Journal of the Mathematical Society of Japan Vol. 6, Nos. 3~4, December, 1954

On algebraic group varieties.

By C. CHEVALLEY

(Received March 3, 1954)

Let G be a linear algebraic group of dimension r. We propose to study the brational type of G as an algebraic variety, i. e. the structure of the field $\mathfrak{R}(G)$ of rational functions on G. In his "Traité d'analyse" (vol. 3, p. 550), E. Picard shows that it is possible to express the coordinates of a point of G as rational functions of r parameters. The proof depends however on the basic field of the group being that of complex numbers; moreover, it is not proved that the parametric representation one obtains is proper (i. e. that a given point of the group corresponds in general to only one system of values of the parameters). In other words, the proof shows that $\mathfrak{R}(G)$ is contained in a purely transcendental extension of transcendence degree r of the basic field, but not that it is itself purely transcendental.

In this paper, we shall prove that, for any basic field (of characteristic 0), the field $\mathfrak{R}(G)$ is contained in some purely transcendental extension of transcendence degree r of the basic field. We shall also establish that, when the basic field is algebraically closed, $\mathfrak{R}(G)$ is itself purely transcendental, while, if the basic field is arbitrary, it may happen that $\mathfrak{R}(G)$ is not purely transcendental.

In what follows, we denote by G an irreducible algebraic group of dimension r composed of automorphisms of a finite dimensional vector space V over a field K of characteristic 0; we denote by $\mathfrak{g}$ the Lie algebra of G.

I. A reduction of the problem.

Let $\mathfrak{n}$ be the largest ideal of $\mathfrak{g}$ composed of nilpotent endomorphisms of V ([1], V, th. 3, 2). Then we have a direct sum decomposition $\mathfrak{g}=\mathfrak{n}+\mathfrak{b}+\mathfrak{s}$ of $\mathfrak{g}$ with the following properties: $\mathfrak{b}$ is an algebraic abelian subalgebra of the radical of $\mathfrak{g}$ whose elements are semi-simple; $\mathfrak{s}$ is a semi-simple subalgebra of $\mathfrak{g}$ whose elements commute with those of $\mathfrak{b}$

([1], V, prop. 5, 4). We set $\mathfrak{a}=\mathfrak{b}+\mathfrak{s}$; $\mathfrak{a}$ is therefore a reductive algebra of center $\mathfrak{b}$. Since $\mathfrak{s}$ is semi-simple, it is algebraic ([1], IV, cor. to prop. 9, 2); it follows that $\mathfrak{a}$ is algebraic ([1], II, th. 14, 14). The representation of $\mathfrak{g}$ on V induces a semi-simple representation of $\mathfrak{a}$ ([1], IV, th. 4, 4).

Since the elements of $\mathfrak{n}$ are nilpotent, $\mathfrak{n}$ is algebraic ([1], V, prop. 14, 3). Let N and A be the irreducible algebraic groups of automorphisms of V whose Lie algebras are $\mathfrak{n}$ and $\mathfrak{a}$ respectively. We propose to prove that any $s \in G$ may be written in one and only one way in the form na, with $n \in N$, $a \in A$.

Let $(V_0=V, V_1,\cdots, V_h=\{0\})$ be a Jordan-Hölder sequence for the representation space V of $\mathfrak{g}$; thus, each V_i is mapped into itself by the operations of $\mathfrak{g}$, and V_{i-1}/V_i is the space of a simple representation ρ_i of $\mathfrak{g}$. Since G is irreducible, V_i is mapped into itself by the operations of G ([1], III, cor. 1 to th. 1); thus, V_{i-1}/V_i is the space of a representation P_i of G; P_i is simple and rational, and its differential is ρ_i ([1], III, lemma 3). Let P be the Cartesian product of the representations $\mathrm{P}_i\,(1 \leqq i \leqq h)$; this is a rational representation of G whose differential is the Cartesian sum ρ of the representations ρ_i. Let Σ (resp.: σ) be the representation of G (resp.: $\mathfrak{g}$) on the space V (i. e. the identity mapping of G (resp.: $\mathfrak{g}$) into the set of endomorphisms of V). Then we shall see that ρ and σ induce equivalent representations of $\mathfrak{a}$. Since σ induces a semi-simple representation of $\mathfrak{a}$, there exists for each i a subspace W_i of V_{i-1} which is mapped into itself by the operations of $\mathfrak{a}$ and which is supplementary to V_i in $V_{i-1}\,(1 \leqq i \leqq h)$. If $X \in \mathfrak{a}$, let $\rho_i'(X)$ be the restriction of X to W_i; then the representation of $\mathfrak{a}$ induced by ρ_i is obviously equivalent to ρ_i'. On the other hand, V is the direct sum of the spaces $W_1,\cdots, W_h$; the representation of $\mathfrak{a}$ induced by σ is therefore equivalent to the Cartesian sum of the representations $\rho_i'\,(1 \leqq i \leqq h)$, which is itself equivalent to ρ. More precisely, let J_i be the isomorphism of W_i with V_{i-1}/V_i induced by the natural mapping of V_{i-1} onto V_{i-1}/V_i; denote by U the product of the spaces V_{i-1}/V_i $(1 \leqq i \leqq h)$—i. e. the space of the representation ρ—and by J the isomorphism of V with U defined by $J(w_1+\cdots+w_h)=(J_1\cdot w_1,\cdots, J_h\cdot w_h)$ $(w_i \in W_i,\ 1 \leqq i \leqq h)$. Then, for $X \in \mathfrak{a}$, we have $\rho(X)=JXJ^{-1}$. It follows that, for any $a \in A$, $\mathrm{P}(a)=JaJ^{-1}$. The group $\mathrm{P}(A)=JAJ^{-1}$ is therefore the irreducible algebraic group of automorphisms of U whose

Lie algebra is $\rho(\mathfrak{a})$ (it will be observed that, in general, if P' is a rational representation of A, $\mathrm{P}'(A)$ need not be an algebraic group). Now, we observe that $\rho(\mathfrak{n})=\{0\}$ ([1], V, Th. 3, 2), whence $\rho(\mathfrak{g})=\rho(\mathfrak{a})$. It follows that $\mathrm{P}(G)$ is contained in the irredusible algebraic group whose Lie algebra is $\rho(\mathfrak{a})$,i. e. in $JAJ^{-1}=\mathrm{P}(A)$; since $A\subset G$, we have $\mathrm{P}(G)=\mathrm{P}(A)$.

Now, let N' be the kernel of the representation P of G. Then N' is the group of elements $s\in G$ such that, for any $i\,(1\leq i\leq h)$ and any $x\in V_{i-1}$, $s\cdot x\equiv x$ (mod. V_i); this implies that, if I is the identity mapping, then $(s-I)^h=0$. Therefore, the smallest algebraic group containing it is irreducible ([1], II, prop. 5, 14) and N' is irreducible. Moreover, the elements of the Lie algebra $\mathfrak{n}'$ of N' are nilpotent; since $\mathfrak{n}'$ is an ideal, $\mathfrak{n}'\subset\mathfrak{n}$. Conversely, $\mathfrak{n}$ is in the kernel of ρ, from which it follows that N is in the kernel of P. This proves that $N'=N$.

Let s be any element of G. Since $\mathrm{P}(G)=\mathrm{P}(A)$, there is an $a\in A$ such that $\mathrm{P}(a)=\mathrm{P}(s)$; then, sa^{-1} belongs to the kernel N of P, which shows that $s\in NA$. In order to prove that the representation of an $s\in G$ in the form na, with $n\in N$, $a\in A$, is unique, it will be sufficent to show that N and A have only the unit element in common. If $n\in N$, then $n-I$ is nilpotent; we may write $n-I=\exp X$, where X is a nilpotent endomorphism of V which belongs to the Lie algebra of any algebraic group containing n ([1], II, prop. 5, 14); thus, $X\in\mathfrak{n}\cap\mathfrak{a}=\{0\}$, and $n=I$.

Let K' be an overfield of K. If M is a vector space, or a Lie algebra, or an algebraic group over K, we shall denote by $M^{K'}$ the vector space, the Lie algebra or the algebraic group over K' which results from M by extending the basic field to K'. Then $\mathfrak{n}^{K'}$ is the largest ideal of $\mathfrak{g}^{K'}$ composed of nilpotent elements ([1], V, prop. 10, 2). The algebra $\mathfrak{a}^{K'}$ is reductive ([1], IV, prop. 8, 4), while $\mathfrak{s}^{K'}$ is semi-simple ([1], IV, prop. 10, 2). The algebra $\mathfrak{b}^{K'}$ is abelian and algebraic, and its elements commute with those of $\mathfrak{s}^{K'}$; since $\mathfrak{a}^{K'}=\mathfrak{b}^{K'}+\mathfrak{s}^{K'}$, $\mathfrak{b}^{K'}$ is the center of $\mathfrak{a}^{K'}$. The elements of $\mathfrak{b}^{K'}$ are semi-simple ([1], I, prop. 1 and 4, 8). Thus we see that every element of $G^{K'}$ is uniquely representable in the form $n'a'$, with $n'\in N^{K'}$, $a'\in A^{K'}$. We shall apply this to the following case. Let s be a generic point of G relatively to K, and $K'=K(s)$; then $s\in G^{K'}$, and we may write $s=na$, $n\in N^{K'}$, $a\in A^{K'}$. It follows from this formula that $K'=K(s)\subset K(n, a)$ (the field obtained by adjunction to K of the coordinates of n, a with respect to some base of the space of endomorphisms of V). Since $K(n)$ and $K(a)$ are in K', we have $K'=K(n, a)$. Let p and q be the dimensions of $\mathfrak{n}$ and $\mathfrak{a}$; since $n \in N^{K'}$, $a \in A^{K'}$, the transcendence degree p' (resp.. q') of $K(n)$ (resp.: $K(a)$) over K is $\leq p$ (resp.: $\leq q$). The transcendence degree of $K'=K(n, a)$ is therefore $\leq p'+q'$; but, since s is generic, this transcendence degree is the dimension $p+q$ of $\mathfrak{g}$. It follows that $p'=p$, $q'=q$, and that any transcendence base of $K(n)$ over K is also a transcendence base of $K(s)$ over $K(a)$. In particular, n and a are generic points of N and A respectively, from which it follows that $K(n)$ and $K(a)$ are respectively isomorphic (as algebras over K) to the fields of rational functions on N and A. Similarly, $K(s)$ is isomorphic to the field of rational functions on G. Making use of prop, 14, [1], V, 3, we see that $K(n)/K$ is a purely transcendental extension. We have therefore proved the following result:

PROPOSITION 1. *Let G be an irreducible algebraic group of automorphisms of a vector space, and let $\mathfrak{g}$ be its Lie algebra. Let $\mathfrak{n}$ be the largest ideal of $\mathfrak{g}$ composed of nilpotent elements, and let $\mathfrak{g}=\mathfrak{n}+\mathfrak{b}+\mathfrak{s}$ be a direct sum decomposition with the following properties: $\mathfrak{b}$ is algebraic and abelian, and its elements are semi-simple, $\mathfrak{s}$ is semi-simple and its elements commute with those of $\mathfrak{b}$. Set $\mathfrak{a}=\mathfrak{b}+\mathfrak{s}$, and let A be the irreducible algebraic subgroup of G whose Lie algebra is $\mathfrak{a}$. Then the field of rational functions on G is a purely transcendental extension of a field isomorphic to the field of rational functions on A.*

II. Reductive algebras of type (D).

Let now G be an irreducible algebraic group of automorphisms of V such that the representation of G on V is semi-simple. Let $\mathfrak{g}$ be the Lie algebra of G; $\mathfrak{g}$ is therefore reductive, and the elements of the center $\mathfrak{z}$ of $\mathfrak{g}$ are semi-simple endomorphisms of V ([1], IV, th. 4, 4). Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$; then $\mathfrak{h}$ contains $\mathfrak{z}$ ([1], VI, prop. 4, 4). The derived algebra $\mathfrak{s}$ of $\mathfrak{g}$ is semi-simple, and $\mathfrak{g}=\mathfrak{z}+\mathfrak{s}$; making use of prop. 20, [1], VI, 4, we see that $\mathfrak{h}$ is the direct sum of $\mathfrak{z}$ and of a Cartan subalgebra $\mathfrak{h}_{\mathfrak{s}}$ of $\mathfrak{s}$. We shall say that $\mathfrak{g}$ is an *algebra of type* (D) if $\mathfrak{g}$ has a Cartan subalgebra $\mathfrak{h}$ with the following property: for any $X \in \mathfrak{h}$, the characteristic polynomial of the endomorphism X of

V splits into linears factors with coefficient in K. This condition is obviously satisfied if K is algebraically closed.

THEOREM 1. *Let G be an irreducible algebraic group of automorphisms of a finite dimensional vector space V over a field K of characteristic* 0. *Assume that the representation of G on V is semi-simple and that the Lie algebra $\mathfrak{g}$ of G is of type* (D). *Then the field of rational functions on G is purely transcendental over K.*

Under our assumption, there exists a base of V composed of vectors which are eigenvectors for all operations in $\mathfrak{h}$, as follows immediately from the fact that $\mathfrak{h}$ is abelian. Let $(x_1,\cdots,x_n)$ be such a base. The algebra $\mathfrak{h}$ is the Lie algebra of a Cartan subgroup H of G, which is an irreducible algebraic abelian subgroup of G ([1], VI, prop. 5 and th. 2, 4). Each x_i is an eigenvector for all operations in H ([1], III, cor. 1 to th. 1). If $s \in H$, set $s \cdot x_i = u_i(s)x_i$, $u_i(s) \in K (1 \leqq i \leqq n)$; then, each u_i is a rational function on H, and the field $\mathfrak{R}(H)$ of rational functions on H is $\mathfrak{R}(H) = K(u_1,\cdots,u_n)$. If $X \in \mathfrak{h}$, set $X \cdot x_i = v_i(X)x_i$ $(1 \leqq i \leqq n)$. Let Z^n be the product of n times the additive group Z of integers by itself; let Λ be the subgroup of Z^n composed of those elements $(e_1,\cdots,e_n)$ such that $\sum_{i=1}^n e_i v_i(X) = 0$ for all $X \in \mathfrak{h}$. Taking into account the fact that H is irreducible, it follows from prop. 3, [1], II, 13 that $\prod_{i=1}^n u_i^{e_i} = 1$ for any $(e_1,\cdots,e_n) \in \Lambda$ and that H is the group of all automorphisms s of V with the following properties: we have $s \cdot x_i = c_i x_i$ $(1 \leqq i \leqq n)$ with elements $c_i \in K$ such that $\prod_{i=1}^n c_i^{e_i} = 1$ for all $(e_1 \cdots, e_n) \in \Lambda$. If $w = (w_1,\cdots,w_n)$ is a sequence of n elements $\neq 0$ of a field and $e = (e_1,\cdots,e_n)$ an element of Z^n, we shall set $w^e = \prod_{i=1}^n w_i^{e_i}$. It is clear that Z^n/Λ has no element $\neq 0$ of finite order; Z^n is therefore the direct sum of Λ and of a subgroup W of Z^n. The functions of the form $(u_1,\cdots,u_n)^e$ $(e \in Z^n)$ form a subgroup U of the group of elements $\neq 0$ in $\mathfrak{R}(H)$; $u_1,\cdots,u_n$ belong to this group, as seen by taking for e an element whose coordinates are all 0 except for one which has the value 1. It follows that $\mathfrak{R}(H) = K(U)$. We have $(u_1,\cdots,u_n)^e = 1$ if $e \in \Lambda$; since $Z^n = \Lambda + W$, U is the set of elements $(u_1,\cdots,u_n)^f$ for all $f \in W$. Let $f(1),\cdots,f(p)$ be a base of W; set $z_k = (u_1,\cdots,u_n)^{f(k)}$ $(1 \leqq k \leqq p)$; then it is clear that $\mathfrak{R}(H) = K(z_1,\cdots,z_p)$. We shall see that $z_1,\cdots,z_p$ are algebraically independent over K. It will obviously be sufficient to prove that, if $d_1,\cdots,d_p$ are any elements $\neq 0$ of K, then there exists an $s \in G$ such that $z_k(s) = d_k$ $(1 \leqq k \leqq p)$. Let K^* be the multiplicative group of elements $\neq 0$ in K; then there is a homomorphism of W into K^* which maps $f(k)$ upon d_k $(1 \leqq k \leqq p)$. Since Z^n is the direct sum of Λ and W, this homomorphism may be extended to a homomorphism θ of Z^n into K^* which maps the elements of Λ upon 1. Set $c_i = \theta((0,\cdots,1,\cdots,0))$ $(1 \leqq i \leqq n)$; then we have $(c_1,\cdots,c_n)^e = 1$ for all $e \in \Lambda$ and $(c_1,\cdots,c_n)^{f(k)} = d_k$ $(1 \leqq k \leqq p)$. It follows that there exists an $s \in G$ such that $u_i(s) = c_i$ $(1 \leqq i \leqq n)$ and that $z_k(s) = d_k$ $(1 \leqq k \leqq p)$, which proves our assertion. Thus we see that the field $\mathfrak{R}(H)$ of rational functions on H is purely transcendental over K.

Let K' be an algebraically closed overfield of K. Then $V^{K'}$ is the space of a representation of the semi-simple algebra $\mathfrak{s}^{K'}$. Each one of the linear functions v_i on $\mathfrak{h}$ introduced above extends to a linear function, still denoted by v_i, on $\mathfrak{h}^{K'}$. Since $\mathfrak{h}_{\mathfrak{s}}$ is a Cartan subalgebra of $\mathfrak{s}$, $\mathfrak{h}_{\mathfrak{s}}^{K'}$ is a Cartan subalgebra of $\mathfrak{s}_{\mathfrak{s}}^{K'}$ ([1], VI, prop. 22, 4). The restrictions to $\mathfrak{h}_{\mathfrak{s}}^{K'}$ of the functions v_i are the weights of the representation of $\mathfrak{s}^{K'}$ on $V^{K'}$. Let l be the rank of $\mathfrak{s}$, i.e. also of $\mathfrak{s}^{K'}$; this is also the dimension of $\mathfrak{h}_{\mathfrak{s}}^{K'}$. The representation of $\mathfrak{h}_{\mathfrak{s}}^{K'}$ on $V^{K'}$ being faithful, there are at least l of the restrictions v_i' to $\mathfrak{h}_{\mathfrak{s}}^{K'}$ of the functions v_i which are linearly independent. Now, it is well known that any weight of any representation of $\mathfrak{s}^{K'}$ is a linear combination with rational coefficients of the roots of $\mathfrak{s}^{K'}$ with respect to $\mathfrak{h}_{\mathfrak{s}}^{K'}$. Since there are l of the functions v_i' which are linearly independent, it follows that all roots of $\mathfrak{s}^{K'}$ are linear combinations with rational coefficients of these functions. In particular, any root of $\mathfrak{s}^{K'}$ with respect to $\mathfrak{h}_{\mathfrak{s}}^{K'}$ is the extension to $\mathfrak{h}_{\mathfrak{s}}^{K'}$ of some linear function on $\mathfrak{h}_{\mathfrak{s}}$. It follows immediately that, for any such root α, we can find an element X_α of $\mathfrak{s}$ which belongs to α, i.e. such that $[X, X_\alpha] = \alpha(X)X_\alpha$ for all $X \in \mathfrak{h}_{\mathfrak{s}}$ (and $X_\alpha \neq 0$). On the other hand, it is well known that it is possible to define an order relation on the additive group of all linear combinations with rational coefficients of the roots of $\mathfrak{s}^{K'}$ with the property that this group becomes an ordered group and that every root $\neq 0$ is either >0 or <0 relatively to this order relation. Let $\mathfrak{n}_+$ (resp.: $\mathfrak{n}_-$) be the subspace of $\mathfrak{s}$ spanned by the elements which belong to roots >0 (resp.: <0). Then $\mathfrak{s}$ is the direct sum $\mathfrak{n}_- + \mathfrak{h}_{\mathfrak{s}} + \mathfrak{n}_+$, and $\mathfrak{g}$ is the direct sum $\mathfrak{n}_- + \mathfrak{h} + \mathfrak{n}_+$. If elements X_α, X_β of $\mathfrak{s}$ belong to roots α, β, then $[X_\alpha, X_\beta]$ is either 0 or an element belonging to the root $\alpha + \beta$; it follows immediately that $\mathfrak{n}_+$ and $\mathfrak{n}_-$ are subalgebras of $\mathfrak{g}$. We shall see that every element of $\mathfrak{n}_+$

is nilpotent. If X_α belongs to a root α, then $X_\alpha \cdot x_i$ is a linear combination of the vectors x_j for which $v'_j = v'_i + \alpha$. It follows that, if $X \in \mathfrak{n}_+$, then, for any i, and for any $k > 0$, $X^k \cdot x_i$ is a linear combination of the vectors x_j with the property that $v'_j - v'_i$ is a sum of k roots >0. Since there are only a finite number of functions v'_i, we can find an integer k such that none of the differences $v'_j - v'_i$ $(1 \leqq i, j \leqq n)$ is expressible as the sum of k roots >0, and we then have $X^k = 0$ for all $X \in \mathfrak{n}_+$. We would see in the same way that all ele ments in $\mathfrak{n}_-$ are nilpotent.

It follows that $\mathfrak{n}_+$ and $\mathfrak{n}_-$ are algebraic subalgebras of $\mathfrak{g}$ ([1], V, prop. 14, 3). Set $\mathfrak{c} = \mathfrak{h} + \mathfrak{n}_+$; then $\mathfrak{c}$ is an algebraic subalgebra of $\mathfrak{g}$ ([1], II, th. 14, 14). The elements of $\mathfrak{h}$ being semi-simple endomorphisms of V, it is clear that $\mathfrak{n}_+$ is the largest ideal of $\mathfrak{c}$ composed of nilpotent elements. Let N_-, N_+, C be the irreducible algebraic subgroups of G whose Lie algebras are $\mathfrak{n}_-, \mathfrak{n}_+$ and $\mathfrak{c}$. Making use of prop. 1, 1, we see that the field $\mathfrak{R}(C)$ of rational functions on C is a purely transcendental extension of a field isomorphic to $\mathfrak{R}(H)$, and is therefore purely transcendental over K. The subgroup $N_- \cap C$ of N_- is irreducible ([1], VI, cor. 1 to prop. 14, 3); its Lie algebra is contained in $\mathfrak{n}_- \cap \mathfrak{c} = \{0\}$, from which it follows that $N_- \cap C$ contains only the neutral element I.

Let Ω be any overfield of K; then the elements of $\mathfrak{n}_-^\Omega$ are nilpotent ([1], VI, prop. 10, 2). Therefore, by the argument we have just used, $N_-^\Omega \cap C^\Omega$ is irreducible, whence $N_-^\Omega \cap C^\Omega = \{I\}$. Now, let c be a generic point of C, and let n_- be a generic point of $N_-^{K(c)}$ with respect to $K(c)$. Set $s = n_- c$, and let Ω be an algebraically closed overfield of $K(n_-, c)$, whence $K(s) \subset \Omega$. We assert that $K(n_-)$ and $K(c)$ are contained in $K(s)$ It will be sufficient to prove that the elements of these fields are left fixed by any automorphism of $\Omega/K(s)$. Let σ be such an automorphism. Denote by n_-^σ, c^σ and s^σ the automorphisms of V^Ω whose coordinates (with respect to a base in the space of endomorphisms of V) are the images of the coordinates of n_-, c and s under σ. Then we have $s = s^\sigma$ since σ leaves the elements of $K(s)$ fixed. Since $s = n_- c$, we have $n_-^\sigma c^\sigma = n_- c$, whence $n_-^{-1} n_-^\sigma = c(c^\sigma)^{-1}$. Since n_- belongs to N_-^Ω, which may be defined by a set of equations with coefficients in K, n_-^σ likely belongs to N_-^Ω; similarly c^σ belong to C^Ω. Thus $n_-^{-1} n_-^\sigma$ is in N^Ω, while $c(c^\sigma)^{-1} \in C^\Omega$. It follows that $n_- = n_-^\sigma$ and $c = c^\sigma$. Since $K(n_-)$ (resp.: $K(c)$) is generated by the coordinates of n_- (resp.: c) with respect to a base of the space of endomorphisms of V, we see that σ leaves all elements of either one of the fields $K(n_-)$ or $K(c)$ fixed, which proves our assertion.

It follows that $K(s)=K(n_-, c)$. The transcendence degree of $K(n_-, c)$ with respect to $K(c)$ is equal to the dimension of $N_-^{K(c)}$, i. e. also to the dimension of $\mathfrak{n}_-$. The transcendence degree of $K(c)$ over K is the dimension of $\mathfrak{c}$. Since $\mathfrak{g}$ is the direct sum $\mathfrak{n}_-+\mathfrak{c}$, we conclude that the transcendence degree of $K(s)=K(n_-, c)$ over K is equal to the dimension of $\mathfrak{g}$ i. e. to that of G, and therefore that s is a generic point of G over K. Therefore, $K(s)$ is isomorphic (as an algebra over K) to the field $\mathfrak{R}(G)$ of rational functions of G. The field $K(c)$ is isomorphic to $\mathfrak{R}(C)$, and $K(n_-, c)$ is isomorphic (as an algebra over $K(c)$) to the field of rational functions on $N_-^{K(c)}$. But the elements of $\mathfrak{n}_-^{K(c)}$ are all nilpotent; it follows that $\mathfrak{R}(N_-^{K(c)})$ is purely transcendental over $K(c)$ ([1], VI, prop. 14, 2). Therefore, $\mathfrak{R}(G)$ is purely transcendental over a field which is isomorphic to $\mathfrak{R}(C)$. We know already that $\mathfrak{R}(C)$ is purely transcendental over K. It follows that $\mathfrak{R}(G)$ is purely transcendental over K, which proves th. 1.

COROLLARY 1. *Let G be an irreducible algebraic group of automorphisms of a finite dimensional vector space V over a field K of characteristic* 0, *and let $\mathfrak{g}$ be the Lie algebra of G. Assume that $\mathfrak{g}$ has a Cartan subalgebra $\mathfrak{h}$ with the following property : for any $X\in\mathfrak{h}$, the characteristic polynomial of the endomorphism X of V splits into linear factors with coefficients in K. Then the field $\mathfrak{R}(G)$ of rational functions on G is purely transcendental over K.*

We use the notation of I. The homomorphism ρ of $\mathfrak{g}$ onto $\rho(\mathfrak{a})$ maps $\mathfrak{h}$ onto a Cartan subalgebra $\mathfrak{h}_\mathfrak{a}$ of $\rho(\mathfrak{a})$ ([1], VI, prop. 17, 4). We know that $\mathfrak{a}$ is reductive and that ρ induces a faithful semi-simple representation of $\mathfrak{a}$; the group $\mathrm{P}(A)=JAJ^{-1}$ is isomorphic to A as an algebraic group. If $X\in\mathfrak{g}$, then the characteristic polynomial of X is obviously equal to the product of the characteristic polynomials of the endomorphisms $\rho_i(X)$ $(1\leqq i\leqq h)$, i. e. also to the characteristic polynomial of $\rho(X)$. Thus, it follows from our assumption that the characteristic polynomials of the elements of $\mathfrak{h}_\mathfrak{a}$ split into linear factors with coefficients in K. Therefore, it follows from th. 1 that the field $\mathfrak{R}(A)$ of rational functions on A, which is isomorphic to $\mathfrak{R}(\mathrm{P}(A))$, is purely transcendental over K, and from prop. 1, 1, that $\mathfrak{R}(G)$ is purely transcendental over K.

COROLLARY 2. *Let G be any irreducible algebraic group over an algebraically closed field K of characteristic* 0. *Then the field of rational functions on G is purely transcendental over K.*

This follows immediately from cor. 1.

PROPOSITION 2. *Let H be an irreducible abelian group of automorphisms of a finite dimensional vector space over a field K of characteristic* 0 *whose elements are semi-simple and whose Lie algebra $\mathfrak{h}$ is of type (D); let p be the dimension of H. Then the field of rational functions on H is generated by p functions $z_1,\cdots,z_p$ which are rational representations of H into the group K^* of elements $\neq 0$ in K; H is isomorphic to $(K^*)^p$.*

It is clear that $\mathfrak{h}$ is a Cartan subalgebra of itself. Using the same notation as in the proof of th. 1, we observe that the functions $u_1,\cdots,u_n$ are representations of H in K^*; the same is therefore true of $z_1,\cdots,z_p$. We have seen that, if $d_1,\cdots,d_p$ are in K^*, then there is an $s\in H$ such that $z_k(s)=d_k$ $(1\leqq k\leqq p)$; the mapping $s\to\big(z_1(s),\cdots,z_p(s)\big)$ is therefore an isomorphism of H with $(K^*)^p$.

III. Functions constant on every Cartan subgroup.

Let s be a generic point of the group G. Denote by I the identity automorphism of the Lie algebra $\mathfrak{g}^{K(s)}$ of $G^{K(s)}$ and by l the nullity of $I-Ad\ s$ (i.e. the multiplicity of 0 as a characteristic root of this endomorphism). Since every point s_0 of G is a specialisation of s, it is clear that the nullity of $I-Ad\ s_0$ is alway $\geqq l$, and is actually equal to l for some $s_0\in G$; i.e. l is the rank of G ([1], VI, déf. 2, 4). The rank of $G^{K(s)}$ being equal to that of G ([1], VI, prop. 22, 4), we see that s is regular in $G^{K(s)}$, and therefore belongs to a uniquely determined Cartan subgroup H of $G^{K(s)}$ ([1], VI, th. 2, 4); let $\mathfrak{h}$ be the Lie algebra of H: this is a Cartan subalgebra of $\mathfrak{g}^{K(s)}$. We shall introduce a field L_s which is, in the sense of algebraic geometry, the field of definition of the linear variety $\mathfrak{h}$.

Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}$, and let $(X_1,\cdots,X_r)$ be a base of $\mathfrak{g}$ which contains a base $(X_1,\cdots,X_l)$ of $\mathfrak{h}_0$. In order for an element $X\in\mathfrak{g}^{K(s)}$ to belong to $\mathfrak{h}$, it is necessary and sufficient that $(I-Ad\ s)^k\cdot X=0$ for some $k>0$ ([1], VI, prop. 8 and cor. 1 to th. 1, 4). Since $\mathfrak{g}$ is of dimension r, it is also necessary and sufficient that $(I-Ad\,s)^r\cdot X=0$. Let $(f_{ij}(s))$ be the matrix which represents $(I-Ad\,s)^r$ with respect to the base $(X_1,\cdots,X_r)$; each f_{ij} is an everywhere defined rational function on G. In order for an element $\sum_{i=1}^r u_iX_i$ to belong to $\mathfrak{h}$, it is necessary and sufficient that the u_i's be a solution of the linear system

$$(1)\qquad \sum_{j=1}^r f_{ij}(s)u_j=0. \qquad (1\leqq i\leqq r)$$

Let k be any index between 1 and l; let us adjoin to the system (1) the equations $u_{k'}=0$ for $1\leqq k'\leqq l$, $k'\neq k$. Since $\mathfrak{h}$ is of dimension l, the system (1) is of rank $r-l$, and the system (1_k) we have just described has a non trivial solution $(v_{1,k},\cdots,v_{r,k})$. Let H_0 be the Cartan subgroup of G whose Lie algebra is $\mathfrak{h}_0$, and let s_0 be a regular element of G contained in H_0 ([1], VI, cor. 1 to th. 1, 4). Denote by $(1^{(0)})$ the system deduced from (1) by replacing the $f_{ij}(s)$ by their values $f_{ij}(s_0)$ at s_0. Since s_0 is regular, the solutions $(u_1,\cdots,u_r)$ of $(1^{(0)})$ in K are the systems of elements $(u_1,\cdots,u_r)$ such that $\sum_{i=1}^r u_i X_i\in\mathfrak{h}_0$, i.e. such that $u_{l+1}=\cdots=u_r=0$. It follows that the system $(1_k^{(0)})$ deduced from $(1^{(0)})$ by adjoining the equations $u_{k'}=0$ for $k'\neq k$, $1\leqq k'\leqq l$, is of rank $r-1$ and has a solution $(u_1,\cdots,u_r)$ for which $u_k\neq0$. This being the case, it is clear that the system (1_k) is of rank $r-1$ and that $v_{k,k}\neq0$. We may therefore assume that $v_{k,k}=1$, and the elements v_{ik} are then uniquely determined. We can extract from the matrix of the system (1_k) a square matrix with $r-1$ rows and columns whose determinant is of the form $D(s)$, D being a rational function on G which is defined and $\neq0$ at s_0. It follows immediately that $v_{i,k}=g_{ik}(s)$, each g_{ik} being a rational function on G which is defined at s_0. We denote by L the subfield of $\mathfrak{R}(G)$ which is generated over K by the functions g_{ik} $(1\leqq i\leqq r,\ 1\leqq k\leqq l)$, and by L_s the subfield of $K(s)$ generated by the elements $g_{ik}(s)$; L_s is the image of L under the isomorphism $f\to f(s)$ of $\mathfrak{R}(G)$ with $K(s)$. The field L does not depend on the choice of $\mathfrak{h}_0$ or of the base $(X_1,\cdots,X_n)$. In order to prove this, set $Y_k=\sum_{i=1}^r g_{ik}(s)X_i$; since $g_{kk'}(s)=\delta_{kk'}$ if $1\leqq k,\ k'\leqq l$, $Y_1,\cdots,Y_l$ form a base of $\mathfrak{h}$. This being said, let $\mathfrak{h}_0'$ be any Cartan subalgebra of $\mathfrak{g}$ and $(X_1',\cdots,X_r')$ any base of $\mathfrak{g}$ containing a base $(X_1',\cdots,X_l')$ of $\mathfrak{h}_0'$. Let $(Y_1',\cdots,Y_l')$ be the base of $\mathfrak{h}$ constructed by means of $\mathfrak{h}_0'$ and $(X_1',\cdots,X_r')$ in the same way $(Y_1,\cdots,Y_l)$ has been constructed in terms of $\mathfrak{h}_0$ and $(X_1,\cdots,X_r)$. We have $Y_k'=\sum_{k'=1}^l w_{kk'}Y_{k'}$. If we write $Y_{k'}=\sum_{j=1}^r a_{k'j}X_j'$, the elements $a_{k'j}$ are in L_s, and the elements $w_{kk'}$ for a given k are uniquely determined by the condition that $\sum_{k'=1}^{l} w_{kk'} a_{k'j}$ should be 0 if $j \neq k$, $1 \leqq j \leqq l$ and 1 if $j=k$. The elements $w_{kk'}$, which constitute the unique solution of a linear system with coefficients in L_s, are therefore in L_s, which shows that the field L'_s defined by means of $\mathfrak{h}'_0$ and the base $(X'_1, \cdots, X'_r)$ is contained in L_s. We would see in the same way that $L_s \subset L'_s$, whence $L_s = L'_s$.

We shall now see that L_s is purely transcendental over K. We may assume without loss of generality that X_1 is a regular element of $\mathfrak{g}$. It follows immediately from the fact that the functions g_{ik} are defined at s_0 that $(s, Y_1, \cdots, Y_l) \to (s_0, X_1, \cdots, X_l)$ is a specialisation over K; in particular, X_1 is a specialisation of Y_1. Since X_1 is regular, it follows immediately that Y_1 is regular. Thus, $\mathfrak{h}$ is the set of elements of $\mathfrak{g}^{K(s)}$ which are mapped upon 0 by some power of *ad* Y_1, i. e. also which are mapped upon 0 by $(ad\ Y_1)^r$ ([1], VI, prop. 16, 4). It follows that, for $1 \leqq k \leqq l$, Y_k is the unique element $\sum_{i=1}^{r} u_i X_i$ of $\mathfrak{g}^{K(s)}$ which satisfies the following conditions: we have $(\mathrm{ad}\ Y_1)^r \cdot (\sum_{i=1}^{r} u_i X_i) = 0$ and $u_i = \delta_{ik}$ if $1 \leqq i \leqq l$. These conditions give a system of linear equations in $u_1, \cdots, u_n$ with coefficients in the field $K(Y_1)$. It follows that the elements $g_{ik}(s)$ $(1 \leqq i \leqq l)$ all belong to the field $K(Y_1)$, i. e. to $K(g_{l+1,1}(s), \cdots, g_{r,1}(s))$. This shows that the transcendence degree of L_s/K is $\leqq r-l$. On the other hand, since $\mathfrak{h}$ has a base in $\mathfrak{g}^{L_s}$. we may write $\mathfrak{h} = \mathfrak{h}_1^{K(s)}$, where $\mathfrak{h}_1$ is a subalgebra of $\mathfrak{g}^{L_s}$, which is a Cartan subalgebra of $\mathfrak{g}^{L_s}$ ([1], VI, prop. 22, 4). Let H_1 be the Cartan subgroup of G^{L_s} with $\mathfrak{h}_1$ as its Lie algebra, whence $H = H_1^{K(s)}$. This group is of dimension l. Since s is a generalized point of H_1, the transcendence degree of $K(s) = L_s(s)$ over L_s is $\leqq l$. The transcendence degree of $K(s)$ over K being r, we conclude on the one hand that s is a generic point of H_1 over L_s, on the other hand that the transcendence degree of L_s over K is $r-l$. Since L_s may be obtained by adjunction of $r-l$ elements to K, we see that L_s is purely transcendental over K.

If K' is any overfield of K and E a subset of $G^{K'}$, we shall say that a rational function f on G is constant on E if it has the same value at all points of E at which it is defined. We shall see that the functions of the field L are those rational functions f on G which are constant on H_1. Let first f be in L, whence $f(s) \in L_s$. Let s' be any point of H_1 at which f is defined; then $s \to s'$ is a specialisation over

L_s, and, since $f(s) \in L_s$, we have $f(s') = f(s)$, which shows that f is constant on H_1. Let conversely f be constant on H_1. Since f is defined at s, which is a generalized point of H_1, it is defined at least one point $s_1 \in H_1$; it is clear that $f(s_1) \in L_s$. We assert that $f(s) = f(s_1)$. Were this not the case, there would exist at least one specialisation s_1' of s over L_s such that f, and therefore $f - f(s_1)$, is defined at s_1' and $(f - f(s_1))(s_1') \neq 0$; but s_1' would then be in H_1 and we would have $f(s_1') \neq f(s_1)$, which is impossible. It follows that $f(s) = f(s_1) \in L_s$; since $h \rightarrow h(s)$ is an isomorphism of $\mathfrak{R}(G)$ with $K(s)$, it follows that $f \in L$.

We shall now prove that the functions of L are constant on every Cartan subgroup H_0 of G. We use the same notation as above. The functions g_{ik} are defined at s_0, and we have $g_{ik}(s_0) = \delta_{ik}$ $(1 \leqq i \leqq r, 1 \leqq k \leqq l)$. Let $\mathfrak{o}$ be the subring of L_s generated by K and the elements $g_{ik}(s)$; then there exists a homomorphism θ of $\mathfrak{o}$ into K such that $\theta(g_{ik}(s)) = \delta_{ik}$. Introduce l letters $T_1, \cdots, T_l$; then θ may be extended to a homomorphism of $\mathfrak{o}[[T_1, \cdots, T_l]]$ (the ring of formal power series with coefficients in $\mathfrak{o}$) into $K[[T_1, \cdots, T_l]]$ which maps any power series upon the power series obtained by applying θ to its coefficients. Set $t = (\exp T_1 Y_1) \cdots (\exp T_l Y_l)$; then t is a generic point of H_1 ([1], II, th. 8, 12). The coordinates of t (with respect to a base of the space of endomorphisms of V, and therefore also of the space of endomorphisms of $V^{K'}$, for any overfield K' of K) are in $\mathfrak{o}[[T_1, \cdots, T_l]]$; set $t_0 = \theta(t)$ (t_0 is the endomorphism of $V^{K((T_1, \cdots, T_l))}$ whose coordinates are the images of those of t under θ). Since $\theta(Y_k) = X_k (1 \leqq k \leqq l)$, it is clear that $t_0 = (\exp T_1 X_1) \cdots (\exp T_l X_l)$; t_0 is therefore a generic point of H_0. Let f be a function in L which is defined at least one point of H_0 (were this not the case, f would be trivially constant on H_0). Then f is defined at t_0 and may be written in the form f_1/f_2, where f_1, f_2 are polynomial functions on G and $f_2(t_0) \neq 0$, whence $f_2(t) \neq 0$. The elements $f_1(t)$ and $f_2(t)$ are in $\mathfrak{o}[[T_1, \cdots, T_l]]$. Since s and t are generic points of H_1, there is an isomorphism of $L_s(s)$ with $L_s(t)$ which leaves the elements of L_s fixed and maps $h(s)$ upon $h(t)$ for any rational function h on G. Since $f \in L$, we have $f(s) \in L_s$, whence $f(t) \in L_s$. On the other hand, $f(t) = f_1(t)/f_2(t)$. Thus the coefficients of the power series $f_2(t)$ in $T_1, \cdots, T_l$ are proportional to those of the power series $f_1(t)$, the proportionality ratio being $f(t) \in L_s$. But one at least of the coefficients of the power series $f_2(t)$ is not mapped upon 0 by θ, since $f_2(t_0) \neq 0$. It follows that we may write $f(t) = a/b$, where

a and b are elements of $\mathfrak{o}$ such that $\theta(b)\neq 0$. It follows immediately that $f(t_0)=\theta(a)/\theta(b)$ is an element of K. Now, let t_1 be any element of H_0 at which f is defined; then t_1 is a specialisation of t_0 over K. and $f(t_1)$ is a specialisation of $f(t_0)$. Since $f(t_0)\in K$, we have $f(t_1)=f(t_0)$, which proves that f is constant on H_0.

Let conversely f be a rational function on G which is constant on every Cartan subgroup of G. Write $f=f_1/f_2$, where f_1, f_2 are polynomial functions, and $f_2\neq 0$. Then we have $f_2(t)\neq 0$. If the formal power series $f_1(t)$, $f_2(t)$ with coefficients in $\mathfrak{o}$ are proportional to each other, then $f(t)\in L_s$, whence $f(s)=f(t)\in L_s$ and $f\in L$. We shall assume for a moment that this is not the case, and we shall derive a contradiction from this assumption. We therefore assume that there exist two coefficients a, b of the formal power series f_1 such that, a' and b' being the corresponding coefficients of f_2, we have $ab'-ba'\neq 0$. Assuming, as we did before, that X_1 is regular, we have seen that Y_1 is regular. The coefficient D of T^l in the characteristic polynomial of $ad\, Y_1$ (T being the variable with which we write this polynomial) is therefore an element $\neq 0$ of $\mathfrak{o}$. Thus, $D(ab'-ba')$ is an element $\neq 0$ of $\mathfrak{o}$. The field of quotients L_s of $\mathfrak{o}$ is purely transcendental over K; expressing the elements $g_{ik}(s)$, $D(ab'-ba')$ as rational fractions in the elements of some transcendence base of L_s/K, we see easily that there exists a homomorphism θ' of $\mathfrak{o}$ into K such that $\theta'\big(D(ab'-ba')\big)\neq 0$. We extend as above θ' to a homomorphism of $\mathfrak{o}[[T_1,\cdots, T_l]]$ into $K[[T_1\cdots, T_l]]$, and we set $X'_k=\theta'(Y_k)$ $(1\leqq k\leqq l)$, $t'=\theta'(t)$, whence $t'=(\exp\, T_1 X'_1)\cdots(\exp\, T_l X'_l)$. It is clear that $\theta'(D)\neq 0$ is the coefficient of T^l in the characteristic polynomial of $ad\, X'_1$, and therefore that X'_1 is regular in $\mathfrak{g}$. From the relations $(ad\, Y_1)^r Y_k=0$ $(1\leqq k\leqq l)$, it follows immediately that $(ad\, X'_1)^r.\ X'_k=0$, and therefore that $X'_1,\cdots, X'_l$ belong to the Cartan subalgebra $\mathfrak{h}'_0$ of $\mathfrak{g}$ which contains X'_1. We have $Y_k=\sum_{i=1}^r g_{ik}(s)\, X_i$, whence $X'_k=\sum_{i=1}^r \theta'\big(g_{ik}(s)\big)X_i$; since $g_{ik}(s)=\delta_{ik}$ if $i\leqq l$, we have also $\theta'\big(g_{ik}(s)\big)=\delta_{ik}$ if $i\leqq l$, which shows that $X'_1,\cdots, X'_l$ are linearly independent and constitute a base of $\mathfrak{h}'_0$. Thus, t' is a generic point of the Cartan subgroup H'_0 of G whose Lie algebra is $\mathfrak{h}'_0$. Since $\theta'(ab'-ba')\neq 0$, $\theta'(a')$ and $\theta'(b')$ are not both 0, from which it follows that the power series $\theta'\big(f_2(t)\big)=f_2(t')$ is $\neq 0$ and that f is defined at t'. We have $f(t')=f_1(t')/f_2(t')$, and, since $\theta'(ab'-ba')\neq 0$, the power series $f_1(t')$, $f_2(t')$ are not proportional to each other, which shows that $f(t')$ is not in K.

Since $f_2(t')\neq 0$, f is defined at least one point t_1' of H_0'; set $c=f(t_1')$. Then $f(t')-c\neq 0$; the restriction to H_0' of $f-c$ being a rational function $\neq 0$, there is at least one point t_2' of H_0' at which $f-c$ is defined and takes a value $\neq 0$. Then f is defined at t_1' and t_2' and $f(t_1')\neq f(t_2')$, in contradiction to the assumption that f is constant on H_0'.

Thus, the functions in L are characterized by the property of being constant on every Cartan subgroup of G, which shows that the field L does not depend on the choice of the generic point s.

Now, let K' be any overfield of K, and choose for s a generic point of $G^{K'}$(and therefore, *a fortiori*, of G). Then the Cartan subgroup of $G^{K'(s)}$ which contains s is clearly $H^{K'(s)}$, and its Lie algebra is $\mathfrak{h}^{K'(s)}$. The elements $Y_1,\cdots, Y_l$ form a base of $\mathfrak{h}^{K'(s)}$. Therefore, the arguments used above show that the field of rational functions on $G^{K'}$ which are constant on every Cartan subgroup of $G^{K'}$ is obtained by adjunction to K' of the elements g_{ik}: this field is $L^{K'}$. Thus we have proved the following redults:

PROPOSITION 3. *The rational functions on G which are constant on every Cartan subgroup of G form a subfield L of the field of rational functions on G. If G is of dimension r and rank l, then L/K is a purely transcendental extension of transcendence degree $r-l$. If s is a generic point of G, and H the Cartan subgroup of $G^{K(s)}$ which contains s, then we may write $H=H_1^{K(s)}$, where H_1 is a Cartan subgroup of G^{L_s}, L_s being the image of L under the isomorphism $f\to f(s)$ of $\mathfrak{R}(G)$ with $K(s)$. The point s is a generic point of H_1; the functions f of L are characterized by either one of the following properties:* a) $f(s)\in L_s$; b) *f is constant on H_1. If K' is an overfield of K, the rational functions on $G^{K'}$ which are constant on every Cartan subgroup are exactly those of $L^{K'}$.*

Consider now the field extension $\mathfrak{R}(G)/L$. The isomorphism $f\to f(s)$ of $\mathfrak{R}(G)$ with $K(s)$ maps L onto L_s, and we have $K(s)=L_s(s)$. Since s is a generic point of H_1, $K(s)$ is isomorphic to the field of rational functions on H_1. Thus, we see that $\mathfrak{R}$ *is isomorphic, as an algebra over L, to the field of rational functions on some Cartan subgroup of G^L.*

If $\mathfrak{g}$ is a nilpotent Lie algebra and $\mathfrak{n}$ the largest ideal of $\mathfrak{g}$ composed of nilpotent elements, then $\mathfrak{g}$ is direct sum of $\mathfrak{n}$ and of an algebraic subalgebra $\mathfrak{a}$ of the center of $\mathfrak{g}$ whose elements are semi-simple ([1], V, prop. 22, 3). Taking prop. 1 into account, we see that the field of rational functions on the irreducible algebraic group whose Lie algebra is $\mathfrak{g}$ is a purely transcendental extension of a field isomorphic to the field of rational functions on the irreducible group A whose Lie algebra is $\mathfrak{a}$. Thus we have the following result:

PROPOSITION 4. *Let G be an irreducible algebraic group and $\mathfrak{R}(G)$ the field of rational functions on G. Then $\mathfrak{R}(G)$ has a subfield M with the following properties: M is purely transcendental over the basic field of G, and $\mathfrak{R}(G)$ is isomorphic (as an algebra over M) to the field of rational functions on some irreducible abelian algebraic subgroup of G^M whose elements are semi-simple.*

IV. Abelian groups.

We shall now assume that the group G is abelian and that its elements are semi-simple. The Lie algebra $\mathfrak{g}$ of G is then abelian and its elements are semi-simple; for, the enveloping associative algebra of $\mathfrak{g}$ is the same as that of G ([1], VI,cor. 2 to th. 8, 12) and the elements of this algebra are all semi-simple ([1], I, prop. 4, 8). We can find a finite galoisian extension L/K of K such that the characteristic polynomials of the elements of a base of $\mathfrak{g}$ split into linear factors with coefficients in L. It is then clear that $\mathfrak{g}^L$ is abelian of type (D). It follows that the field $\mathfrak{R}(G^L)$ of rational functions on G^L may be represented in the form $L(z_1,\cdots,z_r)$, where $z_1,\cdots,z_r$ are algebraically independent over L and are rational representations of G^L in the multiplicative group L^* of elements $\neq 0$ in L; the mapping $s\rightarrow\big(z_1(s),\cdots,z_r(s)\big)$ is an isomorphism of G^L with $(L^*)^r$.

Let $\mathfrak{G}$ be the Galois group of L/K. Then we may make the elements of $\mathfrak{G}$ operate on V^L and on the space of endomorphisms of V^L. The elements (resp.: the endomorphisms) of V are the elements (resp.: endomorphisms) of V^L which are invariant by the operations of $\mathfrak{G}$. In particular, G is the set of elements of G^L invariant by all automorphisms of $\mathfrak{G}$. Moreover, since G^L is defined by a system of equations with coefficients in K, the elements of G^L are permuted among themselves by the operations of $\mathfrak{G}$. Now, since G^L is abelian, it is clear that, for any $s\in G^L$, the element $\prod_{\sigma\in\mathfrak{G}} s^\sigma$ is in G; we shall denote this element by $N(s)$. The mapping $s\rightarrow N(s)$ is a homomorphism of G^L into G.

We propose now to determine the form of the expressions of the elements $z_i(s^\sigma)$ $(s\in G^L, \sigma\in \mathfrak{G})$ in terms of $z_1(s),\cdots,z_r(s)$. We shall first prove that any rational representation z of G^L into L^* is in the group generated by $z_1,\cdots,z_r$. We may write $z=R(z_1,\cdots,z_r)$, where R is a rational fraction defined at all points of L^r whose coordinates are all $\neq 0$. If M is any overfield of L, the rational function on G^M which extends z is a rational representation of G^M into the multiplicative group M^* of elements $\neq 0$ in M; R is therefore defined at every point of M^r whose coordinates are all $\neq 0$. Let $M=L(u_2,\cdots,u_r)$, where $u_2,\cdots,u_r$ are algebraically independent over L. Then the rational fraction $R(U,u_2,\cdots,u_r)=R'(U)$ is defined at every element $u\neq 0$ of M, and we have $R'(uu')=\rho R'(u)R'(u')$, $\rho\in M$, whenever u,u' are elements $\neq 0$ of M. Write $R'(U)=P(U)/Q(U)$ where P,Q are polynomials with coefficients in M, relatively prime to each other. Then, for $u\neq 0$ in M, we have

$$P(uU)/Q(uU)=\rho R(u)P(U)/Q(U).$$

Since $P(uU)$ (resp.: $Q(uU)$) is of the same degree as P (resp.: Q), we have $P(uU)=c(u)P(U)$, $Q(uU)=c'(u)Q(U)$, where $c(u)$, $c'(u)\in M$. This implies that $P(U)=aU^p$, $Q(U)=bU^q$, a,b in M, whence $R'(U)=fU^e$, with $f\in M$, e being an integer. In other words, we have $R(z_1,\cdots,z_r)=z_1^eR_1(z_2,\cdots,z_r)$, R_1 being a rational fraction in $r-1$ variables. We would see in the same way that, for any i, $R(z_1,\cdots,z_r)$ is the product of a power $z_i^{e(i)}$ of z_i by an element which is a rational fraction in the z_j's for $j\neq i$. It follows that $R(z_1,\cdots,z_r)=c\prod_{i=1}^r z_i^{e(i)}$, with $c\in L$, and it is clear that $c=1$, which shows that z belongs to the group generated by $z_1,\cdots,z_r$. This being said, if we denote by $w_1(s),\cdots,w_m(s)$ the coordinates of s with respect to a base of the space of endomorphisms of V (and therefore also of V^L), we have $w_k(s^\sigma)=\sigma\cdot w_k(s)$. Expressing the $z_i(s)$ as rational fractions in $w_1(s),\cdots,w_m(s)$, we see immediately that the mappings $s\to\sigma^{-1}(z_i(s^\sigma))$ $(1\leqq i\leqq r)$ are rational representations of G^L into L^*. Thus we have

$$z_i(s^\sigma)=\sigma\cdot\prod_{j=1}^r z_j^{e_{ij}(\sigma)}$$

where the $e_{ij}(\sigma)$ are integers. It is clear that the mapping $\sigma\to(e_{ij}(\sigma))$ is a representation of $\mathfrak{G}$ by matrices of degree r with integral coefficients.

Now, we shall see that the image $N(G^L)$ of G^L under the homomorphism $s \rightarrow N(s)$ is dense in G in the sense of the Zariski topology. Let P be a polynomial function on G which is zero on $N(G)$. We may extend P to a polynomial function on G^L, still denoted by P; we have $P=R(z_1, \cdots, z_r)$, R being a rational fraction in r variables $Z_1, \cdots, Z_r$. Introduce dr letters $Z_{i,\sigma}$ $(1 \leqq i \leqq r,\ \sigma \in \mathfrak{G})$ (where $d=[L:K]$) and let $R'(\cdots, Z_{i,\sigma}, \cdots)$ be the rational fraction obtained from R by the substitution

$$Z_i \rightarrow \prod_{\sigma \in \mathfrak{G}} \prod_{j=1}^{r} Z_{j,\sigma}^{e_{ij}(\sigma)}\,.$$

Then it follows from the assumption that P vanishes on $N(G^L)$ that, for any elements $\zeta_1, \cdots, \zeta_r$ all $\neq 0$ of L, the result of the substitution $Z_{i,\sigma} \rightarrow \sigma \cdot \zeta_i$ in R' is 0. Making use of Lemma 2, [1], II, 13, we conclude that $R'=0$. Now, if σ_1 is the unit element of G then $e_{ij}(\sigma_1)=\delta_{ij}$, and it follows that $R(Z_1, \cdots, Z_r)$ is the rational fraction which results from R' by the substitution $Z_{i,\sigma_1} \rightarrow Z_i$ $(1 \leqq i \leqq r)$, $Z_{i,\sigma} \rightarrow 1$ for $\sigma \neq \sigma_1$. We conclude that $R=0$, whence $P=0$. This proves that $N(G^L)$ is dense in G.

Let $(\omega_1, \cdots, \omega_d)$ be a base of L/K. Let $L(w)$ be a field obtained from L by adjunction of rd elements w_{ik} $(1 \leqq i \leqq r,\ 1 \leqq k \leqq d)$ which are algebraically independent over L. Then $L(w)$ is galoisian of degree d over $K(w)$, and the Galois group of $L(w)/K(w)$ may be identified to $\mathfrak{G}$. Let s_w be the element of $G^{L(w)}$ such that $z_i(s_w)=\sum_{k=1}^{d} w_{ik}\,\omega_k$. Proceeding as above, we see that $\mathfrak{G}$ operates in a natural manner on $G^{L(w)}$, and that the set of elements of $G^{L(w)}$ which are left fixed by the operations of $\mathfrak{G}$ is $G^{K(w)}$. We set $t_w=N(s_w)=\prod_{\sigma \in \mathfrak{G}} s_w^{\sigma}$. Then t_w is an element of $G^{K(w)}$, and it is clear that every element of $N(G^L)$ is a specialisation of t_w over K. It follows that t_w is a generic point of G. If $f \in \mathfrak{R}(G)$, then $f(t_w) \in K(w)$, and the mapping $f \rightarrow f(t_w)$ is an isomorphism of $\mathfrak{R}(G)$ with a subfield of $K(w)$, which is purely transcendental over K; this isomorphism leaves the elements of K fixed.

Now, we shall prove the following lemma:

LEMMA 2. *Let K be an infinite field, and $K(w_1, \cdots, w_p)$ a purely transcendental extension of transcendence degree p of K. Let R be a subfield of $K(w)=K(w_1, \cdots, w_p)$ containing K and of transcendence degree r over K. Then there is a purely transcendental extension M/K of transcendence degree r of K such that R is isomorphic (as an algebra over K) to a subfield of M.*

The following proof of this lemma has been communicated to me by Mr. Shimura.

Proceeding by induction on p, it is obviously sufficient to prove the following result: let K be an infinite field, L a finitely generated overfield of K of transcendence degree r, $L(w)$ an overfield of L obtained by adjunction to L of an element w which is transcendental over L and R a subfield of $L(w)$ containing K and whose transcendence degree over K is $\leqslant r$; then there exists a K-isomorphism of R with a subfield of L.

By adjoining to R some elements of a transcendence base of $L(w)/K$, we may obviously reduce the problem to the case where R is of transcendence degree r over K. Assume that this is the case. We may further assume that w is transcendental over R. For, if this is not the case, then L must contain some element a which is transcendental over R (since $L(w)$ is not algebraic over R); if we set $w'=w+a$, we have $L(w')=L(w)$, and w' is transcendental over both L and R. Represent L in the form $K(x_1,\cdots,x_n)$, with $x_i\in L$ $(1\leqslant i\leqslant n)$. Since the extension $L(w)/\mathrm{K}$ is finitely generated, it is well known that the same is true of R/K; let $y_m,\cdots,y_n$ be elements of R which generate R over K. We may write $y_i=Y_i(w)$ $(1\leqslant i\leqslant m)$, where each Y_i is a rational fraction in one letter with coefficients in L. On the other hand, it follows from our assumptions that $R(w)$ is of transcendence degree $r+1$ over K. Each x_k is therefore algebraic over $R(w)$, and we have relations of the form

$$\textstyle\sum_{j=0}^{d(k)} X_{jk}(y_1,\cdots,y_m,w)\,x_k^{d(k)-j}=0$$

where each X_{kj} is a polynomial in $m+1$ letters with coefficients in K and $X_{0k}(y_1,\cdots,y_m,w)\neq 0$. We may write

$$X_{0k}(y_1,\cdots,y_m,w)=X'_k(w)$$

where X'_k is a rational fraction $\neq 0$ with coefficients in L. Since K is infinite, there exists an element $w_0\in\mathrm{K}$ such that the rational fractions $Y_i(1\leqslant i\leqslant m)$, $X'_k(1\leqslant k\leqslant n)$ are all defined at w_0 and $X'_k(w_0)\neq 0$ $(1\leqslant k\leqslant n)$. Let $\mathfrak{o}$ be the subring of $L(w)$ composed of all elements of the form $A(w)$, where A is any rational fraction with coefficients in L which is defined at w_0. There exists a homomorphism φ of $\mathfrak{o}$ into L which coincides with the identity on L and which maps w upon w_0.

The elements y_i, w belong to $\mathfrak{o}$, whence $K[y_1,\cdots,y_m,w]\subset\mathfrak{o}$; set $y'_i=\varphi(y_i)$ and

$$\xi_{jk}=\varphi\big(X_{jk}(y_1,\cdots,y_m,w)\big)=X_{jk}(y'_1,\cdots,y'_m,w_0).$$

Then we have $\sum_{j=0}^{d(k)}\xi_{jk}x_k^{d(k)-j}=0$; moreover, $\xi_{0k}=\varphi\big(X'_k(w)\big)=X'_k(w_0)\neq 0$. It follows that $x_1,\cdots,x_n$ are algebraic over the subfield $R'=K(y'_1,\cdots,y'_m)$ of L, and therefore that R' is of transcendence degree r over K. The mapping φ induces a homomorphism φ_1 of $K[y_1,\cdots,y_m]$ onto $K[y'_1,\cdots,y'_m]$. Since both $K(y_1,\cdots,y_m)=R$ and $K(y'_1,\cdots,y'_m)=R'$ are of transcendence degree r over K, it is well known that φ_1 is an isomorphism and therefore extends to an isomorphism of R with R'. Lemma 2 is thereby proved.

This proves that the field $\mathfrak{R}(G)$ of rational functions on an irreducible algebraic group G which is abelian and whose elements are semi-simple is isomorphic to a subfield of a purely transcendental extension of transcendence degree r of the basic field of G, r being the dimension of G.

Taking prop. 4, III into account, we obtain the following result:

THEOREM 2. *Let G be an irreducible algebraic group of dimension r over a field K of characteristic* 0. *Then the field of rational functions on G is isomorphic* (*as an algebra over K*) *to a subfield of a purely transcendental extension of transcendence degree r of K.*

Returning to the notation used above, it is of interest to characterize the subfield $\mathfrak{R}(G)$ of $\mathfrak{R}(G^L)=L(z_1,\cdots,z_r)$. It is clear that a rational function $f\in\mathfrak{R}(G^L)$ belongs to $\mathfrak{R}(G)$ if and only if it satisfies the following condition: for any $s\in G^L$ and $\sigma\in\mathfrak{G}$ such that f is defined at s and s^σ, we have $f(s^\sigma)=\sigma\cdot f(s)$. Now, we may let the group $\mathfrak{G}$ operate in two different manners on the field $\mathfrak{R}(G^L)=L(z_1,\cdots,z_r)$. Let σ be an element of $\mathfrak{G}$. Denote by $\psi_1(\sigma)$ the automorphism of $L(z_1,\cdots,z_r)$ which transforms any $a\in L$ into $\sigma\cdot a$ and which leaves $z_1,\cdots,z_r$ fixed; then ψ_1 is an isomorphism of $\mathfrak{G}$ with a group $\mathfrak{G}_1$ of automorphisms of $L(z_1,\cdots,z_r)$, and the elements which are left fixed by the operations of $\mathfrak{G}_1$ are those of $K(z_1,\cdots,z_r)$. On the other hand, the matrix $\big(e_{ij}(\sigma)\big)$ being of determinant ±1, there is an automorphism $\psi_2(\sigma)$ of $L(z_1,\cdots,z_r)$ which leaves the elements of L fixed and which transforms each z_i into $\prod_{j=1}^{r}z_j^{e_{ij}(\sigma^{-1})}$. It is clear that ψ_2 is a homomorphism of $\mathfrak{G}$ into the group of automorphisms of $L(z_1,\cdots,z_r)$. Let s be an element of G^L and

f an element of $\mathfrak{R}(G^L)$ which is defined at s and s^σ. Set $f=F(z_1,\cdots,z_r)$, where F is a rational fraction with coefficients in L, and set $\zeta_i=z_i(s)$, $\zeta'_i=z_i(s^\sigma)$; then we have $\zeta'_i=\sigma\cdot\Pi_{j=1}^r\zeta_j^{e_{ij}(\sigma)}$. It follows easily that $f(s^\sigma)=\sigma\cdot\big(\psi_1(\sigma^{-1})\cdot\psi_2(\sigma^{-1})\big)\cdot f(s)$; thus, f will belong to $\mathfrak{R}(G)$ if and only if it is invariant by every automorphism of the form $\psi_1(\sigma)\cdot\psi_2(\sigma)$ of $\mathfrak{R}(G^L)$. These automorphisms form a group isomorphic to $\mathfrak{G}$. The field $\mathfrak{R}(G)$ admits a subfield composed of the elements of $K(z_1,\cdots,z_r)$ which are invariant under the automorphisms of this field induced by the operaions of $\psi_2(\mathfrak{G})$. This subfield is of interest in the case where G is a Cartan subgroup of a semi-simple linear group; we hope to come back to this question some time in the future.

V. A counter-example.

We wish to prove that there exists an irreducible algebraic group G over a field of characteristic 0 such that the field of rational functions on G is not purely transcendental over K.

We take K to be the field of p-adic numbers, p being any prime number. It is easily seen that there exists a finite algebraic extension L/K of K which is abelian but not cyclic: we may for instance take L to be the composite field of the unramified extension of degree $p-1$ of K and of the field obtained by adjunction to K of the p-th roots of unity. We consider L as a vector space over K and every element of L as operating on this vector space by means of the multiplication in L. Take G to be the group of elements of L of norm 1 with respect to K. If $(\omega_1,\cdots,\omega_n)$ is a base of L/K, and $u_1,\cdots,u_n\in K$, then we may write

$$N_{L/K}(u_1\,\omega_1+\cdots+u_n\,\omega_n)=F(u_1\cdots,u_n)$$

where F is a polynomial with coefficients in K; in order for $\sum_{i=1}^n u_i\,\omega_i$ to be in G, it is necessary and sufficient that $F(u_1,\cdots,u_n)=1$, which shows that G is algebraic. On the other hand, F, considered as a polynomial with coefficients in L, splits into the product of n linear forms, which shows that G is irreducible.

From now on, we denote by $u_1,\cdots,u_n$ the polynomial functions on G such that $x=\sum_{i=1}^n u_i(x)\,\omega_i$ for every $x\in G$; the field $\mathfrak{R}(G)$ of rational functions on G is therefore $K(u_1,\cdots,u_n)$. We shall assume that this field is purely transcendental over K, and we shall derive a contradiction from this assumption. It is clear that G is of dimension $n-1$. Our assumption then means that $K(u_1, \cdots, u_n)=K(t_1, \cdots, t_{n-1})$, where $t_1, \cdots, t_{n-1}$ are $n-1$ suitable elements of $\mathfrak{R}(G)$. Write $u_i=A_i/D(1 \leqq i \leqq n)$, where $A_1, \cdots, A_n, D$ are in $K[t]=K[t_1, \cdots, t_{n-1}]$. Let $\mathfrak{G}$ be the Galois group of L/K; we then have

$$D^n=\prod_{\sigma \in \mathfrak{G}}(A_1 \omega_1^\sigma+\cdots+A_n \omega_n^\sigma).$$

It is clear that we may write

$$A_1 \omega_1+\cdots+A_n \omega_n=a \prod_{i=1}^r H_i^{f_i}$$

where $H_1, \cdots, H_r$ are prime elements of the ring $L[t_1 \cdots, t_{n-1}]$ such that, for $i \neq j$, H_i is relatively prime to all conjugates of H_j, while each f_i is an element of the group ring of $\mathfrak{G}$ over the ring of rational integers and $a \in L$. Each H_i divides prime element G_i of $K[t_1, \cdots, t_{n-1}]$, which we may assume to be the product of the distinct conjugates of H_i. Let S be the sum of the elements of $\mathfrak{G}$ (in the group ring), and write $f_i=\sum_{\sigma \in \mathfrak{G}} a_1(\sigma)\sigma$, $s_i=\sum_{\sigma \in \mathfrak{G}} a_i(\sigma)$. Then we have $f_i S=s_i S$ and

$$D^n=N_{L/K}a. \quad \prod_{i=1}^r H_i^{s_i S}.$$

On the other hand, if the group of elements $\sigma \in \mathfrak{G}$ such that $H_i=H_i^\sigma$ is of order h_i, we have $H_i^S=G_i^{h_i}$; if d_i is the exponent with which H_i enters into the decomposition of D into prime elements in $K[t_1, \cdots, t_{n-1}]$, then $nd_i=h_i s_i$. Set $G_i=H_i^{q_i}$, where q is in the group ring of $\mathfrak{G}$. Then the sum of the coefficients of q_i, when expressed as a linear comcination of the elements of $\mathfrak{G}$, is n/h_i. We have $D=d\prod_{i=1}^r H_i^{q_i d_i}$, where d is an element of K. The sum of the coefficients of $f_i-q_i d_i$ is 0 in virtue of the relation $nd_i=h_i s_i$. It follows immediately that $D^{-1}. \sum_{i=1}^n A_i \omega_i$ may be expressed in the form

$$a'. \prod_{\sigma \in \mathfrak{G}} R_\sigma^{1-\sigma}$$

where each R_σ is an element of $L(t_1, \cdots, t_{n-1})$ and a' an element of L. Let x be an element of G which satisfies the following conditions: a) the rational functions $t_1, \cdots, t_{n-1}$ are all defined at x; let $\tau_i=t_i(x)$ $(1 \leqq i \leqq n-1)$; b) the rational fractions R_σ are all defined and $\neq 0$ for the values $\tau_1, \cdots, \tau_{n-1}$ of their argument and $D(\tau_1, \cdots, \tau_{n-1}) \neq 0$. Then, if we set $y_\sigma=R_\sigma(\tau_1, \cdots, \tau_{n-1})$, the y_σ 's are in L, and we have

$$x = a' \cdot \prod_{\sigma \in \mathfrak{G}} y_\sigma^{1-\sigma}.$$

Let Γ be the subgroup of G generated by all elements of the form $y^{1-\sigma}$, where y runs over all elements $\neq 0$ of L and σ over all elements of $\mathfrak{G}$; then x belongs to the coset $a'\Gamma$ of G modulo Γ. It is clear that the set of elements $x \in G$ which satisfy our conditions is thick in G(i. e. its complementary set is contained in an algebraic subset of dimension $< n-1$ of G). Now, it has been proved by Matsuhima ([3]) that $\Gamma \neq G$. Let $a'' \Gamma$ be a coset $\neq a' \Gamma$ of G modulo Γ. Then $a'' \Gamma = (a''a'^{-1})(a' \Gamma)$, and, since $a' \Gamma$ is thick, the same is clearly true of $a'' \Gamma$. But this is impossible, since any two thick subsets of G have at least one common point (since G is irreducible), while two distinct cosets of G modulo Γ are disjoint from each other.

Columbia University and Nagoya University

Bibliography.

[1] C. Chevalley. Théorie des groupes de Lie; vol. II, chap. I, II, Hermann, Paris; vol. III, chap. III, IV, V, VI, à paraître prochainement.

[2] A. Weil, Foundations of algebraic geometry, Amer. Math. Soc. Colloquium Publ. 29.

[3] Y. Matsushima, A remark on the Hauptgeschlechtssatz in Minimalen (in Jap.), Zenkoku Shijo Sugaku Danwakai, 252 (1943), 213-217.