k-semisimple elements and pseudotori

Dissertation

zur Erlangung eines Doktorgrades in Mathematik
an der Fakultät für Mathematik der Universität Bielefeld

vorgelegt von

Name: Dietz Vorname: Christian

Geb. am: 10.07.1982 in: Schweinfurt

Erstprüfer: Werner Hoffmann

Bielefeld, den 11th February 2014

Hinweis: Gedruckt auf alterungsbeständigem Papier °° ISO 9706

Contents

Notation and prerequisites

In the whole work k is an infinite field of characteristic p where p is a prime number not equal to 2. We fix an algebraically closed field extension $\overline{k}$ of k. If K is said to be a field extension of k then it is a finite algebraical field extension with $k \subset K \subset \overline{k}$. In this context k_s will denote the separable closure of k.

Any algebra A will be associative, finite dimensional with 1. For $x \in A$ we will always denote the K-subalgebra that is generated by x by $K[x]$. Let B be a subset of A then we denote the centralizer of B in A by $Z_A(B)$ and $K[B]$ is the K-subalgebra of A that is generated by B. The center of A will be denoted by Z. Furthermore we will denote the maximal multiplicative group in A by $A^\times$. We denote the k-algebra of $n \times n$ matrices with entries in k by $M_n(k)$, and for $g \in M_n(k)$ we denote by g^t the transposed matrix. Finally, E will denote the neutral element in a group G.

There are different approaches to linear algebraic k-groups and thus it is necessary to say which one we are going to use in this work. We will follow the book [Spr09]. Consider the algebra of polynomials $\overline{k}[T_1, \ldots, T_n]$ and let I be an ideal in this algebra. Then a quotient algebra $B = \overline{k}[T_1, \ldots, T_n]/I$ that is reduced and of finite type is called an affine $\overline{k}$-algebra. A k-subalgebra B_k of B such that $\overline{k} \times_k B_k \to B$ is an isomorphism is called an affine k-algebra. The set of all affine k-algebras forms a category. Then the affine k-varieties are the dual category. If X is an affine k-variety then we will denote the corresponding affine k-algebra by $k[X]$.

If the affine variety G has the structure of a group and the multiplication and inversion are morphisms of varieties then G is called a linear algebraic group. Accordingly if the k-variety G has the structure of a group and multiplication and inversion are k-regular morphisms of varieties then G is called a linear algebraic k-group. By $G(k)$ we denote the set of k-rational points in G.

We will need the theory of elementary divisors and thus we want to give a short subsumption of this theory as far as we will need it. For a more detailed discussion and the proofs of the following see [Bou03] (chapter VII “Modules over principle ideal domains“).

Let V be some finitely generated free $k[T]$-module. By [Bou03] VII, §4.8, theorem 9 there exist finitely many prime elements P_i in $k[T]$ and positive natural numbers m_i and n_i such that only finitely many $m_i \neq 0$ and such that $V \cong \bigoplus_i (k[T]/(P_i^{n_i}))^{m_i} = \bigoplus_i V_i$. The ideals $P_i^{n_i}$ with $m_i \neq 0$ are called the elementary divisors.

Define

$$\mu(T) := \prod_i P_i^{n_i}.$$

In the case that V is some finitely generated free A-module for some k-algebra A and we endow V with the structure of a $k[T]$-module by $P(T)v = P(x)v$ for some $x \in A$ and $P(T) \in k[T]$ then $\mu(T)$ is the minimal polynomial of x. The decomposition of V into V_i is canonic and it is shown that $V_i = \{v \in V \mid P_i^{n_i}(x) = 0\}$.

1 Introduction

This work deals with a phenomenon that appears when concerning linear algebraic groups over fields with characteristic $p \neq 0$. In the theory of linear algebraic groups over perfect fields the Jordan decomposition is an important tool. But in the case of a field k that is not algebraically closed and of characteristic $p \neq 0$ there might exist k-rational elements in a linear algebraic group $G(k)$ that may not be decomposed in a direct commutative product of a unipotent and a semisimple k-rational element. A standard example for such an element that will accompany us through the whole work is the element

$$g_a = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & \cdots & 0 & 1 \\ a & & \cdots & 0 & 0 \end{pmatrix}$$

in the group $\mathrm{GL}_p(k)$ where k is a field of characteristic p that contains no p'th root of a.

One encounters this problem when trying to generalize the Arthur-Selberg trace formula that is just known for the case of a field of characteristic 0 to a field of characteristic p. This formula allows to compare some geometric and some spectral data of the right regular representation of a reductive linear algebraic group $G(\mathbb{A})$ on the space of cusp forms $L_0^2(G(F)\backslash G(\mathbb{A}))$ where F is some number field. One has a better understanding of the geometric side of the trace formula as we have an explicit expression of this side and we want to calculate some multiplicities that appear on the spectral side. As the formula is quite complicated and needs lots of prerequisites we don't want to give a complete introduction on the Arthur-Selberg trace formula but refer to [Gel96] or [Art05]. Instead we just want to take a look at the geometric side of the formula where the Jordan decomposition comes in place.

To give the geometric side some modified kernels $K_{\mathfrak{o}}^T(x,y)$ are needed which we don't want to explain closer. Then the coarse geometric side of the trace formula is given by

$$\sum_{\mathfrak{o}} \int_{Z(\mathbb{A})G(F)\backslash G(\mathbb{A})} K_{\mathfrak{o}}^T(x,x)dx.$$

The sum is taken over a set of equivalence classes and that is the crucial point. Here $\mathfrak{o}$ runs through equivalence classes in $G(F)$ with respect to the following relation (See [Art05] Part I: 10): Let γ_1 and γ_2 be in $Z(F)\backslash G(F)$. Then the Jordan decomposition is $\gamma_i = \gamma_i^s \gamma_i^u$ where γ_i^s is the semisimple component of γ_i and γ_i^u is the unipotent component. Then we say γ_1 is equivalent to γ_2 if and only if there exists some $g \in G(F)$ such that $g\gamma_1^s g^{-1} = \gamma_2^s$. Such a definition is not possible if the field of definition of the linear algebraic group G is not perfect. The fine geometric expansion also uses the Jordan decomposition as it is derived by decent to the centralizer of the semisimple component. Thus it is natural to look for a property that might replace semisimplicity in groups over non perfect fields. We will call such elements k-semisimple.

Another phenomenon that appears when dealing with non perfect fields k is that there are k-reductive groups that are not reductive. An example is the multiplication group of an inseparable extension of k considered as a k-group. Thus one wants to have a better understanding of k-reductivity and we will see that there is some relation between k-reductivity and k-semisimple elements.

Unlike semisimplicity, k-semisimplicity is not preserved under field extensions i.e. a k-semisimple element need not be K-semisimple for K an algebraic field extension of k. In chapter 1 we will start with a definition for k-semisimplicity of elements in k-algebras A. An important characterisation of such elements will be given in theorem 2.1 where we will see that the minimal polynomial of a k-semisimple element in $k[T]$ is always square free and that any A-module V becomes a semisimple $k[T]$-module if we let any $q(T) \in k[T]$ act by $q(x)$. Unfortunately for a k-semisimple element g the image of g under some k-rational representation (ρ, V) need not be k-semisimple in the endomorphism algebra of V and therefore it is not clear how to transfer the definition of k-semisimplicity from algebras to arbitrary linear algebraic groups. Thus we restrict to classical k-groups that are canonically embedded in some semisimple k-algebra with involution (A, ι). In this situation we will see in theorem 4.1 that for every element g in the classical k-group G there exists some k-semisimple element in the closure of its conjugacy class.

In section 4 we will introduce an analogue of tori, the k-pseudotori. The torus and the pseudotorus in a classical k-group are defined to be commutative, connected subgroups. While for a torus any element needs to be semisimple, for a k-pseudotorus it is enough that all k-rational elements are k-semisimple.

We will see that there exist pseudotori that are not tori and we will show the connection between pseudotori and k-reductivity (sometimes also called pseudo reductivity). That is:
A k-subgroup of G is a k-pseudotorus if and only if it is a connected, commutative k-reductive k-subgroup.
In chapter 5 we will recall the Weil restriction. This is a method to assign to every K-group G (or more generally to every K-variety X) some k-group $R_{K/k}(G)$ (resp. some k-variety $R_{K/k}(X)$) such that there exists some natural bijection between the k-rational points of $R_{K/k}(G)$ and the K-rational points in G. We will use the Weil restriction to show that the k-radical of any k-reductive classical k-group is a k-pseudotorus. We finish with the result that for any k-rational element g in a classical k-group G there exists some finite field extension K such that the unique k-rational element in $R_{K/k}(\mathrm{GL})$ that corresponds to g in G allows a decomposition into the product of some k-semisimple k-rational element and some unipotent k-rational element.

2 k-algebras

2.1 Semisimple elements of k-algebras

It is natural to give a definition of k-semisimple elements in the case of k-algebras first. To get an idea about the definition of k-semisimplicity take a look at the following example.

Example. Let A be the k-algebra $\mathrm{End}_k(k^p)$ and $a \in k$ where a has no p-th root in k. Consider the element

$$g_a = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & \cdots & 0 & 1 \\ a & & \cdots & 0 & 0 \end{pmatrix}.$$

This is the companion matrix to the polynomial $\mu_{g_a}(T) = T^p - a$ and thus this is also the minimal polynomial of this matrix. One should observe that $\mu_{g_a}(T)$ is square free in $k[T]$ but not in $K[T]$ for K any field extension of k that contains the p'th root of a. If we consider the field extension $K_u = k(u)$ where $u^p = a$, then

$$\mu_g(T) = T^p - a = T^p - u^p = (T - u)^p$$

and thus $\mu_{g_a}(T)$ is not square free in $K_u(T)$. We will frequently come back to this example and thus from now on g_a always denotes this element.

For a perfect field k the definition of semisimplicity of an element of an algebra is equivalent to the property that its minimal polynomial is square free. Observe that since k is perfect we know that, if the minimal polynomial of an element g is square free in $k[T]$ then it is also square free in $K[T]$ for any field extension of k. In fact this is an essential property i.e. an element g is semisimple in the k-algebra A if and only if it is semisimple in the K-algebra $K \otimes A$ for any field extension K of k.

If the field k is not perfect then the minimal polynomial of an element g in the k-algebra A might be square free in $k[T]$ but not in every field extension and thus it would not be semisimple. The element g_a is an example for this. Nevertheless it has some expedient properties. Later we will prove that for example the centralizer $Z_A(g_a)$ is simply the subalgebra that is generated by g_a. Furthermore, if we consider g_a to be an element of the endomorphism algebra of the k-vector space k^p then it acts as a semisimple endomorphism i.e. any subspace $U \subset V$ that is invariant under g_a has an invariant complement which is obvious since g_a acts irreducibly.

Although we would like to have a definition of k-semisimplicity for any linear algebraic group we start with a definition of k-semisimplicity in an algebra A to extend this to classical k-groups. For arbitrary linear algebraic groups we will at least give an idea for a possible definition.

Definition. Let A be a k-algebra. An element $x \in A$ is called k-semisimple if the k-subalgebra $k[x]$ that is generated by x is semisimple.(i.e. a direct sum of simple algebras)

We call such an element k-semisimple instead of semisimple to stress the dependence of this property of the field k. We already mentioned that g_a has some properties that are similar to those of semisimple elements and we want to show that this is true for any k-semisimple element. For example it will be essential for us to see that an element is k-semisimple if and only if its minimal polynomial is square free in $k[T]$. But first we have to do some preparations.
Let x be some element in A. We can define a homomorphism of k-algebras from $k[T]$ to A by

$$\sum_{i=0}^{m} \lambda_i T^i \mapsto \sum_{i=0}^{m} \lambda_i x^i. \tag{1}$$

Actually the image of this homomorphism is $k[x]$. The kernel of this homomorphism is an ideal in $k[T]$ and as $k[T]$ is a principle ideal domain the kernel is of the form $(\mu_x(T))$ for some uniquely determined monic polynomial $\mu_x(T)$. This polynomial is called the minimal polynomial of x.
Now let V be an arbitrary finitely generated A-module. Then with help of the homomorphism we just described we can endow V with the structure of a $k[T]$-module and it is obvious that the action of $k[T]$ on V factors through $k[T]/(\mu_x(T))$.

Theorem 2.1. *Let A be a k-algebra and $x \in A$. Then the following statements are equivalent:*

(i) The k-subalgebra $k[x]$ of A generated by x is semisimple (this is equivalent to x being k-semisimple).

(ii) Any finitely generated A-module V, becomes a semisimple module if we consider it as an $k[x]$-module.

(iii) The minimal polynomial of x is square-free in the algebra $k[T]$.

Remark:
If D is a division algebra over k and if V could in addition be endowed with the structure of a finitely generated D-module then this theorem is in particular true for the subalgebra $\mathrm{End}_D(V)$ which will be needed later in this work.

Proof: Let μ_x be the minimal polynomial of x in $k[T]$ and let $\mu_x(T) = \prod_{i=1}^n P_i(T)$ be its unique (up to order) decomposition in irreducible polynomials.
$(i) \leftrightarrow (iii)$
For any $x \in A$ the map that is defined by (1) is a surjective k-algebra homomorphism from $k[T]$ to $k[x]$ where the kernel is the ideal that is generated by $\mu_x(T)$. Therefore $k[x]$ is isomorphic to $k[T]/(\mu_x(T))$. Thus if $k[x]$ is a semisimple k-algebra then $k[T]/(\mu_x(T))$ is semisimple. Suppose $\mu_x(T)$ was not square free. Then there exists some non trivial polynomial $p(T)$ such that $p(T)^2$ divides $\mu_x(T)$. But then the ideal that is generated by $p(T)$ is not trivial and nilpotent and therefore $k[T]/(\mu_x(T))$ is not semisimple.
On the other hand suppose $\mu_x(T)$ is square free. Then the ideal $\mu_x(T)$ is a radical ideal and thus the nilpotent radical of $k[T]/(\mu_x(T))$ is trivial and thus this k-algebra is semisimple and therefore $k[x]$ is semisimple.
$(iii) \rightarrow (ii)$
In the decomposition of $\mu_x(T)$ in irreducible polynomials we have $P_i(T) \neq P_j(T)$ for all $i \neq j$ since μ_x is square-free (in particular this implies that all elementary divisors are of the form P_i^1) and we saw that for $V_i := \{v \in V \mid P_i(x)v = 0\}$ we have $V = \bigoplus_i V_i$. The ideal $(P_i(T))$ generated by $P_i(T)$ is a maximal ideal in $k[T]$ and thus $k[T]/(P_i(T))$ is a field and the V_i become vector spaces. Any such V_i is a direct sum of 1-dimensional $k[T]/(P_i(T))$-vector spaces and since $P(T)$ acts by multiplication with an element of the field all these are invariant and simple as modules. Therefore any V_i is a direct sum of simple modules and therefore V is a direct sum of simple modules and hence semisimple.

$(ii) \rightarrow (iii)$
Suppose $\mu_x(T) = p(T)^2 q(T)$ for polynomials $p(T), q(T)$. Then the set $U := \ker(p(x)q(x))$ is a $k[x]$-submodule of V and as V is a semisimple $k[x]$-module there exists some $k[x]$-submodule W such that $V = U \oplus W$. Since $\mu_x(x)w = 0$ we know that $p(x)w \in U$ and as W is an $k[x]$-submodule $p(x)w \in W$. Thus we have $p(x)w = 0$ and therefore $p(x)q(x)w = 0$. But this implies that $\mu_x(T)|p(T)q(T)$ and thus $p(T) = 1$.

□

This theorem also shows that the element g_a of the example is k-semisimple. This is true since its minimal polynomial is square free in $k[T]$ as we have already seen. Furthermore we saw that the minimal polynomial is not square free in any field extensions of k that contains the p'th root of a. So the element g_a is kind of the simplest example for a k-semisimple element that is not semisimple.

Remarks:

1. Every semisimple element is also k-semisimple. One can see this the easiest way by taking the minimal polynomial condition.

2. An element $x \in A$ is k-semisimple if and only if the image of x in $A \otimes k_s$ is k_s-semisimple for the natural embedding of A in $A \otimes k_s$.
   An element $x \in A$ is k-semisimple if and only if its minimal polynomial $\mu_x(T)$ is square free in $k[T]$. Now consider the minimal polynomial of x considered as an element of $A \otimes k_s$. It is clear that this minimal polynomial equals the image of $\mu_x(T)$ in $k_s[T]$ under the natural embedding of $k[T]$ in $k_s[T]$. Suppose that there exists one factor $q(T)$ in $\mu_x(T) \in k_s[T]$ with power bigger then one. Since k_s is the maximal separable field extension of k this power has to equal p^s for some $s > 1$. Thus $q(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0$ with $a_i \in k_s$. If $a_i \in k$ for all i then $q(T) \in k[T]$ and the minimal polynomial of x was not square-free in $k[T]$. Thus there exists at least one i such that $a_i \notin k$ but $a_i^{p^s} \in k$. But then k_s was not a separable field extension. Thus $\mu_x(T)$ is also square free in $k_s[T]$ and x is k_s-semisimple. On the other hand an element that is k_s-semisimple is also k-semisimple since a polynomial that is square free in $k_s[T]$ is also square free in $k[T]$.

3. Let ρ be a k-algebra representation from A to $\operatorname{End}(V)$ for some k-vector space V and let $x \in A$ be a k-semisimple element in A. Then the minimal polynomial condition shows that $\rho(x)$ is also k-semisimple.

A first approach to obtain a definition of k-semisimplicity for algebraic groups might be the following:

It is well known that any linear algebraic k-group G is isomorphic to some subgroup of the group of automorphisms $\mathrm{GL}(V)$ of some k-vector space V (here the isomorphism is defined over k). Now one can embed $\mathrm{GL}(V)$ in the algebra of endomorphisms of V. Then one could call an element $g \in G$ k-semisimple if it is k-semisimple as an element of the endomorphism algebra.

Unfortunately, this approach does not work . The problem is that different representations of an algebraic group G might map an element $g \in G$ once to a k-semisimple element and another time to an element that is not k-semisimple. An example for a representation that maps k-semisimple elements on unipotent elements is the following:

Lemma 2.1. *Let g be an element of $\mathrm{GL}(V)$ with minimal polynomial $T^{p^n} - a$ where $a \in k$ has no p-th root in k and V is some vector space. Then the map $\operatorname{Ad}(g) : \operatorname{End}(V) \to \operatorname{End}(V)$ is unipotent.*

Proof: Since the minimal polynomial of g equals $T^{p^n} - a$ we can deduce that $g^{p^n} = aE$. Therefore $(g^{-1})^{p^n} = a^{-1}E$ and we have

$$(\operatorname{Ad}(g))^{p^n}(h) = a^{-1}EhaE = \operatorname{id}(h) \qquad \square$$

More generally we can say:

Corollary 2.1. *Let V be a vector space, g be an element of $\mathrm{GL}(V)$ such that $T^{p^n} - a$ divides $\mu_g(T)$ for some natural number n where a has no p'th root in k. Then the map $\operatorname{Ad}(g)$ is not k-semisimple.*

Proof: Since $(T^{p^n} - a) | \mu_g(T)$ there exists some non empty subspace

$$V_0 := \left\{ v \in V \mid (g^{p^n} - a)v = 0 \right\}.$$

By the last lemma the restriction on V_0 maps $\operatorname{Ad}(g)$ to a unipotent endomorphism and therefore the endomorphism $\operatorname{Ad}(g)$ cannot be k-semisimple. $\square$

Thus there exist representations such that k-semisimple elements in GL_n are mapped to unipotent elements that are in particular not k-semisimple. On the other side the tautological representation obviously yields k-semisimple elements.

2.2 Algebras with involution

Before considering classical k-groups we need some results about semisimple k-algebras with involution which will occur in the definition of classical k-groups.

Definition. Let A be a k-algebra. A k-linear map $\iota : A \to A$ is called an involution if it satisfies

(i) $\iota(ab) = \iota(b)\iota(a)$ for all $a, b \in A$

(ii) $\iota(\iota(a)) = a$ for all $a \in A$

Thus, an involution is an antiautomorphism. The pair (A, ι) is an algebra with involution. The involution ι is said to be of the first kind if it is the identity on the center of A. Otherwise it is said to be of the second kind.

A k-algebra A is called simple if there exists no proper ideal in A. Accordingly we say that the pair (A, ι) is a simple k-algebra with involution if there exists no proper ideal in A that is invariant under ι. If (A, ι) is a semisimple k-algebra with involution then it is a direct sum of simple algebras with involution, i.e.

$$(A, \iota) \cong \bigoplus_{i=1}^{n} (A_i, \iota_{|A_i})$$

where $(A_i, \iota_{|A_i})$ are simple k-algebras with involution.

Lemma 2.2. *Let (A, ι) be a simple k-algebra with involution. Then A is simple as a k-algebra or $A \cong A_1 \oplus A_2$ and $\iota_{|A_1}$ is an antiisomorphism $A_1 \to A_2$ with inverse $\iota_{|A_2}$ where A_1 and A_2 are simple k-algebras.*

Proof: Suppose A is not simple. Then there exists some proper ideal $\mathcal{I}$ in A and since ι is an algebra antihomomorphism $\iota(\mathcal{I}) := \mathcal{I}'$ is again an ideal in A. Furthermore $\mathcal{I} \cap \mathcal{I}'$ is an ideal that is invariant under ι and as A is a simple k-algebra with involution $\mathcal{I} \cap \mathcal{I}' = \{0\}$. Take a look at $\mathcal{I} \oplus \mathcal{I}'$. This is an ideal and furthermore we have

$$\iota(\mathcal{I} \oplus \mathcal{I}') = \iota(\mathcal{I}) \oplus \iota(\mathcal{I}') = \mathcal{I}' \oplus \mathcal{I}$$

and therefore this sum is invariant under ι. Thus $\mathcal{I} \oplus \mathcal{I}'$ is a non-empty ideal in A that is invariant under ι. Since (A, ι) was simple as a k-algebra with involution we have $\mathcal{I} \oplus \mathcal{I}' = A$. If we set $\mathcal{I} = A_1$ and $\mathcal{I}' = A_2$ then we see that $A = A_1 \oplus \iota(A_1)$ and as ι is an involution it is an antiisomorphism of A and the inverse of $\iota_{|A_1} : A_1 \to A_2$ is $\iota_{|A_2} : A_2 \to A_1$. Now suppose that A_1 was not simple. Then there exists some proper ideal $\mathcal{I}_1$ in A_1 and it is clear that $\iota(\mathcal{I}_1) := \mathcal{I}_2$ is an ideal in A_2. Again $\mathcal{I}_1 \oplus \mathcal{I}_2$ is an ideal that is invariant under ι and therefore it equals A and thus $\mathcal{I}_1 = A_1$ and $\mathcal{I}_2 = A_2$. □

Corollary 2.2. *In the above situation when A is not simple then $A_2 \cong A_1^{\mathrm{op}}$.*

Proof: This follows immediately from the last lemma. □

Remarks:

1. For (A, ι) a simple k-algebra with involution, A is either simple or $A = A_1 \oplus A_1^{\mathrm{op}}$ and ι is an isomorphism from A_1 on A_1^{op}. If the latter is true then $\iota(x, y) = (y, x)$ for $x \in A_1$ and $y \in A_1^{\mathrm{op}}$.

2. If A_1 is a semisimple k-subalgebra of (A, ι) that is invariant under ι then $(A_1, \iota_{|A_1})$ is a semisimple k-algebra with involution.

In the chapter "Semisimple elements of k-algebras" we defined the element $x \in A$ to be k-semisimple if $k[x]$ is a semisimple k-algebra. It is not clear that $k[x]$ will be invariant under ι if (A, ι) is a k-algebra with involution and in general this needs not be true. The following lemma will show that under some condition $k[x]$ will be invariant under ι.

Lemma 2.3. *Let (A, ι) be a semisimple k-algebra with involution and $x \in A$ a k-semisimple element such that $x\iota(x) = \iota(x)x \in k^\times$. Then the subalgebra $k[x]$ is a semisimple k-algebra with involution $\iota_{|k[x]}$.*

Proof: By definition the fact that x is k-semisimple implies that $k[x]$ is a semisimple k-algebra and thus the only thing that needs to be shown is that $k[x]$ is invariant under ι. As $\iota(k[x]) = k[\iota(x)]$ it is enough to show that $\iota(x)$

is in $k[x]$ i.e. since $\iota(x) = cx^{-1}$ for some $c \in k^{\times}$ it is enough to show that there exist $\lambda_0 \dots \lambda_n \in k$ such that

$$x^{-1} = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$$

for $n = \deg \mu_x(T)$. Let $\mu_x(T) = \alpha_0 + \alpha_1 T + \ldots + \alpha_n T^n$. Since x is invertible $\alpha_0 \neq 0$. We know that $\mu_x(x) = 0$ and multiplication with x^{-1} on both sides yields

$$0 = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \Leftrightarrow x^{-1} = -\frac{1}{\alpha_0}(\alpha_1 + \ldots + \alpha_n x^{n-1})$$

Thus $x^{-1} \in k[x]$ and therefore $cx^{-1} \in k[x]$ and $k[\iota(x)] = k[x]$. □

We need a better understanding of the structure of semisimple k-algebras with involutions. All results we give in this context are well known and this is just a recapitulation of results that are given in the books [Wei95], [Sch85] and especially [Jac96].

The first step in examining semisimple k-algebras with involution is the theorem of Artin-Wedderburn that gives the structure of arbitrary semisimple k-algebras.

Theorem 2.2. *(Artin-Wedderburn) Let A be a semisimple k-algebra. Then there exist division algebras $D_1, \ldots, D_s$ over k and natural numbers $n_1, \ldots, n_s$ such that*

$$A \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$$

where $M_n(D)$ denotes the set of $n \times n$ matrices with entries in D.

The proof of this theorem can be found in [Wei95] (Chapter IX §1 theorem 1). Actually [Wei95] proves this result just for simple algebras but the generalisation to semisimple algebras is trivial. For a better understanding we want to examine this theorem on a simple k-algebra A and to do so we use some more results that are proven in the book [Wei95] Chapter IX §1.

There exists a unique faithful simple left A-module N up to isomorphism and every left A-module is a direct sum of modules, all isomorphic to N (see proposition 1). As N is a simple module the endomorphism ring of N is a division algebra D over k. Here D should be understood as a ring of right operators on N. Now consider the left A-module A. Then A as an A-module is isomorphic to N^n for some natural number $n \geq 1$ and $A \cong M_n(D)$.

Thus if $A = \bigoplus_i A_i$ with A_i simple k-algebras then for every i there exists a faithful simple A_i-module N_i which is unique up to isomorphism and a n_i such that $A_i \cong \operatorname{End}_{D_i} N_i^{n_i}$ for D_i the endomorphism ring on N_i. Then $\bigoplus_i N_i^{n_i}$ is a left A-module in the obvious way and it is unique up to isomorphism.

Our next goal is to understand the involution ι on a simple k-algebra with involution (A, ι). If A is not simple then we saw that ι is the map $(x, y) \to (y, x)$ on $A_1 \oplus A_1^{\mathrm{op}}$. Thus henceforth we assume that A is also simple as a k-algebra.

Let A_1 and A_2 be simple k-algebras and $f : A_1 \to A_2$ an isomorphism. Let V_i be simple faithful A_i modules. Then we may endow V_2 with the structure of an A_1-module by

$$a_1 \cdot v_2 = f(a_1)v_2$$

for $v_2 \in V_2$ and $a_1 \in A_1$. As f is an isomorphism V_2 becomes a simple faithful A_1-module. As a simple faithful A_1-module is unique up to isomorphism we know that there exists some isomorphism of A_1-modules $s : V_1 \to V_2$ such that

$$s(a_1 v_1) = a_1 \cdot s(v_1) = f(a_1)s(v_1).$$

Let d_1 be an A_1-linear endomorphism of V_1 i.e. $d_1(a_1 v_1) = a_1 d_1(v_1)$. As s is a bijective function there exists some uniquely determined additive function $d_2 : V_2 \to V_2$ such that $d_2 \circ s = s \circ d_1$. Then we have

$$\begin{aligned} f(a_1)d_2(s(v_1)) &= f(a_1)s(d_1(v_1)) = s(a_1 d_1(v_1)) \\ &= s(d_1(a_1 v_1)) = d_2(s(a_1 v_1)) = d_2(f(a_1)s(v_1)) \end{aligned}$$

This defines an isomorphism σ between the division algebras D_i of A_i-linear endomorphisms of V_i.

Thus if A_1 and A_2 are isomorphic simple k-algebras and V_i is a left A_i-module such that $A_i \cong \operatorname{End}_D(V_i)$ then the isomorphism between A_1 and A_2 is induced by some σ-semilinear map s i.e. for f the isomorphism between A_1 and A_2

$$a(v_1) = s^{-1} f(a) s(v_1) \tag{2}$$

The proof from the following theorem is basically taken from the book [Jac96] chapter V 5.1. We only filled in some details and changed some minor things.

Theorem 2.3. *If A is a simple k-algebra with involution ι, then there exists a division algebra D over k with an involution σ, a right D-module V and an ϵ-σ-hermitian form H on V ($\epsilon = \pm 1$), such that the k-algebra A with involution ι is isomorphic to* $\operatorname{End}_D(V)$ *with the adjoint involution relative to H.*

Proof: The theorem of Artin-Wedderbrun states that A is isomorphic to $\mathrm{End}_D V$ for D some division algebra over k and V some finitely generated right D-module. We denote by V^* the dual space of V i.e. $V^* = \mathrm{Hom}_D(V, D)$. Then V^* is a left D-module but we can regard it is a right D^{op}-module if we define $dl = ld$ for $l \in V^*$ and d once taken as an element in D^{op} and once taken as an element in D. We want to explain the involutions with help of hermitian and skew hermitian forms and thus we will need some sesquilinearform. Thus define $l(v) = \langle v, l \rangle$. This is a nondegenerate bilinear form from $V \times V^*$ to D. Here we regard V^* as a right D^{op}-module and thus we have

$$\langle vd_1, ld_2 \rangle = d_1 \langle v, l \rangle d_2$$

for $v \in V$, $l \in V^*$ and d_1, $d_2 \in D$. For any $a \in \mathrm{End}_D(V)$ we have the transpose $a^* \in \mathrm{End}_D(V^*)$ defined by $a^*(l) = l \circ a$. This definition yields

$$\langle av, l \rangle = l(av) = a^* l(v) = \langle v, a^* l \rangle$$

and the map $a \to a^*$ is an anti-isomorphism from A to A^*. Therefore the composition of this map with the involution ι is an isomorphism between the algebras A and A^* i.e. an isomorphism between the algebras $\mathrm{End}_D(V)$ and $\mathrm{End}_{D^{\mathrm{op}}}(V^*)$. With help of equation (2) we can see that there exists some isomorphism σ from D to D^{op} and some bijective σ-semilinear map s from V to V^* such that

$$a^* = s\iota(a)s^{-1}.$$

If we consider σ as a map from D to D then it is an anti-isomorphism. Setting

$$H(v, w) = \langle v, sw \rangle$$

we obtain some nondegenerate σ-sesquilinearform on V i.e.

$$H(vd_1, wd_2) = d_1 H(v, w) \sigma(d_2)$$

for v, $w \in V$ and d_1, $d_2 \in D$. Now we have

$$H(v, \iota(a)w) = \langle v, s\iota(a)w \rangle = \langle v, a^* sw \rangle$$

$$= \langle lv, sw \rangle = H(lv, w)$$

and thus $\iota(a)$ is the uniquely determined adjoint of a relative to H.
It is clear that for fixed $v \in V$ the map $f : w \to \sigma^{-1} H(v, w)$ is linear and

therefore it lies in V^*. As s is an isomorphism from V to V^* there exists some element $v' \in V$ such that $s(v') = f$. This is equivalent to

$$\sigma^{-1}H(v,w) = H(w,v'). \tag{3}$$

It is also clear that for fixed w, u the map $v \to uH(v,w)$ is an element of the endomorphism algebra A. Denote this map by a then we saw that

$$H(au,w) = H(u,\iota(a)w)$$

and therefore we have

$$H(au,w) = H(uH(v,w),x) = H(v,w)H(u,x)$$

$$= H(v,w\sigma^{-1}(H(u,x))) = H(u,\iota(a)w)$$

and therefore with help of equation (3) $\iota(a) : x \to w\sigma^{-1}H(u,x) = wH(x,u')$. As ι is an involution we know that $a = \iota(\iota(a))$ and thus we have

$$a(v) = uH(v,w) = \iota(wH(x,u')) = u'H(v,w')$$

But then we know that there exists some $c \in D$ with $uc = u'$ for all $u \in V$. With equation (3) and the equivalence

$$H(w,v') = \sigma^{-1}(H(v,w)) \leftrightarrow \sigma(c)\sigma(H(w,v)) = H(v,w)$$

we obtain (with $d = \sigma(c)^{-1}$)

$$\sigma(H(w,v)) = dH(v,w). \tag{4}$$

Furthermore we have

$$\sigma^2(H(w,v)) = \sigma(H(v,w))\sigma(d) = dH(w,v)\sigma(d).$$

We may choose v, w such that $H(w,v) = 1$ and as $\sigma^2(1) = 1$ we have $d\sigma(d) = 1$. Now we need to consider two different cases.
If $d = -1$ then $\sigma^2 = 1$ and thus σ is an involution on D. Furthermore we have $\sigma H(v,w) = -H(w,v)$. If $\sigma = 1$ then 1 is an isomorphism from D to D^{op} and therefore D is a field. Then H is a skew-symmetric bilinear form.
If $\sigma \neq 1$ then there exists some $d_1 \in D$ such that $q := \sigma(d_1) - d_1 \neq 0$. It is

clear that $\sigma(q) = -q$ and thus the map $\sigma' : d_2 \to q^{-1}\sigma(d_2)q$ has the following property

$$\sigma'(\sigma'(d_2)) = q^{-1}\sigma'(q)d_2\sigma'(q^{-1})q = q^{-1}(-q)d_2(-q^{-1})q = d_2$$

and thus σ' is an involution. Now consider the map

$$H' : (v, w) \to H(v, w)q$$

for v, w in V. We claim that this is a hermitian form relative to σ'. It is obvious that H' is additive in v and w furthermore

$$H'(vc_1, wc_2) = c_1 H(v, w)\sigma(c_2)q = c_1 H(v, w)q\sigma'(c_2)$$

for arbitrary c_1 and c_2 in D. Thus H' is a sesquilinearform relative to σ'. We still have to prove that $H'(v, w) = \sigma'(H'(w, v))$.

$$H'(v, w) = H(v, w)q = -\sigma(H(w, v))q = \sigma'(q)q^{-1}\sigma(H(w, v))q$$
$$= \sigma'(q)\sigma'(H(w, v)) = \sigma'(H(w, v)q) = \sigma'(H'(w, v))$$

For all $a \in A$ we have

$$H'(av, w) = H(av, w)q = H(v, \iota(a)w)q = H'(v, \iota(a)w)$$

and therefore ι is the adjoint map relative to H'.
If $d \neq -1$ then $q = d - 1 \neq 0$. Define again $H'(v, w) = H(v, w)q$ and $\sigma'(d_1) = q^{-1}\sigma(d_1)q$. This time it is not so easy to see that σ' is an involution but the same way as before we can see that H' is again sesquilinear relative to σ'. Furthermore we have

$$\sigma'(H'(v, w)) = \sigma'(H(v, w)q) = \sigma'(q)\sigma'(H(v, w)) = \sigma'(q)q^{-1}\sigma(H(v, w))q$$

and with equation (4) we see that

$$\sigma'(q)q^{-1}\sigma(H(v, w))q = \sigma'(q)q^{-1}dH(w, v)q = \sigma'(q)q^{-1}dH'(w, v)$$

Furthermore with help of the equations $\sigma'(q)q^{-1} = q^{-1}\sigma(q)$, $q = d + 1$ and $\sigma(d)d = 1$ we obtain

$$\sigma'(q)q^{-1}d = q^{-1}\sigma(q)d = (d + 1)^{-1}(1 + \sigma(d))d = 1.$$

This implies that $\sigma'(H'(v, w)) = H'(w, v)$ and therefore σ' is an involution and H' is a hermitian form relative to σ'. Again ι coincides with the adjoint map relative to this form.

□

We will frequently make use of the following theorem.

Theorem 2.4. *Let A be a central simple algebra over k and L a simple subalgebra. Let $Z_A(L)$ be the centralizer of L in A. Then $Z_A(L)$ is simple and*

$$\dim_k(A) = \dim_k(L)\dim_k(Z_A(L))$$

The proof can be found in [Sch85] (Chapter 8. theorem 4.5).

We will need some informations about the centraliser of a k-semisimple element in A.

Lemma 2.4. *Let a be a k-semisimple element in the simple k-algebra A with center Z. Then the centraliser $Z_A(a)$ is semisimple.*

Proof: As the center of A is a field extension of k we know that a is not only k-semisimple but also Z-semisimple. Therefore $Z[a]$ is a semisimple Z-subalgebra of A and thus $Z[a] = \bigoplus_i B_i$ where B_i is a simple Z-algebra. Furthermore it is clear that $Z_A(a) = Z_A(Z[a])$. Denote by e_i the unit element in B_i in particular $1 = \sum_i e_i$. Define the simple Z-algebras $A_i = e_i A e_i$ then $B_i \subset A_i$. Therefore $Z_A(\bigoplus_i B_i) = \bigoplus_i Z_{A_i}(B_i)$. As A_i and B_i are simple algebras and A_i is central we may apply the last lemma and see that $Z_{A_i}(B_i)$ is simple. □

Let A be a simple k-algebra and $a \in A$ a k-semisimple element. We saw that there exists some D-module V such that $A = \mathrm{End}_D(V)$ for some division algebra D over k. Let $\mu_a(T) = \prod_{i=1}^n P_i(T)$ be the minimal polynomial of a for irreducible polynomials $P_i(T)$. Then by the theory of elementary divisors $V = \bigoplus_{i=1}^n V_i$ where $V_i = \{v \in V \mid P_i(a)v = 0\}$. We know that $K_i := k[T]/(P_i)$ is a field and thus we may consider V_i as a K_i-vector space. As a is a k-semisimple element we know that $k[a]$ is a semisimple algebra. Thus $k[a] = \bigoplus_i k[a]_i$. Combine all summands that are isomorphic and denote by e_i the unit of the combinations. Then $V_i = e_i V$ and a acts on V_i by scalar multiplication with an element in K_i. We will see that $Z_A(a)e_i \cong \mathrm{End}_{K_i \otimes_k D^{\mathrm{op}}}(V_i)$.
At first we want to show that V_i is invariant under $Z_A(a)$ and then it is invariant under $Z_A(a)e_i$. So we have to see that $P_i(a)zv = 0$ for $z \in Z_A(a)$. We will use the fact that z commutes with a and therefore z commutes with $P_i(a)$

$$P_i(a)zv = zP_i(a)v = z0 = 0$$

Now V_i is a K_i-vector space and it is also a right D-module and actually the action of K_i and of D commute as K_i acts D-linear on V_i. Thus V_i becomes a K_i-D-bimodule or equivalently a $K_i \otimes_k D^{\mathrm{op}}$-module. Now any $z \in \mathrm{End}_{K_i \otimes_k D^{\mathrm{op}}}(V_i)$ acts D-linear on V_i and as it is K_i-linear it also commutes with a as a acts by scalar multiplication on V_i and therefore $\mathrm{End}_{K_i \otimes_k D^{\mathrm{op}}}(V_i) \subset Z_A(a)e_i$. On the other side it is clear that any element in $Z_A(a)e_i$ is D-linear and K_i-linear. Therefore we have

$$\mathrm{End}_{K_i \otimes_k D^{\mathrm{op}}}(V_i) = Z_A(a)e_i. \tag{5}$$

Lemma 2.5. *Let (A, ι) be a semisimple k-algebra with involution and $a \in A$ a k-semisimple element such that $a\iota(a) = \iota(a)a = 1$. Then the subalgebra $Z_A(a)$ is a semisimple k-algebra with involution $\iota_{|Z_A(a)}$.*

Proof: Let $z \in Z_A(a)$. The fact that $az = za$ implies that $\iota(a)\iota(z) = \iota(z)\iota(a)$ and therefore we have

$$a\iota(z)\iota(a)a = a\iota(a)\iota(z)a \Rightarrow \iota(z)a = a\iota(z)$$

Thus if $z \in Z_A(a)$ then $\iota(z) \in Z_A(a)$ and therefore $Z_A(a)$ is invariant under ι.
Now we want to see that the k-algebra $Z_A(a)$ is semisimple. But this follows straight from lemma 2.4.

□

Definition. Let A be a k-algebra. Then the element $a \in A$ is called k-regular if it is k-semisimple and the k-algebra $k[a]$ is a maximal commutative k-subalgebra.

We will need the following well known lemma about commutative semisimple algebras.

Lemma 2.6. *A commutative semisimple algebra is a direct sum of fields.*

This lemma can be found in [Alb61].(Chapter 3 §5) Actually in this book this result is not proven as it is an obvious consequence of the theorem of Artin-Wedderburn so we want to give a short proof. Suppose A is a simple commutative k-algebra. Then the theorem of Artin-Wedderburn shows that A is isomorphic to $\mathrm{End}_D(V)$ for some division k-algebra D. As A is commutative D needs to be a field. Furthermore V has to be a 1-dimensional D-vector space because else $\mathrm{End}_D(V)$ is never commutative. Thus $A = D$.

Lemma 2.7. *Let A be a central simple K-algebra and L a commutative K-subalgebra. Then the following statements are equivalent:*

1. *L is a maximal commutative K-subalgebra.*
2. *The bicommutant of L in A equals L.*
3. $\dim_K A = (\dim_K L)^2$.

Proof: This is well known if L is a field, see [Bur66]. (Chapter VIII, §10, Prop. 3.) In fact, the equivalence of (i) and (ii) is obvious. We will reduce the general case, in which $L = L_1 \oplus \ldots \oplus L_r$ is a direct sum of fields, to the special case. The unit element e_i of L_i is an idempotent in L, and $e_1 + \ldots + e_r = 1$. Take a simple left A-module V and consider it as a right module for the skewfield $D = \operatorname{End}_A(V)$. Then $V_i = e_i V$ is a L_i-D-bimodule, and $V = V_1 \oplus \ldots \oplus V_r$ is a D-module. Now L_i is a subfield of the central simple K-algebra $A_i = \operatorname{End}_D(V_i) = e_i A e_i$, for which the assertion is known, so that in particular $\dim_K A_i \geq (\dim_K L_i)^2$. By Wedderburn's theorem, $\dim_K A = \dim_D A \dim_K D = (\dim_D V)^2 \dim_K D$ and similarly $\dim_K A_i = (\dim_D V_i)^2 \dim_K D$. We conclude that

$$\begin{aligned}\sqrt{\dim_K A} = \dim_D V \sqrt{\dim_K D} &= \sum_i \dim_D V_i \sqrt{\dim_K D} \\ &= \sum_i \sqrt{\dim_K A_i} \geq \sum_i \dim_K L_i = \dim_K L.\end{aligned}$$

If (i) is satisfied, so is its analogue for each $L_i \subset A_i$, and we have equality for each i, whence (iii) follows. Conversely, if (iii) is satisfied, then so is its analogue for each i due to our formula. By the known special case, assertion (i) for each i follows. If L is contained in a commutative subalgebra L', the latter must preserve each V_i, and its restriction to V_i cannot be larger than L_i. Hence (i) follows. □

In the case we consider, the algebra A is in general not central. However, for A a simple k-algebra we know that the center Z of A is a field. If we consider A as a Z-algebra then it is a central simple algebra.

Lemma 2.8. *Let $a \in A$ be a k-regular element. Then $Z_A(a) = k[a]$.*

Proof: Obviously $k[a] \subset Z_A(a)$ and therefore we only have to show that $Z_A(a) \subset k[a]$. Suppose $z \in Z_A(a)$, then $za = az$ and therefore z commutes with $k[a]$. But as a is k-regular $k[a]$ is a maximal commutative k-subalgebra and therefore $z \in k[a]$. □

Later in this work we will give a definition for k-regularity of elements in groups. Then the following lemma will be important. For the proof we need the notion of reduced characteristic polynomials. We use the definition that is given in [Sch85].(Chapter 8 §5 definition 5.8) Let A be a central simple k algebra and K a splitting field of k. Choose some isomorphism

$$I : A_K = A \otimes_k K \cong M_n(K)$$

and consider A to be contained in A_K. For every $a \in M_n(K)$ we have the characteristic polynomial

$$\chi(X, a) = \chi_L(X, a) = \det(XE - a) \in K[X].$$

For $a \in A_K$ define $\chi(X, a) = \chi(X, i(a))$. This makes sense as the characteristic polynomial does not depend on the choice of I by the theorem of Skolem-Noether. Furthermore Scharlau proves that the characteristic polynomial does not depend on the choice of the splitting field and has coefficients in k.

Lemma 2.9. *If (A, ι) is a noncommutative simple k-algebra with involution, then there exists a regular semisimple element in A^-.*

Proof: For an element a of a simple algebra A, let $\chi_a(T)$ be its (reduced) characteristic polynomial over Z. If ι is an involution on A of the first kind, we set $\tilde{\chi}_a = \chi_a$. If ι is of the second kind, its restriction σ to Z is the nontrivial element of the Galois group of Z over Z^+, and we set $\tilde{\chi}_a = \chi_a \cdot \sigma(\chi_a)$. If ι permutes the simple factors A_1 and A_2 of A, we set $\tilde{\chi}_{(a_1,a_2)} = \chi_{a_1} \cdot \chi_{a_2}$ for $(a_1, a_2) \in A_1 \oplus A_2 = A$. Let $\Delta(a)$ be the discriminant of $\tilde{\chi}_a(T)$. Then Δ is a Z^+-regular function on A.
If now K is a field extension of Z^+, the algebra $A_K = A \otimes_{Z^+} K$ endowed with the K-linear extension of ι is simple, because its centre $Z \otimes_{Z^+} K$ is either K or a direct sum of two copies of K, which are permuted by ι. For $a \in A$ considered as an element of A_K, the meaning of $\tilde{\chi}_a$ is unchanged, and Δ extends to a K-regular function on A_K such that $\Delta(a)$ is still the discriminant of $\tilde{\chi}_a$ for $a \in A_K$.

The principal open subset defined by Δ consists of the regular semisimple elements of A. Thus it is enough to show that A^- is not contained in the zero set of Δ. This will follow if we can prove it for A_K^- when K is the algebraic closure of Z^+. In this case, the simple factors of A are isomorphic to matrix algebras such that, if A is simple, ι corresponds to the adjoint map for the standard bilinear or symplectic form. Since A_K is noncommutative, it is easy to find regular semisimple elements in A_K^-. □

Lemma 2.10. *Every ι-stable commutative semisimple subalgebra L of non-maximal dimension in a central simple algebra A with involution can be extended to a ι-stable commutative semisimple subalgebra L' such that $L'^- \neq L^-$.*

Proof: W.l.o.g. assume that L is a simple algebra with involution. Then we saw that the centraliser $Z_A(L)$ is a semisimple algebra with involution. Again w.l.o.g. suppose that $Z_A(L)$ is a simple algebra with involution. Since $\iota(L) = L$ it is clear that $\iota(Z_A(L)) = Z_A(L)$. Suppose that $Z_A(L)$ is not commutative. Then the last lemma shows that there exists some regular semisimple element z in $Z_A(L)^-$. We saw that $k[z] = Z_A(z)$ and therefore $L \subset k[z]$. Furthermore $k[z]$ is semisimple and ι-stable. As L was not maximal it is clear that $z \notin L$. Thus $k[z]^- \neq L^-$.
If $Z_A(L)$ is commutative then $Z_A(L)$ is a maximal commutative simple subalgebra of A that is ι-stable. If $Z_A(L)$ is commutative then it is a field and it is well known that it is a quadratic field extension of $Z_A(L)^+$ and $\dim Z_A(L)^+ = \dim Z_A(L)^-$. The same is true for the subfield L and if $L^- = Z_A(L)^-$ then it is clear that $L = Z_A(L)$. This is a contradiction as we assumed that L is not maximal. □

Corollary 2.3. *Let (A, ι) be a k-algebra with involution. If L is maximal among the ι-stable commutative semisimple k-subalgebras, then L is also maximal among all commutative semisimple k-algebras.*

Proof: This is an immediate consequence of the last lemma. □

3 Classical k-groups

As our definition for k-semisimplicity does not work for arbitrary linear algebraic k-groups we restrict on groups that are naturally embedded in some k-algebra A. In this work we will restrict ourselves to classical k-groups. In the literature there are several different definitions for these and for this reason we have to specify which definition of classical k-groups is used in this work. Beside this we want to show some properties that will be necessary for us before we come back to the notion of k-semisimplicity.

3.1 Classical k-groups

Definition. Let (A, ι) be a semisimple k-algebra with involution and let G be the group of elements in A with $g\iota(g) = 1$. Then we will call G a classical k-group.

Remark:

1. Let $g \in A$ be an invertible element. Then it defines an inner automorphism $a \to gag^{-1}$ and g commutes with the involution ι if and only if
$$g\iota(a)g^{-1} = \iota(g^{-1})\iota(a)\iota(g).$$
Thus $\iota(g)g$ lies in the center of A

2. Assume (A, ι) is a simple k-algebra with involution and V the A-module induced by the theorem of Artin-Wedderburn. Then we may apply theorem 2.3 and we see that there exists a ϵ-σ-hermitian form H on V such that the involution ι is the adjoint map relative to H. It is an easy consequence that $\iota(g) = g^{-1} \Leftrightarrow H(gv, gw) = H(v, w)$ and therefore the classical k-groups in simple k-algebras with involution are exactly those groups that preserve the corresponding ϵ-σ-hermitian form H.

To get an idea of those classical k-groups we just defined take a look at the following standard examples for classical groups.

Example. 1. Consider the algebra $M_n(D) \times M_n(D^{\mathrm{op}})$ with the involution $\iota(X, Y) = (Y^t, X^t)$ where D is again some division algebra over k. In this case A is a simple k-algebra with involution that is not simple as a k-algebra. Therefore conjugation by an element $g = (X, Y)$ commutes with ι if and only if $(E,E) = g\iota(g) = (XY^t, YX^t) \leftrightarrow Y = (X^t)^{-1}$. This set is obviously isomorphic to GL_n and thus GL_n is a classical k-group. We may also embed the group SL_n by

$$X \to (X, (X^t)^{-1}) : \mathrm{SL}_n \to M_n(D) \times M_n(D).$$

2. Let A be the algebra $M_n(D)$ where D is a division algebra over k, $\iota(X)$ be the conjugate (i.e. some involution σ on D) transpose of X and G be the set of unitary matrices. It is clear that

$$\mathrm{U}_{\sigma,n,D} = \{g \in A \mid g\iota(g) = 1\}.$$

   Actually the Gram matrix h is the identity in this case and $\mathrm{U}_{\sigma,n,D}$ is the group of elements that preserve the corresponding symmetric sesquilinearform H.

3. Let A be the algebra $M_{2n}(D)$ where D is a division algebra over k with involution σ, let

$$h = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$$

   and let $\iota = h^{-1}(\sigma())^t h$. We saw in the last chapter that ι is an involution. Now the group that is defined by the equation $g\iota(g) = 1$ is the symplectic group $\mathrm{Sp}_{\sigma,2n,D}$. Observe that in this case we have $h^t = -h$ and $\mathrm{Sp}_{\sigma,2n,D}$ is the group of elements that preserve the antisymmetric bilinearform H that is induced by h.

Remarks:

1. In fact there is a more general definition for classical k-groups. This is: Let (A, ι) be a semisimple k-algebra with involution and let G be a group that is k-isogenous to an automorphism group G_1, with the property that any $g_1 \in G_1$ is compatible with ι i.e. $g_1(\iota(a)) = \iota(g_1(a))$. Then G is called a classical k-group.
   But since we will only consider classical k-groups with the property that $g\iota(g) = 1$ for all $g \in G$ we will restrict to the first definition.

2. Let A be a semisimple k-algebra with involution. Then $\overline{k} \otimes A$ is a $\overline{k}$-algebra with a k-involution. Since any $\overline{k}$-algebra is in particular a $\overline{k}$-vector space we may consider $\overline{k} \otimes A$ as a finite dimensional $\overline{k}$-vector

space. Thus we have an affine algebra and the equation $g\iota(g) - 1 = 0$ defines a linear algebraic group G. Since ι is k-linear this is a k-closed set. The set of k-rational points in G equals the set of points in A with $g\iota(g) = 1$.

3. The theorem of Artin-Wedderburn states that A is isomorphic to a direct product of matrix algebras. As this isomorphism is a k-algebra isomorphism it maps k-semisimple elements to k-semisimple elements. This allows us to assume that A is a matrix algebra itself and thus G is a subgroup of GL_n for some natural number n.

4. If $A = A_1 \times \ldots \times A_n$ is a semisimple k-algebra with involution ι such that A_i is a simple k-algebra with involution for all i then we have for the classical group $G = G_1 \times \ldots \times G_n$ for G_i the classical group in A_i induced by $\iota_{|A_i}$. This is the reason why we may restrict ourself s on classical k-groups in simple k-algebras with involution in most of the proofs.

5. In fact it is not clear so far that a classical k-group is indeed a k-group. We know that GL_n is a k-group for any n and furthermore in [Bor91] (Chapter V §23 23.9) it is proven that the group of elements that preserves a ϵ-σ-hermitian form is a k-group. We just saw that any classical k-group is a product of groups of this form. Therefore any classical k-group is defined over k.

6. If K is a field extension of k then we may consider some classical k-group G also as a K-group. Also this is not necessarily a classical K-group (since $A \otimes K$ might be not semisimple) we will call it a classical k-group over K.

Summarizing we can say that a classical k-group G equals the set of k-rational points in a linear algebraic k-group we will also denote by G. Considering A as a k-vector space we may also consider G to be a subgroup of $\mathrm{Aut}_k(A)$ (i.e. the automorphism group of the k-vector space A) since any $g \in G$ defines a k-automorphism by $a \to ga$.

It is an interesting question if a classical k-group G spans the corresponding semisimple k-algebra A as a k-vector space. In general it is not true that a classical k-group has this property.

Example.

Consider the simple $\mathbb{R}$-algebra of 1×1 matrices with entries in the quaternions $\mathbb{H}$ together with the $\mathbb{R}$-linear involution ι that is defined by

$$\iota(z + wj) = z - jw$$

with z, $w \in \mathbb{C}$. We want to determine the classical $\mathbb{R}$-group G that is defined by ι. We have

$$(z + wj)\iota(z + wj) = (z + wj)(z - jw) = z^2 + w^2 + (w\overline{z} - z\overline{w})j = 1$$

if and only if $z^2 + w^2 = 1$ and $w\overline{z} = z\overline{w}$. Set $z = re^{i\phi}$ and $w = se^{i\psi}$ then the second equation is equivalent to $\phi = \psi$ modulo π. Thus the first equation becomes $(r^2 + s^2)e^{2i\phi} = 1$. Therefore $e^{2i\phi} = 1$ and $\phi = \lambda\pi$ where λ is an integer. This implies that $z \in \mathbb{R}$ and $w \in \mathbb{R}$ and thus G is isomorphic to $\mathrm{SO}_2(\mathbb{R})$. It is clear that the $\mathbb{R}$-linear span of G does not contain the whole of $\mathbb{H}$.

On the other side we can show that there are classical k-groups that span A.

Lemma 3.1. *Let A be the k-algebra $M_n(D)$ for some division algebra D over k then $A(\mathrm{GL}_n(D)) = A$. If A equals $M_n(k)$ then we also have $A(\mathrm{O}_n(k)) = A$.*

Proof: Fix i and j and define the matrix $b_{ij} = (x_{vw})_{vw}$ where $x_{ij} = 1$ and $x_{vw} = 0$ else with v, and w in $\{1, \dots, n\}$. Then b_{ij} is a D-basis of A. First we want to see that $b_{ij} \in A(\mathrm{GL}_n(k))$ for all i, j. For this purpose consider the element g_1 and $g_2 \in \mathrm{GL}_n(k)$ given by $g_1 = \frac{1}{2}b_{ij} + 1b_{ji} + \sum_{l\neq i,j} 1b_{ll}$ and $g_2 = \frac{1}{2}b_{ij} - 1b_{ji} - \sum_{l\neq i,j} 1b_{ll}$. It is obvious that these element are in $\mathrm{GL}_n(k)$ as exactly one entry in every line and every column is not zero. Furthermore $g_1 + g_2 = b_{ij}$. Thus every b_{ij} lies in $A(\mathrm{GL}_n(k))$. Thus we have $Db_{ij} = Dg_1 + Dg_2$ and as D is a division algebra the elements Dg_1 and Dg_2 both lie in $\mathrm{GL}_n(D)$ and therefore $A(\mathrm{GL}_n(D)) = A$.
In the case of $\mathrm{O}_n(k)$ in the k-algebra $M_n(k)$ we have to consider two different cases. First consider the basiselements of the form b_{ii}. Let $g_1 = \sum_i 1b_{ii}$ and $g_2 = 1b_{ii} - \sum_{j\neq i} 1b_{jj}$. The element $g_1 = E$ is obviously in O_n and the element g_2 is invariant under transposition and $g_2^2 = 1$ thus it is also in O_n. Then $g_1 + g_2 = 2b_{ii}$ and therefore $b_{ii} \in A(\mathrm{O}_n)$.
Secondly consider the elements b_{ij} with $i \neq j$. Here let $g_1 = 1b_{ij} + 1b_{ji} + \sum_{l\neq i,j} 1b_{ll}$ and $g_2 = 1b_{ij} - 1b_{ji} - \sum_{l\neq i,j} 1b_{ll}$. Again it is easy to see that g_1 and $g_2 \in \mathrm{O}_n$ and $g_1 + g_2 = 2b_{ij}$.

□

Thus there exist some examples of classical groups that span the ambient k-algebra.
Let G be the classical k-group associated to the algebra with involution (A, ι). Denote by $k^\times G$ the group of elements a in A with the property that $a\iota(a) \in k^\times$. Let $a \in k^\times$ with $a\iota(a) = c$ with $c \in k^\times$ and $g \in G$ then

$$aga^{-1}\iota(a^{-1})\iota(g)\iota(a) = c^{-1}c = 1$$

and therefore $k^\times G$ lies in the normalizer of G.

Lemma 3.2. *Let A be the k-algebra $M_{2n}(k)$. Let $h = (h_{ij})_{ij}$ with $h_{ij} = 0$ if $i + j \neq 2n + 1$, $h_{ij} = 1$ if $i + j = 2n + 1$ and $i < j$ and $(h_{ij} = -1$ if $i + j = 2n + 1$ and $i > j$. Then $h()^t h^{-1}$ defines an involution ι. The group of elements that is induced by ι is a classical k-group G. Then the normalizer of G spans A.*

Proof: We use the same notation and method we also used in the last lemma. Observe that $g \in G$ if g is symmetric relative to reflection on the diagonal that is defined by all entries g_{ij} with $i + j = 2n + 1$. Furthermore if it is antisymmetric relative to this reflection it lies not in G but in $-1G$ and therefore in the normalizer of G.
First consider the case b_{ij} with $i+j \neq 2n+1$. Then define $g_1 = \sum_i b_{in+1-i} + b_{ij} + b_{2n+1-i2n+1-j}$ and $g_2 = \sum_i -b_{in+1-i} + b_{ij} - b_{2n+1-i2n+1-j}$. Then g_1 is in G and g_2 is in $-1G$ and their sum is $2b_{ij}$.
Now consider b_{ij} with $i + j = 2n + 1$. Define $g_1 = \sum_i b_{ii} + b_{ij}$ and $g_2 = \sum_i -b_{ii} + b_{ij}$. Then g_1 and g_2 are in G and their sum is $2b_{ij}$. □

We saw that the classical group associated to $\mathbb{H}$ is a counterexample to the assumption that every classical k-group spans the ambient algebra. But in fact we can see that the normalizer of this classical group also spans $\mathbb{H}$. Thus we suspect that this is a general property of classical k-groups.
Thus consider again $\mathbb{H}$ with the involution ι given by

$$\iota(z + wj) = z - jw.$$

The normaliser of G is the group of elements satisfying $g\iota(g) \in \mathbb{R}^\times$, and a computation analogous to the one that was done in the counterexample shows that

$$z^2 + w^2 \in \mathbb{R}^\times$$

and z, $w \in \mathbb{R}$. The span of this normaliser is the whole of $\mathbb{H}$.

Lemma 3.3. *Let g be a k-semisimple element in the classical k-group G that is associated to the semisimple k-algebra with involution (A, ι). Then the centralizer $Z_G(g)$ of g in G is a classical k-group.*

Proof: The centralizer of g in G equals the intersection of G with $Z_A(g)$. By lemma 2.5, $Z_A(g)$ is a semisimple k-algebra with involution ι_1. Thus $\{g_1 \in Z_A(g) \mid g_1\iota_1(g_1) = 1\}$ is a classical k-group. But as $\iota_1 = \iota_{|Z(g)}$ this set equals $G \cap Z_A(g)$. □

The fact that $g\iota(g) = 1$ for all $g \in G$ has some consequences for the minimal polynomial of elements of classical k-groups.

Lemma 3.4. *Let G be a classical k-group in the semisimple k-algebra with involution (A, ι). Then for any $g \in G$ the minimal polynomial is either symmetric or antisymmetric i.e. for $f(T) = x_nT^n + \ldots x_0$ we have $x_i = x_{n-i}$ or $x_i = -x_{n-i}$.*

Proof: To see this we have to look at the whole algebra A and consider the linear algebraic group G as a subset of this algebra. Since $\mu_g(T)$ is the minimal polynomial of g we have

$$\mu_g(g) = g^s + \ldots + x_1g + x_0 = 0$$

Therefore we can see that g^{-1} is a zero of $\mu_g(T^{-1})$ and hence it is also a zero of $T^s\mu_g(T^{-1})$. The latter is a polynomial and therefore $T^s\mu_g(T^{-1})|\mu_{g^{-1}}(T)$. Since $\iota(g) = g^{-1}$ and since ι is an algebra antiautomorphism we have

$$\iota(\mu_g(g)) = \mu_g(g^{-1}) = g^{-s} + \ldots + x_1g^{-1} + x_0 = 0$$

Thus $\mu_g(g^{-1})$ is zero and therefore $\mu_g(T)$ divides the minimal polynomial $\mu_{g^{-1}}(T)$ of g^{-1}. Interchanging the roles of g and $\iota(g)$, we see that $\mu_{g^{-1}}(T)$ divides $\mu_g(T)$ and hence $\mu_g(T) = \mu_{g^{-1}}(T)$. So if g is an element in a classical k-group the minimal polynomial of g equals the minimal polynomial of g^{-1}. Since $\mu_{g^{-1}}(T) = \mu_g(T)$ the degree of $\mu_{g^{-1}}(T) = s$ and therefore $\mu_{g^{-1}}(T) = T^s\mu_g(T^{-1})$. Putting these facts together we get for the element g in the linear algebraic group G

$$T^s + \ldots + x_1T + x_0 = \mu_g(T) = \mu_{g^{-1}}(T)$$

$$T^{-s}\mu_g(T^{-1}) = \frac{1}{x_0}(x_0T^s + \ldots + x_{s-1}T + 1).$$

Now this implies that $\frac{1}{x_0} = x_0$ and thus $x_0 = 1$ or $x_0 = -1$ and therefore $\mu_g(T)$ is symmetric or $\mu_g(T)$ is antisymmetric.

□

Remark:
One might think that the standard example for a k-semisimple element g_a does not fulfil this property. But we saw in Example (1) that GL_n as a classical k-group is a subgroup of $M_n(k) \times M_n(k)$ and that $g \in \mathrm{GL}_n$ corresponds to the pair $(g, (g^{-1})^t)$. If we consider g_a then the minimal polynomial is $(T^p - a)(T^p - a^{-1})$ and thus the minimal polynomial is symmetric.

Lemma 3.5. *Let $f(T)$ be a polynomial of degree n and set $f'(T) = T^n f(T^{-1})$ then the following holds:*

1. *If $fg = h$ then $f'g' = h'$.*
2. *If f is irreducible, then so is f'.*
3. *If a polynomial P divides f to the exact power m, then P' divides f' to the exact power m.*

Proof: 1: Let $f(T) = \sum_{i=0}^n x_i T^i$ and let $g(T) = \sum_{j=0}^m y_j T^j$. Then we have

$$h(T) = f(T)g(T) = \sum_{l=0}^{n+m} \sum_{j=0}^{l} y_j x_{l-j} T^l$$

Thus

$$h' = T^{m+n} \sum_{l=0}^{n+m} \sum_{j=0}^{l} y_j x_{l-j} T^{-l}$$

$$= T^{m+n} (\sum_{i=0}^{n} a_i T^{-i})(\sum_{j=0}^{m} y_j T^{-j}) = T^n f(T^{-1}) T^m g(T^{-1}) = f'(T)g'(T)$$

2: Let $f(T) = \sum_{i=0}^n x_i T^i$ then $f'(T) = \sum_{i=0}^n x_i T^{n-i}$. But then

$$(f')'(T) = f(T)$$

Now suppose $f'(T)$ was not irreducible. Then there exist polynomials $P_1(T)$ and $P_2(T)$ such that $f'(T) = P_1(T)P_2(T)$. But then property 1 shows that

$$f(T) = (f')'(T) = P_1'(T)P_2'(T)$$

and thus $f(T)$ is not irreducible.

3: Let $f(T) = Q(T)P(T)^m$ then applying property 1 repeatedly yields

$$\begin{aligned} f'(T) = P'(T)(P^{m-1}Q)'(T) &= (P')^2(T)(P^{m-2}Q)'(T) \\ &= \ldots = (P')^m(T)Q'(T) \end{aligned}$$

Suppose there exists some $P_1(T)$ such that $Q'(T) = P'(T)P_1(T)$ then $Q(T) = P(T)P_1'(T)$ and $P(T)$ does not divide $f(T)$ to the exact power m. □

Corollary 3.1. *Let G be a classical k-group in (A, ι) and let $g \in G$. If the polynomial $P(T)$ divides the minimal polynomial $\mu_g(T)$ to the exact power m then $P'(T)$ divides $\mu_g(T)$ to the exact power m. The product of $P(T)$ with $P'(T)$ is symmetric.*

Proof: Observe that a polynomial $f(T)$ is symmetric (resp. antisymmetric) if and only if $f(T) = \epsilon f'(T)$ where $\epsilon = 1$ if f is symmetric and $\epsilon = -1$ is f is antisymmetric. We saw in lemma 3.4 that $\mu_g(T)$ is symmetric or antisymmetric and therefore $\mu_g(T) = \epsilon\mu_g'(T)$. If $P(T)$ divides $\mu_g(T)$ to the exact power m then property 3 of the last lemma shows that $P'(T)$ divides $\mu_g'(T) = \epsilon\mu_g(T)$ to the exact power m.
Now we want to see that the product of $P'(T)$ with $P(T)$ is symmetric or antisymmetric.

$$P(T)P'(T) = \sum_{j=0}^{2s}\sum_{i=0}^{s} x_i x_{s+i-j} T^j$$

To proof our claim consider the coefficients c_j of T^j and c_{2s-j} of T^{2s-j}. As $x_i = 0$ for $i < 0$ or $i > s$ we have

$$c_j = \sum_{i=0}^{s} x_i x_{i+s-j} = \sum_{\substack{i \\ i \leq j}} x_i x_{i+s-j}$$

and

$$c_{2s-j} = \sum_{i=0}^{s} x_i x_{j+i-s} = \sum_{\substack{i \\ i+j \geq s}} x_i x_{i+j-s}.$$

Now set $i + j - s = l$ and we obtain

$$c_{2s-j} = \sum_{l=0}^{s} x_{l-j+s} x_l = \sum_{\substack{l \\ l \leq j}} x_l x_{l+s-j} = c_j$$

and thus $P(T)P'(T)$ is symmetric. □

Remark:
The last corollary shows the following: Let $\mu_g(T) = \prod_{i=0}^{s} P_i(T)^{m_i}$ be the minimal polynomial of $g \in G$ where $P_i(T)$ are irreducible polynomials with $P_i(T) \neq P_j(T)$ for $i \neq j$ and G is a classical k-group. Then $P_i(T)$ is either symmetric, antisymmetric or there exists some j_i with $m_i = m_{j_i}$ and $P_{j_i}(T) = P_i'(T)$.

We want to make use of the fact that the minimal polynomial of an element in G is symmetric or antisymmetric. Thus suppose $f(T)$ is a symmetric or antisymmetric polynomial. Then we claim that $H(f(g)v, u) = H(v, \epsilon g^{-n} f(g)u)$ where n is the degree of $f(T)$ and $\epsilon = 1$ if f is symmetric and -1 it f is antisymmetric. We saw that the fact that f is symmetric (resp. antisymmetric) implies that $f(T) = f'(T) = T^n f(T^{-1})$ and therefore $f(g) = g^n f(g^{-1})$. Let $f(T) = x_n T^n + \ldots + x_0$ with $x_i = \epsilon x_{n-i}$ then we use the fact that ι is the adjoint map relative to the form H and see that

$$H(f(g)v, u) = \sum_{j=0}^{n} x_j H(g^j v, u) = \sum_{j=0}^{n} x_j H(v, \iota(g^j)u)$$

$$= H(v, f(g^{-1})u) = H(v, \epsilon g^{-n} f(g)u)$$

As an easy consequence we obtain

$$H(f(g)^i v, u) = H(v, \epsilon' g^{-in} f(g)^i u)$$

where $\epsilon' = -1$ if i is odd and f is antisymmetric and 1 else.

We may use this to decompose an A-module in subspaces that are pairwise orthogonal. Let (A, ι) be a simple k-algebra with involution, $g \in G$, $\mu_g(T)$ be the minimal polynomial of g and V be an A-module such that $A = \mathrm{End}_D(V)$. We know that $V = \bigoplus V_i$. Now define $q_i(T) = P_i(T)$ if $P_i(T)$ is symmetric or antisymmetric and define $q_i(T) = P_i(T)P'_{j_i}(T)$ else. Furthermore denote $V_i' = V_i$ if $q_i(T) = P_i(T)$ and $V_i' = V_i \oplus V_{j_i}$ if $q_i(T) = P_i(T)P_i'(T)$. Then we obtain some new decomposition $V = \bigoplus V_i'$. We want to show that $V_i' \perp V_j'$ for all $i \neq j$. To see this observe that $q_i(g)$ acts as an automorphism on V_j' for all $j \neq i$ as $q_i(T)$ and $q_j(T)$ are prime to each other. Thus for every $v \in V_i'$

there exists some $v' \in V_i'$ such that $p_j(g)v' = v$. This yields for all $v \in V_i'$ and $w \in V_j'$

$$H(v, w) = H(q_j(g)v', w) = H(v', \epsilon g^{-n} q_j(g)w) = H(v', 0) = 0$$

where n is the degree of $q_j(T)$. This is true because $V_i' = \{v \in V \mid q_j(g)v = 0\}$.

Suppose (A, ι) is a simple algebra with involution and consider the left A-module V such that $A = \operatorname{End}_D(V)$ for some division algebra D. Let $g \in G$ where G is the classical k-group in A induced by ι. Furthermore let $f(T)$ be a symmetric or antisymmetric element of $k[T]$ such that $f(g)$ is a nilpotent endomorphism of V. We want to use $f(g)$ to induce some selfdual flag. (For example if $f(T)^m = \mu_g(T)$ then these prerequisites are fulfilled.)
Let $f(T)$ be of degree n. Now define

$$V_l = \sum_{\substack{i,j \geq 0 \\ j-i \geq l}} \operatorname{Ker} f(g)^{i+1} \cap \operatorname{Im} f(g)^j.$$

Observe that a summand $i = -1$ is possible but as $\operatorname{Ker} f(g)^0 = \{0\}$ this summand does not change the entire sum.
As $\operatorname{Im} f(g)^0 = V$ and $\operatorname{Ker} f(g)^n = V$ we see that $V_{-n+1} = V$. On the other side if $l = n$ then $j - i \geq n$ implies that $j \geq n$ as $-i \leq 0$. ($-i = 1$ does not change the sum) Since $\operatorname{Im} f(g)^n = \{0\}$ this shows that $V_n = \{0\}$. If$j - i \geq l + 1$ then $j - i \geq l$ and therefore $V_{l+1} \subset V_l$. Thus

$$\{0\} = V_n \subset V_{n-1} \subset \ldots \subset V_{-n+2} \subset V_{-n+1} = V$$

Now we want to examine the action of $f(g)$ on V_l and we claim that $f(g)V_l \subset V_{l+2}$. Let $v \in \operatorname{Ker} f(g)^l$ this implies that $f(g)^l v = 0 = f(g)^{l-1} f(g)v$. Thus $f(g)v$ lies in $\operatorname{Ker} f(g)^{l-1}$. It is also clear that $f(g) \operatorname{Im} f(g)^l \subset \operatorname{Im} f(g)^{l+1}$. Thus

$$f(g) \sum_{\substack{i,j \\ j-i \geq l}} \operatorname{Ker} f(g)^{i+1} \cap \operatorname{Im} f(g)^j \subset \sum_{\substack{i,j \\ j-i \geq l}} \operatorname{Ker} f(g)^{i} \cap \operatorname{Im} f(g)^{j+1}$$

with the substitution $i' = i - 1$ and $j' = j + 1$ we obtain

$$\sum_{\substack{i',j' \\ j'-i' \geq l+2}} \operatorname{Ker} f(g)^{i'+1} \cap \operatorname{Im} f(g)^{j'} = V_{l+2}$$

We will need the following lemma that gives us some more information about V_l.

Lemma 3.6. *Let V be a right D-module and let $f(g)$ be a nilpotent endomorphism of V. Then*

$$\sum_{\substack{i,j\\ j-i\geq l}} \operatorname{Ker} f(g)^{i+1} \cap \operatorname{Im} f(g)^{j} = \bigcap_{\substack{i,j\\ j-i\leq l}} (\operatorname{Ker} f(g)^{i} + \operatorname{Im} f(g)^{j})$$

Proof: Both sides are right D-modules but as $f(g)$ is D-linear it is enough to proof their equality as vector spaces over the center K of D. Furthermore we may assume that V is a cyclic $f(g)$-module. Let $m = \dim_K(V)$ and choose a basis denoted by

$$e_{1-m}, \ldots, e_{m-1}$$

such that $f(g)e_s = e_{s-2}$ where $e_{-m-1} = 0$. Then

$$\operatorname{Ker} f(g)^{i} = \langle e_s \mid s \leq 2i - m - 1 \rangle$$

and

$$\operatorname{Im} f(g)^{j} = \langle e_s \mid s \leq m - 2j - 1 \rangle$$

Thus

$$\operatorname{Ker} f(g)^{i+1} \cap \operatorname{Im} f(g)^{j} = \langle e_s \mid s \leq \min(2i - m + 1, m - 2j - 1) \rangle$$

$$\operatorname{Ker} f(g)^{i} + \operatorname{Im} f(g)^{j} = \langle e_s \mid s \leq \max(2i - m - 1, m - 2j - 1) \rangle$$

Therefore

$$\sum_{\substack{i,j\\ j-i\geq l}} \operatorname{Ker} f(g)^{i+1} \cap \operatorname{Im} f(g)^{j} = \left\langle e_s \mid s \leq \max_{\substack{i,j\\ j-i\geq 1}} \min(2i - m + 1, m - 2j - 1) \right\rangle$$

$$\bigcap_{\substack{i,j\\ j-i\geq l}} (\operatorname{Ker} f(g)^{i} + \operatorname{Im} f(g)^{j}) = \left\langle e_s \mid s \leq \min_{\substack{i,j\\ j-i\geq 1}} \max(2i - m - 1, m - 2j - 1) \right\rangle$$

There are two cases. Case one $j + i \leq m - 1$. Then $2i - m - 1 \leq m - 2j - 1$ and $2i - m + 1 \leq m - 2j - 1$ and we obtain

$$\max_{\substack{i,j\\ j-i=1}} (2i - m - 1) = -l$$

$$\min_{\substack{i,j\\ j-i=l}} (m - 2j - 1) = -l$$

for every l.If $j + i \geq m$ and thus $2i - m - 1 \geq m - 2j - 1$ and $2i - m + 1 \geq m - 2j - 1$ then

$$\max_{\substack{i,j \\ j-i=1}} (m - 2j - 1) = -l - 1$$

$$\min_{\substack{i,j \\ j-i=l}} (2i - m - 1) = -l - 1$$

for every l. □

Then there exists the dual flag

$$\{0\} = V_{-n+1}^{\perp} \subset V_{-n+2}^{\perp} \subset \ldots \subset V_{n-1}^{\perp} \subset V_{n}^{\perp} = V$$

where $V_i^{\perp} := \{v \in V \mid H(v, w) = 0 \, \forall \, w \in V_i\}$.

Lemma 3.7. *If $f(T)$ is a symmetric (resp. antisymmetric) polynomial of exact degree m such that $f(g)$ is a nilpotent endomorphism on V then the flag that is induced by $f(T)$ in the way just described is selfdual relative to H. (i.e. $V_{-n+1+i}^{\perp} = V_{n-i)}$)*

Proof: We saw that $H(f(g)^j v, w) = H(v, \epsilon' g^{-jm} f(g)^j w)$. We claim that this implies that

$$\operatorname{Ker} f(g)^j = (\operatorname{Im} f(g)^j)^{\perp}$$

We first want to show that $\operatorname{Ker} f(g)^j \subset (\operatorname{Im} f(g)^j)^{\perp}$. So let $w \in \operatorname{Ker} f(g)^j$ and v be an arbitrary element in $\operatorname{Im} f(g)^j$. Then we see that

$$H(v, w) = H(f(g)^j v_1, w) = H(v_1, \epsilon' g^{-jm} f(g)^j w) = H(v_1, 0) = 0$$

Now we want to see that $(\operatorname{Im} f(g)^j)^{\perp} \subset \operatorname{Ker} f(g)^j$. So let $v \in (\operatorname{Im} f(g)^j)^{\perp}$ we want to see that $f(g)^j v = 0$. As H is nondegenerate we know that $H(f(g)^j v, u) = 0$ for all u implies that $f(g)^j v = 0$. So let u be an arbitrary element in V then $f(g)^j u \subset \operatorname{Im} f(g)^j$ and therefore

$$H(f(g)^j v, u) = H(v, \epsilon' g^{-jn} f(g)^j u) = 0$$

Thus the equation is shown. Now observe that for the orthogonal compliment we have the equation $(A + B)^{\perp} = A^{\perp} \cap B^{\perp}$ for A and B submodules of V. This implies that

$$(\sum_{\substack{i,j \\ j-i=l}} \operatorname{Ker} f(g)^{i+1} \cap \operatorname{Im} f(g)^j)^{\perp} = \bigcap_{\substack{i,j \\ j-i=l}} (\operatorname{Ker} f(g)^j + \operatorname{Im} f(g)^{i+1})$$

If we exchange $j-i=l$ by $j-i \geq l$ in the index of the sum it is obvious that we obtain $j-i \leq l$ in the index of the intersection. The substitution $j=i'$ and $i+1=j'$ shows that the intersection becomes

$$\bigcap_{\substack{i,j \\ j'-i'=-l+1}} (\operatorname{Ker} f(g)^{i'} + \operatorname{Im} f(g)^{j'})$$

Using lemma 3.6 we see that this is V_{-l+1} and therefore we obtain $V_{n-i}^{\perp} = V_{-n+1+i}$. □

Lemma 3.8. *In the above situation there exist subsets W_i of V such that $V_{i+1} \oplus W_i = V_i$ and $W_i \perp W_j$ for all $j \neq -i$.*

Proof: Set $W_{n-1} = V_{n-1}$. Then W_{n-1} is totally isotropic since $W_{n-1} \subset V_{-n+2} = V_{n-1}^{\perp}$ which follows from the selfduality of the flag. But then there exists some totally isotropic subspace U s.t. $U \cap W_{n-1} = \{0\}$, $\dim U = \dim W_1$ and the bilinear form H is nondegenerate on $U + W_1$. Set $W_{-n+1} = U$ then $W_{-n+1} + V_{-n+2} = V$ because $\dim W_{-n+1} + \dim V_{-n+2} = \dim V$ and $W_{-n+1} \cap V_{n-1}^{\perp} = \{0\}$. The last assertion follows form the fact that H is nondegenerate on $W_{n-1} + W_{-n+1}$.
Let $i \geq 0$. If W_{n-i} is known then define W_{-n+i} to be the totally anisotropic subspace s.t. $W_{-n+i} \cap W_{n-i} = \{0\}$ and $\dim W_{-n+i} = \dim W_{n-i}$. Now define $W_{n-i-1} = (\sum_{0 \leq j \leq i} W_{-n+j-1})^{\perp} \cap V_{n-i-1}$. Obviously $W_{n-i-1} \cap V_{n-i} = \{0\}$ because $W_{-n+i}^{\perp} \cap V_{n-i} = \{0\}$. Thus again by dimensional considerations we can see that $V_{n-i-1} = V_{n-i} + W_{n-i-1}$.
This inductively defines the W_i for all i. Finally we have to show that the subspaces defined this way satisfy $W_i \perp W_j$ for all $j \neq -i$. Still let w.l.o.g $i \geq 0$. If $j > -i+1$ this follows directly from the selfduality of the flag. Because $W_i \subset V_i \subset V_{-i+1} = V_i^{\perp}$. And since $j > -i+1$ we see that $W_j \subset V_{-i+1}$. If $j < -i+1$ then this follows directly from the construction. □

4 k-semisimple elements and pseudotori in classical k-groups

4.1 k-semisimple elements in classical k-groups

As the k-rational points of G are canonically embedded in the k-algebra A we can define an element $g \in G(k)$ to be k-semisimple if the image of g under the canonical embedding is a k-semisimple element of A. This means we make the following definition.

Definition. Let G be a classical k-group associated to the k-algebra A with involution. Then an element $g \in G(k)$ is called k-semisimple if the subalgebra $k[g] \subset A$ that is generated by g is semisimple.

If we restrict A to the set $\{x \in A | x\iota(x) = 1\}$ then lemma 2.3 shows that an element x is k-semisimple in A if and only if the k-algebra with involution $(k[x], \iota_{k[x]})$ is a semisimple k-algebra with involution. Thus for a k-semisimple element g in a classical group G associated to a semisimple k-algebra with involution (A, ι) the algebra $k[g]$ is not only a semisimple k-algebra but a semisimple k-algebra that is invariant under ι.
We want to find an equivalent property for k-semisimplicity in the case of classical k-groups that might replace our definition and extend it to arbitrary linear algebraic k-groups.

Let C_1 and C_2 be conjugacy classes in G that contain k-rational elements. Then we say that $C_1 \leq C_2$ if $\overline{C_1} \subset \overline{C}_2$. In particular we call a conjugacy class k-minimal if its closure contains no other conjugacy classes that contain k-rational elements.
A special case of the following theorem can already be found in an unpublished manuscript by Werner Hoffmann.

Theorem 4.1. *Let G be the classical k-group associated to the semisimple k-algebra with involution (A, ι) and let $g \in G$ be a k-rational element. Then there exists some k-semisimple k-rational element $g_1 \in G$ such that $\overline{C}_{g_1} \leq \overline{C}_g$.*

Proof: If we can see that there exists some k-semisimple k-rational element $g_1 \in \overline{C_g}$ then this implies that the whole conjugacy class C_{g_1} lies in $\overline{C_g}$. ($g_1 \in \overline{C_g} = \bigcap_{S \supset C_g} S$ where S are closed sets. Then for all such S we have aSa^{-1} is closed and contains C_g. This implies that $ag_1a^{-1} \in \overline{C_g}$).

$G(k)$ is embedded in the semisimple k-algebra A and we saw that w.l.o.g. we may assume (A, ι) is a simple k-algebra with involution. (else $G = G_1 \times \dots G_n$ for G_i a classical k-group associated to a simple k-algebra with involution $(A_i, \iota_{|A_i})$ for every i.) By the theorem of Artin-Wedderbrun we know that we furthermore may assume that there exists some A-module V such that $A = \mathrm{End}_D(V)$ for some division algebra D. As the isomorphism from A to $\mathrm{M}_n(D)$ is a k-algebra isomorphism it maps k-semisimple elements on k-semisimple elements. Therefore we can say that G is isomorphic to some subgroup of $\mathrm{GL}_D(V)$. Again using the theory of elementary divisors we can see that V is a direct sum of cyclic primary $k[T]$-modules V_i.

We saw that we may also decompose $V = \bigoplus V'_i$ where the V'_i are pairwise orthogonal. Thus again we can simplify the situation and assume that $V = k[T]/(f(T)^m)$ for some symmetric or antisymmetric polynomial $f(T) \in k[T]$ and some $m \in \mathbb{N}$. As $f(T)^m$ is symmetric or antisymmetric lemma 3.7 yields a selfdual flag. But then with the help of lemma 3.8 we see that $V \cong \bigoplus_{-n}^{n} W_i$ s.t. $W_i \perp W_j$ for all $j \neq -i$ (with respect to the sesquilinearform H that is induced by the involution ι). Next we define a cocharacter $\lambda : k^\times \to \mathrm{GL}_D(V)$. The action on each component W_i is given by $\lambda(u)_{|W_i} := u^i$. Let $v = \sum_i v_i$, $w = \sum_i w_i$ be two arbitrary elements in V with v_i and $w_i \in W_i$ for all i then we have

$$\begin{aligned} H(\lambda(u)v, \lambda(u)w) &= \sum_i H(\lambda(u)v_i, \lambda(u)w_{-i}) \\ &= \sum_i H(u^i v_i, u^{-i} w_{-i}) \\ &= \sum_i H(v_i, w_{-i}) = H(v, w) \end{aligned}$$

Therefore $\lambda(u) \in G$ for all $u \in k^\times$ and therefore $\lambda(u^{-1})g\lambda(u) \in C_g$ for all $u \in k^\times$. We claim that we can extend the map $u \to \lambda(u^{-1})g\lambda(u)$ to the whole of k and that the element $g_1 := \lambda(0^{-1})g\lambda(0) \in \overline{C_g}$ is k-semisimple.

To see that this is true we need to consider $\lambda(u)^{-1}g\lambda(u)$. Decompose $g \in \mathrm{End}_D(V) = \bigoplus_{i,j} \mathrm{Hom}_D(W_j, W_i)$ into its components g_{ij}. Then $(gw)_i = \sum_j g_{ij} w_j$ and $g_{ij} = 0$ for all $i > j$. This is true because the selfdual flag we considered to construct W_i is invariant under G. As the flag was indexed decreasingly i.e. the biggest A-module was the one with the lowest index, and W_i is not contained in some D-module of the flag with index higher then i we can see that $g_{ij} = 0$ for $i > j$. Therefore $(\lambda(u^{-1})g\lambda(u))_{ij} = u^{j-i} g_{ij}$.

As $g_{ij} = 0$ if $i > j$ this is well defined for all $u \in k$. Furthermore g_1 acts as diagonal matrix as $(\lambda(0)^{-1} g \lambda(0))_{ij} = 0$ for all $i \neq j$. Therefore it is k-semisimple. Furthermore $g_1 \in \overline{C_g}(k)$ and in particular $g_1 \in G$.

□

Theorem 4.2. *Let G be the classical k-group $\mathrm{GL}_n(k)$. Then the k-minimal conjugacy classes that contain k-rationale elements are the k-semisimple ones.*

Proof: We just saw that the closure of every conjugacy class contains some k-semisimple k-rational element and thus all that needs to be shown is that the k-semisimple conjugacy classes are minimal.
Thus let g_0 be k-semisimple with minimal polynomial $\mu_{g_0}(T) = \prod_{i=1}^n P_i(T)$ and let C_{g_0} be the conjugacy class of g_0. At first we want to see that $\phi_i : \overline{C}_{g_0} \to \mathbb{N}$ that is defined by $\phi_i(g) = \dim \operatorname{Ker} P_i(g)$ is upper semi-continuous for all i. It is clear that the function ϕ_i is upper semi-continuous if and only if the function $g \to \dim \operatorname{Im} P_i(g)$ is lower semi-continuous. The dimension of the image of $P_i(T)$ equals the rank of the matrix that corresponds to the endomorphism $P_i(T)$. The rank is the maximal order of a minor that is not equal to zero. Thus consider the open subset of elements such that this minor is not zero. In this neighbourhood the rank could only get bigger but not smaller and thus ϕ_i is upper semi-continuous.
The minimal polynomial annihilates all elements in $\overline{C}_{g_0}$. This is true since the associated topology is the Zariski topology and $P_1(g) \cdots P_s(g) = 0$ for all $g \in C_{g_0}$. The dimensions of the primary components V_i have to add up to dim$V$ on $\overline{C}_{g_0}$ and as the dimension is a upper semi-continuous function it also has to be a lower semi-continuous function. Therefore the dimension of the primary components is continuous on $\overline{C}_{g_0}$ and since it is constant on C_{g_0} it is also constant on $\overline{C}_{g_0}$.
A $k[T]$-module annihilated by $P_i(T)$ is a $k[T]/(P_i(T))$-vector space and thus is determined up to isomorphism by its dimension. Therefore any two k-rational elements of $\overline{C}_{g_0}$ define isomorphic $k[T]$-modules, and an isomorphism is given by $h \in \mathrm{GL}_k(V)$ that conjugates one to the other. Therefore there exists no k-rational $g \in C_{g_0}$ such that $\overline{C}_g$ is a proper subset of $\overline{C}_{g_0}$ and thus the conjugacy classes of k-rational, k-semisimple elements are k-minimal.

□

If one tries to generalise this theorem to arbitrary classical k-groups one faces different problems. One problem is that the fact that the dimensions of the

primary components is constant on $\overline{C}_{g_0}$ does not imply that the primary components are isomorphic as $k[T]$-D-bimodules.
The second problem is that the conjugating element h need not lie in the classical k-group G if $G \neq \mathrm{GL}_n$.
If these problems were solved then this theorem would give rise to a new definition for k-semisimplicity of elements in arbitrary linear algebraic k-groups. Anyway this new definition is not very handsome since it is not easy to check whether a conjugacy class is minimal or not.

Lemma 4.1. *Let $\mu : G_1 \to G_2$ be a closed surjective morphism of topological groups. Then μ maps minimal conjugacy classes to minimal conjugacy classes.*

Proof: Let C be a minimal conjugacy class. It is clear that the image of a conjugacy class under a surjective group morphism is a conjugacy class. Therefore we only have to check the minimality.
Since μ is closed $\mu(\overline{C})$ is closed and thus $\overline{\mu(C)} \subset \mu(\overline{C})$. On the other hand $\mu(\overline{C}) \subset \overline{\mu(C)}$ since μ is continuous and thus $\mu(\overline{C}) = \overline{\mu(C)}$.
If $\mu(C)$ was not minimal then there existed some conjugacy class C_1 such that $\overline{C_1} \subsetneq \overline{\mu(C)} = \mu(\overline{C})$ but then $\mu^{-1}(\overline{C_1})$ was a union of closed conjugacy classes in $\overline{C}$ which is a contradiction to the minimality of C. □

In our special case we have to consider two different topologies. The classical k-group G which is in particular an algebraic k-group is initially defined over the algebraically closed field $\overline{k}$ and thus its topology $\mathcal{T}_{\overline{k}}$ is the Zarisky topology that comes from the algebra of polynomials $\overline{k}[G]$. But we examine the algebraic k-group G. This group is provided with the Zarisky topology $\mathcal{T}_k$ that comes from $k[G]$ and this topology is in fact a subtopology of the first one.
It is obvious that a morphism that is closed relative to $\mathcal{T}_{\overline{k}}$ need not be closed relative to $\mathcal{T}_k$.

Lemma 4.2. *Let G be a classical k-group and let μ be a surjective map with finite kernel to a k-group G_1. Then μ is closed relative to $\mathcal{T}_k$.*

Proof: Denote by p the projection from G to $G/\mathrm{ker}\mu$ where the latter is provided with the quotient topology. Then p is continuous by definition and furthermore it is closed. To see this let $\mathcal{O}$ be a closed set in G. Then the image under p is $\mathcal{O}\mathrm{ker}\mu$. Since $\mathrm{ker}\mu$ is finite this set is closed as a finite union of closed sets. Let ϕ be the isomorphism $G/\mathrm{ker}\mu \to G_1$. Since p and

μ are defined over k it is clear that ϕ is also defined over k. But if ϕ is a k-isomorphism then ϕ^{-1} is also a k-isomorphism and thus in particular continuous. But then ϕ is closed.
This finally yields that μ as a composition of two closed morphisms is closed itself. □

4.2 Definition and standard example of k-pseudotori

When dealing with semisimple elements in linear algebraic groups, tori play a significant role. Since k-semisimple elements are a generalisation of semisimple elements we obtain a generalisation of tori by changing the conditions. This gives rise to the following definition.

Definition. Let G be the classical k-group associated to the k-algebra with involution $(A\iota)$. A connected commutative k-subgroup Q of G will be called a k-pseudotorus if every k-rational element of Q is k-semisimple.

It is apparent that any torus is a k-pseudotorus but not every k-pseudotorus is a torus.

Example. Once again consider the classical k-group GL_p in the simple k-algebra $A = M_p(k)$ and take a look at the element $g_a \in \mathrm{GL}_p(k)$ given by

$$g_a = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & \cdots & 0 & 1 \\ a & & \cdots & 0 & 0 \end{pmatrix}$$

where a has no p'th root in k. We already saw that this element is k-semisimple but not semisimple. The set $k[g_a]\backslash\{0\}$ is obviously commutative and we will see that it is a k-subgroup of $\mathrm{GL}_p(k)$. Furthermore it will be shown that every element in this set is k-semisimple. Thus every k-rational element in $\overline{k}\otimes k[g_a]\backslash\{0\}$ is k-semisimple. It is obvious that $k[g_a]$ is isomorphic to the field extension $k(u)$ of k where u is the p'th root of a in $\overline{k}$. Therefore we know that $\mathrm{GL}_p(k) \cap k[g_a] \cong k[g_a]^\times$ and we know that $k[g_a]^\times$ is an irreducible variety ($K^\times$ is an irreducible variety for every field K). Therefore $\mathrm{GL}_p(k) \cap k[g_a]$ is connected and hence $\overline{k} \otimes k[g_a] \cap \mathrm{GL}_p$ is a k-pseudotorus. Because g_a is not semisimple it is not a torus and thus this is an example for a k-pseudotorus that is no torus.

In addition we will see that the centralizer $Z_A(g_a)$ also equals $k[g_a]$ and this will show that $k[g_a]\backslash\{0\}$ is in fact a maximal k-pseudotorus.

We want to calculate the determinant of an arbitrary element in $k[g_a]$ and see that any element in $k[g_a]$ that is not equal to 0 is invertible.

Lemma 4.3. *Consider a k-rational element $g \in A$ with $\mu_g(T) = T^{p^n} - a$ where a has no p'th root in k and*

$$k[g]\backslash\{0\} = x_0 + x_1 g + \dots x_{p^n-1} g^{p^n-1}$$

with $x_i \in k$. Then for any $g_0 \in k[g]$ with $g_0 = x_0 + x_1 g + \dots x_{p^n-1} g^{p^n-1}$ we have $\det(g) = x_0^{p^n} + x_1^{p^n} a + \ldots + x_{p^n-1}^{p^n} a^{p^n-1}$. *In particular this implies that* $\det(g_0) \neq 0$ *and thus g is invertible.*

Proof: Consider the indices of the matrix entries modulo p and denote by C the set of cyclic shifts. Then

$$\sum_{\sigma \in C} \mathrm{sgn}(\sigma) \prod_{i=0}^{p-1} g_{i\sigma(i)} = x_0^{p^n} + x_1^{p^n} a + \dots x_{p^n-1}^{p^n} a^{p^n-1}$$

for g_{ij} the matrix entries of g_0. Thus all that needs to be shown is that all the other summands that contribute to the Leibniz formula for determinants sum up to zero. To see this let C act on the symmetric group by conjugation. Then the C-conjugacy class of any element that is not in C has p^n elements and each of these permutations yields the same summand. Since the field has characteristic p this equals 0.
Suppose $\det(g_0) = 0$. Then $x_0^{p^n} + a(x_1^{p^n} + \dots x_{p-1}^{p^n} a^{p^n-2}) = 0$ but since a has no p'th root in k this implies that $x_0 = 0$. Since $a \neq 0$ this is equivalent to $x_1^{p^n} + \dots x_{p^n-1}^{p^n} a^{p^n-2} = 0$. Now it follows inductively that all $x_i = 0$. □

This shows in particular that any element in $k[g_a]$ has an inverse.

Theorem 2.1 shows that the algebra $k[g]$ is semisimple and it is commutative and thus by lemma 2.6 it is a direct sum of fields. Lemma 2.3 shows that the inverse is also in $k[g] \cap G(k)$ and thus $k[g] \cap G(k)$ is a group.

Corollary 4.1. *Let G be the classical k-group associated to the semisimple k-algebra with involution (A, ι) and let $g \in G(k)$ be a k-semisimple element. Then any element in $k[g]$ is k-semisimple.*

Proof: Lemma 2.6 shows that $k[g]$ is a direct sum of fields. Suppose $g_0 \in k[g]$ was not k-semisimple then the minimal polynomial $\mu_{g_0}(T)$ of g_0 was not square-free. Let $\mu_{g_0}(T) = Q(T)P(T)^n$ for some natural number $n > 1$ and some polynomials $Q(T)$ and $P(T)$. Then the element $Q(g_0)P(g_0)$ lies in $k[g]$, it is not 0 and it is obviously nilpotent. But there exist no nilpotent elements in a direct sum of fields. □

In particular this shows that any element in $k[g_a]$ is k-semisimple.

Lemma 4.4. *Let Q be a k-pseudotorus in the classical k-group G associated to the semisimple k-algebra with involution (A, ι). Then $k[Q(k)]$ is a direct sum of fields.*

Proof: Since Q is commutative the k-algebra $k[Q(k)]$ is also commutative and thus all that needs to be shown is that $k[Q(k)]$ is a semisimple k-algebra. But $k[Q(k)] = \sum_{g \in Q(k)} k[g]$ and every $g \in Q(k)$ is k-semisimple. Therefore $k[g]$ is a semisimple k-algebra for every $g \in Q(k)$ and thus $k[Q(k)]$ is a semisimple k-algebra. □

Thus if we want to see that $k[g_a] \backslash \{0\}$ is a k-pseudotorus all that is left to show is that $k[g_a]$ is a k-group. Again we do this in a more general setting.

Theorem 4.3. *Let G be the classical k-group associated to the semisimple k-algebra with involution (A, ι). If $g \in G(k)$ is a k-semisimple element then $\overline{k} \otimes k[g] \cap G$ is also a classical k-group.*

Proof: As $g \in G(k)$ fulfils $g\iota(g) = 1$ we may apply lemma 2.3 that shows that $k[g]$ is a semisimple k-algebra with involution. Thus $k[g] \cap G(k)$ is the set of all elements a in a semisimple k-algebra with involution that fulfil $a\iota(a) = 1$. This defines a classical k-group. □

Remark:
Actually the same proof shows that for an arbitrary k-pseudotorus Q in the classical k-group G that is associated to the semisimple k-algebra with involution (A, ι) the group $k[Q(k)] \cap G(k)$ is invariant under ι. As $k[Q(k)]$ is a direct product of field extensions of k it is clear that any element in $k[Q(k)]$ is k-semisimple. This implies that $((\overline{k} \otimes k[Q(k)]) \cap G)^0$ is also a k-pseudotorus. Finally we have seen that the group $(\overline{k} \otimes k[g_a]) \cap G = \overline{k} \otimes k[g_a] \backslash \{0\}$ is in fact a k-pseudotorus. Actually we have seen even more.

Corollary 4.2. *Let G be the classical k-group associated to the semisimple k-algebra with involution (A, ι) and let $g \in G(k)$ be a k-semisimple element then $((\overline{k} \otimes k[g]) \cap (G))^0$ is a k-pseudotorus.*

Proof: The algebra $\overline{k} \otimes k[g]$ is abelian. Furthermore corollary 4.1 shows that any $g_0 \in k[g]$ is k-semisimple and thus every k-rational element in $\overline{k} \otimes k[g]$ is k-semisimple. Theorem 4.3 shows that $k[g] \cap G(k)$ is a classical k-group and thus the identity component is in particular a connected k-group. □

4.3 Maximal k-pseudotori

In the theory of linear algebraic groups or Lie groups maximal tori play an important role and thus it seems reasonable to examine maximal k-pseudotori. As in the case of tori we will say a k-pseudotorus Q is maximal if for every k-pseudotorus Q_0 with $Q \subset Q_0$ we have $Q = Q_0$.
We defined the notion of a k-regular element in a k-algebra with involution and now we want to give a definition for k-regularity in a classical k-group G.

Definition. A k-semisimple element g in the classical k-group G is called k-regular if $\dim Z_G(g)$ is minimal.

This definition is closely related to the notion of a regular element in a linear algebraic group as it is given for example in [Bor91] (12.2).
To deal with this definition we want to give some informations about the Lie algebra of a classical k-group. Thus let G be a classical k-group in the semisimple k-algebra with involution (A, ι). We know that this means that

$$G := \{g \in A \mid g\iota(g) = 1\}.$$

Then the Lie algebra $\mathfrak{g}$ of G is given by

$$\mathfrak{g} = \{x \in A \mid \iota(x) = -x\} \tag{6}$$

and therefore the Lie algebra of the classical k-group G equals the eigenspace A^- of ι to the eigenvalue -1 in A. The dimension of G equals the dimension of A^-.

As G is canonically embedded in A we want to see that the notion of k-regularity of g considered as an element of G corresponds to the notion of

k-regularity of g considered as an element of the semisimple k-algebra A. We will assume without loss of generality that A is a central simple k-algebra.(else consider the simple summands over the center of A)
Thus let g be a k-semisimple element. We want to see that $\dim Z_G(g)$ is minimal if and only if the algebra $k[g]$ is a maximal commutative k-subalgebra. By theorem 2.4 (if necessary applied on the single simple summands) it is clear that the dimension of $Z_A(k[g])$ is minimal if and only if the dimension of $k[g]$ is maximal. Thus $Z_A(k[g])$ is minimal under all $g \in G$ if $k[g]$ is maximal under all $g \in G$ i.e. it is maximal under all ι-invariant commutative semisimple k-algebras. Thus we need lemma 2.3 to see that the $k[g]$ are maximal among all commutative semisimple k-algebras. As $Z_G(g) = Z_A(g) \cap G$ we know that in particular $\dim(Z_G(g)) = \dim(Z_A(g))$. Furthermore $Z_A(k[g]) = Z_A(g)$ and thus by theorem 2.4 the equivalence of the two definitions follows.

We claimed that $k[g_a]\backslash\{0\}$ is an example for a maximal k-pseudotorus. To see this we want to examine the centralizer of k-regular elements. We saw in lemma 2.8 that for a k-regular element a we have $Z_A(a) = k[a]$. Thus if we can see that g_a is a k-regular element then it is clear that

$$Z_A(g_a) = \left\{x_0E + x_1g_a + x_2g_a^2 + \cdots + x_{p-1}g_a^{p-1} \mid x_i \in k\right\}.$$

As the dimension of $k[g_a]$ over k is p and the dimension of $A = M_p(k)$ over k is p^2 lemma 2.7 shows that g_a is k-regular and therefore $Z_A(g_a) = k[g_a]$.

Corollary 4.3. *Let G be the classical k-group associated to the semisimple k-algebra with involution (A, ι). If $g \in G^0$ is a k-regular k-semisimple element then $((\overline{k} \otimes k[g]) \cap G)^0$ is a maximal k-pseudotorus.*

Proof: As g is k-regular the set $\overline{k} \otimes k[g] \cap G$ is the maximal set of elements in $\overline{k} \otimes A \cap G$ that commute with g. We saw that $((\overline{k} \otimes k[g]) \cap G)^0$ is a k-pseudotorus by corollary 4.2 and thus it is a maximal k-pseudotorus.

□

Remark:
Actually we can see that for $g \neq 1$ the last corollary implies that the maximal k-pseudotorus $(\overline{k} \otimes k[g] \cap G)^o$ is not trivial. This follows directly from the fact that $(\overline{k} \otimes k[g]) \cap G$ is a classical k-group and thus in particular a linear algebraic k-group. For linear algebraic k-groups G_0 it is known that G_0/G_0^0

is finite. But as $(\overline{k} \otimes k[g]) \cap G$ is not trivial this implies that $((\overline{k} \otimes k[g]) \cap G)^0$ is not trivial.

We can show that every maximal k-pseudotorus Q is the identity component of a classical k-group. To do so use lemma 4.4. In the proof of this lemma we saw that $k[Q(k)]$ is a semisimple k-algebra. Since $Q(k)$ is invariant under ι the algebra $k[Q(k)]$ is also invariant under ι and thus we have a semisimple k-algebra with involution. Suppose $((\overline{k} \otimes k[Q(k)]) \cap G)^0 \neq Q$. We saw in the remark of theorem 4.3 that $((\overline{k} \otimes k[Q(k)]) \cap G)^0$ is a k-pseudotorus. Furthermore it contains Q and since Q is a maximal k-pseudotorus this implies that $((\overline{k} \otimes k[Q(k)]) \cap G)^0 = Q$. As $k[Q(k)]$ is a semisimple k-algebra that is invariant under ι and $G(k)$ is the set of elements with $g\iota(g) = 1$ it is obvious that $(\overline{k} \otimes k[Q(k)]) \cap G$ is a classical k-group. But then Q is the identity component of a classical k-group.

Theorem 4.4. *Let Q be a pseudotorus in the classical k-group G associated to the semisimple k-algebra with involution (A, ι). Then Q lies in a pseudotorus of maximal dimension.*

Proof: Denote by Z the center of A and by L a maximal commutative semisimple Z^+-subalgebra such that $Q \subset L$. We know that Q lies in the classical k-group that is associated to $(L, \iota_{|L})$ and that this classical group is a direct sum of classical groups associated to the simple algebras with involution L_i.
Lemma 2.7 shows that for $L = \bigoplus_i L_i$ a maximal commutative semisimple subalgebra we have $\dim_Z(L) = \sqrt{\dim_Z(A)}$. If $\iota(L_i) = L_i$ then there are two possibilities. If ι acts trivial on L_i then $\dim_Z L_i^- = 0$. If ι does not act trivial then L_i^+ is a subfield of L_i and it is well known that L_i is a quadratic Galois extension of L_i^+. But then $\dim_Z L_i^- = \frac{1}{2}\dim_Z L_i$. If $\iota(L_i) = L_j$ for some $i \neq j$ then we saw that ι interchanges the entries of L_i and L_j and thus it is clear that $\dim_Z(L_i \oplus L_j)^- = \dim_Z(L_i)^- = \dim_Z(L_j)^-$. In particular this shows the following:
If $\sum_i \dim_Z(L_i) = \sqrt{\dim_Z(A)}$ is even then the Z-dimension of the sum L_ι of all L_i that are invariant under ι is also even. If $\sqrt{\dim_Z(A)}$ is odd then this dimension is also odd.
Combining these informations yields that $\dim_{Z^+} L^- \leq [\frac{1}{2}[Z : Z^+]\sqrt{\dim_Z A}]$ where the outer bracket is the floor function. Therefore Q_0 is a pseudotorus of maximal dimension if its dimension over Z^+ is $[\frac{1}{2}[Z : Z^+]\sqrt{\dim_Z A}]$.
If ι acts trivial on L_i then the corresponding classical k-group is finite and

thus its identity component is trivial. Therefore we delete these summands. We denote the remaining sum by L'. As 1 need not lie in L' anymore instead of this we consider $L' + Z^+$. Actually this sum is isomorphic to the direct sum $Z^+ \oplus L'$. This is true as $L_i \cap Z^+$ is a subfield and therefore an ideal. As both are simple we know that $L_i \cap Z^+ = L_i$ or $L_i \cap Z^+ = Z^+$ for all i. This sum is a semisimple commutative subalgebra and if the Z-dimension of L_ι is bigger then 1 then the Z-dimension of this algebra is smaller then the Z-dimension of L. If this is the case then it is not maximal and we may apply the lemma 2.10 and obtain a maximal commutative semisimple subalgebra L_0 such that $L_0^- \neq (L' \oplus Z^+)^-$. Thus we know that $\dim_Z(L_{0\iota}) \leq \dim_Z(L_\iota) - 2$.
The classical group Q_0 that is associated to the commutative semisimple subalgebra with involution L_0 is a pseudotorus. And as $\dim_{Z^+} L_0^- \geq \dim_{Z^+} L^-$ the dimension of Q_0 is bigger then the dimension of Q. If the dimension of L_0^- is not equal to $[\frac{1}{2}[Z : Z^+]\sqrt{\dim_Z A}]$ then $\dim_Z(L_{0\iota}) > 1$ and we may repeat the procedure. □

4.4 k-reductivity and k-pseudotori

Definition. Let G be a classical k-group.

1. The k-radical $\mathcal{R}_k(G)$ of G is the maximal, connected, solvable, normal k-subgroup of G.

2. The unipotent k-radical $\mathcal{R}_{u,k}(G)$ is the maximal, connected, unipotent, normal k-subgroup of G.

3. A k-reductive group (or pseudo-reductive k-group) is a connected classical linear algebraic group such that $\mathcal{R}_{u,k}(G)$ is trivial.

Remarks:

1. It is clear that any reductive group is also pseudo-reductive but the converse is not true. (see example)

2. As any unipotent group is in particular solvable we know that $\mathcal{R}_{u,k}(G) \subset \mathcal{R}_k(G)$.

Example. We will see in this chapter that any k-pseudotorus is k-reductive. This implies that in particular our standard example for a k-pseudotorus namely $k[g_a] \setminus \{0\}$ is k-reductive. But this group is not reductive as the subgroup that is generated by $\frac{1}{u} g_a$ where u is again the p'th root of a is unipotent. Furthermore it is a normal subgroup as $k[g_a] \setminus \{0\}$ is a commutative group.

Lemma 4.5. *Let G be a classical k-group. If there exists some nontrivial unipotent k-subgroup U in $\mathcal{R}_k(G)$ then this implies that G is not k-reductive.*

Proof: The k-radical $\mathcal{R}_k(G)$ is a k-subgroup of the radical $\mathcal{R}(G)$. We know that the unipotent radical $\mathcal{R}_u(G)$ is the set of unipotent elements in $\mathcal{R}(G)$. If there exists a nontrivial k-subgroup U in $\mathcal{R}_k(G)$ then there exists a nontrivial k-subgroup in the unipotent radical $\mathcal{R}_u(G)$. But lemma 14.4.6 in [Spr09] says that G is k-reductive if and only if there exists no nontrivial k-subgroup in $\mathcal{R}_u(G)$. □

We will need the well known theorem of Lie-Kolchin several times. But before using it we want to state it here.

Theorem 4.5. *(Lie-Kolchin) Assume that G is a closed solvable algebraic subgroup of GL_n. Then there exists some $x \in \mathrm{GL}_n$ such that xGx^{-1} is a subgroup of $\boldsymbol{T}_n$.*

For a proof see for example [Spr09] (theorem 6.3.1.).

The next lemma will show that the k-radical and the unipotent k-radical of a connected algebraic k-group are invariant under any automorphism of the group and therefore they are characteristic subgroups. Actually this also follows as they are defined canonically..

Lemma 4.6. *Let H, H' be connected linear algebraic groups and $\pi : H \to H'$ a surjective morphism. Then $\pi(\mathcal{R}(H)) = \mathcal{R}(H')$ and $\pi(\mathcal{R}_u(H)) = \mathcal{R}_u(H')$.*

This lemma and the proof of it can be found in [Bor91] (Chapter IV §14 Corollary 14.11). Denote the normalizer of $G(k)$ in $A^\times$ by $N_A(G(k))$. Then in particular $\mathcal{R}_k(G)(k)$ and $\mathcal{R}_{u,k}(G)(k)$ are normal subgroups in $N_A(G(k))$.

Lemma 4.7. *Let G be a classical k-group associated to the semisimple k-algebra with involution (A, ι) such that the k-linear span of $N_A(G(k))$ is A, then G is k-reductive.*

Proof: As $G = G_1 \times \ldots \times G_n$ for G_i classical k-groups in simple k-algebra with involution we may assume that G itself is a classical k-group in the simple k-algebra A with involution. Choose a simple A-module V and let W be the subspace of vectors fixed by $\mathcal{R}_{u,k}(G)(k)$. In fact, the composition of $\mathcal{R}_{u,k}(G)(k) \times V \to V$ restricts to a k-linear map $V^* \to k[\mathcal{R}_{u,k}(G)(k)] \times V^* = \mathrm{Hom}_k(V, k[\mathcal{R}_{u,k}(G)(k)])$, and W is the set of vectors on which the image of every element of V^* evaluates to a constant. By the theorem of Lie-Kolchin, $W \otimes \overline{k}$ is nonzero, hence so is W. Since $\mathcal{R}_{u,k}(G)(k)$ is normal in $N_A(G(k))$, W is stable under that group, and since the latter spans A, W is an A-submodule. As V is simple this implies that $W = V$ and therefore $\mathcal{R}_{u,k}(G)$ is trivial. □

In particular this last lemma shows that a classical k-group G is always k-reductive if $k[G(k)]$ is a semisimple k-algebra.

We know that the following equivalence is true.
A subgroup of G is a torus if and only if it is a connected commutative reductive subgroup. Thus it seems likely to suppose that a similar statement is true for k-pseudotori and pseudo-reductivity. Thus our next goal is to proof the equivalence:
A k-subgroup of G is a k-pseudotorus if and only if it is a connected, commutative k-reductive k-subgroup.

At first we want to show that a connected, commutative k-reductive k-group is always a k-pseudotorus.
We will need some adjusted version of the exponential map for the case of fields with characteristic not zero. So let A be a commutative k-algebra and denote by N a nilpotent ideal in A. We know that the map $\exp(X) = \sum_{i=0}^{\infty} \frac{1}{i!} X^i$ is a group morphism from the additive group N to the group of unipotent elements if the characteristic of k is zero. However, this morphism is not defined for $\mathrm{char}(k) \neq 0$ since $\frac{1}{i!}$ is not defined for $i \geq p$. We can avoid this problem by restricting the domain of the function $\exp(X)$. For this purpose define

$$N_k := \{x \in N \mid x x_1 \dots x_{k-1} = 0 \, \forall \, x_1, \, \dots, \, x_{k-1} \in N\} .$$

Then N_k is a k-subalgebra of N. Let n be the smallest number such that $N^n = \{0\}$ (i.e. the smallest number such that the product of n elements in N is zero). Such a number exists since N is a nilpotent ideal. Then we have $N_1 = \{0\}$, $N_k = N$ for all $k \geq n$ and $N_i \subset N_j$ if $i \leq j$. We claim that N_k is not trivial if N is not trivial for $k > 1$. If $k \geq n$ then $N_k = N$ and the assertion is proven. Thus suppose $k < n$. Since n is the smallest number such that $N^n = 0$ there exist $x_1, \dots, x_{n-1} \in N$ such that $x_1 \cdot \ldots \cdot x_{n-1} \neq 0$. As $N^n = \{0\}$ we know that $x_1 \cdot \ldots \cdot x_{n-1} x = 0$ for all $x \in N$ and thus $x_1 \cdot \ldots \cdot x_{n-1} \in N_2$. Since $N_2 \subset N_k$ for all $k \geq 2$ we see that N_k is not trivial

if N is not trivial.
Now we want to consider N_p.

Lemma 4.8. *The map* $\exp_p(x) = \sum_{i=0}^{p-1} \frac{1}{i!} x^i$ *is an injective* k*-group morphism from the additive* k*-group* N_p *to some subgroup of the multiplicative group of all unipotent elements.*

Proof: We want to start by showing that $\exp_p$ is a group morphism. It is obvious that $\exp_p(0) = 1$. Furthermore an easy calculation shows that

$$\exp_p(x+y) = \sum_{i+j<p} \frac{x^i y^j}{i!j!}$$

and that

$$\exp_p(x)\exp_p(y) = \sum_{i<p,\, j<p} \frac{x^i y^j}{i!j!}.$$

Since $x^i y^j = 0$ if $i + j \geq p$ these two sums are equal and $\exp_p$ is a group morphism.
As $\exp_p(x)^p = \sum_{i=0}^{p-1} (\frac{1}{i!})^p x^{pi} = 1$ the image is unipotent.
Now suppose $\exp_p$ was not injective. Then there exists some $x \in N_p$ such that

$$\exp_p(x) = \sum_{i=0}^{p-1} \frac{1}{i!} x^i = 1$$

and thus

$$\sum_{i=1}^{p-1} \frac{1}{i!} x^i = x \sum_{i=0}^{p-2} \frac{1}{(i+1)!} x^i = 0.$$

But $\sum_{i=0}^{p-2} \frac{1}{(i+1)!} x^i$ is unipotent and thus in particular invertible and therefore $x = 0$.
Finally $\exp_p$ is defined over k since it is just a polynomial with coefficients in k. □

This group morphism enables us to proof our claim.

Theorem 4.6. *Let* G *be a* k*-reductive classical* k*-group associated to the* k*-algebra with involution* (A, ι)*. Then* G *is a* k*-pseudotorus if and only if it is commutative and connected.*

Proof: Any k-pseudotorus is by definition commutative and connected. Thus only the other direction needs to be shown here.
Suppose G is connected and commutative then it suffices to show that any k-rational element in G is k-semisimple to see that G is a k-pseudotorus. Suppose $x \in G(k)$ is not k-semisimple then the k-algebra $k[x]$ that is generated by x is not semisimple. Thus the nilpotent radical $N(x)$ in $k[x]$ is not trivial. Since $k[x]$ is commutative and Artinian $N(x)$ is a nilpotent ideal in $k[x]$. Thus $N(x)$ is a nilpotent non trivial ideal and hence $N_p(x)$ is not trivial. But then the image $U(x)$ of $N_p(x)$ under $\exp_p$ is not trivial.
Let $g \in U(x)$. Since G is commutative $k[G(k)]$ is also commutative and $k[x]$ is a subalgebra in $k[G(k)]$. Because $U(x) \subset k[G(k)]$ and $k[G(k)]$ is invariant under ι we know that g commutes with $\iota(g^{-1})$. Thus if $g \notin G(k)$ then $g\iota(g^{-1})$ is in $G(k)$ since $\iota(g\iota(g^{-1})) = g^{-1}\iota(g) = \iota(g)g^{-1} = (g\iota(g^{-1}))^{-1}$. As $g \to g\iota(g^{-1})$ is a group morphism (again since G is commutative) that is defined over k the image of $U(x)$ under this k-morphism is a k-group which is non trivial. Furthermore this k-group consists of unipotent elements. Since G is commutative the connected component of the 1 in this k-group is a normal unipotent connected subgroup of G that contains non trivial k-rational elements. Therefore G was not k-reductive but this is a contradiction. □

Lemma 4.9. *Let G be a classical k-group associated to the commutative semisimple k-algebra with involution (A, ι). Then G is k-reductive.*

Proof: This is a consequence of lemma 4.7. As A is commutative the normalizer of $G(k)$ is $A^\times$. As A is a commutative semisimple k-algebra A is a direct sum of fields. But is is clear that the maximal multiplicative subgroup of a direct sum of fields spans A. Therefore the prerequisites of lemma 4.7 are fulfilled and G is k-reductive. □

This enables us to show the remaining part of the equivalence.

Theorem 4.7. *Let Q be a k-pseudotorus in the classical k-group G that is associated to the semisimple k-algebra with involution (A, ι). Then Q is k-reductive.*

Proof: We have seen in the remark after theorem 4.3 that Q lies in the k-pseudotorus $((\overline{k} \otimes k[Q(k)]) \cap G)^0$. If we can see that $((\overline{k} \otimes k[Q(k)]) \cap G)^0$ is k-reductive then it follows by commutativity that Q is k-reductive. We have seen that $((\overline{k} \otimes k[Q(k)]) \cap G)$ is the classical k-group associated to the commutative semisimple k-algebra $A(Q(k))$ with involution $\iota_{|A(Q(k))}$ and therefore all prerequisites of lemma 4.9 are fulfilled. Thus $((\overline{k} \otimes k[Q(k)]) \cap G)$ is k-reductive. This implies that the identity component $((\overline{k} \otimes k[Q(k)]) \cap G)^0$ is k-reductive and therefore Q is k-reductive. $\square$

Remark:
Another possible proof for the last theorem would be to use that Q is a classical k-group associated to the semisimple k-algebra with involution $(k[Q(k)], \iota_{|k[Q(k)]})$. As $Q(k)$ spans the corresponding algebra $k[Q(k)]$ we may apply lemma 4.7 to see that Q is k-reductive.

5 The Weil restriction

In this chapter we will deal with field extensions of k. We denote by K a finite algebraic field extension of k. Our main interest lies in classical k-groups associated to some semisimple k-algebras A with involution ι considered as linear algebraic groups that are defined over k. When dealing with linear algebraic groups one starts with algebraically closed fields but since our fields k won't be algebraically closed in general, restriction of fields will be an important tool. The Weil restriction is a method to assign a k-group (resp. affine k-algebra) with some universal property to a given linear algebraic K-group (resp. affine K-algebra). One may consider any k-group also as a K-group and we will frequently make use of this fact. If there is no possible confusion we will do that without mentioning it.

5.1 Definition and basic results

The Weil restriction was introduced by Andre Weil in [Wei82]. We will follow the book [Spr09] which defines the Weil restriction for affine varieties and linear algebraic groups. In [CGP10] there is a longer discussion about Weil restriction in the more general case of schemes. Anyway for us this level of generality is not necessary. We will only need the Weil restriction in the case of classical k-groups. Since classical k-groups are just a special case of linear algebraic groups we can use the well known fact that any connected algebraic group is smooth and irreducible. For a proof of this result see [Spr09] (theorem 4.3.7.).

Theorem 5.1. *Let B be an affine K-algebra, then there exists a pair $(R_{K/k}B, \rho)$ where $R_{K/k}(B)$ is a k-algebra and ρ is a K-algebra homomorphism*

$$\rho : B \to K \otimes_k R_{K/k}(B)$$

with the following universal property: for any pair (B_0, σ) of a k-algebra B_0 and a K-homomorphism

$$\sigma : B \to K \otimes_k B_0$$

there exists some unique k-homomorphism

$$\tau : R_{K/k}(B) \to B_0$$

with $\sigma = (id \otimes \tau) \circ \rho$. This pair $(R_{K/k}(B), \rho)$ is called the Weil restriction of B.

The existence of the Weil restriction for affine algebras is shown in [Spr09] (corollary 11.4.3. and proposition 11.4.2.). In the same source one can also find the following corresponding statement for affine varieties(theorem 11.4.16.).

Theorem 5.2. *Let X be an irreducible, smooth, affine K-variety. There exists an irreducible, smooth, affine k-variety $R_{K/k}(X)$ together with a surjective K-morphism*

$$\pi : R_{K/k}(X) \to X$$

such that the following holds: for any affine k-variety Y together with a K-morphism

$$\phi : Y \to X$$

there exists a unique k-morphism

$$\psi : Y \to R_{K/k}(X)$$

with $\phi = \pi \circ \psi$. The pair $(R_{K/k}(X), \pi)$ is unique up to isomorphism and is called the Weil restriction.

When dealing with linear algebraic groups G the Weil restriction of G is not only a k-variety but also a k-group, as we will see in the following theorem.

Theorem 5.3. *Let G be a linear algebraic K-group. Then the Weil restriction $R_{K/k}(G)$ is a linear algebraic group over k. There exists a surjective homomorphism of K-groups*

$$\pi : R_{K/k}(G) \to G$$

with the following universal property: if H is a k-group and

$$\phi : H \to G$$

a homomorphism of K-groups, there is a unique homomorphism of k-groups

$$\psi : H \to R_{K/k}(G)$$

such that $\phi = \pi \circ \psi$.

See [Spr09] (Proposition 12.4.2.).
The following commutative diagram will illustrate the situation for linear algebraic K-groups.

$$\begin{tikzcd}
G & R_{K/k}(G) \arrow[l, "\pi"] \\
H \arrow[u, "\phi"'] \arrow[ur, dashed, "\exists!\psi"'] &
\end{tikzcd}$$

Remarks:

1. In the book [Spr09] the Weil restriction of a linear algebraic group G is denoted by ΠG and the Weil restriction of an affine variety is denoted by $R(K[X])$. As there will be no possible confusion we will use the same notation for the Weil restriction in the case of affine algebras and the Weil restriction of linear algebraic groups. The notation $R_{K/k}$ is taken from the book [CGP10].

2. In the proof of theorem 5.2 it is shown that $R_{K/k}(K[X])$ is an affine algebra and the variety $R_{K/k}(X)$ is defined by the affine algebra $R_{K/k}(K[X])$. The map $\pi : R_{K/k}(X) \to X$ is induced by the corresponding map $\rho : K[X] \to R_{K/k}(K[(X)])$. Thus we can say that $R_{K/k}(K[X]) = k[R_{K/k}(X)]$.

3. In particular if X is itself a k-variety then we may choose $Y = X$ and $\phi = \text{id}$ to obtain an injective map $\psi_0 : X \to R_{K/k}(X)$ with the property $\text{id} = \pi \circ \psi_0$. Actually ψ_0 is a k-isomorphism from X to $\psi_0(X)$.

From now on ρ will always denote the K-homomorphism from $K[X]$ to $K \otimes R_{K/k}(K[X])$ and π the K-homomorphism from $R_{K/k}(X)$ to X, both from the definition of the Weil restriction in the case of affine K-algebras resp. affine K-varieties. If we consider different K-varieties and their Weil restrictions that we will denote them with a subscript. (i.e. π_X for the morphism from $R_{K/k}(X)$ to X) Furthermore ψ_0 will denote the k-homomorphism from the remark 3. As linear algebraic k-groups are just a special case of affine k-varieties we will use the same notations for them.
Another result from [Spr09] (corollary 11.4.3.) that will be of some use for us is the following corollary.

Corollary 5.1. $\operatorname{Ker}\pi$ *contains no non-trivial closed, normal k-subgroup of $R_{K/k}(G)$.*

We want to prove a very important fact about the k-rational points in $R_{K/k}(X)$ for some affine K-variety X. Actually this is one of the main ideas that lead to the definition of the Weil restriction. In fact this lemma is a special case of the fact that there exists a natural map

$$\operatorname{Hom}_K(K(X), K \otimes_k B) \cong \operatorname{Hom}_k(R_{K/k}(K[X]), B).$$

where B is a k-algebra. In our case we have $B = k$. This statement can be found in [Spr09] (11.4.6).

Lemma 5.1. *There exists a natural bijection between the functors $X \to X(K)$ and $X \to R_{K/k}(X)(k)$ in the categori of K-varieties.*

Proof: Let $K[X]$ be the affine K-algebra of X. Then $R_{K/k}(K[X])$ is the affine k-algebra of the k-variety $R_{K/k}[X]$. Any K-rational $x \in X$ corresponds to some K-homomorphism σ_x from $K[X]$ to $K = K \otimes_k k$. By the universal property of $R_{K/k}(K[X])$ there exists some unique k-homomorphism τ_x from $R_{K/k}(K[X])$ to k such that $(\mathrm{id} \otimes \tau_x) \circ \rho = \sigma_x$. By definition, the k-rational points in $R_{K/k}(X)$ correspond to the k-homomorphisms from $R_{K/k}(K[X])$ to k. Therefore any such τ_x is in accordance to some k-rational element $x' \in R_{K/k}(X)$.
Since the map π is induced by ρ the picture of x' under π equals x and since τ_x is unique x' is the only k-rational element with this property. It is clear that this bijection is natural. □

We could also reformulate this and say that for x some K-rational element in the affine K-variety X there exists exactly one element $x' \in \pi^{-1}(x)$ that is k-rational. Next we want to prove some properties of the Weil restriction that will be important for us. It is well known that $R_{K/k}$ is a functor from the category of K-algebras (resp.groups) into the category of k-algebras (resp. groups). For Y a K-subvariety of X we want to describe the k-subvariety $R_{K/k}(Y)$ of $R_{K/k}(X)$ in matters of maximality to get a better understanding of it.

Lemma 5.2. *Let Y be a K-subvariety of X. Then $R_{K/k}(Y)$ is a k-subvariety of $R_{K/k}(X)$ and $\pi_Y = \pi_{|Y}$. In fact it is the maximal k-subvariety in $\pi^{-1}(Y)$ i.e. a k-subvariety that contains any other k-subvariety in $\pi^{-1}(Y)$. In particular such a maximal k-subvariety exists.*

Proof: As Y is a K-subvariety of X there exists some surjective K-morphism from $\phi : K[X] \to K[Y]$. As a consequence of the considerations in [Spr09] (11.4.1) the induced k-homomorphism $R_{K/k}(\phi) : R_{K/k}(K[X]) \to R_{K/k}(K[Y])$ is also surjective. This shows that $R_{K/k}(Y)$ is a k-subvariety of $R_{K/k}(X)$.
Consider $R_{K/k}(Y)$ together with the map π_Y from the definition of the Weil restriction. Then we may consider the K-homomorphism $\pi_Y : R_{K/k}(Y) \to Y$ as a K-homomorphism to X. But by the universal property of $R_{K/k}(X)$ there exists some unique k-homomorphism τ_Y from $R_{K/k}(Y)$ to $R_{K/k}(X)$ such that $\pi_Y = \pi \circ \tau_Y$. It is clear that τ_Y is the comorphism of $R_{K/k}(\phi)$ and therefore the image of τ_Y in $R_{K/k}(X)$ is $R_{K/k}(Y)$.
Let W be a k-subvariety in $\pi^{-1}(Y)$. Then the universal property of $R_{K/k}(X)$ tells us that there exists a unique k-homomorphism τ from W to $R_{K/k}(X)$ such that $\pi = \pi \circ \tau$. It is clear that id is a k-homomorphism with this property and by the uniqueness we have $\tau = \text{id}$. But this implies that W lies in $R_{K/k}(Y)$ and thus the latter is a maximal k-subvariety in $\pi^{-1}(Y)$. In particular this implies that such a variety exists. □

Remark:

1. In the case of linear algebraic groups the Weil restriction of some K-subgroup G_1 is the maximal k-subgroup in $\pi^{-1}(G_1)$.

2. Let Y be a K-subvariety of X and π the map from $R_{K/k}(X)$ to X. Then with lemma 5.1 this result shows that the k-rational element in $\pi^{-1}(y)$ for $y \in Y$ lies in $R_{K/k}(Y)$.

Next we want to show that the Weil restriction respects direct products.

Lemma 5.3. *Let X and Y be linear algebraic K-varieties. Then $R_{K/k}(X \times Y) = R_{K/k}(X) \times R_{K/k}(Y)$.*

Proof: We denote by π the K-morphism from $R_{K/k}(X \times Y)$ to $X \times Y$, by π_X the K-morphism from $R_{K/k}(X)$ to X and by π_Y the K-morphism from $R_{K/k}(Y)$ to Y. We claim that $R_{K/k}(X) \times R_{K/k}(Y)$ together with the K-morphism $(\pi_X \circ \text{pr}_1, \pi_Y \circ \text{pr}_2)$ fulfils the universal property of the Weil restriction of $X \times Y$ and is therefore k-isomorphic to $R_{K/k}(X \times Y)$. Here pr_i denotes the projection of $R_{K/k}(X) \times R_{K/k}(Y)$ on the i'th factor.
The composition of π and the projection on the first variable is a K-morphism π_1 from $R_{K/k}(X \times Y)$ to X and therefore by the universal property there exists some unique k-morphism ψ_X from $R_{K/k}(X \times Y)$ to $R_{K/k}(X)$ such that

$\pi_X \circ \psi_X = \pi_1$. Replacing X by Y and using the projection on the second variable we obtain a k-morphism ψ_Y from $R_{K/k}(X \times Y)$ to $R_{K/k}(Y)$ with the according property. Thus by definition we know that

$$(\pi_X \circ \psi_X, \pi_Y \circ \psi_Y) = (\pi_1, \pi_2) = \pi \tag{7}$$

Furthermore by the universal property of the direct product there exists some unique k-morphism γ from $R_{K/k}(X \times Y)$ to $R_{K/k}(X) \times R_{K/k}(Y)$ such that $\psi_X = \mathrm{pr}_1 \circ \gamma$ and $\psi_Y = \mathrm{pr}_2 \circ \gamma$.
Now let C be some arbitrary k-variety and let ϕ be a K-morphism from C to $X \times Y$. By the universal property of $R_{K/k}(X \times Y)$ there exists some k-morphism ψ such that $\pi \circ \psi = \phi$. Applying equation (7) we obtain $(\pi_X \circ \psi_X, \pi_Y \circ \psi_Y) \circ \psi = \phi$. Finally using the universal property of the direct product we get

$$(\pi_X \circ \mathrm{pr}_1, \pi_Y \circ \mathrm{pr}_2) \circ \gamma \circ \psi = \phi.$$

The map $\gamma \circ \psi$ is a k-morphism from C to $R_{K/k}(X \times Y)$. Thus all that is left to show is that $\gamma \circ \psi$ is the unique k-morphism with this property. So suppose there was another k-morphism $\lambda = (\lambda_1, \lambda_2)$ from C to $R_{K/k}(X) \times R_{K/k}(Y)$ with $(\pi_X \circ \mathrm{pr}_1, \pi_Y \circ \mathrm{pr}_2) \circ \lambda = \phi$. But then it is easy to see that $\lambda_1 = \phi_X \circ \psi$ and $\lambda_2 = \phi_Y \circ \psi$ which shows that $\lambda = \gamma \circ \psi$. □

We want to make use of the Weil restriction to show some results concerning the k-radical and the unipotent k-radical of linear algebraic k-groups. Thus it is a question whether the Weil restriction preserves normality and this is the next thing we want to see.

Lemma 5.4. *Let H be a normal K-subgroup in G. Then $R_{K/k}(H)$ is a normal k-subgroup in $R_{K/k}(G)$.*

Proof: Consider the K-morphism $\Phi_G \times H \to G$ given by $\Phi(g, h) = ghg^{-1}$. The group N is normal in G if and only if there exists a K-morphism $\psi : G \times H \to H$ such that $\Phi = i \circ \psi$, where $i : H \to G$ is the embedding. Now we use the functoriality of $R_{K/k}$ and the lemma 5.3. □

Now we want to give some results that will be helpful in the following. The first one will show that the Weil restriction does not only preserve normality but also conjugation, i.e. if G_1 and G_2 are conjugate K-subgroups of G then $R_{K/k}(G_1)$ and $R_{K/k}(G_2)$ are conjugate k-subgroups in $R_{K/k}(G)$. After that we will see that the Weil restriction of a commutative K-group is a commutative k-group.

Lemma 5.5. *Let G_1 and G_2 be two K-subgroups of G with $gG_1g^{-1} = G_2$ for some $g \in G(K)$. Then there exists some $g' \in R_{K/k}(G)(k)$ such that $g'R_{K/k}(G_1)g'^{-1} = R_{K/k}(G_2)$.*

Proof: Since g is K-rational we can conclude by help of lemma 5.1 that there exists a k-rational element $g' \in \pi^{-1}(g)$. Since $\pi(R_{K/k}(G_1)) = G_1$ we have $\pi(g'R_{K/k}(G_1)g'^{-1}) = G_2$ and therefore $g'R_{K/k}(G_1)g'^{-1} \subset \pi^{-1}(G_2)$. Since g' is k-rational $\mathrm{Int}(g')$ is a k-morphism on the k-group $R_{K/k}(G)$ and since $R_{K/k}(G_1)$ is a k-subgroup $\mathrm{Int}(g')(R_{K/k}(G_1))$ is also a k-subgroup in $\pi^{-1}(G_2)$, hence a subgroup of the maximal k-subgroup $R_{K/k}(G_2)$ in $\pi^{-1}(G_2)$. The same way we can see that $g'^{-1}R_{K/k}(G_2)g' \subset R_{K/k}(G_1)$ and therefore $g'R_{K/k}(G_1)g'^{-1} = R_{K/k}(G_2)$. □

The following lemma is formulated as an exercise in [Spr09](Exercise 12.4.7. (3)).

Lemma 5.6. *Let G be a commutative group. Then $R_{K/k}(G)$ is also commutative.*

Proof: Consider the two morphisms $G \times G \to G$ that map (g_1, g_2) once to g_1g_2 and once to g_2g_1. As G is commutative these two morphisms are equal. Now use again the functoriality of $R_{K/k}$ and lemma 5.3. □

Lemma 5.7. *Let G be a K-group and H a normal K-subgroup. Then $R_{K/k}(G/H) = R_{K/k}(G)/R_{K/k}(H)$.*

Proof: We want to use the following commutative diagram to illustrate the situation.

$$\begin{tikzcd}
1 \arrow[r] & R_{K/k}(H) \arrow[r, "R_{K/k}(i)"] \arrow[d, "\pi_H"] & R_{K/k}(G) \arrow[r, "R_{K/k}(p)"] \arrow[d, "\pi_G"] & R_{K/k}(G/H) \arrow[r] \arrow[d, "\pi_{G/H}"] & 1 \\
1 \arrow[r] & H \arrow[r, "i"] & G \arrow[r, "p"] & G/H \arrow[r] & 1
\end{tikzcd}$$

By lemma 5.4 $R_{K/k}(H)$ is a normal k-subgroup of $R_{K/k}(G)$ and thus by [Spr09] (proposition 5.5.10.) $R_{K/k}(G)/R_{K/k}(H)$ is a k-group. Denote the projection from G to G/H by p and the embedding of H into G by i. Both

are K-morphisms (resp. a k-morphism). By the functoriality of $R_{K/k}$ we obtain k-morphisms $R_{K/k}(i)$ from $R_{K/k}(H)$ to $R_{K/k}(G)$ and $R_{K/k}(p)$ from $R_{K/k}(G)$ to $R_{K/k}(G/H)$ such that the diagram commutes. The second line in this diagram is a short exact sequence and if we can see that the first one is also a short exact sequence then the statement is clear.
At first we want to show that $\operatorname{Im} R_{K/k}(i) \subset \operatorname{Ker} R_{K/k}(p)$. This follows from the functoriality of $R_{K/k}$. As $\operatorname{Im} R_{K/k}(i) = R_{K/k}(\operatorname{Im}(i))$ and $p \circ i = 0$ we know that $R_{K/k}(p)(R_{K/k}(\operatorname{Im}(i))) = 0$ which proves the claim.
On the other side $\operatorname{Im} R_{K/k}(i) \supset \operatorname{Ker} R_{K/k}(p)$ as $\pi_G(\operatorname{Ker} R_{K/k}(p)) \subset i(H)$. Then the using the functoriality of $R_{K/k}$ again we see that $\operatorname{Ker} R_{K/k}(p) \subset \operatorname{Im} R_{K/k}(i)$. Next we want to see that $R_{K/k}(i)$ is injective. By exactness of the second line we know that $\pi_G(\operatorname{Ker} R_{K/k}(p)) \subset i(H)$ and thus we have a K-morphism from $\operatorname{Ker} R_{K/k}(p)$ to H. The universal property of $R_{K/k}(H)$ shows that there exists some k-morphism ϕ from $\operatorname{Ker} R_{K/k}(p)$ to $R_{K/k}(H)$ such that $i^{-1} \circ \pi_G = \pi_H \circ \phi$. This shows that $\pi_G = i \circ \pi_H \circ \phi$ and as the diagram is a commutative diagram we have

$$i \circ \pi_H \circ \phi \circ R_{K/k}(i) = i \circ \pi_H$$

which shows that ϕ inverts $R_{K/k}(i)$ and therefore $R_{K/k}(i)$ is injective.
The fact that $R_{K/k}(p)$ is surjective follows as p is an isomorphism from $G/\operatorname{Im}(i)$ to G/H and thus functoriality shows that $R_{K/k}(p)$ is an isomorphism from $R_{K/k}(G)/\operatorname{Im}(R_{K/k}(i))$ to $R_{K/k}(G)$. □

Like lemma 5.6 the following two lemmata are again formulated as exercises in [Spr09](Exercise 12.4.7.(3) and 11.4.7.(4)).

Lemma 5.8. *Let G be a connected linear algebraic K-group. Then the Weil restriction $R_{K/k}(G)$ is also connected.*

Proof: If G is a connected linear algebraic K-group it is in particular an irreducible K-variety. By theorem 5.2 the Weil restriction is an irreducible k-variety. Thus if we take the Weil restriction as a k-group it is a connected k-group. □

Lemma 5.9. *Let X be a K-variety and K_1 be a field extension intermediate between k and K then $R_{K/k}(X) = R_{K_1/k}(R_{K/K_1}(X))$.*

Proof: We show that $R_{K_1/k}(R_{K/K_1}(X))$ fulfils the universal property of the Weil restriction $R_{K/k}(X)$. Thus let Y be an arbitrary k-group and ϕ a K-morphism from Y to X. As Y is in particular a K_1-variety by the universal property of the Weil restriction $R_{K/K_1}(X)$ there exists a unique K_1-morphism ψ_{K_1} from Y to $R_{K/K_1}(X)$. Thus we obtain for every k-variety Y with given K-morphism a unique K_1-morphism from Y to $R_{K/K_1}(X)$ and thus by the universal property of the Weil restriction $R_{K_1/k}(R_{K/K_1}(X))$ there exists some unique k-morphism ψ from Y to $R_{K_1/k}(R_{K/K_1}(X))$. But this is exactly the universal property of the Weil restriction $R_{K/k}(X)$. □

Corollary 5.2. *Let G be a linear algebraic K_1-group where K_1 is a field extension intermediate between k and K. Then $R_{K/k}(G)$ is k-isomorphic to a k-subgroup of $R_{K_1/k}(G)$.*

Proof: As G is a K_1-group we may also consider it as a K-group. We saw that there exists some K_1-isomorphism ψ_0 from G to $\psi_0(G) \subset R_{K/K_1}(G)$. Therefore we may consider G as a K_1-subgroup of $R_{K/K_1}(G)$. But then $R_{K_1/k}(G)$ is k-isomorphic to a k-subgroup of $R_{K_1/k}(R_{K/K_1}(G))$. As the last lemma showed that $R_{K_1/k}(R_{K/K_1}(G)) = R_{K/k}(G)$ the corollary is proven. □

5.2 Examples and calculation of the Weil restriction

We want to make use of the Weil restriction to show some interesting results for k-pseudotori. But before doing this we want to give a more explicit description of the Weil restriction of the affine algebra of a linear algebraic k-group G. We do this to calculate the Weil restriction in a special case. This will show that there is a connection between the Weil restriction of the multiplicative group of certain fields and k-pseudotori.

In the following calculation we will use a simplified notation. Instead of writing $K[T_1, \ldots, T_n]/(P_1, \ldots, P_m)$ for the affine algebra of the group G that is the zero set of the ideal that is spanned by $P_1, \ldots, P_m$ in the affine space of dimension n we just write $K[T]/(P)$. Here $P(T)$ equals the K-regular map $K^n \to K^m$

$$(T_1, \ldots, T_n) \to (P_1(T_1, \ldots, T_n), \ldots, P_m(T_1, \ldots, T_n)).$$

Consider G as a K-group with affine algebra $K[G] = K[T]/(P)$. Now consider K as a k-vector space and let $v_1, \ldots, v_d$ be a k-basis of K. We may perceive the underlying affine K-space of dimension n as an affine k-space of dimension nd and the map P as the k-rational map $P_k : k^{nd} \to k^{md}$

$$(T_{11}, \ldots, T_{nd}) \to (P_{11}(T_{11}, \ldots, T_{nd}), \ldots, P_{md}(T_{11}, \ldots, T_{nd}))$$

where $P_{ij}(T_{11},\dots,T_{nd}) \in k[T_{11},\dots,T_{nd}]$ and P_{ij} is defined by the equation $P_i(T_{11},\dots,T_{nd}) = \sum_j P_{ij}((T_{11},\dots,T_{nd})v_j)$.
We claim that the Weil restriction $R_{K/k}(K[G])$ is the k-algebra

$$k[T_{11},\dots,T_{nd}]/(P_k) \tag{8}$$

To see that this is really the Weil restriction define the K-homomorphism $\rho : K[G] \to K \otimes R_{K/k}(K[G])$ the following way:

$$\rho(T_i) = \sum_{j=1}^{d} v_j \otimes T_{ij}$$

Next we have to see that the universal property of the Weil restriction is fulfilled. Thus consider an arbitrary k-algebra B and a K-homomorphism $\sigma : K[G] \to K \otimes B$. Let $\sigma(T_i) = \sum_{j=1}^{d} v_j \otimes \sigma_j(T_i)$ where $\sigma_j(T_i)$ is a k-homomorphism from $K[G]$ to B. Now define the corresponding map τ by

$$\tau(T_{ij}) = \sigma_j(T_i)$$

It is obvious that $\sigma = (\mathrm{id} \otimes \tau) \circ \rho$ and since τ is defined uniquely on every T_{ij} it is also unique. Now the Weil restriction of the K-group G is the k-group that is induced by $R_{K/k}(K[G])$.

Lemma 5.10. *If G is the classical K-group associated to the semisimple K-algebra with involution (A, ι), then $R_{K/k}(G)$ is the classical k-group associated to the semisimple k-algebra with involution (A_k, ι_k) where ι_k is ι considered as k-antiautomorphism.*

Proof: We use the methods we just introduced to calculate the Weil restriction of the classical K-group G. For this purpose consider the semisimple K-algebra with involution (A, ι). Then we may consider A as a k-vector space and the involution ι as a k-antiautomorphism. We can carry over the multiplication and this way we obtain the semisimple k-algebra with involution we denoted by (A_k, ι_k). As G is the zero set of $g\iota(g) - 1$ we see that the algebra A plays the same role as the affine space in the calculations we just made.
The polynomials that are defined by the term $g\iota(g) - 1$ give rise to a k-regular map $k^{nd} \to k^{nd}$. It is clear that every element g_k in the zero set

of the emerging k-regular polynomials thus satisfies $g_k\iota_k(g_k) - 1$. Hence the Weil restriction of G is the zero set of $g_k\iota(g_k) - 1$ in the semisimple k-algebra A_k. Therefore the Weil restriction of a classical K-group is a classical k-group. □

Now we want to calculate the Weil restriction of some classical k-groups explicitly.

Example. 1. Let k be a field of characteristic p such that $a \in k$ but the p'th root of a denoted by u is not in k. Furthermore let $K = k(u)$ and consider the group $G = G_m(K)$. The affine algebra of G is $K[x, y]/(xy - 1)$. As a basis for K as k-vector space we choose $1, u, \ldots, u^{p-1}$. Define $x = \sum_{i=0}^{p-1} x_i u^i$ and $y = \sum_{i=0}^{p-1} y_i u^i$. This yields the following equations for $xy - 1 = 0$

$$\begin{array}{rcl}
x_0y_0 + \displaystyle\sum_{\substack{i+j\equiv 0 \bmod p \\ i\neq 0}} x_iy_ja & = & 1 \\
x_0y_1 + y_0x_1 + \displaystyle\sum_{\substack{i+j\equiv 1 \bmod p \\ i\neq 0, j\neq 0}} x_iy_ja & = & 0 \\
& \vdots & \\
\displaystyle\sum_{i+j\equiv p-1 \bmod p} x_iy_j & = & 0
\end{array}$$

We may rewrite this in the following way

$$\begin{pmatrix} x_0 & ax_{p-1} & ax_{p-2} & \ldots & ax_1 \\ x_1 & x_0 & ax_{p-1} & \ldots & ax_2 \\ \vdots & & & \ldots & \vdots \\ x_{p-1} & x_{p-2} & x_{p-3} & \ldots & x_0 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{p-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

We already calculated the determinant of this matrix in lemma 4.3 and it equalled $x_0^p + ax_1^p + a^2x_2^p + \ldots + a^{p-1}x_{p-1}^p$ which is never 0 if $x_i \neq 0$ for at least one i. This implies that we can find a solution for these equations for all $(x_0, \ldots, x_{p-1}) \neq (0, \ldots, 0)$. In particular if we map u to g_a and choose arbitrary $(x_0, \ldots, x_{p-1}) \neq (0, \ldots, 0)$ then the set of $\sum_{i=0}^{p-1} x_iu^i$ is indeed isomorphic to the k-pseudotorus $k[g_a]\backslash\{0\}$.

We want to have a similar statement in a more general setting. Thus let K be a field extension of k and denote by $\tilde{K}$ the variety with K-rational points K. On the other side K may also be considered as a $[K : k]$-dimensional k-vector space which we denote by K_k. Then K_k equals the set of k-rational points in some k-variety $\tilde{K}_k$. By all we have seen about the calculation of the Weil restriction it is clear that $\tilde{K}_k = R_{K/k}(\tilde{K})$.
As $\tilde{K}_k$ and $\tilde{K}$ are additive groups the map π is a homomorphism of additive K-groups. This is a consequence of the proof of theorem 5.3. By lemma 5.1 π is a bijection between K and K_k and therefore π is a bijection between $K_k \setminus \{0\}$ and $K \setminus \{0\}$. Denote by $\tilde{K}^\times$ the corresponding K-variety then we just showed that $K_k \setminus \{0\}$ is in $R_{K_A/k}(\tilde{K}^\times)$. Restricting π on this k-variety it becomes a morphism of multiplicative K-groups. Thus π is a k-algebra homomorphism between K_k and K. Given a k-involution ι on K_k we may define an involution ι_1 on K by $\iota_1(x) = \pi(\iota(a))$ where $a \in K_k \cap \pi^{-1}(x)$. Actually this uniquely defines a and ι_1 is an involution as π is a k-algebra homomorphism. By definition we have $\iota_1 \circ \pi = \pi \circ \iota$. This implies that π maps the group $G = \{g \in K_k \mid g\iota(g) = 1\}$ to a group $G_1 = \{g_1 \in K \mid g_1\iota_1(g_1) = 1\}$ resp. π is a K group morphism between the corresponding linear algebraic groups which will be denoted by the same letters. Finally this shows that any k-pseudotorus is a direct product of Weil restrictions of fields intersected with groups of the form G_1. Here we want to stress that G_1 is no classical K-group as ι_1 is no K-linear involution.

We are in particular interested in the Weil restriction of the group of diagonal matrices $\mathbf{D}_n$ and the group of upper triangular matrices $\mathbf{T}_n$ which are subgroups of GL_n. Especially the latter group is important if we want to show some results about the k-radical and the unipotent k-radical. When working with algebraically closed fields we already saw that the theorem of Lie-Kolchin states that any solvable subgroup of GL_n is conjugate to a subgroup of $\mathbf{T}_n$ and this will play an important role for us. For the rest of the chapter we assume that K is a field extension of degree d of k.
We want to start with the Weil restriction of $\mathbf{D}_n(K)$. Since $\mathbf{D}_n(K) = \prod_1^n \mathbb{G}_m(K)$ lemma 5.3 shows that $R_{K/k}(\mathbf{D}_n) = \prod_1^n R_{K/k}(\mathbb{G}_m)$. If we let this group act on some vector space then we can choose a basis such that it becomes a subgroup of the set of $nd \times nd$ matrices with $d \times d$ blocks on the diagonal and zeroes everywhere else.
Furthermore we want to see that $R_{K/k}(\mathbb{G}_m)$ consists of k-semisimple ele-

ments. We just saw that $R_{K/k}(G)$ is a classical k-group for G a classical K-group and thus we have a definition for k-semisimplicity of elements in $R_{K/k}(G)$. Now let $G = \mathbb{G}_m$ and consider the Weil restriction $R_{K/k}(G)$. We saw that the set of k-rational points in this group is isomorphic to $K^\times$. But there are no nilpotent elements in $K^\times$ and thus the minimal polynomial of any k-rational element $g \in R_{K/k}(G)$ is square free and therefore any such element is k-semisimple. Since the blocks commute $R_{K/k}(G)$ is commutative. By lemma 5.8 the group $R_{K/k}(G)$ is connected and thus it is a connected commutative linear algebraic group such that all k-rational elements are k-semisimple. This implies that the Weil restriction of $\mathbb{G}_m$ is a k-pseudotorus. We will see that in general the Weil restriction of a K-pseudotorus is a k-pseudotorus but we need some more results before we can show this.

Now we want to consider $\mathbf{T}_n(K)$. Denote by $\mathbf{N}_n(K)$ the K-algebra of upper triangular matrices with 0 on the diagonal. This is a K-variety with affine K-algebra $K[T_{ij}]/(T_{\alpha\beta})$ for $\alpha \geq \beta$. Thus the Weil restriction of $\mathbf{N}_n(K)$ is a k-variety and by equation (8) we know that its affine algebra is

$$k[(T_{ij})_1, \ldots, (T_{ij})_d]/((T_{\alpha\beta})_1, \ldots (T_{\alpha\beta})_d) \text{ for } \alpha \geq \beta.$$

If we let $R_{K/k}(\mathbf{N}_n(K))$ act on a vector space then we can choose a basis such that $R_{K/k}(\mathbf{N}_n(K))$ becomes a subalgebra of the $nd \times nd$ block-upper triangular matrices with $d \times d$ blocks with zero on the diagonal.
Observe that $\mathbf{T}_n(K) = \mathbf{D}_n(K) \times \mathbf{N}_n(K)$. Therefore lemma 5.3 shows that $R_{K/k}(\mathbf{T}_n(K)) = (R_{K/k}(\mathbf{D}_n(K)), R_{K/k}(\mathbf{N}_n(K)))$ and thus if we let $R_{K/k}(\mathbf{T}_n(K))$ act on some vector space we may choose a basis such that this group becomes a k-subgroupgroup of the $nd \times nd$ block upper triangular matrices with invertible $d \times d$ blocks on the diagonal.
Consider the special case $\mathbf{U}_n(K)$ of upper triangular matrices with 1 on the diagonal. As the Weil restriction of the trivial group 1 is the trivial group 1 we see that $R_{K/k}(\mathbf{U}_n(K))$ is the k-group of $nd \times nd$ block upper diagonal matrices with $d \times d$ blocks on the diagonal that equal the identity element E_d.

5.3 The Weil restriction of the (unipotent) k-radical

Now take a look at the commutator $[R_{K/k}(\mathbf{T}_n(K)), R_{K/k}(\mathbf{T}_n(K))]$. Since the single blocks on the diagonal commute $[R_{K/k}(\mathbf{T}_n(K)), R_{K/k}(\mathbf{T}_n(K))]$ is a subgroup of $\mathbf{T}_{nd}(k)$ and therefore solvable. Hence $R_{K/k}(\mathbf{T}_n(K))$ is solvable. Furthermore lemma 5.5 implies that, if G_1 is a subgroup of $\mathrm{GL}_n(K)$ such that there exists some K-rational element g such that gG_1g^{-1} is a K-subgroup of $\mathbf{T}_n(K)$ then $R_{K/k}(G_1)$ is conjugate to some k-subgroup of $R_{K/k}(\mathbf{T}_n(K))$ via a k-rational element.

Corollary 5.3. *Let K be a finite field extension of k and let G be a solvable K-group, then $R_{K/k}(G)$ is solvable.*

Proof: As G is solvable there exists a sequence of subgroups

$$G = G_0 \supset G_1 \supset \ldots \supset G_{n_0} = \{1\}$$

such that the image of the morphism $G_i \times G_i \to G_i$ defined by the commutator $(g, h) = ghg^{-1}h^{-1}$ lies in G_{i+1}. Applying the functor $R_{K/k}$ we see that the sequence of the groups $R_{K/k}(G_i)$ has the same property. □

As $R_{K/k}(\mathbf{U}_n(K))$ is a k-subgroup of $\mathbf{U}_{nd}(k)$ one sees that it should be possible to generalise this to a statement for arbitrary unipotent K-groups and their Weil restriction.

Theorem 5.4. *Let G be a unipotent linear algebraic K-group. Then $R_{K/k}(G)$ is a unipotent linear algebraic k-group.*

Proof: We may assume that G is a subgroup of GL_n for some natural number n. As G is a unipotent group there exists some element g such that gGg^{-1} is a subgroup of $\mathbf{U}_n$. The element g need not be K-rational and thus the group gGg^{-1} need not be a K-group. Anyway there exists some finite field extension K_1 of K such that g is K_1-rational and thus gGg^{-1} is a K_1-group. As G is a K-group we may consider it also as a K_1-group and since g is a K_1-rational element with gGg^{-1} a K_1-subgroup of $\mathbf{U}_n$ we know that there exists some k-rational element g_1 in $R_{K_1/k}(G)$ such that $g_1 R_{K_1/k}(G) g_1^{-1}$ is a k-subgroup of $R_{K_1/k}(\mathbf{U}_n)$. The latter is a subgroup of $\mathbf{U}_{nd}$. Therefore $R_{K_1/k}(G)$ is a unipotent k-group.
By corollary 5.2 we may consider $R_{K/k}(G)$ as a k-subgroup of $R_{K_1/k}(G)$. This implies that $R_{K/k}(G)$ is a unipotent k-group. □

Remarks:

1. It is clear that a closely related argument shows that π maps a unipotent k-subgroup in $R_{K/k}(G)$ to a unipotent K-subgroup of G.

2. If g is a unipotent K-rational element in G then the same proof shows that the unique k-rational element in $R_{K/k}(G)$ is also unipotent.

This allows us to proof the following lemma that will give us a connection between the unipotent K-radical of a K-group G and the unipotent k-radical of its Weil restriction.

Lemma 5.11. *Let G be a a k-subgroup of GL_n. Then $R_{K/k}(\mathcal{R}_{K,u}(G)) = \mathcal{R}_{k,u}(R_{K/k}(G))$.*

Proof: We just saw that $R_{K/k}(\mathcal{R}_{K,u}(G))$ is unipotent. Furthermore by lemma 5.4 it is a normal subgroup and by lemma 5.8 the Weil restriction of a connected group is connected itself. Thus $R_{K/k}(\mathcal{R}_{K,u}(G))$ is a normal, unipotent, connected k-subgroup. Now suppose that there exists some normal, unipotent, connected k-group $H \in R_{K/k}(G)$ with $R_{K/k}(\mathcal{R}_{k,u}(G)) \subset H$. Then $\pi(H)$ is a normal, unipotent, connected K-group in G that contains $\mathcal{R}_{K,u}(G)$ and hence $\pi(H) = \mathcal{R}_{K,u}(G)$. But then $H \subset R_{K/k}(\mathcal{R}_{K,u}(G))$. Thus $R_{K/k}(\mathcal{R}_{K,u}(G))$ is the maximal unipotent normal connected k-subgroup in $R_{K/k}(G)$. □

Remark:
It is clear that a similar statement is true for $\mathcal{R}_k(G)$.

Theorem 5.5. *The group G is K-reductive if and only if $R_{K/k}(G)$ is k-reductive.*

Proof: Let G be K-reductive and suppose that $R_{K/k}(G)$ was not k-reductive. Then $\mathcal{R}_{k,u}(R_{K/k}(G))$ was a non-trivial k-subgroup. Lemma 5.11 shows that $\mathcal{R}_{k,u}(R_{K/k}(G)) = R_{K/k}(\mathcal{R}_{K,u}(G))$. But as $\mathcal{R}_{K,u}(G)$ is trivial $R_{K/k}(\mathcal{R}_{K,u}(G))$ is also trivial. This is a contradiction.
Now suppose $R_{K/k}(G)$ was k-reductive but the unipotent K-radical of G was not trivial. Then $R_{K/k}(\mathcal{R}_{K,u})$ was not trivial. By theorem 5.4 this k-group is unipotent, by lemma 5.4 it is normal and by lemma 5.8 it is connected. Thus it is a connected, normal unipotent non-trivial k-subgroup of $R_{K/k}(G)$. But then $R_{K/k}(G)$ was not k-reductive. □

We already mentioned that the Weil restriction of a K-pseudotorus is a K-pseudotorus and now we are able to prove this.

Corollary 5.4. *Let Q be a K-pseudotorus in the classical K-group G. Then the Weil restriction $R_{K/k}(Q)$ is a k-pseudotorus in $R_{K/k}(G)$.*

Proof: Theorem 4.7 shows that Q is K-reductive and therefore the last theorem shows that $R_{K/k}(Q)$ is k-reductive. Furthermore we saw in lemma 5.6 that the Weil restriction of Q is commutative and in lemma 5.8 that it is connected. Thus $R_{K/k}(Q)$ is a connected commutative k-reductive linear algebraic k-group. But then theorem 4.6 shows that it is a k-pseudotorus. □

Corollary 5.5. *Let g be a K-rational K-semisimple element in the classical k-group G associated to the semisimple k-algebra with involution (A, ι). Then the unique k-rational element in $\pi^{-1}(g) \in R_{K/k}(G)$ is k-semisimple.*

Proof: Consider the group $(\overline{k} \otimes k[g]) \cap G$. By theorem 4.3 this group is a commutative, classical K-group. We have seen in lemma 5.6 that the Weil restriction $R_{K/k}((\overline{k} \otimes k[g]) \cap G)$ is commutative and in lemma 5.10 that it is a classical k-group in a semisimple commutative k-algebra. Thus $R_{K/k}((\overline{k} \otimes k[g]) \cap G)(k)$ is a group in a direct product of fields and thus every element in $R_{K/k}((\overline{k} \otimes k[g]) \cap G)(k)$ is k-semisimple. □

Lemma 5.12. *Lewt G be a linear algebraic K-group. Then $\mathcal{R}_{K,u} \supset [\mathcal{R}_K, \mathcal{R}_K]$.*

Proof: We know that every linear algebraic k-group G is isomorphic to a k-subgroup of GL_n for some natural number n. By the theorem of Lie-Kolchin there exists some $g \in \mathrm{GL}_n$ such that $g\mathcal{R}_k(G)g^{-1}$ is a subgroup of $\mathbf{T}_n$. The element g need not be k-rational but there exists some finite field extension K of k such that g is a K-rational element. Furthermore since K is a field extension of k any k-group is also a K-group. Now consider the Weil restriction $R_{K/k}(\mathrm{GL}_n)$ and the K-morphism $\mathrm{Int}(g)$ from the k-group $\mathcal{R}_k(G)$ to GL_n. By the universal property of the Weil restriction there exists some k-morphism ψ from $\mathcal{R}_k(G)$ to $R_{K/k}(\mathrm{GL}_n)$ such that $\mathrm{Int}(g) = \pi \circ \psi$. As the map $g_1 \to g g_1 g^{-1}$ is injective the map ψ is also injective and therefore defines a k-isomorphism to its image $\psi(\mathcal{R}_k(G))$. Since π maps this image to a subgroup of $\mathbf{T}_n$ and as $\psi(\mathcal{R}_k(G))$ is a k-group it is a k-subgroup of $R_{K/k}(\mathbf{T}_n)$. We already saw that $R_{K/k}(\mathbf{T}_n)$ can be considered as a subgroup of the upper block diagonal matrices. But then it is clear that the set $[\psi(\mathcal{R}_k(G)), \psi(\mathcal{R}_k(G))]$ which is also a k-subgroup of $R_{K/k}(\mathbf{T}_n)$ is unipotent. But this implies that $\psi^{-1}([\psi(\mathcal{R}_k(G)), \psi(\mathcal{R}_k(G))])$ is a unipotent k-subgroup in the k-radical of G and thus by lemma 4.5 it is in the unipotent k-radical. □

Now we can use this result.

Corollary 5.6. *Let G be a classical k-reductive k-group. Then the k-radical $\mathcal{R}_k(G)$ is a k-pseudotorus.*

Proof: The last lemma shows that $\mathcal{R}_{K,u} \supset [\mathcal{R}_K, \mathcal{R}_K]$. Since G is k-reductive and thus the unipotent k-radical is trivial the k-radical is commutative. Therefore the k-radical is a k-reductive connected commutative k-group and thus by theorem 4.6 it is a k-pseudotorus. □

Theorem 5.6. *Let g be a k-rational element in the k-group G. Then there exists a finite field extension K of k such that there exists exactly one k-semisimple, k-rational element g'_s and exactly one unipotent, k-rational element g'_u in $R_{K/k}(\mathrm{GL}_n)$ such that $g'_s g'_u = \psi_0(g)$.*

Proof: Again we consider the k-group G as a k-subgroup of the k-group GL_n for some n. Then there exists some semisimple element g_s and some unipotent element g_u such that $g = g_s g_u = g_u g_s$. By Lie-Kolchin there exists some element x such that $x g_u x^{-1}$ lies in $\mathbf{U}_n$. Neither g_s nor g_u or x need to be k-rational but again there exists some finite field extension K such that all of them are K-rational and of course again GL_n is also a K-group. Now consider again the Weil restriction $R_{K/k}(\mathrm{GL}_n)$. Lemma 5.1 tells us that there exists exactly one k-rational element g'_s in $\pi^{-1}(g_s)$ and exactly one k-rational element g'_u in $\pi^{-1}(g_u)$. Finally the same is true for g and since g is k-rational the corresponding g' equals $\psi_0(g)$ where ψ_0 is the k-morphism from G to $R_{K/k}(\mathrm{GL}_n)$ that fulfils the universal property of the Weil restriction for the embedding of G into GL_n. But this implies that g' is in $R_{K/k}(G)$. Furthermore we have $g'_u g'_s = g'$. This is true since $g'_u g'_s$ is a k rational element in $\pi^{-1}(g)$ and g' is the unique element with these properties. We saw in corollary 5.5 that g'_s is k-semisimple.

Thus all that is left to show is that g'_u is unipotent. It is enough to show that g_u lies in some unipotent K-subgroup of G. Then theorem 5.4 shows that g'_u lies in a unipotent k-subgroup and is therefore unipotent. But as $x g_u x^{-1}$ lies in the unipotent K-group $\mathbf{U}_n$ and x is K-rational we see that g_u lies in the unipotent K-group $x \mathbf{U}_n x^{-1}$. □

References

[Alb61] A. A. Albert: *Structure of algebras*, Revised printing. American Mathematical Society Colloquium Publications, Vol. XXIV, American Mathematical Society, Providence, R.I. (1961)

[Art05] J. Arthur: An introduction to the trace formula, in *Harmonic analysis, the trace formula, and Shimura varieties*, volume 4 of *Clay Math. Proc.*, pages 1–263, Amer. Math. Soc., Providence, RI (2005)

[Bor91] A. Borel: *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2nd edition (1991)

[Bou03] N. Bourbaki: *Algebra II. Chapters 4–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin (2003), translated from the 1981 French edition by P. M. Cohn and J. Howie, Reprint of the 1990 English edition [Springer, Berlin; MR1080964 (91h:00003)]

[Bur66] N. Burbaki: *Algebra: Moduli, koltsa, formy*, Translated from the French by G. V. Dorofeev. Edited by Ju. I. Manin, Izdat. "Nauka", Moscow (1966)

[CGP10] B. Conrad, O. Gabber, G. Prasad: *Pseudo-reductive groups*, volume 17 of *New Mathematical Monographs*, Cambridge University Press, Cambridge (2010)

[Gel96] S. Gelbart: *Lectures on the Arthur-Selberg trace formula*, volume 9 of *University Lecture Series*, American Mathematical Society, Providence, RI (1996)

[Jac96] N. Jacobson: *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin (1996)

[Kra84] H. Kraft: *Geometrische Methoden in der Invariantentheorie*, Aspects of Mathematics, D1, Friedr. Vieweg & Sohn, Braunschweig (1984)

[New78] P. E. Newstead: *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*, Tata Institute of Fundamental Research, Bombay (1978)

[Sch85] W. Scharlau: *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamen-*

tal Principles of Mathematical Sciences], Springer-Verlag, Berlin (1985)

[Spr09] T. A. Springer: *Linear algebraic groups*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2nd edition (2009)

[Wei60] A. Weil: Algebras with involutions and the classical groups, *J. Indian Math. Soc. (N.S.)*, **24**:589–623 (1961) (1960)

[Wei82] —— *Adeles and algebraic groups*, volume 23 of *Progress in Mathematics*, Birkhäuser Boston, Mass. (1982), with appendices by M. Demazure and Takashi Ono

[Wei95] —— *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin (1995), reprint of the second (1973) edition