \in$ Image of δ_1 locally. We first consider the case $n = 2$. SU_1 is a torus with a quadratic splitting field (See § 3.1 Example 4). Spin_1 being a covering of SU_1 is again a torus with a quadratic splitting field. Clearly Spin_1 satisfies the condition of § 3.2 theorem 6 a), and so Hasse Principle for H^2 of Spin_1 is valid. Spin_1 being comutative the diagram above can be supplemented by the sequences

$$H^1(SU_1) \xrightarrow{\delta_1} H^2(Z_2) \xrightarrow{p} H^2(\mathrm{Spin}_1).$$

Since $\delta_2(a_s) \in$ image of δ_1 locally we have $p(\delta_2(a_s)) = \{1\}$ locally at all places of K. By the Hasse Principle quoted above we have $p(\delta(a_s)) = \{1\}$ in $H^2(K, \mathrm{Spin}_1)$. This clearly implies $\delta_2(a_s)$ is in the image of $H^1(K, SU_1)$ by the map δ_1. Next if $n = 3$ the group SU_2 being semisimple and connected the same conclusion holds by virtue of § 5.2 theorem 2. Hence in either case we can find $(b) \in H'(K, SU_{n-1})$ such that $\delta_1(b) = \delta_2(a)$. Twisting the whole situation by the cocycle b, we **131**
may assume $\delta_2(a) = 1$, i.e. that the cocycle a comes from a cocycle b of the spin group. Now $T' \cong {}_a(SU_n/SU_{n-1}) \cong_b (\mathrm{Spin}_n / \mathrm{Spin}_{n-1})$. Hence we are reduced to proving the following: given an element $b \in H^1(K, \mathrm{Spin}_n)$ which comes from Spin_{n-1} locally at all places of K, to show that b comes from Spin_{n-1}. We shall prove this now. We have a

commutative diagram

$$\begin{array}{ccc} H^1(K, \mathrm{Spin}_{n-1}) & \xrightarrow{g} & H^1(K, \mathrm{Spin}_n) \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ \prod_{v\in\infty} H^1(K_v, \mathrm{Spin}_{n-1}) & \xrightarrow{h} & \prod_{v\in\infty} H^1(K_v, \mathrm{Spin}_n) \end{array}$$

If $n = 2$, Spin_1 is an algebraic torus so that by § 3.2 theorem 6 b) corollary the map β is surjective. If $n = 3$, Spin_2 being connected and semisimple by theorem b) β is surjective again. For $n = 2, 3$, Spin_n is isomorphic to a group of type A_n so that by theorem a) applied to groups of this type, which we have already proved, we find that γ is injective. By assumption $\gamma(b) = h(c)$ for some $c \in \prod_{v\in\infty} h^1(K_v, \mathrm{Spin}_{n-1})$. By the surjectivity of β lift c to 1-cocycle d of Spin_{n-1}; then $\gamma(g(d)) = \gamma(b)$. Using the injectivity of γ we find $g(d) = b$, i.e. b comes from $H^1(K, \mathrm{Spin}_{n-1})$. This is what we wanted to prove. Hence the proposition is established for the cases $n = 2, 3$.

Next let us consider the case $n \geq 4$. Let x_v be the given local solution of $h'(x) = c$ for $v \in S$. Approximate the solutions $x_v, v \in \infty$ by a vector $x \in V$ and let W be a three dimensional regular subspace of V containing
132 x. If the approximation is good enough the restriction h'' of h' to W represent c locally for all $v \in \infty$. BY Lemma 4 of § 4.3 the same is true for $v \notin \infty$. By the case $n = 3$, h'' and therefore h' represents c globally.

Another proof of this proposition, due to T. Springer, is given in an appendix.

5.11 Applications

Classification of quadratic forms

Let $\mathscr{G}$ be a non-degenerate form over any field K. Then $H^1(K, O(\mathscr{G}))$ is isomorphic to the set of K-equivalent classes of quadratic forms over K. The exact sequence $1 \to SO \to O \to Z_2 \to 1$ where $O \to Z_2$ is the determinant map gives rise to an exact sequence of cohomology sets

$$O_K \to Z_2 \to H^1(K, SO) \to H^1(K, O) \to H^1(K, Z_2)$$

Since $O_K \to Z_2$ is surjective in view of the existence of reflections we see that the map $H^1(K, SO) \to H^1(K, O)$ has trivial kernel. By a familiar twisting argument we find that $H^1(K, SO) \to H^1(K, O)$ is injective.

The map $H^1(K, O) \to H^1(K, Z_2) \cong K^*/K^{*2}$ maps a class of quadratic forms onto the quotient of its discriminant by that of q (by an argument similar to the proof of lemma 3 in § 2.6). So $H^1(K, SO)$ is isomorphic to the set of K-classes of quadratic forms of fixed dimension n and discriminant d. Among these let $\mathscr{G}$ be one of maximal index and consider **133**
the exact sequence

$$1 \to Z_2 \to \text{Spin} \to SO \to 1.$$

We arrive at an exact sequence of cohomology sets,

$$\text{Spin}_K \to SO_K \to H^1(K, Z_2) \to H^1(K, \text{Spin}) \to H^1(K, SO) \to H^2(K, Z_2) \quad (2)$$

The map $SO_K \to H^1(Z_2) \cong K^*/K^{*2}$ is the spinor norm (*cf.* [E_3]). Using the exact sequences $1 \to Z_2 G_m \xrightarrow{\text{square}} G_m \to 1$ we get $1 \to H^2(K, Z_2) \to B_K \xrightarrow{\text{multiplication by 2}} B_K$ which is an exact sequence. Hence $H^2(K, Z_2)$ is isomorphic to the subgroup of elements of B_K which are of order 2. The map $H^1(K, SO) \to H^2(K, Z_2)$ is called the Hasse-Witt map (cf. [sp]). Hence we have found three invariants of a quadratic form $\mathscr{G}$ namely *i*) dimension of $\mathscr{G}$ *ii*) discriminant of $\mathscr{G}$ *iii*) the Hasse-Witt invariant.

We claim that over a $\mathscr{P}$-adic field K these invariants completely characterise a given K-equivalent class of quadratic form. This follows immediately from the result $H^1(K, \text{Spin}) = \{1\}$ of chapter 4, the exact sequences (2), and a twisting argument.

Quadratic forms over number fields.

We shall show the connection between theorem 1 and the ordinary Hasse principle for equivalence of quadratic forms. We shall assume first $n =$

$\dim \mathscr{G} \geq 3$, we have a comutative diagram with exact rows:

$$\begin{array}{ccccccc}
H^1(K,Z_2) & \longrightarrow & H^1(K,\mathrm{Spin}) & \xrightarrow{f} & H^1(K,SO) & \xrightarrow{f} & H^2(K,Z_2) \\
\downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\
\prod_{v\in\infty} H^1(K_v,Z_2) & \longrightarrow & \prod_{v\in\infty} H^1(K_v,\mathrm{Spin}) & \longrightarrow & \prod_{v} H^1(K_v,SO) & \longrightarrow & \prod_{v} H^2(K_v,Z_2)
\end{array}$$

134 We want to know if β is injective. By the splitting criterion for simple algebras (in fact quaternion algebras) the map λ is injective. By theorem a) the map α is injective. We claim that λ is surjective; this is because $H^1(K_v,Z_2) \cong K_v^*/K_v^{*2}$ and λ surjective means that we must be able to find an element of K with prescribed signs at the real places. This is clearly possible. Hence by lemma 1 of §5.1 the map β is injective.

Next using the exact sequences $1 \to SO \to O \xrightarrow{\det} Z_2 \to 1$ we get a commutative diagram.

$$\begin{array}{ccccccc}
1 & \longrightarrow & H^1(K,SO) & \longrightarrow & H^1(K,O) & \longrightarrow & H^1(K,Z_2) \\
\downarrow & & \downarrow{\scriptstyle\bar\beta} & & \downarrow{\scriptstyle\bar\alpha} & & \downarrow{\scriptstyle\bar\gamma} \\
1 & \longrightarrow & \prod_{v} H^1(K_v,SO) & \longrightarrow & \prod_{v} H^1(K_v,O) & \longrightarrow & \prod_{v} H^1(K_v,Z_2)
\end{array}$$

By what we showed above $\bar\beta$ is injective; by algebraic number theory if an element of K^* is a square at all places of K, then it is a square in K. This shows that $\bar\gamma$ is injective. Hence again by lemma 1 of §5.1 we see that $\bar\alpha$ is injective. This is what we wanted to prove. If V, V' are two quadratic spaces of dimension $n < 3$, which are isomorphic locally everywhere, let W be a $(3-n)$-dimensional space. Then $(V \perp W)_v \cong (V' \perp W)_v$ for all places v. By what we have just proved $V \perp W \cong V' \perp W$, and Witt's theorem implies $V \cong V'$

Skew-hermitian forms over a quaternion division algebra

If we try to carry over the above investigations to skew hermitian form
135 over quaternion division we find some differences. Let D be a quater-

nion division algebra over K, either a $\mathscr{P}$-adic field or a number field, h a skew-hermitian form over D, and U the unitary group of h. Then the norm mapping $U \to Z_2$ gives rise to the discriminant map $H^1(K,U) \to H^1(K,Z_2)$. Next the exact sequences $1 \to Z_2 \to \mathrm{Spin} \to SU \to 1$ gives rise to the cohomology sequence

$$\mathrm{Spin}_K \to SU_K \to H^1(K,Z_2) \to H^1(K,\mathrm{Spin}) \to H^1(K,SU) \to H^2(K,Z_2) \quad (4)$$

We proved in §2.6, lemma 1 a) that $SU_K = U_K$; using this in the exact sequence

$$(SU)_K \to U_K \to Z_2 \to H^1(K,SU) \to H^1(K,U) \to H^1(K,Z_2)$$

we find that $Z_2 \to H^1(K,SU)$ is injective; now let K be a $\mathscr{P}$-adic field. Then we saw in § 4.1 theorem 1 that $H^1(K,\mathrm{Spin}) = \{1\}$. Using this in (4) we find that there is an injection $H^1(K,SU) \to H^2(K,Z_2)$. But in this case we have seen $H^2(K,Z_2) \cong Z_2$. Hence we have $H^1(K,SU) \cong Z_2$. This shows that in (4) the discriminant mapping $H^1(K,U) \to H^1(K,Z_2) \cong K^*/K^{*2}$ has trivial kernel; by a twisting argument the discriminant map is injective. Hence a complete set of invariants are the dimension and discriminant ($cf.[J],[Ts]$).

In the case of number fields the injectivity of the map $H^1(K,SU) \to \prod_v H^1(K_v,SU)$ follows as in the case of quadratic forms but if we try to apply the argument leading to the proof of the Hasse Principle we find the following diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z_2 & \longrightarrow & H^1(K,SU) & \longrightarrow & H^1(K,U) & \longrightarrow & H^1(K,Z_2) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \prod_{v\in S} Z_2 & \longrightarrow & \prod_v H^1(K_v,SU) & \longrightarrow & \prod_v H^1(K_v,U) & \longrightarrow & \prod_v H^1(K_v,Z_2)
\end{array}$$

where S is the set of places v at which the quaternion division algebra D does not split. From this diagram it is not possible to prove the injectivity of $H^1(K,U) \to \prod_v H^1(K_v,U)$. In fact Hasse principle for skew-hermitian form is false. We shall prove this statement now. **136**

Let V be the n-dimensional vector space over D on which h is defined. We want to find the number of (V', h'), where V' is a n-dimensional vector space over D and h' a skew hermitian from over V' such that $(V, h) \cong (V', h')$ locally everywhere but not globally. We need a

Lemma. *Let $(V, h) \cong (V', h')$ locally everywhere; let W be any hyperplane in V, i.e. a subspace of dimension $n-1$; assume W to be non-degenerate. Then V' contains a subspace W' isometric to W.*

Proof. We shall apply induction on n; for $n = 1$ the result is trivial. So let $n > 2$; by induction assume the result for all spaces of dimension $\leq n-1$. Let $a \in W$ be a vector such that $h(a) \neq 0$; consider the equation $h'(x) = h(a)$. This is solvable locally at all places of K since $(V, h) \cong (V', h')$ locally everywhere. By the proposition of § 5.10 we know that the equation has a global solution; let $a \in V'$ be such that $h'(a') = h(a)$. Write $W = \mathrm{Da} \perp W_1, V = \mathrm{Da} \perp V_1$ and $V' = \mathrm{Da}' \perp$
137 V_1'; since $\mathrm{Da} \cong \mathrm{Da}'$ by construction and $V \cong V'$ locally everywhere by assumption, applying Witt's theorem we find that $V_1 \cong V_1'$ locally everywhere. Clearly $W_1 \subset V_1$, and is a non- degenerate hyperplane. Hence by induction assumption V_1' contains a subspace W_1' which is isometric to W_1. Then clearly $W' = \mathrm{Da} \perp W_1'$ is a subspace of V' isometric to W. This proves the lemma. □

In the notations above write $V = W \perp \bar{V}$, $V' = W' \perp \bar{V}^1$. By construction $W \cong W'$. Hence $V \cong V'$ locally everywhere if and only if $\bar{V} \cong \bar{V}'$ locally everywhere. This reduces the problem of finding the number of (V^1, h^1) which are isomorphic to (v, h) locally everywhere but not globally to the case of 1-dimensional spaces. So let us assume $\dim V = 1$. Then by § 3.1 Example 4 SU is a torus with a quadratic splitting field. Hence by § 3.2 theorem 6a) the Hasse principle is true in any dimension. We then have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z_2 & \longrightarrow & H^1(K, SU) & \xrightarrow{g} & H^1(K, U) & \longrightarrow & H^1(K, Z_2) \\
 & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle r} & & \downarrow \\
1 & \longrightarrow & \prod_{v \in S} Z_2 & \longrightarrow & \prod_v H^1(K_v, SU) & \longrightarrow & \prod_v H^1(K_v, U) & \longrightarrow & \prod_v H^1(K_v, Z_v)
\end{array}$$

Consider $\ker(\psi)$. Since p is injective any element of $\ker(\gamma)$ comes from $H^1(K, SU)$. Hence $\ker\gamma \cong \ker(\gamma g)/Z_2$ since $Z_2 \subset \ker(\gamma g)$; this implies $\ker\gamma \cong \ker(tq)/Z_2 \cong q^{-1}(u(\prod_{v\in S} Z_2))/Z_2$.

Let $X = \mathrm{Hom}(G_m, SU)$. Since SU is a sub torus of the multiplicative **138**
group of D, for any $v \in S$ the decomposition group g_{L_w}/K_v acts non-trivially on X. So we have $H^1(K_v, SU) \cong \hat{H}^{-1}(g_{L_w/K_v}, X) \cong Z_2$ and $u(\prod_{v\in S} Z_2) = \prod_{v\in S} H^1(K_v, SU)$. By § 2.2 we have the commutative diagram with exact bottom row

Here a and b are surjective since $g_{L/K}$ is cyclic, and $\hat{H}^{-1}(g_{L/K}, X) \cong Z_2$. So $\bar{q}$ is injective and the cardinality of $q^{-1}(\prod_{v\in S} \hat{H}^{-1}(g_{L_w/K_v}, X))$ is equal to the cardinality of $\prod_{v\in S} \hat{H}^{-1}(g_{L_w/K_v}, X)$ divided by that of its image under b, *i.e.* equal to 2^{s-1} if S contains s places. Hence $\ker(\gamma)$ has 2^{s-2} elements, *i.e.* there are exactly 2^{s-2} classes of skew hermitian quaternionic forms which are locally isomorphic but not globally. If $s > 2$ then there are skew hermitian quaternionic forms which are locally everywhere isomorphic but not globally.

$$
\begin{array}{ccccccccc}
 & & & & H^1(K, SU) & \longrightarrow & \oplus H^1(K_v, SU) & & \\
 & & & & \uparrow & & \uparrow & & \\
 & & & & H^1(g_{L/K}, X \otimes L^*) & & \oplus H^1(g_{L_w}/K_v, X \otimes L_w^*) & & \\
 & & & & \uparrow & & \uparrow & & \\
\oplus \hat{H}^{-2}(g_{L_w}/K_v, X) & \xrightarrow{a} & \hat{H}^{-2}(g_{L/K}, X) & \longrightarrow & \hat{H}^{-1}(g_{L/K}, X \otimes W) & \xrightarrow{\bar{q}} & \oplus_v \hat{H}^{-1}(g_{L_w}/K_v, X) & \xrightarrow{b} & \hat{H}^{-1}(g_{L/K}, X)
\end{array}
$$

Appendix by T.A. Springer

Hasse's theorem for skew-hermitian forms over quaternion algebras

139

Theorem 5.3.3 below is equivalent to the proposition of §5.10. The following proof was obtained in 1962. It differs from the proof given in the lecture notes in that it uses besides algebraic and local results, only Hasse's theorem for quadratic forms.

1. Algebraic results

Let k be a field of characteristic not 2. Let D be a quaternion algebra with centre k. D is either a division algebra or is isomorphic to the matrix algebra $M_2(k)$. We denote by $\lambda \to \bar{\lambda}$ the standard involution in D, by $\bar{D}$ the set of all $\lambda \in D$ with $\lambda = -\bar{\lambda}$ and by $(D^*)^-$ the set of invertible elements in D^-. N is the quadratic norm form in D and $N(x, y) = N(x + y) - N(x) - N(y)$ the corresponding symmetric bilinear form. Let V be a left D-module which is free and of finite rank n. Let F be a skew-hermitian form on $V \times V$ with respect to the standard involution in D. So

$$F(x, y) = -\overline{F(y, x)}, \quad F(x, x) \in \bar{D} \quad (x, y \in V).$$

Take any basis $(v_i)_{1 \le i \le n}$ of V and consider the matrix $M = (F(v_i, v_j))_{1 \le i, j \le n}$ with entries in D. The reduced norm of M in the matrix algebra $M_n(D)$ is an element of k, whose class $\mod (k^*)^2$ is independent of the particular basis. F is called *non-degenerate* if M is non-singular. We assume henceforth F to be non-degenerate. Then the element of $k^*/(k^*)^2$ defined by the reduced norm of M is called the *discriminant* of **140**

F and is denoted by $\delta(F)$.

An element $x \in V$ is called *non-singular* if the submodule Dx of V is isomorphic to D. This is equivalent to the following: if we express x in terms of a suitable basis of V, then one of the components of x is invertible in D. We say that F *represents zero non-trivially* if $F(x, x) = 0$ for some non-singular x. One has the usual results about existence of orthogonal bases in V etc.

We next describe some algebraic constructions. Let $\lambda \in D$ be such that $K = k(\lambda)$ is a quadratic semi-simple subalgebra of D. Let $\mu \in D^*$ be such that $N(\lambda, 1) = N(\lambda, \mu) = 0$. Then any element ρ of D may be written in the form $\rho = \xi + \eta\mu$ with $\xi, \eta \in K$. We have $\overline{\rho} = \overline{\xi} - \eta\mu$ and $\rho\eta = \overline{\eta}\mu(\eta \in K)$

F and V being as before, we can then write

$$F(x, y) = G(x, y) + H(x, y)\mu, \tag{1}$$

where $G(x, y)$, $H(x, y) \in K$. It readily follows that H is a non-degenerate symmetric bilinear form on V, considered as a K-module and that $G(x, y) = -\overline{G(x, y)} = -H(x, \mu y)$. Define the discriminant class $d(H) \in K^*/(K^*)^2$ in the obvious way. Let φ be the homomorphism $k^*/(k^*)^2 \to K^*/(K^*)^2$ induced by the injection $k \to K$.

Lemma 5.1.1. $d(H) = \varphi(\delta(F))$.

Proof. Using an orthogonal basis of V with respect to F it follows that it suffices to prove this if $V = D$, in which case an easy computation establishes the assertion. □

141 Suppose now that $D = M_2(k)$. If $\lambda \in D$ we denote by λ_1 and λ_2 the upper and lower row vectors of the matrix λ. Identifying V with D^n, we may write $x \in V$ in the form $x = \binom{x_1}{x_2}$, where $x_i \in k^{2n}$. It is easily seen that if F is any non-degenerate skew-hermitian form on V, we have

$$F(x, x) = \begin{pmatrix} f(x_1, x_2) & -f(x_1, x_1) \\ \\ f(x_2, x_2) & -f(x_1, x_2) \end{pmatrix}, \tag{2}$$

where f is a symmetric bilinear form on k^{2n}, whose discriminant class is $\delta(F)$, so that f is non-degenerate.

Lemma 5.1.2. *F represents zero non-trivially if and only if f has Witt-index ≥ 2. If this is so, there exists x in D^n such that $F(x,x) = 0$ and that any given component of x is invertible in D.*

Proof. The first assertion is readily verified, using the relation (2) between F and f, □

Now suppose that the following holds: if $F(x,x) = o$, then the first component of $x \in D^n$ is 0. For f this means that there exists linearly independent vectors $a, b \in k^{2n}$ such that

$$f(x_1,a)f(x_2,b) - f(x_1,b)f(x_2,a) = 0, \tag{3}$$

whenever $f(x_1,x_2) = f(x_1,x_1) = f(x_2,x_2) = 0$.

If the index of f is at least 2 we can find for any two $x_1, x_2 \in k^{2n}$ which are isotropic with respect to f, $a\ y \in k^{2n}$ such that $f(y,y) =$ **142**
$f(x_1,y) = f(x_2,y) = 0$. This implies that (3) holds for *all* pairs of isotropic vectors x_1, x_2. Since the isotropic vectors of f span the whole of k^{2n}, it follows then that (3) holds for all $x_1, x_2 \in k^{2n}$, which contradicts the linear independence of a and b.

This establishes the second assertion.

2. Local fields

Assume now that k is a local field, i.e. complete for a non-archimedian valuation, with finite residue field. With the same notations as before, we then have the following result.

Lemma 5.2.1. *(a) If rank $V > 3$, then F represents 0 non-trivially;*

(b) If is a division algebra, the equivalence classes of non-degenerate F are characterised by their rank and $\delta(F)$;

(c) There is exactly one equivalence class of anisotropic forms of rank 3.

Proof. For the case of a division algebra D see [22]. If D is a matrix algebra, this follows from the known properties of quadratic forms over local fields, by using the relation (2) between F and f. □

Lemma 5.2.2. *If rank $F = 2$ then there exists $\alpha \in k^*$ with the following property: any non-singular $\lambda \in D^-$ with $N(\lambda) \notin \alpha(k^*)^2$ is represented by F.*

Proof. This follows from lemma 5.2.1, (*c*). □

We now assume D to be a matrix algebra. Let $\underline{o}$ be a maximal order in D.

143 **Lemma 5.2.3.** *If $\xi_1, \alpha_1\bar{\xi}_1 + \xi_2\alpha_2\bar{\xi}_2$ is a skew-hermitian form of rank 2 such that α_1 and α_2 are unite in $\underline{o}$ and that $N(\alpha_1)N(\alpha_2)$ is a square, then this form represents any non-singular $\lambda \in D^-$.*

Proof. $\underline{o}$ is isomorphic to the subring of $M_2(k)$ whose entries are integers of k. using the corresponding representation (2) of our skew-hermitian form, we see that f is now a quadratic form in 4 variables over k, with integral coefficients, whose discriminant is the square of a unit of k. Such a form is known to have index 2 (see [12] §9). Lemma 2 implies that F represents 0 non-trivially. It then represents all elements of D^- (this is proved as in the division algebra case). □

3. Global fields

Now let k be a global field of characteristic not 2, i.e. an algebraic number field or a field of algebraic functions of dimension 1, with a finite field of constants. Let D be a quaternion division algebra with centre k. For any place v of k we denote by D_v the algebra $D \otimes_k k_v$ over the completion k_v. D_v is a division algebra for a finite number of places v, by the quadratic reciprocity law this number is even.

Let V and F be as in nr. 1. We put $V_v = V \otimes_k k_v$, this is a free D_v-module. F_v denotes the skew-hermitian form on V_v defined by F.

Lemma 5.3.1. *Suppose that rank $F = 2$ and $\delta(F) = 1$. There exists a finite set S of places of k such that for any $v \in S$ and any $\lambda \in D^-$ the equation $F_v(x, x) = \lambda$ is solvable with $x \in V_v$.*

144 *Proof.* Let $F(x, x) = \xi_1\alpha_1\bar{\xi}_1 + \xi_2\alpha_2\bar{\xi}_2$. with respect to some basis of V. Let $\underline{o}$ be a maximal order in D and take for S the set places consisting of: all infinite places; the finite places for which α_1, α_2 are not units in the

maximal order $\underline{o}_v$ of k_v, defined by $\underline{o}$; those for which D_v is a division algebra . S is finite. By lemma 5.2.3 it satisfies our requirements. □

Proposition 5.3.2. *Let $\lambda \in (D^*)^-$. Suppose that for all places v there exists $x_v \in V_v$ such that $F_v(x_v, x_v) = \lambda$. Then there exists $x \in V$ and $\alpha \in k^*$ such that $F(x, x) = \alpha\lambda$.*

Proof. We put $K = k(\lambda)$. Writing F in the form (1), our assumptions imply that the quadratic form $H(x, x)$ represents 0 non-trivially in all completions of K. By Hasse's theorem for quadratic forms $H(x, x) = 0$ has a non-trivial solution x in the K-vector space V. This is equivalent to the assertion. □

We come now to the proof of Hasse's theorem for skew-hermitian quaternion forms.

Theorem 5.3.3. *Suppose that rank $F \geq 3$. If F_v represents zero non-trivially for all places v, then F represents zero non-trivially*

Proof. Let $n = \operatorname{rank} F$. We distinguish several cases. □

(i) $n = 3$. We first assert that under the assumptions of the theorem there exists $\lambda \in D^-$ such that $\delta(F) = N(\lambda)(k^*)^2$. Such a λ is a solution of a ternary equation $N(\lambda) = \alpha$. By Hasse's theorem for quadratic forms it suffices to verify that this equation is everywhere locally solvable. Solvability for the places v where D_v is a matrix algebra is clear (since N is then isotropic on D_v^-). If D_v is a division algebra, the assumption **145**
that F_v represents 0 non-trivially implies that F_v can be written, after a suitable choice of coordinates, in the form $\xi_1\alpha\bar{\xi}_1 - \xi_2\alpha\bar{\xi}_2 + \xi_3\beta\bar{\xi}_3$. It follows that $\delta(F(k_v^*)^2 = N(\beta)(k_v^*)^2$. Since $\beta \in D_v^-$, this implies the solvability for all places.

We fix such a $\lambda \in D^-$ and let $K = k(\lambda)$. Write F in the form (1). Our assumption imply that the Witt-index of the symmetric bilinear form H is ≥ 2 at all places v of K. Hence the index of H is ≥ 2. by Hasse's theorem. Also $-\lambda^2 = N(\lambda) \in \delta(F)$. by lemma 5.1.1 it follows that $d(H) = -(K^*)^2$. This combined with the fact that the index of H is at least 2 implies that the index of H equals 3, i.e. H is of maximal index.

Consider now V as a 6-dimensional vector space over $K.\mu$ being as in nr. 1, put $Tx = \mu x$. This is a semi-similarity of H (relative to the non-trivial k-automorphism of K) and $T^2x = \mu^2 x$. What we have to prove is that exists a non-trivial solution of

$$H(x, x) = H(Tx, x) = 0. \tag{4}$$

Take a three-dimensional subspace W of V, which is totally isotropic (for H). If $TW \cap W \neq (0)$, any non-zero x in this intersection satisfies (4). Assume now that $TW \cap W = (0)$. Then V is the direct sum of W and TW. Let H be the hermitian form on the 3-dimensional K-vector space W defined by

$$H_1(u, v) = \lambda H(u, Tu).$$

146 It then follows that the solvability of (4) is equivalent to the existence of $u, v \in W$, not both 0, such that

$$H_1(u, v) = H_1(u, v) + \mu^2 H_1(v, v) = 0. \tag{5}$$

Let $\rho \in k^*$ be an element in the discriminant class $d(H_1)$ of H_1. If

$$H_1(w, w) = -\rho\mu^2 \tag{6}$$

has a solution $w \in W$, then an orthogonal basis u, v of the orthogonal complement of w in W will give a solution of (5).

So it suffices to prove that (6) is solvable. Now the values $H_1(w, w)$ are those of a 6-dimensional quadratic form g over k, so that we can prove the solvability of (6) by using again Hasse's principle for quadratic forms. For finite places v a 6-dimensional form represents everything (since then the Witt-index is positive), so we have only to consider an infinite place v (hence we may take k to be a number field). If v is complex there is no problem. If v is a real place of k which splits in K, g_v is easily seen to be an indefinite quadratic form over k_v, which represents everything. So let v be a real place of K such that $K_v = K \otimes_k k_v$ is complex. If H_1 is indefinite (6) is solvable. If not, the solvability of (5) in W_v (which follows from the assumptions) implies that μ^2 is negative in k_v. Then $-\rho\mu^2$ is positive or negative in k_v if H_1 is positive or negative definite, hence can be represented by H_1. This settles the case $n = 3$.

147 (*ii*) $n \geq 4$. Take F in the form $\sum_{i=1}^{n} \xi_i \alpha_i \bar{\xi}_i$. We first prove a lemma.

Lemma 5.3.4. *Let v be a place of k.*

(a) There exists $\delta_v \in D_v^-$ such that the equations

$$\xi_1\alpha_1\bar{\xi_1} + \xi_2\alpha_2\bar{\xi_2} = \delta_v \qquad (7)$$
$$\sum_{i=3}^{n} \xi_i\alpha_i\bar{\xi_i} = -\delta_v$$

have a solution in $(D_v)^n$.

(b) The $\delta_v \in (D_v^*)^-$ for (7) is solvable form an open set in $(D_v^*)^-$.

Proof of the lemma.

(a) is a consequence of lemma 5.2.1 (a). to prove (b) one observes that solvability of (7) depends only on the coset modulo $(k^*)^2$ of $N(\delta_v)$ and that $(k^*)^2$ is open in k^*. By proposition 5.3.2 there exists $\lambda \in k^*$ such that

$$\sum_{i=2}^{n} \xi_i\alpha_i\bar{\xi_i} = \lambda\alpha_1$$

is solvable in D^{n-1}. It follows that we may take $\alpha_2 = \lambda\alpha_1$, so that in particular $N(\alpha_1)N(\alpha_2)$ is a square.

Now consider the global counterpart of (7)

$$\xi_1\alpha_1\bar{\xi_1} + \xi_2\alpha_2\bar{\xi_2} = \delta$$
$$\sum_{i=3}^{n} \xi_i\alpha_i\bar{\xi_i} = -\delta \qquad (8)$$

We wish to prove that there exists $\delta \in (D^*)^-$ such that (8) is solvable **148**
in D^n. This will prove the theorem.

Let S be a finite set of places of k with the property of lemma 5.3.1 for the skew-hermitian form $\xi_1\alpha_1\bar{\xi_1} + \xi_2\alpha_2\bar{\xi_2}$. For each $v \in S$ we let ξ_v be as in lemma 5.3.4 (a). We take $\xi_{iv} \in D_v$ such that

$$\sum_{i=3}^{n} \xi_{iv}\alpha_i\bar{\xi_{iv}} = -\delta_v \ (v \in S).$$

Approximate the ξ_{iv} simultaneously by $\xi_i \in D$ such that, putting

$$\delta = -\sum_{i=3}^{n} \xi_i \alpha_i \bar{\xi}_i,$$

we have $\delta \in (D^*)^-$ and that the equations (8) are solvable in D_v^n for $v \in S$. In particular, the first equation (8) is solvable in D_v^2 for $v \in S$. But by the choice of S, this equation in also solvable in D_v^2 for $v \in S$, so that by the case $n = 3$ of the theorem (using the second part of lemma 5.1.2) this equation has a solution in D^2. Then we have a solution of (8) since the second equation (8) is solvable by the construction of δ.

4. The case n = 2.

For $n = 2$ Hasse's principle for skew-hermitian quaternion forms is no longer true

Representing 0 by a skew-hermitian form rank 2 is tantamount (by the second part of lemma 5.1.2) to solving an equation for $\rho \in D$ of the form

$$\rho\lambda\bar{\rho} = \lambda'$$

149 with $\lambda, \lambda' \in (D^*)^-$.

Using proposition 5.3.2, we see that in investigating Hasse's principle we may assume that λ' is a scalar multiple of λ, so that we have to consider an equation

$$\rho\lambda\bar{\rho} = \tau\lambda \tag{9}$$

with $\lambda \in (D^*)^-$, $\in k^*$. We first investigate such an equation for an arbitrary D. Put $K = k(\lambda)$, let μ be as in nr. 1 (9) is then equivalent to

$$\varrho\lambda\bar{\varrho}^{-1} = N(\varrho)^{-1}\tau\lambda,$$

which implies that either $\varrho \in K$, $N(\varrho) = \tau$, or $\varrho \in K\mu$, $N(\varrho) = -N(\mu)^{-1}\tau$. One concludes from this that (9) is solvable if and only if one of the following equations is solvable in K

$$\begin{aligned} N_{K/k}(\varrho) &= \tau \\ N_{K/k}(\varrho) &= -N(\mu)^{-1}\tau. \end{aligned} \tag{10}$$

It is easily seen that D is a matrix algebra if and only if $-N(\mu) \in N_{K/k}(K^*)$. This implies that the two equations (10) are both solvable or not if D is a matrix algebra and are not both solvable if D is a division algebra. If k is a local field or the field or real numbers and D a division algebra, the fact that $k^*/N_{K/k}(K^*)$ has order 2 implies that precisely one of the equations (10) is solvable.

Form the previous remarks one deduces the following facts about **150**
the equation (10) for the case that D is a division algebra over a global field k. We denote by $(\alpha,\beta)_v$ the quadratic Hilbert symbol. Let S be the finite set of places such that D_v is a division algebra. Solvability of (9) in all D_v is equivalent to

$$(\tau,\lambda^2)_v = 1 \text{ for } v \notin S,$$

solvability of (9) in D is equivalent to:

$$\begin{aligned} \text{either} \quad & (\tau,\lambda^2)_v = 1 \text{ for all } v, \\ \text{or} \quad & (\tau,\mu^2\lambda^2)_v = 1 \text{ for all } v. \end{aligned}$$

From this it follows that the 1–dimensional skew-hermitian forms over D, which are equivalent to a given non-degenerate one at all places of k, form exactly 2^{s-2} equivalence classes (s denoting the number of places in S).

Bibliography

[1] A.A Albert, Structure of algebras, AMS Colloquium Publications, 1939, rev. ed. 1961. **151**

[2] N. Bourbaki, Elements de Mathematique, Algebre

[3] F. Bruhat et J. Tits, C.R. Ac. Sci. Paris 263(1966), 598 - 601, 766-768, 822-825, 867-869.

[4] C. Chevalley, The algebraic theory of spinors, New York 1954.

[5] C. Chevalley, Sur certains groupes simples, Tohoku Math. J. 7(1955), 14 - 66.

[6] C. Chevalley, Classification des groupes de Lie algebriques, Seminaire ENS, Par is 1956 - 1958.

[7] M. Demazure et A Grothendieck, Schemas en groupes, Seminaire IHES, Paris 1963 / 64.

[8] M. Deuring, Algebren, Ergebnisse der Mathematik, Springer Varlag 1935, 2. Aufl. 1968.

[9] J. Dieudonne, La geometrie des groupes classioues, Ergebnisse der Mathematik, Springer Varlag 1955, 2^e ed. 1963.

[10] M. Eichler, Uber die Idealklassenzahl hyperkomplexer Systeme, Math. Z 43(1938), 481 - 494.

[11] M. Eichler, Allgemeine kongruenzklasseneinteilungen der Ideale einfacher Algebren uber algebraischen Zahlkopern and ihro Z Reihen, J reine u. angew Math 179 (1938), 227-251.

[12] M. Eichler, Quadratische Formen and orthogonale Gruppen, Springer - Verlag 1952.

[13] G. Harder, Uber die Galoiskohmologie halbeinfacher Matrizengruppen, Math, Z 90(1965), 404-428; 92(1966), 396 - 415.

[14] N. Jacobson, Simple Lie algebras over a field of characteristic zero, Duke Math. J 4 (1938), 534 - 551.

152 [15] M. Kneser, Starke Apporoximation in algebraishen Gruppen, J. reine u. angew Math. 218(1965), 190-203.

[16] M. Kneser, Galois - Kohomologie halbeinfacher algebraischer Gruppen uber p - adischen Korpern, Math. Z. 88 (1965), 40- 47, 89(1965), 250 -272.

[17] W. Landherr, Liesche Rings vom Typus A uber einem algebraischen Zahlkorper and hermitesche Formen uber einem Schifkorper, Abh. Math. Sem. Hamburg 12 (1938) 200 - 241.

[18] J.-P. Serre, Corhomologie locaux,Paris, Hermann 1962.

[19] J.-P. Serre, Cohologie Galoisienne, Cours au College de France, 1962/63, ed, Springer - Varlag 1964.

[20] T.A. Springer, On the the equivalence of quadratic forms, Indag. Math. 21 (1959) 241-253.

[21] J. Tate, The cohomology groups of tori in finite Galois extensions of number fields, Nagoya Math. J. 27(1966) 709-719.

[22] T. Tsukamoto, On the local theory of quaternionic antihermitian forms, J, Math. Soc. Japan 13(1961), 387-400.

[23] A. Weil, The field of definition of a variety, Amer.J. Math. 78(1956) 509-524.

[24] A. Weil, Algebras with involutions and the classical gruops, J.Ind. Maht. Soc 24(1961) 589-623.