Some rationality questions on algebraic groups (1).

Memoria di MAXWELL ROSENLICHT (a Evanston, Ill., U.S.A.).

Sommario. - *È dato dall'introduzione.*

A theorem going back to MAURER asserts that a connected linear algebraic group over the field of complex numbers can be rationally parametrized. In its algebraic formulation this result says that if G is a connected linear algebraic group defined over a field k, then (under certain conditions on k) the field $k(G)$ of rational functions on G that are defined over k is k-isomorphic to a subfield of a purely transcendental extension of k. CHEVALLEY has recently given a proof of this when k is any field of characteristc zero, and in addition he has shown that if k is also algebraically closed then $k(G)$ is itself a purely transcendental extension of k [2]. The main result of the present paper extends the first of these results to the case where k is an arbitrary perfect field; as to the second, our information is incomplete. Needless to say, our own methods do not depend on LIE algebras, as do the proofs of CHEVALLEY, and are essentially elementary in nature.

Our paper also contains a number of other results on rationality questions, mostly concerning solvable algebraic groups, and assorted counterexamples. Among results of general interest in the theory of algebraic groups we may call attention to our Propositions 2, 3, and 5, which give strong evidence that the study of the type of field extension obtained by adjoining the characteristic roots of a generic element of an algebraic group of matrices to the field of the generic element will provide much information on the structure of the group. Our final section cleans up some material on fields of definition of generalized jacobian varieties of curves, and gives an example of a connected algebraic group whose maximal connected linear algebraic subgroup is not defined over the same field.

The basic references for this paper are [1] and [5], whose terminology will be followed rather closely (that of [5] taking precedence in a few slight conflicts) and whose results will usually be used without explicit reference. For the general notions of algebraic geometry involved, we refer to [10].

---

(1) This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command under contract No. AF 18(600)-1571.

1. Generalities.

A linear algebraic group is an algebraic group which is biregularly isomorphic to an algebraic group of matrices. Note that a distinction is made between the two concepts. However, a linear algebraic group that is defined over a field k is biregularly isomorphic to an algebraic group of matrices that is defined over k, the isomorphism also being defined over k [5, Th. 12, Cor. 1], so that in the course of a proof we may without further ado replace a linear algebraic group by a specific biregularly isomorphic matrix group. In the same way we make a distinction between the concepts « rational homomorphism » and « rational representation », the latter being a rational homomorphism into an algebraic group of matrices.

The word « matrix » will always denote a square matrix of some degree, usually unspecified, whose elements lie in the universal domain. When convenient, a matrix will be considered to operate in the usual way on an underlying vector space (over the universal domain) having dimension equal to the degree of the matrix, and the vector space will be identified with an affine space defined over the prime field. A set of matrices S can be reduced to a set of matrices S' of the same degree if there exists a matrix a such that $S' = aSa^{-1}$; if the elements of a are in a field k, we say that S can be reduced to S' over k. A semisimple matrix is one which can be reduced to a matrix in diagonal form, a unipotent matrix is one all of whose characteristic roots equal 1. An invertible matrix a can be expressed in one and only one way as the product of a semisimple matrix a_s and a unipotent matrix a_u which commute with each other; a_s and a_u are called the semisimple and unipotent parts respectively of a. Under a rational representation of an algebraic group of matrices, semisimple matrices and unipotent matrices are mapped respectively into semisimple and unipotent matrices. Hence it makes sense to speak of semisimple and unipotent elements of a linear algebraic group. The semisimple and unipotent parts of a matrix a are each contained in any algebraic group of matrices containing a. Hence if G is a linear algebraic group and $g \in G$, we can write $g = g_s g_u$, where g_s, $g_u \in G$ commute and are respectively semisimple and unipotent, and this decomposition is unique; g_s and g_u are called the semisimple and unipotent parts respectively of g. Finally, a torus is an algebraic group that is biregularly isomorphic to a direct product $(G_m)^r$ of multiplicative groups in one variable. An algebraic group of matrices G that is defined over k is a torus if and only if it is connected and can be reduced (over some extension field of k) to diagonal form.

For future convenience we bring together in the following lemma and in Prop. 1 a number of easy facts, for the most part well-known.

LEMMA. – *Let g be a matrix and let K be a field containing the elements*

of g. Then the minimal polynomial of g over the field K is independent of the choice of K.

Let k be the smallest field containing the elements of g; then $k \subset K$. Let X be an indeterminate and suppose that $F(X) \in K[X]$, with $F(g) = 0$. Write $F = \Sigma \alpha_i F_i$, where $\{\alpha_i\}$ is a set of elements of K that are linearly independent over k and each $F_i \in k[X]$. Then the equation $\Sigma \alpha_i F_i(g) = 0$ implies that each $F_i(g) = 0$.

PROPOSITION 1. - *If g a semisimple matrix that is rational over the field k then the characteristic roots of g are separably algebraic over k. If g is an arbitrary invertible matrix that is rational over k, then g_s and g_u are rational over a purely inseparable algebraic extension of k; g_s and g_u are rational over k if and only if the characteristic roots of g are separably algebraic over k. If $\{g\}$ is a set of matrices that commute with each other and are rational over k, and if any matrix $g \in \{g\}$ has all of its characteristic roots in k, then the set $\{g\}$ is reducible over k to a set of matrices that split uniformly into square blocks situated on the main diagonal (with zeros outside the blocks) such that each block matrix is in triangular form and has equal diagonal elements.*

We first prove the last part. For any fixed $g \in \{g\}$ and $c \in k$, if m is an integer ≥ 0 then the range and null space of $(g - ce)^m$ (where $e =$ unit matrix) are each $\{g\}$-invariant subspaces of the underlying vector space V, and if m is sufficiently large then V is the direct sum of these two subspaces. It suffices to prove our contention if V is not the direct sum of two $\{g\}$-invariant subspaces that are defined over k, and in this case, if c is a characteristic root of g, we must have $(g - ce)$ nilpotent. Hence we may suppose that each $g \in \{g\}$ is nilpotent, and it suffices to reduce $\{g\}$ to triangular form over k; this we do by noting that the null space of any $g \in \{g\}$ is $\{g\}$-invariant and using induction on dim V. Applying this to the case of a single matrix g that is rational over k, invertible, and has all of its characteristic roots in k, we get that g_s and g_u are rational over k. If g is an arbitrary invertible matrix that is rational over k then the unicity of the decomposition $g = g_s g_u$ shows that g_s and g_u are purely inseparable over k. If the characteristic roots of g are separably algebraic over k then g_s and g_u, by what we have shown above, are also separably algebraic over k, and hence they are rational over k. Noting that g and g_s have the same characteristic roots, it remains only to prove the first statement. What we have done shows that a matrix g that is rational over k is semisimple if and only if its minimal polynomial (over some extension field of k that contains the characteristic roots of g) has no multiple roots, so the first statement follows from the lemma.

PROPOSITION 2. - *Let G, G' be algebraic groups of matrices, $\tau: G \to G'$ a rational homomorphism, and let $g \in G$. Then the characteristic roots of $\tau(g)$ are power products of the characteristic roots of g.*

The characteristic roots of g are the same as those of g_s and those of $\tau(g)$ the same as those of $(\tau(g))_s = \tau(g_s)$; hence we may suppose that g is semisimple. Taking g to be in diagonal form and restricting G, if necessary, to its intersection with the full diagonal group, we see that it is permissible to suppose that G is a group of diagonal matrices. In this case, if $X_1, \dots, X_n$ denote coordinates for the diagonal elements of our matrices, G is defined by a set of monomial equations $\{ X_1^{m_1} \dots X_n^{m_n} = 1 \}$, where $(m_1, \dots, m_n)$ ranges over a set of n-tuples of integers. Since the set of all such n-tuples is a subgroup of the free abelian group of rank n, we can find a basis $\{ (a_{1i}, \dots, a_{ni}) \}$, $i = 1, \dots, n$, for the free abelian group (each a_{ji} being an integer) and integers $d_1, \dots, d_n \geq 0$ such that our subgroup is generated by the n-tuples $(d_i a_{1i}, \dots, d_i a_{ni})$, $i = 1, \dots, n$. The map $(X_1, \dots, X_n) \to (X_1^{a_{11}} \dots X_n^{a_{n1}}, \dots, X_1^{a_{1n}} \dots X_n^{a_{nn}})$ is a biregular automorphism of the full diagonal group, and clearly the multiplicative group generated by the characteristic roots of any diagonal matrix is unaltered by the automorphism. We may thus assume that $X_1^{d_1} = 1, \dots, X_n^{d_n} = 1$ is a set of equations defining G; in particular G is biregularly isomorphic to the direct product of a certain number of multiplicative groups G_m and a number of finite cyclic groups. (Note that in the case of characteristic $p \neq 0$, no $d_i > 0$ is a multiple of p). Since G is commutative and consists of semisimple elements, the same is true of $\tau(G)$; taking $G' = \tau(G)$, we can assume that G' is in diagonal form. Thus it suffices to take $G' \subset GL(1)$, so that τ is a numerical function $\tau: G \to G_m$. If $(x_1, \dots, x_n) \in G$, then $(x_1, \dots, x_n) = (x_1, 1, \dots, 1) \cdot (1, x_2, 1, \dots, 1) \cdots (1, \dots, 1, x_n)$, each of these factors is in G, and $\tau(x_1, \dots, x_n) = \tau(x_1, 1, \dots, 1) \cdots \tau(1, \dots. 1, x_n)$. We may thus assume that $n = 1$. If $d_1 > 0$, let α be a primitive d_1-th root of unity; then $(\alpha) \in G$ and $(\tau(\alpha))^{d_1} = \tau(\alpha^{d_1}) = 1$, so we can write $\tau(\alpha) = \alpha^r$, for some integer r. If $g \in G$, we have $g = (\alpha^t)$, for some integer t, so $\tau(g) = \alpha^{rt} = (\alpha^t)^r$. Finally, if $d_1 = 0$ we have $G = G_m$. If x is a coordinate function on G_m then $\tau(x)$ is a rational function of x, everywhere defined and nowhere 0 or ∞ for $x \in G_m$, so we must have $\tau(x) = cx^\nu$, for some constant c and some integer ν. Since $\tau(1) = 1$, we have $\tau(x) = x^\nu$, completing the proof.

Prop. 2 shows that if G is any linear algebraic group and $g \in G$, we may speak of the « multiplicative group generated by the characteristic roots of g »; this notion is independent of any matrix representation of G.

LEMMA. - *Let V be a variety. Then the multiplicative group of rational functions on V which are everywhere defined and nowhere 0 or ∞, modulo the group of nonzero constant functions, is a free abelian group with a finite number of generators.*

That we have a group is clear. If V' is a variety and $\varphi: V' \to V$ an everywhere defined generically surjective rational map, then there is a natural isomorphism from our group into the corresponding group for V', so it suffices to prove the lemma for V'. Hence we may suppose that V is an open

subset of a normal projective variety $\bar{V}$. If $W_1, \ldots, W_r$ are the various components of $\bar{V} - V$ of codimension one on $\bar{V}$ and f is a rational function on V, then the map $f \to (\mathrm{ord}_{W_1} f, \ldots, \mathrm{ord}_{W_r} f)$ induces an isomorphism of the group we are considering into the free abelian group with r generators.

PROPOSITION 3. - *Let G be a connected algebraic group, f a rational function on G which is everywhere defined, nowhere 0 or ∞, and such that $f(e) = 1$. Then the map $g \to f(g)$ is a rational homomorphism from G to G_m.*

By the lemma, the multiplicative group of all functions on G having the same properties as f is finitely generated, so let $f_1, \ldots, f_n$ be a set of generators for this group. Let k be a field of definition for G, f, $f_1, \ldots, f_n$, and let g_1, g_2 be independent generic points of G over k. Considering g_2 as a fixed and g_1 as a variable point of G, $f(g_1 g_2)/f(g_2)$ becomes an everywhere defined function on G that is nowhere 0 or ∞ and that takes on the value 1 at e. Hence there exist integers $s_1, \ldots, s_n$ such that

$$f(g_1 g_2)/f(g_2) = (f_1(g_1))^{s_1} \cdots (f_n(g_1))^{s_n}.$$

This last equation holds for all g_1, $g_2 \in G$, so $f(g_1 g_2)/f(g_2) = f(g_1 e)/f(e)$. That is, $f(g_1 g_2) = f(g_1) f(g_2)$.

PROPOSITION 4. - *Let V be a variety defined over k, $\{ W_\alpha \}$ $(\alpha \in A)$ a set of subvarieties of V each of which is defined over k. Then each component of the smallest algebraic subset of V that contains $\bigcup_{\alpha \in A} W_\alpha$ is defined over k.*

Let W be the smallest algebraic set containing $\bigcup_{\alpha \in A} W_\alpha$. If $W^{(1)}, \ldots, W^{(s)}$ are the components of W then each W_α is contained in some $W^{(i)}$. It follows that $W^{(i)}$ is the smallest algebraic set containing $\bigcup_{\alpha \in A_i} W_\alpha$, for a certain subset A_i of A. Thus we may suppose that W is irreducible. If V' is any k-open subset of V, then $W \cap V'$ is the smallest algebraic subset of V' that contains each $W_\alpha \cap V'$. Thus we may suppose that V is embedded in an affine space. Replacing each variety by its closure in the affine space, we see that it suffices to assume that V is itself an affine space. Let $X_1, \ldots, X_n$ be coordinates for this affine space and suppose that $F(X)$ is a polynomial vanishing on W. Write $F(X) = \Sigma_{i=1}^{\nu} c_i F_i(X)$, where each $F_i(X) \in k[X]$ and $c_1, \ldots, c_\nu$ are quantities that are linearly independent over k. If p_α is a generic point of W_α over $k(c_1, \ldots, c_\nu)$, we get $0 = F(p_\alpha) = \Sigma c_i F_i(p_\alpha)$, and the linear disjointness of $k(p_\alpha)$ and $k(c_1, \ldots, c_\nu)$ over k implies that each $F_i(p_\alpha) = 0$; i. e. each F_i vanishes on W. So the ideal of W has a basis in $k[X]$. Hence W is defined over k.

COROLLARY. - *Let G be an algebraic group defined over k and let $\{ W_\alpha \}$ $(\alpha \in A)$ be a set of subvarieties of G each of which is defined over k. Then each component of the smallest algebraic subgroup of G that contains $\bigcup_{\alpha \in A} W_\alpha$ is defined over k. If the points of $\bigcup_{\alpha \in A} W_\alpha$ are closed under the group multiplication, then this smallest algebraic subgroup is the smallest algebraic subset of G containing $\bigcup_{\alpha \in A} W_\alpha$.*

If $\alpha_1, \alpha_2 \in A$ and p_1, p_2 are independent generic points of W_{α_1} and W_{α_2} respectively over k, then any algebraic subgroup of G that contains W_{α_1} and W_{α_2} must contain the locus of $p_1 p_2$ over k, since $W_{\alpha_1} W_{\alpha_2}$ is dense in this locus. Thus, enlarging our set $\{ W_\alpha \}$ if necessary, we may assume that the points of $\cup_{\alpha \in A} W_\alpha$ are closed under group multiplication. Let Γ be the smallest algebraic set containing $\cup_{\alpha \in A} W_\alpha$; we know that each component of Γ is defined over k. If $p_\alpha \in W_\alpha$, then the algebraic set $p_\alpha^{-1}\Gamma \supset W_{\alpha'}$, for any $\alpha' \in A$, so $p_\alpha^{-1}\Gamma \supset \Gamma$. Since the components of Γ and those of $p_\alpha^{-1}\Gamma$ are in one-one biregular birational correspondence, $p_\alpha^{-1}\Gamma = \Gamma$. For any fixed $\gamma \in \Gamma$, the set of points $p \in G$ such that $p^{-1}\gamma \in \Gamma$ is an algebraic subset of G, so the set of all points $p \in G$ such that $p^{-1}\Gamma \subset \Gamma$ is an algebraic subset of G that contains each W_α. Thus $\Gamma^{-1}\Gamma \subset \Gamma$, so Γ is an algebraic subgroup of G.

There are a number of obvious extensions of the corollary. For example, if $\{ W_\alpha \}$ $(\alpha \in A)$ are subvarieties of V that do not necessarily have a common field of definition but whose points are closed under group multiplication, the smallest algebraic set containing $\cup_{\alpha \in A} W_\alpha$ is still an algebraic subgroup of G; the difficulty here is that the universal domain may not be of infinite transcendence degree over the compositum of the fields of definition of the various W_α's, but this difficulty is eliminated by a temporary extension of the universal domain. Also, if the W_α's are all subvarieties of G that are defined over k and pass through e, then the sets by which we augmented $\{ W_\alpha \}$ in the proof of the corollary are also subvarieties of G that are defined over k, pass through e, and contain some of the original sets W_α; since algebraic subsets of G are of bounded dimension, it follows that the smallest algebraic subgroup of G containing $\cup_{\alpha \in A} W_\alpha$ must be the subvariety in our augmented set of W_α's that has maximal dimension, and this has as generic point over k a point $p_1 p_2 \dots p_\nu$, where the p_i's are independent generic points over k of various of the varieties W_α. Finally, if $\{ W_\alpha \}$ is an arbitrary set of subvarieties of G that pass through e (but do not necessarily have a common field of definition), for any finite subset A' of A we can consider the smallest algebraic subgroup of G containing $\cup_{\alpha \in A'} W_\alpha$, and the subgroup of maximal dimension which can be obtained in this way is the smallest algebraic subgroup of G that contains $\cup_{\alpha \in A} W_\alpha$. Thus for any set $\{ W_\alpha \}$ $(\alpha \in A)$ of subvarieties of G that pass through e, the smallest algebraic subgroup Γ of G that contains $\cup_{\alpha \in A} W_\alpha$ is the same as that got from a finite subset of $\{ W_\alpha \}$, and is connected. If k is a field of definition for G and enough of the W_α's, then k is also a field of definition for Γ, and a generic point of Γ over k can be got as the group product of independent generic points over k of certain of the W_α's that are defined over k. Since any generic point of Γ over k must be of the same form, and since any point of Γ is the product of two of its generic points over k, we see that Γ is simply the group generated by all the points of $\cup_{\alpha \in A} W_\alpha$.

It may be worthwhile to indicate explicitly a slight extension of the preceding paragraph: Let G be an algebraic group, let $\{W_\alpha\}$ $(\alpha \in A)$ be a set of subvarieties of G that pass through e, and let W_α', for each $\alpha \in A$, be a nonempty open subset of W_α. Then the subgroup generated by the points of $\cup_\alpha W_\alpha'$ is the same as that generated by the points of $\cup_\alpha W_\alpha$, and hence is a connected algebraic subgroup of G. (For suppose, as we may, that the set A is finite, let k be a field of definition for G and each W_α, and let each W_α' be k-open on W_α. We have shown at the end of the last paragraph that each point of the group generated by $\cup_\alpha W_\alpha$ is the product of generic points over k of various of the W_α's. Since a generic point over k of W_α is in W_α', we are done). An easy consequence in the following: Let G be an algebraic group defined over k and let V, W be subvarieties of G that are defined over k such that at least one point of V commutes with a point of W. Then $[V, W]$ (i. e., the group generated by all commutators of points of V with points of W) is a connected algebraic subgroup of G that is defined over k. For $[V, W]$ contains an open subset of the locus over k of $vwv^{-1}w^{-1}$, where v, w are independent generic points over k of V, W respectively.

2. Solvable groups.

As in [5], the word « solvable » (and, a fortiori, the word « nilpotent »), when applied to an algebraic group, presupposes that the group is linear. The unipotent elements of a connected solvable algebraic group G are known to form a connected normal algebraic subgroup G_u of G such that G/G_u is a torus. If k is a field of definition of G, then G_u is left fixed by all k-automorphisms of the universal domain, hence is k-closed. If T is any maximal torus of G, the map $T \times G_u \to G$ defined by $t \times g_u \to tg_u$ is birational and surjective; if G is nilpotent, then the maximal torus T is unique, consisting precisely of all semisimple elements of G, and is central, and G is biregularly isomorphic to the direct product $T \times G_u$. (For all these matters cf. [1]). By the theorem of LIE-KOLCHIN, a connected solvable algebraic group of matrices G can be reduced to triangular form; in fact if k is a field of definition for G, then G can be reduced to triangular form by a matrix that is rational over the algebraic closure $\bar{k}$ of k. (The simplest proof of the latter modification is probably got by noting that if H_1, H_2 are any k-closed algebraic sets of matrices, then the invertible matrices a such that $aH_1a^{-1} \subset H_2$ constitute a k-closed subset of the full linear group). One knows that if G is a torus then G is reducible to diagonal form, so if G is a torus defined over k, then G is reducible to diagonal form over k.

PROPOSITION 5. – *Let G be a connected algebraic group of matrices defined over k, with g a generic point of G over k. Then a necessary and sufficient condition that G be reducible to triangular form over k is that all the characteristic roots of g be contained in $k(g)$. If this condition is verified, it also holds*

for any rational representation of G that is defined over k, the unipotent part G_u of G is also defined over k, and G can be reduced to triangular form over k in such a way as to send any given torus of G that is defined over k into diagonal form.

The necessity of the given condition is clear, so suppose that all the characteristic roots of g are in $k(g)$. If $f(g)$ is one of these characteristic roots, then the determinant $|g - f(g)e|$ is zero, so the rational function $f \in k(G)$ is integrally dependent on the ring of everywhere finite rational functions on G, hence is itself an everywhere finite rational function on G. In particular, since G is a nonsingular variety f is everywhere defined on G. If $g' \in G$, the equation $|g' - f(g')e| = 0$ shows that $f(g')$ is a characteristic root of g'; thus f is nowhere 0 or ∞ on G and assumes the value 1 at e. By Prop. 3, the map $g \to f(g)$ gives a rational homomorphism defined over k from G into G_m. Suppose $G \subset GL(n)$, and that $f_1(g), \ldots, f_n(g)$ are all the characteristic roots of g, each repeated as many times as it occurs. Then $\Pi_{i=1}^n (g - f_i(g)e) = 0$, so for any $g' \in G$ we have $\Pi_{i=1}^n (g' - f_i(g')e) = 0$, implying that the characteristic roots of g' are to be found among $f_1(g'), \ldots, f_n(g')$. The map $g \to (f_1(g), \ldots, f_n(g))$ gives a rational homomorphism defined over k from G into a torus, and each element of the kernel H of this homomorphism is unipotent. Since H is solvable and G/H is commutative, G is solvable. Now let $\varphi: G \to G'$ be a surjective rational representation that is defined over k. Then G' is connected, solvable, and defined over k, hence reducible to triangular form over $\bar{k}$. Thus the characteristic roots of $\varphi(g)$ are all contained in $\bar{k}(\varphi(g))$. But by our assumptions and Prop. 2, these characteristic roots are contained in $k(g)$, hence in $\bar{k}(\varphi(g)) \cap k(g)$. But $\bar{k}$ and $k(g)$ are linearly disjoint over k, so (by [6, § 2, Lemma 3]) this intersection is precisely $k(\varphi(g))$; hence G' also satisfies the conditions of the proposition. We now prove the part about the reducibility of G to triangular form over k by induction on the dimension of the underlying vector space V on which G operates. If $\dim V = 0$ there is nothing to prove, so suppose $\dim V > 0$. Since G is reducible to triangular form over $\bar{k}$, there exists a nonzero vector $v \in V$ that is rational over $\bar{k}$ and is a characteristic vector for all $\gamma \in G$. Write $v = \Sigma_{i=1}^{\nu} \alpha_i v_i$, where each $v_i \in V$ is nonzero and rational over k and $\alpha_1, \ldots, \alpha_\nu \in \bar{k}$ are linearly independent over k. Then $g(v) = f(g)v$, where $f(g) \in k(g)$ is one of the characteristic roots of g, so $\Sigma \alpha_i(g(v_i) - f(g)v_i) = 0$. By the linear disjointness of $\bar{k}$ and $k(g)$ over k, we get $g(v_i) = f(g)v_i$ for $i = 1, \ldots, \nu$. Thus there exists a nonzero vector $v_i \in V$ that is rational over k and is a characteristic vector for each $\gamma \in G$. Application of our induction assumption to the natural representation of G by a group of linear transformations on the vector space $V/(v_i)$ shows that G is reducible to triangular form over k. If G is a torus, then V is direct sum of invariant one-dimensional subspaces defined over $\bar{k}$, and the above proof shows that these subspaces may actually be taken to be

defined over k; thus if G is a torus it is reducible to diagonal form over k. Now suppose that the group G satisfies the condition of the proposition and that T is a torus of G that is defined over k. Since G is reducible to triangular form over k, T also satisfies the condition of the theorem. Let $V = V_0 \supset V_1 \supset V_2 \supset \ldots$ be G-invariant subspaces of V, all defined over k, such that for $i = 0, 1, \ldots$, $\dim V_i/V_{i+1} = 1$. The natural representation of T by a group of linear transformations on V_i is reducible over k to diagonal form, so there exists a vector $v_i \in V_i$, $v_i \notin V_{i+1}$ that is rational over k and is a characteristic vector for each $t \in T$. If we use the basis $(v_0, v_1, \ldots)$ of V, we reduce G to triangular form over k in such a way that T goes into a diagonal group. It remains only to show that G_u is defined over k. Let $\tau: G \to G/G_u$ be the natural rational homomorphism and suppose that the torus G/G_u is taken to be an algebraic group of matrices in diagonal form. Suppose our point g is generic for G over the compositum of k and a field of definition of τ. Each diagonal element of $\tau(g)$ is a characteristic root of $\tau(g)$, hence (by Prop. 2 and our assumptions) is an element of $k(g)$. Thus the separable rational homomorphism τ is defined over k. The kernel G_u of τ is a rational cycle over k [5, Prop. 1, Cor.]. Since G_u is connected, it is defined over k. Q. E. D.

If G is any connected solvable algebraic group of matrices that is defined over k, Prop. 5 shows that there is a smallest extension field $k_1 \supset k$ over which G can be reduced to triangular form (namely, $k_1 =$ the smallest overfield of k that is a field of definition for the various rational functions on G got from the characteristic roots). If a certain matrix rational over $\bar{k}$ reduces G to triangular form, so does any of its conjugates over k. Thus k_1 is a finite normal algebraic extension of k. If G' is an algebraic group of matrices that is biregularly isomorphic over k to G, then by Prop. 2 the two fields k_1 and k_1' are equal. Thus a well-defined extension field k_1 of k can be associated with any connected solvable algebraic group defined over k.

COROLLARY 1. - *If G is an algebraic group of matrices each of whose components is defined over k and each of whose elements is unipotent, then G is reducible to triangular form over k.*

Even when G is not connected it can be reduced to triangular form (a result of KOLCHIN which appears in [1, Ch. IV]), so the only modification which need be made in the pertinent part of the above proof is to replace the single point g by a set of generic points over k of the various components of G.

We recall that a connected solvable algebraic group G is said to have k as a field of definition for its solvability if G possesses a normal chain of connected algebraic subgroups (starting with G and going down to $|e|$), each defined over k, whose successive factor groups (being taken, together with the various canonical rational homomorphisms involved, to be defined over k)

are each biregularly isomorphic over k to either the additive group G_a or the multiplicative group G_m [5, § 4].

COROLLARY 2. - *If the connected algebraic group of matrices G, defined over the perfect field k, satisfies the condition of Prop. 5 then k is a field of definition for the solvability of G. Furthermore, a normal chain of algebraic subgroups of G exhibiting this fact can be found which consists entirely of subgroups that are normal in G.*

We may assume that G is in triangular form. If $\mathcal{T}$ is the full group of triangular matrices, it is known that $\mathcal{T}$ has a normal chain $\mathcal{T} = \mathcal{T}^{(0)} \supset \mathcal{T}^{(1)} \supset \ldots$ such that each $\mathcal{T}^{(i)}$ is normal in $\mathcal{T}$ and defined over the prime field, the unipotent part $\mathcal{T}_u$ of $\mathcal{T}$ is $\mathcal{T}^{(n)}$ (if $\mathcal{T} \subset GL(n)$), and the dimensions of the groups in this chain go down one at each step. $G_u = G \cap \mathcal{T}^{(n)}$, and the connected k-closed groups $G = G \cap \mathcal{T}^{(0)} \supset (G \cap \mathcal{T}^{(1)})_0 \supset (G \cap \mathcal{T}^{(2)})_0 \supset \ldots$ are each normal in G and the dimensions of the groups in this chain go down by at most one at each step. If we eliminate repetitions, we get a normal chain of connected normal k-closed subgroups of G, say $G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \ldots$, going down in dimension by one at each step and such that $G_u = G^{(\nu)}$ for some $\nu \geq 0$. Since k is perfect, each $G^{(i)}$, $i = 0, 1, \ldots$, is defined over k, so we may take the various natural rational homomorphism $G^{(i)} \to G^{(i)}/G^{(i+1)}$ to be defined over k. For any $i < \nu$, $G^{(i)}/G^{(i+1)}$ is biregularly isomorphic over k to a subgroup of the torus $G/G^{(i+1)}$. If we take $G/G^{(i+1)}$ to be an algebraic group of matrices, the proposition shows that it is reducible to diagonal form over k, so $G^{(i)}/G^{(i+1)}$ is biregularly isomorphic over k to a group of matrices in diagonal form, hence to G_m. On the other hand if $i \geq \nu$, then $G^{(i)}/G^{(i+1)}$ consists entirely of unipotent elements, so it remains only to show that if H is an algebraic group defined over the perfect field k that is biregularly isomorphic to G_a over some extension field of k, then H is biregularly isomorphic to G_a over k. Since k is perfect, the genus of the curve H does not change upon ground field extensions, so $k(H)/k$ is of genus zero; since H has a rational point over k, $k(H)$ is a simple transcendental extension of k, so we may take H to be a k-open subset of the projective line D. $(D - H)$ consists of only one point, which must be purely inseparable over k, hence rational over k. If we take (0) to be the identity of H and (∞) the point $(D - H)$, it is trivial to verify that the group operation on H is got by the addition of coordinates.

Cor. 2 shows that if G is a connected solvable algebraic group defined over the field k, then $\bar{k}$ is a field of definition for the solvability of G; if G contains only unipotent elements and k has characteristic p, then $k^{p^{-\infty}}$ is a field of definition for the solvability of G. The author does not know if there exists a minimal overfield of k that is a field of definition for the solvability of G.

We may make the following comment relative to the latter part of the

above proof: If G is an algebraic group defined over k, biregularly isomorphic to G_a (over some extension field of k), and if G is a rational curve over k, then G is biregularly isomorphic to G_a over k, except possibly when k has characteristic two. For we may take G to be the projective line D minus a point (P) that is purely inseparable over k. If x_1, x_2 are independent variables over k and $x_1 \circ x_2$ denotes the coordinate function of the group product of the points (x_1) and (x_2), then the relations $k(x_1, x_2) = k(x_1, x_1 \circ x_2) = k(x_2, x_1 \circ x_2)$ show that $x_1 \circ x_2 = (a + bx_1 + cx_2 + dx_1x_2)/(e + fx_1 + gx_2 + hx_1x_2)$, for certain $a, \ldots, h \in k$, and since $P = x_1 \circ P$ we get that P is quadratic over k. If k has characteristic $\neq 2$, P must be rational over k and the proof given above obtains. A counterexample in the case of a field k of characteristic two is given by $x_1 \circ x_2 = (x_1 + x_2)/(1 + ax_1x_2)$, where $a \in k$, $a \notin k^2$. Here an additive parameter for the group is $x/(x - a^{-1/2})$.

The next two propositions will tie together more closely the notion of a field of definition for the solvability of a group and the content of Prop. 5.

PROPOSITION 6. - *Let G be a connected solvable algebraic group, k a field of definition for its solvability, and $\tau: G \to G'$ a surjective rational homomorphism defined over k. Then G' also has k as a field of definition for its solvability.*

If $\dim G = 1$, embed G in the usual way in the projective line D ($D = G \cup (\infty)$ or $G \cup (0) \cup (\infty)$ according as G is a G_a or G_m). If we exclude the trivial case $\dim G' = 0$, G' is a curve that is rational over k; since G' is nonsingular, it can be identified with a k-open subset of a projective line D'. τ then extends to an everywhere defined surjective map $\tau: D \to D'$, and $D' = G' \cup \tau(\infty)$ or $G' \cup \tau(0) \cup \tau(\infty)$. The points $\tau(0)$ and $\tau(\infty)$ are distinct and rational over k, so by changing coordinates on D' we get $\tau(0) = 0$ and $\tau(\infty) = \infty$; if G is a multiplicative group we can also take $\tau(1) = 1$. One shows immediately that G' is either G_a or G_m. Finally, for a G of arbitrary dimension, let $G = G^{(0)} \supset G^{(1)} \supset \ldots$ be a normal chain exhibiting k as a field of definition for the solvability of G. Then $\tau G = \tau G^{(0)} \supset \tau G^{(1)} \supset \ldots$ is a normal chain for G' each member of which is defined over k. Taking the natural homomorhism from $\tau G^{(i)}$ to $\tau G^{(i)}/\tau G^{(i+1)}$ to be defined over k, we need only show that the latter group is biregularly isomorphic over k to G_a, G_m or the trivial group. But we have a natural surjective rational homomorphism defined over k from $G^{(i)}$ to $\tau G^{(i)}/\tau G^{(i+1)}$ and the kernel of this homomorphism contains $G^{(i+1)}$. Hence there is a natural surjective rational homomorphism defined over k from $G^{(i)}/G^{(i+1)}$ to $\tau G^{(i)}/\tau G^{(i+1)}$. Since $\dim G^{(i)}/G^{(i+1)} = 1$, we are reduced to the first part of the proof.

The following lemma and proposition give slight sharpenings of the corresponding results in [1, Ch. IV]. The proofs follow BOREL' s.

LEMMA. - *Let the connected solvable algebraic group G operate regularly on the complete variety V and let k be a field of definition for the solvability of G, for V, and for the operation of G on V. Then if V possesses a point*

that is rational over k, it possesses a point that is rational over k and left fixed by all elements of G.

This is trivial if $\dim G = 0$, so suppose that $\dim G > 0$ and use induction. Let G_1 be a connected normal algebraic subgroup of G having k as a field of definition for its solvability and such that, taking the natural rational homomorphism from G to G/G_1 to be defined over k, we have $G/G_1 = G_a$ or G_m. Then G_1 operates regularly on V, so by our induction assumption there exists a point $p \in V$ that is rational over k and such that $g_1 p = p$ for all $g_1 \in G_1$. Let g be a generic point of G over k. Then G operates regularly on the locus of gp over k, so we may suppose that V is this locus; i. e. V is a prehomogeneous space for G. G_1 operates trivially on Gp, hence on V, so by [5, Th. 5] G/G_1 operates on V, and this operation is defined over k. It is clear that V is a prehomogeneous space for G/G_1, but not at all clear that G/G_1 operates regularly on V. So let V' be a variety birationally equivalent to V that is a homogeneous space for G/G_1 (cf. [8]); then V' is also homogeneous for G, hence (by the unicity of homogeneous spaces) is biregularly equivalent to $Gp \subset V$. Thus Gp is a homogeneous space for G/G_1. Embed G/G_1 in the usual way in the projective line D ($D = (G/G_1) \cup (\infty)$ or $(G/G_1) \cup (0) \cup (\infty)$). The rational map $\tau: G/G_1 \to Gp$ defined by $\tau(gG_1) = gp$ is defined over k and extends to an everywhere defined surjective map $\tau: D \to V$. Hence $(V - Gp) \subset \tau(D - G/G_1)$ consists of points that are rational over k. If V is a curve, it is a rational curve, and any birational transformation on it admits at least one fixed point. Since G/G_1 is commutative, if $V = Gp$ we must have $Gp = p$. In the contrary case, $V - Gp$ consists of one or two points that are rational over k and are permuted among themselves by the elements of G. If q is one of them, the connectedness of G implies $Gq = q$.

PROPOSITION 7. - *If the connected solvable algebraic group of matrices G has k as a field of definition for its solvability, then G is reducible to triangular form over k.*

Let S be the underlying vector space of G. A flag of S is a maximal sequence of vector subspaces of S each of which properly contains its successor. The flag manifold of S (i. e. the variety of all flags) is complete, defined over the prime field, a homogeneous space with respect to the full linear group, and contains a rational point. A flag that is rational over k and left fixed by G exists by the lemma. Taking a basis of S that is adapted to this flag reduces G to triangular form.

PROPOSITION 8. - *Let V be a homogeneous space with respect to the connected solvable algebraic group G, all defined over a field k which is a field of definition for the solvability of G. Then $k(V)$ is a purely transcendental extension of k.*

By [5, Th. 10] there exists a point $a \in V$ that is rational over k. If g is generic for G over k then ga is generic for V over k and $k(ga) \subset k(g)$. If

dim $G = 1$ we get the proposition from LÜROTH' s theorem if dim $V = 1$ and from the triviality $V = a$ if dim $V = 0$. Hence suppose that dim $G > 1$ and use induction on dim G. Let G_1 be a connected normal algebraic subgroup of G having k as a field of definition for its solvability and such that, if the natural homomorphism $\varphi: G \to G/G_1$ is taken to be defined over k, G/G_1 is biregularly isomorphic over k to G_a or G_m. Let W be the variety of G_1-orbits on V, both W and the natural rational map $\tau: V \to W$ being taken to be defined over k. By [5, Th. 5], G/G_1 operates on W, this operation is defined over k, and is such that if g, v are independent generic points of G, V respectively over k then $\varphi g(\tau v) = \tau(gv)$. Since gv is generic for V over $k(v)$, $\varphi g(\tau v)$ is generic for W over $k(\tau v)$, so W is a prehomogeneous space with respect to G/G_1; without any loss of generality we assume that W is homogeneous for G/G_1. Considering W as a homogeneous space with respect to G, [5, Prop. 1] shows that the map $\tau: V \to W$ is everywhere defined and surjective, and we have $\varphi\gamma(\tau\alpha) = \tau(\gamma\alpha)$ for any $\gamma \in G$, $\alpha \in V$. If v_1, v_2 are generic for V over k then $\tau v_1 = \tau v_2$ if and only if $v_2 \in Gv_1$; hence, by transitivity, the same is true for all v_1, $v_2 \in V$. Thus, if w is generic for W over k and if $\sigma: W \to V$ is a cross section ([5, Th. 10]) for the map $\tau: V \to W$, σ being taken to be defined over k, we have $\tau^{-1} | w | = G_1(\sigma w)$. Since $\tau^{-1} | w |$ includes a generic point of V over k, we deduce that if g_1 is generic for G_1 over $k(w)$ then $g_1(\sigma w) \in G_1(\sigma w)$ is generic for V over k, so that $k(V)$ is k-isomorphic to $k(g_1(\sigma w))$. It also follows that the closed subset $\tau^{-1} | w | = G_1(\sigma w)$ of V is a homogeneous space with respect to G_1, defined over $k(w)$ and having $g_1(\sigma w)$ as a generic point over $k(w)$. By our induction assumption, $k(w, g_1(\sigma w))$ is a purely transcendental extension of $k(w)$. Since w is generic over k for the (G/G_1)-homogeneous space W and dim $G/G_1 = 1$, $k(w)$ is a purely transcendental extension of k. Since $\tau(g_1(\sigma w)) = w$, we have $k(g_1(\sigma w)) = k(w, g_1(\sigma w)) =$ a purely transcendental extension of k.

PROPOSITION 9. - *If G is a connected nilpotent algebraic group that is defined over k, then the maximal torus of G is also defined over k.*

Both G_u and the maximal torus T of G are invariant under all k-automorphisms of the universal domain, hence k-closed, hence defined over a purely inseparable algebraic extension k' of k. There is nothing to prove if the characteristic of k is zero, so suppose k has characteristic $p \neq 0$. Let t, u be independent generic points over k' of T, G_u respectively. If n is sufficiently large, $u^{p^n} = e$ and $(tu)^{p^n} = t^{p^n}$ is a generic point of T over k'. Since G is defined over k and tu is generic for G over k', tu is generic for G over k and $k(tu)$ is a regular extension of k. Hence $k((tu)^{p^n})$ is a regular extension of k, so T is defined over k.

If G is a connected nilpotent group defined over k then G_u need not be defined over k. In the next paragraph we give a counterexample in which G is commutative. In order to do this in a reasonably wide setting we discuss a well-known procedure for constructing linear algebraic groups from asso-

ciative algebras; a particular case is the algebraic group associated with the multiplicative group of an algebraic extension field.

A subset R of the ring of all $n \times n$ matrices (with coefficients in the universal domain) that contains the unit matrix and is closed under matrix multiplication gives rise to a connected algebraic subgroup G of $GL(n)$ in an easy way: namely G consists of all invertible matrices in the linear space of matrices spanned by R. It is clear that if each matrix of R is rational over k, then G is defined over k. If, in addition, R is an algebra over k then the points of G that are rational over k are precisely the units of R, and if k is infinite these points are dense in G. If now A is any associative algebra with unit element of dimension n over k, the regular representation of A gives rise to such a ring R and hence to a group G of dimension n. To be explicit, if $\omega_1, \ldots, \omega_n$ is a k-basis of A, to each $\omega \in A$ we associate the matrix $\varphi(\omega) = (\alpha_{ij})$ which is rational over k and satisfies $\omega\omega_i = \sum_{j=1}^{n} \alpha_{ji}\omega_j$, $i = 1, \ldots, n$; the map $\omega \to \varphi(\omega)$ is then an isomorphism from A to an algebra of matrices from which we get our group G, and G does not depend essentially on the basis (ω). For example, if A is an algebraic extension field K of k and $[K:k] = n$, then G is a connected commutative group of dimension n; here G is the direct product of a torus and a group of unipotent matrices, whose dimensions we now calculate. For any $\omega \in K$, ${}^t\varphi(\omega)$ applied to the vector $(\omega_1, \ldots, \omega_n)$ gives the vector $(\Sigma_j \alpha_{j1}\omega_j, \ldots, \Sigma_j \alpha_{jn}\omega_j) = (\omega\omega_1, \ldots, \omega\omega_n)$, so ω is a characteristic root of ${}^t\varphi(\omega)$, hence also of $\varphi(\omega)$. If $x_1, \ldots, x_n$ are algebraically independent over k then $\omega_1, \ldots, \omega_n$ are still a basis for $K(x)/k(x)$, and if we extend φ to this larger algebra we get that $\varphi(\Sigma x_i\omega_i) = \Sigma x_i\varphi(\omega_i)$ has $\Sigma x_i\omega_i$ has a characteristic root. But the matrix $\Sigma x_i\varphi(\omega_i)$ is rational over $k(x)$ so for any k-isomorphism σ of K, $x_i\omega_i{}^\sigma$ is a characteristic root of $\Sigma x_i\varphi(\omega_i)$. The various characteristic roots we obtain this way as σ ranges over the distinct k-isomorphisms of K are algebraically independent over k. Hence G contains a torus of dimension $\geq [K:k]_s$. Now let λ be transcendental over $k(x)$. Then the norm $N_{K(x,\lambda)/k(x,\lambda)}(\Sigma x_i\omega_i - \lambda)$ equals the determinant $|\varphi(\Sigma x_i\omega_i - \lambda)| = |\Sigma x_i\varphi(\omega_i) - \lambda e|$, so from the definition of the norm as a product of conjugates we deduce that the characteristic polynomial of $\Sigma x_i\varphi(\omega_i)$ has each root repeated at least $[K:k]_i$ times. Hence the characteristic roots of $\Sigma x_i\varphi(\omega_i)$ are precisely the distinct $\Sigma x_i\omega_i{}^\sigma$'s, each repeated $[K:k]_i$ times. Thus the maximal torus of G has dimension exactly $[K:k]_s$, and G_u has dimension $(n - [K:k]_s) = [K:k]_s([K:k]_i - 1)$. In the special case where $K = k(\alpha)$, and $\alpha^n = a \in k$ is the irreducible equation for α, we can let $\omega_i = \alpha^{i-1}$ for $i = 1, \ldots, n$ and the generic point $\Sigma x_i\varphi(\omega_i)$ of G over k has the form

$$\begin{pmatrix} x_1 & ax_n & ax_{n-1} & \ldots & ax_2 \\ x_2 & x_1 & ax_n & \ldots & ax_3 \\ x_3 & x_2 & x_1 & \ldots & ax_4 \\ \vdots & \vdots & \vdots & & \vdots \\ x_{n-1} & x_{n-2} & x_{n-3} & \ldots & ax_n \\ x_n & x_{n-1} & x_{n-2} & \ldots & x_1 \end{pmatrix}.$$

If we take $n = p \neq 0$ the characteristic of k and $\alpha \notin k$, $\alpha^p = a \in k$, the maximal torus of G has dimension 1 and is merely the group of scalar matrices. The determinant of the matrix above is simply $(\Sigma x_i \alpha^{i-1})^p$, so G_u is given by the equation $\Sigma_{i=1}^p x_i \alpha^{i-1} = 1$, hence is not defined over k.

PROPOSITION 10. - *Let G be a torus defined over the field k. Then $k(G)$ is k-isomorphic to a subfield of a purely transcendental extension of k.*

The proof we give is essentially the same as that given by CHEVALLEY in [2, § IV] for the case of characteristic zero. Take G to be an algebraic group of matrices. The points of G that are rational over k_s, the separable part of the algebraic closure of k, are dense in G. By Prop. 1, these points have all of their characteristic roots in k_s, hence can be simultaneously reduced to diagonal form over k_s. Thus G can be reduced to diagonal form over a finite separable normal algebraic extension K of k. Let a be a matrix rational over K such that aGa^{-1} is in diagonal form. The group aGa^{-1} is defined by monomial equations, hence is defined over the prime field, so if σ is any k-automorphism of K we have $(aGa^{-1})^\sigma = aGa^{-1}$, that is, $a^\sigma G (a^\sigma)^{-1} = aGa^{-1}$. If $\dim G = r$, a generic point of aGa^{-1} over k is of the form $f(u_1, \ldots, u_r)$, where $u_1, \ldots, u_r$ are quantities that are algebraically independent over k, $f(u_1, \ldots, u_r)$ is a diagonal matrix each of whose diagonal elements is a power product of $u_1, \ldots, u_r$, and $k(f(u)) = k(u)$. For any automorphism σ of K over k, $(a^\sigma)^{-1} f(u_1, \ldots, u_r) a^\sigma \in G$. Let $\omega_1, \ldots, \omega_n$ be a basis of K over k and $\| t_{ij} \|$ $(i = 1, \ldots, r;\ j = 1, \ldots, n)$ be quantities that are algebraically independent over k, and define $F(\| t_{ij} \|) = \prod_\sigma (a^\sigma)^{-1} f(t_{11}\omega_1^\sigma + \ldots + t_{1n}\omega_n^\sigma, \ldots, t_{r1}\omega_1^\sigma + \ldots + t_{rn}\omega_n^\sigma) a^\sigma$, where σ ranges over all k-automorphisms of K and the product is taken in G. Since the determinant $\| \omega_j^\sigma \| \neq 0$, the rn various quantities $\Sigma_{j=1}^n t_{ij}\omega_j^\sigma$ are algebraically independent over k, so the n various points $f(t_{11}\omega_1^\sigma + \ldots + t_{1n}\omega_n^\sigma, \ldots, t_{r1}\omega_1^\sigma + \ldots + t_{rn}\omega_n^\sigma)$ are independent generic points of aGa^{-1} over k. Thus $F(\| t_{ij} \|)$ is generic for G over k. But the GALOIS group $\| \sigma \|$ of K over k is naturally isomorphic to the GALOIS group of $K(\| t_{ij} \|)$ over $k(\| t_{ij} \|)$, each σ extending to $K(\| t_{ij} \|)$ by $t_{ij}^\sigma = t_{ij}$ for all i, j. $F(\| t_{ij} \|)$ is rational over $K(\| t_{ij} \|)$ and invariant under each σ, hence rational over $k(\| t_{ij} \|)$. Q. E. D.

An example of CHEVALLEY [2, § V] shows that if G is a torus defined over a field k of characteristic zero that is not algebraically closed, then $k(G)$ need not be a purely transcendental extension of k.

3. The main result.

LEMMA 1. - *Let G be a connected linear algebraic group that is defined over k, $\mathfrak{m}$ the maximal ideal of the local ring of the identity in the function field of G, and τ the rational representation of G given by the action of its inner automorphisms on the vector space $\mathfrak{m}/\mathfrak{m}^2$. Then the kernel of τ is a k-closed nilpotent subgroup of G.*

We first recall some of the facts and notations developed in the proof

of Theorem 13 of [5]. For any $g \in G$, let ω_g denote the automorphism of the function field of G defined by $(\omega_g f)(p) = f(g^{-1}pg)$. Then for any integer $\nu > 0$, ω_g induces a linear transformation $\bar{\omega}_g$ on the vector space $\mathfrak{m}/\mathfrak{m}^\nu$ and the map $\bar{\omega}: g \to \bar{\omega}_g$ is a rational representation. If $\dim G = n$ and $f_1, \ldots, f_n \in \mathfrak{m} \cap k(G)$ are uniformizing parameters at e, then $\mathfrak{m}/\mathfrak{m}^\nu$ has as a basis the various elements $\bar{f}_1^{i_1} \ldots \bar{f}_n^{i_n}$, where $i_1, \ldots, i_n$ are integers ≥ 0 of strictly positive sum $< \nu$ and where $\bar{f}$ denotes the residue class of a function $f \in \mathfrak{m}$ in the natural map $\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^\nu$. Furthermore, $\bar{\omega}$ is given by equations

$$\bar{\omega}_g \bar{f}_i = \sum_{i_1 + \ldots + i_n < \nu} c^{(i)}_{i_1 \ldots i_n}(g) \bar{f}_1^{i_1} \ldots \bar{f}_n^{i_n},$$

where each $c^{(i)}_{i_1 \ldots i_n} \in k(G)$ is an everywhere finite rational function on G. The various functions $c^{(i)}_{i_1 \ldots i_n}$ do not depend on ν (as long as $\nu > i_1 + \ldots + i_n$). We get τ by taking $\nu = 2$; in particular, τ is a rational representation of G defined over k, so that its kernel Λ is k-closed. Now fix a sufficiently large integer ν so that the kernel of $\bar{\omega}$ is precisely the center $\mathfrak{C}$ of G. If $\lambda \in \Lambda$ we have each $c^{(i)}_{0 \ldots 010 \ldots 0}(\lambda)$ equal to 1 or 0, according as the nonzero lower index is or is not in the i^{th} place, that is, we have

$$\bar{\omega}_\lambda \bar{f}_i = \bar{f}_i + (\textit{terms of degree} > 1 \textit{ in } \bar{f}_1, \ldots, \bar{f}_n).$$

It follows that if $\lambda \in \Lambda$ then

$$\bar{\omega}_\lambda(\bar{f}_1^{i_1} \ldots \bar{f}_n^{i_n}) = \bar{f}_1^{i_1} \ldots \bar{f}_n^{i_n} + (\textit{terms of total degree} > (i_1 + \ldots + i_n) \textit{ in } \bar{f}_1, \ldots, \bar{f}_n),$$

so $\bar{\omega}_\lambda$ is a unipotent matrix. Therefore $\bar{\omega}\Lambda$ is a nilpotent algebraic group. There is a rational isomorphism from $G/\mathfrak{C}$ to $\bar{\omega}G$, hence from $\Lambda/\mathfrak{C}$ to $\bar{\omega}\Lambda$, so $\Lambda/\mathfrak{C}$ is nilpotent. Since $\mathfrak{C}$ is central in Λ, Λ is nilpotent as an abstract group. Note that we have not yet used the linearity of G. If G is linear then clearly Λ is nilpotent as an algebraic group.

LEMMA 2. - *Let H be the subgroup of $GL(n)$ consisting of all matrices in $GL(n)$ all of whose entries directly below the upper left hand element are zero. Then if a ranges over all matrices in $GL(n)$ that are rational over the prime field, $\bigcap_a aHa^{-1}$ is the group of scalar matrices.*

Let V be the underlying vector space. Our intersection is characterized as the set of those invertible linear transformations on V which, when represented as matrices with respect to any basis of V consisting of vectors that are rational over the prime field, have only zeros below the first element. Let $v_1, \ldots, v_n$ be such a basis of V and let (x_{ij}) be in our intersection. Then $x_{i1} = 0$ for $i = 2, \ldots, n$. Replacing the basis $v_1, \ldots, v_n$ by the same vectors in different order, and doing this in all possible ways, shows that $x_{ij} = 0$ if $i \neq j$, so (x_{ij}) is a diagonal matrix. Replacing the basis $v_1, \ldots, v_n$ by the same basis, except for the replacement of v_i by $v_i + v_1$ $(i > 1)$, we get $x_{ii} = x_{11}$. Thus (x_{ij}) is scalar. It is clear that H is a group and that the group of scalar matrices is in our intersection.

THEOREM. – *If the connected linear algebraic group G is defined over the perfect field k, then $k(G)$ is k-isomorphic to a subfield of a purely transcendental extension of k.*

First suppose that G is solvable. Then its unipotent part G_u is connected and k-closed. Since k is perfect, G_u is defined over k. By Prop. 5, Cor. 2, k is a field of definition for the solvability of G_u. Taking the natural rational homomorphism $G \to G/G_u$ to be defined over k, the cross section theorem (cf. [5, Th. 10, Cor. 1]) implies that G is birationally equivalent over k to $G_u \times G/G_u$. But $k(G_u)$ is a purely transcendental extension of k by Prop. 8 and Prop. 10 is applicable to the torus G/G_u. This finishes the solvable case. Note that if G is solvable and k perfect and infinite then, since there exists a generically surjective rational map defined over k from an affine space to G, the points of G that are rational over k are dense in G. As a matter of fact, this last argument will apply to any connected linear algebraic group G defined over a perfect infinite field k, once the theorem has been proved; this will be stated explicitly as a corollary.

The general case of the theorem will depend on the following contentions, which apply to any connected k-closed algebraic group of matrices G, k an arbitrary field:

(A) Either G is solvable or it is generated by its K-closed connected proper subgroups, for some purely transcendental extension K of k.

(B) G is generated by its K-closed connected solvable subgroups, for some purely transcendental extension K of k.

(C) The K-closed points of G are dense in G, for some purely transcendental extension K of k.

Before proceeding with the proofs of (A), (B), and (C), we make a few preliminary remarks. First, since $GL(n)$ (for any n) is defined over the prime field, it makes sense to speak of a «k-closed algebraic group of matrices»; applied to a connected group, «k-closed» means «defined over a purely inseparable algebraic extension of k». A point is k-closed if and only if it is rational over a purely inseparable algebraic extension of k. If $G' \subset G$ are k-closed algebraic groups of matrices with G' normal in G, we may take the natural rational homomorphism $G \to G/G'$ to be defined over a purely inseparable algebraic extension of k; if G/G' is taken to be an algebraic group of matrices, it is then k-closed. Finally, for material on the generation of an algebraic group by subsets we refer to the end of § 1 of this paper.

We shall now prove (A), (B), and (C) simultaneously by induction on $\dim G$. If G it solvable then (A) and (B) are clear; (C) also holds since we may take K to be a simple transcendental extension of k, so that $K^{p^{-\infty}}$ is infinite ($p =$ characteristic of k if this is not zero, $p = 1$ if characteristic is zero) and our previous remarks on solvable groups obtain. In particular (A), (B), (C) hold if $\dim G \leq 1$. We now assume that G is a connected k-closed

algebraic group of matrices of dimension >1 and that our three contentions hold for all groups of smaller dimension, with any field k. We prove that (A) holds for G by distinguishing several cases.

First suppose that G contains a connected k-closed normal solvable subgroup G' of dimension >0. Take the natural homomorphism $\tau: G \to G/G'$ to be defined over a purely inseparable algebraic extension of k, and take G/G' to be a group of matrices. Then G/G' is k-closed and we may apply (B) to it to get a purely transcendental extension K of k and a family $|\Gamma|$ of K-closed connected solvable subgroups of G/G' that generate G/G'. The family of groups $|\tau^{-1}\Gamma|$ then consists of K-closed connected solvable subgroups of G that generate G, so (B) holds for G. Hence (A) holds for G.

Next suppose that G contains a connected k-closed normal subgroup G' of dimension >0 and such that G/G' is not solvable. Take the natural homomorphism $\tau: G \to G/G'$ to be defined over a purely inseparable algebraic extension of k and apply (A) to G/G' to get a purely transcendental extension K of k and a family $|\Gamma|$ of K-closed connected proper subgroups of G/G' that generate G/G'. Then $|\tau^{-1}\Gamma|$ is a family of K-closed connected proper subgroups of G that generate G, so (A) holds for G.

Now suppose that G contains an arbitrary connected k-closed proper normal subgroup G' of dimension >0. If the center $\mathfrak{C}$ of G has dimension >0 we can apply the first case treated above to the connected k-closed subgroup $\mathfrak{C}_0$ of G; hence we may suppose that $\mathfrak{C}$ is finite. If G/G' is not solvable the second case applies, so we may suppose that G/G' is solvable. Hence $[G/G', G/G'] \neq G/G'$. Thus $[G, G] \neq G$. Since $[G, G]$ is connected, k-closed, and normal in G, it is permissible to suppose that G/G' is commutative. Let U be the closed subset of G' consisting of all its unipotent elements. If we had $U = G'$ then G' would be solvable and a previous case would apply, so suppose $U \neq G'$. Since G' is connected and $\mathfrak{C}$ is finite, $G' \supset \mathfrak{C}U$. Applying (C) to G' we get a purely transcendental extension K of k and a K-closed point $P \in G'$, $P \notin \mathfrak{C}U$. Replacing P by its semisimple part if necessary, we can assume that P is K-closed and semisimple and $P \in G'$, $P \notin \mathfrak{C}$. The connected centralizer Γ of P in G is therefore a connected K-closed proper subgroup of G that contains a CARTAN subgroup of G (cf. [1, Ch. V]). Since $\Gamma G'$ is a normal algebraic subgroup of G that contains a CARTAN subgroup and the conjugates of any CARTAN subgroup are dense in G, we get $\Gamma G'$ dense in G. Hence $G = \Gamma G'$, proving (A) for the G of this paragraph.

To complete the proof of (A) for G, it remains to consider the case of a nonsolvable group G whose only k-closed connected normal subgroups are G and $|e|$. Let τ be the rational representation of G given by the action of its inner automorphisms on $\mathfrak{m}/\mathfrak{m}^2$, as in Lemma 1. By Lemma 1 the kernel of τ is finite. Furthermore the proof of the lemma shows that the map $\tau: G \to \tau G$ may be taken to be defined over a purely inseparable algebraic

extension of k, in which case τG is also a k-closed matrix group. We claim that it is sufficient to prove (A) for τG. For, since τG is not solvable, if (A) holds for τG then there exists a purely transcendental extension K of k such that τG is generated by its K-closed connected proper subgroups $|\Gamma|$. Then the connected subgroups $|(\tau^{-1}\Gamma)_0|$ of G are K-closed and proper and generate an algebraic subgroup of G which must be all of G, since its τ-image is all of τG. Hence, replacing G by τG if necessary, we may assume that $G \subset GL(n)$, where $n = \dim G$. Let H be the subgroup of $GL(n)$ considered in Lemma 2; H is a connected algebraic group defined over the prime field and of dimension $(n^2 - n + 1)$. If $g \in GL(n)$ then $g^{-1}Gg \subset H$ if and only if for each $\gamma \in G$ that is algebraic over k we have $g^{-1}\gamma g \in H$. Thus the totality of g' s in $GL(n)$ such that $G \subset gHg^{-1}$ is k-closed; by Lemma 2 and our assumptions on G, this a k-closed proper subset of $GL(n)$. Thus if u is generic for $GL(n)$ over k, we have $G \subset \bigcup uHu^{-1}$. For any u that is generic for $GL(n)$ over k we define $\Gamma_u = (G \cap uHu^{-1})_0$; this is a $k(u)$-closed connected proper subgroup of G of dimension $\geq n + (n^2 - n + 1) - n^2 = 1$. Let $u_1, u_2, \ldots$ be independent generic points of $GL(n)$ over k and let Γ be the subgroup of G generated by $\Gamma_{u_1}, \Gamma_{u_2}, \ldots$. Γ is generated by a finite subset of these groups, hence by $\Gamma_{u_1}, \Gamma_{u_2}, \ldots, \Gamma_{u_\nu}$ for some finite ν. Since $\Gamma_{u_{\nu+1}} \subset \Gamma$, we deduce that $\Gamma_u \subset \Gamma$ whenever u is generic for $GL(n)$ over $k(u_1, \ldots, u_\nu)$. If $v_1, \ldots, v_\nu$ are independent generic points of $GL(n)$ over $k(u_1, \ldots, u_\nu)$ and Γ' is the group generated by $\Gamma_{v_1}, \ldots, \Gamma_{v_\nu}$, we have $\Gamma' \subset \Gamma$; since their dimensions are clearly equal, $\Gamma' = \Gamma$. As a consequence Γ is k-closed. Hence $\Gamma_u \subset \Gamma$ for *any* u that is generic for $GL(n)$ over k. If $\gamma \in G$ is algebraic over k we have $\gamma\Gamma_u\gamma^{-1} = \gamma(G \cap uHu^{-1})_0\gamma^{-1} = (G \cap \gamma uHu^{-1}\gamma^{-1})_0 = \Gamma_{\gamma u} \subset \Gamma$, since γu is generic for $GL(n)$ over k. Applying this to $u = u_1, \ldots, u_\nu$, we get $\gamma\Gamma\gamma^{-1} \subset \Gamma$; this holds for all $\gamma \in G$ that are algebraic over k, hence for all $\gamma \in G$. Since Γ is k-closed and normal in G we must have $\Gamma = G$. Hence G is generated by its K-closed connected proper subgroups $\Gamma_{u_1}, \ldots, \Gamma_{u_\nu}$, where K is the purely transcendental extension $k(u_1, \ldots, u_\nu)$ of k. This completes the proof of (A) for G.

We now prove that (B) holds for G. This is trivial if G is solvable. Otherwise (A) gives us a purely transcendental extension K of k such that G is generated by its K-closed connected proper subgroups. Therefore G is generated by a finite number $\Gamma_1, \ldots, \Gamma_s$ of such K-closed connected proper subgroups. For each $i = 1, \ldots, s$, (B) applied to Γ_i and K shows that there exists a purely transcendental extension K_i of K such that Γ_i is generated by its K_i-closed connected solvable subgroups. If $K \subset K_i'$ and K_i' is K-isomorphic to K_i, then Γ_i is also generated by its K_i'-closed connected solvable subgroups. We may thus take $K_1, \ldots, K_s$ to be free over K, in which case the compositum $K_1 \ldots K_s$ is a purely transcendental extension of K, hence of k, and G is generated by its $K_1 \ldots K_s$-closed connected solvable subgroups. Hence (B) holds for G.

We prove that (C) holds for G: Using (B), find a purely transcendental extension K of k such that G is generated by its K-closed connected solvable subgroups $|\Gamma|$ and assume, as we may, that K is infinite. The set S of K-closed points of G is a subgroup of G, hence the smallest algebraic subset X of G containing S is an algebraic subgroup of G. For each $\Gamma \in |\Gamma|$ we already know that $S \cap \Gamma$ is dense in Γ. Hence $\Gamma \subset X$. Therefore X contains the subgroup generated by $|\Gamma|$, i. e. $X \supset G$. Thus S is dense in G. This proves (C), completing the induction process that proves the general validity of (A), (B), (C).

We shall now use (B) to prove the theorem. Let G, k be as given, and let $K = k(|x_\alpha|)$ (where the x_α's are algebraically independent over k) be such that G is generated by its K-closed connected solvable subgroups $|\Gamma|$. The field $K^{p^{-\infty}}$ (where, as usual, p is the field characteristic if this is not zero, and otherwise $p = 1$) is perfect and is a field of definition for each group in $|\Gamma|$. We know the theorem to hold for solvable groups. Since a suitable product of independent generic points over $K^{p^{-\infty}}$ of various groups in $|\Gamma|$ is generic for G over the same field, we can find a set $|y_\beta|$ of algebraically independent quantities over $K^{p^{-\infty}}$ and a point P rational over $K^{p^{-\infty}}(|y_\beta|)$ that is generic for G over $K^{p^{-\infty}}$. But P is rational over $K^{p^{-\nu}}(|y_\beta|)$ for a suitable integer $\nu \geq 0$, that is, since k is perfect, over the purely transcendental extension $k(|x_\alpha^{p^{-\nu}}, y_\beta|)$ of k. Since P is generic for G over k, the proof of the theorem is complete.

COROLLARY. - *If the connected linear algebraic group G is defined over the infinite perfect field k, then the points of G that are rational over k are dense in G.*

The proof of this has been indicated in the first paragraph of the proof of the theorem. Note that if the connected linear algebraic group G is defined over a field k which is not perfect, the theorem shows that there exists a finite purely inseparable algebraic extension k' of k such that $k'(G)$ is k'-isomorphic to a subfield of a purely transcendental extension of k'; since k is infinite in this case, we deduce that the points of G that are rational over k' are dense in G.

The purely transcendental extension of k in which we embed the function field $k(G)$ of the theorem may, a priori, be of very large transcendence degree over k. Since $k(G)$ is a finite extension of k, this transcendence degree may of course be taken to be finite. In fact, a result in CHEVALLEY's paper [2] shows that $k(G)$ is k-isomorphic to a subfield of a purely transcendental extension of k whose transcendence degree over k is $\dim G$ (or $(\dim G + 1)$ if k is finite). For the convenience of the reader we include this result as a proposition, giving a proof that is more geometric, and therefore, perhaps, somewhat more transparent, than the proof of SHIMURA given in [2].

PROPOSITION 11. - *If $k \subset K \subset k(x_1, \ldots, x_n)$ are fields, with k infinite, $x_1, \ldots, x_n$ algebraically independent over k, and K of transcendence degree r over k, then K is k-isomorphic to a subfield of $k(x_1, \ldots, x_r)$.*

It clearly suffices to show that if $r < n$, then K is k-isomorphic to a subfield of $k(x_1, \ldots, x_{n-1})$. Considering $(1, x_1, \ldots, x_n)$ as a generic point over k of a projective space P_n and letting V be a projective variety defined over k such that $k(V)$ is k-isomorphic to K, we get a generically surjective rational map $\tau: P_n \to V$ that is defined over k. We have only to show that if $\dim V < n$ then there exists a hyperplane H of P_n that is defined over k and such that τ induces a generically surjective map from H to V. Let x be a generic point of P_n over k, T the graph of τ on $P_n \times V$, and let X be a component of $\mathrm{pr}_{P_n}((P_n \times \tau x) \cap T)$ that contains x; then $\dim X \geq 1$. Let W be the k-closed proper subset of P_n consisting of the points at which τ is not defined and let $p_1, \ldots, p_s$ be a finite set of points of P_n, one chosen from each component of $X \cap W$. Since k is infinite, we can find a hyperplane H of P_n that has coefficients in k and contains no p_i, $i = 1, \ldots, s$. Since τ is defined at x, we have $X \subset\!\!\!| W$; since $\dim X \cap H = \dim X - 1$, we conclude that $X \cap H \subset\!\!\!| X \cap W$. If $y \in X \cap H$, $y \notin W$, we have $\tau y = \tau x$, which is generic for V over k; in particular, τ induces a generically surjective map from H to V.

Let G be a connected linear algebraic group defined over the infinite perfect field k. The regular elements of G [1, Ch. V] include a nonempty open subset of G, so the points of G that are rational over k and regular are dense in G. If $g \in G$ is regular, then the connected centralizer of g_s is a CARTAN subgroup of G containing g; if g is rational over k, so is g_s, hence also the connected centralizer of g_s. Hence G has CARTAN subgroups that are defined over k, and G is generated by the set of such CARTAN subgroups. The author does not know whether these same facts are true if k is a finite field (2).

Another consequence of the corollary is the following: In [3, pp. 117-119], CHEVALLEY discusses rational representations of his « groupes algébriques » (which are not quite the same as our algebraic groups) and shows that the kernel of such a representation has dimension less than or equal to what one would expect. He shows that equality holds when the base field is algebraically closed or of characteristic zero, but need not hold for a nonperfect base field. If one takes into account the differences in terminology, our corollary implies the equality in question whenever the base field is perfect.

---

(2) After the completion of this paper, SERRE communicated to the author the following proof that a connected linear algebraic group G that is defined over a finite field k has at least one CARTAN subgroup that is defined over k: Letting q be the number of elements of k, coordinatewise application of the FROBENIUS automorphism $x \to x^q$ defines a surjective rational isomorphism $g \to g^{(q)}$ from G to itself. If C is a CARTAN subgroup of G, then so is $C^{(q)}$, so we can write $C^{(q)} = aCa^{-1}$, for some $a \in G$. But a result of LANG says that the rational map from G to itself given by $g \to g^{(q)}g^{-1}$ is surjective, so there exists $b \in G$ such that $a = b^{(q)}b^{-1}$. Setting $C_1 = b^{-1}Cb$, we get $(C_1)^{(q)} = C_1$. Hence the CARTAN subgroup C_1 of G is defined over k. The same argument shows that G possesses at least one maximal connected solvable algebraic subgroup that is defined over k.

The corollary is false if any of the conditions on the algebraic group G and the field k is dropped. For if we drop the condition that k be infinite, then G has only a finite number of rational points. If we drop the condition that G be linear, an abelian variety with a finite number of rational points gives a counterexample: for example let k be the field of rational numbers and G the elliptic curve $x^3 + y^3 = 1$. A counterexample when G is not connected is got by taking k to be the real numbers and G the group of all matrices

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

with $a^2 + b^2 = \pm 1$. For an example of a connected linear algebraic group G that is defined over a nonperfect field k and does not have a dense set of rational points we proceed as follows: Let k_0 be any field of characteristic $p > 2$, let the quantity t be transcendental over k_0 and let $k = k_0(t)$. Let G be the subgroup of the plane $G_a \times G_a$ defined by the equation $y^p - y = tx^p$. G is defined over k and is biregularly isomorphic to G_a over the field $k(t^{1/p})$, having as an additive parameter the function $(y - t^{1/p}x)$, but we claim that G has only a finite number of points that are rational over k. For suppose $(\xi, \eta) \in G$, with $\xi, \eta \in k = k_0(t)$. Then the equation $\eta^p - \eta = t\xi^p$ implies

$$\frac{1}{t}\left(\left(\frac{1}{\eta}\right)^{p-1} - 1\right) \in k_0(t^p).$$

Differentiating with respect to t gives

$$1 = \left(\frac{1}{\eta}\right)^{p-2}\left(\left(\frac{1}{\eta}\right) + t\left(\frac{1}{\eta}\right)'\right).$$

Writing $\eta = u(t)/v(t)$, where $u, v \in k_0[t]$ are relatively prime polynomials, we see that any prime factor of $v(t)$ must divide 1, so $v(t) \in k_0$. Thus $\eta \in k_0[t]$. Hence $t\xi^p \in k_0[t]$, so $\xi \in k_0[t]$. Comparing terms of highest degree in the polynomial equation $\eta^p - \eta = t\xi^p$ gives $\xi = 0$. Thus the points of G that are rational over k are precisely the points $(0, i)$, $i = 0, 1, \ldots, p - 1$.

It is almost certainly true that if G is a connected linear algebraic group defined over an algebraically closed field k, then $k(G)$ is a purely transcendental extension of k. In [2], CHEVALLEY proves this if k has characteristic zero. We can reduce the proof of this for the case of arbitrary characteristic to either of the following equivalent statements, which are proved in the classical case by use of the theory of roots:

(S) If R is a maximal connected solvable algebraic subgroup of the connected linear algebraic group G, then the G-homogeneous space of left cosets G/R is prehomogeneous with respect to R.

(S′) If R is a maximal connected solvable algebraic subgroup of the connected linear algebraic group G, if K is a field of definition for G and R,

and g, r_1, r_2 are independent generic points over K of G, R, R respectively, then $r_1 g r_2$ is a generic point of G over $K(g)$.

Granting these, we can proceed as follows: Take a maximal connected solvable algebraic subgroup R of G that is defined over k (this can be done since k is algebraically closed) and take G/R and the natural map $G \to G/R$ also to be defined over k. Since k is a field of definition for the solvability of R, we know [5, Th. 10, Cor. 1] that G is birationally equivalent over k to $R \times G/R$. Prop. 8 shows that $k(R)$ is a purely transcendental extension of k, and Prop. 8 together with (S) shows the same for G/R. The same type of argument gives a very easy proof of the following fact, which is known only in the case of characteristic zero: if G is a connected linear algebraic group and V is a complete homogeneous space for G, all defined over the algebraically closed field k, then $k(V)$ is a purely transcendental extension of k. For if R is a maximal connected solvable algebraic subgroup of G that is defined over k, there exists a point of V that is rational over k and left fixed by R, hence V is a rational image of the left coset space G/R, therefore prehomogeneous with respect to R, so Prop. 8 applies.

4. On generalized jacobian varieties.

In this section we shall discuss generalized jacobian varieties with specific reference to fields of definition. This has also been done by IGUSA in [4], where the method of CHOW is used to construct generalized jacobians as projective varieties defined over the smallest field to be expected. Here we shall use the method WEIL has applied in [9] to the construction of the ordinary jacobian variety of a curve and, except for the question of projective embedding, shall derive some more specific results.

We assume, to avoid too long-winded an account, that the reader has at hand [6], [7], and [9], and merely indicate the necessary modifications in the various arguments used. A major difficulty is that some change in [7] is necessary to be able to handle the case of a curve having points that are simple with respect to some ground field, but not absolutely simple. The necessary modification is in Theorem 11 of [7]: one must add the statement that, under all the conditions of Theorem 11, if $\mathfrak{A}$ is a divisor of K/k that is prime to the places of $\mathfrak{o}$, then $r(\mathfrak{A})$ and $i(\mathfrak{A})$ remain unchanged when we extend the ground field from k to k' (i. e., we have to move part of the statement of Theorem 12 of [7] back to Theorem 11 and its weaker hypotheses). To prove this we use precisely the proof given for the corresponding part of Theorem 12 [7, p. 182], except that on line 20 of p. 182 the part « each $f_i \in K$ is a multiple of $\mathfrak{A}^{-1}$ » must be replaced by « each $f_i \in K$ is a multiple of $\mathfrak{A}^{-1}$, except possibly that f_i may have poles at the places of $\mathfrak{o}$ ». We remark that in IGUSA's paper [4, Lemma 2, p. 182] this point is seemingly bypassed, but this is an omission.

We now construct the generalized jacobian group of a curve. Let C be a complete curve defined over the field k and let $\mathfrak{o}$ be a semilocal subring of $k(C)$ which is the intersection of the local rings in $k(C)$ of a finite number of points of C, including all the singular points of C. Under these circumstances we say that our equivalence relation on C is defined over k; [7, Th. 11] and its modification in the preceding paragraph enable us to extend the ground field k in an arbitrary manner without destroying any of the basic properties of the equivalence relation on C associated with $\mathfrak{o}$. Lemmas 1, 2, 3 of [6, p. 515] go though without change. We can now apply the method of [9, § 7] to our equivalence relation on C; with a few trivial changes (such as replacing the genus g of C by its $\mathfrak{o}$-genus π) everything there applies directly to the present case, up through the end of the first paragraph on p. 510 of [9]. Thus we get a commutative connected algebraic group J that is defined over k, is a rational image over k of the direct product $C^{2\pi}$, and has certain other properties. Now let J' be the « generalized jacobian » of $\mathfrak{o}$, $\varphi: C \to J'$ the « canonical map », both as constructed in [6] and both defined over some extension field k' of k. One shows immediately that the characteristic properties of J' [6, pp. 518-519] are satisfied by J, so that J and J' are birationally equivalent over k', and in such a way that their group laws correspond. Thus J and J' are biregularly isomorphic, and hence we may identify J' with J. We then have a map $\varphi: C \to J$, but φ is defined over k', and not necessarily over k. If $M_1, \ldots, M_{2\pi}, N$ are independent generic points of C over k' and ψ is the map defined over k from $C^{2\pi}$ to J (ψ is denoted by φ on p. 509 of [9]), then $\varphi(M_1) - \varphi(N) = \psi(M_1, M_2, \ldots, M_{2\pi}) - \psi(N, M_2, \ldots, M_{2\pi})$. Since $\varphi(M_1) - \varphi(N)$ is independent of $M_2, \ldots, M_{2\pi}$ we get that for independent generic points M, N of C over k, $\varphi(M) - \varphi(N) \in J$ is rational over $k(M, N)$. Now apply [9, Prop. 4, p. 502] to the case $G = J$, $V = W = C$, $F(M, N) = \varphi(M) - \varphi(N)$. We obtain a principal homogeneous space U with respect to J and rational mappings f, g of C into U, all defined over k, such that $f(M) = F(M, N)g(N)$. Since φ is defined everywhere except at the singular points of C, we have $f(M) = F(M, M)g(M) = g(M)$; thus $f(M) = (\varphi(M) - \varphi(N))f(N)$. We now follow the procedure of the bottom of p. 511 and p. 512 of [9] to get a commutative group $\mathfrak{G}$ consisting of disjoint principal homogeneous spaces with respect to J such that $J, U \subset \mathfrak{G}$, $\mathfrak{G}/J$ is infinite cyclic, and each component of $\mathfrak{G}$ and all the group operations are defined over k. It now makes sense to write $f(M) - f(N) = \varphi(M) - \varphi(N)$ and, if we also denote by f its linear extension to divisors on C that are independent of the places of $\mathfrak{o}$, then the map $\mathfrak{A} \to f(\mathfrak{A})$ is a surjective isomorphism from divisor classes on C that are independent of the places of $\mathfrak{o}$ into $\mathfrak{G}$. Each component of $\mathfrak{G}$ represents divisor classes on C of a given degree (degree 0 for J and degree 1 for U), and we can write $\varphi(M) = f(M) - a$, where a is a fixed point of U. This group $\mathfrak{G}$, with all its structure, is the generalized jacobian group of C, and $f: C \to \mathfrak{G}$ is the canonical map.

We now indicate briefly how these results affect the results of our paper [6]. Things being as in the preceding paragraph, we first note that the original «canonical map» φ could have been taken to be defined over k if and only if U has a point that is rational over k; if this is the case we say that k is *complete for* $\mathfrak{o}$. (This is in accord with the definition given on p. 519 of [6], except that we have dropped the requirement that C have a complete nonsingular birational model over k). Theorem 7 of [6] and all its corollaries now hold under weaker conditions, namely that C carry a divisor of degree 1 that is rational over k (for in this case the independence of places gives a similar divisor that is independent of the places of $\mathfrak{o}$, and hence we get a rational point on U). Theorem 8, its corollaries, and Theorem 9 remain unaltered. (As a matter of fact, Theorem 8 can be strengthened as follows: If $\mathfrak{o} \subset \mathfrak{o}'$ are semilocal subrings of $k(C)$ such that the corresponding equivalence relations are defined over k, but k is not necessarily complete for $\mathfrak{o}$ or $\mathfrak{o}'$, if $\mathcal{G}$, $\mathcal{G}'$ are the corresponding generalized jacobian groups and f, f' the corresponding canonical maps, all defined over k, then there exist a natural surjective homomorphism $\tau: \mathcal{G} \to \mathcal{G}'$ such that $f' = \tau f$, and τ is rational and defined over k on each component of $\mathcal{G}$. Here τ is the extension of the natural map $f(C) \to f'(C)$. The τ of [6, § 4] is the restriction of the present τ to the component of the identity J of $\mathcal{G}$). The author does not know whether Theorem 10 is true under our more general conditions; however, the argument of the top of p. 524 shows that the first statement of Theorem 10, and also Corollary 1 of Theorem 10, hold if C has an infinity of points that are rational over k. But no change at all is necessary in Theorems 11 through 13.

If G is a connected algebraic group defined over the field k then there exists a unique maximal connected linear algebraic subgroup L of G, and L is k-closed. We can now give an easy example in which L is not defined over k: Let k be a nonperfect field of characteristic $p \neq 0$. Let C be a complete curve that is defined over k, of genus $g > 0$, is everywhere relatively simple with reference to k, but has singular points. (For example, if $p \neq 2$ we can take C to be a projective model that is relatively normal with reference to k of the field $k(x, y)$, where $y^2 = x(x-1)(x^p - a)$, a being an element of k that is not a p^{th} power. The genus of C is clearly 1, while the function field $k(x, y)/k$ has genus $(p+1)/2$). Consider the natural equivalence relation on C (got from the intersection of the local rings of its singular points) and let J be the generalized jacobian variety of C, J being taken to be defined over k. We claim that the maximal connected linear algebraic subgroup L of J is not defined over k. To show this, we may assume that C has a point that is rational over k, for otherwise we can replace k by a separable algebraic extension field, and this doesn't alter the situation. Thus we may assume that there exists a «canonical map» $\varphi: C \to J$, φ also being defined over k. If L is defined over k, then the natural rational homomorphism $\tau: J \to J/L$ can also be taken to be defined over k. By the results of [6, § 4],

J/L is the ordinary jacobian variety of C and $\tau\varphi: C \to J/L$ the ordinary « canonical map » of C into its jacobian variety. $\tau\varphi$ is then a birational map defined over k from C to a complete non-singular curve. This contradiction shows that L cannot be defined over k.

REFERENCES

[1] A. BOREL, *Groupes linéaires algébriques*, « Annals of Mathematics », vol. 64 (1956).
[2] C. CHEVALLEY, *On algebraic group varieties*, « Journal of the Mathematical Society of Japan », vol. 6 (1954).
[3] — — *Théorie des Groupes de Lie*, vol. II, Paris, 1951.
[4] J. IGUSA, *Fibre systems of jacobian varieties*, « American Journal of Mathematics », vol. 78 (1956).
[5] M. ROSENLICHT, *Some basic theorems on algebraic groups*, « American Journal of Mathematics », vol. 78 (1956).
[6] — — *Generalized jacobian varieties*, « Annals of Mathematics », vol. 59 (1954).
[7] — — *Equivalence relations on algebraic curves*, « Annals of Mathematics », vol. 56 (1952).
[8] A. WEIL, *On algebraic groups of transformations*, « American Journal of Mathematics », vol. 77 (1955).
[9] — — *On algebraic groups and homogeneous spaces*, « American Journal of Mathematics », vol. 77 (1955).
[10] — — *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publication, New York, 1946.