Tôhoku Math. Journ.
20(1968), 443-497.

RATIONALITY PROPERTIES OF LINEAR ALGEBRAIC GROUPS II

A. BOREL AND T. A. SPRINGER

(Received March 5, 1968)

This paper is a development of [4], and gives a more detailed treatment of the topic named in the title. It includes in particular the birational equivalence with affine space, over the groundfield, of the variety of Cartan subgroups of a k-group G, the splitting of G over a separable extension of k if G is reductive, some results on unipotent groups operated upon by tori, and on the existence of subgroups of G whose Lie algebra contains a given nilpotent element of the Lie algebra $\mathfrak{g}$ of G.

Discussing as it does a number of known results (due mostly to Rosenlicht and Grothendieck), this paper is to be viewed as partly expository. In fact, besides proving some new results, our main goal is to provide a rather comprehensive, albeit not exhaustive, account of our topic, from the point of view sketched in [4].

Our basic tools are some rationality properties of transversal intersections and of separable mappings, the Jordan decomposition in $\mathfrak{g}$, and purely inseparable isogenies of height one. They are reviewed or discussed in section 1.13, §3 and §5 respectively. Thus Lie algebras of algebraic groups play an important role in this paper and, for the sake of completeness, we have collected in §1 a number of definitions and facts pertaining to them.

§2 reproves a result of Grothendieck ([12], Exp. XIV) stating that $\mathfrak{g}$ is the union of the subalgebras of its Borel subgroups. Its main use for us is to reduce to Lie algebras of solvable groups the existence proof of the Jordan decomposition.

§4 discusses subalgebras $\mathfrak{s}$ of $\mathfrak{g}$ consisting of semi-simple elements, to be called "toral subalgebras" of $\mathfrak{g}$. They are tangent to maximal tori, and have several properties similar to that of tori in G, in particular: the centralizer $Z(\mathfrak{s})=\{g \in G,\ \mathrm{Ad}g(X)=X(X \in \mathfrak{s})\}$ of $\mathfrak{s}$ in G is defined over k if $\mathfrak{s}$ is, (see 4.3 for $Z(\mathfrak{s})^0$, 6.14 for $Z(\mathfrak{s})$), its Lie algebra is $\mathfrak{z}(\mathfrak{s}) = \{X \in \mathfrak{g}, [\mathfrak{s}, X] = 0\}$. If $\mathfrak{s}$ is spanned by one element X, the conjugacy class of X is isomorphic to $G/Z(\mathfrak{s})$. This paragraph also gives some conditions under which a subalgebra of $\mathfrak{g}$ is algebraic, and reproves some results of Chevalley [8] in characteristic zero.

§6 introduces regular elements, Cartan subalgebras in $\mathfrak{g}$, and the subgroups of type (C) of ([12], Exp. XIII) in G. By definition here, a Cartan subalgebra of $\mathfrak{g}$ is the centralizer in $\mathfrak{g}$, and a subgroup of type (C) is the identity component of the centralizer in G, of a maximal toral subalgebra $\mathfrak{t}$ of $\mathfrak{g}$; subgroups of type (C) always contain Cartan subgroups of G, but may be bigger. The map which associates to a closed subgroup of G its Lie algebra yields a one-one correspondence between subgroups of type (C) and Cartan subalgebras, preserving fields of definition (6. 6). The existence of Cartan subalgebras defined over k, which is an easy fact, yields then, as a first step to rationality properties, the existence of subgroups of type (C) defined over k. In fact, G is separably generated by such subgroups (6. 10). Moreover, if k is separably closed, two Cartan subgroups or two Cartan subalgebras defined over k are conjugate under $G(k)$, (6. 13).

§7 gives first some conditions under which the field of definition of a homogeneous space of G can be brought down to k (7. 6). They apply in particular to the set of Cartan subgroups or of Cartan subalgebras of G (7. 7). We then show that both are rational varieties over k (7. 9). The proof is to a large extent an adaptation in our framework of the one given by Grothendieck ([12], Exp. XIV) for the former variety. Some consequences are derived. §8 is devoted to the splitting of a reductive k-group over a separable extension of k.

In characteristic $p \neq 0$, a nilpotent element $X \in \mathfrak{g}(k)$ need not be tangent to a one-dimensional subgroup, even if $X^{[p]}=0$ (9. 2). §9 is mainly concerned with the finding of subgroups to which X is tangent, assuming X to be an eigenvector of a subtorus T of G, corresponding to a non-trivial character b of T. If G is reductive or solvable, X is tangent to a unipotent k-subgroup stable under T, in which the weights of T are certain multiples of b. Sufficient conditions under which H may be chosen to be commutative, or isomorphic to $\boldsymbol{G}_a$, are given (9. 8, 9. 16). As an application, some properties of unipotent groups operated upon by tori are derived.

0. Notations and conventions. *Throughout the paper, k is a commutative field, p its characteristic, K an algebraically closed extension of k, $\bar{k}$ the algebraic closure of k in K, and k_s the separable closure of k in $\bar{k}$. G is an affine k-group, $\mathfrak{g}$ its Lie algebra.*

The notation is basically that of [3], with which familiarity is assumed, with the following additions or modifications.

0.1. Our varieties are those of "classical" algebraic geometry, although not necessarily irreducible, and are all affine or quasi-projective. Algebraic variety defined over k and k-variety will be used synonymously. In order to avoid any ambiguity, let us briefly define that notion in the quasi-projective case. An algebraic subset V of affine (resp. projective) space is defined over

k if the ideal of polynomials (resp. homogeneous polynomials) vanishing on V, with coefficients in $\bar{k}$, is generated by polynomials with coefficients in k. A k-variety is, in this paper, either an affine or projective algebraic set defined over k, or the complement of a k-closed subset in a projective k-variety. For a quasi-projective variety V, the following conditions are equivalent: (i) V is defined over k; (ii) the irreducible components of V are defined over k_s and are permuted by the Galois group of k_s over k, acting by conjugation; (iii) the cycle sum of the irreducible components of V, with coefficients one, is rational over k in the sense of ([27], Chap. VIII, §1). This follows immediately from ([27], Lemma 2, p. 209). Our notion of k-variety is also equivalent to that of absolutely reduced quasi-projective scheme over k. If V is defined over k, the points of V rational over k_s are dense in V (see e.g. S. Lang, Introduction to Algebraic Geometry, Interscience Publ., Prop. 10, p. 76).

0.2. Let V be a k-variety. Then $k[V]$ denotes the k-algebra of regular functions defined over k on V, or, as we shall say, of k-morphic functions on V. The fact that V is defined over k implies that for any extension field k' of k, we have $k'[V] = k[V] \otimes_k k'$. If V is irreducible, $k(V)$ is the field of rational functions on V, defined over k, on V.

The set of points of V rational over an extension field k' of k will be denoted $V(k')$, (and not $V_{k'}$, as in [3]). Often, we let V stand for $V(\bar{k})$, i.e., we identify V with its set of points over $\bar{k}$. The tangent space to V at a simple point x is denoted $T(V)_x$. If $x \in V(k)$, the space $T(V)_x$ carries a canonical k-structure. Let W be a k-variety and $f\colon W \to V$ a k-morphism. If $x \in W(k)$ and $f(x)$ are simple points, f induces a linear map $T(W)_x \to T(V)_{f(x)}$, defined over k, to be denoted df_x and to be called the *differential* of f at x. The map f induces a homomorphism $f^0\colon k[V] \to k[W]$, the "*comorphism*" associated to f. Similarly, if V, W are irreducible, and $f(W)$ is dominant in V, then f induces an injective homomorphism of $k(V)$ into $k(W)$, also to be denoted f^0. We recall that $f\colon W \to V$ is *dominant* if $f(W)$ is dense in V. In that case it contains an open everywhere dense subset of V.

0.3. If A, B are two subsets of a group H, we let $\mathrm{Tr}(A, B)$ or $\mathrm{Tr}_H(A,B)$ be the set of $h \in H$ such that $\mathrm{Int}\, h(A) \subset B$. If $A = B$, then $\mathrm{Tr}(A, B)$ is the normalizer $N_H(A)$ or $N(A)$ of A in H.

0.4. Let $\mathfrak{h}$ be a Lie algebra over k. We let $\mathrm{ad}\, X$ denote the map $Y \mapsto [X, Y]$ of $\mathfrak{h}$ into itself. Let $p \neq 0$. We recall that $\mathfrak{h}$ is *restricted* if it is endowed with a map $[p]\colon X \mapsto X^{[p]}$ into itself, having the following properties:

(a) $(\mathrm{ad}\, X)^p = \mathrm{ad}\, X^{[p]}$

(b) $(a\cdot X)^{[p]} = a^p \cdot X^{[p]} \quad (X \in \mathfrak{h},\ a \in k)$

(c) $(X_1+X_2)^{[p]} = X_1^{[p]} + X_2^{[p]} + \Sigma'_{0<i<p} i^{-1} \cdot s_i(X_1, X_2)$

where $s_i(X_1, X_2)$ is the coefficient of λ^{i-1} in $(\mathrm{ad}(\lambda X_1+X_2))^{p-1}(X_1)$. If s is a positive integer and $q = p^s$, we write $[q]: X \mapsto X^{[q]}$ for the s-th power of $[p]$.

By convention, if $p=0$, any Lie algebra over k is restricted.

0.5. Let $\mathfrak{a}$, $\mathfrak{b}$ be subsets of $\mathfrak{g}$. We put

$$\mathfrak{z}(\mathfrak{a}) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{a}) = \{X \in \mathfrak{g}, [X, \mathfrak{a}] = 0\}\ ,$$

$$Z_G(\mathfrak{a}) = Z(\mathfrak{a}) = \{g \in G, \mathrm{Ad}\, g(X) = X (X \in \mathfrak{a})\}\ ,$$

$$\mathfrak{n}(\mathfrak{a}) = \mathfrak{n}_{\mathfrak{g}}(\mathfrak{a}) = \{X \in \mathfrak{g}, [X, \mathfrak{a}] \subset \mathfrak{a}\}$$

$$N_G(\mathfrak{a}) = N(\mathfrak{a}) = \{g \in G, \mathrm{Ad}\, g(\mathfrak{a}) = \mathfrak{a}\}$$

$$\mathrm{tr}(\mathfrak{a}, \mathfrak{b}) = \{X \in \mathfrak{g}, [X, \mathfrak{a}] \subset \mathfrak{b}\}$$

$$\mathrm{Tr}_G(\mathfrak{a}, \mathfrak{b}) = \mathrm{Tr}(\mathfrak{a}, \mathfrak{b}) = \{g \in G, \mathrm{Ad}\, g(\mathfrak{a}) \subset \mathfrak{b}\}\ .$$

$Z(\mathfrak{a})$ and $N(\mathfrak{a})$ are the *centralizer* and the *normalizer* of $\mathfrak{a}$ in G. (The definition of $\mathfrak{g}$ and of the adjoint representation will be recalled in §1.)

0.6. Let H (resp. H') be a group and A (resp. A') a set on which it operates. Let $f: H \to H'$ be a homomorphism. A map $u: A \to A'$ is *f-equivariant* if $u(h\cdot a) = f(h)\cdot u(a) (h \in H, a \in A)$. If $H = H'$ and $f = \mathrm{id.}$, then u is said to be equivariant or H-equivariant.

1. The Lie algebra of a linear group.

1.1. In this paragraph, we let A stand for the algebra $k[G]$ of k-morphic functions on G. We have $k[G\times G] = A \otimes_k A$, hence the comorphism associated to the product map $\nu: G\times G \to G$ is a homomorphism $\mu: A \to A\otimes A$. We let ι be the inverse map $x \mapsto x^{-1}$ of G and ε the homomorphism $a \mapsto a(e)$ of A into k defined by the neutral element e of G. We have

$$(\varepsilon \otimes \mathrm{id}) \circ \mu = \mathrm{id} = (\mathrm{id} \otimes \varepsilon) \circ \mu\ . \tag{1}$$

The existence of the group law on G is equivalent to a number of properties of μ, ε, ι which can be found, e.g., in [14, 0.8.2].

1.2. The Lie algebra of *G*. The group G operates by left and right translations on $\bar{k}[G] = A \otimes_k \bar{k}$. For $g \in G$, let $\lambda_g, \rho_g: \bar{k}[G] \to \bar{k}[G]$ be defined by

$$\lambda_g a(x) = a(g^{-1} \cdot x)\,, \qquad \rho_g a(x) = a(x \cdot g)\,.$$

Then $\lambda: g \mapsto \lambda_g$ (resp. $\rho: g \mapsto \rho_g$) is a representation of G into $\bar{k}[G]$, called the *left* (resp. *right*) *regular representation of* G *in* $\bar{k}[G]$. The latter space is the union of finite dimensional subspaces, defined over k, stable under λ and ρ. The restriction of λ (resp. ρ) to such a subspace is a rational representation defined over k. The representations λ and ρ commute with each other.

A *k-derivation X of A is left-* (resp. *right-*) *invariant* if its natural extension to $A \otimes \bar{k}$ commutes with the left (resp. right) translations. Left-invariance can also be described by the relation

$$(1) \qquad \mu \circ X = (\mathrm{id} \otimes X) \circ \mu\,.$$

We denote by $L(G)(k)$ the k-vector space of all left invariant k-derivations of A. Endowed with the bracket operation $[X, Y] = X \cdot Y - Y \cdot X$ and the p-th power operation $X^{[p]} = X^p$, it is readily seen to be a restricted Lie algebra over k. If k' is an extension of k, then $L(G)(k') = L(G)(k) \otimes_k k'$. We shall also write $L(G)$ for $L(G)(\bar{k})$ and call $L(G)$ the *Lie algebra of* G. We shall soon identify $L(G)$ and $T(G)_e$. Until then, we let $\mathfrak{g}$ stand for $T(G)_e$. Since e is the identity, it is clear that

$$d\nu_{(e,e)}(X, 0) = d\nu_{(e,e)}(0, X) = X\,, \quad (X \in \mathfrak{g})\,,$$

whence

$$(2) \qquad d\nu_{(e,e)}(X, Y) = X + Y\,, \qquad (X, Y \in \mathfrak{g})\,.$$

Since the composition of the map $G \to G \times G$ defined by $x \mapsto (x^{-1}, x)$, with ν is the constant map, it follows that

$$(3) \qquad (d\iota)_e(X) = -X \quad (X \in \mathfrak{g})\,.$$

Furthermore, using induction and the composition law of differentials, we deduce from (2)

1.3. PROPOSITION. *Let $V_1, \cdots, V_m$ be k-varieties, $u_i \in V_i$, and $f_i : V_i \to G$ a k-morphism which maps u_i onto e. Let $u = (u_1, \cdots, u_m)$ and let f: $V_1 \times \cdots \times V_m \to G$ be the k-morphism defined by $f(v_1, \cdots, v_m) = f_1(v_1) \cdot \cdots \cdot f_m(v_m)$. Then $df_u(X_1, \cdots, X_m) = df_1(X_1) + \cdots + df_m(X_m)$ $(X_i \in T(V_i)_{u_i}$, $i = 1, \cdots, m)$.*

1.4. In this section and the following, $\mathfrak{g}$ stands for $T(G)_e$. We recall that $\mathfrak{g}(k)$ may be viewed as the k-vector space of k-derivations of A into k, where k is made into an A-module by means of ε. Let now $X \in L(G)(k)$. We associate to X a k-linear map $\sigma(X)$ of A into k by

$$(1) \qquad \sigma(X)(a) = \varepsilon \cdot Xa = Xa(e), \quad (a \in A).$$

X is in fact a k-derivation of A into k, hence σ is a k-linear map of $L(G)(k)$ into $\mathfrak{g}(k)$, obviously compatible with field extensions.

On the other hand,

$$(2) \qquad \tau(Y) = (\mathrm{id} \otimes Y) \circ \mu, \quad (Y \in \mathfrak{g}(k)),$$

is a derivation of A into A. The obvious equality

$$(3) \qquad \mu \circ \lambda_g = (\lambda_g \otimes \mathrm{id}) \circ \mu,$$

shows at once that $\mathrm{id} \otimes \tau(Y)$ and $\lambda_g (g \in G)$ commute. Therefore τ is a k-linear map of $\mathfrak{g}(k)$ into $L(G)(k)$.

1.5. PROPOSITION. *We keep the previous notation. σ and τ are isomorphisms, inverse of each other. In particular,* $\dim_k L(G)(k) = \dim G$, *and* $L(G) = L(G^0)$.

To prove 1.5, we may assume $k = \bar{k}$. It suffices to show that σ is injective and that $\sigma \circ \tau = \mathrm{id}$. Let $\sigma(X) = 0$. Then, by 1.4(1), applied to $\lambda_g a$, $(g \in G, a \in A)$, we get $Xa(g) = 0$, whence $X = 0$. Let $X \in \mathfrak{g}(k)$. Then, in view of 1.1(1), 1.2(1):

$$\sigma \circ \tau(X) = (\mathrm{id} \otimes \varepsilon) \circ (\mathrm{id} \otimes X) \circ \mu = (\mathrm{id} \otimes \varepsilon) \circ \mu \circ X = X.$$

From now on, we identify $L(G)(k)$ and $\mathfrak{g}(k)$ via σ. Thus $\mathfrak{g}(k)$ is canonically endowed with a structure of restricted Lie algebra over k. An explicit description of this structure is as follows: for a positive integer s, let $\mu^{(s)} : A \to \otimes^s A$ be the comorphism defined by the product map $G^s \to G$. For $a \in A$, let us write

$$(1) \qquad \mu^{(s)} a = \Sigma_i a_{i,1} \otimes \cdots \otimes a_{i,s}.$$

Then, for $s = 3$, we have

$$(2) \qquad [X, Y]a = \Sigma_i (Xa_{i1} \cdot Ya_{i2} - Ya_{i1} \cdot Xa_{i2})\, a_{i3}(e), \quad (X, Y \in \mathfrak{g}(k)),$$

and, if $p > 0$, for $s = p+1$

$$(3) \qquad X^{[p]}a = \Sigma_i (Xa_{i1} \cdot \cdots \cdot Xa_{ip}) \cdot a_{i,p+1}(e), \quad (X \in \mathfrak{g}(k)),$$

as follows from 1.4(2).

1.6. Let H be a k-group and $f\colon H \to G$ a k-morphism. Then $df_e\colon \mathfrak{h}(k) \to \mathfrak{g}(k)$ is a homomorphism of restricted Lie algebras over k, as follows from 1.5 (2), (3), and it is then clear that $G \mapsto L(G)(k)$ is a functor from the category of k-groups and k-morphisms to the category of restricted Lie algebras over k. We write also $L(f)$ or df for df_e. If f is the inclusion of a subgroup, then $L(f)$ identifies $L(H)$ with a restricted subalgebra of $L(G)(k)$.

1.7. Examples. (a) $G = \boldsymbol{G}_a$, the additive group of the one-dimensional vector space. We have $A = k[T]$ and $\mu(T) = T\otimes 1 + 1\otimes T$, $\mathcal{E}(T) = 0$. An easy computation, based on 1.5(2), (3), shows that $\mathfrak{g}$ is one-dimensional and $\mathfrak{g}^{[p]} = 0$.

(b) $G = \boldsymbol{GL}_n$. Then $A = k[T_{11}, T_{12}, \cdots, T_{nn}, D^{-1}]$, where $D = \det(T_{ij})$, $(1 \leqq i, j \leqq n)$. The comorphism $\mu\colon A \to A\otimes A$ is given by

$$(1)\qquad \mu(T_{ij}) = \Sigma_k T_{ik} \otimes T_{kj},$$

and

$$(2)\qquad \mathcal{E}(T_{ij}) = \delta_{ij}, \quad (1 \leqq i, j \leqq n).$$

$X \in \mathfrak{g}(k)$ is determined by the elements $a_{ij} = XT_{ij}$ of k, hence by a matrix $(a_{ij}) \in \boldsymbol{M}_n(k)$. In the notation of 1.4, we have, by 1.4(2):

$$(3)\qquad \tau(X)(T_{ij}) = \Sigma_k T_{ik} \cdot a_{kj}.$$

It follows from (3) that $X \mapsto (XT_{ij})$ identifies $\mathfrak{g}(k)$ with $\boldsymbol{M}_n(k)$, endowed with the usual commutator $[X, Y] = XY - YX$, and the *ordinary* p-th power as $[p]$-operation.

(c) $G = T$ is a torus and $p > 0$. Then $\mathfrak{g}$ is commutative, $[p]$ is a bijective F_p-linear map of $\mathfrak{g}(\bar{k})$ onto itself, where F_p is the Frobenius automorphism $x \mapsto x^p$ of $\bar{k}$. The set $\mathfrak{g}_0$ of fixed elements of $[p]$ is a vector space over the prime field $\boldsymbol{F}_p$ with p elements, such that $\mathfrak{g}(\bar{k}) = \mathfrak{g}_0 \otimes \bar{k}$. If T splits over k, then $\mathfrak{g}_0 \subset \mathfrak{g}(k)$ and $\mathfrak{g}(k) = \mathfrak{g}_0 \otimes k$ (the tensor products being over $\boldsymbol{F}_p$).

Let X_* be the group of morphisms of $\boldsymbol{GL}_1$ into T. It is a free abelian group of rank equal to $\dim T$. Let us associate to $x \in X_*$ the element $dx(1) \in \mathfrak{g}(\bar{k})$. This is a homomorphism, which induces a surjective homomorphism $f\colon X_* \otimes \bar{k} \to \mathfrak{g}(\bar{k})$. The image of X_* is pointwise fixed under $[p]$, and contains a basis of $\mathfrak{g}$ over k. If T splits over k, then $f(X_* \otimes 1) = \mathfrak{g}_0$. All these facts follow readily from (b), since T splits over $\bar{k}$, and a k-split torus is a direct product over k of some copies of $\boldsymbol{GL}_1$.

1.8. The adjoint representation. Let $X \in L(G)$. Since left translations commute with right translations

$$\operatorname{Ad} g(X) = \lambda_g \circ X \circ \lambda_g^{-1} \quad (g \in G)$$

is again an element of $L(G)$. From the definition of the bracket and p-th power operations in $L(G)$, it is clear that $\operatorname{Ad} g$ is an automorphism of $L(G)$. The map $g \mapsto \operatorname{Ad} g$ is a representation of G into $L(G)$, to be called the *adjoint representation* of G. If we identify $\mathfrak{g}(\bar{k})$ and $L(G)$ by τ, we see immediately that $\operatorname{Ad} g$ *is the differential at e of the inner automorphism* $\operatorname{Int} g : x \mapsto g \cdot x \cdot g^{-1}$. If $f \colon H \to G$ is a k-morphism, then

$$(1) \qquad L(f)(\operatorname{Ad} h(X)) = \operatorname{Ad} f(h)(L(f)(X)) \quad (X \in L(H),\ h \in H).$$

1.9. PROPOSITION. *The adjoint representation of G is a k-morphism of G into* $GL(\mathfrak{g})$. *The differential of* Ad *is the homomorphism* ad: $X \mapsto \operatorname{ad} X$ *defined by* $\operatorname{ad} X(Y) = [X, Y]$ $(X, Y \in \mathfrak{g})$.

In view of 1.8(1), it suffices to prove that if H is a k-subgroup of $\boldsymbol{GL}_n$ and $\mathfrak{m}$ a subspace defined over k of $\mathfrak{gl}_n$ stable under $\operatorname{Ad} g$ $(g \in H)$, (where Ad is the adjoint representation of $\boldsymbol{GL}_n$), then the representation $h \mapsto \operatorname{Ad} h|_{\mathfrak{m}}$ of h into $\mathfrak{m}$ is defined over k, and its differential is $\operatorname{ad} X|_{\mathfrak{m}}$. This follows readily from the formula

$$(1) \qquad \operatorname{Ad} g(X) = g \cdot X \cdot g^{-1} \quad (g \in \boldsymbol{GL}_n,\ X \in \mathfrak{gl}_n)$$

which in turn is a simple consequence of 1.7(3).

1.10. Applications. (a) We identify $T(G)_g$ to $\mathfrak{g}$ by means of the left translation $l_g : x \mapsto g \cdot x$. Then, by definition $(dl_g)_e = \mathrm{id}$. The right translation $r_g : x \mapsto x \cdot g$ can be written as $l_g \circ \operatorname{Int} g^{-1}$. Therefore $(dr_g)_e = \operatorname{Ad} g^{-1}$. As a consequence the differential at e of the map $g \mapsto g \cdot a \cdot g^{-1}$ is $(\operatorname{Ad} a^{-1} - \mathrm{Id})$.

(b) Let $X \in \mathfrak{g}$. Identify the tangent space to $\mathfrak{g}$ at X in the usual manner to $\mathfrak{g}$. Then the differential at e of $g \mapsto \operatorname{Ad} g(X)$ is $-\operatorname{ad} X$. This follows, e.g., from 1.9(1).

1.11. PROPOSITION. *Let L, M be two connected k-subgroups of G and $Q = (L, M)$ be the group generated by the commutators $(x, y) = x \cdot y \cdot x^{-1} \cdot y^{-1}$ $(x \in L,\ y \in M)$. Then the Lie algebra $\mathfrak{q}$ of Q contains all elements of the form* $\operatorname{Ad} x(X) - X$ $(x \in L,\ X \in \mathfrak{m})$ *or* $(x \in M,\ X \in \mathfrak{l})$ *and all commutators* $[X, Y]$, $(X \in \mathfrak{l},\ Y \in \mathfrak{m})$.

(We recall that Q is a connected k-group, see, e.g., ([1], Lemme 4.3).) Let $x \in L$. Then $y \mapsto x \cdot y \cdot x^{-1} \cdot y^{-1}$ $(y \in M)$, may be viewed as the composition of the two morphisms (of varieties) $y \mapsto x \cdot y \cdot x^{-1}$ and $y \mapsto y^{-1}$ of M into Q, with the product in Q. By 1.2, its differential at (e, e) is the sum of the differential of $\operatorname{Int} x$, which is $\operatorname{Ad} x$, and of the differential $-\operatorname{Id}$ of $y \mapsto y^{-1}$ (see 1.2(3)). Thus $\operatorname{Ad} x(X) - X \in \mathfrak{q}$ if $X \in \mathfrak{m}$. Similarly, $\operatorname{Ad} x(X) - X \in \mathfrak{q}$ if $x \in M$, $X \in \mathfrak{l}$.

Let $X \in \mathfrak{m}$. Then $x \mapsto \operatorname{Ad} x(X) - X$ is a morphism of L into $\mathfrak{q}$, whose differential at e is $Y \mapsto \operatorname{ad} Y(X) = [Y, X]$, $(Y \in \mathfrak{l})$, whence the second assertion.

1.12. COROLLARY. (i) *If G is solvable (resp. nilpotent, resp. commutative), then $\mathfrak{g}$ is solvable (resp. nilpotent, resp. commutative).* (ii) *The Lie algebra $\mathfrak{z}$ of the center Z of G belongs to the center of $\mathfrak{g}$.*

REMARK. If $p > 0$, the converse to (i) or (ii) is well known to be false. To mention one example, $\mathfrak{sl}_2$ is solvable with one-dimensional center if $p = 2$, while $\boldsymbol{SL}_2$ is simple.

1.13. Separable morphisms. Let X, Y be irreducible k-varieties and $f \colon X \to Y$ a dominant k-morphism. The comorphism f^0 defines a monomorphism of $k(Y)$ into $k(X)$. f is said to be *separable* if $k(X)$ is a separable extension of $k(Y)$. It is then so for every extension k' of k. We recall that the following conditions on f are equivalent:

(i) f is dominant, separable.

(ii) f is dominant. There exists a simple point $a \in X$ whose image b is simple and such that $df_a : T(X)_a \to T(Y)_b$ is surjective.

(iii) There exists an open dense subset U of X, consisting of simple points, whose image consists of simple points, and such that df_x is surjective for all $x \in U$.

Let $F_x = f^{-1}(f(x))$ be the fibre through $x \in X$. Let m be a positive integer. It is well kown that the set of points for which $\dim F_x \geqq m$ is closed, and that $\min \dim F_x = \dim X - \dim f(X)$, and so $\dim F_x = \dim X - \dim f(X)$ for x in an open dense subset of X. Also the set of points for which $\dim \ker df_x \geqq m$ is closed. If x is simple on X and F_x, then $T(F_x)_x \subset \ker df_x$. It follows then that the minimum of $\dim \ker df_x$ is attained on a non-empty open set, and is $\geqq \dim X - \dim f(X)$.

(ii) $\Longrightarrow$ (iii). We have $\dim \ker df_a = \dim X - \dim f(X)$, hence by the above, there is an open set U in X such that $\dim \ker df_x = \dim \ker df_a$ for $x \in U$, whence (iii).

(iii) $\Longrightarrow$ (ii). We have $\dim \operatorname{Im} df_x \leqq \dim f(X)$ for all simple $x \in X$, hence df_x cannot be surjective if $\dim f(X) < \dim Y$, which implies that f is dominant. For the equivalence (i) $\Longleftrightarrow$ (iii), see, e.g., ([27], Prop. 15, p. 12, and Chap. IV, §6).

We shall be mainly concerned with the case where X, Y are smooth over k, X is affine, f is surjective, and df_x is surjective for every $x \in X$. In this case, if Z is a closed subvariety defined over k of Y, then $f^{-1}(Z)$ is defined over k. In fact, $f^{-1}(Z)$ is obviously k-closed. By (0.1), it suffices to show that its irreducible components are defined over k_s. We may therefore assume Z to be irreducible. The assumptions imply that $X \times Z \subset X \times Y$ cuts the graph of f transversally, therefore the cycle sum of the irreducible components of $f^{-1}(Z)$, each affected with coefficient one, is rational over k ([27], Thm. 6, p. 200, Thm. 4, p. 223). But (0.1) this is equivalent to $f^{-1}(Z)$ being defined over k as an algebraic set. In particular $f^{-1}(Z)(k_s) \neq \emptyset$. If we apply this to the k_s-points of Y, we see that $f(X(k_s)) = Y(k_s)$.

1.14. Separable actions. Let G act k-morphically on the k-variety X. We say that G acts separably if, for each $x \in X$, the map φ_x: $g \mapsto g \cdot x$ is a separable map of G onto the orbit $G(x)$ of x. In view of 1.13, this is the case if and only if the kernel of $(d\varphi_x)_e$ is the Lie algebra of the stability group G_x of x. It suffices of course to check this condition for one point of each orbit.

1.15. Generation by subgroups. Assume G to be connected. Let $\mathcal{M} = (H_i)_{1 \leq i \leq m}$ be a family of connected k-subgroups of G. We say that $\mathcal{M}$ *spans* G (separably) if the product morphism f: $H_1 \times \cdots \times H_m \to G$ is surjective (and separable). Assume now that $\mathcal{M}$ *generates* G, i.e., that no proper closed subgroup of G contains all the H_i's. It is then known that there exists a family $\mathcal{M}' = (H'_j)_{1 \leq j \leq n}$, such that each H'_j is one of the H_i's, which spans G. We say that $\mathcal{M}$ *generates G separably* if there exists such an $\mathcal{M}'$ which spans G separably.

1.16. PROPOSITION. *Let G be connected, and $(H_i)_{1 \leq i \leq m}$ a family of connected k-subgroups of G.*

(i) *If the Lie algebras $\mathfrak{h}_i$ span $\mathfrak{g}$, then (H_i) generates G separably.*

(ii) *If (H_i) generates G separably, then $\mathfrak{g}$ is spanned by the subalgebras* $\mathrm{Ad}\, g(\mathfrak{h}_i)$, $(i = 1, \cdots, m,\ g \in G)$.

(i) Let H be the subgroup generated by the H_i. It is a connected k-subgroup whose Lie algebra contains the $\mathfrak{h}_i$, hence is equal to $\mathfrak{g}$. Therefore (1.5), $\dim H = \dim G$, and $H = G$. Thus the H_i generate G. If (H'_j) is a family consisting of elements of (H_i), which spans G, then the differential of the product morphism at e is surjective, whence the separability (1.13).

(ii) Let $(H'_j)_{1 \leq j \leq n}$ span G separably, where each H'_j is one of the H_i's. There exists then a point $h = (h_1, \cdots, h_n)$ $(h_j \in H'_j)$ such that df_h is surjective.

After having made a translation by $f(h)^{-1}$ we may assume that $f(h) = e$. Put now

$$v_i = h_1 \cdots h_i, \quad H_i'' = \mathrm{Int}\, v_i(H_i') \qquad (1 \leqq i \leqq n).$$

Let q be the isomorphism

$$\mathrm{Int}\, v_1 \times \cdots \times \mathrm{Int}\, v_n \colon \; H_1' \times \cdots \times H_n' \to H_1'' \times \cdots \times H_n'',$$

and r the product morphism: $H_1'' \times \cdots \times H_n'' \to G$. Then $r \circ q$ is the map $(x_1, \cdots, x_n) \mapsto h_1 \cdot x_1 \cdots h_n \cdot x_n \cdot v_n^{-1}$. Therefore, $d(r \circ q)_e$ is surjective. But (1.3) the image of dr_e is $\mathfrak{h}_1'' + \cdots + \mathfrak{h}_m''$. Since $\mathfrak{h}_i'' = \mathrm{Ad}\, v_i(\mathfrak{h}_i')$, this proves our contention.

1.17. Example. Let $G = \boldsymbol{SL}_2$. Then $\mathfrak{g} = \mathfrak{sl}_2$ is the Lie algebra of 2×2 matrices with trace zero. Let T be the torus of G consisting of the diagonal matrices of determinant one. Its Lie algebra $\mathfrak{t}$ is the Lie algebra of diagonal 2×2 matrices with trace zero. Let now $p = 2$. Then $\mathfrak{t}$ consists of scalar matrices and is pointwise fixed under the adjoint representation. Since the 1-dimensional tori of G are conjugate by inner automorphisms it follows that $\mathfrak{t}$ is the Lie algebra of any such torus. Thus $\mathfrak{g}$ is not generated by the Lie algebras of the tori of G, although G is generated by its tori, in fact, by two suitably chosen tori.

1.18. PROPOSITION. *Let G' be a k-group and $f \colon G \to G'$ a surjective k-morphism. Let H' be a k-subgroup of G' and $H = f^{-1}(H')$. Assume that $\mathfrak{g}' = \mathfrak{h}' + df(\mathfrak{g})$. Then G acts separably on G'/H' via f, the group H is defined over k, and f induces an f-equivariant k-isomorphism of G/H onto G'/H'.*

Let $\pi \colon G' \to G'/H'$ be the canonical projection. Then $d\pi_e$ is surjective with kernel $\mathfrak{h}'$, therefore $d(\pi \circ f)_e$ is surjective, and $\pi \circ f$ is surjective, separable. Then, $H = f^{-1}(\pi(H'))$ is defined over k (1.13), and f induces a bijective f-equivariant k-morphism $\bar{f}$ of G/H onto G'/H'. In view of the assumption $d\bar{f}$ is surjective at the origin, hence $\bar{f}$ is an isomorphism.

2. Solvable subgroups. The following lemma is a Lie algebra analogue of [1, Prop. 17.1]. Mcre general results may be found in [12, Exp. XIII, §1].

2.1. LEMMA. *Let H be a closed subgroup of G. Assume that there exists $X \in \mathfrak{h}$ such that the set* $\mathrm{Tr}(X, \mathfrak{h})$ *of $g \in G$ for which* $\mathrm{Ad}\, g(X) \in \mathfrak{h}$ *consists of finitely many left classes* $\mathrm{mod}\, H$. *Then* $N_G(\mathfrak{h})^0 = H^0$, *and*

$V = \cup_{g \in G} \operatorname{Ad} g(\mathfrak{h})$ *contains an open non-empty subset of* $\mathfrak{g}$. *If* G/H *is complete, then* $V = \mathfrak{g}$.

$N_G(\mathfrak{h})$ is a closed subgroup of G contained in $\operatorname{Tr}(X, \mathfrak{h})$, hence its identity component is equal to H^0.

Let M be the set of pairs (gH, Y) in $G/H \times \mathfrak{g}$ such that $\operatorname{Ad} g^{-1}(Y) \in \mathfrak{h}$. We claim that M is a closed subvariety of $G/H \times \mathfrak{g}$. To see this, we consider the morphisms

$$\begin{tikzcd} G \times \mathfrak{h} \arrow[r, "a"] & G \times \mathfrak{g} \arrow[r, "b"] & G/H \times \mathfrak{g}, \end{tikzcd}$$

where $a(g, Y) = (g, \operatorname{Ad} g(Y))$ and b is the canonical projection on the first factor, the identity on the second factor. The morphism a is a closed immersion, hence $\operatorname{Im} a$ is closed. Clearly, $(g, Y) \in \operatorname{Im} a$ implies $(g \cdot H, Y) \in \operatorname{Im} a$, hence $\operatorname{Im} a = b^{-1}(b(\operatorname{Im} a))$ and $\operatorname{Im}(b \circ a)$ is closed. But $\operatorname{Im}(b \circ a) = M$. The morphism $p_1 \colon M \to G/H$ induced by the projection of $G/H \times \mathfrak{g}$ onto its first factor is surjective, and its fibres are isomorphic to $\mathfrak{h}$, hence $\dim M = \dim G/H + \dim \mathfrak{h} = \dim G$. Let now $p_2 \colon M \to \mathfrak{g}$ be the morphism induced by the projection on the second factor. By definition $V = \operatorname{Im} p_2$. By assumption, at least one fibre of p_2 consists of finitely many points, hence $\dim V = \dim M = \dim \mathfrak{g}$, which implies our first assertion. If G/H is moreover complete, then p_2 is a closed morphism, and V is also closed, which yields the last part of the lemma.

2.2. A *Borel subalgebra* $\mathfrak{b}$ of $\mathfrak{g}$ is a subalgebra which is the Lie algebra of a Borel subgroup of G. The conjugacy of Borel subgroups by inner automorphisms of G^0 implies the conjugacy of Borel subalgebras under $\operatorname{Ad} G^0$. The main result on Borel subalgebras is 2.3, due to A. Grothendieck ([12], Exp. XIV, Thm. 4.11, p. 33). The proof presented here is somewhat different from that of Grothendieck's. It was sketched in [4].

2.3. PROPOSITION. *The Lie algebra* $\mathfrak{g}$ *is the union of its Borel subalgebras.*

Let R be the radical of G (i.e., the greatest connected solvable normal subgroup of G). It is contained in every Borel subgroup and its Lie algebra is contained in all Borel subalgebras of $\mathfrak{g}$. We may therefore replace G by G/R and assume G to be semi-simple.

Let B be a Borel subgroup of G, T a maximal torus of B and Φ the set of roots of G with respect to T. We let Δ denote the set of simple roots for the ordering defined by B. We have

(1) $$\mathfrak{g} = \mathfrak{t} \oplus \Sigma_{a\in\Phi}\mathfrak{g}_a \qquad \mathfrak{b} = \mathfrak{t} + \Sigma_{a>0}\mathfrak{g}_a$$

where

(2) $$\mathfrak{g}_a = \{X \in \mathfrak{g},\ \mathrm{Ad}\,t(X) = t^a \cdot X\}\ .$$

Furthermore, given $b \in \Phi$, there is an isomorphism θ_b of $\boldsymbol{G}_a$ onto a unipotent subgroup U_b of G such that

(3) $$\theta_b(t^b \cdot x) = t \cdot \theta_b(x) \cdot t^{-1} \qquad (x \in \boldsymbol{G}_a,\ t \in T),$$

and $\mathfrak{g}_b$ is the Lie algebra of U_b. Since G/B is complete, 2.3 will follow from 2.1 and the following lemma

2.4. LEMMA. *We keep the notation of* 2.3. *Let* X_a *be a non-zero element of* $\mathfrak{g}_a$ $(a \in \Delta)$ *and* $X = \Sigma_{a\in\Delta}X_a$. *Then* $\{g \in G,\ \mathrm{Ad}\,g(X) \subset \mathfrak{b}\} = B$.

Let U be the unipotent radical of B, and W the Weyl group $N(T)/T$. For $w \in W$, let n_w be a representative of w in $N(T)$. Let $g \in \mathrm{Tr}(X, \mathfrak{b})$. By the Bruhat decomposition [10, Exp. 13], we have $g = b' \cdot n_w \cdot b$ $(b, b' \in B)$, with $b \in U$, $b' \in B$. Since $\mathrm{Ad}_G B(\mathfrak{b}) = \mathfrak{b}$, we may assume $b' = e$. By 1.11, $\mathrm{Ad}\,b(X) - X$ lies in the Lie algebra of the commutator subgroup (U, U) of U. But (U, U) is contained in the subgroup of U generated by the $U_c (c > 0,\ c \notin \Delta)$ (see, e.g., [3], Prop. 2.5, p. 66), hence

$$\mathrm{Ad}\,b(X) - X \in \Sigma_{c>0, c\notin\Delta}\,\mathfrak{g}_c\ .$$

We conclude that

$$\mathrm{Ad}\,g(X) = \Sigma_{a\in\Phi}\xi_a X_{w(a)}$$

with $\xi_a \neq 0$ if $a \in \Delta$. Since the $w(a)$ are distinct roots, the $X_{w(a)}$ are linearly independent, and $\mathrm{Ad}\,g(X) \in \mathfrak{b}$ implies that $w(a) > 0$ for $a \in \Delta$. As is well known, we have then $w = e$, hence $g \in B$.

2.5. PROPOSITION. *Assume* G *to be connected. Let* U *be the unipotent radical and* T *a maximal torus of* G. *There exist two Borel subgroups* B, B' *of* G, *which generate* G *separably, such that* $B \cap B' = T \cdot U$ *and* $\mathfrak{g} = \mathfrak{b} + \mathfrak{b}'$, $\mathfrak{b} \cap \mathfrak{b}' = \mathfrak{t} + \mathfrak{u}$.

It suffices to prove this for the reductive group G/U. For the latter take two opposed Borel subgroups containing T (see [3], 2.3, p. 64).

2.6. PROPOSITION. *Assume* G *to be connected. Let* P *be a parabolic subgroup of* G. *Then* $P = N_G(\mathfrak{p})$.

Let B be a Borel subgroup of G contained in P and let $Q = N_G(\mathfrak{p})$. The Borel subalgebras of $\mathfrak{q}$ are the conjugates of $\mathfrak{b}$, hence are contained in $\mathfrak{p}$. We have then $\mathfrak{p} = \mathfrak{q}$ by either 2.3 or 2.5. Since parabolic subgroups of a connected group are connected, it follows that $P = Q$.

2.7. For the sake of reference we recall here some facts about groups over finite fields.

Let k be finite. Then G has a Cartan subgroup (resp. maximal torus, resp. Borel subgroup) defined over k. Any two Borel subgroups defined over k are conjugate by an element of $G(k)$. Let H be a k-group and f: $G \to H$ a surjective k-morphism. Then a Cartan subgroup (resp. maximal torus, resp. Borel subgroup) defined over k of H is the image of such a subgroup of G.

For the existence, see [17, p. 45], or apply Lang's theorem [16] to the variety of maximal tori or of Borel subgroups (see §7). The conjugacy follows from Lang's theorem, too.

2.8. Let k be finite, G be connected reductive. Let B and $T \subset B$ be a Borel subgroup and a maximal torus of G defined over k. Then the Borel subgroup B' opposed to B and containing T is defined over k. Since the unipotent radical of a k-group is defined over k when k is perfect, it follows from 2.7 that if k is finite, we may choose B, B' and T in 2.5 to be defined over k. We want to use this remark to prove 2.9, which answers a question raised in ([12], Exp. XIV, p. 46). A proof has also been given by Steinberg (unpublished).

2.9. PROPOSITION. *Let k be finite and G be connected. Then G is generated by its Cartan subgroups which are defined over k.*

Let B, B', T as in 2.8. Since the Cartan subgroups defined over k of a k-group are the centralizers of its maximal tori defined over k, we see that the Cartan subgroups defined over k of B or B' are contained in Cartan subgroups defined over k of G. Consequently, it is enough to consider the case where G is solvable, where we proceed by induction on $\dim G$. If G is nilpotent, in particular if $\dim G = 1$, our assertion is obvious. Let U be the unipotent part of G and N a non-trivial connected normal k-subgroup of G contained in the center of U, of minimal dimension. Let H be the subgroup of G generated by the Cartan subgroups of G defined over k. If we apply the induction assumption to G/N, and use 2.7, we see that $G = H \cdot N$. Let T' be a maximal torus of G/N defined over k and L its inverse image in G. By 2.7, the maximal tori of L are maximal tori in G, hence the Cartan subgroups defined over k of L are contained in Cartan subgroups defined over

k of G. If $L \neq G$, then, by induction, L is generated by Cartan subgroups defined over k. Since $N \subset L$, this proves our assertion in this case.

There remains to consider the case where $G/N=T'$. Then (2.7), $G=T \cdot N$ where T is a maximal torus defined over k of G. Furthermore, the assumptions made on N imply that N has no proper non-trivial connected subgroup normalized by T. In particular, if $H \cap N \neq N$, then $(H \cap N)^0 = \{e\}$ and $H=T$, and since $Z(T)$ is connected [1, §13], we have either $Z(T) \cap N=N$, and then $G = Z(T)$ is its own Cartan subgroup, or $Z(T) \cap N=\{e\}$. So assume $Z(T) \cap N=\{e\}$. In view of the minimality assumption on N, we have $N^p=\{e\}$, hence ([18], Prop. 1,2, p. 688), N is isomorphic over k to a product of groups $\mathbf{G}_a$. In particular $N(k)$ has at least two elements. Let $x \in N(k)$, $x \neq e$. Then $x \cdot T \cdot x^{-1}$ is defined over k. Since $Z(T) \cap N=\{e\}$ and since in a connected solvable group, the centralizer and the normalizer of a torus coincide ([1], Prop. 10.2 p. 52), we have $x \cdot T \cdot x^{-1} \neq T$, hence $H \neq T$, $H \cap N \neq \{e\}$ and finally $H \supset N$, $G=H$.

2.10. Let H be a k-group. As in [3, 0.4], we say that it acts k-morphically on G if it acts k-morphically on the underlying variety of G and if, for each $h \in H$, the map φ_h: $g \mapsto h \cdot g$ is an automorphism of G. Then $h \mapsto (d\varphi_h)_e$ is a k-morphism of H into the group $\mathrm{Aut}(\mathfrak{g})$ of automorphisms of the restricted Lie algebra $\mathfrak{g}$.

2.11. PROPOSITION. *Assume G to be connected. Let S be a k-torus which acts k-morphically on G. Then S acts trivially on G if and only if it acts trivially on $\mathfrak{g}$.*

The necessity of the condition is obvious.

The set of $s \in S$ whose centralizer in $\mathfrak{g}$ is equal to that of S is a non-empty open subset A (consisting of the elements which do not annihilate the non-trivial weights of S in $\mathfrak{g}$). Similarly the set B of $s \in S$ whose centralizer in G is equal to $Z(S)$ contains an open non-empty set [3, 1.10, p. 62]. The sufficiency then follows from [3, 10.1] applied to an element of $A \cap B$.

3. Jordan decomposition in the Lie algebra of an algebraic group.

3.1. An element $X \in \mathfrak{g}$ is *semi-simple* (resp. *nilpotent*) if it belongs to the Lie algebra of a subtorus (resp. unipotent subgroup) of G.

(a) *Any element $X \in \mathfrak{g}$ can be written uniquely as $X = X_s + X_n$ where X_s is semi-simple, X_n is nilpotent and $[X_s, X_n] = 0$. If f: $G \rightarrow H$ is a morphism then $df(X_s) = (df(X))_s$, $df(X_n) = (df(X))_n$. If $G = \mathbf{GL}_n$ then $X=X_s+X_n$ is the Jordan decomposition of the linear transformation X.*

For the proof see [4]. The decomposition $X = X_s+X_n$ is called the

Jordan decomposition of X, and X_s (resp. X_n) is the *semi-simple* (resp. *nilpotent*) *part* of X. We state some consequences of (a).

(b) *If k is perfect, and $X \in \mathfrak{g}(k)$, then $X_s, X_n \in \mathfrak{g}(k)$.*

To see this we may identify G to a k-subgroup of $\boldsymbol{GL}_n$, and then we use the corresponding fact for the Jordan decomposition of a linear transformation over a perfect field.

(c) *Let G be connected, solvable. Then $X \in \mathfrak{g}$ is nilpotent if and only if it is tangent to the unipotent part of G.*

This follows from the fact that the unipotent radical of G contains all unipotent elements of G [1, Prop. 10.1, p. 52].

(d) *Let G be connected. It is a torus (resp. a unipotent group) if and only if its Lie algebra consists of semi-simple (resp. nilpotent) elements.*

The necessity of the condition is obvious. Let $g \in G$. It belongs to a Borel subgroup B of G, which, in view of (c) is a torus (resp. unipotent group). Thus g is semi-simple (resp. unipotent). We then use the fact that a connected group consisting of semi-simple (resp. unipotent) elements is a torus (resp. unipotent group) [1, §19].

3.2. PROPOSITION. *Let $p>0$. Then the p-th power operation $[p]$ is a k-morphism of $\mathfrak{g}$ into itself, which maps the set of semi-simple (resp. nilpotent) elements onto (resp. into) itself. There exists a power q of p such that $X^{[q]} = X_s^{[q]}$ for all $X \in \mathfrak{g}$. The image of $[q]$ is the set of semi-simple elements of $\mathfrak{g}$.*

We may assume $\mathfrak{g} \subset \mathfrak{gl}_n$. Then (1.7(b)), $X^{[p]} = X^p$, which proves that $[p]$ is a k-morphism of $\mathfrak{g}$ into itself leaving the set of semi-simple (resp. nilpotent) elements stable. Moreover, $X^{[q]} = 0$ if $q > n$ and X is nilpotent. For such a q we have then, since $[X_s, X_n] = 0$,

$$X^{[q]} = (X_s + X_n)^{[q]} = X_s^{[q]} + X_n^{[q]} = X_s^{[q]},$$

which shows that $\operatorname{Im}[q]$ consists of semi-simple elements. On the other hand, $[p]$ is surjective on $\mathfrak{g}$ if G is a torus (1.7(c)), hence $\operatorname{Im}[p^s]$ contains the set of semi-simple elements of $\mathfrak{g}$ for every $s \geqq 1$.

3.3. Let X be a non-zero nilpotent element of $\mathfrak{g}(k)$. If $p=0$, then it is well known that X is tangent to a unique one-dimensional unipotent k-subgroup U of G. If $G \subset \boldsymbol{GL}_n$, then U is the set of elements

$$\exp s \cdot X = \Sigma_{n \geqq 0} (n!)^{-1} \cdot s^n \cdot X^n$$

(see, e.g., [8], Prop. 1, p. 159).

However, if $p > 0$, there is not always a one-dimensional unipotent subgroup U of G whose Lie algebra is spanned by X. We shall come back to this question in §9.

4. Toral subalgebras.

4.1. PROPOSITION. *Let $X \in \mathfrak{g}(k)$ be semi-simple. Then $\mathfrak{z}(X)$ is the Lie algebra of $Z(X)$, and $Z(X)$ is defined over k. The conjugacy class $\operatorname{Ad} G(X)$ of X in $\mathfrak{g}$ is closed, and the map $g \mapsto \operatorname{Ad} g(X)$ induces a k-isomorphism of $G/Z(X)$ onto $\operatorname{Ad} G(X)$.*

By ([4], 1.5, 1.6, p. 28), $\operatorname{Ad} G(X)$ is closed in $\mathfrak{g}$, and $\mathfrak{z}(X)$ is the Lie algebra of $Z(X)$. Since $\operatorname{ad} X$ is semi-simple, we have $\mathfrak{g} = \mathfrak{z}(X) + [X, \mathfrak{g}]$. On the other hand (1.10), the differential of $f\colon g \mapsto \operatorname{Ad} g(X)$ at e is $-\operatorname{ad} X$. Therefore f is a separable map of G onto $\operatorname{Ad} G(X)$, which implies the other assertions of the proposition.

4.2. DEFINITION. A subalgebra $\mathfrak{S}$ of $\mathfrak{g}$ is called a *toral subalgebra* if it consists of semi-simple elements.

4.3. PROPOSITION. *Let $\mathfrak{S}$ be a toral subalgebra of $\mathfrak{g}$ which is defined over k. Then $\mathfrak{z}(\mathfrak{S})$ is the Lie algebra of $Z(\mathfrak{S})$. The group $Z(\mathfrak{S})$ is defined over k, contains maximal tori of G, and $\mathfrak{S}$ belongs to the Lie algebra of every maximal torus of $Z(\mathfrak{S})$. The group $Z(\mathfrak{S})^0$ is equal to $N(\mathfrak{S})^0$.*

We show first that $\mathfrak{S}$ is commutative. Assume it is not. Since $\operatorname{ad} X$ $(X \in \mathfrak{S})$ is a semi-simple linear transformation of $\mathfrak{g}$, there exist then $X, Y \in \mathfrak{S}$, not zero, such that $[X, Y] = Y$. But then $\operatorname{ad} Y$ leaves the two-dimensional space $\mathfrak{m}$ spanned by X, Y stable, and its restriction to $\mathfrak{m}$ is non-zero, nilpotent, a contradiction.

Let $X \in \mathfrak{S}(k)$. Assume first that $[X, \mathfrak{g}] = 0$. Let T be a maximal torus of G whose Lie algebra contains X. Since $G^0 \subset Z(X)$, by 4.1, X belongs to the Lie algebra of the group $g \cdot T \cdot g^{-1}$ $(g \in G^0)$, which runs through all maximal tori of G as g runs through G^0. Thus, if $\mathfrak{S}$ is central in $\mathfrak{g}$, then $\mathfrak{S}$ belongs to the Lie algebra of all maximal tori of G, and $Z(\mathfrak{S}) \supset G^0$. Since $\mathfrak{S}$ is defined over k, $Z(\mathfrak{S})$ is defined over a purely inseparable extension of k. But any subgroup of G containing G^0 is defined over a separable extension of k, hence $Z(\mathfrak{S})$ is defined over k if $[\mathfrak{S}, \mathfrak{g}] = 0$.

Let now $\mathfrak{S}$ not be central in $\mathfrak{g}$. There exists then $X \in \mathfrak{S}(k)$ such that $[X, \mathfrak{g}] \neq 0$. We have then $\dim Z(X) \neq \dim G$ by 4.1. The group $Z(X)$ is defined over k, contains a maximal torus T whose Lie algebra contains X. We may then prove the second assertion by induction on $\dim G$.

Let T be a maximal torus of $Z(\mathfrak{s})^0$. Then $Z(T) \subset Z(\mathfrak{s})^0$. Using the conjugacy of maximal tori in $Z(\mathfrak{s})^0$, we see that $N(\mathfrak{s}) = (N(T) \cap N(\mathfrak{s})) \cdot Z(\mathfrak{s})^0$. Since $Z(T) \subset Z(\mathfrak{s})^0$ and $N(T)^0 = Z(T)$, it follows that $N(\mathfrak{s})^0 = Z(T) \cdot Z(\mathfrak{s})^0 = Z(\mathfrak{g})^0$.

4.4. COROLLARY. *Let G' be a k-group and $f: G \rightarrow G'$ a separable surjective morphism. Then $f(Z(\mathfrak{s})^0) = Z(df(\mathfrak{s}))^0$.*

We have $f(Z(\mathfrak{s})^0) \subset Z(df(\mathfrak{s}))^0$. To prove surjectivity, it is enough, in view of 4.3, to show that $\mathfrak{z}(df(\mathfrak{s})) = df(\mathfrak{z}(\mathfrak{s}))$, which follows from the full reducibility of $\mathrm{ad}_{\mathfrak{g}}\, \mathfrak{s}$.

4.5. COROLLARY. *The maximal toral subalgebras are the Lie algebras of the maximal tori of G, and are conjugate under G^0.*

REMARK. Toral subalgebras have also been introduced by Humphreys in [15, §13]. 4.5 is also proved there.

We shall have to use frequently the known global analogues of the previous results. For the ease of references, we collect them, and sharpen them slightly, in the following proposition.

4.6. PROPOSITION. *Let H be a k-subgroup of G, S a k-torus of G and $s \in G(k)$ a semi-simple element which normalizes H. Then $Z(S) \cap H$ and $Z(s) \cap H$ are defined over k, the orbit $M = \mathrm{Int}_G H(s)$ is closed in G, and the map $h \mapsto h \cdot s \cdot h^{-1}$ induces a k-isomorphism of $H/(Z(s) \cap H)$ onto M. The Lie algebra of $Z(S) \cap H$ (resp. $Z(s) \cap H$) is $\mathfrak{z}(S) \cap \mathfrak{h}$ (resp. $\mathfrak{z}(s) \cap \mathfrak{h}$). If G is connected, G' is a k-group and $f: G \rightarrow G'$ a surjective k-morphism, then $f(Z(S)) = Z(f(S))$ and $f(Z(s)^0) = f(Z(s))^0$.*

For the part pertaining to s of the first assertion, see ([3], 10.2, p. 128 and 10.3, p. 129), taking into account that the connectedness restrictions made in 10.3 are superfluous, in view of the facts recalled in 0.1. For the second assertion about s, see ([3], 10.1, p. 128).

The group $S(k_s)$ contains an element t such that $Z(t) = Z(S)$ ([3], 1.10, p. 62); consequently, $Z(S) \cap H$ is defined over k_s. Since it is purely inseparable over k, it is then defined over k. If G is connected, $Z(S)$ is connected by ([1], Prop. 18.4, p. 72).

We now prove the last assertion. Clearly $f(Z(S)) \subset Z(f(S))$. Since both groups are connected, it suffices to show that they have the same dimension.

Let N be the kernel of f. By the above, the Lie algebras of $Z(S)$ and $Z(S)\cap N$ are $\mathfrak{z}(S)$ and $\mathfrak{z}(S)\cap\mathfrak{n}$, hence

$$\dim f(Z(S)) = \dim Z(S) - \dim (Z(S)\cap N) = \dim df(\mathfrak{z}(S)) .$$

But $\mathrm{Ad}_G S$ is fully reducible, whence $df(\mathfrak{z}(S)) = \mathfrak{z}(f(S))$ and $\dim df(\mathfrak{z}(S)) = \dim \mathfrak{z}(f(S)) = \dim Z(f(S))$. The proof of the equality $f(Z(s)^0) = Z(f(s))^0$ is quite similar.

4.7. PROPOSITION. *Let G be connected, solvable, and $\mathfrak{s}$ a toral subalgebra of $\mathfrak{g}$. Then $N(\mathfrak{s})$ and $Z(\mathfrak{s})$ are equal, and connected.*

Let T be a maximal torus of $Z(\mathfrak{s})$. Then $\mathfrak{s}\subset\mathfrak{t}$, hence $Z(T)\subset Z(\mathfrak{s})$. Let $x\in N(\mathfrak{s})$. Then $x\cdot T\cdot x^{-1}$ is a maximal torus of $Z(\mathfrak{s})^0$, and there exists $y\in Z(\mathfrak{s})^0$ such that $y\cdot x\in N(T)$, which shows that $N(\mathfrak{s})\subset N(T)\cdot Z(\mathfrak{s})^0$. But $Z(T)$ is equal to $N(T)$ ([1], Prop. 10.2, p. 52), and is connected ([1], Thm. 13.2, p. 60), whence $N(T)\subset Z(\mathfrak{s})^0$, and $N(\mathfrak{s})\subset Z(\mathfrak{s})^0$.

4.8. A Lie subalgebra of $\mathfrak{g}$ is *algebraic* if it is the Lie algebra of an algebraic subgroup. In the remaining part of this paragraph, we reprove some known results on algebraic Lie algebras.

Let $p=0$. Then the Lie algebra of the intersection of two algebraic subgroups is the intersection of the Lie algebras of the two subgroups. Therefore, if M is a subset of $\mathfrak{g}$, there is a unique smallest algebraic subgroup, to be denoted $\mathcal{A}(M)$, whose Lie algebra contains M, namely the intersection of all algebraic subgroups whose Lie algebras contain M. If M is a subspace of $\mathfrak{g}$, defined over k, then $\mathcal{A}(M)$ is defined over k. If X is a non-zero nilpotent element of $\mathfrak{g}$, then $\mathcal{A}(X)$ is the one-dimensional group constructed in 3.3.

If $p\neq 0$, then the opening statement of the preceding paragraph may be false, as is already shown by the example (1.17) of the tori in $\boldsymbol{SL}_2$ in characteristic two.

4.9. PROPOSITION. *Let $\mathfrak{s}$ be a toral subalgebra of $\mathfrak{g}$.*

(i) *If $p=0$, then $\mathcal{A}(\mathfrak{s})$ is a torus.*

(ii) ([13], Prop. 2, p. 5) *If $p>0$, then $\mathfrak{s}$ is algebraic if and only if $\mathfrak{s}^{[p]}\subset\mathfrak{s}$.*

$\mathfrak{s}$ belongs to the Lie algebra of a torus, whence (i).

To prove (ii), we may assume that G is a torus (4.3), and, by going over to an extension of k, that G splits over k.

If $\mathfrak{s}$ is algebraic, then $\mathfrak{s}^{[p]}=\mathfrak{s}$. Assume conversely that $\mathfrak{s}^{[p]}\subset\mathfrak{s}$. We have then $\mathfrak{s}^{[p]}=\mathfrak{s}$. It is elementary that this implies

$$\mathfrak{s} = \mathfrak{s}_0 \otimes_{F_p} k, \qquad (\mathfrak{s}_0 = \mathfrak{s} \cap \mathfrak{g}_0),$$

where $\mathfrak{g}_0$ is the fixed point set of $[p]$ (see 1.7(c)). There exists then a direct summand Y of $X_* = X_*(G)$, of rank equal to $\dim \mathfrak{s}$, such that $f(Y \otimes k) = \mathfrak{s}$, in the notation of 1.7(c). But then the images in G of the elements of Y generate a subtorus of G whose Lie algebra is $\mathfrak{s}$.

4.10. LEMMA. *Let $p = 0$. Let $X \in \mathfrak{g}$ be either semi-simple or nilpotent. Let V be a finite dimensional vector space over k and $f\colon G \to GL(V)$ be a morphism. Let W be a subspace of V stable under $df(X)$. Then $f(g)(W) \subset W$ for all $g \in \mathcal{A}(X)$.*

Let X be nilpotent. Then it follows from 3.3 that $f(g)$ $(g \in \mathcal{A}(X))$ is a polynomial in $df(X)$, hence $f(g)$ leaves W stable.

Let now X be semi-simple. We may assume k to be algebraically closed. Then $df(X)$ is diagonalizable over k, and it suffices to consider the case where W is spanned by one element, say Y. Since $\mathcal{A}(X)$ is a torus, $f(\mathcal{A}(X))$ is also diagonalizable. Let then (X_i) $(1 \leqq i \leqq n)$ be a basis of V and a_i be characters of $\mathcal{A}(X)$ such that $f(t) \cdot X_i = t^{a_i} \cdot X_i$ $(i = 1, \cdots, n)$. We have then $df(U) \cdot X_i = da_i(U) \cdot X_i$ for U in the Lie algebra of $\mathcal{A}(X)$ $(i = 1, \cdots, n)$. Write $df(X) \cdot Y = a \cdot Y$ and $Y = \Sigma c_i X_i$; let J be the set of indices for which $c_i \neq 0$. Then $c_i = da_i(X)$ $(i \in J)$. Since $\mathcal{A}(X)$ is the smallest torus whose Lie algebra contains X, this implies that the a_i's $(i \in J)$ are equal to one another, hence Y is an eigenvector of $\mathcal{A}(X)$.

4.11. PROPOSITION. *Let $p = 0$. A subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is algebraic if and only if it satisfies the following conditions:*

(i) *$X \in \mathfrak{h}$ implies $X_s, X_n \in \mathfrak{h}$*

(ii) *if $X \in \mathfrak{h}$ is semi-simple, then the Lie algebra of $\mathcal{A}(X)$ belongs to $\mathfrak{h}$.*

The necessity of these conditions is obvious. Let us assume conversely that they are fulfilled. Let L be the algebraic subgroup of G generated by the groups $\mathcal{A}(X)$, $(X \in \mathfrak{h}(k)$, X semi-simple or nilpotent). Then, by 4.10, $\mathfrak{h}$ is stable under $\mathrm{Ad}_{\mathfrak{g}} L$. It follows then from 1.16 that the Lie algebra $\mathfrak{l}$ of L is spanned by the elements $\mathrm{Ad}\, x(X)$ $(x \in L;\ X \in \mathfrak{h};\ X$ semi-simple or nilpotent). Therefore $\mathfrak{l} \subset \mathfrak{h}$. But $\mathfrak{l} \supset \mathfrak{h}$ in view of (i); hence $\mathfrak{l} = \mathfrak{h}$, and $\mathfrak{h}$ is algebraic.

4.12. COROLLARY. *Let V be a finite dimensional vector space over $\bar{k}$ and $G \to GL(V)$ a morphism. Let $\mathfrak{h}$ be a subalgebra of $\mathfrak{g}$, and W a subspace of V such that $df(\mathfrak{h})(W) \subset W$. Then $f(\mathcal{A}(\mathfrak{h})) \cdot (W) \subset W$.*

Let $\mathfrak{l} = \{X \in \mathfrak{g},\ df(X)(W) \subset W\}$. Since the semi-simple and the nilpotent parts of a linear transformation Y are polynomials in Y, it follows from 3.1(a) that $\mathfrak{l}$ verifies the condition (i) of 4.9. By 4.10, it also fulfills condition (ii) of 4.11, hence $\mathfrak{l}$ is algebraic. The connected algebraic group L with Lie algebra $\mathfrak{l}$ is generated by the subgroups $\mathcal{A}(X)$ ($X \in \mathfrak{l}$, X semi-simple or nilpotent), hence L leaves W stable (4.10). Moreover, since $\mathfrak{l} \supset \mathfrak{h}$, we have $L \supset A(\mathfrak{h})$.

4.13. COROLLARY. *Let $\mathfrak{h}$ be a subalgebra of $\mathfrak{g}$. Assume $\mathfrak{h}$ to be spanned by algebraic subalgebras. Then $\mathfrak{h}$ is algebraic.*

We may write $\mathfrak{h} = \mathfrak{h}_1 + \cdots + \mathfrak{h}_q$, with $\mathfrak{h}_i$ algebraic ($1 \leqq i \leqq q$). Let H_i be the connected group with Lie algebra $\mathfrak{h}_i$, and L the group generated by the H_i's. We have $[\mathfrak{h}_i, \mathfrak{h}] \subset \mathfrak{h}$ whence $\mathrm{Ad}_G H_i(\mathfrak{h}) = \mathfrak{h}$ by 4.12, and therefore $\mathrm{Ad}_G L(\mathfrak{h}) = \mathfrak{h}$. But $\mathfrak{l}$ is generated by subalgebras of the form $\mathrm{Ad}\, g(\mathfrak{h}_i)$ ($g \in L$, $1 \leqq i \leqq q$) by 1.16, therefore $\mathfrak{l} \subset \mathfrak{h}$, and finally $\mathfrak{l} = \mathfrak{h}$.

REMARK. 4.11 to 4.13 are known results of Chevalley [8].

5. Inseparable isogenies.

5.1. In this paragraph, we assume $p \neq 0$. An *inseparable k-isogeny of height* 1 $\pi: G \to H$ of k-groups is a k-isogeny such that the image of $k[H]$ under the comorphism π^0 contains $(k[G])^p$. The next result is known (see [21], Theorem 1 or [7], §3). It is a very special result about the existence of quotients in group schemes (for which we refer to [12], exp. V). For the convenience of the reader a sketch of a proof is given below.

5.2. PROPOSITION. *Let $\mathfrak{m}$ be an ideal in $\mathfrak{g}$, which is stable under the p-th power operation and under* $\mathrm{Ad}(G)$, *and which is defined over k. Then there exists a k-group $G/\mathfrak{m}$ and a purely inseparable k-isogeny π of height* 1, *which has the following properties*:

(i) $\mathrm{Ker}\, d\pi = \mathfrak{m}$,

(ii) *if π': $G \to G'$ is a purely inseparable k-isogeny with* $\mathrm{Ker}\, \pi' \supset \mathfrak{m}$, *then there exists a unique k-isogeny $\theta: G/\mathfrak{m} \to G'$ such that $\pi' = \theta \circ \pi$. The pair $(G/\mathfrak{m}, \pi)$ is unique up to k-isomorphism.*

The proof of uniqueness is standard and will be left to the reader. Let $A = k[G]$. By §1, $\mathfrak{g}(k)$ is an algebra of derivations of A and so is $\mathfrak{m}(k)$. Let B be the ring of invariants of $\mathfrak{m}$ in A:

$$B = \{a \in A, Xa = 0 \text{ for all } X \in \mathfrak{m}(k)\} .$$

Since $B \supset k[A^p]$, a well-known argument shows that B is finitely generated over k (see, e.g., [22], p. 50, Lemma 10). Moreover if l is an extension of k, then $B \otimes_k l$ is canonically imbedded in $A \otimes_k l$, which is a reduced ring (i.e., a ring without nilpotents $\neq 0$), because G is defined over k. It follows that $B \otimes_k l$ is reduced.

We conclude that B is the k-algebra of a variety $G/\mathfrak{m}$ which is defined over k. The injection $B \rightarrow A$ induces a morphism of k-varieties $\pi: G \rightarrow G/\mathfrak{m}$ which is bijective on $G(\bar{k})$ (since $B \supset k[A^p]$). We next prove that $G/\mathfrak{m}$ is an algebraic group and that π is a homomorphism. It will follow that π is a k-isogeny.

Let $\mu: A \rightarrow A \otimes_k A$ define the group law on G. It suffices to prove that μB is contained in the subring $B \otimes B$ of $A \otimes A$. Let $X \in \mathfrak{m}(k)$. Then the right invariance of X implies by 1.2(1) that $(X \otimes \mathrm{id})\mu b = 0$ for $b \in B$. The invariance of $\mathfrak{m}$ under $\mathrm{Ad}(G)$ implies that $(\mathrm{id} \otimes X)\mu b = 0$ for $b \in B$. From these two facts it follows that $\mu B \subset B \otimes B$. To finish the existence proof it remains to be shown that $\operatorname{Ker} d\pi = \mathfrak{m}$. Let $X \in \mathfrak{g}(k)$. The canonical image Y of X in the Lie algebra of $G/\mathfrak{m}$ is obtained as follows (see 1.5). Let $b \in B$, $\mu b = \Sigma_i b_i \otimes b'_i$, then $Yb = \Sigma_i X b_i(e) b'_i$. From this it is clear that $\mathfrak{m} \subset \operatorname{Ker} d\pi$. Next let $X \in \operatorname{Ker} d\pi$. Then $\Sigma_i X b_i(e) b'_i = 0$. Taking (as we may) the b'_i to be linearly independent, we get $X b_i(e) = 0$. Clearly $\operatorname{Ker} d\pi$ is invariant under $\mathrm{Ad}(G)$, which implies that $X b_i = 0$. Since $b = \Sigma_i b'_i(e) b_i$, we see, finally, that $Xb = 0$ for $b \in B$, $X \in \operatorname{Ker} d\pi \cap \mathfrak{g}(k)$. The proof will be finished if we show: if k is algebraically closed and if $X \in \mathfrak{g}$, $Xb = 0$ for all $b \in B$, then $X \in \mathfrak{m}$.

We may then take G to be connected. Let L (resp. M) be the quotient field of the integral domain A (resp. B). L is a purely inseparable extension of M of height 1, $\mathfrak{n} = \mathfrak{m} \otimes_k M$ is an algebra of deriviations of L/M and M is exactly the field of invariants of $\mathfrak{n}$. We can now apply the Galois theory of purely inseparable extensions of height 1, due to Jacobson, to get the desired result (see [6], Prop. 6, p. 194). To prove (ii), let f: $C \rightarrow A$ be the L-algebra homomorphism defining π'. Then $\operatorname{Ker} d\pi' \supset \mathfrak{m}$ implies that $f(C) \subset B$, whence the result.

5.3. Proposition. *Let S be a subtorus of G which is not contained in the center of G and whose Lie algebra $\mathfrak{s}$ is central in $\mathfrak{g}$. Then there exists an algebraic group G' and a purely inseparable isogeny $\pi: G \rightarrow G'$, whose differential $d\pi$ has kernel $\mathfrak{s}$ and such that the Lie algebra $\mathfrak{s}'$ of $S' = \pi(S)$ is non-central in $\mathfrak{g}'$. The algebra $\mathfrak{g}'$ is the direct sum of $d\pi(\mathfrak{g})$ and $\mathfrak{s}'$.*

Let $\Phi = \Phi(S, G)$ be the set of roots of G with respect to S. By 2.11, $\Phi(S, G) \neq \emptyset$. $\mathfrak{g}$ is the direct sum of the Lie algebra $\mathfrak{z}(S)$ of $Z(S)$ (see (4.6)) and of the root spaces

$$\mathfrak{g}_a = \{X \in \mathfrak{g} \mid \mathrm{Ad}(s)X = s^a X \text{ for } s \in S\}\ ,$$

where $a \in \Phi$.

The differential of $a\colon S \to \boldsymbol{GL}_1$ can be identified with a linear form on $\mathfrak{s}$ and we have $[Y, X] = da(Y)X$ for $Y \in \mathfrak{s}$, $X \in \mathfrak{g}_a$. The form da is zero if and only if a is divisible by p in the character group $X^*(S)$ of S.

Let c be the smallest positive integer such that $\Phi \not\subset p^{c+1} X^*(S)$. $\mathfrak{s}$ is central in $\mathfrak{g}$ if and only if $c \geqq 1$. We prove the first statement of 5.3 by induction on c.

From 4.3 it follows that 5.2 is applicable with $\mathfrak{m} = \mathfrak{s}$. Let $G_1 = G/\mathfrak{s}$, let $\pi_1\colon G \to G_1$ be the isogeny of 5.2. Let $\mathrm{S}_1 = \pi_1(S)$. From $d\pi_1(\mathfrak{s}) = 0$ it follows that the transposed homomorphism ${}^t\pi_1\colon X^*(S_1) \to X^*(S)$ maps $X^*(S_1)$ into $pX^*(S)$. If c_1 has the same meaning for S_1 as c for S we have $c_1 < c$. If $c_1 = 0$, we can take $G' = G_1$, $\pi = \pi_1$, if $c_1 > 0$ we can apply induction to get the required pair (G', π).

To prove the last assertion, it suffices, by dimensions, to show that $d\pi(\mathfrak{g}) \cap \mathfrak{s}' = 0$. Let $X \in \mathfrak{g}$, $d\pi(X) \in \mathfrak{s}'$. Write $X = X_s + X_n$ according to 3.1(a). Then $d\pi(X_s) + d\pi(X_n)$ is in $\mathfrak{s}'$, hence semi-simple. By 3.1 this means that $X_n \in \mathrm{Ker}\, d\pi = \mathfrak{s}$. But $\mathfrak{s}$ consists of semi-simple elements, hence $X_n = 0$. So X is semi-simple. By 4.2, X and $\mathfrak{s}$ are contained in the Lie algebra $\mathfrak{t}$ of a maximal torus T of G. Replacing G by T, we are reduced to prove the assertion for the case that G is a *torus*. 4.9 (ii) then shows that $\mathfrak{s}$ is the Lie algebra of a subtorus of G. We may then assume $S = (\boldsymbol{GL}_1)^m$, $G = (\boldsymbol{GL}_1)^n$, with the imbedding $(x_1, \cdots, x_m) \mapsto (x_1, \cdots, x_m, 1, \cdots, 1)$. The isogeny $\pi\colon G \to G'$ can then be described as follows, identifying G' with $(\boldsymbol{GL}_1)^n$:

$$\pi(x_1, \cdots, x_n) = (x_1^{a_1}, \cdots, x_m^{a_m}, x_{m+1}, \cdots, x_n)\,,$$

where the a_i are p-powers > 1. Identifying $\mathfrak{g}$ and $\mathfrak{g}'$ with n-dimensional space, we have

$$d\pi(x_1, \cdots, x_n) = (0, \cdots, 0\,, x_{m+1}, \cdots, x_n)\,,$$

and $\mathfrak{s}'$ consists of the elements $(x_1, \cdots, x_n, 0, \cdots, 0)$ of $\mathfrak{g}'$. This shows that $d\pi(\mathfrak{g}) \cap \mathfrak{s}' = 0$, as had to be proved.

6. Regular elements, Cartan subalgebras, subgroups of type (C).

6.1. Regular elements. For $X \in \mathfrak{g}$, the nilspace of X is the space of elements in $\mathfrak{g}$ annihilated by some power of $\mathrm{ad}\, X$, and nil (X) denotes the dimension of the nilspace of X, i.e., the multiplicity of the eigenvalue zero of $\mathrm{ad}\, X$. If X is semi-simple, the nilspace of X is then $\mathfrak{z}(X)$.

We may write

$$\det(\operatorname{ad} X - T) = T^m \cdot (P_0(X) + P_1(X) \cdot T + \cdots + P_{n-m}(X) \cdot T^{n-m}),$$

($n = \dim \mathfrak{g}$), where T is an indeterminate, and the P_i's are non-identically vanishing polynomial functions on $\mathfrak{g}$, defined over k. Then X is regular if and only if $P_0(X) \neq 0$. The set $R(\mathfrak{g})$ of regular elements of $\mathfrak{g}$ is therefore open, non-empty.

6.2. LEMMA. *Let $X \in \mathfrak{g}$ and $X = X_s + X_n$ its Jordan decomposition.*

(i) *X is regular if and only if X_s is regular.*

(ii) *Let $p > 0$. Then X is regular if and only if $X^{[p]}$ is regular.*

(iii) *Let k be infinite. Then $R(\mathfrak{g}) \cap \mathfrak{g}(k)$ is Zariski-dense in $\mathfrak{g}$. The space $\mathfrak{g}(k)$ contains regular semi-simple elements.*

(i) Since $\operatorname{ad} X = \operatorname{ad} X_s + \operatorname{ad} X_n$ is the Jordan decomposition of $\operatorname{ad} X$ (3.1), $\operatorname{ad} X$ has the same eigenvalues as $\operatorname{ad} X_s$, hence $\operatorname{nil}(X) = \operatorname{nil}(X_s)$.

(ii) Since $\mathfrak{g}$ is restricted, $\operatorname{ad} X^{[p]} = (\operatorname{ad} X)^p$, hence $\operatorname{nil}(X) = \operatorname{nil}(X^{[p]})$.

(iii) The set of regular elements is open non-empty, and $\mathfrak{g}(k)$ is Zariski-dense in $\mathfrak{g}$, whence the first part of (iii). Let $X \in \mathfrak{g}(k)$ be regular. If $p = 0$, then $X_s \in \mathfrak{g}(k)$, and is regular by (i). If $p > 0$, there is a power q of p such that $X^{[q]} = X_s^{[q]}$ (3.2). But then $X^{[q]}$ is regular (by (ii)), semi-simple, and rational over k.

6.3. LEMMA. *Let S be a torus in G. Let $\Phi = \Phi(S, G)$ be the set of roots of G with respect to S, and Φ' the set of $a \in \Phi$ whose differential da is zero. The set $R_{\mathfrak{s}}$ of $X \in \mathfrak{s}$ such that $da(X) \neq 0$ $(a \in \Phi - \Phi')$ is the set of elements $X \in \mathfrak{s}$ for which $\mathfrak{z}(X) = \mathfrak{z}(\mathfrak{s})$, and is non-empty open in $\mathfrak{s}$. If $X \in R_{\mathfrak{s}}$, then $Z(X)^o = Z(\mathfrak{s})^o$. If S is a maximal torus, then $R_{\mathfrak{s}}$ consists of regular elements of $\mathfrak{g}$. If k is infinite and $\mathfrak{s}$ is defined over k, then $\mathfrak{s}(k) \cap R_{\mathfrak{s}} \neq \emptyset$.*

(In this statement, the differential db of a morphism $b\colon S \to \boldsymbol{GL}_1$ is identified to a linear form on $\mathfrak{s}$.)

For a character b of S, let

$$\mathfrak{g}_b^{(S)} = \mathfrak{g}_b = \{X \in \mathfrak{g}, \operatorname{Ad} s \cdot X = s^b \cdot X, \quad (s \in S)\}\ . \tag{1}$$

We have then

$$\mathfrak{g} = \mathfrak{g}_o \oplus \Sigma_{a \in \Phi} \mathfrak{g}_a\ . \tag{2}$$

Moreover,

$$[X, Y] = db(X) \cdot Y\ , \qquad (X \in \mathfrak{s},\ Y \in \mathfrak{g}_b)\ ; \tag{3}$$

consequently:

$$(4) \qquad \mathfrak{z}(\mathfrak{s}) = \mathfrak{g}_o \oplus \Sigma_{a\in\Phi'}\mathfrak{g}_a$$

$$(5) \qquad \mathfrak{z}(X) = \mathfrak{g}_o \oplus \Sigma_{a\in\Phi, da(X)=0}\mathfrak{g}_a$$

from which our first assertion follows. The second one is then a consequence of 4.3. Since $R_\mathfrak{s}$ is open and non-empty, its intersection with $\mathfrak{s}(k)$ is not empty if k is infinite. Let finally S be a maximal torus. By 6.2, $\mathfrak{g}$ has a regular semi-simple element Y, which belongs necessarily to a maximal toral subalgebra of $\mathfrak{g}$. By conjugacy, $\mathfrak{s}$ then contains regular semi-simple elements of $\mathfrak{g}$. But, clearly, $\mathrm{nil}(X) = \min \mathrm{nil}(Y)$ $(Y \in \mathfrak{s})$, if $X \in R_\mathfrak{s}$, which implies our last assertion.

If k is finite, $\mathfrak{g}(k)$ does not always contain regular elements. It was shown however by Chevalley that this is the case if G is the adjoint group of a semi-simple group (see [12] Exp. XIV, Appendix by J.-P. Serre). We outline briefly how the same method can be used for any reductive group.

6.4. PROPOSITION. *Let k be finite and G be reductive. Then $\mathfrak{g}(k)$ contains regular elements.*

One shows first (loc. cit. lemme 1) that it suffices to consider the case where G is quasi-simple over $\bar{k}$. Let T be a maximal torus of G which is defined over k, and $\Phi = \Phi(T, G)$. Let Φ' be the set of $a \in \Phi$ whose differential is identically zero. By 6.3, $X \in \mathfrak{g}$ is regular if and only if $da(X) \neq 0$ for all $b \in \Phi - \Phi'$.

The Galois group $\Gamma = \mathrm{Gal}(\bar{k}/k)$ operates on $T(\bar{k})$, on Φ, and leaves Φ' stable. It is proved in loc. cit. Lemme 3, that one can choose T in such a way that there are $r = \dim T$ roots $a_1, \cdots, a_r$, which form a basis of the lattice spanned by the roots, and such that $\Phi = \cup_i \Gamma \cdot a_i$. It suffices then to exhibit $X \in \mathfrak{t}(k)$ such that $da_i(X) \neq 0$ whenever $a_i \in \Phi - \Phi'$, $i = 1, \cdots, r$. Such an element exists by lemme 4, of loc. cit.

6.5. DEFINITION. A *Cartan subalgebra* of $\mathfrak{g}$ is the centralizer in $\mathfrak{g}$ of the Lie algebra of a maximal torus of G. A *subgroup of type* (C) of G is the identity component of the centralizer in G of the Lie algebra of a maximal torus of G.

In view of 6.6, 6.7 below, these notions are equivalent to those introduced in ([12], Exp. XIII) under the same terminology. A subgroup of type (C) always contains a Cartan subgroup, but it may be bigger; for example, in characteristic two, $\boldsymbol{SL_2}$ is its own subgroup of type (C), while its Cartan subgroups are its maximal tori.

6.6. PROPOSITION. (i) *Two Cartan subalgebras of* $\mathfrak{g}$ (*resp. subgroups of type* (C) *of* G) *are conjugate.*

(ii) *The transform of a subgroup of type* (C) *of* G (*resp. Cartan subalgebra of* $\mathfrak{g}$) *by an automorphism of* G (*resp. the differential of an automorphism of* G) *is a subgroup of type* (C) (*resp. a Cartan subalgebra*).

(iii) *The Cartan subalgebras defined over* k *of* $\mathfrak{g}$ *are the Lie algebras of the subgroups of type* (C) *defined over* k *of* G.

(i) and (ii) follow from the definitions and the conjugacy of maximal tori, (iii) from the definitions and 4.3.

6.7. PROPOSITION. *Let* $\mathfrak{h}$ *be a subalgebra* (*not necessarily restricted*) *of* $\mathfrak{g}$. *The following conditions are equivalent*:

(i) $\mathfrak{h}$ *is a Cartan subalgebra of* $\mathfrak{g}$;

(ii) $\mathfrak{h}$ *is the nilspace of a regular element*;

(iii) $\mathfrak{h}$ *is the centralizer of a regular semi-simple element*;

(iv) $\mathfrak{h}$ *is nilpotent, equal to its normalizer.*

If those conditions are fulfilled, $\mathfrak{h}$ *is maximal nilpotent, contains one and only one maximal toral subalgebra* $\mathfrak{t}$ *of* $\mathfrak{g}$, *and* $\mathfrak{t}$ *is the set of all semi-simple elements of* $\mathfrak{h}$.

The equivalence of (i), (ii), (iii) follows from 6.2, 6.3 and from the fact that the nilspace of X is equal to the centralizer of X_s.

We now prove that (i) implies (iv) and the last assertion. By assumption $\mathfrak{h}=\mathfrak{z}(\mathfrak{t})$, where $\mathfrak{t}$ is a maximal toral subalgebra of $\mathfrak{g}$. Let $X\in\mathfrak{t}$ be such that $\mathfrak{h}=\mathfrak{z}(X)$; such an X exists and is regular by 6.3. Let $\mathfrak{n}$ be the normalizer of $\mathfrak{h}$. It is stable under $\mathrm{Ad}_G T$, hence, in the notation of 6.3:

$$\mathfrak{n}=\mathfrak{g}_0+\Sigma_{a\in\Phi}\mathfrak{n}\cap\mathfrak{g}_a\,.$$

On the other hand

$$\mathfrak{h}=\mathfrak{g}_0+\Sigma_{a\in\Phi,\,da(X)=0}\mathfrak{g}_a\,.$$

Let $Y\in\mathfrak{n}\cap\mathfrak{g}_a$. Then $[X,Y]=da(X)\cdot Y\in\mathfrak{h}$, hence $da(X)=0$, and $Y\in\mathfrak{h}$. Thus $\mathfrak{h}=\mathfrak{n}$. The algebra $\mathfrak{h}$ is algebraic (6.6), therefore $Z\in\mathfrak{h}$ implies $Z_s, Z_n\in\mathfrak{h}$, and, by 4.3, $Z_s\in\mathfrak{t}$, which shows that $\mathfrak{t}$ contains all semi-simple elements of $\mathfrak{h}$. This also proves that $[Z,U]=[Z_n,U]$ $(U\in\mathfrak{h})$. Consequently, $\mathrm{ad}\,Z$, restricted to $\mathfrak{h}$ is nilpotent. $\mathfrak{h}$ is then nilpotent by Engel's theorem. Let finally $\mathfrak{m}$ be a nilpotent algebra containing $\mathfrak{h}$. If $\mathfrak{h}\neq\mathfrak{m}$, then the normalizer of $\mathfrak{h}$ in $\mathfrak{m}$ is not equal to $\mathfrak{h}$, a contradiction with what has already been proved.

(iv)$\Longrightarrow$(i). Let $X \in \mathfrak{h}$. By 3.1 and standard facts on linear transformations, $\operatorname{ad} X_s$ and $\operatorname{ad} X_n$ are polynomials in $\operatorname{ad} X$, hence X_s, X_n normalize $\mathfrak{h}$, and therefore belong to $\mathfrak{h}$. But the restriction of $\operatorname{ad} X_s$ to $\mathfrak{h}$ is nilpotent, since $\mathfrak{h}$ is nilpotent, and semi-simple since X_s is semi-simple. Therefore X_s is in the center of $\mathfrak{h}$, and the set $\mathfrak{s}$ of all semi-simple elements of $\mathfrak{h}$ is a toral subalgebra, central in $\mathfrak{h}$. We want to prove that $\mathfrak{s}$ is maximal. Let $\mathfrak{t}$ be a maximal toral subalgebra containing $\mathfrak{s}$. If $\mathfrak{s} \neq \mathfrak{t}$, then the fixed point set V of $\mathfrak{s}$ in $\mathfrak{g}/\mathfrak{h}$ is not zero. The image of $\mathfrak{h}$ in $\mathfrak{gl}(V)$ consists of nilpotent transformations, hence, by Engel's theorem, $\mathfrak{h}$ has a non-trivial fixed point set in V; but this contradicts the assumption $\mathfrak{h} = \mathfrak{n}(\mathfrak{h})$. Thus $\mathfrak{s} = \mathfrak{t}$, and $\mathfrak{h} \subset \mathfrak{z}(\mathfrak{t})$. By the first part of the proof, $\mathfrak{z}(\mathfrak{t})$ is nilpotent, and therefore $\mathfrak{h} = \mathfrak{z}(\mathfrak{t})$.

6.8. PROPOSITION. (a) *Let C be a subgroup of type* (C) *of G, and* $\mathfrak{t}$ *the maximal toral subalgebra of its Lie algebra* $\mathfrak{c}$. *The following conditions are equivalent*: (i) *C is defined over k,* (ii) $\mathfrak{c}$ *is defined over k,* (iii) $\mathfrak{t}$ *is defined over k.*

(b) *Let k be infinite. A subgroup H of G (resp. subalgebra* $\mathfrak{h}$ *of* $\mathfrak{g}$) *is of type* (C), *defined over k (resp. a Cartan subalgebra defined over k) if and only if it is the identity component of the centralizer in G (resp. the centralizer in* $\mathfrak{g}$) *of a regular semi-simple element of* $\mathfrak{g}$ *contained in* $\mathfrak{g}(k)$.

(a) Clearly (i)$\Longrightarrow$(ii). Let $\mathfrak{c}$ be defined over k. By 6.7, $\mathfrak{t}$ is the set of all semi-simple elements of $\mathfrak{c}$, hence is defined over k (3.2). This proves that (ii)$\Longrightarrow$(iii). We have $C = Z(\mathfrak{t})^0$ by definition, hence (iii)$\Longrightarrow$(i) follows from 4.3.

(b) follows from (a), 4.3 and 6.3.

6.9. LEMMA. *Let H be a closed connected subgroup of G whose Lie algebra contains a Cartan subalgebra* $\mathfrak{c}$ *of* $\mathfrak{g}$. *Then $H = N(\mathfrak{h})^0$, has finite index in its normalizer, and is the only closed connected subgroup of G with Lie algebra* $\mathfrak{h}$.

Obviously, $H \subset N(\mathfrak{h})^0$. Let now $g \in N(\mathfrak{h})$. Then, (6.6) $\mathfrak{c}$ and $\operatorname{Ad} g(\mathfrak{c})$ are both Cartan subalgebras of $\mathfrak{h}$, and we may find therefore $h \in H$ such that $h^{-1} \cdot g \in N(\mathfrak{c})$, whence $N(\mathfrak{h}) \subset H \cdot N(\mathfrak{c})$. By 6.7, $\mathfrak{c}$ is equal to its normalizer in $\mathfrak{g}$; therefore, if C is a subgroup of type (C) of H with Lie algebra $\mathfrak{c}$, we have $C = N(\mathfrak{c})^0$. From this we get $(H \cdot N(\mathfrak{c}))^0 = H \cdot C = H$, and $N(\mathfrak{h})^0 \subset H$. Since $N(H) \subset N(\mathfrak{h})$, it follows that H has finite index in its normalizer. Finally, the equality $H = N(\mathfrak{h})^0$ shows the uniqueness of H.

6.10. PROPOSITION. (a) *Let H be a closed connected subgroup of G, whose Lie algebra* $\mathfrak{h}$ *is defined over k, and contains a Cartan subalgebra* *of* $\mathfrak{g}$. *Then H is defined over k and is separably generated by its subgroups of type* (C) *defined over k.*

(b) *Let G' be a k-group and $f: G^0 \to G'$ a surjective separable k-morphism. Then f (resp. df) maps the set of k-subgroups of type* (C) *of G (resp. of Cartan subalgebras of* $\mathfrak{g}$) *defined over k onto the set of subgroups of type* (C) *of G' (resp. of Cartan subalgebras of* $\mathfrak{g}'$) *defined over k.*

(i) We prove first (a) when k is *infinite*. In view of 6.6 (iii), 1.16, it suffices to show that $\mathfrak{g}$ is spanned by its Cartan subalgebras which are defined over k. Let $X \in \mathfrak{g}(k)$. We let Y be equal to X_s if $p = 0$, to $X^{[q]}$ if $p \neq 0$ where q is a power of p big enough so that $Z^{[q]} = 0$ for all nilpotent $Z \in \mathfrak{g}$ (3.2). We have $[X, Y] = 0$ and $Y \in \mathfrak{g}(k)$. If X is regular, so is Y (6.2) and $\mathfrak{z}(Y)$ is a Cartan subalgebra of $\mathfrak{g}$, defined over k (6.8). Thus X belongs to a Cartan subalgebra defined over k. Since $R(\mathfrak{g}) \cap \mathfrak{g}(k)$ is dense in $\mathfrak{g}$ (6.2), this proves our assertion.

(ii) We now prove (b). In view of 6.6, it suffices to prove the part of (b) pertaining to df. Let $\mathfrak{n} = \ker df$. Let $\mathfrak{c}$ be a Cartan subalgebra defined over k and $\mathfrak{t}$ its maximal toral subalgebra. $\mathfrak{t}$ is defined over k (6.8). Let T be a maximal torus of G whose Lie algebra is $\mathfrak{t}$. Since f is separable, df is surjective, and $df(\mathfrak{t}) = \mathfrak{t}'$ is the Lie algebra of $T' = f(T)$, which is a maximal torus of G' ([1], §22). $\mathrm{ad}_{\mathfrak{g}}\, \mathfrak{t}$ is a commutative algebra of semi-simple transformations, which leaves $\mathfrak{n}$ stable. There exists then a subspace $\mathfrak{a} \subset \mathfrak{g}$ stable under $\mathrm{ad}_{\mathfrak{g}}\, \mathfrak{t}$ and such that $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{n}$. We have $\mathfrak{z}(\mathfrak{t}) = \mathfrak{z}(\mathfrak{t}) \cap \mathfrak{a} + \mathfrak{z}(\mathfrak{t}) \cap \mathfrak{n}$. This implies immediately that

$$df(\mathfrak{c}) = df(\mathfrak{z}(\mathfrak{t})) = \mathfrak{z}(df(\mathfrak{t})) = \mathfrak{z}(\mathfrak{t}'),$$

hence $df(\mathfrak{c})$ is a Cartan subalgebra defined over k.

Let now C' be a subgroup of type (C) of G' defined over k and $H = f^{-1}(C')^0$. The group H is defined over k (since f is separable), and contains a maximal torus of G ([1], §22). Let us show that a subgroup C of type (C) of H is also of type (C) in G. Let T be a maximal torus of C. It is maximal in H, hence in G, and maps onto a maximal torus T' of C'. Then $\mathfrak{c}' = \mathfrak{z}(\mathfrak{t}')$. Let $\mathfrak{b}$ be a subspace of $\mathfrak{g}$, supplementary to $\mathfrak{h}$, and stable under $\mathrm{Ad}_{\mathfrak{g}}\, T$. Then df maps $\mathfrak{b}$ isomorphically onto a supplement of $\mathfrak{c}'$ in $\mathfrak{g}'$, hence $\mathfrak{z}(\mathfrak{t}') \cap df(\mathfrak{b}) = 0$. It follows that $\mathfrak{z}(\mathfrak{t}) \cap \mathfrak{b} = 0$. Since $\mathfrak{z}(\mathfrak{t})$ is sum of its intersections with $\mathfrak{h}$ and $\mathfrak{b}$, we see that $\mathfrak{c}$ is the centralizer of $\mathfrak{t}$ in $\mathfrak{g}$.

Let now k be infinite. Then, by (i), $\mathfrak{h}$ has a Cartan subalgebra defined over k. By what has already been proved, $\mathfrak{c}$ is a Cartan subalgebra of $\mathfrak{g}$ and $df(\mathfrak{c})$ is a Cartan subalgebra of $\mathfrak{c}'$, hence is equal to $\mathfrak{c}'$.

Let k be finite. Then H has a maximal torus T defined over k (2.7), $\mathfrak{c} = \mathfrak{z}(\mathfrak{t})$ is a Cartan subalgebra of $\mathfrak{g}$ defined over k, contained in $\mathfrak{h}$, and $df(\mathfrak{c}) = \mathfrak{c}'$.

(iii) There remains to prove (a) for k finite. Let B, B', T be as in 2.8. Since the maximal tori of B, B' are maximal in G, the Cartan subalgebras defined over k of $\mathfrak{b}$ or $\mathfrak{b}'$ are contained in Cartan subalgebras defined over k of $\mathfrak{g}$. In view of 2.8, we are reduced to the case where G is solvable. We proceed by induction on $\dim G$. There is nothing to prove if G is nilpotent, in particular if $\dim G=1$. Let N be a non-trivial normal closed connected subgroup of G, contained in the center of the unipotent radical of G, minimal for these properties. Let $f\colon G \to G' = G/N$ be the canonical projection. Let $\mathfrak{a}$ be the subspace of $\mathfrak{g}$ spanned by the Cartan subalgebras defined over k of $\mathfrak{g}$. In view of (ii) and of the induction assumption, applied to G', we have $\mathfrak{g}=\mathfrak{a}+\mathfrak{n}$. Let T' be a maximal torus defined over k of G' and $H=f^{-1}(T')$. Let T be a maximal torus defined over k of H. We have $H=T\cdot N$ (semi-direct). If $T'\neq G'$, then $H\neq G$, and, by induction assumption, $\mathfrak{h}$ is spanned by its Cartan subalgebras defined over k. But T is a maximal torus of G, too, hence the Cartan subalgebras defined over k of $\mathfrak{h}$ are contained in Cartan subalgebras defined over k of $\mathfrak{g}$. Since $\mathfrak{n}\subset\mathfrak{h}$, we have $\mathfrak{g}=\mathfrak{a}$ in this case. So assume $G=H=T\cdot N$. The subgroup $C=Z(\mathfrak{t})^0$ of G is of type (C), defined over k, and contains T. Then $C\cap N$ is normal connected in G. By the minimality assumption on N, we have either $C\cap N=N$, and $G=C$, in which case our assertion is proved, or $C\cap N=\{e\}$. So assume $T=C$. Then $\mathfrak{t}$ is not central in $\mathfrak{g}$, and there exists $X\in\mathfrak{t}(k)$ not central in $\mathfrak{g}$. Then (4.3), $Z(X)^0\neq G$ whence again $Z(X)^0=T$ and $\mathfrak{z}(X)=\mathfrak{t}$. We claim that $Z=X+Y$ is semisimple for any $Y\in\mathfrak{n}$. In fact, since $Z_n\in\mathfrak{n}$, we see, by considering the projection of G onto $G/N\cong T$, and using 3.1, that $Z_s=X+U$ $(U\in\mathfrak{n})$. Since $\mathfrak{n}$ is commutative, we have then

$$0=[Z_s,Z_n]=[X,Z_n],$$

hence $Z_n=0$, $U=Y$. We see also that $\mathfrak{z}(X+Y)\cap\mathfrak{n}=0$. Thus $X+Y$ is regular, and, if $Y\in\mathfrak{n}(k)$, $\mathfrak{z}(X+Y)$ is a Cartan subalgebra defined over k. It follows that the space $\mathfrak{a}$ spanned by the Cartan subalgebras defined over k of $\mathfrak{g}$ contains $\mathfrak{t}$ and $X+\mathfrak{n}(k)$. It is then elementary that $\mathfrak{a}=\mathfrak{g}$.

6.11. COROLLARY. *Let H, K be closed subgroups of G. Assume that H is connected and that $\mathfrak{h}$ contains a Cartan subalgebra of $\mathfrak{g}$. Then $H\subset K$ if and only if $\mathfrak{h}\subset\mathfrak{k}$.*

This follows from 6.10, with k standing for a common field of definition for G, H, K.

6.12. LEMMA. *Let G be connected, and T be a maximal torus of G. Then T is defined over k if and only if $Z(T)$ is.*

If T is defined over k, then so is $Z(T)$ by (4.6). The group $Z(T)$ being connected, nilpotent, the converse follows from the fact that if a connected nilpotent group H is defined over k, then the unique maximal torus S of H is defined over k. This was noticed first in ([17], Prop. 9, p. 37), and follows from the fact that, for a suitable power q of p, the map $x \mapsto x^q$ is k-morphism of varieties of H onto S.

6.13. PROPOSITION. *Let H, K be two subgroups of type* (C) (*resp. Cartan subgroups, resp. maximal tori*) *of G and $\mathfrak{a}, \mathfrak{b}$ two Cartan subalgebras* (*resp. maximal toral subalgebras*) *of* $\mathfrak{g}$. *If H, K* (*resp.* $\mathfrak{a}, \mathfrak{b}$) *are defined over k, then* $\mathrm{Tr}(H, K)$ (*resp.* $\mathrm{Tr}(\mathfrak{a}, \mathfrak{b})$) *is defined over k, and H, K* (*resp.* $\mathfrak{a}, \mathfrak{b}$) *are conjugate under $G(k_s)$. The group $N(H)$* (*resp.* $N(\mathfrak{a})$) *is defined over k if and only if H* (*resp.* $\mathfrak{a}$) *is so.*

The Lie algebra of $N(\mathfrak{a})$ is $\mathfrak{a}$ if $\mathfrak{a}$ is a Cartan subalgebra, $\mathfrak{z}(\mathfrak{a})$ if $\mathfrak{a}$ is a maximal toral subalgebra (4.3). Taking 6.8 into account, it follows that $\mathfrak{a}$ is defined over k if $N(\mathfrak{a})$ is so. If H is of type (C) or is a Cartan subgroup, it is the identity component of $N(H)$. If H is a maximal torus, then it is the unique maximal torus of the Cartan subgroups $Z(H)^0 = N(H)^0$ of G^0. Using 6.12 in the latter case, we see that H is defined over k if $N(H)$ is so.

To prove the remaining part of the proposition, we may assume $H, K, \mathfrak{a}, \mathfrak{b}$ to be defined over k. Then $\mathrm{Tr}(H, K)$ and $\mathrm{Tr}(\mathfrak{a}, \mathfrak{b})$ are defined over purely inseparable extensions of k, and it suffices to prove that they are defined over k_s. For the rest of the proof we may (and shall) assume k to be *separably closed.*

Let $\mathfrak{a}$ be a Cartan subalgebra, $\mathfrak{t}$ its maximal toral subalgebra. Since k is infinite, there exists $X \in \mathfrak{a}(k)$, regular, semi-simple, and we have $Z(X)^0 = Z(\mathfrak{t})^0$ by 6.3. Let $M = \mathrm{Ad}\,G(X)$. Then M is closed and f: $g \mapsto \mathrm{Ad}\,g(X)$ is a surjective separable k-morphism of G onto M (4.1). Let us show that M and $\mathfrak{a}$ intersect transversally. Let $g \in G$ be such that $Y = \mathrm{Ad}\,g(X) \in \mathfrak{a}$. Then $Y \in \mathfrak{t}$ and $\mathfrak{z}(Y) = \mathfrak{a}$, hence $g \in N(\mathfrak{a})$. But $N(\mathfrak{a})^0 = Z(X)^0$ by 6.9; therefore $M \cap \mathfrak{a}$ is zero-dimensional and the intersection is proper. Since $M \cap \mathfrak{a}$ is an orbit of $N(\mathfrak{a})$, it suffices to check transversality at X. The space $T(M)_X$ is the translate by X of $[X, \mathfrak{g}]$ (see 1.10). Since X is semi-simple, $\mathfrak{g} = \mathfrak{z}(X) \oplus [X, \mathfrak{g}] = \mathfrak{a} + [X, \mathfrak{g}]$, which yields our assertion. By conjugacy, M is transversal to any Cartan subalgebra. In particular $M \cap \mathfrak{b}$ is defined over k (1.13) and its points are rational over k (recall that $k = k_s$ here). A simple application of 1.13 shows then that $\mathrm{Tr}(\mathfrak{a}, \mathfrak{b}) = f^{-1}(M \cap \mathfrak{b})$ is defined over k and has points rational over k. Also, $N(\mathfrak{a}) = \mathrm{Tr}(\mathfrak{a}, \mathfrak{a})$ is defined over k. This settles the proposition for Cartan subalgebras, hence also, in view of 6.8 and 4.3, for maximal toral subalgebras and for subgroups of type (C).

The argument for Cartan subgroups is quite similar, but proceeds in the group rather than in the Lie algebra, and we outline it briefly. Let T be the unique maximal torus of H. It is defined over k (6.12) and we may find $x \in T(k)$ such that $Z(x)^0 = H$. The conjugacy class $M = \operatorname{Int} G(x)$ is closed and $g \mapsto g\cdot x\cdot g^{-1}$ is a surjective separable k-morphism of G onto M (4.6). Using 1.13 and the conjugacy of Cartan subgroups we see exactly as above that it suffices to check that M and H intersect transversally. If $g\cdot x\cdot g^{-1} \in H$, then x is a regular semi-simple element of H, $Z(g\cdot x\cdot g^{-1})^0 = H$, and $g \in N(H)$. Thus $M \cap H$ is zero dimensional, hence the intersection is proper. Since $M \cap H$ is an orbit of $N(H)$, there remains to check transversality at x. By 1.10, $T(M)_x$ is the translate by x of $(1-\operatorname{Ad} x)(\mathfrak{g})$. Since x is semi-simple, $\mathfrak{g} = \mathfrak{z}(x) + (1-\operatorname{Ad} x)(\mathfrak{g}) = \mathfrak{h} + (1-\operatorname{Ad} x)(\mathfrak{g})$, whence the result. By 6.12 this also implies the corresponding assertion for maximal tori.

6.14. COROLLARY. *Let $\mathfrak{s}$ be a toral subalgebra of G defined over k. Then $Z(\mathfrak{s})$ is defined over k.*

In fact, $Z(\mathfrak{s})$ consists of finitely many components of $N(\mathfrak{s})$, hence is defined over k_s, and on the other hand, $Z(\mathfrak{s})$ is purely inseparable over k.

7. Varieties of subgroups.

In §§7, 8, for an extension k' of k in K, $C_{k'}$ denotes the category of extension fields of k' in K, where the morphisms are the inclusion homomorphisms. For $k' \in C_k$, $\bar{k}'$ is the algebraic closure of k' in K, k'_s the separable closure of k' in $\bar{k}'$, and $\Gamma(k')$ the Galois group of k'_s over k'.

7.1. A (G,k)-set M is a set with the following properties:

(i) $G(K)$ operates on M. For each $m \in M$, the isotropy group of m is the set of K-points of an algebraic subgroup of G, to be denoted G_m.

(ii) There is given an inclusion preserving map $k' \mapsto M(k')$ from C_k to subsets of M, such that $M = M(K)$ and $M(k')$ is stable under $G(k')$.

(iii) For $k' \in C_k$, $\Gamma(k')$ operates on $M(k'_s)$ continuously, ($\Gamma(k')$ being endowed with the usual pro-finite topology, and $M(k'_s)$ with the discrete topology, (see [2])). We have

$$ {}^s(g\cdot m) = {}^sg\cdot {}^sm\,, \quad (g \in G(k'_s),\ m \in M(k'_s),\ s \in \Gamma(k'))\,, \tag{1} $$

and for $k \subset k' \subset k'' \subset K$, the following diagram

$$\begin{tikzcd}
\Gamma(k') & \times\, M(k'_s) \arrow[r] \arrow[d, "i"] & M(k'_s) \arrow[d, "i"] \\
\Gamma(k'') \arrow[u, "j"] & \times\, M(k''_s) \arrow[r] & M(k''_s)
\end{tikzcd}$$

where i is the inclusion map, and j the natural restriction homomorphism, is commutative.

The (G, k)-set is *homogeneous* if $G(K)$ acts transitively on M.

We can view M as a functor from C_k to sets. Our conditions mean that the functors $G: k' \mapsto G(k')$ and $\Gamma: k' \mapsto \Gamma(k')$ operate on M, and verify a compatibility relation (1).

A (G, k)-set defines in an obvious way a (G, k')- set for every $k' \in C_k$.

If G' is a k-group, and $f: G' \to G$ is a k-morphism, then $G'(K)$ operates on M, and M is a (G', k)-set. It is homogeneous if M is so and f is surjective.

7.2. Examples. (a) Let X be a k-variety on which G acts k-morphically, transitively and separably. Then $M = X(K)$, with $M(k') = X(k')$, $(k' \in C_k)$, is a homogeneous (G, k)-set.

(b) Let V be a k-variety. We recall that to a k'_s-subvariety W of V $(k' \in C_k)$, and to $s \in \Gamma(k')$ there is associated a conjugate k'_s-subvariety, to be denoted ${}^sW$. In this way $\Gamma(k')$ operates on the set of k'_s-subvarieties of V. Assume that G operates k-morphically on V. Then $G(K)$ operates on the set M of K-subvarieties of V, which is easily seen to be a (G, k)-set, $M(k')$ being by definition the set of elements of $M(K)$ which are defined over k' $(k' \in C_k)$. An orbit Q of $G(K)$ in M such that $Q(k'_s)$ is stable under $\Gamma(k')$ for every $k' \in C_k$ is then a homogeneous (G, k)-set. In this case, $Q(k')$ is the fixed point set of $\Gamma(k')$ in $M(k'_s)$.

In this paper, we shall be interested only in two special cases of this situation, namely:

(i) $V = G$, operated upon by inner automorphisms, M is a conjugacy class of closed subgroups;

(ii) $V = \mathfrak{g}$, operated upon by the adjoint representation, and M is a conjugacy class of subalgebras.

In both cases G_m is the normalizer of m in G.

7.3. Let M be a homogeneous (G, k)-set. Then $M = G(K)/G_m(K)$, which allows one to identify M with the set of K-points of a K-variety X on which G operates separably and transitively. We want to give conditions under which the field of definition of X can be brought down to k. More precisely, let X be a k-variety and φ a map from $X(K)$ to $M(K)$. We shall say that (X, φ), or simply X, *is the* (G, k)*-variety of elements of* M, or that M *is defined over* k, or that the functor M is *representable*, and *represented* by X, if it satisfies the following conditions:

(A) *G operates k-morphically, transitively and separably on X, and φ is a $G(K)$-equivariant bijection of $X(K)$ onto M which induces an isomorphism of (G, k)-sets.*

Clearly (X, φ) is also the (G, k')-variety of elements in M for $k' \in C_k$. It is immediate, and will follow from 7.5 (i), that (X, φ) is determined up to a unique k-isomorphism by (A), which justifies calling X "the" k-variety of elements in M. Note that in order to show that φ is compatible with 7.1 (ii), (iii) it is enough to check:

(B) *$M(k')$ is the set of fixed points of $\Gamma(k')$ in $M(k'_s)$. The map φ is a $G(K)$-equivariant bijection of $X(K)$ onto $M(K)$ which, for every $k' \in C_k$, induces a $\Gamma(k')$-equivariant bijection of $X(k'_s)$ onto $M(k'_s)$.*

In fact, since the fixed point set of $\Gamma(k')$ in $X(k'_s)$ is $X(k')$, φ induces then a $G(k')$-equivariant bijection of $X(k')$ onto $M(k')$, for every $k' \in C_k$, and all our conditions are fulfilled.

7.4. LEMMA. *Let M be a homogeneous (G, k)-set and (X, φ) the (G, k)-variety of elements in M. Let G' be a k-group and $f \colon G' \to G$ a surjective k-morphism. Assume that $\mathfrak{g}$ is spanned by $df(\mathfrak{g}')$ and by the Lie algebra of some isotropy group $G_m (m \in M)$. Then (X, φ), acted upon by G' via f, is the (G', k)-variety of elements in M, viewed as a (G', k)-set.*

Let $a \in X(K)$. By assumption $T(X)_a$ is the image of $\mathfrak{g}$ under the differential of the morphism $g \mapsto g \cdot a$. By the condition imposed on df, it follows that $T(X)_a$ is the image of $\mathfrak{g}'$ under the differential of the morphism $g' \mapsto f(g') \cdot a$ of G' onto X, hence G' acts on X transitively and *separably*. It is then clear that the other conditions in 7.3 are fulfilled for G'.

7.5. LEMMA. *Let G' be a k-group, and $f \colon G' \to G$ a surjective k-morphism. Let M' (resp. M) be a homogeneous (G', k)-set (resp. (G, k)-set). Assume that $\mathfrak{g}$ is spanned by $df(\mathfrak{g}')$ and the Lie algebra of G_m $(m \in M)$. Let (X', φ') and (X, φ) be (G', k)- and (G, k)-variety structures on M' and M respectively. Let $\lambda \colon M' \to M$ be an f-equivariant map which, for each extension k' of k in K, induces a $\Gamma(k')$-equivariant map of $M'(k'_s)$ into $M(k'_s)$.*

(i) *There exists a unique f-equivariant k-morphism $\psi \colon X' \to X$ which coincides with $\varphi^{-1} \circ \lambda \circ \varphi'$ on $X(K)$. The map ψ is surjective, separable.*

(ii) *Let k' be an extension of k in K. Let $m \in M(k')$, and $a = \varphi^{-1}(m)$. Then $\psi^{-1}(a)$ is the k'-variety of elements in $\lambda^{-1}(m)$, acted upon in the natural way by $f^{-1}(G_a)(K)$.*

In view of 7.4, we may assume that $G = G'$ and f is the identity.

(i) Let $a' \in X'(k_s)$, $m' = \varphi'(a')$, $m = \lambda(m')$, $a = \varphi^{-1}(m)$. The groups $G_a = G_m$ and $G_{a'} = G_{m'}$ are defined over k'_s; moreover, $G_{a'} \subset G_a$, since λ is a G-morphism.

Let μ: $G/G_{a'} \to G/G_a$ be the canonical projection. It is a surjective separable k_s-morphism. The maps $g \mapsto g\cdot a$ and $g \mapsto g\cdot a'$ define k_s-isomorphisms α: $G/G_a \xrightarrow{\sim} X$ and α': $G/G_{a'} \xrightarrow{\sim} X'$ such that

$$(1) \qquad \alpha\circ\mu\circ\alpha'^{-1} = \varphi^{-1}\circ\lambda\circ\varphi' ,$$

on $X'(K)$. Let $\psi = \alpha\circ\mu\circ\alpha'^{-1}$. It is a separable surjective k_s-morphism of X' onto X. The assumption implies that it commutes with $\Gamma(k)$, hence ψ is defined over k. Since ψ is given on $X'(K)$ it is clearly unique.

(ii) The variety $Y=\psi^{-1}(a)$ is defined over k', since ψ is separable. The group G_a is also defined over k', being the inverse image of a under the k'-morphism $g \mapsto g\cdot a$ of G onto X, which is separable. It is then readily checked that 7.3 (A), with k replaced by k' is fulfilled by Y, $\varphi|Y$ and $\lambda^{-1}(m)$.

The following proposition extends, for homogeneous M, 4.9 of [2] to non-necessarily perfect groundfields. More general results on representability of such functors may be found in ([12], Exp. XIII).

7.6. PROPOSITION. *Let M be a homogeneous (G, k)-set. Assume*:

(a) *for every extension k' of k in $\bar{k}$, the set $M(k'_s)$ is a non-empty orbit of $G(k'_s)$ stable under $\Gamma(k')$, the set of fixed points of $\Gamma(k')$ in $M(k'_s)$ is $M(k')$, and $m\in M$ belongs to $M(k'_s)$ if and only if G_m is defined over k'_s.*

Then M is representable by a (G,k)-variety (7.3).

We first show the existence of (X,φ) verifying 7.3 (B) for $k'=k$. The proof is the same as that of an analogous result in [2, 4.10], where k was assumed to be perfect, and we sketch it briefly.

Let k_1 be a finite Galois extension of k in k_s such that $M(k_1)\neq\emptyset$ and let $m\in M(k_1)$. Let $Y=G/G_m$. The map $g\mapsto g\cdot m$ induces a $G(\bar{k})$-equivariant bijection α of $Y(\bar{k})$ onto M and a $G(k_s)$-equivariant bijection of $Y(k_s)$ onto $M(k_s)$. The latter allows one to define an action of $\Gamma(k)$ on $Y(k_s)$ by

$$(1) \qquad y \mapsto s(y) = \alpha^{-1}({}^s(\alpha(y))), \quad (y\in Y(k_s),\ s\in\Gamma(k)).$$

It follows from 7.1 (1) that

$$(2) \qquad s(g\cdot y) = {}^sg\cdot s(y), \quad (y\in Y(k_s),\ g\in G(k_s)).$$

Since $G(k_s)$ is transitive on $M(k_s)$ we can, given $s\in\Gamma(k)$, choose $u_s\in G(k_s)$ such that ${}^sm=u_s\cdot m$. We have then

$$(3) \qquad \alpha\cdot s(y) = {}^sg\cdot\alpha(u_s\cdot m) \quad (y=g\cdot\alpha^{-1}(m)\,;\ g\in G(k_s)).$$

It follows from 7.1 (1) that ${}^sG_m = G_{s_m}$, whence ${}^sY = G/{}^sG_m = G/G_{s_m}$, and

$$(4) \qquad u_s \cdot G_m \cdot u_s^{-1} = G_{s_m}.$$

The latter relation shows that $g \mapsto g \cdot u_s$ induces a k_s-isomorphism F_s of ${}^sY$ onto Y. Let f_s: ${}^sY(k_s) \to Y(k_s)$ be the bijection characterized by

$$f_s({}^sy) = s(y) \qquad (y \in {}^sY(k_s)).$$

It follows immediately from (3) that f_s is the restriction of F_s to ${}^sY(k_s)$. Thus condition (a) of ([2], lemma 2.12, p. 132) is fulfilled. Conditions (b), (c) of that lemma are checked to hold true exactly in the same way as in ([2], p. 143). The lemma yields then the existence of a k-variety X and of a k_1-isomorphism β: $X \to Y$ which commutes with $\Gamma(k)$, where $\Gamma(k)$ acts on X in the natural way, on Y by (1). We let G act on X in the obvious way via β, i.e.,

$$g \cdot x = \beta^{-1}(g(\beta(x))) \qquad (g \in G,\ x \in X).$$

This action is transitive, separable, defined over k_1. For $s \in \Gamma(k)$, $g \in G(k_s)$, $x \in X(k_s)$, we have, using (2)

$${}^sg \cdot {}^sx = \beta^{-1}({}^sg(\beta({}^sx))) = \beta^{-1}({}^sg \cdot s(\beta(x))) = \beta^{-1}(s(g \cdot \beta(x))) = {}^s(\beta^{-1}(g \cdot \beta(x)))$$

hence

$${}^sg \cdot {}^sx = {}^s(g \cdot x),$$

which implies that the k_1-morphism $G \times X \to X$ defining the action of G on X commutes with $\Gamma(k)$, hence is defined over k. It is then clear that (X, φ), where $\varphi = \alpha \circ \beta$, verifies the condition 7.3 (B) for $k' = k$.

We now prove that (X, φ) verifies 7.3 (B) in general. Given k' ($k \subset k' \subset K$) we have to show

$$(5) \qquad \varphi(X(k'_s)) = M(k'_s),$$

$$(6) \qquad \varphi({}^sb) = {}^s(\varphi(b)), \qquad (b \in X(k'_s),\ s \in \Gamma(k')).$$

Let $b \in X(k'_s)$. Since G operates separably on X, the isotropy group G_b of b is defined over k'_s. Since $G_b = G_{\varphi(b)}$, the condition imposed on M shows that $\varphi(b) \in M(k'_s)$. Let now $m \in M(k'_s)$. There exists $g \in G(k'_s)$ such that $m = g \cdot \varphi(b)$. We have therefore $m = g \cdot \varphi(b) = \varphi(g \cdot b) \in \varphi(X(k'_s))$, whence (5).

Choose $a \in X(k_s)$, and let again $b \in X(k'_s)$. The k_s-morphism $g \mapsto g \cdot a$

being separable, there exists $g \in G(k_s')$ such that $b = g \cdot a$. We have then ${}^s b = {}^s g \cdot {}^s a$, hence

$$(7) \qquad \varphi({}^s b) = {}^s g \cdot \varphi({}^s a) \qquad (s \in \Gamma(k'))\,.$$

Let $s' \in \Gamma(k)$ be the restriction of s to k_s. Then s and s' have the same action on $X(k_s)$ and on $M(k_s)$, (see 7.1), therefore

$$\varphi({}^s a) = \varphi({}^{s'} a) = {}^{s'}(\varphi(a)) = {}^s(\varphi(a))\,,$$

since (X, φ) verifies (B) for $k' = k$; taking (7) and 7.1(1) into account, we get

$$\varphi({}^s b) = {}^s g \cdot {}^s(\varphi(a)) = {}^s(g \cdot \varphi(a)) = {}^s(\varphi(g \cdot a)) = {}^s(\varphi(b))\,.$$

7.7. PROPOSITION. (i) *The varieties of maximal tori and of Cartan subgroups of G are defined over k and are canonically isomorphic over k.*

(ii) *The varieties of subgroups of type* (C), *of Cartan subalgebras, and of maximal toral subalgebras of G are defined over k, and are canonically isomorphic over k.*

(iii) *Let $\mathscr{T}$ and C be the varieties of maximal tori and of subgroups of type* (C) *of G. Then the map $T \mapsto Z(\mathfrak{t})^0$ induces a surjective separable k-morphism $\tau = \tau_G \colon \mathscr{T} \to C$ of G-spaces. If $k' \in C_k$, and $H \in C(k')$, then $\tau^{-1}(H)$ is the k'-variety of maximal tori of H.*

Let M be one of the sets of subgroups or subalgebras listed in the statement. Then M is a conjugacy class of G (see 6.6 and [1], [10]) hence is an orbit of G in the set of irreducible subvarieties of G or $\mathfrak{g}$, operated upon by inner automorphisms or by the adjoint representation. 7.6 (a) is fulfilled in view of 6.12, 6.13, which yields the existence of the (G, k)-variety structures listed in 7.7.

As was remarked earlier (6.12), the Cartan subgroups of G defined over an extension k' of k are the centralizers of the maximal tori defined over k' of G. Consequently, the map which assigns to a maximal torus its centralizer is a bijection of the set A of maximal tori on the set B of Cartan subgroups, which induces a bijection of $A(k_s')$ onto $B(k_s')$ commuting with $\Gamma(k')$, whence the isomorphism of (i). The isomorphisms of (ii) follow similarly, using 6.6, 6.8.

(iii) is an application of 7.5 (ii).

7.8. PROPOSITION. *Let G' be a k-group and $f \colon G' \to G$ a surjective k-morphism such that $\mathfrak{g}$ is spanned by $df(\mathfrak{g}')$ and some maximal toral subalgebra. Let $\mathscr{T}'$ and C' (resp. $\mathscr{T}$ and C) be the k-varieties of maximal tori and of subgroups of type* (C) *of G' (resp. G).*

(i) *The map f induces a surjective separable k-morphism α of $\mathscr{T}'$ onto $\mathscr{T}$, which is an isomorphism if f is an isogeny.*

(ii) *If f is separable, it induces a surjective separable k-morphism $\beta\colon \mathcal{C}' \to \mathcal{C}$ such that $\tau_{G'} \circ \alpha = \beta \circ \tau_G$.*

The map f induces a surjective map of the set of maximal tori of G' onto the set of maximal tori of G ([1], §22), and is bijective if f is an isogeny. If f is separable, then f induces a surjective map of the sets of subgroups of type (C), by 6.10. The proposition follows therefore from 7.4.

The following theorem, for $\mathscr{T}$, is Grothendieck's main rationality result ([12], Exp. XIV, Th. 6.2, p. 39):

7.9. THEOREM. *The (G, k)-varieties $\mathscr{T}$ of maximal tori and $\mathcal{C}$ of subgroups of type* (C) *of G are rational varieties over k.*

We may assume G to be connected. The proof proceeds by induction on $\dim G$. There is nothing to prove if G is nilpotent, in particular if $\dim G=1$. If G is its own subgroup of type (C), then $\mathcal{C}$ is reduced to a point rational over k. Using 7.8, 5.3 we see that it suffices to consider the case where the subgroups of type (C) of G are *proper*. Let $\tau\colon \mathscr{T} \to \mathcal{C}$ be the canonical morphism (7.7). Let $k' \in C_k$. By 7.7 and 7.5, if $H \in \mathcal{C}(k')$ then $\tau^{-1}(H)$ is the k'-variety of maximal tori of H. By our induction assumption, it is a rational variety over k'. In particular, $\tau^{-1}(H)(k') \neq \emptyset$, if k' is infinite. If we apply this to a generic point over k, we see that the field $k(\mathscr{T})$ is a purely transcendental extension of $k(\mathcal{C})$. It suffices therefore to prove that $\mathcal{C}$ is a rational variety over k. In the sequel, we view $\mathcal{C}$ as the k-variety of Cartan subalgebras of $\mathfrak{g}$, which is possible (7.7).

We assume first that $\mathfrak{g}(k)$ contains a regular semi-simple element X. This is the case notably if k is infinite (6.2) or if G is reductive (6.4). Let $\mathfrak{h}=\mathfrak{z}(X)$ and $\mathfrak{m}$ be a supplementary subspace to $\mathfrak{h}$ in $\mathfrak{g}$, defined over k. Then $N(\mathfrak{h})$ is defined over k (6.13), and $\mathcal{C}$ may be identified, over k, with $G/N(\mathfrak{h})$. To prove the assertion, we shall set up a k-isomorphism between non-empty open subsets of $\mathcal{C}$ and $\mathfrak{m}$. The set U of $Z \in \mathfrak{m}$ such that $X+Z$ is regular is non-empty, since $0 \in U$, and open, since the set of regular elements in $\mathfrak{g}$ is open (6.1). Such an element is contained in a unique Cartan subalgebra $\mathfrak{h}_Z$, namely its nilspace. Let V be the set of $Z \in U$ such that $\mathfrak{h}_Z \cap \mathfrak{m} = 0$. It is open, non-empty. The set of Cartan subalgebras $\mathfrak{h}'$ such that $\mathfrak{h}' \cap \mathfrak{m} = 0$ is open, not empty in $\mathcal{C}$, therefore the set W of Cartan subalgebras $\mathfrak{h}_Z (Z \in V)$ is open, non-empty, in $\mathcal{C}$. To prove our assertion, it is then enough to show that $\alpha\colon Z \mapsto \mathfrak{h}_Z$ is a k-isomorphism of V onto W. The nilspace of ad $(X+Z)$ is also the kernel of $(\mathrm{ad}\,(X+Z))^n$ $(n = \dim \mathfrak{g})$ which implies immediately that

α is a k-morphism. Any subspace $\mathfrak{q}$ of $\mathfrak{g}$ supplementary to $\mathfrak{m}$ intersects $X+\mathfrak{m}$ at only one point, which is rational over the smallest field of definition of $\mathfrak{q}$ containing k, hence α is bijective, birational over k, and therefore is a k-isomorphism.

There remains to consider the case where k is *finite* and G is not reductive. Its unipotent radical U is then defined over k, (since k is perfect), and $\neq \{e\}$. Let N be a non-trivial central connected k-subgroup of exponent p, normal in G (e.g., a suitable p-th power of the last non-trivial term in the descending central series of U). Let $\pi : G \rightarrow G' = G/N$ be the canonical projection. By 7.5, 7.7, it induces a separable surjective k-morphism β of $\mathcal{C}$ onto the k-variety $\mathcal{C}'$ of subgroups of type (C) of G', and, for $H' \in \mathcal{C}'(k')$, $\beta^{-1}(H')$ is the k'-variety of subgroups of type (C) of $\pi^{-1}(N(H'))$, $(k' \in C_k)$. If $H' \neq G'$, then induction, and the argument used earlier in the reduction to varieties of Cartan subalgebras, show that $\mathcal{C}$ is a rational variety over k. So assume $H' = G'$. Let A be a subgroup of type (C) of G defined over k, (6.10). Then, by 6.10 (b), we have $G = A \cdot N$, and also, since π is separable, $\mathfrak{g} = \mathfrak{a} + \mathfrak{n}$. Since $G/N = A/(A \cap N)$, it follows that $\dim(A \cap N) = \dim(\mathfrak{a} \cap \mathfrak{n})$, hence N and A intersect transversally. Then so do N and $N(A)$. Consequently, the natural bijective morphism of varieties of $N' = N/(N \cap N(A))$ onto $G/N(A) \cong \mathcal{C}$ is a k-isomorphism. But N' is a connected commutative k-group of exponent p. Since k is perfect, N' is k-solvable, in the sense of [20], and is k-isomorphic to a vector group by Prop. 1.2, p. 688 of [18]. In particular, it is a rational variety over k.

REMARK. If G is solvable, we have the stronger result that $\mathcal{C}$ and $\mathscr{G}$ are k-isomorphic to affine spaces (see 9.14).

We mention some consequences of 7.9. For more results, see ([12], Exp. XIV).

7.10. PROPOSITION. *G has a maximal torus defined over k. If G is connected, it is generated by its Cartan subgroups defined over k.*

It suffices to prove the second assertion (6.12). If k is finite, see 2.9. Let k be infinite. The k-variety M of Cartan subgroups of G is a rational variety over k (7.7, 7.9), hence $M(k)$ is Zariski-dense, and in particular not empty. There exists therefore a Cartan subgroup C defined over k. Its normalizer $N(C)$ is also defined over k (6.13), and M is k-isomorphic to $G/N(C)$. Let H be the subgroup of G generated by the Cartan subgroups defined over k of G. Assume $H \neq G$. Since $C \subset H$ and C has finite index in $N(C)$, the image of H in $G/N(C)$ has a strictly smaller dimension than $G/N(C)$. But it contains $(G/N(C))(k)$, which is Zariski-dense, whence a contradiction.

7.11. COROLLARY. *Let G be connected. Assume that the Cartan subgroups of G defined over k are unirational over k. Then G is unirational over k. If k is infinite, $G(k)$ is dense in G.*

(We recall that an irreducible k-variety V is unirational over k if there exists a dominant k-morphism of an open subset of an affine space into V, or, equivalently, if the field $k(V)$ is contained in a purely transcendental extension of k. If k is infinite, this implies that $V(k)$ is Zariski-dense in V.)

In view of 7.10 we can find finitely many Cartan subgroups $C_1, \cdots, C_t$ of G, defined over k, such that the product map: $C_1 \times \cdots \times C_t \to G$ is surjective, whence our assertion.

7.12. COROLLARY. *Let G be connected. Then G is unirational over k if either k is perfect or G is reductive. In particular if k is infinite and either k is perfect or G is reductive, $G(k)$ is dense in G.*

If G is reductive, its Cartan subgroups are maximal tori, hence are unirational over their fields of definition ([17], Prop. 6, p. 39). If k is perfect, any connected nilpotent k-group is unirational over k.

REMARK. For perfect infinite fields, 7.10 to 7.12 are due to Rosenlicht [17]. For solvable groups and infinite fields the existence of a maximal torus defined over k is also proved in ([20], Thm. 4). See also ([3], §11).

8. Some results on reductive groups.

8.1. Let G be connected, reductive, T a maximal torus of G, and Φ the set of roots of G with respect to T. Given $b \in \Phi$, there exists an isomorphism θ_b of the additive group $\boldsymbol{G}_a$ onto a unipotent subgroup U_b of G, uniquely determined by b, such that

$$(1) \qquad t \cdot \theta_b(x) \cdot t^{-1} = \theta_b(t^b \cdot x), \qquad (x \in G_a;\ t \in T).$$

The group G is said to *split over k*, or to be *k-split*, if we can choose T to be k-split, and the θ_b's to be defined over k.

The theorem below is due to P. Cartier (unpublished). More general results can be found in ([12], Exp. XXII):

8.2. THEOREM. *Assume that G is connected, reductive, and contains a maximal torus which is defined over k and splits over k. Then G splits* *over k.*

We keep the notation of 8.1 and assume T to be k-split. Then b is defined over k ([3], 1.3, p. 60). Let $S = (\ker b)^0$. It is a subtorus of T, of codimension one, defined over k ([3], 1.6, p. 61). By 8.1 (1), $Z(S) \supset U_b$, U_{-b}. The group $Z(S)$ is defined over k (4.6), is reductive and contains T. It is known that its commutator subgroup H' is three-dimensional, generated by U_b, U_{-b}, ([10], Exp. 13) and defined over k. Moreover $L_b = (H' \cap T)^0$ is one-dimensional, defined over k, and split over k. The roots of H' with respect to L_b are $\pm b'$, where b' is the restriction of b to L_b. Since $\ker b' = (L_b \cap \ker b)$, it is clear that a monomorphism $\theta_{b'}: \boldsymbol{G}_a \to H'$ verifying $t \cdot \theta_{b'}(x) t^{-1} = \theta_{b'}(t^b \cdot x)$ for $x \in G_a$, $t \in L_b$ may also be viewed as a homomorphism θ_b verifying 8.1 (1). We are therefore reduced to the case where G is of type A_1; we denote by $\pm b$ the roots of G. We have $\mathfrak{g} = \mathfrak{t} + \mathfrak{g}_b + \mathfrak{g}_{-b}$. Since T splits over k, $\mathrm{Ad}_G T$ is diagonalizable over k, and $\mathfrak{g}_b$, $\mathfrak{g}_{-b}$ are defined over k. Let $\mu: G \to G'$ be as in 5.3 if $\mathfrak{t}$ is central in $\mathfrak{g}$, the identity otherwise. We want to prove that $U_{\pm b}$ is defined over k and is k-isomorphic to $\boldsymbol{G}_a$. It suffices to show that $B^{\pm} = T \cdot U_{\pm b}$ is defined over k, because $U_{\pm b}$ is its derived group, and then μ is a k-isomorphism of $U_{\pm b}$ onto its image (since $\ker d\mu = \mathfrak{t}$), and $\mu(U_{\pm b})$ is k-isomorphic to $\boldsymbol{G}_a$ by [4, 1.2]. Let $B' = \mu(B^+)$. It follows readily from 2.6 that B is the stability group of $\mathfrak{b}'$ in G, acting on $\mathfrak{g}'$ via $\mathrm{Ad} \circ \mu$. Since $L(\mu(T))$ is not central in $\mathfrak{g}'$, it is clear that $\mathfrak{b}'$ is its own normalizer in $\mathfrak{g}'$. Since $\ker d\mu = \mathfrak{t}$, it follows then that the orbit map $f: g \mapsto \mathrm{Ad}(g) \cdot (\mathfrak{b}')$ in the Grassmannian of two-planes in $\mathfrak{g}'$ is separable. Then $B = f^{-1}(\mathfrak{b}')$ is defined over k by 1.13. Similarly for B^-.

Let $\alpha: \boldsymbol{G}_a \to U_b$ be a k-isomorphism. Then $\alpha^{-1} \circ \theta_b$ is an automorphism of G_a, hence is of the form $x \mapsto c \cdot x$ for some $c \in \bar{k}^*$. But then it is obvious that 8.1 (1) holds for α too, i.e., we may choose θ_b to be defined over k.

8.3. COROLLARY. *The group G splits over a finite separable extension of k.*

This follows from 8.2 and from the fact that a k-torus splits over a separable extension of k [3, 1.5, p. 61].

8.4. PROPOSITION. *Assume that G is connected and has a unipotent radical U defined over k. Let $\mathcal{P}$ be a conjugacy class of parabolic subgroups, such that the set $\mathcal{P}(k_s)$ of elements of $\mathcal{P}$ defined over k_s is stable under $\Gamma(k)$. Then the variety of elements in $\mathcal{P}$ is defined over k. In particular, the variety of Borel subgroups of G is defined over k.*

A parabolic subgroup is equal to its normalizer (cf. [10], Exp. 9 for Borel subgroups, the general case follows immediately) therefore the last condition of 7.6 (a) is automatically fulfilled. The second one holds true, since we deal with subvarieties of a k-variety (7.2 (b)).

Let $\pi: G \to G/U$ be the canonical projection. Since U is assumed to be defined over k, π is a separable k'-morphism for every extension k' of k, hence defines a surjective morphism of $G(k'_s)$ onto $G/U(k'_s)$. Moreover π maps $\mathcal{P}$ onto a conjugacy class of parabolic subgroups of G/U. To check the first condition of 7.6 (a), we may therefore assume G to be reductive. Since then two parabolic subgroups of G defined over $k' \in C_k$, and conjugate over $\bar{k}$, are conjugate over k' ([3], Th. 4.13, p. 90), it suffices to show that $\mathcal{P}(k'_s)$ is stable under $\Gamma(k')$, $(k' \in C_k)$. This is clear for Borel subgroups of course.

Fix a maximal k-torus T of G, and an ordering of the roots of G with respect to T. Let Δ be the set of simple roots. Since G splits over k_s, $\mathcal{P}$ contains one and only one standard parabolic k_s-subgroup $P_\theta(\theta \subset \Delta)$, (see [3], 4.3, p. 86). Moreover, $\mathcal{P}(k_s)$ is stable under $\Gamma(k_s)$ if and only if θ is stable under the action of $\Gamma(k)$ on Δ defined in ([3], 6.2, p. 104). Since T splits over k_s, the analogous action of $\Gamma(k')$ on Δ goes through the restriction homomorphism $\Gamma(k') \to \Gamma(k)$, hence θ is also stable under $\Gamma(k')$, which implies our contention.

8.5. COROLLARY. *The variety of Borel subgroups of a k-group H is defined over k if either H is reductive or if k is perfect.*

In the first case, $U = \{e\}$, and in the second one, U is defined over k.

REMARK. Similar results in the framework of schemes are to be found in ([12], Exp. XXII; in particular Cor. 5.8.3, p. 74). If U is not defined over k, the (G, k)-set of Borel subgroups is not always representable by a (G, k)-variety ([12], Exp. XIV, Rem. 4.6, p. 30).

8.6. Using 8.2, one can extend some results of Steinberg [23] to non-perfect ground fields. The following result is proved there for perfect k (Th. 1.7, p. 51):

Let G be a connected, semi-simple simply connected k-group, which is quasi-split (i.e., contains a Borel subgroup which is defined over k). Then any regular semi-simple conjugacy class of G which is defined over k contains an element of $G(k)$.

Using 8.2, the proof given in loc. cit. carries over to arbitrary ground fields, if one observes that, with the notations of ([23], p. 305), any regular semi-simple conjugacy class intersects N in exactly one point, with multiplicity 1 (as follows from loc. cit., 8.1).

The arguments of ([23], §§10, 11) then show:

If k is a field of dimension $\leqq 1$ and G a connected reductive k-group, then $H^1(k, G)=0$.

This answers a question of Serre ([23], p. 58, Remarques).

9. Nilpotent elements in Lie algebras.

9.1. Let X be a non-zero nilpotent element in $\mathfrak{g}(k)$. If $p=0$, we have seen (3.3) that X is tangent to a unique one-dimensional unipotent k-subgroup of G. This is no longer true if $p\neq 0$. A necessary (but not sufficient) condition for this is that $X^{[p]}=0$, a condition which easily is seen not to be always fulfilled (e.g., in $\mathfrak{gl}_n$ for $n>2$). In this paragraph, we give a few positive results in that direction. The example below shows that the sufficient conditions of 9.8, 9.16 (ii), (iii) are also necessary. We assume $p>0$ throughout.

9.2. EXAMPLE. Let q, r be two distinct powers of p, with strictly positive exponents. We let G be the connected unipotent k-group which is k-isomorphic, as a variety, to the 2-dimensional affine space, with the product given by

$$(x,y)\cdot(z,t)=(x+z,\ y+t+x^q\cdot z^r). \tag{1}$$

Since $q\neq r$, G is non-commutative and so yields a (known) example of a 2-dimensional non-commutative nilpotent group in non-zero characteristic. The k-algebra of morphic k-functions on G is $A=k[T,U]$, with the coproduct $\mu\colon A\to A\otimes_k A$ given by

$$\mu(T)=T\otimes 1+1\otimes T,\ \mu(U)=U\otimes 1+1\otimes U+T^q\otimes T^r.$$

One checks that $\mathfrak{g}$ is commutative, spanned by $X=\partial/\partial T$, $Y=\partial/\partial U$ and that $\mathfrak{g}^{[p]}=\{0\}$.

Let H be the k-subgroup of G whose elements are the pairs $(0, y)$. It is k-isomorphic to $\boldsymbol{G}_a$. We claim that any k-morphism $f\colon \boldsymbol{G}_a\to G$ has its image in H. We have $f(x)=(g(x), h(x))$ where g, h are polynomials which verify

$$g(x+y)=g(x)+g(y),\quad g(0)=0, \tag{2}$$

$$h(x+y)-h(x)-h(y)=g(x)^q g(y)^r,\ h(0)=0\quad (x,y\in \boldsymbol{G}_a). \tag{3}$$

If $g\not\equiv 0$, the left hand side of (3) is a symmetric polynomial in x and y, whereas the right hand side is not. This is impossible, hence $g \equiv 0$, which proves our contention. Thus X is not tangent to any one-dimensional subgroup of G and G has elements which are not contained in a connected one-dimensional subgroup. Moreover, as $q \neq r$, X is not tangent to any commutative subgroup of G, and G has elements which do not belong to any connected commutative subgroup.

Let $T = \boldsymbol{GL}_1$ and b a non-trivial character of T. We let T act on G by means of the map $\{t, (x,y)\} \mapsto (t^b x, t^{(q+r)b} y)$. It is readily seen that in this way T acts k-morphically on G, and X, Y are eigen-vectors of T with weights b and $(q+r)\cdot b$.

9.3. Let T be a k-torus, F a finite dimensional vector space defined over k, and $r\colon T \to GL(F)$ a k-morphism. We let $H^1(T, F)$ be the first cohomology group of T with coefficients in the T-module F, based on cochains $T \to F$ which are k-morphisms of varieties. Thus a cocycle is a k-morphism $f\colon T \to F$ such that $f(s \cdot t) = f(s) + r(s) \cdot f(t)$ $(s,\ t \in T)$ and a coboundary is a cocycle of the form $t \mapsto (1 - r(t))u$ $(u \in F(k))$.

LEMMA. *We keep the previous notation. Then* $H^1(T, F) = 0$.

This is a special case of Th. 3.1, p. 10 of [12, Exp. IX]. For the sake of completeness, we sketch a proof. It is first easily seen from the definitions that if k' is an extension of k, then

$$H^1(T \times_k k', F \otimes_k k') = H^1(T, F) \otimes_k k'.$$

It suffices therefore to consider the case where T splits over k, and consequently where F is one-dimensional. Let $a \in X^*(T)$ be such that $r(t) \cdot x = t^a \cdot x$ $(x \in F,\ t \in T)$. The regular k-functions on T are the finite linear combinations with coefficients in k of characters of T. Let f be a 1-cocycle. We have then

$$f(t) = \Sigma_{b \in X^*(T)} c_b \cdot t^b, \qquad (c_b \in k,\ t \in T),$$

with $c_b \neq 0$ for at most finitely many b's. The cocycle condition and the independence of the characters over $\bar{k}$ imply immediately that $f(t) = c_0(1 - t^a)$ $(t \in T)$, which yields the lemma.

9.4. LEMMA. *Let T be a k-torus, U a commutative unipotent connected k-group on which T acts k-morphically, and which verifies $U^p = \{e\}$. Let V be a connected k-subgroup of U stable under T. Assume that V and U/V are T-equivariantly k-isomorphic to vector groups over k on which T acts linearly. Then U is the direct product of V and of a*

k-subgroup stable under T.

Let $\pi: U \to U' = U/V$ be the canonical projection. By ([18], Prop. 1, 2, p. 688) V is a direct factor over k in U. There exists therefore a k-morphism $s: U' \to U$ such that $\pi \circ s = \mathrm{id}$. We have to show the existence of such an s which is T-equivariant. Let F be the set of morphisms of U' into V. Identifying U' and V over k with vector groups, we see that F is the vector space of p-polynomial mappings of U' into V. It has a k-structure, where $F(k)$ consists of the k-morphisms of U' into V. We define a representation r of T in F by

$$r(t) \cdot f(x) = t \cdot f(t^{-1} \cdot x) \qquad (f \in F,\ t \in T,\ x \in U') .$$

Then F is the union of finite dimensional subspaces defined over k, stable under T, on which this representation is rational.

To $t \in T$ let us associate the map:

$$f(t) \colon x \longmapsto (t \cdot s(t^{-1} \cdot x)) \cdot s(x)^{-1} , \qquad (x \in U') .$$

This is readily checked to be a k-morphism of U' into V, which is a cocycle of T with coefficients in a finite dimensional subspace of F, stable under T, and defined over k. By 9.3, there exists $c \in F(k)$ such that $f(t) = c - r(t) \cdot c$. It then follows that $s' \colon x \mapsto s(x) \cdot c(x)$ is the desired cross-section.

9.5. REMARK. The existence of an equivariant cross-section, which is not necessarily a subgroup however, can be proved similarly in a more general case, namely if U is unipotent, V is central and T-equivariantly k-isomorphic to the additive group of a vector space W over k on which T acts via a k-morphism $T \to GL(W)$.

In fact, Cor. 1, p. 100 of [20] still gives the existence of a cross-section $s: U/V \to U$ defined over k. To get an equivariant one, we argue as before with F replaced by the space of k-morphisms of varieties of U/V into V.

9.6. Under the previous conditions, U is T- and V-equivariantly k-isomorphic to $U/V \times V$. More generally let U be a unipotent k-group on which T acts k-morphically, and V a connected k-subgroup stable under T. Assume that there is a T-equivariant cross-section $s: U/V \to U$ defined over k. Then, obviously, the map $\psi\colon (U/V) \times V \to U$ defined by $(x, v) \mapsto s(x) \cdot v$ is a k-isomorphism of varieties which is T-equivariant and commutes with V, acting by right translations. We note also that if A is a k-variety on which T acts k-morphically, such that U is T- and V-equivariantly k-isomorphic to $A \times V$, then the projection of U on U/V induces a T-equivariant k-isomorphism of A onto U/V.

9.7. LEMMA. *Let G be solvable, connected, U the unipotent part of G and T a k-torus of G. Then G has a normal k-subgroup M contained in U, such that $G = Z(T) \cdot M$ and $U = (Z(T) \cap U) \cdot M$. The Lie algebra of M contains all eigenvectors of T not fixed by T. If U is commutative, $M = (T, G)$ and G (resp. U) is the semi-direct (resp. direct) product of $Z(T)$ (resp. $Z(T) \cap U$) and M.*

Let first U be commutative. Let $t \in T(\bar{k})$ be such that $Z(t) = Z(T)$, and M be the image of the commutator map $x \mapsto (t, x)$ $(x \in U)$. Then ([3], 11.1, p. 131), U is the direct product of $N = Z(t) \cap U$ and M. The group M is normalized by $Z(t)$, and also by U since U is commutative, hence M is normal in G. It follows that M containts (s, U) for any $s \in T$ and also, that $(s, U) = (s, G)$ for any $s \in T$, hence $M = (T, U) = (T, G)$. The Lie algebra of N is the fixed point set of T in $\mathfrak{u}$ (4.6), hence $\mathfrak{m}$ is the unique supplementary subspace to $\mathfrak{n}$ in $\mathfrak{u}$ which is stable under T. It contains then all non-zero eigenvectors of T corresponding to non-zero weights.

If V is a normal k-subgroup of G contained in U and $\pi: G \to G/V$ is the canonical projection, then $\pi(Z(T)) = Z(\pi(T))$ ([1], 13.1, p. 60). The proposition in the general case follows then by induction, dividing out by (G, G).

9.8. THEOREM. *Assume G to be connected, solvable and to have a commutative unipotent radical U. Let T be a k-torus of G. Let X be a non-zero nilpotent element of $\mathfrak{g}(k)$, and b a non-trivial character of T such that* $\mathrm{Ad}\, t(X) = t^b \cdot X (t \in T)$. *Assume that either* (a): $U^p = \{e\}$, *or* (b): *no p-power multiple of b is a root of G with respect to T. Then there exists a closed k-subgroup V of G contained in U, stable under T, whose Lie algebra is spanned by X, and a k-isomorphism $\theta: \boldsymbol{G}_a \xrightarrow{\sim} V$, such that $t \cdot \theta(x) \cdot t^{-1} = \theta(t^b \cdot x)$ $(t \in T$, $x \in \boldsymbol{G}_a)$.*

(a) We show first that the proof can be reduced to the case where T is a maximal torus, is one-dimensional, k-split, U is defined over k, $Z(T) \cap U = \{e\}$, and $Z(\mathrm{t})^0 \neq G$.

Replacing G by $T \cdot (T, G)$ we may, in view of 9.7, assume T to be maximal, U to be defined over k, and $Z(T) = T$. Since the representation of T in $\bar{k} \cdot X$ is defined over k, the character b is also defined over k. Let $S = (\ker b)^0$. It is a subtorus of T, defined over k, (see [3], 1.6, p. 61). The groups $Z(S)$ and $Z(S) \cap U$ are connected, defined over k (4.6), and X is in the Lie algebra of $Z(S)$. The canonical projection of $Z(S)$ onto $Z(S)/S$ induces a T-equivariant k-isomorphism of U onto the unipotent radical of $Z(S)/S$. This reduces us to $Z(S)/S$, hence we may assume that T has dimension one. It has a non-trivial character b defined over k, hence is k-split ([3], 1.3, p. 60).

If $\mathfrak{t}$ is central in $\mathfrak{g}$, we perform an isogeny $\pi\colon G\to G'$ of the type of 5.3 onto a group G' whose subgroups of type (C) are proper. We have $G'=\pi(T)\cdot\pi(U)$, and π is a T-equivariant k-isomorphism of U onto $\pi(U)$. It suffices then to consider G', which yields the desired reduction.

(b) Assume $Z(\mathfrak{t})^0=T$. In this case, we shall exhibit a T-equivariant k-isomorphism of U onto $\mathfrak{u}$, the latter being viewed as a vector group. Let Φ be the set of roots of G with respect to T. Our assumption is equivalent to $dc\neq 0$ for all $c\in\Phi$ (1.9, 6.3 (5)). Let A be a non-zero element of $\mathfrak{t}(k)$. Then, since T is one-dimensional, $dc(A)\neq 0$ for all $c\in\Phi$. Thus A is regular, semi-simple and we have $Z(A)\subset N(T)$. Since the normalizer and the centralizer of a torus in a connected solvable group coincide and are connected ([1], 10.2, p. 52, 13.2, p. 60) we have $Z(A)=T$. For $u\in U$, we may write

$$\operatorname{Ad} u(A) = A + f(u) \qquad (f(u)\in\mathfrak{u})$$

and, clearly, f is a T-equivariant k-morphism. Since $Z(A)=T$, the map f is injective, hence bijective. We have $df(\mathfrak{u})=[A,\mathfrak{u}]$ by 1.10, and therefore $df(\mathfrak{u})=\mathfrak{u}$, which shows that f is an isomorphism. It has then the required properties.

(c) We now proceed by induction on $\dim U$. If $\dim U=1$, then, by the condition of (a), $Z(\mathfrak{t})^0=T$, and we are in the case (b). So let $\dim U\geqq 2$, and assume the proposition to hold true for groups with unipotent radical of dimension $<\dim U$.

If $db=0$, then X is in the Lie algebra of $Z(\mathfrak{t})^0$, which is a k-subgroup (4. 3), proper by (a), and induction applies. So let $db\neq 0$. By (b), we have to consider only the case where $C=Z(\mathfrak{t})^0\neq T$. Since $Z(T)=T$, there exists in $\mathfrak{c}(k)$ a non-zero eigenvector Y of T, with non-trivial weight a, no multiple of which is a weight of T in $\mathfrak{c}$. By induction, $Z(\mathfrak{t})\cap U$ contains then a k-subgroup W, k-isomorphic to $\boldsymbol{G}_a$, tangent to Y, and stable under T. Since U is commutative, W is then normal in G. Let $\pi\colon G\to G/W$ be the canonical projection. Then $d\pi(X)\neq 0$. The induction assumption yields a one-dimensional k-subgroup V' of G', tangent to $d\pi(X)$, stable under $\pi(T)$, and T-equivariantly isomorphic to $\bar{k}\cdot X$.

Replacing G by $T\cdot\pi^{-1}(V')$, we are reduced to the case where $\dim U=2$ and $\mathfrak{u}$ is spanned by X, Y. Let us show now that $U^p=\{e\}$, also under the assumption (b) of the proposition. The p-th power $g\mapsto g^p$ is a T-equivariant k-morphism of U or U/W, trivial on W and U/W, hence defines a T-equivariant k-morphism $\mu\colon U/W\to W$. Let $\alpha\colon \boldsymbol{G}_a\to U/W$ and $\beta\colon \boldsymbol{G}_a\to W$ be the k-isomorphisms given by the induction assumption. Then $f=\beta^{-1}\circ\mu\circ\alpha$ is a k-morphism of $\boldsymbol{G}_a$ into itself which verifies $f(t^b\cdot x)=t^c\cdot f(x)$ $(x\in\boldsymbol{G}_a)$. But f is a p-power polynomial. Therefore if $f\neq 0$, then $c=p^j\cdot b$ for some $j\neq 0$, a contradiction. Consequently $f=0$ and $U^p=\{e\}$. Our assertion now follows from 9.4. As an application. we deduce a slight extension and sharpening of a result of Rosenlicht's ([20], lemma on p. 109).

9.9. COROLLARY. *Let G be connected solvable, with a commutative unipotent radical U of exponent p, and T a k-torus of G. Then U is the direct product of $Z(T)\cap U$ and of a k-subgroup M of G contained in U, stable under T, and T-equivariantly k-isomorphic to its Lie algebra, viewed as a vector group. In particular, if T splits over k, M is k-isomorphic to a product of $\mathbf{G}_a$'s stable under T.*

We may write $\mathfrak{u}$ as the direct sum of the fixed point set $\mathfrak{u}_0$ of T and of subspaces $\mathfrak{m}_i$ $(1\leqq i\leqq r)$ defined over k, stable under T, and irreducible over k as T-modules. We have $\mathfrak{u}(k_s)=\mathfrak{u}(k)\otimes_k k_s$, which allows us to view in the usual manner $\mathfrak{u}(k_s)$ as a module for the Galois group $\Gamma(k)$ of k_s over k. Since T splits over k_s, it is elementary that we may find a basis X_{ij} $(1\leqq j\leqq m_i=\dim\mathfrak{m}_i)$ of $\mathfrak{m}_i(k_s)$ formed by eigenvectors of T permuted transitively by $\Gamma(k)$. Let k_i be the smallest overfield of k in k_s such that $X_{i1}\in\mathfrak{m}_i(k_i)$. Choose a one-parameter k_i-subgrpup V_{i1} of U stable under T and tangent to X_{i1} (9.8). It is then stable by $\Gamma(k_i)$. It follows that the transforms ${}^sV_{i1}$, where s runs through a set of representatives of $\Gamma(k)/\Gamma(k_i)$ are m_i distinct k_s-subgroups tangent to the transforms ${}^sX_{i1}$ of X_{i1}. Let $M_i=\Pi_s\,{}^sV_{i1}$. Then M_i is defined over k, with Lie algebra $\mathfrak{m}_i$, and is T-equivariantly k-isomorphic to $\mathfrak{m}_i$. We claim that $M=M_1\cdots M_r$ fulfills our conditions. The Lie algebra of M contains the sum of the $\mathfrak{m}_i$'s, but is not bigger for dimensional reasons. Let $f\colon M_1\times\cdots\times M_r\rightarrow M$ be the product map. It is surjective, T-equivariant and separable. Its kernel is finite, stable under T, hence consists of fixed points of T, and therefore is reduced to $\{e\}$. Thus f is an isomorphism. Similarly, since $\mathfrak{u}_0$ is the Lie algebra of $Z(T)\cap U$ (see 4.6), it follows that $U=(Z(T)\cap U)\times M$.

9.10. PROPOSITION. *Assume G to be connected, solvable, with a commutative unipotent radical U. Let T be a k-split subtorus of G. Then U is the direct product of $Z(T)\cap U$ and of k-subgroups $U_1,\cdots,U_m$ of G, contained in U, stable under T, such that the weights of T in U_i are p-power multiples of one of them, and not zero.*

The proof is by induction on $\dim U$. In view of 9.9, it is enough to consider the case where $T=Z(T)$. Then U is defined over k (9.7). Let Φ be the set of roots of G with respect to T. Write Φ as a disjoint union of sets Φ_i where Φ_i consists of the p-power multiples of one of its elements, and is maximal among subsets having that property. Let a_i be an element of Φ_i such that no p-power multiple of a_i belongs to Φ and let $X_i\in\mathfrak{u}(k)$ be a non-zero eigenvector of T with weight a_i. By 9.8, there exists a k-subgroup N_i of U which is stable under T, tangent to X_i. Let $G_i = G/N_i$. The induction assumption yields a direct k-factor V_i of the unipotent part of G_i stable under T, such that the weights of T in $\mathfrak{v}_i$ are elements of Φ_i. Let U_i be the inverse image of V_i in U. The set of weights of T in U_i is Φ_i, and it is obvious that U is the direct product of the U_i's.

9.11. COROLLARY. *Assume that $Z(T) = T$ and that no root of G with respect to T is a p-power multiple of another one. Then U is a vector group over k, on which T acts linearly.*

We now turn to the case where U is not necessarily commutative.

9.12. COROLLARY. *Let G be connected, solvable, U its unipotent radical, T a k-torus of G, and assume that either $Z(T) \cap U = \{e\}$ or k is perfect. There exists a series $U = U_0 \supset U_1 \supset \cdots \supset U_m = \{e\}$ of connected normal k-subgroups of G stable under T with the following properties: U_i/U_{i+1} is central in U/U_{i+1} and is T-equivariantly k-isomorphic to its Lie algebra $\mathfrak{u}_i/\mathfrak{u}_{i+1}$, on which the representation of T is irreducible over k, $(i = 0, \cdots, m-1)$. There is a T-equivariant k-isomorphism of varieties of U onto $\mathfrak{u}$ which maps U_i onto $\mathfrak{u}_i$ $(i = 0, \cdots, m-1)$.*

U is defined over k (9.7). We may find a non-trivial connected central k-subgroup V of U, stable under T, of exponent p, (e.g., a suitable p-th power of the last non-trivial term in the descending central series of U). Our assertion is true for V: if $Z(T) \cap U = \{e\}$, it follows from 9.9; if k is perfect, it follows from 9.9 and the fact that $Z(T) \cap V$ is k-isomorphic to a vector group ([18], Prop. 1,2, p. 688). The assertion follows then using induction on $\dim U$ and 9.5.

REMARK. This implies in particular that U is k-solvable, in the sense of [20], as follows also from ([20], Cor. to Thm. 3, p. 108). If T is k-split, the groups U_i/U_{i+1} are k-isomorphic to $\boldsymbol{G}_a$. In the general case, U_i/U_{i+1} splits over k_s into a sum of one-dimensional T-modules which are inequivalent, since otherwise U_i/U_{i+1} would not be k-irreducible. Consequently, every closed subgroup of U_i/U_{i+1} stable under T is defined over k_s.

9.13. PROPOSITION. *Let G be solvable, connected, with a unipotent radical U defined over k, and T a k-torus of G. Let V be a connected k-subgroup of U stable under T. Assume that $Z(T) \cap U \subset V$ or that k is perfect. Then $M = U/V$ is T-equivariantly k-isomorphic, as a variety, to its tangent space $T(M)_0$ at the origin, and U is T- and V-equivariantly* *isomorphic, as a variety, to $U/V\times V$. In particular M is k-isomorphic to an affine space.*

In this proof, $\cong$ stands for T-equivariant k-isomorphism of varieties. Moreover, if B is a k-subgroup of U stable under T, and A a k-variety on which T operates k-morphically, then $U\cong_{(B)}A\times B$ means that U is T- and B-equivariantly k-isomorphic to $A\times B$. This is equivalent to the existence of a T-equivariant k-cross-section $s: U/B\to U$, and furthermore, in this case, $A\cong U/B$ (see 9.6).

The proof is by induction on $\dim U$ and, for fixed U, by induction on $\dim U/V$. We distinguish several cases.

(a) There exists a connected k-subgroup N of U, stable under T, containing V, and distinct from U and V.

By induction

$$U\cong_{(N)}U/N\times N,\quad N\cong_{(V)}N/V\times V \tag{1}$$

hence

$$U\cong_{(V)}U/N\times N/V\times V\,. \tag{2}$$

By 9.6, this implies

$$U/V\cong U/N\times N/V \tag{3}$$

hence

$$U\cong_{(V)}U/V\times V\,. \tag{4}$$

By induction

$$T(U/N)_0\cong U/N,\quad T(N/V)_0\cong N/V\,. \tag{5}$$

By full reducibility

$$T(U/V)_0\cong T(U/N)_0\times T(N/V)_0\,. \tag{6}$$

The equality

$$T(U/V)_0\cong U/V$$

follows then from (3), (5), (6).

From now on, we assume that we are not in case (a). Let W be a non-trivial connected central k-subgroup of U, of exponent p, stable under T, minimal for these properties.

(b) Assume $W\subset V$, and W to be T-equivariantly k-isomorphic to a vector group on which T acts linearly. There exist then T-equivariant k-cross-sections

$$s_1\colon U/V \to U/W, \quad s_2\colon U/W \to U$$

as follows from the induction assumption for s_1, from 9.5 for s_2. But then, $s_2 \circ s_1$ is a T-equivariant k-cross-section for the fibration of U by V, hence (9.6):

$$U \cong_{(V)} U/V \times V .$$

Since

$$U/V \cong (U/W)/(V/W) ,$$

the equality

$$T(U/V)_0 \cong U/V ,$$

also follows by induction.

(c) $W \subset V$, $W \not\subset Z(T)$. By the minimality assumption on W, and 9.12, we have $W \cong \mathfrak{W}$, hence we are back to case (b).

(d) $W \subset Z(T)$, k is perfect. Then W is k-isomorphic to a vector group, and we are back to case (b).

(e) $W \subset Z(T)$, k is infinite. Let $Z = Z(T) \cap U$. This group is contained in V. By [3, 11.1, p. 131], it is defined over k and

$$(7) \qquad U \cong_{(Z)} U/Z \times Z, \quad V \cong_{(Z)} V/Z \times Z .$$

(The T-equivariance is clear from the construction.) Let then $s_1\colon U/Z \to U$ be a T-equivariant k-cross-section, and $t_1\colon U/W \to U/Z$ the natural projection. By induction, there exists a T-equivariant k-cross-secion

$$s_2\colon U/V \cong (U/W)/(V/W) \to U/W .$$

It is then readily checked that

$$(8) \qquad s_1 \circ t_1 \circ s_2\colon U/V \to U$$

is a T-equivariant k-cross-section, whence

$$U \cong_{(V)} U/V \times V .$$

The equality

$$T(U/V)_0 \cong U/V$$

follows from $U/V \cong (U/W)/(V/W)$ and induction.

(f) $W \not\subset V$. Since case (a) is excluded, we have then $U = W \cdot V$. In particular, V is normal in U, and the last non-trivial term V of the descending central series of V is also central in U. Let W' be a non-trivial connected k-subgroup of V', stable under T, minimal for these properties. Then, we are reduced to one of the cases (b), (c), (d), (e) (with W' playing the role of W there).

As an application of 9.13, we deduce a sharpening of 7.9 for solvable groups, due to Grothendieck in the case of $\mathscr{T}$ ([12], Exp. XVI, Cor. 6.2, p. 41):

9.14. COROLLARY. *Let G be solvable. Then the (G, k)-varieties of maximal tori $\mathscr{T}$ and of subgroups of type* (C) *C of G are k-isomorphic to affine spaces.*

We may assume G to be connected. Let T be a maximal torus of G defined over k (7.10), and $\mathfrak{t}$ its Lie algebra. We know that $N(T) = Z(T)$ and $N(\mathfrak{t}) = Z(\mathfrak{t})$ are connected (4.8, and [1], Prop. 10.1, 13.2), and defined over k (4.3, 4.6). Therefore $\mathscr{T}$ and C are k-isomorphic to $G/Z(T)$ and $G/Z(\mathfrak{t})$, respectively. By 9.7, there is a connected normal k-subgroup M of G, contained in the unipotent radical U of G, such that $G = Z(T) \cdot M$. *A fortiori*, we have $G = Z(\mathfrak{t}) \cdot M$. We claim that M intersects $Z(T)$ and $Z(\mathfrak{t})$ transversally. We have

$$\dim(Z(T) \cap M) + \dim(G/M) = \dim Z(T),$$

hence

$$\dim(Z(T) \cap M) = \dim M + \dim Z(T) - \dim G,$$

and similarly

$$\dim(Z(\mathfrak{t}) \cap M) = \dim Z(\mathfrak{t}) + \dim M - \dim G,$$

which shows that these intersections are proper. It suffices to check that the Lie algebra $\mathfrak{m}$ of M is transversal to those of $Z(T)$ and of $Z(\mathfrak{t})$. The latter are the centralizer of T and of $\mathfrak{t}$ in $\mathfrak{g}$ (4.3, 4.6). The transversality follows then from the full reducibility of $\mathrm{Ad}_{\mathfrak{g}} T$ and the fact that $\mathfrak{m}$ contains all eigenvectors of T corresponding to non-trivial characters (9.7). The natural bijective k-morphisms $M/(Z(T) \cap M) \rightarrow G/Z(T)$ and $M/(Z(\mathfrak{t}) \cap M) \rightarrow G/Z(\mathfrak{t})$ are then separable, and therefore are k-isomorphisms. Our assertion now follows from 9.13.

9.15. LEMMA. *Let U be a connected unipotent k-group, T a k-torus which acts k-morphically on U, and N a connected normal k-subgroup of*

U, stable under T, such that T has no fixed point $\neq e$ in $U' = U/N$. Let Φ and Ψ be the sets of weights of T in N and U', respectively.

(i) *Assume Φ not to contain any linear combination with strictly positive integral coefficients of elements of Ψ. Then any T-equivariant k-cross-section $s\colon U' \to U$ is a group homomorphism. The extension of U' by N splits T-equivariantly over k.*

(ii) *If Φ does not contain any element of the form $(p^i + p^j)\cdot a$ $(a \in \Psi;$ $i,j \geqq 0)$, N is central and U/N is commutative, then U is commutative.*

(i) Let $f\colon U' \times U' \to N$ be defined by

$$f(x,y) = s(x\cdot y)\cdot s(y)^{-1}\cdot s(x)^{-1}, \qquad (x,y \in U').$$

We have to prove that $f(x,y) = e$ for all $x,y \in U'$. The map f is clearly T-equivariant. Over $\bar{k}$, U' and N are T-equivariantly isomorphic to their Lie algebras (9.12). Hence, f yields a T-equivariant morphism of varieties:

$$F\colon \mathfrak{u}' \times \mathfrak{u}' \to \mathfrak{n}.$$

It suffices to show that any such F is the zero map. Take coordinates in $\mathfrak{u}'$ and $\mathfrak{n}$ with respect to bases formed by eigenvectors of T. Then the coordinates F_i of $F(X,Y)$, $(X,Y \in \mathfrak{u}')$ are polynomials in the coordinates (X_i) and (Y_i) of X and Y which satisfy relations of the form

$$F_i(t^{a_1}\cdot x_1,\cdots,t^{a_m}X_m;\ t^{a_1}\cdot Y_1,\cdots,t^{a_m}Y_m) = t^{b_i}\cdot F_i(X_1,\cdots,X_m;\ Y_1,\cdots,Y_m).$$

$(t \in T,\ \Psi = \{a_1,\cdots,a_m\},\ b_i \in \Phi,\ X_1,\cdots,X_m,\ Y_1,\cdots,Y_m \in \bar{k})$. *If* $F_i \not\equiv 0$, this implies that b_i is a linear combination with positive, not all zero, integral coefficients, which contradicts the assumpton made on Φ and Ψ. Hence $F \equiv 0$, which proves the first part of (i). The second part then follows from the existence of a T-equivariant k-cross-section (9.6).

(ii) By ([10], Exp. 9, lemme 2, p. 1), we may find composition series

$$U = U_m \supset U_{m-1} \supset \cdots \supset U_0 = N,\quad N = N_0 \supset N_1 \supset \cdots N_q = \{e\},$$

of connected subgroups stable under T, such that the successive quotients are isomorphic to $\boldsymbol{G}_a$. The set of weights of T in U_i/N is then a subset of Ψ.

We prove by induction on i that U_i is central in U. This being true for $i = 0$, we may assume U_{m-1} to be in the center of U. The commutator map $(x,y) \mapsto x\cdot y\cdot x^{-1}\cdot y^{-1}$ induces then a T-equivariant morphism α of varieties of $U/U_{m-1} \times U/U_{m-1}$ into N. Using elementary facts on commutators, we check immediately that the restriction of α to $U/U_{m-1} \times \{y\}$ or to

$\{x\}\times U/U_{m-1}$ is a group homomorphism. Assume that $\operatorname{Im}\alpha\subset N_j$. We want to prove that $\operatorname{Im}\alpha\subset N_{j+1}$. The map α defines a T-equivariant morphism of varieties $\beta\colon U/U_{m-1}\times U/U_{m-1}\rightarrow N_j/N_{j+1}$ which is a group homomorphism if one of the two variables is left fixed. Identify U/U_{m-1} and N_j/N_{j+1} to $\boldsymbol{G}_a$. Then β is given by a polynomial $F\in\bar{k}[X,Y]$ which verifies the conditions

$$(1)\qquad F(X+X',Y)=F(X,Y)+F(X',Y),\qquad (X,Y',Y\in\boldsymbol{G}_a),$$

$$(2)\qquad F(X,Y+Y')=F(X,Y)+F(X,Y'),\qquad (X,Y,Y'\in\boldsymbol{G}_a),$$

and

$$(3)\qquad F(t^bX,t^bY)=t^aF(X,Y),\qquad (X,Y\in\boldsymbol{G}_a,\ t\in T)$$

for some $a\in\Phi$, $b\in\Psi$. (1) and (2) show that F is a linear combination of monomials $X^{p^i}\cdot Y^{p^j}$ $(i,j\geqq 0)$. Then, if $F\neq 0$, (3) implies that a is of the from $(p^i+p^j)\cdot b$ $(i,j\geqq 0)$ which contradicts the assumption made in (ii). Hence $F=0$. By induction on j, this shows that $(U,U)=\{e\}$.

9.16. THEOREM. *Assume that the unipotent radical U of G is defined over k or that G is solvable. Let S be a k-torus in G, b a non-trivial character of S, and X a nilpotent non-zero element of $\mathfrak{g}(k)$ such that* $\operatorname{Ad}s(X)=s^b\cdot X$ $(s\in S)$.

(i) *X is tangent to a unipotent k-subgroup V of G, stable under S, in which the weights of S are non-zero multiples of b;*

(ii) *if $\Phi(S,G)$ dose not contain any element of the form $(p^i+p^j)\cdot b$ $(i,j\geqq 0)$, V may be chosen to be commutative and so that the weights of S in V are p-power multiples of b;*

(iii) *if $\Phi(S,G)$ does not contain any element of the form $p^i\cdot b$ $(i\geqq 1)$ or $(p^i+p^j)\cdot b$ $(i,j\geqq 0)$, V may be chosen to be one-dimensional, k-isomorphic to $\boldsymbol{G}_a$.*

The proof proceeds by induction on $\dim G$. We distinguish three cases:

(a) G is solvable. Exactly as in 9.8 (a), we first reduce the proof to the case where S is one-dimensional, maximal, k-split, and U is defined over k. Let N be a non-trivial connected central k-subgroup of U, stable under S, and minimal for these properties. If $X\in\mathfrak{n}$, our assertion follows from 9.8. If not, applying induction to G/N, we may assume that the weights of S in U/N are non-zero multiples of b in case (i), p-power multiples of b in case (ii) and that U/N is k-isomorphic to $\boldsymbol{G}_a$ in case (iii). By 9.7, $Z(S)\cap N$ is a direct factor over k, in N. In view of the minimality assumption on N, we have either $Z(S)\supset N$ or $Z(S)\cap N=\{e\}$. If $Z(S)\supset N$, then $N=Z(S)\cap U$ and

9.15 (i) shows that U is the direct product of N and of a k-subgroup M, stable under S. Clearly $X \in \mathfrak{m}$, so that we may apply induction. Assume now $Z(S) \cap N = \{e\}$. Then, since N is minimal, 9.8 shows that N is k-isomorphic to $\boldsymbol{G}_a$. Let c be the weight of S in N. We consider the three cases of the theorem separately.

(i) If c is a multiple of b, we are done. If not, then (9.15) U is k-isomorphic to $U/N \times N$ and we may apply induction.

(ii) By 9.15 (ii), U is commutative. If c is a p-power multiple of b, there is nothing more to prove, so assume it is not. Let $d = p^s \cdot b$ be the greatest p-power multiple of b occurring among the weights of S in U, and let Y be an eigenvector of T in $\mathfrak{u}$ with weight d. By 9.8, Y is tangent to a one-dimensional k-subgroup P, stable under S and k-isomorphic to $\boldsymbol{G}_a$. If $k \cdot X = k \cdot Y$, we are done; if not, we apply the induction assumption to U/P.

(iii) By (ii) and the assumption, V may be chosen so that S has only the weight b in V. Then (iii) follows from 9.8.

(b) G is reductive. Let $L = (\ker b)^0$. It is a connected k-torus; $Z(L)$ is connected, defined over k (4.6), and reductive ([3], 2.15 (d), p. 70). The element X belongs to the Lie algebra of $Z(L)$. If $L \neq \{e\}$, the result follows, using induction on $Z(L)/L$, and (a). Thus we may again assume S to be one-dimensional, k-split. Choose a maximal k-split torus T of G containing S and defined over k. Fix an ordering on $X^*(T)$ compatible with the ordering of $X^*(S)$ such that $b > 0$ ([3], 3.1, p. 71). Standard facts about parabolic subgroups ([3], 5.12, p. 99) show that X belongs to the Lie algebra of the unipotent radical $R_u(P)$ of the minimal parabolic k-group P containing $Z(T)$ and associated to the given ordering. Since $R_u(P)$ is defined over k ([3], 3.14, p. 80), we are back to case (a).

(c) G is neither solvable nor reductive. If $X \in \mathfrak{u}$, we may apply (a) to $S \cdot U$. If not, we apply (b) to the image of X in the Lie algebra of G/U, under the canonical projection, and get a suitable k-unipotent subgroup V' to which $d\pi(X)$ is tangent. Then we apply (a) to $S \cdot \pi^{-1}(V')$.

REFERENCES

[1] A. BOREL, Groupes linéaires algébriques, Ann. of Math. (2) 64(1956), 20-82.

[2] A. BOREL ET J.-P. SERRE, Théorèmes de finitude en cohomologie galoisienne, Comm. Math. Helv., 39(1964), 111-164.

[3] A. BOREL ET J. TITS, Groupes réductifs, Publ. Math. I. H. E. S., no. 27(1965), 55-150.

[4] A. BOREL AND T. A. SPRINGER, Rationality properties of linear algebraic groups, Proc. Symp. Pure Math., vol. IX(1966), 26-32.

[5] H. CARTAN AND S. EILENBERG, Homological Algebra, Princeton University Press, 1956.

[6] P. CARTIER, Questions de rationalité des diviseurs en géométrie algébrique, Bull. Soc. Math., 86(1958), 177-251.

[7] P. CARTIER, Isogénies des variétés de groupes, Bull. Soc. Math., 87(1959), 191-220.

[8] C. CHEVALLEY, Théorie des groupes de Lie, Tome II, Act. Sci. Ind., no. 1151, Hermann, Paris, 1951.

[9] C. Chevalley, On algebraic group varieties, J. Math. Soc. Japan, 6(1954), 303-324.

[10] C. Chevalley, Séminaire sur la classification des groupes de Lie algébriques, 2 vol., Paris, 1958.

[11] C. Chevalley, Fondements de la géométrie algébrique, Paris, 1958.

[12] M. Demazure et A. Grothendieck, Schémas en groupes, I. H. E. S., 1964.

[13] J. Dieudonné, Sur les groupes de Lie algébriques sur un corps de caractéristique $p > 0$, Rend. Cir. Mat. Palermo (2), 1(1953), 380-402.

[14] A. Grothendieck et J. Dieudonné, Eléments de géométrie algébrique, III, Publ. Math. I. H. E. S., 11(1961).

[15] J. E. Humphreys, Algebraic groups and modular Lie algebras, Memoirs AMS, 71(1967), 76 p.

[16] S. Lang, Algebraic groups over finite fields, Amer. J. Math., 78(1956), 555-563.

[17] M. Rosenlicht, Some rationality questions on algebraic groups, Annali di Mat. (IV), 43(1957), 25-50.

[18] M. Rosenlicht, Extensions of vector groups by abelian varieties, Amer. J. Math., 80 (1958), 685-714.

[19] M. Rosenlicht, On quotient varieties and the affine embedding of certain homogeneous spaces, Trans. Amer. Math. Soc., 101(1961), 211-223.

[20] M. Rosenlicht, Questions of rationality for solvable algebraic groups over nonperfect fields, Annali di Mat. (IV), 61(1963), 97-120.

[21] J.-P. Serre, Quelques propriétés des variétés abéliennes en caractéristique p, Amer. J. Math., 80(1958), 715-739.

[22] J.-P. Serre, Groupes algébriques et corps de classes, Act. Sci. Ind., no. 1264, Hermann, Paris, 1959.

[23] J.-P. Serre, Cohomologie Galoisienne des groupes algébriques linéaires, Colloque sur la Théorie des groupes algébriques, Bruxelles, 1962, 53-67.

[24] J.-P. Serre, Cohomologie Galoisienne, Lecture Notes in mathematics, no. 5, Springer-Verlag, 1964.

[25] R. Steinberg, Regular elements of semisimple algebraic groups, Publ. Math. I. H. E. S., no. 25(1965), 49-80.

[26] J. Tits, Classification of algebraic semisimple groups, Proc. Symp. Pure Math., vol. IX (1966), 33-62.

[27] A. Weil, Foundations of algebraic geometry, Amer. Math. Soc. Colloq. Publ., vol. XXIX, 2nd. ed., Amer. Math. Soc., Providence, R. I. 1962.

The Institute for Advanced Study
Princeton, New Jersey, U. S. A.

and

University of Utrecht
Netherlands