

Automorphism groups of finite dimensional simple algebras

By NIKOLAI L. GORDEEV and VLADIMIR L. POPOV*

Abstract

We show that if a field k contains sufficiently many elements (for instance, if k is infinite), and K is an algebraically closed field containing k , then every linear algebraic k -group over K is k -isomorphic to $\text{Aut}(A \otimes_k K)$, where A is a finite dimensional simple algebra over k .

1. Introduction

In this paper, ‘algebra’ over a field means ‘nonassociative algebra’, i.e., a vector space A over this field with multiplication given by a linear map $A \otimes A \rightarrow A$, $a_1 \otimes a_2 \mapsto a_1 a_2$, subject to no *a priori* conditions; cf. [Sc].

Fix a field k and an algebraically closed field extension K/k . Our point of view of algebraic groups is that of [Bor], [H], [Sp]; the underlying varieties of linear algebraic groups will be the affine algebraic varieties over K . As usual, algebraic group (resp., subgroup, homomorphism) defined over k is abbreviated to k -group (resp., k -subgroup, k -homomorphism). If E/F is a field extension and V is a vector space over F , we denote by V_E the vector space $V \otimes_F E$ over E .

Let A be a finite dimensional algebra over k and let V be its underlying vector space. The k -structure V on V_K defines the k -structure on the linear algebraic group $\text{GL}(V_K)$. As $\text{Aut}(A_K)$, the full automorphism group of A_K , is a closed subgroup of $\text{GL}(V_K)$, it has the structure of a linear algebraic group. If $\text{Aut}(A_K)$ is defined over k (that is always the case if k is perfect; cf. [Sp, 12.1.2]), then for each field extension F/k the full automorphism group $\text{Aut}(A_F)$ of F -algebra A_F is the group $\text{Aut}(A_K)(F)$ of F -rational points of the algebraic group $\text{Aut}(A_K)$.

*Both authors were supported in part by The Erwin Schrödinger International Institute for Mathematical Physics (Vienna, Austria).

Let \mathcal{A}_k be the class of linear algebraic k -groups $\text{Aut}(A_K)$ where A ranges over all finite dimensional simple algebras over k such that $\text{Aut}(A_K)$ is defined over k . It is well known that many important algebraic groups belong to \mathcal{A}_k : for instance, some finite simple groups (including the Monster) and simple algebraic groups appear in this fashion; cf. [Gr], [KMRT], [Sp], [SV]. Apart from the ‘classical’ cases, people studied the automorphism groups of ‘exotic’ simple algebras as well; cf. [Dix] and discussion and references in [Pop]. The new impetus stems from invariant theory: for $k = K$, $\text{char } k = 0$, in [Ilt] it was proved that if a finite dimensional simple algebra A over k is generated by s elements, then the field of rational $\text{Aut}(A)$ -invariant functions of $d \geq s$ elements of A is the field of fractions of the trace algebra (see [Pop] for a simplified proof). This yields close approximation to the analogue of classical invariant theory for some modules of nonclassical groups belonging to \mathcal{A}_k (for instance, for all simple E_8 -modules); cf. [Pop].

So \mathcal{A}_k is the important class. For $k = K$, $\text{char } k = 0$, it was asked in [K1] whether all groups in \mathcal{A}_k are reductive. In [Pop] this question was answered in the negative¹ and the general problem of finding a group theoretical characterization of \mathcal{A}_k was raised; in particular it was asked whether each finite group belongs to \mathcal{A}_k . Notice that each abstract group is realizable as the full automorphism group of a (not necessarily finite) field extension E/F , and each finite abstract group is realizable as the full automorphism group of a finite (not necessarily Galois) field extension F/\mathbb{Q} , cf. [DG], [F], [Ge].

In this paper we give the complete solution to the formulated problem. Our main result is the following.

THEOREM 1. *If k is a field containing sufficiently many elements (for instance, if k is infinite), then for each linear algebraic k -group G there is a finite dimensional simple algebra A over k such that the algebraic group $\text{Aut}(A_K)$ is defined over k and k -isomorphic to G .*

The constructions used in the proof of Theorem 1 yield a precise numerical form of the condition ‘sufficiently many’. Moreover, actually we show that the algebra A in Theorem 1 can be chosen absolutely simple (i.e., A_F is simple for each field extension F/k).

From Theorem 1 one immediately deduces the following corollaries.

¹ It was then asked in [K2] whether, for a simple algebra A , the group $\text{Aut}(A)$ is reductive if the trace form $(x, y) \mapsto \text{tr } L_x L_y$ is nondegenerate (here and below L_a and R_a denote the operators of left and right multiplications of A by a). The answer to this question is negative as well: one can verify that for some of the simple algebras with nonreductive automorphism group constructed in [Pop] all four trace forms $(x, y) \mapsto \text{tr } L_x L_y$, $(x, y) \mapsto \text{tr } R_x R_y$, $(x, y) \mapsto \text{tr } L_x R_y$ and $(x, y) \mapsto \text{tr } R_x L_y$ are nondegenerate (explicitly, in the notation of [Pop, (5.18)], this holds if and only if $\alpha_1 \neq 0$).

COROLLARY 1. *Under the same condition on k , for each linear algebraic k -group G there is a finite dimensional simple algebra A over k such that $G(F)$ is isomorphic to $\text{Aut}(A_F)$ for each field extension F/k .*

COROLLARY 2. *Let G be a finite abstract group. Under the same condition on k , there is a finite dimensional simple algebra A over k such that $\text{Aut}(A_F)$ is isomorphic to G for each field extension F/k .*

One can show (see Section 7) that each linear algebraic k -group can be realized as the stabilizer of a k -rational element of an algebraic $\text{GL}(V_K)$ -module M defined over k for some finite dimensional vector space V over k . Theorem 1 implies that such M can be found among modules of the very special type:

THEOREM 2. *If k is a field containing sufficiently many elements (for instance, if k is infinite), then for each linear algebraic k -group G there is a finite dimensional vector space V over k such that the $\text{GL}(V_K)$ -stabilizer of some k -rational tensor in $V_K^* \otimes V_K^* \otimes V_K$ is defined over k and k -isomorphic to G .*

Regarding Theorem 2 it is worthwhile to notice that $\text{GL}(V_K)$ -stabilizers of points of some dense open subset of $V_K^* \otimes V_K^* \otimes V_K$ are trivial; cf. [Pop].

Another application pertains to the notion of essential dimension. Let $k = K$ and let A be a finite dimensional algebra over k . If F is a field of algebraic functions over k , and A' is an F/k -form of A (i.e., A' is an algebra over F such that for some field extension E/F the algebras A_E and A'_E are isomorphic), put

$$\zeta(A') := \min_{F_0} \{\text{trdeg}_k F_0 \mid A' \text{ is defined over the subfield } F_0 \text{ of } F \text{ containing } k\}.$$

Define the *essential dimension* $\text{ed } A$ of algebra A by

$$\text{ed } A := \max_F \max_{A'} \zeta(A').$$

On the other hand, there is the notion of essential dimension for algebraic groups introduced and studied (for $\text{char } k = 0$) in [Re]. The results in [Re] show that the essential dimension of $\text{Aut}(A_K)$ coincides with $\text{ed } A$ and demonstrate how this fact can be used for finding bounds of essential dimensions of some linear algebraic groups. The other side of this topic is that many (Galois) cohomological invariants of algebraic groups are defined via realizations of groups as the automorphism groups of some finite dimensional algebras, cf. [Se], [KMRT], [SV]. These invariants are the means for finding bounds of essential dimensions of algebraic groups as well; cf. [Re]. Theorem 1 implies that the essential dimension of *each* linear algebraic group is equal to $\text{ed } A$ for some simple algebra A over k .

Also, by [Se, Ch. III, 1.1], Theorem 1 reduces finding Galois cohomology of *each* algebraic group to describing forms of the corresponding simple algebra.

Finally, there is the application of our results to invariant theory as explained above. For the normalizers G of linear subspaces in some modules of unimodular groups our proof of Theorem 1 is constructive, i.e., we explicitly construct the corresponding simple algebra A (we show that every algebraic group is realizable as such a normalizer but our proof of this fact is not constructive). Therefore for such G our proof yields constructive description of some G -modules that admit the close approximation to the analogue of classical invariant theory (in particular they admit constructive description of generators of the field of rational G -invariant functions). However for Corollary 2 of Theorem 1 we are able to give another, constructive proof (see Section 5).

Given all this we hope that our results may be the impetus to finding new interesting algebras, cohomological invariants, bounds for essential dimension, and modules that admit the close approximation to the analogue of classical invariant theory.

The paper is organized as follows. In Section 2 for a finite dimensional vector space U over k , we construct (assuming that k contains sufficiently many elements) some algebras whose full automorphism groups are $\mathrm{SL}(U)$ -normalizers of certain linear subspaces in the tensor algebra of U . In Section 3 we show that the group of k -rational points of each linear algebraic k -group appears as such a normalizer. In Section 4 for each finite dimensional algebra over k , we construct a finite dimensional simple algebra over k with the same full automorphism group. In Section 5 the proofs of Theorems 1, 2 are given. In Section 6 we give the constructive proof of Corollary 2 of Theorem 1. Since the topic of realizability of groups as stabilizers and normalizers is crucial for this paper, for the sake of completeness we prove in the appendix (Section 7) several additional results in this direction.

In September 2001 the second author delivered a talk on the results of this paper at The Erwin Schrödinger International Institute (Vienna).

Acknowledgement. We are grateful to W. van der Kallen for useful correspondence and to the referee for remarks.

Notation, terminology and conventions.

- $|X|$ is the number of elements in a finite set X .
- $\mathrm{Aut}(A)$ is the full automorphism group of an algebra A .
- $\mathrm{vect}(A)$ is the underlying vector space of an algebra A .
- $K[X]$ is the algebra of regular function of an algebraic variety X .
- \mathfrak{S}_n is the symmetric group of the set $\{1, \dots, n\}$.

- $\langle S \rangle$ is the linear span of a subset S of a vector space.

• Let $V_i, i \in I$, be the vector spaces over a field. When we consider V_j as the linear subspace of $\bigoplus_{i \in I} V_i$, we mean that V_j is replaced with its copy given by the natural embedding $V_j \hookrightarrow \bigoplus_{i \in I} V_i$. We denote this copy also by V_j in order to avoid bulky notation; as the meaning is always clear from the contents, this does not lead to confusion.

• For a finite dimensional vector space V over a field F we denote by $T(V)$ (resp. $\text{Sym}(V)$) the tensor (resp. symmetric) algebra of V , and by $T(V)_+$ (resp. $\text{Sym}(V)_+$) its maximal homogeneous ideal with respect to the natural grading,

$$(1.1) \quad T(V)_+ := \bigoplus_{i \geq 1} V^{\otimes i}, \quad \text{Sym}(V)_+ := \bigoplus_{i \geq 1} \text{Sym}^i(V),$$

endowed with the natural $\text{GL}(V)$ -module structure:

$$(1.2) \quad g \cdot t_i := g^{\otimes i}(t_i), \quad g \cdot s_i := \text{Sym}^i(g)(s_i), \quad g \in \text{GL}(V), \quad t_i \in V^{\otimes i}, \quad s_i \in \text{Sym}^i(V).$$

The $\text{GL}(V)$ -actions on $T(V)$ and $\text{Sym}(V)$ defined by (1.2) are the faithful actions by algebra automorphisms. Therefore we may (and shall) identify $\text{GL}(V)$ with the corresponding subgroups of $\text{Aut}(T(V))$ and $\text{Aut}(\text{Sym}(V))$.

• For the finite dimensional vector spaces V and W over a field F , a nondegenerate bilinear pairing $\Delta : V \times W \rightarrow F$ and a linear operator $g \in \text{End}(V)$ we denote by $g^* \in \text{End}(W)$ the conjugate of g with respect to Δ .

• Δ_E denotes the bilinear pairing obtained from Δ by a field extension E/F .

• For a linear operator $t \in \text{End}(V)$ the eigenspace of t corresponding to the eigenvalue α is the nonzero linear subspace $\{v \in V \mid t(v) = \alpha v\}$.

- If a group G acts on a set X , and S is a subset of X , we put

$$(1.3) \quad G_S := \{g \in G \mid g(S) = S\};$$

this is a subgroup of G called the *normalizer of S in G* .

• ‘Ideal’ means ‘two-sided ideal’. ‘Simple algebra’ means algebra with a nonzero multiplication and without proper ideals. ‘Algebraic group’ means ‘linear algebraic group’. ‘Module’ means ‘algebraic (‘rational’ in terminology of [H], [Sp]) module’.

2. Some special algebras

Let F be a field. In this section we define and study some finite dimensional algebras over F to be used in the proof of our main result.

Algebra $A(V, S)$. Let V be a nonzero finite dimensional vector space over F . Fix an integer $r > 1$. Let S be a linear subspace of $V^{\otimes r}$, resp. $\text{Sym}^r(V)$. Then

$$(2.1) \quad I(S) := \begin{cases} S \oplus (\bigoplus_{i>r} V^{\otimes i}) & \text{if } S \subseteq V^{\otimes r}, \\ S \oplus (\bigoplus_{i>r} \text{Sym}^i(V)) & \text{if } S \subseteq \text{Sym}^r(V) \end{cases}$$

is the ideal of $T(V)_+$, resp. $\text{Sym}(V)_+$. By definition, $A(V, S)$ is the factor algebra modulo this ideal,

$$(2.2) \quad A(V, S) := A_+/I(S), \quad \text{where } A_+ := \begin{cases} T(V)_+ & \text{if } S \subseteq V^{\otimes r}, \\ \text{Sym}(V)_+ & \text{if } S \subseteq \text{Sym}^r(V). \end{cases}$$

It readily follows from the definition that $A(V, S)_E = A(V_E, S_E)$ for each field extension E/F .

By (1.1), (2.1), there is natural identification of graded vector spaces

$$(2.3) \quad \text{vect}(A(V, S)) = \begin{cases} (\bigoplus_{i=1}^{r-1} V^{\otimes i}) \oplus (V^{\otimes r}/S) & \text{if } S \subseteq V^{\otimes r}, \\ (\bigoplus_{i=1}^{r-1} \text{Sym}^i(V)) \oplus (\text{Sym}^r(V)/S) & \text{if } S \subseteq \text{Sym}^r(V). \end{cases}$$

Restriction of action (1.2) to $\text{GL}(V)_S$ yields a $\text{GL}(V)_S$ -action on A_+ . By (2.1), the ideal $I(S)$ is $\text{GL}(V)_S$ -stable. Hence (2.2) defines a $\text{GL}(V)_S$ -action on $A(V, S)$ by algebra automorphisms, and the canonical projection π of A_+ to $A(V, S)$ is $\text{GL}(V)_S$ -equivariant. The condition $r > 1$ implies that $V = V^{\otimes 1} = \text{Sym}^1(V)$ is a submodule of the $\text{GL}(V)_S$ -module $A(V, S)$. Hence $\text{GL}(V)_S$ acts on $A(V, S)$ faithfully, and we may (and shall) identify $\text{GL}(V)_S$ with the subgroup of $\text{Aut}(A(V, S))$.

PROPOSITION 1. $\{\sigma \in \text{Aut}(A(V, S)) \mid \sigma(V) = V\} = \text{GL}(V)_S$.

Proof. It readily follows from (1.1)–(2.2) that the right-hand side of this equality is contained in its left-hand side.

To prove the inverse inclusion, take an element $\sigma \in \text{Aut}(A(V, S))$ such that $\sigma(V) = V$. Put $g := \sigma|_V$. Consider g as the automorphism of A_+ defined by (1.2). We claim that the diagram

$$(2.4) \quad \begin{array}{ccc} A_+ & \xrightarrow{g} & A_+ \\ \pi \downarrow & & \downarrow \pi \\ A(V, S) & \xrightarrow{\sigma} & A(V, S) \end{array} ,$$

cf. (2.2), is commutative. To prove this, notice that as the algebra A_+ is generated by its homogeneous subspace V of degree 1 (see (2.3)), it suffices to check the equality $\sigma(\pi(x)) = \pi(g(x))$ only for $x \in V$. But in this case it is evident since $g(x) = \sigma(x) \in V$ and $\pi(y) = y$ for each $y \in V$.

Commutativity of (2.4) implies that $g \cdot \ker \pi = \ker \pi$. As $\ker \pi = I(S)$, formulas (2.1), (1.2), (1.3) imply that $g \in \text{GL}(V)_S$. Hence g can be considered as the automorphism of $A(V, S)$ defined by (2.2). Since its restriction to the subspace V of $A(V, S)$ coincides with that of σ , and V generates the algebra $A(V, S)$, this automorphism coincides with σ , whence $\sigma \in \text{GL}(V)_S$. \square

Algebra $B(U)$. Let U be a nonzero finite dimensional vector space over F , and $n := \dim U$.

The algebra $B(U)$ over F is defined as follows. Its underlying vector space is that of the exterior algebra of U ,

$$(2.5) \quad \text{vect}(B(U)) = \bigoplus_{i=1}^n \wedge^i U.$$

To define the multiplication in $B(U)$ fix a basis of each $\wedge^i U$, $i = 1, \dots, n$. For $i = n$, it consists of a single element b_0 . The (numbered) union of these bases is a basis $\mathcal{B}_{B(U)}$ of $\text{vect}(B(U))$. By definition, the multiplication in $B(U)$ is given by

$$(2.6) \quad pq = \begin{cases} p \wedge q, & \text{for } p, q \in \mathcal{B}_{B(U)}, \text{ and } p \text{ or } q \neq b_0, \\ b_0, & \text{for } p = q = b_0. \end{cases}$$

It is immediately seen that up to isomorphism $B(U)$ does not depend on the choice of $\mathcal{B}_{B(U)}$, and $B(U)_E = B(U_E)$ for each field extension E/F .

The $\text{GL}(U)$ -module structure on $T(U)$ given by (1.2) for $V = U$ induces the $\text{GL}(U)$ -module structure on $\text{vect}(B(U))$ given by

$$(2.7) \quad g \cdot x_i = (\wedge^i g)(x_i), \quad g \in \text{GL}(U), \quad x_i \in \wedge^i U.$$

In particular

$$(2.8) \quad g \cdot b_0 = (\det g)b_0, \quad g \in \text{GL}(U).$$

As $U = \wedge^1 U$ is the submodule of $\text{vect}(B(U))$, the $\text{GL}(U)$ -action on $\text{vect}(B(U))$ is faithful. Therefore we may (and shall) identify $\text{GL}(U)$ with the subgroup of $\text{GL}(\text{vect}(B(U)))$.

PROPOSITION 2. $\{\sigma \in \text{Aut}(B(U)) \mid \sigma(U) = U\} = \text{SL}(U)$.

Proof. First we show that the left-hand side of this equality is contained in its right-hand side. Take an element $\sigma \in \text{Aut}(B(U))$ such that $\sigma(U) = U$. By (2.5) and (2.6), the algebra $B(U)$ is generated by U . Together with (2.5), (2.6), (2.7), this shows that $\sigma(x) = \sigma|_U \cdot x$ for each element $x \in B(U)$. In particular, $\sigma(b_0) \in \wedge^n U$. As σ is an automorphism of the algebra $B(U)$, it follows from (2.6) that b_0 and $\sigma(b_0) \in \wedge^n U$ are the idempotents of this algebra. But $\dim \wedge^n U = 1$ readily implies that b_0 is the unique idempotent in $\wedge^n U$. Hence $\sigma|_U \cdot b_0 = b_0$. By (2.8), this gives $\sigma \in \text{SL}(U)$.

Next we show that the right-hand side of the equality under the proof is contained in its left-hand side. Take an element $g \in \mathrm{SL}(U)$ and the elements $p, q \in \mathcal{B}_{B(U)}$. We have to prove that

$$(2.9) \quad g \cdot (pq) = (g \cdot p)(g \cdot q).$$

Let, say, $p \neq b_0$. Then by (2.7) we have $g \cdot p = \sum_{b \in \mathcal{B}_{B(U)}} \alpha_b b$ for some $\alpha_b \in F$ where $\alpha_{b_0} = 0$. By (2.6) and (2.7), we have $g \cdot (pq) = g \cdot (p \wedge q) = (g \cdot p) \wedge (g \cdot q) = \sum_{b \in \mathcal{B}_{B(U)}} \alpha_b (b \wedge (g \cdot q)) = \sum_{b \in \mathcal{B}_{B(U)}} \alpha_b (b(g \cdot q)) = (\sum_{b \in \mathcal{B}_{B(U)}} \alpha_b b)(g \cdot q) = (g \cdot p)(g \cdot q)$. Thus (2.9) holds in this case. Then similar arguments show that (2.9) holds for $q \neq b_0$. Finally, from (2.6), (2.8) and $\det g = 1$ we obtain $g \cdot (b_0 b_0) = g \cdot b_0 = b_0 = b_0 b_0 = (g \cdot b_0)(g \cdot b_0)$. Thus (2.9) holds for $p = q = b_0$ as well. \square

Algebra $C(L, U, \gamma)$.

LEMMA 1. *Let A be an algebra over F with the left identity $e \in A$ such that $\mathrm{vect}(A) = \langle e \rangle \oplus A_1 \oplus \cdots \oplus A_r$, where A_i is the eigenspace with a nonzero eigenvalue α_i of the operator of right multiplication of A by e . Then*

- (i) *e is the unique left identity in A ;*
- (ii) *if $\sigma \in \mathrm{Aut}(A)$, then $\sigma(e) = e$ and $\sigma(A_i) = A_i$ for all i .*

Proof. (i) Let e' be a left identity of A . As $e' = \alpha e + a_1 + \cdots + a_r$ for some $\alpha \in F$, $a_i \in A_i$, we have $e = e' e = (\alpha e + a_1 + \cdots + a_r) e = \alpha e + \alpha_1 a_1 + \cdots + \alpha_r a_r$. Since $\alpha_i \neq 0$ for all i , this implies $\alpha = 1$ and $a_i = 0$ for all i , i.e., $e' = e$.

(ii) As $\sigma(A_i)$ is the eigenspace with the eigenvalue α_i of the operator of right multiplication of A by $\sigma(e)$, and $1 \neq \alpha_i \neq \alpha_j$ for all i and $j \neq i$ because of the definition of eigenspace (cf. Introduction), (ii) follows from (i). \square

Fix two nonzero finite dimensional vector spaces L and U over F . Put $s := \dim L$, $n := \dim U$ and assume that

$$(2.10) \quad |F| \geq \max\{n + 3, s + 1\}.$$

LEMMA 2. *There is a structure of F -algebra on L such that $\mathrm{Aut}(L_E) = \{\mathrm{id}_{L_E}\}$ for each field extension E/F .*

Proof. If $s = 1$, each nonzero multiplication on L gives the structure we are after. If $s > 1$, consider a basis e, e_1, \dots, e_{s-1} of L and fix any algebra structure on L satisfying the following conditions (by (2.10), this is possible):

- (L1) e is the left identity;
- (L2) each $\langle e_i \rangle$ is the eigenspace with a nonzero eigenvalue of the operator of right multiplication of L by e .
- (L3) $e_i^2 \in \langle e_i \rangle \setminus \{0\}$ for each i .

By Lemma 1, if $\sigma \in \text{Aut}(L_E)$, we have $\sigma(e) = e$ and $\sigma(\langle e_i \rangle_E) = \langle e_i \rangle_E$ for each i . Whence $\sigma = \text{id}_{L_E}$. □

Fix a sequence $\gamma = (\gamma_1, \dots, \gamma_{n+1}) \in F^{n+1}$, $\gamma_i \neq 0, 1$, $\gamma_i \neq \gamma_j$ for $i \neq j$; by (2.10), this is possible. Using Lemma 2, fix a structure of F -algebra on L such that $\text{Aut}(L_E) = \{\text{id}_{L_E}\}$ for each field extension E/F . We use the same notation L for this algebra.

The algebra $C(L, U, \gamma)$ is defined as follows. By definition, the direct sum of algebras L and $B(U)$ is the subalgebra of $C(L, U, \gamma)$, and there is an element $c \in C(L, U, \gamma)$ such that

$$(2.11) \quad \text{vect}(C(L, U, \gamma)) = \langle c \rangle \oplus \text{vect}(L \oplus B(U)) \stackrel{(2.5)}{=} \langle c \rangle \oplus \text{vect}(L) \oplus (\bigoplus_{i=1}^n \wedge^i U)$$

and the following conditions hold:

- (C1) c is the left identity of $C(L, U, \gamma)$;
- (C2) $\text{vect}(L)$ and $\wedge^i U$, $i = 1, \dots, n$, in (2.11) are respectively the eigenspaces with eigenvalues $\gamma_1, \dots, \gamma_{n+1}$ of the operator of right multiplication of $C(L, U, \gamma)$ by c .

It is immediately seen that $C(L, U, \gamma)_E = C(L_E, U_E, \gamma)$ for each field extension E/F .

Define the $\text{GL}(U)$ -module structure on $\text{vect}(C(L, U, \gamma))$ by the condition that in (2.11) the subspaces $\langle c \rangle$ and $\text{vect}(L)$ are trivial $\text{GL}(U)$ -submodules, and $\bigoplus_{i=1}^n \wedge^i U$ is the $\text{GL}(U)$ -submodule with $\text{GL}(U)$ -module structure defined by (2.7). Thus for all $g \in \text{GL}(U)$, $\alpha \in F$, $l \in L$, $x_i \in \wedge^i U$,

$$(2.12) \quad g \cdot (\alpha c + l + \sum_{i=1}^n x_i) = \alpha c + l + \sum_{i=1}^n (\wedge^i g)(x_i).$$

The $\text{GL}(U)$ -action on $\text{vect}(C(L, U, \gamma))$ given by (2.12) is faithful. Therefore we may (and shall) consider $\text{GL}(U)$ as the subgroup of $\text{GL}(\text{vect}(C(L, U, \gamma)))$.

PROPOSITION 3. $\text{Aut}(C(L, U, \gamma)) = \text{SL}(U)$.

Proof. The claim follows from the next two:

- (i) $\text{Aut}(C(L, U, \gamma)) \subset \text{GL}(U)$;
- (ii) $g \in \text{GL}(U)$ lies in $\text{Aut}(C(L, U, \gamma))$ if and only if $g \in \text{SL}(U)$.

To prove (i), take an element $\sigma \in \text{Aut}(C(L, U, \gamma))$. By (2.12), we have to show that all direct summands in the right-hand side of (2.11) are σ -stable, and $\sigma(x) = \sigma|_U \cdot x$ for all $x \in C(L, U, \gamma)$. The first statement follows from (C1), (C2) and Lemma 1. As L and $B(U)$ are the subalgebras of $C(L, U, \gamma)$, the second statement follows from the first, the condition $\text{Aut}(L) = \{\text{id}_L\}$, Lemma 1, Proposition 2 and formulas (2.7), (2.12).

To prove the ‘only if’ part of (ii), assume that $g \in \text{Aut}(C(L, U, \gamma))$. As by (i) and (2.12) the subalgebra $B(U)$ is g -stable, $g|_{B(U)}$ is a well-defined element of $\text{Aut}(B(U))$. By Proposition 2, this gives $g \in \text{SL}(U)$.

To prove the ‘if’ part of (ii) assume that $g \in \text{SL}(U)$. By (2.12) the subalgebra $L \oplus B(U)$ of $C(L, U, \gamma)$ is g -stable, and by Proposition 2 the transformation $g|_{L \oplus B(U)}$ is its automorphism. Hence it remains to show that if x is an element of some direct summand of the right-hand side of (2.11), then the following equalities hold:

$$g \cdot (cx) = (g \cdot c)(g \cdot x) \quad \text{and} \quad g \cdot (xc) = (g \cdot x)(g \cdot c).$$

By (2.12), $g \cdot c = c$. Together with (C1) this yields the first equality needed: $g \cdot (cx) = g \cdot x = c(g \cdot x) = (g \cdot c)(g \cdot x)$. By (C2), $xc = \alpha x$ for some $\alpha \in F$. Hence (C1), (C2) and (2.12) imply $(g \cdot x)c = \alpha(g \cdot x)$. This yields the second equality needed: $g \cdot (xc) = g \cdot (\alpha x) = \alpha(g \cdot x) = (g \cdot x)c = (g \cdot x)(g \cdot c)$. \square

Algebra $D(L, U, S, \gamma, \delta, \Phi)$. Let L and U be two nonzero finite dimensional vector spaces over F . Put $s := \dim L$, $n := \dim U$ and

$$(2.13) \quad V := L \oplus U.$$

Let $r > 1$ be an integer. Assume that

$$(2.14) \quad |F| \geq \max\{n + 3, s + 1, r + 3\}$$

and fix the following data:

- (i) a linear subspace S of $V^{\otimes r}$;
- (ii) two sequences $\gamma = (\gamma_1, \dots, \gamma_{n+1}) \in F^{n+1}$, $\delta = (\delta_1, \dots, \delta_m) \in F^m$, where $m = r + 1$ if $S \neq V^{\otimes r}$ and $m = r$ otherwise, and $\gamma_i, \delta_j \in F \setminus \{0, 1\}$, $\gamma_i \neq \gamma_j$, $\delta_i \neq \delta_j$ for $i \neq j$ (by (2.14), this is possible);
- (iii) a structure of F -algebra on L such that $\text{Aut}(L_E) = \{\text{id}_{L_E}\}$ for each field extension E/F (by (2.14) and Lemma 2, this is possible); we use the same notation L for this algebra.

Define the algebra $D(L, U, S, \gamma, \delta, \Phi)$ as follows. First, $A(V, S)$, $C(L, U, \gamma)$ are the subalgebras of $D(L, U, S, \gamma, \delta, \Phi)$ and the sum of their underlying vector spaces is direct. Thus $\text{vect}(D(L, U, S, \gamma, \delta, \Phi))$ contains two distinguished copies of V : the copy V_A corresponds to the summand $V^{\otimes 1}$ in (2.3), and the copy V_C to the summand $\text{vect}(L) \oplus \wedge^1 U$ in (2.11).

Denote by L_A, U_A , resp. L_C, U_C , the copies of resp. L, U (see (2.13)) in V_A , resp. V_C , and fix a nondegenerate bilinear pairing $\Phi : V_A \times V_C \rightarrow F$ such that L_A is orthogonal to U_C , and U_A to L_C ,

$$(2.15) \quad \Phi|_{L_A \times U_C} = 0, \quad \Phi|_{U_A \times L_C} = 0.$$

Second, there is an element $d \in D(L, U, S, \gamma, \delta, \Phi)$ such that

$$(2.16) \quad \text{vect}(D(L, U, S, \gamma, \delta, \Phi)) = \langle d \rangle \oplus \text{vect}(A(V, S)) \oplus \text{vect}(C(L, U, \gamma))$$

and the following conditions hold:

- (D1) d is the left identity of $D(L, U, S, \gamma, \delta, \Phi)$;
- (D2) $\text{vect}(C(L, U, \gamma))$ in (2.16) and all summands in decomposition (2.3) of the summand $\text{vect}(A(V, S))$ in (2.16) are the eigenspaces with eigenvalues $\delta_1, \dots, \delta_m$ of the operator of right multiplication of the algebra $D(L, U, S, \gamma, \delta, \Phi)$ by d ;
- (D3) if $x \in \text{vect}(A(V, S))$ and $y \in \text{vect}(C(L, U, \gamma))$ are the elements of some direct summands in the right-hand sides of (2.3) and (2.11) respectively, then their product in $D(L, U, S, \gamma, \delta, \Phi)$ is given by

$$(2.17) \quad xy = yx = \begin{cases} \Phi(x, y)d & \text{if } x \in V_A, y \in V_C, \\ 0 & \text{otherwise.} \end{cases}$$

It is immediately seen that for each field extension E/F

$$(2.18) \quad D(L, U, S, \gamma, \delta, \Phi)_E = D(L_E, U_E, S_E, \gamma, \delta, \Phi_E).$$

We identify $g \in \text{GL}(U)$ with $\text{id}_L \oplus g \in \text{GL}(V)$ and consider $\text{GL}(U)$ as the subgroup of $\text{GL}(V)$. Formulas (2.2), (1.2), (2.12) and (1.3) define the $\text{GL}(U)_S$ -module structures on $\text{vect}(A(V, S))$ and $\text{vect}(C(L, U, \gamma))$.

PROPOSITION 4. *With respect to decomposition (2.16) and the bilinear pairing Φ ,*

$$(2.19) \quad \text{Aut}(D(L, U, S, \gamma, \delta, \Phi)) = \{\text{id}_{\langle d \rangle} \oplus g \oplus (g^*)^{-1} \mid g \in \text{SL}(U)_S\}.$$

Proof. Take an element $\sigma \in \text{Aut}(D(L, U, S, \gamma, \delta, \Phi))$. Lemma 1 and conditions (D1), (D2) imply that $\sigma(d) = d$ and that the summands in (2.16) and (2.3) are σ -stable. From condition (D1) and Propositions 1, 3 we deduce that $\sigma = \text{id}_{\langle d \rangle} \oplus g \oplus h$ for some $g \in \text{GL}(V)_S$, $h \in \text{SL}(U)$.

Let $x \in V_A$, $y \in V_C$. Then $\sigma(x) = g \cdot x \in V_A$, $\sigma(y) = h \cdot y \in V_C$. So from (2.17) we obtain $\Phi(g \cdot x, h \cdot y)d = \sigma(x)\sigma(y) = \sigma(xy) = \sigma(\Phi(x, y)d) = \Phi(x, y)\sigma(d) = \Phi(x, y)d$. Hence

$$(2.20) \quad \Phi(g \cdot x, h \cdot y) = \Phi(x, y), \quad x \in V_A, y \in V_C.$$

As $h \cdot L = L$ and $h \cdot U = U$, it follows from (2.15), (2.20) and nondegeneracy of Φ that $g \cdot L = L$ and $g \cdot U = U$. Besides, (2.15) and nondegeneracy of Φ show that the pairings $\Phi|_{L_A \times L_C}$ and $\Phi|_{U_A \times U_C}$ are nondegenerate. Hence by (2.20)

$$(2.21) \quad h = (g^*)^{-1}, \quad g|_L = ((h|_L)^*)^{-1}, \quad g|_U = ((h|_U)^*)^{-1}.$$

As $h \in \text{SL}(U)$, we have $h|_L = \text{id}_L$ and $\det(h|_U) = 1$. By (2.21), this gives $g|_L = \text{id}_L$ and $\det(g|_U) = 1$, i.e., $g \in \text{SL}(U)$. Thus $g \in \text{SL}(U)_S$, i.e., the left-hand side of equality (2.19) is contained in its right-hand side.

To prove the inverse inclusion, take an element $\varepsilon = \text{id}_{\langle d \rangle} \oplus q \oplus (q^*)^{-1}$, where $q \in \text{SL}(U)_S$. We have to show that

$$(2.22) \quad \varepsilon(xy) = \varepsilon(x)\varepsilon(y), \quad x, y \in D(L, U, S, \gamma, \delta, \Phi).$$

By Proposition 1, we have $\varepsilon|_{A(V, S)} \in \text{Aut}(A(V, S))$. By (D1), this gives (2.22) for $x, y \in A(V, S)$.

As above, we have $(q^*)^{-1} \in \text{SL}(U)$. Hence $\varepsilon|_{C(L, U, \gamma)} \in \text{Aut}(C(L, U, \gamma))$ by Proposition 3. By (D1) this gives (2.22) for $x, y \in C(L, U, \gamma)$.

If $x = d$, then (2.22) follows from (D1) and the equality $\varepsilon(d) = d$. If $y = d$, then (2.22) follows from (D2) as $\varepsilon(C(L, U, \gamma)) = C(L, U, \gamma)$ and each summand in (2.3) is ε -stable.

Further, let x (resp., y) be an element of some direct summand of $A(V, S)$ in decomposition (2.3), and y (resp., x) be an element of some direct summand of $C(L, U, \gamma)$ in the right-hand side of (2.16). As these summands are ε -stable, (2.11) implies that $xy = yx = 0$ and $\varepsilon(x)\varepsilon(y) = \varepsilon(y)\varepsilon(x) = 0$, and hence (2.22) holds, unless $x \in V_A$ and $y \in V_C$ (resp., $x \in V_C$ and $y \in V_A$).

Finally, let $x \in V_A$, $y \in V_C$. Then $\varepsilon(x) = q \cdot x$, $\varepsilon(y) = (q^*)^{-1} \cdot y$, so by (2.17) we have $\varepsilon(xy) = \varepsilon(\Phi(x, y)d) = \Phi(x, y)\varepsilon(d) = \Phi(x, y)d = \Phi(x, q^*(q^*)^{-1} \cdot y)d = \Phi(q \cdot x, (q^*)^{-1} \cdot y)d = \varepsilon(x)\varepsilon(y)$. Hence (2.22) holds in this case. This and (2.17) show that (2.22) holds for $x \in V_C$, $y \in V_A$ as well. \square

COROLLARY. *Assume that $F = K$ and L, U, S, Φ are defined over k . If $\text{SL}(U)_S$ is the k -group, then $\text{Aut}(D(L, U, S, \gamma, \delta, \Phi))$ is the k -group k -isomorphic to $\text{SL}(U)_S$.*

Proof. As $\text{Aut}(D(L, U, S, \gamma, \delta, \Phi))$ is the image of the k -homomorphism of k -groups $\text{SL}(U)_S \rightarrow \text{GL}(\text{vect}(D(L, U, S, \gamma, \delta, \Phi)))$, $g \mapsto \text{id}_{\langle d \rangle} \oplus g \oplus (g^*)^{-1}$, it is the k -group as well; cf. [Sp, 2.2.5]. Considered as the k -homomorphism of k -groups $\text{SL}(U)_S \rightarrow \text{Aut}(D(L, U, S, \gamma, \delta, \Phi))$, this k -homomorphism is k -isomorphism since there is the inverse k -homomorphism $\text{id}_{\langle d \rangle} \oplus g \oplus (g^*)^{-1} \mapsto g$. \square

3. Normalizers of linear subspaces in some modules

In Section 2 we realized normalizers of linear subspaces in some modules of unimodular groups as the full automorphism groups of some algebras. Now we shall show that each group appears as such a normalizer.

PROPOSITION 5. *Let G be an algebraic k -group. There is a finite dimensional vector space U over K endowed with a k -structure, and an integer $b \geq 0$ such that the following holds. Let r be an integer, $r \geq b$, and L be a trivial finite dimensional $\text{SL}(U)$ -module defined over k , $\dim L \geq 2$. Then the $\text{SL}(U)$ -module $(L \oplus U)^{\otimes r}$ contains a linear subspace S defined over k such that $\text{SL}(U)_S$ is the k -subgroup of $\text{SL}(U)$ k -isomorphic to G .*

Proof. One may realize G as a closed k -subgroup of $\text{GL}_m(K)$ for some m , cf. [Sp, 2.3.7], and obviously $\text{GL}_m(K)$ may be realized as a closed k -subgroup of $\text{SL}_{m+1}(K)$. Therefore we may (and shall) consider G as a closed k -subgroup of $\text{SL}(U)$ for some finite dimensional vector space U over K endowed with a k -structure.

Consider the k -structure on $\text{End}(U)$ defined by the k -structure of U . Define the $\text{SL}(U)$ -module structure on $\text{End}(U)$ by left multiplications, $g \cdot h := g \circ h$, $g \in \text{SL}(U)$, $h \in \text{End}(U)$. The $\text{SL}(U)$ -module $\text{End}(U)$ is defined over k . The subvariety $\text{SL}(U)$ of $\text{End}(U)$ is closed, defined over k and $\text{SL}(U)$ -stable. The restriction to $\text{SL}(U)$ of the $\text{SL}(U)$ -action on $\text{End}(U)$ is the action by left translations.

These $\text{SL}(U)$ -actions endow the algebras $K[\text{SL}(U)]$ and $K[\text{End}(U)]$ with the structures of algebraic $\text{SL}(U)$ -modules defined over k . Restriction of functions yields the k -defined $\text{SL}(U)$ -equivariant epimorphism of algebras $K[\text{End}(U)] \rightarrow K[\text{SL}(U)]$, $f \mapsto f|_{\text{SL}(U)}$. Since the $\text{SL}(U)$ -module $\text{End}(U)$ is isomorphic over k to $U^{\oplus d}$, where $d := \dim U$, we deduce from here that there is a k -defined $\text{SL}(U)$ -equivariant epimorphism of algebras $K[U^{\oplus d}] \rightarrow K[\text{SL}(U)]$. In turn, as $K[U^{\oplus d}] = \text{Sym}((U^*)^{\oplus d})$, this and the definition of symmetric algebra yield that there is a k -defined $\text{SL}(U)$ -equivariant epimorphism of algebras

$$(3.1) \quad \alpha : \text{T}((U^*)^{\oplus d}) \rightarrow K[\text{SL}(U)].$$

The classical Chevalley argument, cf. [Sp, 5.5.1], shows that $K[\text{SL}(U)]$ contains a finite dimensional linear subspace W defined over k such that

$$(3.2) \quad \text{SL}(U)_W = G.$$

As W is finite dimensional and (3.1) is an epimorphism, there is an integer $h > 0$ such that

$$(3.3) \quad W \subseteq \alpha(\bigoplus_{i \leq h} ((U^*)^{\oplus d})^{\otimes i}).$$

Put $W' := \alpha^{-1}(W) \cap (\bigoplus_{i \leq h} ((U^*)^{\oplus d})^{\otimes i})$. Since $((U^*)^{\oplus d})^{\otimes i}$ is $\mathrm{SL}(U)$ -stable, (3.3) implies that

$$(3.4) \quad \mathrm{SL}(U)_{W'} = \mathrm{SL}(U)_W.$$

Because of $\dim L \geq 2$, one can find in L two linearly independent k -rational elements l_1 and l_2 . We claim that there is a k -defined injection of $\mathrm{SL}(U)$ -modules

$$(3.5) \quad \iota : \mathrm{T}((U^*)^{\oplus d}) \hookrightarrow \mathrm{T}(\langle l_1 \rangle \oplus U^*).$$

To prove this, let U_i^* be the i^{th} direct summand of $(U^*)^{\oplus d}$ considered as the linear subspace of $(U^*)^{\oplus d}$. Fix a basis $\{f_{ij} \mid j = 1, \dots, d\}$ of U_i^* consisting of k -rational elements. For any $i_1, j_1, \dots, i_t, j_t \in [1, d]$, $t = 1, 2, \dots$, define the element of $\mathrm{T}(\langle l_1 \rangle \oplus U^*)$ by

$$(3.6) \quad \iota(f_{i_1 j_1} \otimes \dots \otimes f_{i_t j_t}) := l_1^{\otimes i_1} \otimes f'_{i_1 j_1} \otimes \dots \otimes l_1^{\otimes i_t} \otimes f'_{i_t j_t},$$

where f'_{ij} is the image of f_{ij} under the natural isomorphism $U_i^* \rightarrow U^*$. Then one easily verifies that the linear mapping $\iota : \mathrm{T}((U^*)^{\oplus d}) \rightarrow \mathrm{T}(\langle l_1 \rangle \oplus U^*)$ defined on the basis $\{f_{i_1 j_1} \otimes \dots \otimes f_{i_t j_t}\}$ of $\mathrm{T}((U^*)^{\oplus d})_+$ by formula (3.6) and sending 1 to 1 has the properties we are after.

From existence of embedding (3.5) it follows that retaining the normalizer in $\mathrm{SL}(U)$ one can replace the subspace W' with another one, $W'' := \iota(W')$:

$$(3.7) \quad \mathrm{SL}(U)_{W''} = \mathrm{SL}(U)_{W'}.$$

Since W'' is finite dimensional, there is an integer $b \geq 0$ such that

$$(3.8) \quad W'' \subseteq \bigoplus_{i \leq b} (\langle l_1 \rangle \oplus U^*)^{\otimes i}.$$

Take an integer $r \geq b$ and consider the linear mapping

$$\iota_r : \bigoplus_{i \leq b} (\langle l_1 \rangle \oplus U^*)^{\otimes i} \rightarrow (L \oplus U^*)^{\otimes r}, \quad f_i \mapsto l_2^{\otimes (r-i)} \otimes f_i, \quad f_i \in (\langle l_1 \rangle \oplus U^*)^{\otimes i}.$$

It is immediately seen that ι_r is the injection of $\mathrm{SL}(U)$ -modules defined over k . From this and (3.8) we deduce that the normalizers in $\mathrm{SL}(U)$ of the subspaces W'' and $\iota_r(W'')$ coincide,

$$(3.9) \quad \mathrm{SL}(U)_{\iota_r(W'')} = \mathrm{SL}(U)_{W''}.$$

Now we take into account that there is a k -automorphism $\sigma \in \mathrm{Aut}(\mathrm{SL}(U))$ of order 2 such that the $\mathrm{SL}(U)$ -module U is isomorphic over k to the $\mathrm{SL}(U)$ -module with underlying vector space U^* and $\mathrm{SL}(U)$ -action defined by

$$(3.10) \quad g * f := \sigma(g)(f), \quad g \in \mathrm{SL}(U), f \in U^*$$

(fixing a k -rational basis in U and the dual basis in U^* , identify $\text{SL}(U)$ with $\text{SL}_d(K)$, and U, U^* with K^d ; then $\sigma(g) = (g^T)^{-1}$). Hence replacing the standard $\text{SL}(U)$ -action on $(L \oplus U^*)^{\otimes r}$ with the action defined by (3.10) (and trivial on L) we obtain the $\text{SL}(U)$ -module that is isomorphic to $(L \oplus U)^{\otimes r}$ over k . The normalizer in $\text{SL}(U)$ of the subspace $\iota_r(W'')$ of this module is the subgroup $\sigma(\text{SL}(U)_{\iota_r(W'')})$. Since it is k -isomorphic to $\text{SL}(U)_{\iota_r(W'')}$, the claim follows from (3.2), (3.4), (3.7) and (3.9). \square

4. Simple and nonsimple algebras

Let R be a finite dimensional algebra over a field F . Assume that $|F| \geq 4$ (however see the remark at the end of this section). Fix the following data:

- (a) two nonzero elements $\alpha, \zeta \in F, \alpha, \zeta \neq 1, \alpha \neq \zeta$,
- (b) an algebra Z over F of the same dimension as R and with zero multiplication,

$$(4.1) \quad z_1 z_2 = 0 \text{ for all } z_1, z_2 \in Z,$$

- (c) a nondegenerate bilinear pairing $\Delta : Z \times R \rightarrow F$.

In this section we construct a finite dimensional algebra $R(\alpha, \zeta, \Delta)$ over F such that the following properties hold:

$$(4.2) \quad \left\{ \begin{array}{l} \text{(i) } R(\alpha, \zeta, \Delta)_E = R_E(\alpha, \zeta, \Delta_E) \text{ for each field extension } E/F; \\ \text{(ii) } R(\alpha, \zeta, \Delta) \text{ is a simple algebra;} \\ \text{(iii) } R \text{ is the subalgebra of } R(\alpha, \zeta, \Delta); \\ \text{(iv) } \text{Aut}(R(\alpha, \zeta, \Delta)) \text{ stabilizes } R; \\ \text{(v) } \text{Aut}(R(\alpha, \zeta, \Delta)) \rightarrow \text{Aut}(R), \sigma \mapsto \sigma|_R, \text{ is the isomorphism;} \\ \text{(vi) if } F = k \text{ and } \text{Aut}(R_K) \text{ is the } k\text{-group, then } \text{Aut}(R(\alpha, \zeta, \Delta)_K) \\ \text{is the } k\text{-group and } \text{Aut}(R(\alpha, \zeta, \Delta)_K) \stackrel{(i)}{=} \text{Aut}(R_K(\alpha, \zeta, \Delta_K)) \rightarrow \\ \rightarrow \text{Aut}(R_K), \sigma \mapsto \sigma|_{R_K}, \text{ is the } k\text{-isomorphism.} \end{array} \right.$$

Remark. It follows from the properties (ii) and (i) that the F -algebra $R(\alpha, \zeta, \Delta)$ is absolutely simple, i.e., $R(\alpha, \zeta, \Delta)_E$ is simple for each field extension E/F .

By definition, R and Z are the subalgebras of $R(\alpha, \zeta, \Delta)$, the sum of their underlying vector spaces is direct, and there is an element $e \in R(\alpha, \zeta, \Delta)$ such that

$$(4.3) \quad \text{vect}(R(\alpha, \zeta, \Delta)) = \langle e \rangle \oplus \text{vect}(Z) \oplus \text{vect}(R)$$

and the following conditions hold:

(R1) e is the left identity of $R(\alpha, \zeta, \Delta)$;

(R2) $\text{vect}(Z)$ and $\text{vect}(R)$ in (4.3) are respectively the eigenspaces with eigenvalues ζ and α of the operator of right multiplication of $R(\alpha, \zeta, \Delta)$ by e ;

(R3) for all $a \in R$ and $z \in Z$, their products in $R(\alpha, \zeta, \Delta)$ are given by

$$(4.4) \quad az = 0, \quad za = \Delta(z, a)e.$$

Properties (4.2)(i) and (4.2)(iii) immediately follow from this definition. Let us show that (4.2)(ii) holds.

PROPOSITION 6. *The algebra $R(\alpha, \zeta, \Delta)$ is simple.*

Proof. Let I be a nonzero ideal of $R(\alpha, \zeta, \Delta)$. Take an element $x \in I$, $x \neq 0$. By (4.3) we have $x = \gamma e + x_Z + x_R$ for some $\gamma \in F$, $x_Z \in Z$, $x_R \in R$. From (R1), (R2) we deduce that

$$(4.5) \quad I \ni xe = \gamma ee + x_Z e + x_R e = \gamma e + \zeta x_Z + \alpha x_R.$$

Fix an element $z \in Z$, $z \neq 0$. As Δ is nondegenerate, there is an element $a \in R$ such that

$$(4.6) \quad \Delta(z, a) = 1.$$

As R and Z are the subalgebras of $R(\alpha, \zeta, \Delta)$, formulas (4.5), (4.1), (4.4) and condition (R1) imply that

$$(4.7) \quad I \ni (xe)z = \gamma ez + \zeta x_Z z + \alpha x_R z = \gamma z.$$

From (4.7), (4.4), (4.6) we deduce that

$$(4.8) \quad I \ni ((xe)z)a = \gamma za = \gamma e.$$

As I is the ideal, (4.8) and (R1) give $I = R(\alpha, \zeta, \Delta)$ whenever $\gamma \neq 0$.

Consider the remaining case where $\gamma = 0$, i.e., $x = x_Z + x_R$. As $x \neq 0$, either x_Z or $x_R \neq 0$. If $x_Z \neq 0$ (resp., $x_R \neq 0$), then by nondegeneracy of Δ there is $a' \in R$ (resp., $z' \in Z$) such that $\Delta(x_Z, a') = 1$ (resp., $\Delta(z', x_R) = 1$). Then since R and Z are the subalgebras of $R(\alpha, \zeta, \Delta)$, we deduce from (4.4), (4.1) that $I \ni xa' = x_Z a' + x_R a' = e + a''$ for some $a'' \in R$ (resp., $I \ni z'x = z'x_Z + z'x_R = e$). Thereby we have returned to the case $\gamma \neq 0$. \square

The following statement immediately implies (4.2)(iv) and (4.2)(v).

PROPOSITION 7. *With respect to decomposition (4.3) and the pairing Δ ,*

$$(4.9) \quad \text{Aut}(R(\alpha, \zeta, \Delta)) = \{\text{id}_{(e)} \oplus (g^*)^{-1} \oplus g \mid g \in \text{Aut}(R)\}.$$

Proof. As R and Z are the subalgebras of $R(\alpha, \zeta, \Delta)$, formula (4.3), Lemma 1 and conditions (R1), (R2) imply that each element $\sigma \in \text{Aut}(R)$ has the form $\text{id}_{\langle e \rangle} \oplus h \oplus g$, $h \in \text{GL}(Z)$, $g \in \text{Aut}(R)$. As in the proof of Proposition 4 we obtain $h = (g^*)^{-1}$. Thus the left-hand side of equality (4.9) is contained in its right-hand side.

To prove the inverse inclusion take an element $\varepsilon = \text{id}_{\langle e \rangle} \oplus (t^*)^{-1} \oplus t$, where $t \in \text{Aut}(R)$. We have to show that

$$(4.10) \quad \varepsilon(xy) = \varepsilon(x)\varepsilon(y), \quad x, y \in R(\alpha, \zeta, \Delta).$$

If $x, y \in Z$ or $x, y \in R$, then, since R and Z are the subalgebras of $R(\alpha, \zeta, \Delta)$, equality (4.10) follows from (4.1). If $x = e$ (resp., $y = e$), then (4.10) follows from (R1) (resp., (R2)). Further, (4.4) readily implies (4.10) for $x \in R$ and $y \in Z$. Finally, if $x \in Z$ and $y \in R$, then (4.10) follows from (4.4) by the arguments similar to those at the end of the proof of Proposition 4; the details are left to the reader. \square

COROLLARY. *Property (4.2)(vi) holds.*

Proof. Similar to that of the corollary of Proposition 4. \square

Remark. A slight modification of the arguments makes it possible to drop the condition $\zeta \neq 0$, and thereby to replace the condition $|F| \geq 4$ by $|F| \geq 3$. That is, put $\zeta = 0$ in the definition of $R(\alpha, \zeta, \Delta)$. Then Proposition 6 holds with the same proof. Proposition 7 holds as well but as $\zeta = 0$, Lemma 1 is not applicable, so the proof of Proposition 7 should be modified. This can be done as follows (with the same notation).

We have $\sigma(e) = \lambda e + e_Z + e_R$ for some $\lambda \in F$, $e_Z \in Z$, $e_R \in R$. As $\sigma(e)$ is the left identity, $e = \sigma(e)e = \lambda ee + e_Z e + e_R e = \lambda e + \alpha e_R$. Hence $\lambda = 1$, $e_R = 0$. If $e_Z \neq 0$, nondegeneracy of Δ implies that $\Delta(e_Z, a) = 1$ for some $a \in R$. Therefore $a = \sigma(e)a = (e + e_Z)a = a + \Delta(e_Z, a)e = a + e$ which is impossible as $e \neq 0$. Thus $\sigma(e) = e$. This and (R2) imply that $\sigma(Z) = Z$, $\sigma(R) = R$. The rest of the proof remains unchanged.

5. Proofs of theorems

Proof of Theorem 1. Let U , b , r , L and S be as in the formulation of Proposition 5. We may (and shall) assume that $r > 1$. The vector spaces U , L and S being defined over k , let U_0 , L_0 and S_0 be the corresponding k -structures. Put $s := \dim L$, $n := \dim U$.

Assume that the number of elements in k satisfies inequality (2.14) for $F = k$. Then we may (and shall) fix some γ , δ , Φ , α , ζ , Δ and consider the k -algebra $A := R(\alpha, \zeta, \Delta)$, where $R := D(L_0, U_0, S_0, \gamma, \delta, \Phi)$ (see Sections 2 and 4).

It follows from Proposition 5, Corollary of Proposition 4 and property (2.18) that $\text{Aut}(R_K)$ is the k -group k -isomorphic to G . Now the claim follows from Proposition 6 and Corollary of Proposition 7. \square

Proof of Theorem 2. By Theorem 1, there is a finite dimensional algebra A over k such that $\text{Aut}(A_K)$ is the k -group k -isomorphic to G . Put $V := \text{vect}(A)$. Then $V_K^* \otimes V_K^* \otimes V_K$ is the variety of all K -algebra structures (i.e., multiplications) on V_K (to $\sum f \otimes l \otimes v \in V_K^* \otimes V_K^* \otimes V_K$ corresponds the multiplication defined by $xy = \sum f(x)l(y)v$, $x, y \in V_K$). Two K -algebra structures correspond to isomorphic algebras if and only if their $\text{GL}(V_K)$ -orbits coincide. In particular the $\text{GL}(V_K)$ -stabilizer of a tensor $t \in V_K^* \otimes V_K^* \otimes V_K$ is the full automorphism group of the algebra corresponding to t , cf. [Se]. Therefore the tensor corresponding to multiplication in A is the one we are after. \square

6. Constructive proof of Corollary 2 of Theorem 1

Using the fact that regular representation of a finite abstract group G yields its faithful representation by permutation matrices, one immediately deduces Corollary 2 from Theorem 1. Since our proof of Theorem 1 is non-constructive, this proof of Corollary 2 is nonconstructive as well. Here we give another, constructive proof of this corollary. Combined with our proof of Theorem 2, it yields a constructive realization of G as the $\text{GL}(V_K)$ -stabilizer of a k -rational tensor in $V_K^* \otimes V_K^* \otimes V_K$ for some finite dimensional vector space V over k . Our constructive proof works if k contains sufficiently many elements (for instance, if k is infinite).

By Lemma 2, we may (and shall) assume that G is nontrivial. For an appropriate $n > 1$ fix an embedding $\iota : G \hookrightarrow \mathfrak{S}_n$ and identify G with the subgroup $\iota(G)$ of \mathfrak{S}_n . Let E_n be the n -dimensional split étale algebra over k , i.e., the direct sum of n copies of the field k . Put $V := \text{vect}(E_n)$ and denote by e_i the 1 of the i^{th} direct summand of E_n . Consider the natural action of \mathfrak{S}_n on E_n and V given by

$$(6.1) \quad \sigma \cdot e_i = e_{\sigma(i)}, \quad \sigma \in \mathfrak{S}_n, 1 \leq i \leq n.$$

As \mathfrak{S}_n acts faithfully, we may (and shall) identify \mathfrak{S}_n with the subgroup of $\text{GL}(V)$. Then it is easily seen that $\text{Aut}(E_n) = \mathfrak{S}_n$.

If k contains sufficiently many elements, one can find a sequence of nonzero elements $\boldsymbol{\lambda} := (\lambda_1, \dots, \lambda_n) \in k^n$ such that

$$(6.2) \quad \lambda_i/\lambda_j \neq \lambda_s/\lambda_t \text{ for all } 1 \leq i, j, s, t \leq n, i \neq j, s \neq t, (i, j) \neq (s, t).$$

Fix such a sequence.

PROPOSITION 8. Put $f := \prod_{\sigma \in G} \sigma \cdot (\lambda_1 e_1 + \cdots + \lambda_n e_n) \in \text{Sym}^{|G|}(V)$. Then $G = (\mathfrak{S}_n)_{\langle f \rangle}$.

Proof. The definition of f clearly implies that $G \subseteq (\mathfrak{S}_n)_{\langle f \rangle}$. To prove the inverse inclusion, take an element $\delta \in (\mathfrak{S}_n)_{\langle f \rangle}$. As $\lambda_1 e_1 + \cdots + \lambda_n e_n \in \text{Sym}(V)$ divides f , and $\delta \in \text{Aut}(\text{Sym}(V))$, we deduce that $\delta \cdot (\lambda_1 e_1 + \cdots + \lambda_n e_n)$ divides $\delta \cdot f$. As the algebra $\text{Sym}(V)$ is factorial and $\lambda_1 e_1 + \cdots + \lambda_n e_n$ is its prime element, this, plus the definition of f and the inclusion $\delta \cdot f \in \langle f \rangle$ yield

$$(6.3) \quad \delta \cdot (\lambda_1 e_1 + \cdots + \lambda_n e_n) = \alpha(\sigma \cdot (\lambda_1 e_1 + \cdots + \lambda_n e_n)) \quad \text{for some } \sigma \in G, \alpha \in k.$$

We claim that $\delta = \sigma$. If not, there are two indices i_0 and j_0 , $i_0 \neq j_0$, such that

$$(6.4) \quad \delta^{-1}(i_0) \neq \sigma^{-1}(i_0) \quad \text{and} \quad \delta^{-1}(j_0) \neq \sigma^{-1}(j_0).$$

From (6.3) and (6.1) we obtain $\lambda_{\delta^{-1}(i)} = \alpha \lambda_{\sigma^{-1}(i)}$ for each $i = 1, \dots, n$. Hence $\lambda_{\delta^{-1}(i_0)} / \lambda_{\delta^{-1}(j_0)} = \lambda_{\sigma^{-1}(i_0)} / \lambda_{\sigma^{-1}(j_0)}$. By (6.2), this implies $\delta^{-1}(i_0) = \sigma^{-1}(i_0)$, $\delta^{-1}(j_0) = \sigma^{-1}(j_0)$, contrary to (6.4). \square

Remark. It follows from the definition of f that $G \subseteq (\mathfrak{S}_n)_f$. Hence $(\mathfrak{S}_n)_f = (\mathfrak{S}_n)_{\langle f \rangle} = G$.

Assuming that k contains sufficiently many elements, fix a sequence $\boldsymbol{\mu} := (\mu_1, \dots, \mu_{|G|+1}) \in k^{|G|+1}$ where $\mu_i \in k \setminus \{0, 1\}$, $\mu_i \neq \mu_j$ for $i \neq j$, and define the algebra $E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})$ as follows.

Put $S := \langle f \rangle \subset \text{Sym}^{|G|}(V)$. First, $A(V, S)$ and E_n are the subalgebras of $E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})$ and the sum of their underlying vector spaces is direct. So $\text{vect}(E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu}))$ contains two distinguished copies of V : the copy V_A corresponds to the summand $\text{Sym}^1(V)$ in (2.3), and the copy V_E to the subalgebra E_n .

Let $(,) : V_A \times V_E \rightarrow k$ be the nondegenerate bilinear pairing defined by the condition

$$(6.5) \quad (e_i, e_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Second, there is an element $e \in E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})$ such that

$$(6.6) \quad \text{vect}(E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})) = \langle e \rangle \oplus \text{vect}(A(V, S)) \oplus \text{vect}(E_n)$$

and the following conditions hold:

(E1) e is the left identity of $E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})$;

(E2) $\text{vect}(E_n)$ in (6.6) and each summand in decomposition (2.3) of the summand $\text{vect}(A(V, S))$ in (6.6) are respectively the eigenspaces with eigenvalues $\mu_1, \dots, \mu_{|G|+1}$ of the operator of right multiplication of $E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})$ by e ;

(E3) if x is an element of a direct summand in (2.3), and $y \in V_E$, then

$$xy = yx = \begin{cases} (x, y)e & \text{if } x \in V_A, \\ 0 & \text{otherwise,} \end{cases}$$

It readily follows from the definition that for each field extension F/k we have

$$(6.7) \quad E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})_F = E(F, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu}).$$

PROPOSITION 9. *With respect to decomposition (6.6),*

$$(6.8) \quad \text{Aut}(E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})) = \{\text{id}_{\langle e \rangle} \oplus g \oplus g \mid g \in G\}.$$

Proof. Lemma 1, Proposition 1 and conditions (E2), (E3), (E1) yield that with respect to decomposition (6.6) each element of $\text{Aut}(E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu}))$ has the form $\text{id}_{\langle e \rangle} \oplus g \oplus h$ for some $g \in \text{GL}(V)_S$, $h \in \mathfrak{S}_n$. As in the proof of Proposition 4 we obtain $h = (g^*)^{-1}$. On the other hand, (6.1), (6.5) imply that

$$(6.9) \quad (\sigma^*)^{-1} = \sigma \text{ for each } \sigma \in \mathfrak{S}_n.$$

Now Proposition 8 and (6.9) yield that $g \in \text{GL}(V)_S \cap \mathfrak{S}_n = (\mathfrak{S}_n)_S = G$. Thus the left-hand side of equality (6.8) is contained in its right-hand side. The inverse inclusion is verified as at the end of proof of Proposition 4 (with (6.9) taken into account); we leave the details to the reader. \square

From (6.7) and (6.8) we immediately deduce the following.

COROLLARY 1. *The groups G and $\text{Aut}(E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})_F)$ are isomorphic for each field extension F/k .*

In turn, this implies the constructive proof of Corollary 2 of Theorem 1. Namely, assume that k contains sufficiently many elements, fix some $\boldsymbol{\lambda}, \boldsymbol{\mu}, \iota, \alpha, \zeta, \Delta$ and consider the k -algebra $A := R(\alpha, \zeta, \Delta)$ (see Section 4), where $R := E(k, G, \iota, \boldsymbol{\lambda}, \boldsymbol{\mu})$. Then properties (4.2)(i),(ii),(v) and Corollary 1 yield the following.

COROLLARY 2. *The finite dimensional k -algebra A is simple and $\text{Aut}(A_F)$ is isomorphic to G for each field extension F/k .*

7. Appendix

Realization of algebraic groups as normalizers and stabilizers is crucial for this paper: our proof of Theorem 1 is based on realization of algebraic groups as normalizers of some linear subspaces; Theorem 2 concerns realization of algebraic groups as stabilizers of some very specific tensors. This appendix contains further results on this topic. In particular it yields a refinement of Proposition 5.

PROPOSITION 10. *Let G be an algebraic k -group. There are an integer $n > 0$ and a closed k -embedding $G \hookrightarrow R := \mathrm{GL}(1, K) \times \mathrm{GL}(n, K)$ such that for each closed k -embedding of R in an algebraic k -group Q the group G is the stabilizer of a k -rational element of a finite dimensional Q -module defined over k .*

Proof. As G is algebraic, we may (and shall) consider it as a closed k -subgroup of $\mathrm{GL}(n, K)$ for some n . By Chevalley's theorem, cf. [H, 11.2, 34.1], [Sp, 5.5.3], there are a finite dimensional $\mathrm{GL}(n, K)$ -module U and a one-dimensional linear subspace S of U , both defined over k , such that $G = \mathrm{GL}(n, K)_S$. We have $g \cdot s = \chi(g)s$, $g \in G, s \in S$, for some character $\chi: G \rightarrow \mathrm{GL}(1, K)$ defined over k . Consider the reductive k -group $R := \mathrm{GL}(1, K) \times \mathrm{GL}(n, K)$ and define the R -module structure on U by $(\lambda, g) \cdot u := \lambda(g \cdot u)$, $\lambda \in \mathrm{GL}(1, K), g \in \mathrm{GL}(n, K), u \in U$. The R -module U is defined over k . For every $s \in S, s \neq 0$, we have $R_s = \{(\chi(g^{-1}), g) \mid g \in G\}$. Hence $G \rightarrow R, g \mapsto (\chi(g^{-1}), g)$, is the closed k -embedding whose image is R_s .

Let R be the closed k -subgroup of some Q . By Hilbert's theorem, cf. [MF], [PV], as R is reductive, the homogeneous space Q/R is affine. Hence R is an observable subgroup of Q , cf. [BHM]. As R_s is an R -stabilizer of a vector in an R -module, R_s is an observable k -subgroup of R ; cf. [BHM]. This implies that R_s is an observable k -subgroup of Q , which in turn implies existence of a finite dimensional Q -module M defined over k such that R_s is a stabilizer of a k -rational element of M ; cf. [BHM], [PV, 1.2, 3.7]. \square

The following statement was used in the first version of our proof of Theorem 1 found in the summer of 2001. Combined with Proposition 10, it yields that in Proposition 5 one may take $\dim S = 1$ and $\dim L \geq 1$. We believe that it is of interest in its own right and might be useful in other situations.

Fix a nonzero finite dimensional vector space U over K endowed with a k -structure U_0 .

PROPOSITION 11. *Let M be a finite dimensional $\mathrm{SL}(U)$ -module defined over k and let L be a nonzero trivial $\mathrm{SL}(U)$ -module defined over k . Then*

(i) $\mathrm{T}(U)_+$ contains a submodule defined over k and k -isomorphic to M ;

(ii) *there is an integer $b > 0$ such that $(L \oplus U)^{\otimes m}$ contains a submodule defined over k and k -isomorphic to M for each $m \geq b$.*

Proof. (i) Let \mathcal{M} be the class of finite dimensional submodules of $T(U)_+$.

Let u_1, \dots, u_n be a k -rational basis of U . For every $d = 1, \dots, n$ put $t_d := \sum_{\sigma \in \mathfrak{S}_d} \text{sgn}(\sigma) u_{\sigma(1)} \otimes \dots \otimes u_{\sigma(d)}$. This is a k -rational skew-symmetric element of $U^{\otimes d}$, fixed by $\text{SL}(U)$ for $d = n$. Hence for all $m, l > 0$ the module $U^{\otimes(m+ln)}$ contains the submodule $t_n^{\otimes l} \otimes U^{\otimes m}$ defined over k and isomorphic to $U^{\otimes m}$ over k . This implies that if $M_1, M_2 \in \mathcal{M}$ (resp., $M_1, M_2 \in \mathcal{M}$ and are defined over k), then $M_1 \oplus M_2$ and $M_1 \otimes M_2$ are isomorphic (resp., isomorphic over k) to the modules from \mathcal{M} (resp., defined over k). The class \mathcal{M} is also closed under taking submodules. In particular it is closed under taking direct summands. On the other hand, \mathcal{M} contains all ‘fundamental’ $\text{SL}(U)$ -modules: the d^{th} one is the minimal submodule of $T(U)_+$ containing t_d . If $\text{char } k = 0$, using complete reducibility and ‘highest weight theory’, we immediately deduce from these facts that every finite dimensional $\text{SL}(U)$ -module is isomorphic to a module from \mathcal{M} . We claim that this is true for $\text{char } k > 0$ as well. To prove this, and then to complete the proof of (i), we use the arguments communicated to us by W. van der Kallen, [vdK2]. We use the standard notation, [J].

The above arguments show that, for $p := \text{char } k > 0$, each tilting module is isomorphic to a module from \mathcal{M} (see the necessary information on tilting modules at the end of this section).

LEMMA 3 (Cf. [Don]). *For m sufficiently large, $M \otimes \text{St}_m \otimes \text{St}_m$ is tilting.*

Proof. As St_m is self-dual, it suffices to show that $M \otimes \text{St}_m \otimes \text{St}_m$ has good filtration for m large. In fact we will show that $M \otimes \text{St}_m$ has good filtration for m large. Take m so large that for each weight λ of M the weight $\lambda + (p^m - 1)\rho$ is dominant. Then $M \otimes (p^m - 1)\rho$ is what is called in [Pol] a module with excellent filtration for the Borel group B whose roots are negative; cf. [vdK1]. Indeed it has a filtration with each layer one-dimensional of dominant weight. Therefore, by Kempf vanishing, $M \otimes \text{St}_m = \text{ind}_B^G(M \otimes (p^m - 1)\rho)$ has good filtration. □

As $\text{St}_m \otimes \text{St}_m$ contains a trivial one-dimensional submodule, Lemma 3 shows that M can be embedded in a tilting module, whence the claim.

Now we take into account the field of definition k . According to what we proved, M is isomorphic to a submodule of some $N := \bigoplus_{i=1}^r U^{\otimes i}$. Let $M_0 \subset M$ be the k -structure of M . As $N_0 := \bigoplus_{i=1}^r U_0^{\otimes i}$ is the k -structure of N , $\text{Hom}_{\text{SL}(U_0)}(M_0, N_0)$ is the k -structure of $\text{Hom}_{\text{SL}(U)}(M, N)$; cf. [J, I, 2.10(7)]. So there are $h_i \in \text{Hom}_{\text{SL}(U_0)}(M_0, N_0)$ and $\lambda_i \in K$, $i = 1, \dots, m$, such that $\sum_{i=1}^m \lambda_i (h_i \otimes 1) : M \rightarrow N$ is an injection of $\text{SL}(U)$ -modules. But this implies that $\bigoplus_{i=1}^m (h_i \otimes 1) : M \rightarrow N^{\oplus m}$ is the injection of $\text{SL}(U)$ -modules

defined over k . Now we remark that, according to what is already proved, as N is a submodule of $T(U)_+$ defined over k , there is an injection $N^{\oplus m} \rightarrow T(U)_+$ defined over k . This completes the proof of (i).

(ii) As M is finite dimensional, by (i) there is an integer b such that M is isomorphic over k to a submodule of $\bigoplus_{i=1}^b U^{\otimes i}$ defined over k . Take a nonzero k -rational element $l \in L$. Then, for each i , $1 \leq i \leq b$, the $\mathrm{SL}(U)$ -module $U^{\otimes i}$ defined over k is isomorphic over k to the submodule $l^{\otimes(m-i)} \otimes U^{\otimes i}$ of $(L \oplus U)^{\otimes m}$ defined over k (here $l^{\otimes 0} \otimes U^{\otimes m}$ stands for $U^{\otimes m}$), whence the claim. \square

COROLLARY. *Let G be an algebraic k -group. Then there is a finite dimensional vector space U defined over k , a closed k -embedding $G \hookrightarrow \mathrm{SL}(U)$ and an integer $b > 0$ such that for each integer $m \geq b$ and nonzero trivial $\mathrm{SL}(U)$ -module L defined over k the group G is the $\mathrm{SL}(U)$ -stabilizer of a k -rational tensor in $(L \oplus U)^{\otimes m}$.*

Proof. As each algebraic k -group is a closed k -subgroup of $\mathrm{SL}(U)$ for some vector space U defined over k , the claim follows from Propositions 10 and 11. \square

Tilting modules. For the reader's convenience, we collect here the basic definitions and (nontrivial) facts about tilting modules used in the proof of Proposition 11; cf. [Don] and the references therein.

Let G be a reductive connected linear algebraic group, T a maximal torus and $B \supseteq T$ a Borel subgroup of G . Let $X = X(T)$ be the character group of T . We fix in X the system of simple roots of G which makes B the negative Borel. For $\lambda \in X$ we denote by K_λ the one-dimensional B -module on which T acts with weight λ . Let $\nabla(\lambda)$ be the induced G -module $\mathrm{Ind}_B^G(K_\lambda)$ (i.e., the G -module of global sections of the homogeneous line bundle over G/B with the fiber K_λ over B). Then $\nabla(\lambda)$ is finite dimensional and is nonzero if and only if λ belongs to the monoid X^+ of dominant weights; cf. [J].

An ascending filtration of a G -module is called *good* if each successive quotient is either zero or isomorphic to $\nabla(\lambda)$ for some $\lambda \in X^+$. Let \mathcal{T} be the class of finite dimensional G -modules V such that both V and its dual V^* have good filtration. Then one can prove the following.

(i) A direct sum and a tensor product of modules in \mathcal{T} belong to \mathcal{T} and also, a direct summand of a module in \mathcal{T} belongs to \mathcal{T} .

(ii) For each $\lambda \in X^+$ there is an indecomposable (into a direct sum) module $M(\lambda) \in \mathcal{T}$ which has unique highest weight λ ; furthermore, λ occurs with multiplicity 1 as a weight of $M(\lambda)$, and the modules $M(\lambda)$, $\lambda \in X^+$, form a complete set of inequivalent indecomposable modules in \mathcal{T} ; cf. [Don].

The module $M(\lambda)$ ($\lambda \in X^+$) is called the *tilting* module of highest weight λ .

RUSSIAN STATE PEDAGOGICAL UNIVERSITY, ST. PETERSBURG, RUSSIA

E-mail address: nickgordeev@mail.ru

STEKLOV MATHEMATICAL INSTITUTE, RUSSIAN ACADEMY OF SCIENCES, MOSCOW, RUSSIA

E-mail address: popovvl@orc.ru

REFERENCES

- [BHM] A. BIALYNIKI-BIRULA, G. HOCHSHILD, and G. D. MOSTOW, Extensions of representations of algebraic linear groups, *Amer. J. Math.* (1963) **65**, 131–144.
- [Bor] A. BOREL, *Linear Algebraic Groups*, 2nd ed., *Graduate Texts in Math.* **126**, Springer-Verlag, New York, 1991.
- [Don] S. DONKIN, On tilting modules for algebraic groups, *Math. Z.* **212** (1993), 39–60.
- [Dix] J. DIXMIER, Certaines algèbres non associatives simples définies par la trasvections du formes binaires, *J. fur die reine und angew. Math.* **346** (1984), 110–128.
- [DG] M. DUGAS and R. GÖBEL, Automorphism groups of fields, *Manuscripta Math.* **85** (1994), 227–242.
- [F] M. FRIED, A note on automorphism groups of algebraic number fields, *Proc. Amer. Math. Soc.* **80** (1980), 386–388.
- [Ge] W. D. GEYER, Jede endliche Gruppe ist Automorphismengruppe einer endlichen Erweiterung K/\mathbf{Q} , *Arch Math.* **41** (1983), 139–142.
- [Gr] R. L. GRIESS, JR., The friendly giant, *Invent. Math.* **69** (1982), 1–102.
- [H] J. E. HUMPHREYS, *Linear Algebraic Groups*, 3rd ed., *Graduate Texts in Math.* **21**, Springer-Verlag, New York, 1987.
- [Ilt] A. V. ILTYAKOV, Trace polynomials and invariant theory, *Geom. Dedicata* **58** (1995), 327–333.
- [J] J. C. JANTZEN, *Representations of Algebraic Groups, Pure and Applied Mathematics* **131**, Academic Press, Inc., Boston, 1987.
- [K1] V. KAC Some remarks on nilpotent orbits, *J. Algebra* **64** (1980), 190–213.
- [K2] ———, Letter of March 2, 2002.
- [KMRT] M.-A. KNUS, A. MERKURJEV, M. ROST, and J.-P. TIGNOL, *The Book of Involutions, Colloq. Publ. Amer. Math. Soc.* **44**, Providence, RI, 1998.
- [MFK] D. MUMFORD, J. FOGARTY, and F. KIRWAN, *Geometric Invariant Theory*, 3rd enl. ed., *Ergeb. Math. Grenzgeb.* **34**, Springer-Verlag, New York, 1994.
- [Pol] P. POLO, Variétés de Schubert et excellentes filtrations, in *Orbites Unipotentes et Representations. III*, *Astérisque* **173–174** (1989), 281–311.
- [Pop] V. L. POPOV, An analogue of M. Artin’s conjecture on invariants for non-associative algebras, *Amer. Math. Soc. Transl.* **169** (1995), 121–143.
- [PV] V. L. POPOV and E. B. VINBERG, Invariant theory, in *Algebraic Geometry IV, Encycl. Math. Sci.* **55**, 123–284, Springer-Verlag, New York, 1994.
- [Re] Z. REICHSTEIN, On the notion of essential dimension for algebraic groups, *Transformation Groups* **5** (2000), 265–304.
- [Sc] R. D. SCHAFER, *Introduction to Nonassociative Algebras*, Academic Press, New York, 1966.
- [Se] J.-P. SERRE, *Galois Cohomology*, Springer-Verlag, New York, 1997.
- [Sp] T. A. SPRINGER, *Linear Algebraic Groups*, Second Edition, *Progr. Math.* **9**, Birkhäuser, Boston, 1998.
- [SV] T. A. SPRINGER, and F. D. VELDKAMP *Octonians, Jordan Algebras and Exceptional Groups*, Springer-Verlag, New York, 2000.

- [vdK1] W. VAN DER KALLEN, *Lectures on Frobenius Splittings and B-Modules. Notes by S. P. Inamdar*, Published for the Tata Institute of Fundamental Research, Bombay, by Springer-Verlag, Berlin, 1993.
- [vdK2] W. VAN DER KALLEN, Letters of May 25 and August 2, 2001.

(Received February 15, 2002)