PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

ROBERT STEINBERG

Regular elements of semi-simple algebraic groups

Publications mathématiques de l'I.H.É.S., tome 25 (1965), p. 49-80
<http://www.numdam.org/item?id=PMIHES_1965__25__49_0>

REGULAR ELEMENTS OF SEMISIMPLE ALGEBRAIC GROUPS

by Robert STEINBERG

§ 1. Introduction and statement of results

We assume given an algebraically closed field K which is to serve as domain of definition and universal domain for each of the algebraic groups considered below; each such group will be identified with its group of elements (rational) over K. The basic definition is as follows. An element x of a semisimple (algebraic) group (or, more generally, of a connected reductive group) G of rank r is called *regular* if the centralizer of x in G has dimension r. It should be remarked that x is not assumed to be semisimple; thus our definition is different from that of [8, p. 7-03]. It should also be remarked that, since regular elements are easily shown to exist (see, e.g., 2.11 below) and since each element of G is contained in a (Borel) subgroup whose quotient over its commutator subgroup has dimension r, a regular element is one whose centralizer has the least possible dimension, or equivalently, whose conjugacy class has the greatest possible dimension.

In the first part of the present article we obtain various criteria for regularity, study the varieties of regular and irregular elements, and in the simply connected case construct a closed irreducible cross-section N of the set of regular conjugacy classes of G. Then assuming that G is (defined) over a perfect field k and contains a Borel subgroup over k we show that N (or in some exceptional cases a suitable analogue of N) can be constructed over k, and this leads us to the solution of a number of other problems of rationality. In more detail our principal results are as follows. Until 1.9 the group G is assumed to be semisimple.

1.1. *Theorem. — An element of* G *is regular if and only if the number of Borel subgroups containing it is finite.*

1.2. *Theorem. — The map $x \to x_s$, from x to its semisimple part, induces a bijection of the set of regular classes of* G *onto the set of semisimple classes. In other words:*

a) *every semi-simple element is the semisimple part of some regular element;*

b) *two regular elements are conjugate if and only if their semisimple parts are.*

The author would like to acknowledge the benefit of correspondence with T. A. Springer on these results (cf. 3.13, 4.7 *d)* below). The special case of *a)* which asserts the existence of regular unipotent elements (all of which are conjugate by *b)*) is proved in § 4. The other parts of 1.2 and 1.1, together with the fact that the number in 1.1, if finite, always divides the order of the Weyl group of G, are proved in § 3, where other characterizations of regularity may be found (see 3.2, 3.7, 3.11, 3.12 and 3.14). This material follows a preliminary section, § 2, in which we recall some basic facts about semisimple groups and some known characterizations of regular semisimple elements (see 2.11).

1.3. *Theorem.* — a) *The irregular elements of* G *form a closed set* Q.

b) *Each irreducible component of* Q *has codimension* 3 *in* G.

c) Q *is connected unless* G *is of rank* 1, *of characteristic not* 2, *and simply connected, in which case* Q *consists of* 2 *elements.*

This is proved in § 5 where it is also shown that the number of components of Q is closely related to the number of conjugacy classes of roots under the Weyl group. An immediate consequence of 1.3 is that the regular elements form a dense open subset of G.

It may be remarked here that 1.1 to 1.3 and appropriate versions of 1.4 to 1.6 which follow hold for connected reductive groups as well as for semisimple groups, the proofs of the extensions being essentially trivial.

In § 6 the structure of the algebra of class functions (those constant on conjugacy classes) is determined (see 6.1 and 6.9). In 6.11, 6.16, and 6.17 this is applied to the study of the closure of a regular class and to the determination of a natural structure of variety for the set of regular classes, the structure of affine r-space in case G is simply connected.

1.4. *Theorem.* — *Let* T *be a maximal torus in* G *and* $\{\alpha_i \mid 1 \leq i \leq r\}$ *a system of simple roots relative to* T. *For each i let* X_i *be the one-parameter unipotent subgroup normalized by* T *according to the root* α_i *and let* σ_i *be an element of the normalizer of* T *corresponding to the reflection relative to* α_i. *Let* $N = \prod_{i=1}^{r} (X_i \sigma_i) = X_1\sigma_1 X_2\sigma_2 \dots X_r\sigma_r$. *If* G *is a simply connected group, then* N *is a cross-section of the collection of regular classes of* G.

In 7.4 an example of N is given: in case G is of type $SL(r+1)$ we obtain one of the classical normal forms under conjugacy. This special case suggests the problem of extending the normal form N from regular elements to arbitrary elements. In 7.1 it is shown that N is a closed irreducible subset of G, isomorphic as a variety to affine r-space V, and in 7.9 (this is the main lemma concerning N) that, if G is simply connected, and χ_i $(1 \leq i \leq r)$ denote the fundamental characters of G, then the map $x \rightarrow (\chi_1(x), \chi_2(x), \dots, \chi_r(x))$ induces an isomorphism of N on V. Then in § 8 the proof of 1.4 is given and simultaneously the following important criterion for regularity is obtained.

1.5. *Theorem.* — *If* G *is simply connected, the element x is regular if and only if the differentials* $d\chi_i$ *are independent at* x.

At this point some words about recent work of B. Kostant are in order. In [3] and [4] he has proved, among other things, the analogues of our above discussed results that are obtained by replacing the semisimple group G by a semisimple Lie algebra L over the complex field (any algebraically closed field of characteristic 0 will serve as well) and the characters χ_i of G by the basic polynomial invariants u_i of L. The χ_i turn out to be considerably more tractable than the u_i. Thus the proofs for G with no restriction on the characteristic are simpler than those for L in characteristic 0. Assuming both G and L are in characteristic 0, substantial parts of 1.1, 1.2, and 1.3 can be derived from their analogues for L, but there does not seem to be any simple way of relating 1.4 and 1.5 to their analogues for L.

We now introduce a perfect subfield k of K, although it appears from recent results of A. Grothendieck on semisimple groups over arbitrary fields that the assumption of perfectness is unnecessary for most of what follows.

1.6. *Theorem. — Let* G *be over* k, *and assume either that* G *splits over* k *or that* G *contains a Borel subgroup over* k *but no component of type* A_n *(*n *even). Then the set* N *of* 1.4 *can be constructed over* k *(by appropriate choice of* T, σ_i, *etc.).*

Together with 1.4 this implies that if G is simply connected in 1.6 the natural map from the set of regular elements over k to the set of regular classes over k is surjective. For a group of type A_n (n even) we have a substitute (see 9.7) for 1.6 which enables us to show:

1.7. *Theorem. — Assume that* G *is simply connected and over* k *and that* G *contains a Borel subgroup over* k. *Then the natural map from the set of semisimple elements over* k *to the set of semisimple classes over* k *is surjective. In other words, each semisimple class over* k *contains an element over* k.

Theorems 1.6 and 1.7 are proved in § 9 where it is also shown (see 9.1 and 9.10) that the assumption that G contains a Borel subgroup over k is essential.

1.8. *Theorem. — Under the assumptions of* 1.7 *each element of the cohomology set* $H^1(k, G)$ *can be represented by a cocycle whose values are in a torus over* k.

In § 10 this result is deduced from 1.7 by a method of proof due to M. Kneser, who has also proved 1.7 in a number of special cases and has formulated the general case as a conjecture. In 9.9 and 10.1 it is shown that 1.7 and 1.8 hold for arbitrary simply connected, connected linear groups, not just for semisimple ones.

In § 10 it is indicated how Theorem 1.8 provides the final step in the proof of the following result, 1.9, the earlier steps being due to J.-P. Serre and T. A. Springer (see [12], [13] and [15]). We observe that G is no longer assumed to be semisimple, and recall [12, p. 56-57] that (cohomological) dim $k \leq 1$ means that every finite-dimensional division algebra over k is commutative.

1.9. *Theorem. — Let* k *be a perfect field. If* a) dim $k \leq 1$, *then* b) $H^1(k, G) = 0$ *for every connected linear group* G *over* k, *and* c) *every homogeneous space* S *over* k *for every connected linear group* G *over* k *contains a point over* k.

The two parts of 1.9 are the conjectures I and I' of Serre [12]. Conversely *b)* implies *a)* by [12, p. 58], and is the special case of *c)* in which only principal homogeneous spaces are considered; thus *a)*, *b)* and *c)* are equivalent. They are also equivalent to: every connected linear group over k contains a Borel subgroup over k [15, p. 129].

After some consequences of 1.9, of which only the following (cf. 1.7) will be stated here, the paper comes to a close.

1.10. *Theorem. — Let k be a perfect field such that* $\dim k \leq 1$ *and* G *a connected linear group over k. Then every conjugacy class over k contains an element over k.*

After the remark that Kneser, using extensions of 1.8, has recently shown (cf. 1.9) that $H^1(k, G) = 0$ if k is a p-adic field and G a simply connected semisimple group over k, this introduction comes to a close.

§ 2. Some recollections

In this section we recall some known facts, including some characterizations 2.11 of regular semisimple elements, and establish some notations which are frequently used in the paper. If k is a field, k^* is its multiplicative group. The term " algebraic group " is often abbreviated to " group ". If G is a group, G_0 denotes its identity component. If x is an element of G, then G_x denotes the centralizer of x in G, and x_s and x_u denote the semisimple and unipotent parts of x when G is linear. Assume now that G is a semisimple group, that is, G is a connected linear group with no nontrivial connected solvable normal subgroup. We write r for the rank of G. Assume further that T is a maximal torus in G and that an ordering of the (discrete) character group of T has been chosen. We write Σ for the system of roots relative to T and X_α for the subgroup corresponding to the root α.

2.1. X_α *is unipotent and isomorphic (as an algebraic group) to the additive group (of* K*). If x_α is an isomorphism from* K *to* X_α, *then* $tx_\alpha(c)t^{-1} = x_\alpha(\alpha(t)c)$ *for all α and c.*

For the proof of 2.1 to 2.6 as well as the other standard facts about linear groups, the reader is referred to [8].

We write U (resp. U^-) for the group generated by those X_α for which α is positive (resp. negative), and B for the group generated by T and U.

2.2. a) U *is a maximal unipotent subgroup of* G, *and* B *is a Borel (maximal connected solvable) subgroup.*

b) *The natural maps from the Cartesian product* $\prod_{\alpha>0} X_\alpha$ *(fixed but arbitrary order of the factors) to* U *and from* $T \times U$ *to* B *are isomorphisms of varieties.*

In *b)* the X_α component of an element of U may change with the order, but not if α is simple.

2.3. *The natural map from* $U^- \times T \times U$ *to* G *is an isomorphism onto an open subvariety of* G.

We write W for the Weyl group of G, that is, the quotient of T in its normalizer. W acts on T, via conjugation, hence also on the character group of T and on Σ. For each w in W we write σ_w for an element of the normalizer of T which represents w.

2.4. a) *The elements* σ_w $(w \in W)$ *form a system of representatives of the double cosets of* G *relative to* B.

b) *Each element of* $B\sigma_w B$ *can be written uniquely* $u\sigma_w b$ *with u in* $U \cap \sigma_w U^- \sigma^{-1}$ *and b in* B.

The simple roots are denoted α_i $(1 \leq i \leq r)$. If $\alpha = \alpha_i$ we write X_i, x_i for X_α, x_α, and G_i for the group (semisimple of rank 1) generated by X_α and $X_{-\alpha}$. The reflection in W corresponding to α_i is denoted w_i. If $w = w_i$ we write σ_i in place of σ_w.

2.5. *The element* σ_i *can be chosen in* G_i. *If this is done, and* $B_i = B \cap G_i = (T \cap G_i)X_i$, *then* G_i *is the disjoint union of* B_i *and* $X_i \sigma_i B_i$.

The following may be taken as a definition of the term " simply connected ".

2.6. *The semisimple group* G *is simply connected if and only if there exists a basis* $\{\omega_j\}$ *of the dual (character group) of* T *such that* $w_i \omega_j = \omega_j - \delta_{ij} \alpha_i$ *(Kronecker delta,* $1 \leq i, j \leq r$*).*

An arbitrary connected linear group is simply connected if its quotient over its radical satisfies 2.6. If G is as in 2.6 we write χ_i for the i^{th} fundamental character of G, that is, for the trace of the irreducible representation whose highest weight on T is ω_i.

2.7. *Let* G *be a semisimple group of rank* r *and* x *a semisimple element of* G.

a) G_{x0} *is a connected reductive group of rank* r. *In other words,* $G_{x0} = G'T'$ *with* G' *a semisimple group,* T' *a central torus in* G_{x0}, *the intersection* $G' \cap T'$ *finite, and* $\operatorname{rank} G' + \operatorname{rank} T' = r$. *Further* G' *and* T' *are uniquely determined as the commutator subgroup and the identity component of the centre of* G_{x0}.

b) *The unipotent elements of* G_x *are all in* G'.

Part *b)* follows from *a)* because G_{x0} contains the unipotent elements of G_x by [8, p. 6-15, Cor. 2]. For the proof of *a)* we may imbed x in a maximal torus T and use the above notation. If y in G_x is written $y = u\sigma_w b$ as in 2.4 then the uniqueness in 2.4 implies that u, σ_w and b are in G_x. By 2.1 and 2.2 we get:

2.8. G_x *is generated by* T, *those* X_α *for which* $\alpha(x) = 1$, *and those* σ_w *for which* $wx = x$.

Then G_{x0} is generated by T and the X_α alone because the group so generated is connected and of finite index in G_x (see [8, p. 3-01, Th. 1]). Let G' be the group generated by the X_α alone, and let T' be the identity component of the intersection of the kernels of the roots α such that $\alpha(x) = 1$. Then G' is semisimple by [8, p. 17-02, Th. 1], and the other assertions of *a)* are soon verified.

2.9. *Corollary.* — *In* 2.7 *every maximal torus containing* x *also contains* T'.

For in the above proof T was chosen as an arbitrary torus containing x.

2.10. *Remark.* — That G_x in 2.7 need not be connected, even if x is regular, is shown by the example: $G = PSL(2)$, $x = \operatorname{diag}(i, -i)$, $i^2 = -1$. If G is simply connected, however, G_x is necessarily connected and in 2.8 the elements σ_w may be omitted. More generally, the group of fixed points of a semisimple automorphism of a semisimple group G is reductive, and if the automorphism fixes no nontrivial point of the fundamental group of G, it is connected. (The proofs of these statements are forthcoming.)

2.11. *Let* G *and* x *be as in* 2.7. *The following conditions are equivalent:*

a) x *is regular.*

b) G_{x0} *is a maximal torus in* G.

c) x *is contained in a unique maximal torus* T *in* G.

d) G_x *consists of semisimple elements.*

e) *If* T *is a maximal torus containing* x *then* $\alpha(x) \neq 1$ *for every root* α *relative to* T.

G_{x0} contains every torus which contains x. Thus *a)* and *b)* are equivalent and *b)* implies *c)*. If *c)* holds, G_x normalizes T, whence G_x/T is finite and $G_{x0}=T$, which is *b)*. By 2.7 *b)*, *b)* implies *d)*, which in turn, by 2.1, implies *e)*. Finally *e)* implies, by 2.8, that G_x/T is finite, whence *b)*.

2.12. *Lemma. — Let* $B'=T'U'$ *with* B' *a connected solvable group,* T' *a maximal torus, and* U' *the maximal unipotent subgroup. If* t *and* u *are elements of* T' *and* U', *there exists* u' *in* U' *such that* tu' *is conjugate to* tu *via an element of* U', *and* u' *commutes with* t.

For the semisimple part of tu is conjugate, under U', to an element of T' by [8, p. 6-07], an element which must be t itself because U' is normal in B'.

2.13. *Corollary. — In the semisimple group* G *assume that* t *is a regular element of* T *and* u *an arbitrary element of* U. *Then* tu *is a regular element, in fact is conjugate to* t.

By 2.12 we may assume that u commutes with t, in which case $u=1$ by 2.1 and 2.2 *b)*.

2.14. *The regular semisimple elements form a dense open set* S *in* G.

By 2.12, 2.13 and 2.11 (see *a)* and *e)*), $S\cap B$ is dense and open in B. Since the conjugates of B cover G by [8, p. 6-13, Th. 5], S is dense in G. Let A be the complement of $S\cap B$ in B, and let C be the closed set in $G/B\times G$ consisting of all pairs $(\overline{x},y)$ (here $\overline{x}$ denotes the coset xB) such that $x^{-1}yx\in A$. The first factor, G/B, is complete by [8, p. 6-09, Th. 4]. By a characteristic property of completeness, the projection on the second factor is closed. The complement, S, is thus open.

We will call an element of G *strongly regular* if its centralizer is a maximal torus. Such an element is regular and semisimple, the converse being true if G is simply connected by 2.10.

2.15. *The strongly regular elements form a dense open set in* G.

The strongly regular elements form a dense open set in T, characterized by $\alpha(t)\neq 1$ for all roots α, and $wt\neq t$ for all $w\neq 1$ in W. Thus the proof of 2.14 may be applied.

§ 3. Some characterizations of regular elements

Throughout this section and the next G denotes a semisimple group. Our aim is to prove 1.1 and 1.2 (of § 1). The case of unipotent elements will be considered first. The following critical result is proved in § 4.

3.1. *Theorem. — There exists in* G *a regular unipotent element.*

3.2. *Lemma. — There exists in* G *a unipotent element contained in only a finite number of Borel subgroups. Indeed let* x *be a unipotent element and* n *the number of Borel subgroups containing it. Then the following are equivalent:*

a) n *is finite.*

b) n *is* 1.

c) *If* x *is imbedded in a maximal unipotent subgroup* U *and the notation of* § 2 *is used, then for* $1\leq i\leq r$ *the* X_i *component of* x *is different from* 1.

Let T be a maximal torus which normalizes U, let $B=TU$, and let B′ be an arbitrary Borel subgroup. By the conjugacy theorem for Borel subgroups and 2.4 we have $B'=u\sigma_w B\sigma_w^{-1}u^{-1}$ with u and σ_w as in 2.4 *b)*. If *c)* holds and B′ contains x, then B contains $\sigma_w^{-1}u^{-1}xu\sigma_w$ and every X_i component of $u^{-1}xu$ is different from 1. Thus $w\alpha_i$ is positive for every simple root α_i and w is 1, whence $B'=B$ and *b)* holds. If *c)* fails, then for some i the Borel subgroups $u\sigma_i B\sigma_i^{-1}u^{-1}$ $(u\in X_i)$ all contain x, whence *a)* fails. Thus *a)*, *b)* and *c)* are equivalent. Since elements which satisfy *c)* exist in abundance, the first statement in 3.2 follows.

3.3. *Theorem. — For a unipotent element x of* G *the following are equivalent:*

a) *x is regular.*

b) *The number of Borel subgroups containing x is finite.*

Further the unipotent elements which satisfy a) *and* b) *form a single conjugacy class.*

Let y and z be arbitrary unipotent elements which satisfy *a)* and *b)*, respectively. Such elements exist by 3.1 and 3.2. We will prove all assertions of 3.3 together by showing that y is conjugate to z. By replacing y and z by conjugates we may assume they are both in the group U of § 2 and use the notations there. Let y_i and z_i denote the X_i components of y and z. By 3.2 every z_i is different from 1. We assert that every y_i is also different from 1. Assume the contrary, that $y_i=1$ for some i, and let U_i be the subgroup of elements of U whose X_i components are 1. Then y is in U_i, so that in the normalizer $P_i=G_iTU_i$ of U_i we have $\dim(P_i)_y=\dim P_i-\dim(\text{class of } y)\geq \dim P_i-\dim U_i=r+2$. This contradiction to the regularity of y proves our assertion. Hence by conjugating y by an element of T we may achieve the situation: $y_i=z_i$ for all i, or, in other words, zy^{-1} is in U′, the intersection of all U_i. Now the set $\{uyu^{-1}y^{-1}\mid u\in U\}$ is closed (by [7] every conjugacy class of U is closed). Its codimension in U is at most r because y is regular, whence its codimension in U′ is at most $r-(\dim U-\dim U')=0$. The set thus coincides with U′. For some u in U we therefore have $uyu^{-1}y^{-1}=zy^{-1}$, whence $uyu^{-1}=z$, and 3.3 is proved.

In the course of the argument the following result has been proved.

3.4. *Corollary. — If x is unipotent and irregular, then* $\dim G_x\geq r+2$.

If P_i is replaced by B in the above argument, the result is:

3.5. *Corollary. — If x is unipotent and irregular and* B *is any Borel subgroup containing x, then* $\dim B_x\geq r+1$.

3.6. *Lemma. — Let x be an element of* G, *and y and z its semisimple and unipotent parts. Let* $G_{y0}=G'T'$ *with* G′ *and* T′ *as in* 2.7, *and let r' be the rank of* G′. *Let* S (*resp.* S′) *be the set of Borel subgroups of* G (*resp.* G′) *containing x* (*resp.* z):

a) $\dim G_x=\dim G'_z+r-r'$.

b) *If* B *in* S *contains* B′ *in* S′ *then* $\dim B_x=\dim B'_z+r-r'$.

c) *Each element* B *of* S *contains a unique element of* S′, *namely,* $B\cap G'$.

d) *Each element of* S′ *is contained in at least one but at most a finite number of elements of* S.

We have $G_x = (G_y)_z$ by [8, p. 4-08]. Thus $\dim G_x = \dim G'_z + \dim T'$, whence *a)*. Part *b)* may be proved in the same way, once it is observed that $B_y = B'T'$. For B_y is solvable, connected by [8, p. 6-09], and contains the Borel subgroup $B'T'$ of G_y. Let B be in S. Let T be a maximal torus in B containing y, and let the roots relative to T be ordered so that B corresponds to the set of positive roots. The group G' is generated by those X_α for which $\alpha(y) = 1$, and the corresponding α form a root system Σ' for G' by [8, p. 17-02, Th. 1]. By 2.2 *a)* the groups $T \cap G'$ and X_α $(\alpha > 0, \alpha \in \Sigma')$ generate a Borel subgroup of G' which is easily seen to be none other than $B \cap G'$ (by 2.1 and 2.2 *b)*), whence *c)* follows. Let B' be in S'. Then a Borel subgroup B of G contains B' and is in S if and only if it contains $B'T'$. For if B contains x, it also contains y, then a maximal torus containing y by [8, p. 6-13], then T' by 2.9; while if B contains the Borel subgroup $B'T'$ of G_{y0}, it contains the central element y by [8, p. 6-15], thus also x. The number of possibilities for B above is at least 1 because $B'T'$ is a connected solvable group, but it is at most the order of the Weyl group of G because $B'T'$ contains a maximal torus of G (this last step is proved in [8, p. 9-05, Cor. 3], and also follows from 2.4).

3.7. *Corollary. — In* 3.6 *the element x is regular in* G *if and only if z is regular in* G', *and the set* S *is finite if and only if* S' *is.*

The first assertion follows from 3.6 *a)*, the second from *c)* and *d)*.

3.8. *Corollary. — In* 3.6 *the element x is regular in* G *if and only if the set* S *is finite.*

Observe that this is Theorem 1.1 of § 1. It follows from 3.7 and 3.3 (applied to z).

3.9. *Corollary. — The assertions* 3.4 *and* 3.5 *are true without the assumption that x is unipotent.*

For the first part we use 3.6 *a)*, for the second *b)* and *c)*.

3.10. *Conjecture. — For any x in* G *the number* $\dim G_x - r$ *is even.*

It would suffice to prove this when x is unipotent. The corresponding result for Lie algebras over the complex field is a simple consequence of the fact that the rank of a skew symmetric matrix is always even (see [4, p. 364, Prop. 15]).

3.11. *Corollary. — If x is an element of* G, *the following are equivalent.*

a) $\dim G_x = r$, *that is, x is regular.*

b) $\dim B_x = r$ *for every Borel subgroup* B *containing x.*

c) $\dim B_x = r$ *for some Borel subgroup* B *containing x.*

As we remarked in the first paragraph of § 1, $\dim B_x \geq r$. Thus *a)* implies *b)*. By 3.5 as extended in 3.9 we see that *c)* implies *a)*.

3.12. *Corollary. — In* 3.6 *let x be regular and n the number of Borel subgroups containing x.*

a) $n = |W|/|W'|$, *the ratio of the orders of the Weyl groups of* G *and* G'.

b) $n = 1$ *if and only if z is a regular unipotent element of* G *and y is an element of the centre.*

c) $n = |W|$ *if and only if x is a regular semisimple element of* G.

By 3.7, 3.2 and 3.3 the element z is regular and contained in a unique Borel subgroup B' of G'. Let T be a maximal torus in $B'T'$. Then n is the number of Borel subgroups of G containing B' and T. Now each of the $|W'|$ Borel subgroups of G' normalized by T (these are just the conjugates of B' under W') is contained in the same number of Borel subgroups of G containing T, and each of the $|W|$ groups of the latter type contains a unique group of the former type by 3.6 *c)*. Thus *a)* follows. Then $n=1$ if and only if $|W'|=|W|$, that is, $G'=G$, which yields *b)*; and $n=|W|$ if and only if $|W'|=1$, that is, $G'=1$ and $G_{y0}=T'$, which by 2.11 (see *a)*, *b)* and *d)*) is equivalent to y regular and $x=y$, whence *c)*.

3.13. *Remark.* — Springer has shown that if x is regular in G then G_{x0} is commutative. Quite likely the converse is true (it is for type A_r). It would yield the following characterization of the regular elements, in the abstract group, G_{ab}, underlying G. The element x of G_{ab} is regular in G if and only if G_x contains a commutative subgroup of finite index. We have the following somewhat bulkier characterization.

3.14. *Corollary.* — *The element x of G_{ab} is regular if and only if it is contained in only a finite number of subgroups each of which is maximal solvable and without proper subgroups of finite index.*

For each such subgroup is closed and connected, hence a Borel subgroup. We remark that G_{ab} determines also the sets of semisimple and unipotent elements (hence also the decomposition $x=x_s x_u$), as well as the semisimplicity, rank, dimension, and base field (to within an isomorphism), all of which would be false if G were not semisimple. If G is simple, then G_{ab} determines the topology (the collection of closed sets) in G completely, which is not always the case if G is semisimple.

To close this section we now prove Theorem 1.2. Let y be semisimple in G, and $G_{y0}=G'T'$ as in 3.6. By 3.1 there exists in G' a regular unipotent element z. Let $x=yz$. Then x is regular in G by 3.7 and $x_s=y$, whence *a)* holds. Let x and x' be regular elements of G. If x is conjugate to x', then clearly x_s is conjugate to x'_s. If x_s is conjugate to x'_s, we may assume $x_s=x'_s=y$, say. Then in G' (as above) the elements x_u and x'_u are regular by 3.7, hence conjugate by 3.3, whence x and x' are conjugate.

§ 4. The existence of regular unipotent elements

This section is devoted to the proof of 3.1. Throughout G is a semisimple group, T a maximal torus in G, and the notations of § 2 are used. In addition V denotes a real totally ordered vector space of rank r which extends the dual of T and its given ordering.

4.1. *Lemma.* — *Let the simple roots α_i be so labelled that the first q are mutually orthogonal as are the last $r-q$. Let $w=w_1 w_2 \dots w_r$.*

a) *The roots are permuted by w in r cycles.*

The space V *can be reordered so that*

b) *roots originally positive remain positive,*

and

c) *each cycle of roots under w contains exactly one relative maximum and one relative minimum.*

We observe that since the Dynkin graph has no circuits [9, p. 13-02] a labelling of the simple roots as above is always possible. In *c)* a root α is, for example, a maximum in its cycle under w if $\alpha > w\alpha$ and $\alpha > w^{-1}\alpha$ for the order on V. The proof of 4.1 depends on the following results proved in [16]. (These are not explicitly stated there, but see 3.2, 3.6, the proof of 4.2, and 6.3.)

4.2. *Lemma. — In* 4.1 *assume that* Σ *is indecomposable, that a positive definite inner product invariant under* W *is used in* V, *and that* n *denotes the order of* w.

a) *The roots of* Σ *are permuted by* w *in* r *cycles each of length* n.

If $\dim \Sigma > 1$, *there exists a plane* P *in* V *such that*

b) P *contains a vector* v *such that* $(v, \alpha) > 0$ *for every positive root* α,

and

c) w *fixes* P *and induces on* P *a rotation through the angle* $2\pi/n$.

For the proof of 4.1 we may assume that Σ is indecomposable, and, omitting a trivial case, that $\dim \Sigma > 1$. We choose P and v as in 4.2. Let α' denote the orthogonal projection on P of the root α. By 4.2 *b)* it is nonzero. Since by 4.2 *c)* the vectors $w^{-i}v$ $(1 \leq i \leq n)$ form the vertices a regular polygon, it can be arranged, by a slight change in v, that for each α these vectors make distinct angles with α'. It is then clear that there is one relative maximum and one relative minimum for the cycle of numbers $(w^{-i}v, \alpha')$. Since $(w^{-i}v, \alpha') = (w^{-i}v, \alpha) = (v, w^{i}\alpha)$, we can achieve *c)* by reordering V so that vectors v' for which $(v, v') > 0$ become positive. Then *a)* and *b)* also hold by 4.2 *a)* and 4.2 *b)*.

4.3. *Lemma. — Let* G *be simply connected, otherwise as above. Let* $\mathfrak{g}$ *be the Lie algebra of* G. *Let* $\mathfrak{t}$ *be the subalgebra corresponding to* T, *and* $\mathfrak{z}$ *the subalgebra of elements of* $\mathfrak{t}$ *which vanish at all roots on* T. *Let* w *be as in* 4.1. *Let* x *be an element of the double coset* $\mathrm{B}\sigma_w\mathrm{B}$, *and let* $\mathfrak{g}_x$ *denote the algebra of fixed points of* x *acting on* $\mathfrak{g}$ *via the adjoint representation. Then* $\dim \mathfrak{g}_x \leq \dim \mathfrak{z} + r$.

We identify $\mathfrak{g}$ with the tangent space to G at 1. Then by 2.3 we have a direct sum decomposition $\mathfrak{g} = \mathfrak{t} + \sum_{\alpha} \mathrm{K}\mathfrak{x}_\alpha$ in which $\mathrm{K}\mathfrak{x}_\alpha$ may be identified with the tangent space of X_α. We order the weights of the adjoint representation, that is, 0 and the roots, as in 4.1. By replacing x by a conjugate, we may assume $x = b\sigma_w$ $(b \in \mathrm{B})$.

1) *If* $\mathfrak{v}$ *in* $\mathfrak{g}$ *is a weight vector, then* $(1-x)\mathfrak{v} = \mathfrak{v} - c\sigma_w\mathfrak{v} +$ *terms (corresponding to weights) higher than (that of)* $\sigma_w\mathfrak{v}$ $(c \in \mathrm{K}^*)$. This follows from 7.15 *d)* below, which holds for any rational representation of G.

2) *If the root* α *is not maximal in its cycle under* w, *then* $(1-x)\mathfrak{g}$ *contains a vector of the form* $c\mathfrak{x}_\alpha +$ *higher terms* $(c \in \mathrm{K}^*)$. If $w\alpha > \alpha$ we apply 1) with $\mathfrak{v} = \mathfrak{x}_\alpha$, while if $w\alpha < \alpha$ we use $\mathfrak{v} = \sigma_w^{-1}\mathfrak{x}_\alpha$ instead.

3) *There exist* $r - \dim \mathfrak{z}$ *independent elements* $\mathfrak{t}_i$ *of* $\mathfrak{t}$ *such that for every* i *the space* $(1-x)\mathfrak{g}$ *contains a vector of the form* $\mathfrak{t}_i +$ *higher terms.* Because of 1), in which $c = 1$ if $\mathfrak{v}$ is in $\mathfrak{t}$, this follows from:

4) *The kernel of* $1 - \sigma_w$ *on* $\mathfrak{t}$ *is* $\mathfrak{z}$. Because the adjoint action of σ_w on $\mathfrak{t}$ stems from the action of w on T by conjugation, we may write w in place of σ_w, on $\mathfrak{t}$. Assume

$(1-w)\mathfrak{t}_0=0$ with $\mathfrak{t}_0$ in $\mathfrak{t}$. Then $(1-w_1)\mathfrak{t}_0=(1-w_2\ldots w_r)\mathfrak{t}_0$. If we evaluate the left side at the functions $\omega_2, \ldots, \omega_r$ of 2.6 or the right side at ω_1 then by 2.6 we always get 0, whence both sides are 0. By an obvious induction we get that $(1-w_i)\mathfrak{t}_0=0$ for all i, and on evaluation at ω_i, that $\mathfrak{t}_0(\alpha_i)=\mathfrak{t}_0((1-w_i)\omega_i)=0$. Thus $\mathfrak{t}_0$ is in $\mathfrak{z}$. One may reverse the steps to show that $\mathfrak{z}$ is contained in the kernel of $1-\sigma_w$, whence 4).

Lemma 4.3 is a consequence of 2) and 3).

4.4. *Remark.* — One can show that $\mathfrak{z}$ in 4.3 is the centre of $\mathfrak{g}$.

4.5. *Lemma.* — *Let the notation be as in* 4.1. *Let w_0 be the element of* W *which maps each positive root onto a negative one, and π the permutation defined by $-w_0\alpha_i=\alpha_{\pi i}$ $(1\leq i\leq r)$. Let σ_0 be an element of the normalizer of* T *which represents w_0. For each i let u_i be an element of $X_{\pi i}$ different from* 1 *and let $x=u_1u_2\ldots u_r$. Then $\sigma_0x\sigma_0^{-1}$ is in $B\sigma_wB$.*

We have $\sigma_0u_i\sigma_0^{-1}$ in G_i-B, hence in $B\sigma_iB$ by 2.5. Since

$$B\sigma_1\ldots\sigma_{i-1}B\sigma_iB=B\sigma_1\ldots\sigma_{i-1}X_i\sigma_iB=B\sigma_1\ldots\sigma_iB,$$

because w_i permutes the positive roots other than α_i by [8, p. 14-04, Cor. 3], and each root $w_1w_2\ldots w_{i-1}\alpha_i$ is positive (cf. 7.2 *a)*) we get 4.5.

4.6. *Theorem.* — *The element x of* 4.5 *is regular.*

By going to the simply connected covering group, we may assume that G is simply connected. For any subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ we write $\mathfrak{a}_x$ for the subalgebra of elements fixed by x. Let $\mathfrak{b}$ and $\mathfrak{u}$ denote the subalgebras corresponding to B and U. By 4.3 and 4.5 we have $\dim\mathfrak{b}_x\leq\dim\mathfrak{g}_x\leq\dim\mathfrak{z}+r$. An infinitesimal analogue of 2.1 yields $x_\alpha(c)\mathfrak{t}_0=\mathfrak{t}_0+c'c\mathfrak{t}_0(\alpha)\mathfrak{x}_\alpha$ for all $\mathfrak{t}_0$ in $\mathfrak{t}$ and some c' in K, whence $\mathfrak{t}_x$ contains $\mathfrak{z}$, and $\dim\mathfrak{b}_x\geq\dim\mathfrak{z}+\dim\mathfrak{u}_x$. Combined with the previous inequality this yields $\dim\mathfrak{u}_x\leq r$, whence $\dim U_x\leq r$. From the form of x we see that B is the unique Borel subgroup containing x. Each element of G_x normalizes B, hence belongs to B by [8, p. 9-03, Th. 1], or else by 2.4. Now if $ut\,(t\in T, u\in U)$ is in B_x then, working in B modulo the commutator subgroup of U, and using the fact that each X_i component of x is different from 1, we get $\alpha_i(t)=1$ for all i, whence t is in the centre of G, a finite group. Hence $\dim G_x=\dim U_x\leq r$, as required.

4.7. *Remarks.* — *a)* The condition $\dim U_x=r$ on x in U is not enough to make x regular, as one sees by examples in a group of type A_2. The added condition that all X_i components are different from 1 is essential.

b) If the characteristic of K is 0, or, more generally, if $\dim\mathfrak{z}\leq 1$ in 4.3, we may conclude from 4.3 and 3.4 as extended in 3.9 that all elements of $B\sigma_wB$ are regular, and then (cf. 7.3) that all elements of N in 1.4 are regular. There is, however, an exception: $\dim\mathfrak{z}=2$ if G is of type D_r (r even) and of characteristic 2. It is nevertheless true that all elements of $B\sigma_wB$ are regular (cf. 8.8). By 4.5 this implies that if x is the regular element of 4.6 and t in T is arbitrary, then tx is regular. If u is an arbitrary regular element of U, however, tu need not be regular: consider in SL(3) the superdiagonal matrix with diagonal entries $-1, 1, -1$ and superdiagonal entries all 2. In contrast if t is regular and u is arbitrary, then tu is regular by 2.13.

c) In characteristic 0 one may, in the simply connected case, imbed the element x of 4.6 in a subgroup isomorphic to SL(2) and then use the theory of the representations of this latter group to prove that x is regular. This is the method of Kostant, worked out in [3] for Lie algebras over the complex field. In the general case, however, a regular unipotent element can not be imbedded in the group SL(2), or even in the $ax+b$ group: in characteristic $p \neq 0$, a unipotent element of either of these groups has order at most p, while in a group G of type A_r, for example, a regular unipotent element has order at least $r+1$, so that if $r+1>p$ the imbedding is impossible.

d) Springer has studied U_x (x as in 4.6) by a method depending on a knowledge of the structural constants of the Lie algebra of U. His methods yield a proof of the regularity of x only if

($*$) p does not divide any coefficient in the highest root of any component of G,

but it yields also that U_x is connected if and only if ($*$) holds, a result which quite likely has cohomological applications, since ($*$) is necessary and quite close to sufficient for the existence of p-torsion in the simply connected compact Lie group of the same type as G (see [1]).

e) The group G of type B_2 and characteristic 2 yields the simplest example in which U_x is not connected (it has 2 pieces). In this group every sufficiently general element of the centre of U is an irregular unipotent element whose centralizer is unipotent. Hence not every unipotent element is the unipotent part of a regular element (cf. 1.2 *a)*).

§ 5. Irregular elements

Our aim is to prove 1.3. The assumptions of § 4 continue. We write T_i for the kernel of α_i on T, U_i for the group generated by all X_α for which $\alpha>0$ and $\alpha \neq \alpha_i$, B_i for $T_i U_i$ ($1 \leq i \leq r$). The latter is a departure from the notation of 2.5.

5.1. *Lemma. — An element of* G *is irregular if and only if it is conjugate to an element of some* B_i.

For the proof we may restrict attention to elements of the form $x=yz$ ($y \in T$, $z \in U \cap G_y$) by 2.12. Let G′ be as in 3.6. The root system Σ′ for G′ consists of all roots α such that $\alpha(y)=1$. It inherits an ordering from that of Σ. Assume first that x is in B_i. Then α_i is in Σ′, and the X_i component of z is 1. Thus z is irregular in G′ by 3.2 and 3.3, whence x is irregular in G by 3.7. Assume now that x is irregular in G so that z is irregular in G′. If we write $z=\prod_\alpha u_\alpha$ ($u_\alpha \in X_\alpha$, $\alpha>0$, $\alpha \in \Sigma'$), we have $u_\alpha=1$ for some root α simple in Σ′, by 3.2 and 3.3. We prove by induction on the height of α (this is $\sum_i n_i$ if $\alpha=\sum_i n_i \alpha_i$) that x may be replaced by a conjugate such that α above is simple in Σ. This conjugate will be in some B_i, and 5.1 will follow. We assume the height to be greater than 1. We have $(\alpha, \alpha_i)>0$ for some i, and α_i is not in Σ′ since otherwise $\alpha-\alpha_i$ would be in Σ′ in contradiction to the simplicity of α in Σ′. Thus $\sigma_i z \sigma_i^{-1}$ is in U. Since $w_i\alpha = \alpha - 2\alpha_i(\alpha, \alpha_i)/(\alpha_i, \alpha_i)$ has smaller height than α, we may apply our inductive assumption to $\sigma_i x \sigma_i^{-1}$ to complete the proof of the assertion and of 5.1.

5.2. *Lemma. — If* B_i' *is an irreducible component of* B_i, *the union of the conjugates of* B_i' *is closed, irreducible, and of codimension* 3 *in* G.

The normalizer P_i of B_i has the form $P_i = G_i B_i$ and is a parabolic subgroup of G, since it contains the Borel subgroup B. The number of components of T_i, hence of B_i, is either 1 or 2: if $\alpha_i = n\alpha_i'$ with α_i' a primitive character on T, then $(2\alpha_i', \alpha_i)/(\alpha_i, \alpha_i)$ is an integer [8, p. 16-09, Cor. 1], whence $n=1$ or 2. Thus P_i also normalizes B_i', whence if easily follows that P_i is the normalizer of B_i'. Since G/P_i is complete (because P_i is parabolic) by [8, p. 6-09, Th. 4], it follows by a standard argument (cf. [8, p. 6-12] or 2.14 above) that the union of the conjugates of B_i' is closed and irreducible and of codimension in G at least $\dim(P_i/B_i') = 3$, with equality if and only if there is an element contained in only a finite, nonzero number of conjugates of B_i'. Thus 5.2 follows from:

5.3. *Lemma. —* a) *There exists in* $B_i' \cap T_i$ *an element t such that* $\alpha(t) \neq 1$ *for every root* $\alpha \neq \pm\alpha_i$.

b) *If t is as in* a) *it is contained in only a finite number of conjugates of* B_i' (*or* B_i).

For *a)* we choose the notation so that $i=1$. Then for some number $c_1 = \pm 1$, the set $B_i' \cap T_1$ consists of all t for which $\alpha_1'(t) = c_1$. That values c_j may be assigned for $\alpha_j(t)$ $(2 \leq j \leq r)$ so that *a)* holds then follows by induction: having chosen $c_2, \ldots, c_j$ so that $\alpha(t) \neq 1$ if α is a combination of $\alpha_1, \alpha_2, \ldots, \alpha_j$ and $\alpha \neq \pm\alpha_1$, one has only a finite set of numbers to avoid in the choice of c_{j+1}. For *b)* let C be either B_i' or B_i, and let t be as in *a)*. Let yCy^{-1} be a conjugate of C containing t. Since B normalizes C we may take y in the form $u\sigma_w$ of 2.4. Writing $u^{-1}tu = tu'$, the inclusion $y^{-1}ty \in C$ yields

$$(*) \qquad \sigma_w^{-1} t \sigma_w . \sigma_w^{-1} u' \sigma_w \in C.$$

Since $\sigma_w^{-1} u \sigma_w$ is in U^-, so is $\sigma_w^{-1} u' \sigma_w$, whence $u'=1$. Thus u commutes with t, hence it is in X_i because of the choice of t. By $(*)$ we have $\sigma_w^{-1} t \sigma_w \in C$, hence $(w\alpha_i)(t) = 1$, and $w\alpha_i = \pm\alpha_i$. Thus $\sigma_w^{-1} u \sigma_w$ is in G_i and normalizes C, whence using $y = \sigma_w . \sigma_w^{-1} u \sigma_w$ we get $yCy^{-1} = \sigma_w C \sigma_w^{-1}$. The number in *b)* is thus finite and in fact equal to the number of elements of the Weyl group which fix α_i.

We now turn to the proof of Theorem 1.3. Parts *a)* and *b)* follow from 5.1 and 5.2. If $i \neq j$ the independence of α_i and α_j implies that each component of B_i meets each component of B_j. Thus by 5.2 the set Q is connected if $r > 1$. If $r=1$, the irregular elements form the centre of G, whence *c)* follows.

5.4. *Corollary. — The set of regular elements is dense and open in* G.

This is clear.

5.5. *Corollary. — In the set of irregular elements the semisimple ones are dense.*

The set of elements of B_i of the form tu with t as in 5.3 *a)* and u in U_i is open in B_i, dense in B_i by 5.3 *a)*, and consists of semisimple elements: by 2.12 the last assertion need only be proved when u commutes with t and in that case $u=1$ by 2.1 and 2.2 *b)*. By 5.1 this yields 5.5.

By combining 5.1, 5.5 and the considerations of 5.2 we may determine the number of components of Q. We state the result in the simplest case, omitting the proof, which is easy. We recall that G is an adjoint group if the roots generate the character group of T.

5.6. *Corollary.* — *If* G *is a simple adjoint group, the number of irreducible components of* Q *is just the number of conjugacy classes of roots under the Weyl group, except that when* G *is of type* C_r $(r \geq 2)$ *and of characteristic not* 2 *the number of components is* 3 *rather than* 2.

The method of the first part of the proof of 5.2 yields the following result, to be used in 6.11.

5.7. *Lemma.* — *The union of the conjugates of* U_i *is of codimension at least* $r+2$ *in* G.

§ 6. Class functions and the variety of regular classes

G, T, etc. are as before. By a function on G (or any variety over K) we mean a rational function with values in K. Each function is assumed to be given its maximum domain of definition. A function which is everywhere defined is called regular. A function f on G which satisfies the condition $f(x)=f(y)$ whenever x and y are conjugate points of definition of f, is called a class function. As is easily seen, the domain of definition of a class function consists of complete conjugacy classes.

6.1. *Theorem.* — *Let* C[G] *denote the algebra (over* K*) of regular class functions on* G.

a) C[G] *is freely generated as a vector space over* K *by the irreducible characters of* G.

b) *If* G *is simply connected,* C[G] *is freely generated as a commutative algebra over* K *by the fundamental characters* χ_i $(1 \leq i \leq r)$ *of* G.

Let C[T/W] denote the algebra of regular functions on T invariant under W. Since two elements of T are conjugate in G if and only if they are conjugate under W (this follows easily from 2.4), there is a natural map β from C[G] to C[T/W].

6.2. *Lemma.* — *The map* β *is injective.*

For if f in C[G] is such that $\beta f=0$, then $f=0$ on the set of semisimple elements, a dense set in G by 2.14, e.g., whence $f=0$.

6.3. *Lemma.* — *If in* 6.1 *we replace* C[G] *by* C[T/W] *and the irreducible characters by their restrictions to* T, *the resulting statements are true.*

Let X, the character group of T, be endowed with a positive definite inner product invariant under W, and let D consist of the elements δ of X such that $(\delta, \alpha_i) \geq 0$ for all i. We wish to be able to add characters as functions on T. Thus we switch to a multiplicative notation for the group X. For each δ in D we write sym δ for the sum of the distinct images of δ under W. We write $\delta_1 < \delta_2$ if $\delta_1^{-1}\delta_2$ is a product of positive roots. Now the elements of X freely generate the vector space of regular functions on T [8, p. 4-05, Th. 2], and each element of X is conjugate under W to a unique element of D [8, p. 14-11, Prop. 6]. Thus the functions sym δ $(\delta \in D)$ freely generate C[T/W]. Now there is a $1-1$ correspondence between the elements of D and the irreducible characters of G, say $\delta \leftrightarrow \chi_\delta$, such that one has $\chi_\delta|_T = \operatorname{sym}\delta + \sum_{\delta'} c(\delta')\operatorname{sym}\delta'$ $(\delta' < \delta, c(\delta') \in K)$

(see 7.15). Thus *a)* holds. Now if G is simply connected, the characters ω_i of 2.6 form a basis for D as a free commutative semigroup, and the corresponding irreducible characters on G are the χ_i. If $\delta = \prod_i \omega_i^{n(i)}$ is arbitrary in D, then on T we have $\chi_\delta = \prod_i \chi_i^{n(i)} + \sum_{\delta'} c(\delta')\chi_{\delta'}$ $(\delta' < \delta)$, whence by induction, the $\chi_i|_T$ generate the algebra $C[T/W]$. Using the above order one sees that the only polynomial in the $\chi_i|_T$ which is 0 is 0. Thus *b)* holds.

6.4. *Corollary. — The map* β *is surjective. Hence it is an isomorphism.*

The first statement follows from 6.3 *a)*, the second from 6.2.

Theorem 6.1 is now an immediate consequence of 6.3 and 6.4.

6.5. *Corollary. — For all* f *in* $C[G]$ *and* x *in* G, *we have* $f(x) = f(x_s)$.

For this equation holds when f is a character on G.

6.6. *Corollary. — Assume that the elements* x *and* y *of* G *are both semisimple or both regular. Then the following conditions are equivalent.*

a) x *and* y *are conjugate.*

b) $f(x) = f(y)$ *for every* f *in* $C[G]$.

c) $\chi(x) = \chi(y)$ *for every character* χ *on* G.

d) $\rho(x)$ *and* $\rho(y)$ *are conjugate for every representation* ρ *of* G.

If G *is simply connected,* c) *and* d) *need only hold for the fundamental characters and representations of* G.

Here *a)* implies *d)*, which implies *c)*, which implies *b)* by 6.1 *a)*; and the modified implications when G is simply connected also hold by 6.1 *b)*. To prove *b)* implies *a)* we may by 1.2 and 6.5 assume that x and y are semisimple, and then that they are in T and that $f(x) = f(y)$ for every f in $C[T/W]$ by 6.4. Since W is a finite group of automorphisms of the variety T, it follows, among other things, by [10, p. 57, Prop. 18] that $C[T/W]$ separates the orbits of T under W. Thus x and y are conjugate under W, and *a)* holds. This proves 6.6.

6.7. *Corollary. — If* x *is in* G, *the following are equivalent.*

a) x *is unipotent.*

b) *Either* b) *or* c) *of* 6.6, *or its modification when* G *is simply connected, holds with* $y = 1$.

Since x is unipotent if and only if $x_s = 1$, this follows from 6.5 and the equivalence of *a)*, *b)* and *c)* in 6.6.

6.8. *Corollary. — The set* S *of regular semisimple elements has codimension* 1 *in* G.

By 6.4 the function $\prod_\alpha (\alpha - 1)$ (α root) on T has an extension to an element f of $C[G]$. It is then a consequence of 2.11 (see *a)* and *e)*), 2.12, 6.5 and 2.13 that S is defined by $f \neq 0$, whence 6.8.

6.9. *Theorem. — Every element of* C(G), *the algebra of class functions on* G, *is the ratio of elements of* $C[G]$.

Each element of C(G) is defined at semisimple elements of G by 2.14, hence at a dense open set in T, whence by the argument of the proof of 6.4, the natural map from $C(G)$ to $C(T/W)$ is an isomorphism. Now if f is in $C(T/W)$, then $f=g/h$ with g and h regular on T, and because W is finite it can be arranged that h is in $C[T/W]$, whence g is also, and 6.9 follows.

The class functions lead to a quotient structure on G which we now study. We say that the elements x and y of G are *in the same fibre* if $f(x)=f(y)$ for every regular class function f. We observe that if G is simply connected the fibres are the inverse images of points for the map p from G to affine r-space V defined thus:

6.10 $$p(x)=(\chi_1(x), \chi_2(x), \ldots, \chi_r(x)).$$

This is because of 6.1 *b)* and the surjectivity of p (see proof of 6.16). As the next result shows, the fibres are identical with the closures of the regular classes.

6.11. *Theorem. — Let* F *be a fibre.*

a) F *is a closed irreducible set of codimension r in* G.

b) F *is a union of classes of* G.

c) *The regular elements of* F *form a single class, which is open and has a complement of codimension at least* 2 *in* F.

d) *The semisimple elements of* F *form a single class, which is the unique closed class in* F *and the unique class of minimum dimension in* F, *and which is in the closure of every class in* F.

Clearly F is closed in G and a union of classes. By 1.2, 6.5 and 6.6 the fibre F contains a unique class R of regular elements and a unique class S of semisimple elements. Fix y in S and write $G_{y0}=G'T'$ as in 3.6. By 3.2 and 3.3 the regular unipotent elements are dense in U, hence also in the set of all unipotent elements. Applying this to G′, and using 3.7, we see that among the elements x of F for which $x_s=y$ the regular ones, that is, the ones in R, are dense. Thus R is dense in F, which, being closed, is the closure of R. Since R is irreducible and of codimension r in G, the same is true of F. By 5.4 the class R is open in F. Applying 3.2, 3.3 and 5.7 to the group G′ above, we see that the part of $F-R$ for which $x_s=y$ has codimension at least $r+2$ in G_{y0}. Thus $F-R$ itself has codimension at least $r+2$ in G, and at least 2 in F. It remains to prove that S is in the closure of every class in F, since the other parts of *d)* then follow, and by a shift to the group G′ it suffices to prove this when $S=\{1\}$, that is, when F is the set of unipotent elements. Thus *d)* follows from:

6.12. *Lemma. — A nonempty closed subset* A *of* U *normalized by* T *contains the element* 1.

Let u in A be written $\prod_\alpha x_\alpha(c_\alpha)$ as in 2.2 *b)*. Let $n(\alpha)$ denote the height of α, and for each c in K let $u_c=\prod_\alpha x_\alpha(c^{n(\alpha)}c_\alpha)$. If $c\neq 0$, then u_c is conjugate to u via an element of T, whence it belongs to A. If f is a regular function on U vanishing on A, then $f(u_c)$ is a polynomial in c (by 2.2 *b)*) vanishing for $c\neq 0$, hence also for $c=0$. Thus u_0 is in A, which proves 6.12.

From 6.11 *d)* we get the known result.

6.13. *Corollary. — In a semisimple group a class is closed if and only if it is semisimple.*

More generally we have:

6.14. *Proposition. — In a connected linear group* G′ *each class which meets a Cartan subgroup is closed.*

Let B′ be a Borel subgroup of G′. Since G′/B′ is complete [8, p. 6-09, Th. 4], it is enough to prove 6.14 with B′ in place of G′. Let x be an element of a Cartan subgroup of B′. Then x centralizes some maximal torus T′ in B′ [8, p. 7-01, Th. 1], whence if $B'=T'U'$ as usual then the class of x in B′ is an orbit under U′ acting by conjugation on B′. Because U′ is unipotent it follows from [7] that this class is closed.

6.15. *Remarks. — a)* Almost all fibres in 6.11 consist of a single class which is regular, semisimple, and isomorphic to G/T. This follows from 2.15.

b) Almost all of the remaining fibres consist of exactly 2 classes R and S with $\dim R = \dim S + 2$.

c) It is natural to conjecture that every fibre is the union of a finite number of classes, or, equivalently, that the number of unipotent classes is finite. In characteristic 0 the finiteness follows from the corresponding result for Lie algebras [4, p. 359, Th. 1]. In characteristic $p \neq 0$ one may assume that G is over the field k of p elements and make the stronger conjecture that each unipotent class has a point over k, or equivalently, by 1.10, that each unipotent class is over k. The last result would follow from the plausible statement: if γ is an automorphism of K, the element $\prod_{\alpha>0} x_\alpha(c_\alpha)$ of U is conjugate to $\prod_\alpha x_\alpha(\gamma c_\alpha)$.

d) It should be observed that for a given type of group the number of unipotent classes can change with the characteristic. Thus for the group of type B_2 the number is 5 in characteristic 2 but only 4 otherwise.

e) The converse of 6.14 is false.

6.16. *Theorem. — Assume that* G *is simply connected and that* p *is the map* 6.10 *from* G *to affine r-space* V. *Then* G/p *exists as a variety, isomorphic to* V.

The points to be proved are 1), 2) and 3) below.

1) *p is regular and surjective.* Clearly p is regular. The algebra of regular functions on T is integral over the subalgebra fixed by W. Thus any homomorphism of the latter into K extends to one of the former [2, p. 420, Th. 5.5]. Applying this to the homomorphism for which $\chi_i|_T \to c_i$ $(c_i \in K, i \leq i \leq r)$ (see 6.1 and 6.4), we get the existence of t in T such that $\chi_i(t) = c_i$ for all i, whence p is surjective.

2) *Let f be a function on* V *and x an element of* G. *Then f is defined at $p(x)$ if and only if $f \circ p$ is defined at x.* Write $f = g/h$, the ratio of relatively prime polynomials in the natural coordinates on V. Then the restrictions to T of $g \circ p$ and $h \circ p$, as linear combinations of characters on T, are also relatively prime: otherwise suitable powers of these functions would have a nontrivial common factor invariant under W, which by 6.1 and 6.4 would contradict the fact that g and h are relatively prime. If $h(p(x)) \neq 0$, then clearly f is defined at $p(x)$ and $f \circ p$ at x. Assume $h(p(x)) = 0$. Because g and h are relatively prime, f is not defined at $p(x)$. We may take x in B and write $x = tu$ with t in T and u in U. Let A be an open set in G containing x. Then $Au^{-1} \cap T$ is an open

subset of T containing t, and because $g\circ p$ and $h\circ p$ are relatively prime on T and $h(p(t))=h(p(x))=0$ by 2.12 and 6.5, it also contains a point t' at which $h\circ p=0$ and $g\circ p\neq 0$. Then A contains the point $t'u$ at which the same equations hold, at which $f\circ p$ is not defined. Since A is arbitrary, $f\circ p$ is not defined at x, whence 2). From this discussion we see that

(*) *the domain of definition of a class function on* G *consists of complete fibres relative to* p.

3) *Under the map* $f\to f\circ p$ *the field of functions on* V *is mapped (isomorphically) onto the field of functions on* G *constant on the fibres of* p. The latter field consists of class functions, so that 3) follows from 6.1 *b)* and 6.9.

We recall that the regular elements form an open subvariety G^r of G.

6.17. *Corollary. — If* G *is simply connected, the set of regular classes of* G *has a structure of variety, that of* V, *given by the restriction of* p *to* G^r.

This means that the restriction of p to G^r has as its fibres the regular classes of G, and that 1), 2) and 3) above hold with G^r in place of G. All of this is clear.

To close this section we describe the situation when G is not simply connected. The proofs, being similar to those above, are omitted. Let $\pi: G'\to G$ be the simply connected covering of G, and let F be the kernel of π. An element f of F acts on the i^{th} fundamental representation of G' as a scalar $\omega_i(f)$. We define an action of F on V thus: $f.(c_i)=(\omega_i(f)c_i)$.

6.18. *Theorem. — Assume* G *semisimple but not necessarily simply connected. Then the set of regular classes of* G *has a structure of variety, isomorphic to that of the quotient variety* V/F.

§ 7. Structure of N

In this section G, N, etc. are as in 1.4. Our aim is to prove that N is isomorphic to affine r-space V, under the map p of 6.10 when G is simply connected.

7.1. *Theorem. — The set* N *of* 1.4 *is closed and irreducible in* G. *It is isomorphic as a variety to affine r-space* V *under the map* $(c_i)\to\prod_i(x_i(c_i)\sigma_i)$. *In particular, an element of* N *uniquely determines its components in the product that defines* N.

7.2. *Lemma. — Let* $\beta_i=w_1w_2\dots w_{i-1}\alpha_i$ $(1\leq i\leq r)$ *and* $w=w_1w_2\dots w_r$.

a) *The roots* β_i *are positive, distinct and independent.*

b) *They form the set of positive roots which become negative under* w^{-1}.

c) *The sum of two* β*'s is never a root.*

Since β_i is α_i increased by a combination of roots α_j $(j<i)$, we have *a)*. The roots $w^{-1}\beta_i=-w_rw_{r-1}\dots w_{i+1}\alpha_i$ are all negative by *a)* applied with $\alpha_r, \dots, \alpha_1$ in place of $\alpha_1, \dots, \alpha_r$. Since w^{-1} is a product of r reflections corresponding to simple roots, no more than r positive roots can change sign under w^{-1} by [8, p. 14-04, Cor. 3], whence *b)*. If the sum of two β's were a root, this root would be a β by *b)*, which is impossible by *a)*.

7.3. *Lemma. — If* β_i *and* w *are as in* 7.2 *the product* $\prod_i X_{\beta_i}$ *in* U *is direct, and if* X_w *denotes this product and* $\sigma_w=\sigma_1\sigma_2\dots\sigma_r$, *then* $N=X_w\sigma_w$.

The first part follows from *a)* and *c)* of 7.2, and the second from the equation $X_{\beta_i} = \sigma_1 \dots \sigma_{i-1} X_i \sigma_{i-1}^{-1} \dots \sigma_1^{-1}$.

Consider now 7.1. By 2.2 *b)* the set $X_w \sigma_w$ is closed, irreducible, and isomorphic to V via the map $(c_i) \to \prod_i x_{\beta_i}(c_i)\sigma_w = \prod_i (x_i(a_i c_i)\sigma_i)$ (a_i fixed element of K^*), whence 7.1 follows.

7.4. *Examples of* N. — *a)* Assume $r=1$ and $G = SL(2, K)$. Here we may choose X_1 as the group of superdiagonal unipotent matrices and σ_1 as the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then N consists of all matrices of the form $y(c) = \begin{pmatrix} c & -1 \\ 1 & 0 \end{pmatrix}$.

b) Assume $r > 1$ and $G = SL(r+1, K)$. Here we may choose for $x_i(c)\sigma_i$ the matrix $1_{i-1} \overset{\circ}{+} y(c) \overset{\circ}{+} 1_{r-i}$, with $y(c)$ as in *a)* and 1_j the identity matrix of rank j. Then the element $\prod_i (x_i(c_i)\sigma_i)$ of N has the entries $c_1, -c_2, \dots, (-1)^{r-1}c_r, (-1)^r$ across the first row, 1 in all positions just below the main diagonal, and 0 elsewhere. We thus have one of the classical normal forms for a matrix which is regular in the sense that its minimal and characteristic polynomials are equal. We observe that the parameters c in this form are just the values of the characters χ_i at the element considered. A similar situation exists in the general case. The group X_w of 7.3 in the present case consists of all unipotent matrices which agree with the identity in all rows below the first.

Next we show (7.5 and 7.8 below) that N does not depend essentially on the choice of the σ_i and the labelling of the simple roots, or equivalently, the order of the factors in the product for N. The other choices necessary to define N, namely the maximal torus T and a corresponding system of simple roots, are immaterial because of well known conjugacy theorems.

7.5. *Lemma. — Let each σ_i be replaced by an element σ'_i equivalent to it* mod T, *and let* $N' = \prod_i (X_i \sigma'_i)$. *Then there exist t and t' in* T *such that* $N' = t'N = tNt^{-1}$.

Because T normalizes each X_i and is itself normalized by each σ_i, the first equality holds. We may write $tNt^{-1} = tw(t^{-1})N$, with w as in 7.3. Thus the second equality follows from:

7.6. *Lemma. — If w is as in 7.2, the endomorphism $1-w$ of* T $(t \to tw(t^{-1}))$ *is surjective, or equivalently, its transpose $1-w'$ on the dual* X *of* T *is injective.*

Suppose $(1-w')x = 0$ with x in X. Then $(1-w_1)x = (1-w_2 \dots w_r)x$. The left side being a multiple of α_1 and the right side a combination of $\alpha_2, \dots, \alpha_r$, both sides are 0. Since x is fixed by w_1 it is orthogonal to α_1. Similarly it is orthogonal to $\alpha_2, \dots, \alpha_r$, hence is 0. Thus $1-w'$ is injective.

7.7. *Remarks. — a)* The argument shows that the conclusion of 7.6 holds if w is the product of reflections corresponding to any r independent roots.

b) If G is simply connected, one can show by an argument like that in 4) of 4.3 that the kernel of $1-w$ on T is just the centre of G.

7.8. *Proposition.* — *For each* i *let* y_i *be an element of* $X_i\sigma_i$. *Then the products obtained by multiplying the* y_i *in the* $r!$ *possible orders are conjugate.*

This result is not used in the sequel. Consider the Dynkin graph in which the nodes are the simple roots and the relation is nonorthogonality. Since the graph has no circuits [9, p. 13-02], it is a purely combinatorial fact that any cyclic arrangement of the simple roots can be obtained from any other by a sequence of moves each consisting of the interchange of 2 roots adjacent in the arrangement and not related in the graph (see [16, Lemma 2.3]). Now if α_i and α_j are not related in the graph, that is, orthogonal, then G_i and G_j commute elementwise (because $\alpha_i \pm \alpha_j$ are not roots), so that in case y_i is in G_i for each i our result follows. In the general case, if one interchanges y_i and y_j in the above situation, a factor from T appears, but this can be eliminated by conjugation by a suitable element of T, whence 7.8 follows.

7.9. *Theorem.* — *Let* G *be simply connected and let* p *be the map* 6.10 *from* G *to affine* r*-space* V. *Then* p *maps* N, *as a variety, isomorphically onto* V.

As in § 6, D denotes the set of characters on T of the form $\omega = \sum_j n_j \omega_j$ ($n_j \geq 0$, ω_j as in 2.6). We write $n_j = n_j(\omega)$ in this situation.

7.10. *Definition.* — $\omega_j \prec \omega_i$ means that *a)* $i \neq j$, and *b)* there exists ω in D such that $\omega_i - \omega$ is a sum of positive roots and $n_j(\omega) > 0$.

7.11. *Lemma.* — *The relation* $\prec$ *of* 7.10 *is a relation of strict partial order.*

If $\omega_k \prec \omega_j$ and $\omega_j \prec \omega_i$, then $k \neq i$ since a sum of positive roots and nonzero elements of D can not be 0 unless it is vacuous. Thus 7.11 follows.

7.12. *Remark.* — For simple groups of type A_r, B_2, or D_4 the relation $\prec$ is vacuous; for the other simple groups it is nonvacuous.

7.13. *Lemma.* — *Assume that* σ_i *is in* G_i, *and let* $T_i = G_i \cap T$. *Then there exists a bijection* β *from* T_i *to* $X_i - \{1\}$ *such that* $x = \beta t$ *if and only if* $(xt\sigma_i)^3 = 1$.

The group G_i is isomorphic to SL(2) by [8, p. 23-02, Prop. 2]. Identifying T_i (resp. X_i) with the subgroup of diagonal (resp. unipotent superdiagonal) matrices of SL(2), we get 7.13 by a simple calculation.

7.14. *Lemma.* — *Assume that* G *is simply connected, and that* σ_i *is chosen in* G_i *for each* i, *in the definition of* N. *Let the isomorphisms* $x_i : K \to X_i$ *be so normalized that* $x_i(-1) = \beta(1)$ *if* β *is as in* 7.13. *Let* ψ_i *be the function on* N *defined by* $\prod_j (x_j(c_j)\sigma_j) \to c_i$. *Then there exist functions* f_i *and* g_i ($1 \leq i \leq r$) *such that*:

a) f_i *(resp.* g_i*) is a polynomial with integral coefficients in those* ψ_j *(resp.* χ_j*) such that* $\omega_j \prec \omega_i$ *(see* 7.10*).*

b) *On* N *we have* $\chi_i = \psi_i + f_i$ *and* $\psi_i = \chi_i + g_i$.

Let i be fixed and let V_i be the space of the i^{th} fundamental representation of G. For each weight (character on T) ω, let V_ω be the subspace of vectors which transform according to ω. We recall, in the form of a lemma, the properties of irreducible representations needed for our proof.

7.15. *Lemma.* — a) $\sum_\omega V_\omega = V_i$, *the total space.*

b) *If* $\omega=\omega_i$, *the highest weight, then* $\dim V_\omega = 1$.

c) *If* $\omega_i-\omega$ *is not a sum of positive roots,* $V_\omega=0$.

d) *If* v *is in* V_ω, *if* $1\leq j\leq r$, *and if we set* $\omega(n)=\omega+n\alpha_j$ *for* $n\geq 1$, *then there exist vectors* v_n *in* $V_{\omega(n)}$ *such that* $x_j(c)v=v+\sum_n c^n v_n$ *for all* c *in* K.

The proofs may be found in [8, Exp. 15 and p. 21-01, Lemme 1].

Now let x be an element of N. We write $x=\prod_j y_j$ and $y_j=x_j(c_j)\sigma_j$, and proceed to calculate $\chi_i(x)$, in several steps:

1) *If* v *is in* V_ω *and* $\omega(n)=\omega+(n-n_j(\omega))\alpha_j$ *for* $n\geq 1$, *there exist vectors* v_n *in* $V_{\omega(n)}$ *such that* $y_jv=\sigma_jv+\sum_n \psi_j(x)^n v_n$. This follows from 7.15 *d)* because σ_jv corresponds to the weight $w_j\omega=\omega-n_j(\omega)\alpha_j$.

2) *Let* π_ω *be the projection on* V_ω *determined by* 7.15 a). *Then* $\pi_\omega x\pi_\omega=\prod_j(\pi_\omega y_j\pi_\omega)$. This follows from 1) and the independence of the roots α_j.

3) $\chi_i(x)=\sum_\omega \operatorname{tr}\pi_\omega x\pi_\omega$. This follows from the orthogonal decomposition $1=\sum_\omega \pi_\omega$, which holds by 7.15 *a)*.

4) *If* $\omega=\omega_i$, *the highest weight, then* $\operatorname{tr}\pi_\omega x\pi_\omega=\psi_i(x)$. Let v be a basis for V_ω (see 7.15 *b)*), and let $v'=-\sigma_iv$. Then $y_i=x_i(c_i)\sigma_i$ fixes the space V′ generated by v and v', by 7.15 *c)* and *d)*, and maps these vectors onto $-v'+ac_iv$ and bv $(a, b\in K)$, respectively. A simple calculation shows that $y_i^3=1$ on V′ if and only if $b=1$ and $ac_i=-1$. Because of our normalization of x_i, this is true only if $c_i=-1$, so that $a=1$. Thus $\pi_\omega y_i\pi_\omega v=c_iv$. If $j\neq 1$, then $w_j\omega=\omega$ by 2.6, so that X_j and σ_j, and hence also the group G_j they generate, fix the line of v, and then v itself because G_j is equal to its commutator group. By 2) we conclude that $\pi_\omega x\pi_\omega v=c_iv$, whence 4) follows.

5) *If* ω *is in* D *and* $\omega\neq\omega_i$, *then* $\operatorname{tr}\pi_\omega x\pi_\omega$ *depends only on those* $\psi_j(x)$ *for which* $\omega_j\prec\omega_i$. We may assume $V_\omega\neq 0$. It follows from 1) and 2) that $\pi_\omega x\pi_\omega$ depends only on those $\psi_j(x)$ for which $n_j(\omega)$ is positive. Because $\omega_i-\omega$ is a sum of positive roots by 7.15 *c)*, this yields 5).

6) *If* ω *is not in* D, *then* $\pi_\omega x\pi_\omega=0$. If j is such that $n_j(\omega)<0$, then $\pi_\omega y_j\pi_\omega=0$ by 1), whence 6) follows from 2).

7) *In terms of the* ψ_j *the function* χ_i *is a polynomial with integral coefficients.* That we have a polynomial follows from 1). The integrality follows from the fact, proved in [17] when the characteristic is not 0 and in [14] when the characteristic is 0, that there exists a basis of V_i relative to which each σ_j acts integrally and each $x_j(c_j)$ as a polynomial with integral coefficients.

To prove 7.14 now, we need only combine 3), 4), 5), 6) and 7) above to get the assertions concerning f_i and then solve the equations $\chi_i=\psi_i+f_i$ recursively for the ψ_i to get the assertions concerning g_i.

Now we can prove Theorem 7.9. By 7.5 we may assume σ_i is in G_i for each i. Then by 7.1 the functions ψ_i of 7.14 are affine coordinates on N, so that 7.9 follows from 7.14.

7.16. *Corollary.* — a) N *is a cross-section of the fibres of* p *in* 7.9.

b) *The corresponding retraction* q *from* G *to* N, *given by* $q(x)=\prod_i x_i(\chi_i(x)+g_i(x))\sigma_i$ *if the normalization of* 7.14 *is used, yields on* G *a quotient structure isomorphic to that for* p.

c) *The set* $s(\mathrm{N})$ *made up of the semisimple parts of the elements of* N *is a cross-section of the semisimple classes of* G.

The formula for q follows from 7.14, and the other parts of *a)* and *b)* from 7.9. Then *c)* follows from 6.11 *d)*. We observe that $s(\mathrm{N})$ is never closed or connected, only constructible.

§ 8. Proof of 1.4 and 1.5

It follows from 7.9 that if G is simply connected distinct elements of N lie in distinct conjugacy classes. Thus 1.4 and 1.5 are consequences of the following result.

8.1. *Theorem.* — *Let* G *be simply connected (and semisimple),* x *an element of* G, *and* N *as in* 1.4. *Then the following are equivalent.*

a) x *is regular.*

b) x *is conjugate to an element of* N.

c) *The differentials* $d\chi_i$ *are independent at* x.

First we prove some lemmas.

8.2. *Lemma.* — *Under the assumptions of* 8.1 *let* ψ_i *denote the restriction of* χ_i *to* T, *let* ω_0 *denote the product* $\prod_i \omega_i$ *of the fundamental weights, and let the function* f *on* T *be defined by* $\prod_i (d\psi_i)=f\prod_i(\omega_i^{-1}d\omega_i)$, *the products being exterior products of differential forms. Then* $f=\sum_w(\det w)w\omega_0=\omega_0\prod_\alpha(1-\alpha^{-1})$, *the sum over* w *in* W *and the product over the positive roots* α.

We will deduce this from $\psi_i=\operatorname{sym}\omega_i+\sum_\delta c_i(\delta)\operatorname{sym}\delta$ ($\delta\in\mathrm{D}$, $\delta<\omega_i$, $c_i(\delta)\in\mathrm{K}$, notation of 6.3). Replacing the c's by indeterminates, we may view the equations to be proved as formal identities with integral coefficients in the group algebra of the dual of T, thus need only prove them in characteristic 0. First f is skew: $wf=(\det w)^{-1}f$ for every w in W. We have $wd\psi_i=d\psi_i$, and if $w\omega_i=\prod_j\omega_j^{n(i,j)}$, then $w(\omega_i^{-1}d\omega_i)=\sum_j n(i,j)\omega_j^{-1}d\omega_j$, which, because $\prod_i\omega_i^{-1}d\omega_i\neq 0$, yields $f=wf.\det(n(i,j))=wf.\det w$. Because f is skew and the characteristic is 0, we have

$$(*)\qquad f=\sum_\delta c(\delta)\sum_w(\det w)w\delta\quad(\delta\in\mathrm{D},\ c(\delta)\in\mathrm{K}),$$

the inner sum being over W and the outer over D. From the expression for ψ_i, we have $d\psi_i=\omega_i(\omega_i^{-1}d\omega_i)+$ a combination of terms $\omega(\omega_j^{-1}d\omega_j)$, with ω lower (by a product of positive roots) than ω_i, whence $f=\omega_0+$lower terms. Thus in $(*)$ above $c(\omega_0)=1$ and $c(\delta)=0$ when δ is not lower than ω_0. If δ is lower than, and different from, ω_0, then δ is orthogonal to some α_i (if $\delta=\prod_i\omega_i^{n(i)}$, then some $n(i)$ is less than the corresponding object for ω_0, hence is 0), whence $\sum_w (\det w) w\delta = 0$. Thus $(*)$ becomes $f = \sum_w (\det w) w\omega_0$. The final equality in 8.2 is a well known identity of Weyl [18, p. 386].

8.3. *Remark.* — $\prod_i (\omega_i^{-1} d\omega_i)$ above is, to within a constant factor, the unique differential r-form on T invariant under translations, that is, the "volume element" of T.

8.4. *Lemma.* — *Let* G' *denote the neighborhood* U^-TU *of* T (*see* 2.3), *and let* π *denote the natural projection from* G' *to* T. *For each* α *let* y_α *be the composition of the projection from* G *to* X_α *and an isomorphism from* X_α *to* K.

a) *If* f *is a regular function on* G, *its restriction to* G' *is a combination of monomials in the functions* y_α *and* $\omega_i^{\pm 1} \circ \pi$.

b) *If* f *is also a class function and the combination is irredundant, then each monomial has a total degree in the* y_α*'s which is either* 0 *or at least* 2.

Here *a)* follows from 2.3. In *b)* no monomial could involve exactly one y_α (to the first degree), because then conjugation by t in T and use of 2.1 would yield $\alpha(t) = 1$ for all t in T, a contradiction.

8.5. *Lemma.* — *Let* ψ_i *be as in* 8.2 *and* π *as in* 8.4. *Then* $d\chi_i = d\psi_i \circ d\pi$ *at all points of* T.

Here the tangent space at t as an element of G is being identified with its tangent space as an element of G'. By 8.4 *b)* we have on G' an equation $\chi_i = \psi_i \circ \pi +$ terms of degree at least 2 in the y_α. Since each y_α is 0 on T, we have there $d\chi_i = d\psi_i \circ d\pi$.

8.6. *Lemma.* — *If* x *is semisimple,* a) *and* c) *of* 8.1 *are equivalent.*

We may take x in T. By 8.5 and the surjectivity of $d\pi$ (from the tangent space of x in G' to its tangent space in T), the $d\chi_i$ are independent at x if and only if the $d\psi_i$ are, and by 8.2 this is so if and only if $\alpha(x) \neq 1$ for every root α, that is, if and only if x is regular, by 2.11.

We can now prove 8.1. From 7.9 it follows that *b)* implies *c)*, and from 5.5 and 8.6 that *c)* implies *a)*. Now assume x is regular. By 7.9 there is a unique element y in both N and the fibre of p which contains x. Then y is regular because *b)* $\rightarrow$ *a)* has already been shown, whence x is conjugate to y by 6.11 *c)*. Thus *a)* implies *b)*, and 8.1 is proved.

Using the above methods one can also show:

8.7. *Theorem.* — *Without the assumption of simple connectedness in* 8.1, *conditions* a) *and* b) *are equivalent and are implied by*

c′) *there exist* r *regular class functions on* G *whose differentials are independent at* x.

One can also show that the elements of N conjugate to a given one $\prod_i x_i(c_i)\sigma_i$ are those of the form $\prod_i x_i(\omega_i(f)c_i)\sigma_i$ $(f \in F)$, in the notation of the paragraph before 6.18.

8.8. *Remark.* — If $w = w_1 w_2 \ldots w_r$, all elements of the double coset $B\sigma_w B$ are regular, not just those of N. This depends on 7.3, 7.5 and the following result, whose proof is omitted.

8.9. *Proposition.* — *If* w *is as above, then the map from the Cartesian product of* $\sigma_w U^- \sigma_w^{-1} \cap U$ *and* $\sigma_w^{-1} U \sigma_w \cap U$ *to* U *given by* $(u_1, u_2) \rightarrow u_2^{-1}.u_1.\sigma_w u_2 \sigma_w^{-1}$ *is bijective.*

§ 9. Rationality of N

Henceforth k denotes a perfect subfield of our universal field K, which for convenience is assumed to be an algebraic closure of k, and Γ denotes the Galois group of K over k. In this section G is a simply connected semisimple group. If G is (defined) over k, it is natural to ask whether N or a suitable analogue thereof can be constructed over k. As the following result shows, the answer is in general no.

9.1. *Theorem. — If* G *is over* k, *then a necessary condition for the existence over* k *of a cross-section* C *of the regular classes is the existence of a Borel subgroup over* k.

For the unique unipotent element of C is clearly over k, and so is the unique Borel subgroup that contains it (see 3.2 and 3.3).

As we now show, this necessary condition comes quite close to being sufficient. First we consider a more restrictive situation, that in which G splits over k, that is, is over k and contains a maximal torus which with all of its characters is over k.

9.2. *Theorem. — If* G *splits over* k, *then* N *in* 1.4 *(and hence also* $s(\mathrm{N})$ *in* 7.16 c)) *can be constructed over* k.

Let G split relative to the maximal torus T. Since the simple root α_i is over k, so is X_i, and it remains to choose each σ_i over k. We start with an arbitrary choice for σ_i. Then the map $\gamma \rightarrow \sigma_i^{-1}\gamma(\sigma_i) = x_\gamma$ is a cocycle from Γ to a group isomorphic to K^*, namely, $\mathrm{G}_i \cap \mathrm{T}$. In other words:

9.3. a) $x_{\gamma\delta} = x_\gamma \gamma(x_\delta)$ *for all* γ *and* δ *in* Γ.

b) *There exists a subgroup* Γ_1 *of finite index in* Γ *such that* $x_\gamma = 1$ *if* γ *is in* Γ_1.

By a famous theorem of Hilbert (see, e.g., [11, p. 159]), this cocycle is trivial, that is, there exists t_i in T such that $x_\gamma = t_i \gamma(t_i^{-1})$ for all γ in Γ. Then $\sigma_i t_i$ is over k, as required.

9.4. *Theorem. — Assume that* G *is over* k, *and contains a Borel subgroup over* k. *Assume further that* G *contains no simple component of type* A_n *(n even). Then the set* N *of* 1.4 *can be constructed over* k.

Let B be a Borel subgroup over k. It contains a maximal torus T over k. If k is infinite, this follows from 2.14 and Rosenlicht's theorem [6, p. 44] that G_k is dense in G, while if k is finite with q elements and β is the q^{th} power automorphism, one picks an arbitrary maximal torus T′, then x in B so that $x\beta(\mathrm{T}')x^{-1} = \mathrm{T}'$ (conjugacy theorem), then y in B so that $x = y^{-1}\beta(y)$ (Lang's theorem [5]), and then $\mathrm{T} = y\mathrm{T}'y^{-1}$. We order the roots so that B corresponds to the set of positive roots. Γ permutes the simple roots α_i in orbits. We order the α_i so that those in each orbit come together. If for each orbit we can construct over k the corresponding part of the product for N, then we can construct N over k. Thus we may (and shall) assume that there is a single orbit. Let Γ_1 be the stabilizer of α_1 in Γ, and k_1 the corresponding subfield of K. Then α_1 is over k_1, whence G_1 (the corresponding group of rank 1) is also, so that by 9.2 applied with G_1 in place of G the set $\mathrm{X}_1\sigma_1$ can be constructed over k_1. Then Γ operates on this set to produce, in an unambiguous way, sets $\mathrm{X}_i\sigma_i$ $(1 \leq i \leq r)$. But these sets commute pairwise: the roots (in each orbit) are orthogonal because of the exclusion of the type A_n (n even). Their product is thus fixed by all of Γ, hence is over k, as required.

Observe that 9.2 and 9.4 yield 1.6.

9.5. *Corollary.* — *Under the assumptions of* 9.2 *or* 9.4 *the natural map (inclusion) from the set of regular elements over k to the set of regular classes over k is surjective. In other words, each regular class over k contains an element over k.*

Let C be a regular class over k. Then $C \cap N$ is over k by 9.2 or 9.4, and it consists of one element by 1.4, whence 9.5.

9.6. *Remark.* — For the group of type A_n (n even) we do not know whether there exists over k a global closed irreducible cross-section of the regular classes of G, or even of the fibres of the map p of 6.10 (which can be taken over k if V is suitably defined over k), although a study of the group of type A_2 casts some doubt on these possibilities. All that we can show, 9.7 *c)* below, is that there exists a local cross-section (covering a dense open set in V) with the above properties.

9.7. *Theorem.* — *Assume that* G *is over k, and contains a Borel subgroup over k. Assume that every simple component of* G *is of type* A_n *(n even). Then there exists in* G *a set* N′ *with the following properties.*

a) N′ *is a disjoint union of a finite number of closed irreducible subsets of* G.

b) N′ *is a cross-section of the fibres of p in* 6.10.

c) *p maps each component of* N′ *isomorphically onto a subvariety of* V, *and one component consisting of regular elements onto a dense open subvariety of* V.

d) $s(N')$ *is a cross-section of the semisimple classes of* G.

e) *Each component of* N′ *is over k.*

In order to continue our main development, we postpone the construction of N′ to the end of the section.

9.8. *Theorem.* — *If* G *(with or without components of type* A_n *(n even)) is over k and contains a Borel subgroup over k, the natural map from the set of semisimple elements over k to the set of semisimple classes over k is surjective.*

Observe that this is Theorem 1.7 of the introduction. As is easily seen, we may assume either that no components of G are of type A_n (n even) or that all are. In the first case we replace N by $s(N)$ and 1.4 by 7.16 *c)* in the proof of 9.5, while in the second case we use $s(N')$ and 9.7 *d)* instead.

9.9. *Remark.* — G need not be semisimple for the validity of 9.8. For let A be a connected linear group satisfying the other assumptions. If R is the unipotent radical, then A/R is a connected reductive group, hence the direct product of a torus and a simply connected semisimple group because A is simply connected, whence the result to be proved holds for A/R. A semisimple class of A over k thus contains an element x over k mod R. The map $\gamma \to x^{-1}\gamma(x)$ then defines a cocycle into R which is trivial because R is unipotent (see [12, Prop. 3.1.1]), whence 9.9.

Theorem 9.8 admits a converse.

9.10. *Theorem. — If* G *is over* k *and the map of* 9.8 *is surjective, then* G *contains a Borel subgroup over* k.

If k is finite, this follows from Lang's theorem (see the proof of 9.4), even without the assumption of surjectivity. Henceforth let k be infinite. Let F be the centre of G, n the order of F, h the height of the highest root, and c and c' elements of k^* such that $c = c'^n$ and c has order greater than $h+1$. Let T be a maximal torus over k (for the existence, see the proof of 9.4), and t' an element of T such that $\alpha_i(t') = c'$ for every α_i in some system of simple roots. Set $t = t'^n$, so that $\alpha_i(t) = c$.

1) *t is regular.* If α is a root of height m, then $\alpha(t) = c^m \neq 1$, whence 1). Since $c^m = c$ only if $m = 1$ we also have:

2) *If α is a root such that $\alpha(t) = c$, then α is simple.*

3) *The class of t is over k.* Each element γ of the Galois group Γ acts as an automorphism on the root system, hence determines a unique element w_γ of the Weyl group such that $w_\gamma \circ \gamma$ permutes the simple roots. Since $\alpha_i(t')$ is independent of i and is in k, we have $\alpha_i((w_\gamma \circ \gamma)(t')) = ((w_\gamma \circ \gamma)^{-1}(\alpha_i))(t') = \alpha_i(t')$, whence $(w_\gamma \circ \gamma)(t') = ft'$ for some f in F. Thus $(w_\gamma \circ \gamma)(t) = f^n t = t$, which yields 3).

4) *One can normalize the pair* T, t *above so that* 1) *and* 2) *hold and also t is over k.* By the surjectivity assumption in 9.10 there exists t'' over k and conjugate to t. Any inner automorphism which maps t to t'' maps T onto a maximal torus T$''$ which must be over k because it is the unique maximal torus containing t'' by 1) and 2.11, and also maps the simple system relative to T into one relative to T$''$ so that the equations $\alpha_i(t) = c$ are preserved. On replacing T, t by T$''$, t'', we get 4).

Now by 4) we have $(\gamma\alpha_i)(t) = (\gamma\alpha_i)(\gamma t) = \gamma(\alpha_i(t)) = \gamma(c) = c$, whence $\gamma\alpha_i$ is simple by 2). Thus each γ preserves the set of positive roots, hence also the corresponding Borel subgroup, which is thus over k, as required.

It remains to construct the set N$'$ of 9.7. If G is a group of type A_n (n even) in which T, etc. are given, the following notation is used. The simple roots are labelled $\alpha_1, \alpha_2, \ldots, \alpha_n$ from one end of the Dynkin graph to the other (see [8, p. 19-03]). We write $n = 2m$, set $\alpha = \alpha_m + \alpha_{m+1}$, a root, let G_α denote the group of rank 1 generated by X_α and $X_{-\alpha}$, write T_α for $T \cap G_\alpha$, and σ_α for an element normalizing T according to the reflection relative to α. The group of automorphisms of the system of simple roots pairs α_i with α_{2m+1-i}, which is orthogonal to α_i unless $i = m$. Hence (see the proof of 9.4) only the part of N corresponding to α_m and α_{m+1} need be modified.

9.11. *Theorem. — Let* G *be as in* 9.7. *If* G *contains a single component, assume (in the above notation) that the choices σ_i and σ_α are normalized to be in G_i and G_α ($i \neq m, m+1$), that u_m and u_{m+1} are elements of X_m and X_{m+1} and different from* 1, *that* N$''$ (*resp.* N$'''$) *is the product of $X_\alpha\sigma_\alpha$ (resp. $u_{m+1}u_m X_\alpha \sigma_\alpha T_\alpha$) and $\prod_j X_j\sigma_j$ ($j \neq m, m+1$), and that* N$'$ *is the union of* N$''$ *and* N$'''$. *If* G *is a product of several components, assume that* N$'$ *is constructed as a product accordingly. Then one has* a) *to* e) *of* 9.7.

We proceed to study N″ and N‴ as we did N in § 7. The following observation will be useful.

9.12. *Lemma.* — a) *The sequence of roots* $S=\{\alpha_1, \ldots, \alpha_{m-1}, \alpha, \alpha_{m+2}, \ldots, \alpha_{2m}\}$ *yields a simple system of type* A_{2m-1}.

b) *If* G′ *is the corresponding semisimple subgroup of* G, *then* N″ *as constructed in* G′ *fulfills the rules of construction of* N *in* G.

The verification of *a)* is easy, while *b)* is obvious.

9.13. *Lemma.* — *The sets* N″ *and* N‴ *are closed and irreducible in* G. *The natural maps from the Cartesian products* $X_\alpha \times \prod_j X_j$ *and* $X_\alpha \times T_\alpha \times \prod_j X_j$ *to* N″ *and* N‴, *respectively, are isomorphisms of varieties. In particular each element of* N″ *or* N‴ *uniquely determines its components.*

The assertions about N″ follow from 7.1 and 9.12. Those concerning N‴ are proved similarly.

9.14. *Lemma.* — *If* u_m *and* u_{m+1} *in* 9.11 *are replaced by alternates* u'_m *and* u'_{m+1}, *then* N‴ *is replaced by a conjugate, under* T.

We can find t in T to transform u_m and u_{m+1} into u'_m and u'_{m+1}, and, because only the values $\alpha_m(t)$ and $\alpha_{m+1}(t)$ are relevant (see 2.1), so that also $\alpha_j(t)=1$ if $j\neq m, m+1$; we are using the independence of the simple roots here. By conjugating N‴ by t, we get 9.14.

9.15. *Lemma.* — *Let the functions* $\psi_i\ (i\neq m, m+1)$ *and* ψ_α *be defined on* N″ *as the functions* ψ_i *of* 7.14 *are defined on* N. *Further, set* $\chi_0=\chi_{2m+1}=1$ *and* $\psi_0=\psi_{2m+1}=1$. *Then on* N″ *on has*

a) $\chi_i=\psi_i+\psi_{i-1}$ *if* $1\leq i\leq m-1$.

b) $\chi_i=\psi_i+\psi_{i+1}$ *if* $m+2\leq i\leq 2m$.

c) $\chi_m=\psi_\alpha+\psi_{m-1}$.

d) $\chi_{m+1}=\psi_\alpha+\psi_{m+2}$.

1) *Let* ρ_i *be the* i^{th} *fundamental representation of* G *and* ρ'_i *that of* G′ (*according to the sequence* S *in* 9.12). *Then the restriction of* ρ_i *to* G′ *is isomorphic to the direct sum of* ρ'_i *and* ρ'_{i-1}. Here ρ'_0 is the trivial representation. We may identify G with SL(L) and G′ with the subgroup SL(L′)×SL(L″), if L′ and L″ are vector spaces of rank $2m$ and 1 and L is their direct sum. Then ρ_i is realized by the action of G on the space $\wedge^i L$ of skew tensors of rank i over L. Combining this with the canonical decomposition $\wedge^i L=\wedge^i L' \mathbin{\overset{\circ}{+}} \wedge^{i-1} L' \wedge L''$, we get 1).

We will use the notation D, V_ω, π_ω, etc. of 7.14.

2) *If* G *in* 7.14 *is of type* A_r, *then one has*:

a) *The only weight* ω *in* D *such that* $V_\omega\neq 0$ *if* $\omega=\omega_i$.

b) *The function* f_i *is* 0.

Using the realization of ρ_i as in 1), we see that the transforms of V_{ω_i} under the Weyl group W generate V_i. Since D is a fundamental domain for the action of W, this proves *a)*. Referring to the proof of 7.14, the contribution to $\chi_i(x)$ coming from step 5) is 0, by *a)*, whence *b)* follows.

3) *Proof of* 9.15. — Writing 1) in terms of characters, $\chi_i = \chi'_i + \chi'_{i-1}$, and then using 9.12 and 7.14 as refined in 2 *b)* above, for the group G′, we get 9.15.

9.16. *Lemma.* — *Let* ψ_i *and* ψ_α *be as in* 9.15, *but on* N‴ *instead of* N″. *Let* u_m *and* u_{m+1} *be so chosen that the final stage of* ψ_α *(isomorphism from* X_α *to* K*) maps the commutator* (u_{m+1}, u_m) *onto* 1. *Let* φ_α *denote the composition of the projection* $N''' \to T_\alpha$ *and the evaluation* $t \to \alpha_m(t)$ *(or* $\alpha_{m+1}(t)$*). Then on* N‴ *one has* a) *and* b) *of* 9.15 *and also*

c) $\chi_m = \varphi_\alpha \psi_\alpha + \psi_{m-1}$,

d) $\chi_{m+1} = \varphi_\alpha + \varphi_\alpha \psi_\alpha + \psi_{m+2}$.

1) *Assume that* $1 \leq i \leq m$. *Then there exist exactly two weights* ω *such that* $(\omega, \beta) \geq 0$ *for all* β *in the sequence* S *of* 9.12, *and* $V_\omega \neq 0$. *For both,* $\dim V_\omega = 1$. *One is the highest weight* ω_i *and the other, say* ω'_i, *is orthogonal to all terms of* S *but the* $(i-1)^{\text{th}}$. The highest weights of the representations ρ'_i and ρ'_{i-1} in 1) of 9.15 satisfy the first two statements by 2 *a)* of 9.15 and 7.15 *b)*. Finally ω_i must correspond to ρ'_i rather than ρ'_{i-1} because ω_i is not orthogonal to the i^{th} term of S.

Now let $x = y_\alpha \prod_j y_j = y_\alpha y$ be an element of N‴ with y_α in $u_{m+1} u_m X_\alpha \sigma_\alpha T_\alpha$ and y_j in $X_j \sigma_j$ $(j \neq m, m+1)$.

2) $\pi_\omega x \pi_\omega = \pi_\omega y_\alpha \pi_\omega \prod_j (\pi_\omega y_j \pi_\omega) = \pi_\omega y_\alpha \pi_\omega . \pi_\omega y \pi_\omega$.

The proof is like that of 2) in the proof of 7.14.

3) $\chi_i(x) = \sum_\omega \operatorname{tr} \pi_\omega x \pi_\omega$ $(\omega = \omega_i, \omega'_i)$. This follows from 1) above, by a proof like that of 6) of 7.14.

4) *Proof of* a). — Since $1 \leq i \leq m-1$, both ω_i and ω'_i in 1) are orthogonal to α_m, α_{m+1} and α. Thus if $\omega = \omega_i$ or ω'_i and z is any element of the group generated by G_m and G_{m+1}, then $\pi_\omega z \pi_\omega = 1$ on V_ω, whence $\pi_\omega x \pi_\omega = \pi_\omega \sigma_\alpha y \pi_\omega$, and by a slight extension of 3) we get $\chi_i(x) = \chi_i(\sigma_\alpha y)$. Here $\sigma_\alpha y$ is in N″, so that 9.15 *a)* may be applied. The result is *a)*.

5) *Proof of* c). — Here $i = m$. If $\omega = \omega'_m$, then ω is orthogonal to α, whence $\pi_\omega x \pi_\omega = \pi_\omega \sigma_\alpha y \pi_\omega$ as in 4). Now applying 7.14 as refined in 2 *b)* of the proof of 9.15 to the representation ρ'_{m-1} of G′ (see step 1) of 9.15), we get

$$(*) \qquad \operatorname{tr} \pi_\omega x \pi_\omega = \psi_{m-1}(x).$$

Assume now that $\omega = \omega_n$. We write $y_\alpha = u_{m+1} u_m u_\alpha \sigma_\alpha t_\alpha$ as in 9.11, and normalize the choices σ_m and σ_{m+1} so that they are in G_m and G_{m+1} and $\sigma_\alpha = \sigma_{m+1} \sigma_m \sigma_{m+1}^{-1}$, and then write $y_\alpha = z_1 z_2 z_3 t_\alpha$ with $z_1 = u_{m+1} \sigma_{m+1}$, and $z_2 = \sigma_{m+1}^{-1} u_\alpha \sigma_\alpha \sigma_{m+1}$, and $z_3 = \sigma_{m+1}^{-1} \sigma_\alpha^{-1} u_m \sigma_\alpha$. Here z_1 and z_3 are in G_{m+1}, while z_2 is in G_m. The factor t_α acts on V_ω as the scalar $\alpha_m(t_\alpha) = \varphi_\alpha(x)$. Then because ω is orthogonal to α_{m+1} the factor z_3 may be suppressed. By the independence of α_m and α_{m+1} (see 7.15 *d)*) we may also suppress z_1. Thus $\pi_\omega x \pi_\omega = \varphi_\alpha(x) \pi_\omega z_2 \pi_\omega = \varphi_\alpha(x) \psi_\alpha(x)$ on V_ω, by 4) of 7.14. Combining this with $(*)$ above, we get *c)*.

6) *Proof of* b) *and* d). — By applying to G an automorphism which fixes T and interchanges the roots α_i and α_{2n+1-i} $(1 \leq i \leq m)$, we get *b)* from *a)* and *d)* from *c)*, if we observe that in the latter case we must take the product of u_m and u_{m+1} in the opposite order, so that u_α in 5) above must be replaced by $(u_{m+1}, u_m)u_\alpha$, which because of the original assumption on this commutator yields the extra term φ_α.

9.17. *Remark.* — Observe that the extra term φ_α, which turns out to be just the term we need, owes its existence directly to the noncommutativity of X_m and X_{m+1}. This is only fair, since the present development does also.

9.18. *Corollary.* — $\sum_0^{n+1} (-1)^i \chi_i$ *is* 0 *on* N″ *and* $(-1)^{m+1}\varphi_\alpha$ *on* N‴.

If we use 9.15 and 9.16, then in the first case all terms cancel while in the second the one term remains.

One may also express 9.18 thus: if G is represented as $SL(n+1)$, the elements of N″ have 1 as a characteristic value, those of N‴ do not.

9.19. *Corollary.* — *Let* p *and* V *be as in* 6.10. *Let* f *be the function* $(c_1, \ldots, c_n) \to \sum_0^{n+1} (-1)^i c_i$ $(c_0 = c_{n+1} = 1)$, *and* V″ *and* V‴ *the subvarieties of* V *defined by* $f = 0$ *and* $f \neq 0$, *respectively.*

a) p *maps* N″ *and* N‴ *isomorphically onto* V″ *and* V‴.

b) *All elements of* N‴ *are regular.*

The functions ψ_i $(i \neq m, m+1)$ and ψ_α may be used as coordinates on N″ by 9.12 and 7.1. So may the functions χ_i $(i \neq m)$, in terms of which the first set may be expressed by the recursive solution of *a)*, *b)* and *d)* of 9.15. The latter functions are the images under p of the canonical coordinates of V excluding the m^{th}, which may be taken as coordinates on V″. Thus p maps N″ isomorphically onto V″. The proof for N‴ and V‴ is similar: first we normalize u_m and u_{m+1} as in 9.16, which is permissible by 9.4, and then in 9.16 we solve in turn for φ_α (see 9.18), ψ_i and $\varphi_\alpha\psi_\alpha$. The second isomorphism in *a)* implies that the differentials $d\chi_i$ are independent at all points of N‴, whence 1.5 implies *b)*.

9.20. *Remark.* — One can show that the regular elements of N″ are those for which $\sum_0^{n+1} (-1)^j j \chi_j \neq 0$.

Now we can prove 9.7 and 9.11. By 9.13 we have *a)*, and by 9.19 we have *b)* and *c)*, thus by *b)* also *d)*. The argument using k_1 and Γ_1 in the proof of 9.4 may be used to reduce the proof of *e)* to the case in which G consists of a single component. Proceeding as in the proof of 9.4 we are reduced to proving that the part of N″ and N‴ corresponding to the indices m, $m+1$, and α can be constructed over k. Since α is over k, so are T_α and X_α, and we can form $X_\alpha\sigma_\alpha$ over k by 9.3. Finally, by Hilbert's theorem [11, p. 159] and the k_1, Γ_1 reduction referred to above, we can choose u_m and u_{m+1} in 9.11 so that the class of $u_m u_{m+1}$ in $X_m X_{m+1} X_\alpha / X_\alpha$ is over k, whence *e)*.

§ 10. Some cohomological applications

The convention in § 9 concerning k and K continues.

First we prove 1.8. We recall that $H^1(k, G)$ consists of all cocycles from the Galois group Γ to the group G, that is, functions $\gamma \to x_\gamma$ which satisfy 9.3, modulo the equivalence relation, $(x_\gamma) \sim (x'_\gamma)$ if $x'_\gamma = a^{-1} x_\gamma \gamma(a)$ for some a in G and all γ in Γ. For the significance of this concept, as well as its basic properties, the reader is referred to [11, 12, 13]. We start with an arbitrary cocycle (x_γ) and wish to construct an equivalent one with values in a torus over k. Assume first that k is finite. Let q be the order of k, and β the q^{th} power homomorphism. By Lang's theorem [5] there exists a in G such that $a^{-1} x_\beta \beta(a) = 1$. Since β and any subgroup Γ_1 of finite index generate Γ (in other words, the Galois group of any finite extension of k is generated by the restriction of β), it follows from 9.3 *b)* that $a^{-1} x_\gamma \gamma(a) = 1$ for all γ, whence $(x_\gamma) \sim (1)$. Assume now that k is infinite. We form $x(G)$, the group G twisted by the cocycle x (see, e.g., [13]). This is a group over k, isomorphic to G over K. If $x(G)$ is identified with G, then γ in Γ acts on $x(G)$ as $x(\gamma) = i(x_\gamma) \circ \gamma$; here $i(x_\gamma)$ denotes the inner automorphism by x_γ. By 2.15 and the Rosenlicht density theorem [6, p. 44] there exists in $x(G)$ an element y which is strongly regular and over k. Thus

$(*) i(x_\gamma)\gamma(y) = y$ for all γ in Γ.

Hence the conjugacy class of y in G is over k, whence by 1.7 it contains an element z over k. Writing $y = i(a)z$, with a in G, and substituting into $(*)$, we conclude that $a^{-1} x_\gamma \gamma(a)$ is in the centralizer of z, a torus because z is strongly regular, and over k because z is, whence 1.8.

10.1. *Corollary. — The assumption of semisimplicity in* 1.8 *can be dropped. In other words,* G *can be any simply connected, connected linear group with a Borel subgroup over* k.

By applying the semisimple case to G divided by its radical, we are reduced to the case in which G is solvable, which we henceforth assume. As in 9.4 we can find a Cartan subgroup C over k, and then the unique maximal torus T of C is over k and maximal also in G (see [8, p. 7-01 to p. 7-04]), whence we have over k the decomposition $G = UT$, with U the unique maximal unipotent subgroup. Now let $\gamma \to x_\gamma = u_\gamma t_\gamma$ be a cocycle. Then (t_γ) is also a cocycle, and (u_γ) is a cocycle in the group U twisted by (t_γ). Since U is unipotent, the last cocycle is trivial: $u_\gamma = a t_\gamma \gamma(a)^{-1} t_\gamma^{-1}$ for some a in U, by [12, Prop. 3.11]. Then $(x_\gamma) = (a t_\gamma \gamma(a)^{-1}) \sim (t_\gamma)$, whence 10.1 follows.

Next we consider 1.9. Assume that *a)* holds. By [12, Prop. 3.1.2] we have $H^1(k, G) = 0$ in case G is a torus, hence, by 1.8, also in case G is simply connected, semisimple, and contains a Borel subgroup over k, and then, by [12, Prop. 3.1.4], in case " simply connected " is replaced by " adjoint ". Now if G is an arbitrary semisimple adjoint group (over k, of course), there exists a group G_0 split over k and isomorphic to G over K, and the argument of [13, p. III-12] together with $H^1(k, G_0) = 0$ shows that G contains a Borel subgroup over k, whence $H^1(k, G) = 0$ by the result above. By [12, Prop. 3.1.4 Cor.] it now follows that *b)* holds in general. Now a result of

Springer [13, p. III-16, Th. 3] asserts that if $\dim k \leq 1$ and G and S are as in *c)*, then there exists a principal homogeneous space P and a G-map from P to S, all over k. By *b)*, P has a point over k, hence so does S, whence *c)*.

10.2. *Corollary. — Let k be a perfect field of* $\dim \leq 1$, *and* G *a connected linear group over k.*

a) G *contains a Borel subgroup over k.*

b) *Each conjugacy class over k contains an element over k.*

Observe that *b)* is the same as 1.10. Both results follow from 1.9. In the first case we take as the homogeneous space the variety of Borel subgroups, in the second case the conjugacy class under consideration.

10.3. *Corollary. — If k is as above and* G *is simply connected, the natural map from the set of semisimple classes of* G_k *to the set of semisimple classes of* G *over k is bijective.*

By 10.2 *a)* and 9.9 the map is surjective. To prove injectivity we must show that if x and y are semisimple elements of G_k which are conjugate in G they are also conjugate in G_k. We have $axa^{-1}=y$ with a in G. Then for γ in Γ we have $\gamma(a)x\gamma(a)^{-1}=y$, whence $a^{-1}\gamma(a)$ is in G_x. Now $\gamma \to a^{-1}\gamma(a)$ is a cocycle and G_x is connected (cf. 2.10), and over k because x is. Thus by 1.9 there exists b in G_x such that $b^{-1}a^{-1}\gamma(a)\gamma(b)=1$ for all γ. Thus ab is over k, and x and y are conjugate in G_k, under ab in fact, whence 10.3.

10.4. *Remarks. — a)* For regular classes 10.3 is false, since regular elements of G_k conjugate in G need not be conjugate in G_k.

b) For the split adjoint group of type A_r over any field k one can show, by the usual normal forms, that any elements of G_k, semisimple or not, are conjugate in G_k if they are conjugate in G. Does the same result hold for the other simple types, and is it enough to assume a Borel subgroup over k?

§ 11. Added in proof

M. Kneser has informed me that in 1.8 the assumption that G is simply connected can be dropped. If k is finite, the proof is as before (see § 10). If k is infinite, the key point is that the group $x(G)$ of the proof of 1.8 can be constructed even if (x_γ) is only a cocycle modulo the centre of G, so that if G is simply connected such a " cocycle " is equivalent to one with values in a torus over k. By applying this to the simply connected covering group of a group which is as in 1.8 but not simply connected, we get the improved version of 1.8. Proceeding then as in the proof of 10.1 we can drop the assumption of semisimplicity. The result is:

11.1. *Theorem. — Let k be a perfect field and* G *a connected linear group which is over k and contains a Borel subgroup over k. Then each element of* $H^1(k, G)$ *can be represented by a cocycle whose values are in a torus over k.*

Using 11.1 we now give a simplified proof of the implication *a)*$\to$*b)* of 1.9. The assumption $\dim k \leq 1$ is used only in the proof, for which we refer the reader to [12, Prop. 3.1.2], that $H^1(k, G)=0$ if G is a torus over k, since we show:

11.2. *Theorem. — Let k be a perfect field and n a positive integer such that* $H^1(k, T)=0$ *for every torus* T *of rank n and over k. Then* $H^1(k, G)=0$ *for every connected linear group* G *of rank n and over k.*

By 11.1 and the assumption in 11.2 we have

(*) $H^1(k, G)=0$ if G in 11.2 contains a Borel subgroup over k.

In the general case let R be the radical of G and Z the centre of G/R. There exists a group G_0 (the split one, e.g.) which is over k and contains a Borel subgroup B over k, and an isomorphism φ over K of G_0 onto $(G/R)/Z$. Since G_0 is a centreless semisimple group, we have the split extension $\mathrm{Aut}\, G_0=G_0E$, in which E is a finite group which fixes B (see [8, p. 17-07, Prop. 1]). For $\gamma\in\Gamma$, write $\varphi^{-1}\gamma(\varphi)=g_\gamma e_\gamma(g_\gamma\in G_0,\, e_\gamma\in E)$. Then (e_γ) is a cocycle and (g_γ) is a cocycle in the group G_0 twisted by (e_γ). In this group (g_γ) is equivalent to the trivial cocycle by (*) because B is over k. Thus $(g_\gamma e_\gamma)$ is equivalent to (e_γ) in $H^1(k, \mathrm{Aut}\, G_0)$, whence φ may be normalized so that $\varphi^{-1}\gamma(\varphi)=e_\gamma$. Then φB is a Borel subgroup over k in $(G/R)/Z$, and its inverse image is one in G, whence $H^1(k, G)=0$ by (*).

BIBLIOGRAPHY

[1] A. Borel, Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes, *Tôhoku Math. J.*, 13 (1961), 216-240.

[2] S. Helgason, *Differential geometry and symmetric spaces*, Academic Press, New York (1962).

[3] B. Kostant, The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *Amer. J. Math.*, 81 (1959), 973-1032.

[4] —, Lie group representations on polynomial rings, *Amer. J. Math.*, 85 (1963), 327-404.

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

[6] M. Rosenlicht, Some rationality questions on algebraic groups, *Ann. di Mat.*, 43 (1957), 25-50.

[7] —, On quotient varieties and the affine imbedding of certain homogeneous spaces, *Trans. Amer. Math. Soc.*, 101 (1961), 211-223.

[8] Séminaire C. Chevalley, *Classification des Groupes de Lie algébriques* (two volumes), Paris (1956-58).

[9] Séminaire « Sophus Lie », *Théorie des algèbres de Lie...*, Paris (1954-5).

[10] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris (1959).

[11] —, *Corps locaux*, Hermann, Paris (1962).

[12] —, Cohomologie galoisienne des groupes algébriques linéaires, *Colloque sur la théorie des groupes algébriques*, Bruxelles (1962), 53-68.

[13] —, *Cohomologie galoisienne*, Cours fait au Collège de France ((1962-3).

[14] D. A. Smith, *Dissertation*, Yale University (1963).

[15] T. A. Springer, Quelques résultats sur la cohomologie galoisienne, *Colloque sur la théorie des groupes algébriques*, Bruxelles (1962), 129-135.

[16] R. Steinberg, Finite reflection groups, *Trans. Amer. Math. Soc.*, 91 (1959), 493-504.

[17] —, Representations of algebraic groups, *Nagoya Math. J.*, 22 (1963), 33-56.

[18] H. Weyl, Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen III, *Math. Zeit.* (1926), 377-395.

University of California, Los Angeles.

Reçu le 25-8-1964.